



Panduan Developer

AWS Lambda



AWS Lambda: Panduan Developer

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

| | |
|--|----|
| Apa itu AWS Lambda? | 1 |
| Kapan menggunakan Lambda | 1 |
| Fitur utama | 2 |
| Buat fungsi pertama Anda | 4 |
| Prasyarat | 4 |
| Membuat fungsi Lambda dengan konsol | 6 |
| Memanggil fungsi Lambda menggunakan konsol | 12 |
| Bersihkan | 15 |
| Sumber daya tambahan dan langkah selanjutnya | 16 |
| Buat aplikasi pertama Anda | 18 |
| Prasyarat | 20 |
| Mengunduh contoh file aplikasi | 20 |
| Menerapkan aplikasi | 28 |
| Menyebarkan sumber daya secara manual | 28 |
| Menyebarkan sumber daya menggunakan AWS SAM | 36 |
| Menguji aplikasi | 38 |
| Menguji aplikasi secara manual | 38 |
| Menguji aplikasi dengan skrip otomatis | 40 |
| Langkah selanjutnya | 41 |
| Konsep Lambda Utama | 43 |
| Fungsi | 43 |
| Pemicu | 43 |
| Peristiwa | 44 |
| Lingkungan eksekusi | 44 |
| Paket deployment | 45 |
| Waktu Aktif | 45 |
| Lapisan | 45 |
| Konkurensi | 46 |
| Pengualifikasi | 46 |
| Tujuan | 47 |
| Infrastruktur sebagai kode (IAC) | 48 |
| Alat IAC untuk Lambda | 48 |
| Memulai dengan IAC untuk Lambda | 50 |
| Prasyarat | 51 |

| | |
|---|-----|
| Buat fungsi Lambda | 51 |
| Lihat AWS SAM template untuk fungsi Anda | 52 |
| Gunakan Komposer Aplikasi AWS untuk mendesain aplikasi tanpa server | 54 |
| Terapkan aplikasi tanpa server Anda menggunakan AWS SAM (opsional) | 59 |
| Menguji aplikasi yang Anda gunakan (opsional) | 62 |
| Langkah selanjutnya | 63 |
| Daerah yang didukung untuk integrasi Lambda dengan Application Composer | 63 |
| Model pemrograman | 65 |
| Waktu aktif Lambda | 67 |
| Waktu aktif yang didukung | 67 |
| Rilis runtime baru | 70 |
| Kebijakan penghentian runtime | 70 |
| Model tanggung jawab bersama | 71 |
| Penggunaan runtime setelah penghentian | 73 |
| Menerima pemberitahuan penghentian runtime | 74 |
| Waktu pengoperasian terdepresiasi | 75 |
| Pembaruan versi runtime | 78 |
| Mode pembaruan runtime | 79 |
| Peluncuran versi runtime dua fase | 80 |
| Mengkonfigurasi manajemen runtime | 81 |
| Versi runtime roll-back | 82 |
| Mengidentifikasi perubahan versi runtime Lambda | 83 |
| Model tanggung jawab bersama | 85 |
| Izin | 87 |
| Dapatkan data tentang fungsi berdasarkan runtime | 88 |
| Daftar versi fungsi yang menggunakan runtime tertentu | 88 |
| Mengidentifikasi fungsi yang paling umum dan paling baru dipanggil | 90 |
| Modifikasi waktu pengoperasian | 95 |
| Variabel lingkungan spesifik bahasa | 95 |
| Skrip pembungkus | 95 |
| Runtime API | 99 |
| Invokasi berikutnya | 99 |
| Respons invokasi | 101 |
| Kesalahan inisialisasi | 101 |
| Kesalahan invokasi | 103 |
| Runtime khusus OS | 105 |

| | |
|---|-----|
| Membangun runtime kustom | 106 |
| Tutorial runtime kustom | 110 |
| Lingkungan eksekusi | 119 |
| Siklus hidup lingkungan runtime | 120 |
| Fase inisialisasi | 120 |
| Kegagalan selama fase Init | 121 |
| Fase pemulihan (hanya Lambda SnapStart) | 122 |
| Fase invokasi | 122 |
| Kegagalan selama fase pemanggilan | 123 |
| Fase pematian | 125 |
| Menerapkan tanpa kewarganegaraan | 126 |
| Mengkonfigurasi fungsi | 128 |
| arsip file .zip | 130 |
| Membuat fungsi | 130 |
| Menggunakan editor kode konsol | 132 |
| Memperbarui kode fungsi | 132 |
| Mengubah runtime | 133 |
| Mengubah arsitektur | 133 |
| Menggunakan Lambda API | 134 |
| AWS CloudFormation | 134 |
| Gambar kontainer | 136 |
| Persyaratan | 137 |
| Menggunakan gambar AWS dasar | 138 |
| Menggunakan gambar AWS dasar khusus OS | 139 |
| Menggunakan gambar AWS non-dasar | 140 |
| Klien antarmuka runtime | 140 |
| ECR Izin Amazon | 141 |
| Siklus hidup fungsi | 144 |
| Memori | 145 |
| Kapan harus menambah memori | 145 |
| Menggunakan konsol | 146 |
| Menggunakan AWS CLI | 146 |
| Menggunakan AWS SAM | 147 |
| Menerima rekomendasi memori fungsi (konsol) | 147 |
| Penyimpanan sementara | 148 |
| Kasus penggunaan | 148 |

| | |
|---|-----|
| Menggunakan konsol | 149 |
| Menggunakan AWS CLI | 149 |
| Menggunakan AWS SAM | 150 |
| Set instruksi (ARM/x86) | 151 |
| Keuntungan menggunakan arsitektur arm64 | 151 |
| Persyaratan untuk migrasi ke arsitektur arm64 | 152 |
| Kompatibilitas kode fungsi dengan arsitektur arm64 | 152 |
| Cara bermigrasi ke arsitektur arm64 | 152 |
| Mengkonfigurasi arsitektur set instruksi | 153 |
| Waktu habis | 155 |
| Kapan harus menambah batas waktu | 155 |
| Menggunakan konsol | 156 |
| Menggunakan AWS CLI | 156 |
| Menggunakan AWS SAM | 156 |
| Mengonfigurasi variabel lingkungan | 158 |
| Variabel lingkungan runtime yang ditetapkan | 162 |
| Contoh skenario untuk variabel lingkungan | 164 |
| Mengamankan variabel lingkungan | 164 |
| Mengambil variabel lingkungan | 167 |
| Melampirkan fungsi ke a VPC | 169 |
| Diperlukan izin IAM | 169 |
| Melampirkan fungsi Lambda ke Amazon VPC di Anda Akun AWS | 171 |
| Akses internet saat dilampirkan ke VPC | 175 |
| IPv6dukungan | 175 |
| Praktik terbaik untuk menggunakan Lambda dengan Amazon VPCs | 176 |
| Memahami Antarmuka Jaringan Elastis Hyperplane () ENIs | 177 |
| Menggunakan tombol IAM kondisi untuk VPC pengaturan | 178 |
| VPCtutorial | 183 |
| Akses internet untuk VPC fungsi | 184 |
| Jaringan masuk | 209 |
| Pertimbangan untuk titik akhir antarmuka Lambda | 209 |
| Membuat titik akhir antarmuka untuk Lambda | 210 |
| Membuat kebijakan titik akhir antarmuka untuk Lambda | 212 |
| Sistem file | 214 |
| Peran eksekusi dan izin pengguna | 214 |
| Mengonfigurasi sistem file dan titik akses | 215 |

| | |
|--|-----|
| Menyambung ke sistem file (konsol) | 216 |
| Alias | 218 |
| Menggunakan alias | 220 |
| Konfigurasi perutean | 221 |
| Versi | 224 |
| Membuat versi fungsi | 225 |
| Menggunakan versi | 226 |
| Memberi izin | 227 |
| Tag | 228 |
| Izin | 228 |
| Menggunakan tag dengan konsol | 228 |
| Menggunakan tag dengan AWS CLI | 231 |
| Persyaratan untuk tag | 232 |
| Streaming respons | 233 |
| Batas bandwidth untuk streaming respons | 234 |
| Fungsi menulis | 234 |
| Memanggil fungsi | 236 |
| Tutorial: Membuat fungsi streaming respons dengan URL fungsi | 237 |
| Memanggil fungsi | 242 |
| Memanggil fungsi secara sinkron | 244 |
| Invokasi asinkron | 248 |
| Penanganan kesalahan | 249 |
| Konfigurasi | 250 |
| Mempertahankan catatan | 252 |
| Pemetaan sumber peristiwa | 259 |
| Pemetaan dan pemicu sumber peristiwa | 259 |
| Perilaku batching | 260 |
| API pemetaan sumber kejadian | 263 |
| Penyaringan acara | 264 |
| Memahami dasar-dasar penyaringan acara | 265 |
| Menangani catatan yang tidak memenuhi kriteria filter | 267 |
| Filter sintaks aturan | 268 |
| Melampirkan kriteria filter ke pemetaan sumber peristiwa (konsol) | 270 |
| Melampirkan kriteria filter ke pemetaan sumber peristiwa (AWS CLI) | 271 |
| Melampirkan kriteria filter ke pemetaan sumber peristiwa (AWS SAM) | 272 |
| Enkripsi kriteria filter | 272 |

| | |
|--|-----|
| Menggunakan filter dengan berbeda AWS layanan | 279 |
| Pengujian di konsol | 280 |
| Memanggil fungsi dengan acara pengujian | 280 |
| Membuat acara pengujian pribadi | 281 |
| Membuat acara uji yang dapat dibagikan | 281 |
| Menghapus skema acara uji yang dapat dibagikan | 283 |
| Status fungsi | 284 |
| Status fungsi saat memperbarui | 285 |
| Percobaan ulang | 287 |
| Deteksi loop rekursif | 289 |
| Memahami deteksi loop rekursif | 289 |
| Didukung AWS layanan dan SDKs | 291 |
| Pemberitahuan loop rekursif | 293 |
| Menanggapi notifikasi deteksi loop rekursif | 294 |
| Mengizinkan fungsi Lambda berjalan dalam loop rekursif | 295 |
| Wilayah yang didukung untuk deteksi loop rekursif Lambda | 297 |
| Fungsi URLs | 299 |
| Membuat fungsi URL (konsol) | 300 |
| Membuat fungsi URL (AWS CLI) | 302 |
| Menambahkan fungsi URL ke CloudFormation template | 302 |
| Berbagi sumber daya lintas asal () CORS | 304 |
| Fungsi pelambatan URLs | 305 |
| Menonaktifkan fungsi URLs | 306 |
| Menghapus fungsi URLs | 306 |
| Kontrol akses | 307 |
| Fungsi pemanggilan URLs | 315 |
| URL fungsi pemantauan | 327 |
| Tutorial: Membuat fungsi dengan URL fungsi | 329 |
| Penskalaan fungsi | 334 |
| Memahami dan memvisualisasikan konkurensi | 334 |
| Menghitung konkurensi untuk suatu fungsi | 339 |
| Memahami konkurensi cadangan dan konkurensi yang disediakan | 341 |
| Konkurensi terpesan | 341 |
| Konkurensi terprovisi | 343 |
| Bagaimana Lambda mengalokasikan konkurensi yang disediakan | 348 |
| Membandingkan konkurensi cadangan dan konkurensi yang disediakan | 349 |

| | |
|--|-----|
| Memahami konkurensi dan permintaan per detik | 350 |
| Kuota konkurensi | 352 |
| Mengonfigurasi konkurensi terpesan | 354 |
| Mengonfigurasi konkurensi terpesan | 355 |
| Memperkirakan secara akurat konkurensi cadangan yang diperlukan untuk suatu fungsi | 356 |
| Mengonfigurasi konkurensi yang tersedia | 358 |
| Mengonfigurasi konkurensi yang tersedia | 359 |
| Memperkirakan konkurensi yang disediakan secara akurat untuk suatu fungsi | 361 |
| Mengoptimalkan kode fungsi saat menggunakan konkurensi yang disediakan | 362 |
| Menggunakan variabel lingkungan untuk melihat dan mengontrol perilaku konkurensi yang disediakan | 363 |
| Memahami perilaku pencatatan dan penagihan dengan konkurensi yang disediakan | 363 |
| Menggunakan Application Auto Scaling untuk mengotomatiskan manajemen konkurensi yang disediakan | 364 |
| Perilaku penskalaan | 368 |
| Tingkat penskalaan konkurensi | 368 |
| Memantau konkurensi | 370 |
| Metrik konkurensi umum | 370 |
| Metrik konkurensi terprovisi | 370 |
| Bekerja dengan ClaimedAccountConcurrency metrik | 373 |
| Membangun dengan Node.js | 377 |
| Inisialisasi Node.js | 379 |
| Menunjuk penanganan fungsi sebagai modul ES | 379 |
| Versi termasuk runtime SDK | 380 |
| Menggunakan keep-alive | 380 |
| Pemuatan sertifikat CA | 381 |
| Handler | 382 |
| Dasar-dasar penanganan Node.js | 382 |
| Penamaan | 383 |
| Menggunakan async/await | 384 |
| Menggunakan callback | 386 |
| Praktik terbaik kode untuk fungsi Lambda Node.js | 389 |
| Deploy arsip file .zip | 391 |
| Dependensi runtime di Node.js | 391 |
| Membuat paket penerapan.zip tanpa dependensi | 392 |
| Membuat paket penerapan.zip dengan dependensi | 392 |

| | |
|--|-----|
| Membuat layer Node.js untuk dependensi Anda | 393 |
| Jalur pencarian ketergantungan dan pustaka yang disertakan runtime | 394 |
| Membuat dan memperbarui fungsi Lambda Node.js menggunakan file.zip | 395 |
| Deploy gambar kontainer | 402 |
| AWS gambar dasar untuk Node.js | 403 |
| Menggunakan gambar AWS dasar | 404 |
| Menggunakan gambar AWS non-dasar | 410 |
| Konteks | 420 |
| Pencatatan log | 422 |
| Membuat fungsi yang mengembalikan log | 422 |
| Menggunakan kontrol logging lanjutan Lambda dengan Node.js | 424 |
| Melihat log di konsol Lambda | 430 |
| Melihat log di CloudWatch konsol | 430 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 431 |
| Menghapus log | 434 |
| Pelacakan | 435 |
| Menggunakan ADOT untuk menginstruksikan fungsi Node.js Anda | 436 |
| Menggunakan X-Ray SDK untuk instrumen fungsi Node.js Anda | 436 |
| Mengaktifkan penelusuran dengan konsol Lambda | 437 |
| Mengaktifkan penelusuran dengan Lambda API | 438 |
| Mengaktifkan penelusuran dengan AWS CloudFormation | 438 |
| Menafsirkan jejak X-Ray | 439 |
| Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK | 442 |
| Membangun dengan TypeScript | 443 |
| Lingkungan pengembangan | 444 |
| Handler | 446 |
| Dasar-dasar penanganan TypeScript | 446 |
| Menggunakan async/await | 447 |
| Menggunakan callback | 448 |
| Menggunakan tipe untuk objek acara | 450 |
| Praktik terbaik kode untuk fungsi Lambda TypeScript | 451 |
| Deploy arsip file .zip | 453 |
| Menggunakan AWS SAM | 453 |
| Menggunakan AWS CDK | 455 |
| Menggunakan AWS CLI dan esbuild | 458 |
| Deploy gambar kontainer | 461 |

| | |
|--|-----|
| Menggunakan image dasar Node.js untuk membangun dan mengemas kode TypeScript fungsi | 461 |
| Konteks | 469 |
| Pencatatan log | 471 |
| Alat dan pustaka | 471 |
| Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS SAM untuk logging terstruktur | 472 |
| Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS CDK untuk logging terstruktur | 474 |
| Melihat log di konsol Lambda | 478 |
| Melihat log di CloudWatch konsol | 478 |
| Pelacakan | 480 |
| Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS SAM untuk tracing | 481 |
| Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS CDK for tracing | 483 |
| Menafsirkan jejak X-Ray | 487 |
| Membangun dengan Python | 488 |
| Versi yang disertakan runtime SDK | 489 |
| Format respons | 490 |
| Shutdown anggun untuk ekstensi | 490 |
| Handler | 491 |
| Penamaan | 491 |
| Cara kerjanya | 492 |
| Mengembalikan nilai | 492 |
| Contoh | 493 |
| Praktik terbaik kode untuk fungsi Lambda Python | 495 |
| Deploy arsip file .zip | 498 |
| Dependensi runtime dengan Python | 498 |
| Membuat paket penerapan.zip tanpa dependensi | 499 |
| Membuat paket penerapan.zip dengan dependensi | 500 |
| Jalur pencarian ketergantungan dan pustaka yang disertakan runtime | 502 |
| Menggunakan folder <code>__pycache__</code> | 504 |
| Membuat paket penerapan.zip dengan pustaka asli | 504 |
| Membuat dan memperbarui fungsi Lambda Python menggunakan file.zip | 505 |
| Deploy gambar kontainer | 513 |
| AWS gambar dasar untuk Python | 514 |
| Menggunakan gambar AWS dasar | 516 |

| | |
|--|-----|
| Menggunakan gambar AWS non-dasar | 522 |
| Lapisan | 532 |
| Prasyarat | 532 |
| Kompatibilitas lapisan Python dengan Amazon Linux | 533 |
| Jalur lapisan untuk runtime Python | 534 |
| Mengemas konten lapisan | 534 |
| Membuat layer | 536 |
| Menambahkan layer ke fungsi Anda | 536 |
| Bekerja dengan distribusi manylinux roda | 539 |
| Konteks | 544 |
| Log dan pantau fungsi Python Lambda | 546 |
| Mencetak ke log | 546 |
| Menggunakan pustaka logging | 547 |
| Menggunakan kontrol logging lanjutan Lambda dengan Python | 549 |
| Melihat log di konsol Lambda | 553 |
| Melihat log di CloudWatch konsol | 554 |
| Melihat log dengan AWS CLI | 554 |
| Menghapus log | 557 |
| Alat dan pustaka | 558 |
| Menggunakan Powertools untuk AWS Lambda (Python) AWS SAM dan untuk logging terstruktur | 558 |
| Menggunakan Powertools untuk AWS Lambda (Python) AWS CDK dan untuk logging terstruktur | 562 |
| Pengujian | 569 |
| Menguji aplikasi tanpa server Anda | 570 |
| Pelacakan | 572 |
| Menggunakan Powertools untuk AWS Lambda (Python) AWS SAM dan untuk melacak | 573 |
| Menggunakan Powertools untuk AWS Lambda (Python) dan AWS CDK untuk melacak | 576 |
| Menggunakan ADOT untuk instrumen fungsi Python Anda | 581 |
| Menggunakan X-Ray SDK untuk instrumen fungsi Python Anda | 581 |
| Mengaktifkan penelusuran dengan konsol Lambda | 582 |
| Mengaktifkan penelusuran dengan Lambda API | 582 |
| Mengaktifkan penelusuran dengan AWS CloudFormation | 583 |
| Menafsirkan jejak X-Ray | 583 |
| Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK | 586 |
| Membangun dengan Ruby | 588 |

| | |
|---|-----|
| Versi yang disertakan runtime SDK | 589 |
| Mengaktifkan Ruby JIT Lainnya () YJIT | 590 |
| Handler | 591 |
| Dasar-dasar penanganan Ruby | 591 |
| Praktik terbaik kode untuk fungsi Ruby Lambda | 592 |
| Deploy arsip file .zip | 595 |
| Dependensi di Ruby | 595 |
| Membuat paket penerapan.zip tanpa dependensi | 596 |
| Membuat paket penerapan.zip dengan dependensi | 596 |
| Membuat layer Ruby untuk dependensi Anda | 598 |
| Membuat paket penerapan.zip dengan pustaka asli | 599 |
| Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip | 601 |
| Deploy gambar kontainer | 608 |
| AWS gambar dasar untuk Ruby | 609 |
| Menggunakan gambar AWS dasar | 609 |
| Menggunakan gambar AWS non-dasar | 616 |
| Konteks | 626 |
| Pencatatan log | 627 |
| Membuat fungsi yang mengembalikan log | 627 |
| Melihat log di konsol Lambda | 628 |
| Melihat log di CloudWatch konsol | 629 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 629 |
| Menghapus log | 632 |
| Bekerja dengan pustaka logger Ruby | 633 |
| Pelacakan | 634 |
| Mengaktifkan penelusuran aktif dengan Lambda API | 639 |
| Mengaktifkan penelusuran aktif dengan AWS CloudFormation | 640 |
| Menyimpan dependensi runtime dalam satu lapisan | 640 |
| Membangun dengan Java | 642 |
| Handler | 645 |
| Contoh handler: Java 17 runtime | 645 |
| Contoh handler: Java 11 runtime dan di bawahnya | 647 |
| Kode inisialisasi | 648 |
| Memilih tipe input dan output | 649 |
| Antarmuka handler | 650 |
| Praktik terbaik kode untuk fungsi Java Lambda | 652 |

| | |
|---|-----|
| Kode handler sampel | 654 |
| Deploy arsip file .zip | 656 |
| Prasyarat | 656 |
| Alat dan pustaka | 656 |
| Membangun paket deployment dengan Gradle | 658 |
| Membuat layer Java untuk dependensi Anda | 659 |
| Membangun paket deployment dengan Maven | 660 |
| Mengunggah paket penerapan dengan konsol Lambda | 662 |
| Mengunggah paket penerapan dengan AWS CLI | 664 |
| Mengunggah paket penerapan dengan AWS SAM | 666 |
| Deploy gambar kontainer | 668 |
| AWS gambar dasar untuk Java | 669 |
| Menggunakan gambar AWS dasar | 670 |
| Menggunakan gambar AWS non-dasar | 679 |
| Lapisan | 691 |
| Prasyarat | 691 |
| Kompatibilitas lapisan Java dengan Amazon Linux | 692 |
| Jalur lapisan untuk runtime Java | 692 |
| Mengemas konten lapisan | 693 |
| Membuat layer | 695 |
| Menambahkan layer ke fungsi Anda | 696 |
| Lambda SnapStart | 700 |
| Fitur yang didukung dan batasan | 701 |
| Wilayah yang Didukung | 701 |
| Pertimbangan kompatibilitas | 702 |
| Harga | 703 |
| SnapStart dan konkurensi yang disediakan | 703 |
| Sumber daya tambahan | 704 |
| Mengaktifkan SnapStart | 705 |
| Menangani keunikan | 711 |
| Kait runtime | 714 |
| Pemantauan | 717 |
| Model keamanan | 720 |
| Praktik terbaik | 721 |
| Kustomisasi Java | 724 |
| Memahami variabel JAVA_TOOL_OPTIONS lingkungan | 724 |

| | |
|--|-----|
| Konteks | 727 |
| Konteks dalam aplikasi sampel | 729 |
| Pencatatan log | 731 |
| Membuat fungsi yang mengembalikan log | 731 |
| Menggunakan kontrol logging lanjutan Lambda dengan Java | 733 |
| Menerapkan logging lanjutan dengan Log4j2 dan SLF4J | 736 |
| Alat dan pustaka | 740 |
| Menggunakan Powertools untuk AWS Lambda (Java) dan AWS SAM untuk logging terstruktur | 740 |
| Melihat log di konsol Lambda | 744 |
| Melihat log di CloudWatch konsol | 745 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 745 |
| Menghapus log | 748 |
| Kode pencatatan sampel | 749 |
| Pelacakan | 750 |
| Menggunakan Powertools untuk AWS Lambda (Java) dan AWS SAM untuk melacak | 751 |
| Menggunakan Powertools untuk AWS Lambda (Java) dan AWS CDK untuk melacak | 753 |
| Menggunakan ADOT untuk instrumen fungsi Java Anda | 765 |
| Menggunakan X-Ray SDK untuk instrumen fungsi Java Anda | 765 |
| Mengaktifkan penelusuran dengan konsol Lambda | 766 |
| Mengaktifkan penelusuran dengan Lambda API | 766 |
| Mengaktifkan penelusuran dengan AWS CloudFormation | 767 |
| Menafsirkan jejak X-Ray | 767 |
| Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK | 770 |
| Penelusuran X-Ray dalam aplikasi sampel (SDKX-Ray) | 771 |
| Aplikasi sampel | 773 |
| Membangun dengan Go | 775 |
| Dukungan runtime Go | 775 |
| Alat dan pustaka | 776 |
| Handler | 777 |
| Dasar-dasar Go handler | 777 |
| Penamaan | 779 |
| Handler fungsi Lambda menggunakan tipe terstruktur | 779 |
| Menggunakan status global | 781 |
| Praktik terbaik kode untuk fungsi Go Lambda | 783 |
| Konteks | 785 |

| | |
|---|-----|
| Mengakses informasi konteks aktif | 785 |
| Deploy arsip file .zip | 788 |
| Membuat file .zip pada macOS dan Linux | 788 |
| Membuat file .zip pada Windows | 790 |
| Membuat dan memperbarui fungsi Go Lambda menggunakan file.zip | 793 |
| Deploy gambar kontainer | 800 |
| AWS gambar dasar untuk menerapkan fungsi Go | 800 |
| Klien antarmuka Go runtime | 801 |
| Menggunakan gambar AWS dasar khusus OS | 801 |
| Menggunakan gambar AWS non-dasar | 809 |
| Lapisan | 818 |
| Pencatatan log | 819 |
| Membuat fungsi yang mengembalikan log | 819 |
| Melihat log di konsol Lambda | 821 |
| Melihat log di CloudWatch konsol | 821 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 821 |
| Menghapus log | 825 |
| Pelacakan | 826 |
| Menggunakan ADOT untuk instrumen fungsi Go Anda | 827 |
| Menggunakan X-Ray SDK untuk instrumen fungsi Go Anda | 827 |
| Mengaktifkan penelusuran dengan konsol Lambda | 827 |
| Mengaktifkan penelusuran dengan Lambda API | 828 |
| Mengaktifkan penelusuran dengan AWS CloudFormation | 828 |
| Menafsirkan jejak X-Ray | 829 |
| Membangun dengan C # | 833 |
| Lingkungan pengembangan | 833 |
| Menginstal template proyek.NET | 833 |
| Menginstal dan memperbarui alat CLI | 834 |
| Handler | 835 |
| .NETmodel eksekusi untuk Lambda | 835 |
| Penangan perpustakaan kelas | 836 |
| Penangan perakitan yang dapat dieksekusi | 837 |
| Serialisasi dalam fungsi Lambda | 838 |
| Sederhanakan kode fungsi dengan kerangka kerja Anotasi Lambda | 840 |
| Pembatasan handler fungsi Lambda | 843 |
| Praktik terbaik kode untuk fungsi C# Lambda | 843 |

| | |
|---|-----|
| Paket deployment | 846 |
| NET Lambda Global CLI | 847 |
| AWS SAM | 853 |
| AWS CDK | 856 |
| ASP.NET | 860 |
| Deploy gambar kontainer | 866 |
| AWS gambar dasar untuk .NET | 867 |
| Menggunakan gambar AWS dasar | 867 |
| Menggunakan gambar AWS non-dasar | 870 |
| Kompilasi AOT asli | 874 |
| waktu aktif Lambda | 874 |
| Prasyarat | 875 |
| Memulai | 875 |
| Serialisasi | 878 |
| Pemangkasan | 879 |
| Pemecahan Masalah | 880 |
| Konteks | 881 |
| Pencatatan log | 883 |
| Membuat fungsi yang mengembalikan log | 883 |
| Alat dan pustaka | 884 |
| Menggunakan Powertools untuk AWS Lambda (.NET) dan AWS SAM untuk logging terstruktur | 884 |
| Melihat log di konsol Lambda | 887 |
| Melihat log di CloudWatch konsol | 887 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 888 |
| Menghapus log | 891 |
| Pelacakan | 892 |
| Menggunakan Powertools untuk AWS Lambda (.NET) dan AWS SAM untuk melacak | 893 |
| Menggunakan X-Ray SDK untuk instrumen Anda .NET fungsi | 896 |
| Mengaktifkan penelusuran dengan konsol Lambda | 897 |
| Mengaktifkan penelusuran dengan Lambda API | 898 |
| Mengaktifkan penelusuran dengan AWS CloudFormation | 898 |
| Menafsirkan jejak X-Ray | 899 |
| Pengujian | 902 |
| Menguji aplikasi tanpa server | 903 |
| Membangun dengan PowerShell | 907 |

| | |
|--|-----|
| Lingkungan Pengembangan | 909 |
| Paket deployment | 910 |
| Membuat fungsi Lambda | 910 |
| Handler | 912 |
| Mengembalikan data | 913 |
| Konteks | 914 |
| Pencatatan log | 915 |
| Membuat fungsi yang mengembalikan log | 915 |
| Melihat log di konsol Lambda | 917 |
| Melihat log di CloudWatch konsol | 917 |
| Melihat log menggunakan AWS Command Line Interface (AWS CLI) | 918 |
| Menghapus log | 921 |
| Membangun dengan Karat | 922 |
| Handler | 924 |
| Dasar-dasar penanganan karat | 924 |
| Menggunakan status bersama | 925 |
| Praktik terbaik kode untuk fungsi Rust Lambda | 926 |
| Konteks | 929 |
| Mengakses informasi konteks aktif | 929 |
| Acara HTTP | 931 |
| Deploy arsip file .zip | 934 |
| Prasyarat | 934 |
| Membangun fungsi | 934 |
| Menerapkan fungsi | 935 |
| Memanggil fungsi | 937 |
| Pencatatan log | 939 |
| Membuat fungsi yang menulis log | 939 |
| Menerapkan logging lanjutan dengan peti Tracing | 939 |
| Praktik terbaik | 942 |
| Kode fungsi | 942 |
| Konfigurasi fungsi | 943 |
| Skalabilitas fungsi | 945 |
| Metrik dan alarm | 945 |
| Bekerja dengan stream | 946 |
| Praktik terbaik keamanan | 947 |
| Menguji fungsi tanpa server | 948 |

| | |
|---|------|
| Hasil bisnis yang ditargetkan | 949 |
| Apa yang harus diuji | 949 |
| Cara menguji tanpa server | 950 |
| Teknik pengujian | 951 |
| Pengujian di cloud | 952 |
| Menguji dengan tiruan | 954 |
| Pengujian dengan emulasi | 956 |
| Praktik terbaik | 957 |
| Prioritaskan pengujian di cloud | 957 |
| Struktur kode Anda untuk pengujian | 957 |
| Mempercepat loop umpan balik pengembangan | 958 |
| Fokus pada tes integrasi | 958 |
| Buat lingkungan pengujian yang terisolasi | 959 |
| Gunakan tiruan untuk logika bisnis yang terisolasi | 960 |
| Gunakan emulator dengan hemat | 961 |
| Tantangan pengujian secara lokal | 961 |
| Contoh: Fungsi Lambda membuat bucket S3 | 961 |
| Contoh: Fungsi Lambda memproses pesan dari antrian Amazon SQS | 962 |
| FAQ | 963 |
| Langkah dan sumber daya selanjutnya | 964 |
| Mengintegrasikan layanan lain | 965 |
| Membuat pemicu | 965 |
| Daftar layanan | 966 |
| Apache Kafka | 969 |
| Contoh peristiwa | 970 |
| Konfigurasi sumber acara | 971 |
| Memproses pesan | 980 |
| Penyaringan acara | 987 |
| Destinasi yang gagal | 993 |
| Pemecahan Masalah | 997 |
| API Gerbang | 1001 |
| Memilih API tipe | 1001 |
| Menambahkan titik akhir ke fungsi Lambda Anda | 1004 |
| Integrasi proxy | 1004 |
| Format acara | 1005 |
| Format respons | 1006 |

| | |
|--|------|
| Izin | 1007 |
| Aplikasi sampel | 1009 |
| Tutorial | 1009 |
| Kesalahan | 1031 |
| Komposer Aplikasi | 1032 |
| Mengekspor fungsi Lambda ke Komposer Aplikasi | 1032 |
| Sumber daya lainnya | 1035 |
| CloudFormation | 1036 |
| CloudFront (Lambda @Edge) | 1040 |
| Amazon DocumentDB | 1042 |
| Contoh acara Amazon DocumentDB | 1043 |
| Prasyarat dan izin | 1044 |
| Konfigurasi jaringan | 1046 |
| Membuat pemetaan sumber peristiwa Amazon DocumentDB (konsol) | 1048 |
| Membuat pemetaan sumber peristiwa Amazon DocumentDB (atau) SDK CLI | 1050 |
| Posisi awal polling dan streaming | 1053 |
| Memantau sumber acara Amazon DocumentDB Anda | 1053 |
| Tutorial | 1054 |
| DynamoDB | 1088 |
| Polling dan batching stream | 1088 |
| Posisi awal polling dan streaming | 1090 |
| Pembaca simultan | 1090 |
| Contoh peristiwa | 1090 |
| Buat pemetaan | 1092 |
| Kegagalan item batch | 1094 |
| Penanganan kesalahan | 1107 |
| Pemantauan | 1110 |
| Pemrosesan stateful | 1110 |
| Parameter | 1115 |
| Penyaringan acara | 1117 |
| Tutorial | 1126 |
| EC2 | 1143 |
| Memberikan izin untuk EventBridge (Acara) CloudWatch | 1144 |
| Elastic Load Balancing (Application Load Balancer) | 1145 |
| Memanggil menggunakan Scheduler EventBridge | 1147 |
| Mengatur peran eksekusi | 1147 |

| | |
|---|------|
| Buat jadwal | 1147 |
| Sumber daya terkait | 1152 |
| IoT | 1153 |
| Kinesis Data Streams | 1155 |
| Polling dan batching stream | 1155 |
| Contoh peristiwa | 1157 |
| Buat pemetaan | 1158 |
| Kegagalan item batch | 1164 |
| Penanganan kesalahan | 1179 |
| Pemrosesan stateful | 1182 |
| Parameter | 1185 |
| Penyaringan acara | 1188 |
| Tutorial | 1192 |
| MQ | 1210 |
| Memahami grup konsumen Lambda untuk Amazon MQ | 1212 |
| Buat pemetaan | 1216 |
| Parameter | 1223 |
| Penyaringan acara | 1224 |
| Pemecahan Masalah | 1230 |
| MSK | 1232 |
| Contoh peristiwa | 1233 |
| Konfigurasi sumber acara | 1234 |
| Memproses pesan | 1246 |
| Penyaringan acara | 1256 |
| Destinasi yang gagal | 1261 |
| Tutorial | 1265 |
| RDS | 1282 |
| Mengkonfigurasi fungsi Anda untuk bekerja dengan sumber daya RDS | 1282 |
| Menghubungkan ke RDS database Amazon dalam fungsi Lambda | 1285 |
| Memproses pemberitahuan acara dari Amazon RDS | 1301 |
| Lengkap Lambda dan Amazon tutorial RDS | 1302 |
| S3 | 1303 |
| Tutorial: Menggunakan pemicu S3 | 1305 |
| Tutorial: Gunakan pemicu Amazon S3 untuk membuat thumbnail | 1331 |
| SQS | 1361 |
| Memahami perilaku polling dan batching untuk pemetaan sumber SQS acara Amazon | 1361 |

| | |
|--|------|
| Contoh acara pesan antrian standar | 1362 |
| Contoh FIFO acara pesan antrian | 1364 |
| Buat pemetaan | 1364 |
| Perilaku penskalaan | 1368 |
| Penanganan kesalahan | 1370 |
| Parameter | 1383 |
| Penyaringan acara | 1384 |
| Tutorial | 1389 |
| Tutorial lintas akun SQS | 1408 |
| S3 Batch | 1415 |
| Memanggil fungsi Lambda dari operasi batch Amazon S3 | 1416 |
| SNS | 1418 |
| Menambahkan pemicu topik Amazon SNS untuk fungsi Lambda menggunakan konsol | 1418 |
| Menambahkan pemicu topik Amazon SNS secara manual untuk fungsi Lambda | 1419 |
| Contoh bentuk acara SNS | 1420 |
| Tutorial | 1421 |
| Izin Lambda | 1443 |
| Peran eksekusi (izin untuk fungsi untuk mengakses sumber daya lain) | 1445 |
| Membuat peran eksekusi di IAM konsol | 1445 |
| Menciptakan dan mengelola peran dengan AWS CLI | 1446 |
| Berikan akses hak istimewa paling rendah ke peran eksekusi Lambda Anda | 1448 |
| Perbarui peran eksekusi | 1448 |
| AWS kebijakan terkelola | 1450 |
| Fungsi sumber ARN | 1453 |
| Izin akses (izin untuk entitas lain untuk mengakses fungsi Anda) | 1458 |
| Kebijakan berbasis identitas | 1458 |
| Kebijakan berbasis sumber daya | 1465 |
| Kontrol akses berbasis atribut | 1473 |
| Sumber Daya dan Kondisi | 1480 |
| Keamanan, tata kelola, dan kepatuhan | 1491 |
| Perlindungan data | 1492 |
| Enkripsi bergerak | 1493 |
| Enkripsi diam | 1493 |
| Identity and Access Management | 1499 |
| Audiens | 1499 |
| Mengautentikasi dengan identitas | 1500 |

| | |
|--|------|
| Mengelola akses menggunakan kebijakan | 1504 |
| Bagaimana AWS Lambda bekerja dengan IAM | 1506 |
| Contoh kebijakan berbasis identitas | 1513 |
| Kebijakan yang dikelola oleh AWS | 1516 |
| Pemecahan Masalah | 1522 |
| Tata Kelola | 1524 |
| Kontrol proaktif dengan Guard | 1527 |
| Kontrol proaktif dengan AWS Config | 1531 |
| Detektif kontrol dengan AWS Config | 1539 |
| Penandatanganan kode | 1544 |
| Pemindaian kode | 1547 |
| Observabilitas | 1552 |
| Validasi kepatuhan | 1560 |
| Ketahanan | 1560 |
| Keamanan infrastruktur | 1561 |
| Penandatanganan kode | 1562 |
| Validasi tanda tangan | 1563 |
| Mengkonfigurasi penandatanganan kode dengan Lambda API | 1564 |
| Buat konfigurasi | 1564 |
| Perbarui konfigurasi | 1566 |
| Izin | 1567 |
| Pemantauan fungsi | 1569 |
| Harga | 1569 |
| Lihat metrik fungsi | 1570 |
| Melihat metrik di konsol CloudWatch | 1570 |
| Tipe metrik | 1571 |
| Log fungsi | 1576 |
| Diperlukan izin IAM | 1576 |
| Harga | 1577 |
| Konfigurasikan log fungsi | 1577 |
| Lihat log fungsi | 1591 |
| CloudTrail log | 1597 |
| Peristiwa data Lambda di CloudTrail | 1598 |
| Acara manajemen Lambda di CloudTrail | 1600 |
| Menggunakan CloudTrail untuk memecahkan masalah sumber acara Lambda yang dinonaktifkan | 1602 |

| | |
|--|------|
| Contoh acara Lambda | 1603 |
| AWS X-Ray | 1606 |
| Memahami jejak X-Ray | 1607 |
| Izin peran eksekusi | 1612 |
| AWS X-Ray Daemon | 1612 |
| Mengaktifkan penelusuran aktif dengan Lambda API | 1612 |
| Mengaktifkan penelusuran aktif dengan AWS CloudFormation | 1613 |
| Wawasan fungsi | 1614 |
| Cara kerjanya | 1614 |
| Harga | 1615 |
| Runtime yang didukung | 1615 |
| Mengaktifkan Lambda Insights di konsol | 1615 |
| Mengaktifkan Lambda Insights secara terprogram | 1615 |
| Menggunakan dasbor Lambda Insights | 1616 |
| Mendeteksi anomali fungsi | 1618 |
| Memecahkan masalah fungsi | 1620 |
| Apa selanjutnya? | 1622 |
| Lapisan Lambda | 1623 |
| Cara menggunakan lapisan | 1625 |
| Versi lapisan dan lapisan | 1625 |
| Lapisan kemasan | 1626 |
| Jalur lapisan untuk setiap runtime Lambda | 1626 |
| Membuat dan menghapus lapisan | 1630 |
| Membuat lapisan | 1630 |
| Menghapus versi lapisan | 1632 |
| Menambahkan lapisan | 1633 |
| Mengakses konten lapisan dari fungsi Anda | 1635 |
| Menemukan informasi lapisan | 1635 |
| Lapisan dengan AWS CloudFormation | 1638 |
| Lapisan dengan AWS SAM | 1639 |
| Ekstensi Lambda | 1640 |
| Lingkungan eksekusi | 1641 |
| Dampak pada performa dan sumber daya | 1642 |
| Izin | 1642 |
| Mengonfigurasi ekstensi | 1643 |
| Mengonfigurasi ekstensi (arsip file .zip) | 1643 |

| | |
|---|------|
| Menggunakan ekstensi dalam gambar kontainer | 1643 |
| Langkah selanjutnya | 1644 |
| Mitra ekstensi | 1645 |
| AWS ekstensi terkelola | 1646 |
| Ekstensi API | 1647 |
| Siklus hidup lingkungan eksekusi Lambda | 1648 |
| APIReferensi ekstensi | 1658 |
| Telemetry API | 1664 |
| Membuat ekstensi menggunakan Telemetry API | 1665 |
| Mendaftarkan ekstensi Anda | 1667 |
| Membuat pendengar telemetry | 1667 |
| Menentukan protokol tujuan | 1669 |
| Mengkonfigurasi penggunaan memori dan buffering | 1670 |
| Mengirim permintaan berlangganan ke Telemetry API | 1671 |
| Pesan API Telemetry Masuk | 1672 |
| Referensi API | 1675 |
| Eventreferensi skema | 1679 |
| Mengonversi acara ke OTel Span | 1700 |
| Log API | 1706 |
| Pemecahan Masalah | 1719 |
| Deployment | 1719 |
| Umum: Izin ditolak/Tidak dapat memuat file tersebut | 1720 |
| Umum: Terjadi kesalahan saat memanggil UpdateFunctionCode | 1721 |
| Amazon S3: Kode Kesalahan. PermanentRedirect | 1721 |
| Umum: Tidak dapat menemukan, tidak dapat memuat, tidak dapat mengimpor, kelas tidak ditemukan, tidak ada file atau direktori tersebut | 1721 |
| Umum: Metode handler tidak didefinisikan | 1722 |
| Lambda: Konversi lapisan gagal | 1723 |
| Lambda: atau InvalidParameterValueException RequestEntityTooLargeException | 1723 |
| Lambda: InvalidParameterValueException | 1724 |
| Lambda: Konkurensi dan kuota memori | 1724 |
| Invokasi | 1725 |
| IAM: lambda: InvokeFunction tidak diizinkan | 1725 |
| Lambda: Tidak dapat menemukan bootstrap yang valid (Runtime. InvalidEntrypoint) | 1725 |
| Lambda: Operasi tidak dapat dilakukan ResourceConflictException | 1726 |
| Lambda: Fungsi tertahan dalam Tertunda | 1726 |

| | |
|--|------|
| Lambda: Salah satu fungsi menggunakan semua konkurensi | 1726 |
| Umum: Tidak dapat memanggil fungsi dengan akun atau layanan lain | 1727 |
| Umum: Invokasi fungsi adalah perulangan | 1727 |
| Lambda: Perutean alias dengan konkurensi terprovisi | 1727 |
| Lambda: Mulai awal dengan konkurensi terprovisi | 1727 |
| Lambda: Mulai awal dengan versi baru | 1728 |
| EFS: Fungsi tidak dapat me-mount sistem EFS file | 1729 |
| EFS: Fungsi tidak dapat terhubung ke sistem EFS file | 1729 |
| EFS: Fungsi tidak dapat me-mount sistem EFS file karena batas waktu | 1729 |
| Lambda: Lambda mendeteksi proses IO yang memakan waktu terlalu lama | 1729 |
| Eksekusi | 1730 |
| Lambda: Eksekusi memerlukan waktu yang lama | 1730 |
| Lambda: Log atau jejak tidak muncul | 1730 |
| Lambda: Tidak semua log fungsi saya muncul | 1731 |
| Lambda: Fungsi kembali sebelum eksekusi selesai | 1732 |
| AWS SDK: Versi dan pembaruan | 1732 |
| Python: Pustaka memuat dengan tidak benar | 1733 |
| Java: Fungsi Anda membutuhkan waktu lebih lama untuk memproses peristiwa setelah memperbarui ke Java 17 dari Java 11 | 1733 |
| Jaringan | 1734 |
| VPC: Fungsi kehilangan akses internet atau waktu habis | 1734 |
| VPC: Fungsi membutuhkan akses ke AWS layanan tanpa menggunakan internet | 1734 |
| VPC: Batas antarmuka jaringan elastis tercapai | 1735 |
| EC2: Antarmuka jaringan elastis dengan jenis "lambda" | 1735 |
| DNS: Gagal terhubung ke host dengan UNKNOWNHOSTEXCEPTION | 1735 |
| Aplikasi Lambda | 1736 |
| Memantau aplikasi | 1737 |
| Deployment bergulir | 1739 |
| Contoh template AWS SAM Lambda | 1739 |
| Kubernetes | 1741 |
| AWSPengontrol untuk Kubernetes (ACK) | 1741 |
| Crossplane | 1742 |
| Aplikasi sampel | 1743 |
| Bekerja dengan AWS SDKs | 1746 |
| Contoh kode | 1748 |
| Hal-hal mendasar | 1760 |

| | |
|--|------|
| Halo Lambda | 1761 |
| Tindakan | 1771 |
| Skenario | 1885 |
| Secara otomatis mengonfirmasi pengguna yang dikenal dengan fungsi Lambda | 1886 |
| Secara otomatis memigrasikan pengguna yang dikenal dengan fungsi Lambda | 1906 |
| Buat data REST API untuk melacak COVID -19 | 1927 |
| Buat perpustakaan pinjaman REST API | 1928 |
| Membuat aplikasi messenger | 1929 |
| Membuat aplikasi nirserver untuk mengelola foto | 1930 |
| Membuat aplikasi obrolan websocket | 1934 |
| Buat aplikasi untuk menganalisis umpan balik pelanggan | 1935 |
| Memulai dengan fungsi | 1941 |
| Menginvokasi fungsi Lambda dari browser | 2054 |
| Mengubah data dengan S3 Object Lambda | 2055 |
| Gunakan API Gateway untuk menjalankan fungsi Lambda | 2056 |
| Menggunakan Step Functions untuk menginvokasi fungsi Lambda | 2058 |
| Menggunakan peristiwa terjadwal untuk menginvokasi fungsi Lambda | 2059 |
| Menulis data aktivitas kustom dengan fungsi Lambda setelah otentikasi pengguna Amazon Cognito | 2061 |
| Contoh nirserver | 2081 |
| Menghubungkan ke RDS database Amazon dalam fungsi Lambda | 2082 |
| Memanggil fungsi Lambda dari pemicu Kinesis | 2098 |
| Memanggil fungsi Lambda dari pemicu DynamoDB | 2109 |
| Memanggil fungsi Lambda dari pemicu Amazon DocumentDB | 2118 |
| Memanggil fungsi Lambda dari pemicu Amazon MSK | 2126 |
| Menginvokasi fungsi Lambda dari pemicu Amazon S3 | 2130 |
| Memanggil fungsi Lambda dari pemicu Amazon SNS | 2142 |
| Memanggil fungsi Lambda dari pemicu Amazon SQS | 2151 |
| Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Kinesis | 2160 |
| Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu DynamoDB | 2173 |
| Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Amazon SQS | 2185 |
| Kuota Lambda | 2195 |
| Komputasi dan penyimpanan | 2195 |
| Konfigurasi fungsi, penyebaran, dan eksekusi | 2196 |
| Permintaan Lambda API | 2198 |
| Layanan lainnya | 2200 |

| | |
|----------------------------|----------|
| Riwayat dokumen | 2201 |
| Pembaruan sebelumnya | 2226 |
| | mmccxxxv |

Apa itu AWS Lambda?

Anda dapat menggunakan AWS Lambda untuk menjalankan kode tanpa menyediakan atau mengelola server.

Lambda menjalankan kode Anda pada infrastruktur komputasi ketersediaan tinggi dan melakukan semua administrasi sumber daya komputasi, termasuk pemeliharaan server dan sistem operasi, penyediaan kapasitas dan penskalaan otomatis, dan pencatatan. Dengan Lambda, yang perlu Anda lakukan hanyalah menyediakan kode Anda di salah satu runtime bahasa yang didukung Lambda.

Anda mengatur kode Anda ke fungsi Lambda. Layanan Lambda menjalankan fungsi Anda hanya jika diperlukan dan menskalakan secara otomatis. Anda hanya membayar untuk waktu komputasi yang Anda konsumsi — tidak ada biaya ketika kode Anda tidak berjalan. Untuk informasi selengkapnya, silakan lihat [Harga AWS Lambda](#).

Tip

Untuk mempelajari cara membuat solusi tanpa server, lihat [Panduan Pengembang Tanpa Server](#).

Kapan menggunakan Lambda

Lambda adalah layanan komputasi yang ideal untuk skenario aplikasi yang perlu ditingkatkan dengan cepat, dan skala turun ke nol saat tidak diminati. Misalnya, Anda dapat menggunakan Lambda untuk:

- Pemrosesan file: Gunakan Amazon Simple Storage Service (Amazon S3) untuk memicu pemrosesan data Lambda secara real time setelah upload.
- Pemrosesan streaming: Gunakan Lambda dan Amazon Kinesis untuk memproses data streaming waktu nyata untuk pelacakan aktivitas aplikasi, pemrosesan pesanan transaksi, analisis aliran klik, pembersihan data, penyaringan log, pengindeksan, analisis media sosial, telemetri data perangkat Internet of Things (IoT), dan pengukuran.
- Aplikasi web: Gabungkan Lambda dengan AWS layanan lain untuk membangun aplikasi web yang kuat yang secara otomatis meningkatkan dan menurunkan skala dan berjalan dalam konfigurasi yang sangat tersedia di beberapa pusat data.
- Backend IoT: Bangun backend tanpa server menggunakan Lambda untuk menangani permintaan web, seluler, IoT, dan pihak ketiga. API

- Backend seluler: Buat backend menggunakan Lambda dan API Amazon Gateway untuk mengautentikasi dan memproses permintaan. API Gunakan AWS Amplify untuk mengintegrasikan dengan mudah dengan frontend iOS, Android, Web, dan React Native Anda.

Saat menggunakan Lambda, Anda hanya bertanggung jawab atas kode Anda. Lambda mengelola armada komputasi yang menawarkan keseimbangan memori, jaringan CPU, dan sumber daya lainnya untuk menjalankan kode Anda. Karena Lambda mengelola sumber daya ini, Anda tidak dapat masuk untuk menghitung instans atau menyesuaikan sistem operasi di runtime yang disediakan. Lambda melakukan aktivitas operasional dan administrasi atas nama Anda, termasuk mengelola kapasitas, memantau, dan mencatat fungsi Lambda Anda.

Fitur utama

Fitur utama berikut membantu Anda mengembangkan aplikasi Lambda yang dapat diskalakan, aman, dan dapat diperluas dengan mudah:

[Variabel lingkungan](#)

Gunakan variabel lingkungan untuk menyesuaikan perilaku fungsi Anda tanpa memperbarui kode.

[Versi](#)

Kelola penerapan fungsi Anda dengan versi, sehingga, misalnya, fungsi baru dapat digunakan untuk pengujian beta tanpa memengaruhi pengguna versi produksi stabil.

[Gambar kontainer](#)

Buat gambar kontainer untuk fungsi Lambda dengan menggunakan gambar dasar yang AWS disediakan atau gambar dasar alternatif sehingga Anda dapat menggunakan kembali perkakas kontainer yang ada atau menerapkan beban kerja yang lebih besar yang bergantung pada dependensi yang cukup besar, seperti pembelajaran mesin.

[Lapisan](#)

Package library dan dependensi lainnya untuk mengurangi ukuran arsip deployment dan membuatnya lebih cepat untuk menyebarkan kode Anda.

[Ekstensi Lambda](#)

Tingkatkan fungsi Lambda Anda dengan alat untuk pemantauan, pengamatan, keamanan, dan tata kelola.

[Fungsi URLs](#)

Tambahkan titik akhir khusus HTTP (S) ke fungsi Lambda Anda.

[Streaming respons](#)

Konfigurasi fungsi Lambda Anda URLs untuk mengalirkan muatan respons kembali ke klien dari fungsi Node.js, untuk meningkatkan waktu ke kinerja byte (TTFB) pertama atau mengembalikan muatan yang lebih besar.

[Kontrol konkurensi dan penskalaan](#)

Terapkan kontrol berbutir halus atas penskalaan dan daya tanggap aplikasi produksi Anda.

[Penandatanganan kode](#)

Verifikasi bahwa hanya pengembang yang disetujui yang menerbitkan kode tepercaya yang tidak berubah di fungsi Lambda Anda

[Jaringan pribadi](#)

Buat jaringan pribadi untuk sumber daya seperti database, instance cache, atau layanan internal.

[Akses sistem file](#)

Konfigurasi fungsi untuk memasang Amazon Elastic File System (AmazonEFS) ke direktori lokal, sehingga kode fungsi Anda dapat mengakses dan memodifikasi sumber daya bersama dengan aman dan pada konkurensi tinggi.

[Lambda SnapStart untuk Jawa](#)

Tingkatkan kinerja startup untuk runtime Java hingga 10x tanpa biaya tambahan, biasanya tanpa perubahan pada kode fungsi Anda.

Buat fungsi Lambda pertama Anda

Untuk memulai Lambda, gunakan konsol Lambda untuk membuat fungsi. Dalam beberapa menit, Anda dapat membuat dan menerapkan fungsi dan mengujinya di konsol.

Saat Anda menjalankan tutorial, Anda akan mempelajari beberapa konsep dasar Lambda, seperti cara meneruskan argumen ke fungsi Anda menggunakan objek acara Lambda. Anda juga akan mempelajari cara mengembalikan output log dari fungsi Anda, dan cara melihat log pemanggilan fungsi Anda di Log. CloudWatch

Agar semuanya tetap sederhana, Anda membuat fungsi Anda menggunakan runtime Python atau Node.js. Dengan bahasa yang ditafsirkan ini, Anda dapat mengedit kode fungsi langsung di editor kode bawaan konsol. Dengan bahasa yang dikompilasi seperti Java dan C#, Anda perlu membuat paket penerapan di mesin build lokal Anda dan mengunggahnya ke Lambda. Untuk mempelajari tentang penerapan fungsi ke Lambda menggunakan runtime lain, lihat tautan di bagian. [the section called “Sumber daya tambahan dan langkah selanjutnya”](#)

Tip

Untuk mempelajari cara membuat solusi tanpa server, lihat [Panduan Pengembang Tanpa Server](#).

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai

praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi <https://aws.amazon.com/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftarkan Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Membuat fungsi Lambda dengan konsol

Dalam contoh ini, fungsi Anda mengambil JSON objek yang berisi dua nilai integer berlabel "length" dan "width". Fungsi ini mengalikan nilai-nilai ini untuk menghitung area dan mengembalikan ini sebagai JSON string.

Fungsi Anda juga mencetak area yang dihitung, bersama dengan nama grup CloudWatch lognya. Kemudian dalam tutorial, Anda akan belajar menggunakan [CloudWatch Log](#) untuk melihat catatan pemanggilan fungsi Anda.

Untuk membuat fungsi Anda, pertama-tama Anda menggunakan konsol untuk membuat fungsi Hello world dasar. Pada langkah berikut, Anda kemudian menambahkan kode fungsi Anda sendiri.

Untuk membuat fungsi Hello world Lambda dengan konsol

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih Buat fungsi.
3. Pilih Penulis dari awal.
4. Di panel Informasi dasar, untuk nama Fungsi masukkan **myLambdaFunction**.
5. Untuk Runtime, pilih Node.js 20.x atau Python 3.12

6. Biarkan arsitektur diatur ke x86_64 dan pilih Create function.

Lambda menciptakan fungsi yang mengembalikan pesan Hello from Lambda! Lambda juga menciptakan peran eksekusi untuk fungsi Anda. Peran [eksekusi adalah peran](#) AWS Identity and Access Management (IAM) yang memberikan izin fungsi Lambda untuk AWS layanan mengakses dan sumber daya. Untuk fungsi Anda, peran yang dibuat Lambda memberikan izin dasar untuk menulis ke Log. CloudWatch

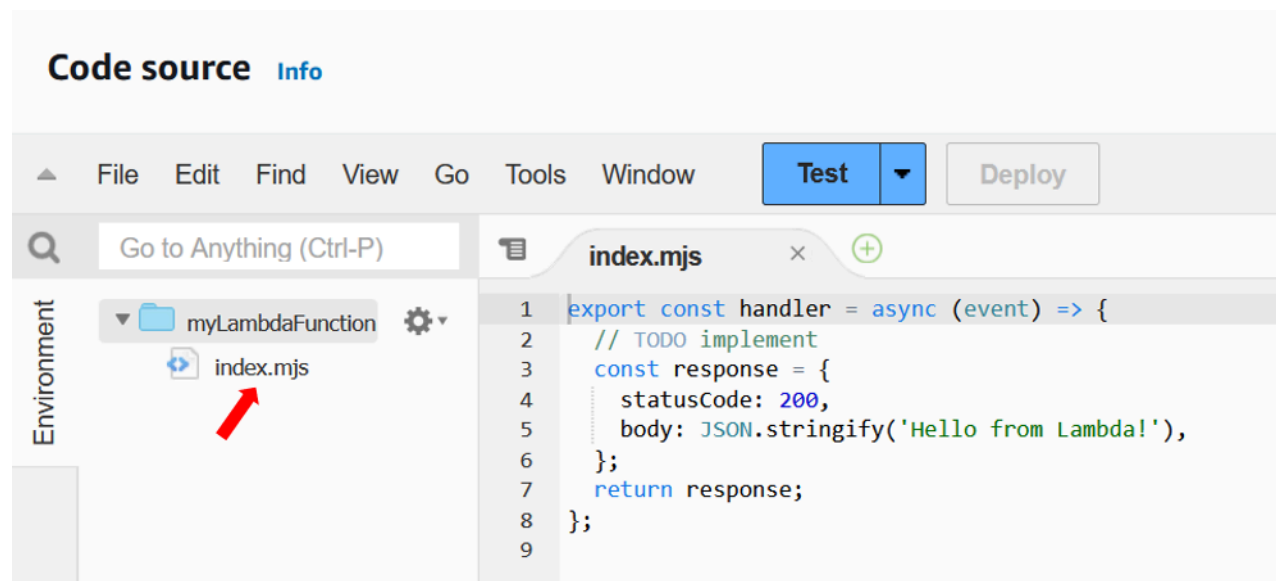
Anda sekarang menggunakan editor kode bawaan konsol untuk mengganti kode Hello world yang dibuat Lambda dengan kode fungsi Anda sendiri.

Node.js

Untuk memodifikasi kode di konsol

1. Pilih tab Kode.

Di editor kode bawaan konsol, Anda akan melihat kode fungsi yang dibuat Lambda. Jika Anda tidak melihat tab index.mjs di editor kode, pilih index.mjs di file explorer seperti yang ditunjukkan pada diagram berikut.



2. Tempelkan kode berikut ke tab index.mjs, ganti kode yang dibuat Lambda.

```
export const handler = async (event, context) => {

  const length = event.length;
  const width = event.width;
```

```
let area = calculateArea(length, width);
console.log(`The area is ${area}`);

console.log('CloudWatch log group: ', context.logGroupName);

let data = {
  "area": area,
};
return JSON.stringify(data);

function calculateArea(length, width) {
  return length * width;
}
};
```

3. Pilih Deploy untuk memperbarui kode fungsi Anda. Ketika Lambda telah menerapkan perubahan, konsol menampilkan spanduk yang memberi tahu Anda bahwa itu berhasil memperbarui fungsi Anda.

Memahami kode fungsi Anda

Sebelum Anda pindah ke langkah berikutnya, mari kita luangkan waktu sejenak untuk melihat kode fungsi dan memahami beberapa konsep Lambda utama.

- Pawang Lambda:

Fungsi Lambda Anda berisi fungsi Node.js bernama `handler`. Fungsi Lambda di Node.js dapat berisi lebih dari satu fungsi Node.js, tetapi fungsi handler selalu menjadi titik masuk ke kode Anda. Ketika fungsi Anda dipanggil, Lambda menjalankan metode ini.

Saat Anda membuat fungsi Hello world menggunakan konsol, Lambda secara otomatis menyetel nama metode handler untuk fungsi Anda. `handler` Pastikan untuk tidak mengedit nama fungsi Node.js ini. Jika Anda melakukannya, Lambda tidak akan dapat menjalankan kode Anda ketika Anda menjalankan fungsi Anda.

Untuk mempelajari selengkapnya tentang penanganan Lambda di Node.js, lihat [the section called "Handler"](#)

- Objek acara Lambda:

Fungsi ini `handler` mengambil dua argumen, `event` dan `context`. Peristiwa di Lambda adalah dokumen yang JSON diformat yang berisi data untuk fungsi Anda untuk diproses.

Jika fungsi Anda dipanggil oleh yang lain AWS layanan, objek acara berisi informasi tentang peristiwa yang menyebabkan pemanggilan. Misalnya, jika bucket Amazon Simple Storage Service (Amazon S3) memanggil fungsi Anda saat objek diunggah, acara tersebut akan berisi nama bucket Amazon S3 dan kunci objek.

Dalam contoh ini, Anda akan membuat acara di konsol dengan memasukkan dokumen yang JSON diformat dengan dua pasangan nilai kunci.

- Objek konteks Lambda:

Argumen kedua yang diambil fungsi Anda adalah `context`. Lambda meneruskan objek konteks ke fungsi Anda secara otomatis. Objek konteks berisi informasi tentang fungsi pemanggilan dan lingkungan eksekusi.

Anda dapat menggunakan objek konteks untuk menampilkan informasi tentang pemanggilan fungsi Anda untuk tujuan pemantauan. Dalam contoh ini, fungsi Anda menggunakan `logGroupName` parameter untuk menampilkan nama grup CloudWatch lognya.

Untuk mempelajari lebih lanjut tentang objek konteks Lambda di Node.js, lihat [the section called "Konteks"](#)

- Masuk ke Lambda:

Dengan Node.js, Anda dapat menggunakan metode konsol seperti `console.log` dan `console.error` untuk mengirim informasi ke log fungsi Anda. Kode contoh menggunakan `console.log` pernyataan untuk menampilkan area terhitung dan nama grup CloudWatch Log fungsi. Anda juga dapat menggunakan pustaka logging apa pun yang menulis ke `stdout` atau `stderr`.

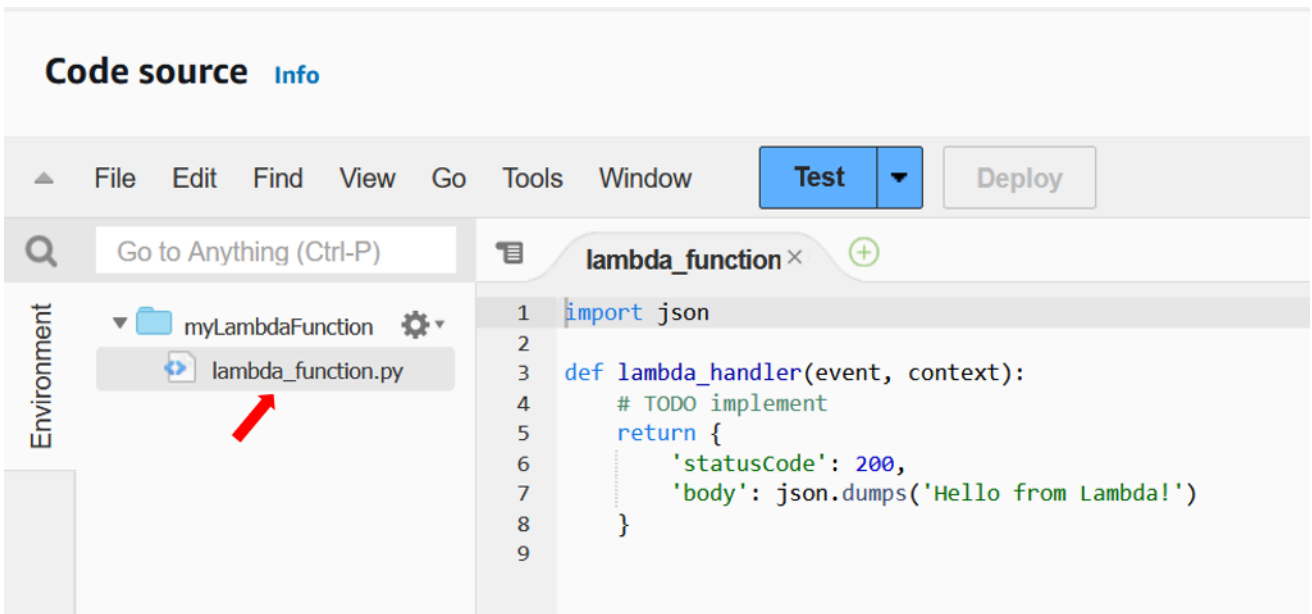
Untuk mempelajari selengkapnya, lihat [the section called "Pencatatan log"](#). Untuk mempelajari tentang login di runtime lain, lihat halaman 'Membangun dengan' untuk runtime yang Anda minati.

Python

Untuk memodifikasi kode di konsol

1. Pilih tab Kode.

Di editor kode bawaan konsol, Anda akan melihat kode fungsi yang dibuat Lambda. Jika Anda tidak melihat tab `lambda_function.py` di editor kode, pilih `lambda_function.py` di file explorer seperti yang ditunjukkan pada diagram berikut.



2. Tempelkan kode berikut ke tab `lambda_function.py`, ganti kode yang dibuat Lambda.

```
import json
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):

    # Get the length and width parameters from the event object. The
    # runtime converts the event object to a Python dictionary
    length = event['length']
    width = event['width']

    area = calculate_area(length, width)
    print(f"The area is {area}")

    logger.info(f"CloudWatch logs group: {context.log_group_name}")

    # return the calculated area as a JSON string
    data = {"area": area}
    return json.dumps(data)
```

```
def calculate_area(length, width):  
    return length*width
```

3. Pilih Deploy untuk memperbarui kode fungsi Anda. Ketika Lambda telah menerapkan perubahan, konsol menampilkan spanduk yang memberi tahu Anda bahwa itu berhasil memperbarui fungsi Anda.

Memahami kode fungsi Anda

Sebelum Anda pindah ke langkah berikutnya, mari kita luangkan waktu sejenak untuk melihat kode fungsi dan memahami beberapa konsep Lambda utama.

- Pawang Lambda:

Fungsi Lambda Anda berisi fungsi Python bernama `lambda_handler`. Fungsi Lambda di Python dapat berisi lebih dari satu fungsi Python, tetapi fungsi handler selalu menjadi titik masuk ke kode Anda. Ketika fungsi Anda dipanggil, Lambda menjalankan metode ini.

Saat Anda membuat fungsi Hello world menggunakan konsol, Lambda secara otomatis menyetel nama metode handler untuk fungsi Anda `lambda_handler`. Pastikan untuk tidak mengedit nama fungsi Python ini. Jika Anda melakukannya, Lambda tidak akan dapat menjalankan kode Anda ketika Anda menjalankan fungsi Anda.

Untuk mempelajari selengkapnya tentang penanganan Lambda dengan Python, lihat [the section called "Handler"](#)

- Objek acara Lambda:

Fungsi ini `lambda_handler` mengambil dua argumen, `event` dan `context`. Peristiwa di Lambda adalah dokumen yang JSON diformat yang berisi data untuk fungsi Anda untuk diproses.

Jika fungsi Anda dipanggil oleh yang lain AWS layanan, objek acara berisi informasi tentang peristiwa yang menyebabkan pemanggilan. Misalnya, jika bucket Amazon Simple Storage Service (Amazon S3) memanggil fungsi Anda saat objek diunggah, acara tersebut akan berisi nama bucket Amazon S3 dan kunci objek.

Dalam contoh ini, Anda akan membuat acara di konsol dengan memasukkan dokumen yang JSON diformat dengan dua pasangan nilai kunci.

- Objek konteks Lambda:

Argumen kedua yang diambil fungsi Anda adalah `context`. Lambda meneruskan objek konteks ke fungsi Anda secara otomatis. Objek konteks berisi informasi tentang fungsi pemanggilan dan lingkungan eksekusi.

Anda dapat menggunakan objek konteks untuk menampilkan informasi tentang pemanggilan fungsi Anda untuk tujuan pemantauan. Dalam contoh ini, fungsi Anda menggunakan `log_group_name` parameter untuk menampilkan nama grup CloudWatch lognya.

Untuk mempelajari lebih lanjut tentang objek konteks Lambda dengan Python, lihat [the section called "Konteks"](#)

- Masuk ke Lambda:

Dengan Python, Anda dapat menggunakan `print` pernyataan atau pustaka logging Python untuk mengirim informasi ke log fungsi Anda. Untuk mengilustrasikan perbedaan dalam apa yang ditangkap, kode contoh menggunakan kedua metode. Dalam aplikasi produksi, kami menyarankan Anda menggunakan pustaka logging.

Untuk mempelajari selengkapnya, lihat [the section called "Log dan pantau fungsi Python Lambda"](#). Untuk mempelajari tentang login di runtime lain, lihat halaman 'Membangun dengan' untuk runtime yang Anda minati.

Memanggil fungsi Lambda menggunakan konsol

Untuk menjalankan fungsi Anda menggunakan konsol Lambda, pertama-tama Anda membuat acara pengujian untuk dikirim ke fungsi Anda. Acara ini adalah dokumen JSON diformat yang berisi dua pasangan kunci-nilai dengan kunci `length` dan `width`

Untuk membuat acara pengujian

1. Di panel Sumber kode, pilih Uji.
2. Pilih Buat acara baru.
3. Untuk nama Acara masukkan **myTestEvent**.
4. Di JSON panel Event, ganti nilai default dengan menempelkan berikut ini:

```
{  
  "length": 6,
```

```
"width": 7
}
```

5. Pilih Simpan.

Anda sekarang menguji fungsi Anda dan menggunakan konsol Lambda dan CloudWatch Log untuk melihat catatan pemanggilan fungsi Anda.

Untuk menguji fungsi Anda dan melihat catatan pemanggilan di konsol

- Di panel Sumber kode, pilih Uji. Ketika fungsi Anda selesai berjalan, Anda akan melihat log respons dan fungsi ditampilkan di tab Hasil eksekusi. Anda akan melihat hasil yang mirip dengan berikut ini.

Node.js

```
Test Event Name
myTestEvent
```

```
Response
"{\\"area\\":42}"
```

Function Logs

```
START RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Version: $LATEST
2023-08-31T23:39:45.313Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO The area is
42
2023-08-31T23:39:45.331Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO CloudWatch
log group: /aws/lambda/myLambdaFunction
END RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a
REPORT RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Duration: 20.67 ms Billed
Duration: 21 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration:
163.87 ms
```

```
Request ID
5c012b0a-18f7-4805-b2f6-40912935034a
```

Python

```
Test Event Name
myTestEvent
```

```
Response
```

```
"{\"area\": 42}"
```

Function Logs

```
START RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Version: $LATEST
The area is 42
[INFO] 2023-08-31T23:43:26.428Z 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b CloudWatch
  logs group: /aws/lambda/myLambdaFunction
END RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
REPORT RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Duration: 1.42 ms Billed
  Duration: 2 ms Memory Size: 128 MB Max Memory Used: 39 MB Init Duration: 123.74
  ms
```

Request ID

```
2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
```

Dalam contoh ini, Anda memanggil kode menggunakan fitur pengujian konsol. Ini berarti Anda dapat melihat hasil eksekusi fungsi Anda secara langsung di konsol. Saat fungsi Anda dipanggil di luar konsol, Anda perlu menggunakan CloudWatch Log.

Untuk melihat catatan pemanggilan fungsi Anda di Log CloudWatch

1. Buka halaman [Grup log](#) CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (/aws/lambda/myLambdaFunction). Ini adalah nama grup log yang fungsi Anda cetak ke konsol.
3. Di tab Log streams, pilih aliran log untuk pemanggilan fungsi Anda.

Anda akan melihat output yang serupa dengan yang berikut:

Node.js

```
INIT_START Runtime Version: nodejs:20.v13 Runtime Version ARN:
  arn:aws:lambda:us-
  west-2::runtime:e3aaabf6b92ef8755eaae2f4bfdcb7eb8c4536a5e044900570a42bdba7b869d9
START RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20 Version: $LATEST
2023-08-23T22:04:15.809Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO The area
  is 42
2023-08-23T22:04:15.810Z aba6c0fc-cf99-49d7-a77d-26d805dacd20 INFO
  CloudWatch log group: /aws/lambda/myLambdaFunction
END RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20
```

```
REPORT RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20    Duration: 17.77 ms
Billed Duration: 18 ms    Memory Size: 128 MB    Max Memory Used: 67 MB    Init
Duration: 178.85 ms
```

Python

```
INIT_START Runtime Version: python:3.12.v16    Runtime Version ARN:
arn:aws:lambda:us-
west-2::runtime:ca202755c87b9ec2b58856efb7374b4f7b655a0ea3deb1d5acc9aee9e297b072
START RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e Version: $LATEST
The area is 42
[INFO] 2023-09-01T00:05:22.464Z 9315ab6b-354a-486e-884a-2fb2972b7d84 CloudWatch
logs group: /aws/lambda/myLambdaFunction
END RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e
REPORT RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e    Duration: 1.15 ms
Billed Duration: 2 ms    Memory Size: 128 MB    Max Memory Used: 40 MB
```

Bersihkan

Ketika Anda selesai bekerja dengan fungsi contoh, hapus itu. Anda juga dapat menghapus grup log yang menyimpan log fungsi, dan [peran eksekusi](#) yang dibuat konsol.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Tindakan, Hapus.
4. Di kotak dialog Hapus fungsi, masukkan hapus, lalu pilih Hapus.

Untuk menghapus grup log

1. Buka [halaman Grup log](#) CloudWatch konsol.
2. Pilih grup log fungsi (/aws/lambda/my-function).
3. Pilih Tindakan, Hapus grup log.
4. Di kotak dialog Hapus grup log, pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) pada konsol AWS Identity and Access Management (IAM).
2. Pilih peran eksekusi fungsi (misalnya, `myLambdaFunction-role-31exxmpl`).
3. Pilih Hapus.
4. Di kotak dialog Hapus peran, masukkan nama peran lalu pilih Hapus.

Anda dapat mengotomatiskan pembuatan dan pembersihan fungsi, grup log, dan peran dengan AWS CloudFormation dan AWS Command Line Interface (AWS CLI).

Sumber daya tambahan dan langkah selanjutnya

Sekarang Anda telah membuat dan menguji fungsi Lambda sederhana menggunakan konsol, ambil langkah berikut:

- Pelajari cara menambahkan dependensi ke kode Anda dan menerapkannya menggunakan paket.zip deployment. Pilih dari tautan berikut untuk bahasa yang Anda minati.

Node.js

Lihat [the section called “Deploy arsip file .zip”](#)

Typescript

Lihat [the section called “Deploy arsip file .zip”](#)

Python

Lihat [the section called “Deploy arsip file .zip”](#)

Ruby

Lihat [the section called “Deploy arsip file .zip”](#)

Java

Lihat [the section called “Deploy arsip file .zip”](#)

Go

Lihat [the section called “Deploy arsip file .zip”](#)

C#

Lihat [the section called "Paket deployment"](#)

- Lakukan tutorial [Menggunakan pemicu Amazon S3 untuk menjalankan fungsi Lambda untuk mempelajari cara mengonfigurasi fungsi Lambda](#) agar dipanggil oleh yang lain. AWS layanan
- Pilih salah satu tutorial berikut untuk contoh yang lebih kompleks menggunakan Lambda dengan yang lain. AWS layanan
 - [Menggunakan Lambda dengan API Gateway](#): Buat Amazon API Gateway REST API yang memanggil fungsi Lambda.
 - [Menggunakan fungsi Lambda untuk mengakses RDS database Amazon](#): Gunakan fungsi Lambda untuk menulis data ke database Amazon Relational Database Service (RDSAmazon) melalui Proxy. RDS
 - [Menggunakan pemicu Amazon S3 untuk membuat gambar thumbnail](#): Gunakan fungsi Lambda untuk membuat thumbnail setiap kali file gambar diunggah ke bucket Amazon S3.

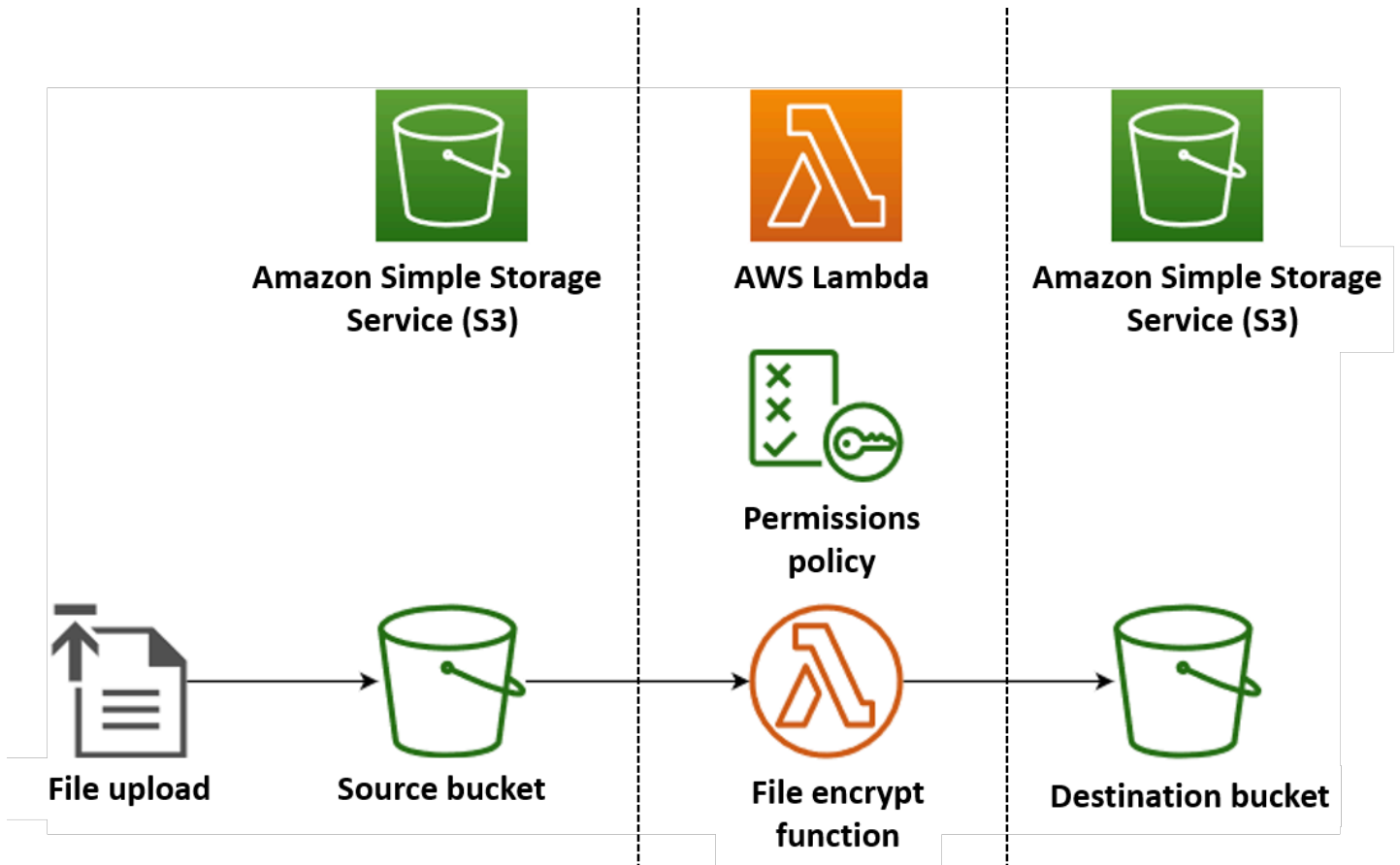
Membuat aplikasi pemrosesan file tanpa server

Salah satu kasus penggunaan yang paling umum untuk Lambda adalah melakukan tugas pemrosesan file. Misalnya, Anda mungkin menggunakan fungsi Lambda untuk secara otomatis membuat PDF file dari HTML file atau gambar, atau untuk membuat thumbnail saat pengguna mengunggah gambar.

Dalam contoh ini, Anda membuat aplikasi yang secara otomatis mengenkripsi PDF file saat diunggah ke bucket Amazon Simple Storage Service (Amazon S3). Untuk mengimplementasikan aplikasi ini, Anda membuat sumber daya berikut:

- Bucket S3 bagi pengguna untuk mengunggah PDF file
- Fungsi Lambda dalam Python yang membaca file yang diunggah dan membuat versi terenkripsi yang dilindungi kata sandi
- Bucket S3 kedua untuk Lambda untuk menyimpan file terenkripsi

Anda juga membuat kebijakan AWS Identity and Access Management (IAM) untuk memberikan izin fungsi Lambda Anda untuk melakukan operasi baca dan tulis pada bucket S3 Anda.

**Tip**

Jika Anda baru mengenal Lambda, kami sarankan Anda melakukan tutorial [Buat fungsi pertama Anda](#) sebelum membuat aplikasi contoh ini.

Anda dapat menerapkan aplikasi secara manual dengan membuat dan mengonfigurasi resource dengan AWS Management Console atau AWS Command Line Interface (AWS CLI). Anda juga dapat menerapkan aplikasi dengan menggunakan AWS Serverless Application Model (AWS SAM). AWS SAM adalah alat infrastruktur sebagai kode (IaC). Dengan IaC, Anda tidak membuat sumber daya secara manual, tetapi mendefinisikannya dalam kode dan kemudian menerapkannya secara otomatis.

Jika Anda ingin mempelajari lebih lanjut tentang menggunakan Lambda dengan IaC sebelum menerapkan aplikasi contoh ini, lihat [Infrastruktur sebagai kode \(IaC\)](#)

Prasyarat

Sebelum Anda dapat membuat aplikasi contoh, pastikan Anda memiliki alat baris perintah yang diperlukan diinstal.

- AWS CLI

Anda dapat menerapkan resource untuk aplikasi secara manual menggunakan aplikasi AWS Management Console atau file. AWS CLI Untuk menggunakan CLI, instal dengan mengikuti [petunjuk instalasi](#) di Panduan AWS Command Line Interface Pengguna.

- AWS SAM CLI

Jika Anda ingin menerapkan aplikasi contoh menggunakan AWS SAM, Anda perlu menginstal aplikasi AWS CLI dan aplikasi. AWS SAM CLI Untuk menginstal AWS SAM CLI, ikuti [petunjuk instalasi](#) di Panduan AWS SAM Pengguna.

- modul pytest

Setelah menerapkan aplikasi, Anda dapat mengujinya menggunakan skrip pengujian Python otomatis yang kami sediakan. Untuk menggunakan skrip ini, instal `pytest` paket di lingkungan pengembangan lokal Anda dengan menjalankan perintah berikut:

```
pip install pytest
```

Untuk menerapkan aplikasi menggunakan AWS SAM, [Docker](#) juga harus diinstal pada mesin build Anda.

Mengunduh contoh file aplikasi

Untuk membuat dan menguji aplikasi contoh, Anda membuat file berikut di direktori project:

- `lambda_function.py`- kode fungsi Python untuk fungsi Lambda yang melakukan enkripsi file
- `requirements.txt`- file manifes yang mendefinisikan dependensi yang dibutuhkan kode fungsi Python Anda
- `template.yaml`- AWS SAM Template yang dapat Anda gunakan untuk menyebarkan aplikasi
- `test_pdf_encrypt.py`- skrip pengujian yang dapat Anda gunakan untuk menguji aplikasi Anda secara otomatis

- `pytest.ini`- file konfigurasi untuk skrip pengujian

Perluas bagian berikut untuk melihat kode dan mempelajari lebih lanjut tentang peran setiap file dalam membuat dan menguji aplikasi Anda. Untuk membuat file di mesin lokal Anda, salin dan tempel kode di bawah ini, atau unduh file dari [aws-lambda-developer-guide GitHub repo](#).

Kode fungsi Python

Salin dan tempel kode berikut ke dalam file bernama `lambda_function.py`.

```
from pypdf import PdfReader, PdfWriter
import uuid
import os
from urllib.parse import unquote_plus
import boto3

# Create the S3 client to download and upload objects from S3
s3_client = boto3.client('s3')

def lambda_handler(event, context):
    # Iterate over the S3 event object and get the key for all uploaded files
    for record in event['Records']:
        bucket = record['s3']['bucket']['name']
        key = unquote_plus(record['s3']['object']['key']) # Decode the S3 object key to
        # remove any URL-encoded characters
        download_path = f'/tmp/{uuid.uuid4()}.pdf' # Create a path in the Lambda tmp
        # directory to save the file to
        upload_path = f'/tmp/converted-{uuid.uuid4()}.pdf' # Create another path to
        # save the encrypted file to

        # If the file is a PDF, encrypt it and upload it to the destination S3 bucket
        if key.lower().endswith('.pdf'):
            s3_client.download_file(bucket, key, download_path)
            encrypt_pdf(download_path, upload_path)
            encrypted_key = add_encrypted_suffix(key)
            s3_client.upload_file(upload_path, f'{bucket}-encrypted', encrypted_key)

# Define the function to encrypt the PDF file with a password
def encrypt_pdf(file_path, encrypted_file_path):
    reader = PdfReader(file_path)
    writer = PdfWriter()
```

```
for page in reader.pages:
    writer.add_page(page)

# Add a password to the new PDF
writer.encrypt("my-secret-password")

# Save the new PDF to a file
with open(encrypted_file_path, "wb") as file:
    writer.write(file)

# Define a function to add a suffix to the original filename after encryption
def add_encrypted_suffix(original_key):
    filename, extension = original_key.rsplit('.', 1)
    return f'{filename}_encrypted.{extension}'
```

Note

Dalam contoh kode ini, kata sandi untuk file terenkripsi (`my-secret-password`) di-hardcode ke dalam kode fungsi. Dalam aplikasi produksi, jangan sertakan informasi sensitif seperti kata sandi dalam kode fungsi Anda. Gunakan AWS Secrets Manager untuk menyimpan parameter sensitif dengan aman.

Kode fungsi python berisi tiga fungsi - fungsi [handler](#) yang dijalankan Lambda saat fungsi Anda dipanggil, dan dua fungsi terpisah bernama `add_encrypted_suffix` dan `encrypt_pdf` yang dipanggil handler untuk melakukan enkripsi. PDF

Saat fungsi Anda dipanggil oleh Amazon S3, Lambda meneruskan argumen peristiwa JSON yang diformat ke fungsi yang berisi detail tentang peristiwa yang menyebabkan pemanggilan. Dalam hal ini, informasi termasuk nama bucket S3 dan kunci objek untuk file yang diunggah. Untuk mempelajari lebih lanjut tentang format objek acara untuk Amazon S3, lihat. [the section called "S3"](#)

Fungsi Anda kemudian menggunakan AWS SDK for Python (Boto3) untuk mengunduh PDF file yang ditentukan dalam objek acara ke direktori penyimpanan sementara lokalnya, sebelum mengenkripsi mereka menggunakan perpustakaan. [pypdf](#)

Terakhir, fungsi menggunakan Boto3 SDK untuk menyimpan file terenkripsi di bucket tujuan S3 Anda.

requirements.txt file manifes

Salin dan tempel kode berikut ke dalam file bernama `requirements.txt`.

```
boto3
pypdf
```

Untuk contoh ini, kode fungsi Anda hanya memiliki dua dependensi yang bukan bagian dari pustaka Python standar - untuk SDK Python (Boto3) dan pypdf paket yang digunakan fungsi untuk melakukan enkripsi. PDF

Note

Versi SDK untuk Python (Boto3) disertakan sebagai bagian dari runtime Lambda, sehingga kode Anda akan berjalan tanpa menambahkan Boto3 ke paket penerapan fungsi Anda. Namun, untuk mempertahankan kontrol penuh dependensi fungsi Anda dan menghindari kemungkinan masalah dengan misalignment versi, praktik terbaik untuk Python adalah menyertakan semua dependensi fungsi dalam paket penerapan fungsi Anda. Lihat [the section called “Dependensi runtime dengan Python”](#) untuk mempelajari selengkapnya.

AWS SAM template

Salin dan tempel kode berikut ke dalam file bernama `template.yaml`.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Resources:
  EncryptPDFFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: EncryptPDF
      Architectures: [x86_64]
      CodeUri: ./
      Handler: lambda_function.lambda_handler
      Runtime: python3.12
      Timeout: 15
      MemorySize: 256
      LoggingConfig:
        LogFormat: JSON
      Policies:
        - AmazonS3FullAccess
      Events:
        S3Event:
```

```
Type: S3
Properties:
  Bucket: !Ref PDFSourceBucket
  Events: s3:ObjectCreated:*
```

```
PDFSourceBucket:
  Type: AWS::S3::Bucket
  Properties:
    BucketName: EXAMPLE-BUCKET
```

```
EncryptedPDFBucket:
  Type: AWS::S3::Bucket
  Properties:
    BucketName: EXAMPLE-BUCKET-encrypted
```

AWS SAM Template menentukan sumber daya yang Anda buat untuk aplikasi Anda. Dalam contoh ini, template mendefinisikan fungsi Lambda menggunakan `AWS::Serverless::Function` tipe dan dua bucket S3 menggunakan tipe `AWS::S3::Bucket`. Nama bucket yang ditentukan dalam template adalah placeholder. Sebelum menerapkan aplikasi AWS SAM, Anda perlu mengedit template untuk mengganti nama bucket dengan nama unik global yang memenuhi aturan penamaan bucket [S3](#). Langkah ini dijelaskan lebih lanjut dalam [the section called “Menyebarkan sumber daya menggunakan AWS SAM”](#).

Definisi sumber daya fungsi Lambda mengonfigurasi pemicu untuk fungsi menggunakan properti event. `S3Event` Pemicu ini menyebabkan fungsi Anda dipanggil setiap kali objek dibuat di bucket sumber Anda.

Definisi fungsi juga menentukan kebijakan AWS Identity and Access Management (IAM) yang akan dilampirkan ke [peran eksekusi](#) fungsi. [Kebijakan AWS terkelola](#) `AmazonS3FullAccess` memberi fungsi Anda izin yang diperlukan untuk membaca dan menulis objek ke Amazon S3.

Skrip pengujian otomatis

Salin dan tempel kode berikut ke dalam file bernama `test_pdf_encrypt.py`.

```
import boto3
import json
import pytest
import time
import os

@pytest.fixture
```



```
def lambda_client():
    return boto3.client('lambda')

@pytest.fixture
def s3_client():
    return boto3.client('s3')

@pytest.fixture
def logs_client():
    return boto3.client('logs')

@pytest.fixture(scope='session')
def cleanup():
    # Create a new S3 client for cleanup
    s3_client = boto3.client('s3')

    yield

    # Cleanup code will be executed after all tests have finished

    # Delete test.pdf from the source bucket
    source_bucket = 'EXAMPLE-BUCKET'
    source_file_key = 'test.pdf'
    s3_client.delete_object(Bucket=source_bucket, Key=source_file_key)
    print(f"\nDeleted {source_file_key} from {source_bucket}")

    # Delete test_encrypted.pdf from the destination bucket
    destination_bucket = 'EXAMPLE-BUCKET-encrypted'
    destination_file_key = 'test_encrypted.pdf'
    s3_client.delete_object(Bucket=destination_bucket, Key=destination_file_key)
    print(f"Deleted {destination_file_key} from {destination_bucket}")

@pytest.mark.order(1)
def test_source_bucket_available(s3_client):
    s3_bucket_name = 'EXAMPLE-BUCKET'
    file_name = 'test.pdf'
    file_path = os.path.join(os.path.dirname(__file__), file_name)

    file_uploaded = False
    try:
        s3_client.upload_file(file_path, s3_bucket_name, file_name)
        file_uploaded = True
    except:
        print("Error: couldn't upload file")
```

```
    assert file_uploaded, "Could not upload file to S3 bucket"

@pytest.mark.order(2)
def test_lambda_invoked(logs_client):

    # Wait for a few seconds to make sure the logs are available
    time.sleep(5)

    # Get the latest log stream for the specified log group
    log_streams = logs_client.describe_log_streams(
        logGroupName='/aws/lambda/EncryptPDF',
        orderBy='LastEventTime',
        descending=True,
        limit=1
    )

    latest_log_stream_name = log_streams['logStreams'][0]['logStreamName']

    # Retrieve the log events from the latest log stream
    log_events = logs_client.get_log_events(
        logGroupName='/aws/lambda/EncryptPDF',
        logStreamName=latest_log_stream_name
    )

    success_found = False
    for event in log_events['events']:
        message = json.loads(event['message'])
        status = message.get('record', {}).get('status')
        if status == 'success':
            success_found = True
            break

    assert success_found, "Lambda function execution did not report 'success' status in logs."

@pytest.mark.order(3)
def test_encrypted_file_in_bucket(s3_client):
    # Specify the destination S3 bucket and the expected converted file key
    destination_bucket = 'EXAMPLE-BUCKET-encrypted'
    converted_file_key = 'test_encrypted.pdf'
```

```

try:
    # Attempt to retrieve the metadata of the converted file from the destination
    S3 bucket
    s3_client.head_object(Bucket=destination_bucket, Key=converted_file_key)
except s3_client.exceptions.ClientError as e:
    # If the file is not found, the test will fail
    pytest.fail(f"Converted file '{converted_file_key}' not found in the
destination bucket: {str(e)}")

def test_cleanup(cleanup):
    # This test uses the cleanup fixture and will be executed last
    pass

```

Skrip pengujian otomatis menjalankan tiga fungsi pengujian untuk mengonfirmasi pengoperasian aplikasi Anda yang benar:

- Pengujian `test_source_bucket_available` mengonfirmasi bahwa bucket sumber Anda telah berhasil dibuat dengan mengunggah PDF file pengujian ke bucket.
- Pengujian `test_lambda_invoked` menginterogasi aliran CloudWatch log Log terbaru untuk fungsi Anda guna mengonfirmasi bahwa saat Anda mengunggah file pengujian, fungsi Lambda Anda berjalan dan melaporkan keberhasilan.
- Pengujian `test_encrypted_file_in_bucket` mengonfirmasi bahwa bucket tujuan Anda berisi file terenkripsi. `test_encrypted.pdf`

Setelah semua pengujian ini berjalan, skrip menjalankan langkah pembersihan tambahan untuk menghapus `test.pdf` dan `test_encrypted.pdf` file dari bucket sumber dan tujuan Anda.

Seperti halnya AWS SAM template, nama bucket yang ditentukan dalam file ini adalah placeholder. Sebelum menjalankan pengujian, Anda perlu mengedit file ini dengan nama bucket asli aplikasi Anda. Langkah ini dijelaskan lebih lanjut dalam [the section called “Menguji aplikasi dengan skrip otomatis”](#)

File konfigurasi skrip uji

Salin dan tempel kode berikut ke dalam file bernama `pytest.ini`.

```

[pytest]
markers =
    order: specify test execution order

```

Ini diperlukan untuk menentukan urutan pengujian dalam `test_pdf_encrypt.py` skrip berjalan.

Menerapkan aplikasi

Anda dapat membuat dan menerapkan sumber daya untuk aplikasi contoh ini baik secara manual atau dengan menggunakan AWS SAM. Dalam lingkungan produksi, kami menyarankan Anda menggunakan alat IAC AWS SAM untuk menyebarkan seluruh aplikasi tanpa server dengan cepat dan berulang tanpa menggunakan proses manual.

Untuk contoh ini, ikuti konsol atau AWS CLI instruksi untuk mempelajari cara mengonfigurasi setiap AWS sumber daya secara terpisah, atau lanjutkan [the section called “Menyebarkan sumber daya menggunakan AWS SAM”](#) untuk menerapkan aplikasi dengan cepat menggunakan beberapa CLI perintah.

Menyebarkan sumber daya secara manual

Untuk menerapkan aplikasi secara manual, Anda melakukan langkah-langkah berikut:

- Buat bucket S3 sumber dan tujuan
- Buat fungsi Lambda yang mengenkripsi PDF file dan menyimpan versi terenkripsi ke bucket S3
- Konfigurasi pemicu Lambda yang memanggil fungsi Anda saat objek diunggah ke bucket sumber

Ikuti petunjuk dalam paragraf berikut untuk membuat dan mengonfigurasi sumber daya Anda.

Buat dua ember S3

Pertama buat dua ember S3. Bucket pertama adalah bucket sumber tempat Anda akan mengunggah PDF file Anda. Bucket kedua digunakan oleh Lambda untuk menyimpan file terenkripsi saat Anda menjalankan fungsi.

Console

Untuk membuat bucket S3 (konsol)

1. Buka halaman [Bucket](#) konsol Amazon S3.
2. Pilih Buat bucket.
3. Pada Konfigurasi umum, lakukan hal berikut:

- a. Untuk nama Bucket, masukkan nama unik global yang memenuhi aturan [penamaan Amazon S3 Bucket](#). Nama bucket hanya dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-).
 - b. Untuk Wilayah AWS, pilih yang paling [Wilayah AWS](#) dekat dengan lokasi geografis Anda. Kemudian dalam proses penerapan, Anda harus membuat fungsi Lambda Anda dalam Wilayah AWS hal yang sama, jadi catat wilayah yang Anda pilih.
4. Biarkan semua opsi lain disetel ke nilai defaultnya dan pilih Buat bucket.
 5. Ulangi langkah 1 hingga 4 untuk membuat bucket tujuan Anda. Untuk nama Bucket **SOURCEBUCKET-encrypted**, masukkan, di **SOURCEBUCKET** mana nama bucket sumber yang baru saja Anda buat.

AWS CLI

Untuk membuat bucket S3 ()AWS CLI

1. Jalankan CLI perintah berikut untuk membuat bucket sumber Anda. Nama yang Anda pilih untuk bucket Anda harus unik secara global dan ikuti aturan [penamaan Amazon S3 Bucket](#). Nama hanya dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-). Untuk region dan LocationConstraint, pilih yang paling [Wilayah AWS](#) dekat dengan lokasi geografis Anda.

```
aws s3api create-bucket --bucket SOURCEBUCKET --region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2
```

Kemudian dalam tutorial, Anda harus membuat fungsi Lambda Anda Wilayah AWS sama dengan bucket sumber Anda, jadi catat wilayah yang Anda pilih.

2. Jalankan perintah berikut untuk membuat bucket tujuan Anda. Untuk nama bucket, Anda harus menggunakan **SOURCEBUCKET-encrypted**, di **SOURCEBUCKET** mana nama bucket sumber yang Anda buat di langkah 1. Untuk region dan LocationConstraint, pilih yang sama dengan yang Wilayah AWS Anda gunakan untuk membuat bucket sumber Anda.

```
aws s3api create-bucket --bucket SOURCEBUCKET-encrypted --region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2
```

Buat peran eksekusi (AWS CLI hanya)

Peran eksekusi adalah IAM peran yang memberikan izin fungsi Lambda untuk AWS layanan mengakses dan sumber daya. Saat Anda membuat fungsi menggunakan konsol Lambda, Lambda secara otomatis membuat peran eksekusi. Anda hanya perlu membuat peran secara manual jika Anda memilih untuk menerapkan aplikasi menggunakan AWS CLI Untuk memberikan akses baca dan tulis fungsi Anda ke Amazon S3, Anda melampirkan kebijakan [AWS terkelola](#). `AmazonS3FullAccess`

Console

Langkah ini hanya diperlukan jika Anda memilih untuk menerapkan aplikasi Anda menggunakan AWS CLI

AWS CLI

Untuk membuat peran eksekusi dan melampirkan kebijakan **AmazonS3FullAccess** terkelola (AWS CLI)

1. Simpan berikut ini JSON dalam file bernama `trust-policy.json`. Kebijakan kepercayaan ini memungkinkan Lambda untuk menggunakan izin peran dengan memberikan `lambda.amazonaws.com` izin utama layanan untuk memanggil tindakan AWS Security Token Service (`sts:AssumeRole`)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Dari direktori tempat Anda menyimpan dokumen kebijakan JSON kepercayaan, jalankan CLI perintah berikut untuk membuat peran eksekusi.

```
aws iam create-role --role-name LambdaS3Role --assume-role-policy-document
file://trust-policy.json
```

3. Untuk melampirkan kebijakan AmazonS3FullAccess terkelola, jalankan CLI perintah berikut.

```
aws iam attach-role-policy --role-name LambdaS3Role --policy-arn
arn:aws:iam::aws:policy/AmazonS3FullAccess
```

Buat paket penerapan fungsi

Untuk membuat fungsi Anda, Anda membuat paket deployment yang berisi kode fungsi dan dependensinya. Untuk aplikasi ini, kode fungsi Anda menggunakan pustaka terpisah untuk PDF enkripsi.

Untuk membuat paket deployment

1. Arahkan ke direktori proyek yang berisi `lambda_function.py` dan `requirements.txt` file yang Anda buat atau unduh dari GitHub sebelumnya dan buat direktori baru bernama `package`.
2. Instal dependensi yang ditentukan dalam `requirements.txt` file di `package` direktori Anda dengan menjalankan perintah berikut.

```
pip install -r requirements.txt --target ./package/
```

3. Buat `file.zip` yang berisi kode aplikasi Anda dan dependensinya. Di Linux atau macOS, jalankan perintah berikut dari antarmuka baris perintah Anda.

```
cd package
zip -r ../lambda_function.zip .
cd ..
zip lambda_function.zip lambda_function.py
```

Di Windows, gunakan alat zip pilihan Anda untuk membuat `file.zip`. Pastikan bahwa `lambda_function.py` file Anda dan folder yang berisi dependensi Anda semuanya berada di root `file.zip`.

Anda juga dapat membuat paket deployment menggunakan lingkungan virtual Python. Lihat [Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#)

Buat fungsi Lambda

Anda sekarang menggunakan paket penyebaran yang Anda buat pada langkah sebelumnya untuk menyebarkan fungsi Lambda Anda.

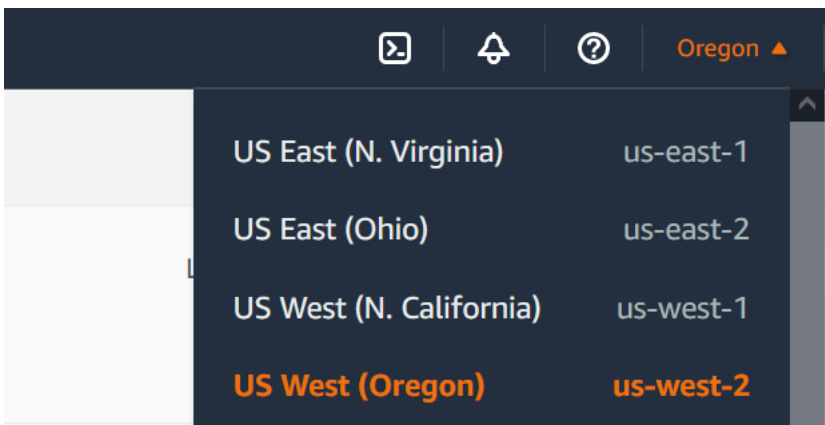
Console

Untuk membuat fungsi (konsol)

Untuk membuat fungsi Lambda Anda menggunakan konsol, pertama-tama Anda membuat fungsi dasar yang berisi beberapa kode 'Hello world'. Anda kemudian mengganti kode ini dengan kode fungsi Anda sendiri dengan mengunggah file the.zip yang Anda buat pada langkah sebelumnya.

Untuk memastikan bahwa fungsi Anda tidak habis saat mengenkripsi PDF file besar, Anda mengonfigurasi pengaturan memori dan batas waktu fungsi. Anda juga mengatur format log fungsi keJSON. Mengkonfigurasi log JSON yang diformat diperlukan saat menggunakan skrip pengujian yang disediakan sehingga dapat membaca status pemanggilan fungsi dari CloudWatch Log untuk mengonfirmasi pemanggilan yang berhasil.

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pastikan Anda bekerja di tempat yang sama saat Wilayah AWS Anda membuat bucket S3. Anda dapat mengubah wilayah Anda menggunakan daftar drop-down di bagian atas layar.



3. Pilih Buat fungsi.
4. Pilih Penulis dari scratch.
5. Di bagian Informasi dasar, lakukan hal berikut:

- a. Untuk Nama fungsi, masukkan **EncryptPDF**.
 - b. Untuk Runtime pilih Python 3.12.
 - c. Untuk Arsitektur, pilih x86_64.
6. Pilih Buat fungsi.

Untuk mengunggah kode fungsi (konsol)

1. Di panel Sumber kode, pilih Unggah dari.
2. Pilih file.zip.
3. Pilih Unggah.
4. Di pemilih file, pilih file.zip Anda dan pilih Buka.
5. Pilih Simpan.

Untuk mengkonfigurasi memori fungsi dan batas waktu (konsol)

1. Pilih tab Konfigurasi untuk fungsi Anda.
2. Di panel konfigurasi Umum, pilih Edit.
3. Atur Memori ke 256 MB dan Timeout menjadi 15 detik.
4. Pilih Simpan.

Untuk mengkonfigurasi format log (konsol)

1. Pilih tab Konfigurasi untuk fungsi Anda.
2. Pilih Alat pemantauan dan operasi.
3. Di panel konfigurasi Logging, pilih Edit.
4. Untuk konfigurasi Logging, pilih JSON.
5. Pilih Simpan.

AWS CLI

Untuk membuat fungsi (AWS CLI)

- Jalankan perintah berikut dari direktori yang berisi `lambda_function.zip` file Anda. Untuk region parameternya, ganti `us-west-2` dengan wilayah tempat Anda membuat bucket S3.

```
aws lambda create-function --function-name EncryptPDF \  
--zip-file fileb://lambda_function.zip --handler lambda_function.lambda_handler \  
\  
--runtime python3.12 --timeout 15 --memory-size 256 \  
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-west-2 \  
--logging-config LogFormat=JSON
```

Konfigurasi pemicu Amazon S3 untuk menjalankan fungsi

Agar fungsi Lambda dapat berjalan saat mengunggah file ke bucket sumber, Anda perlu mengonfigurasi pemicu untuk fungsi Anda. Anda dapat mengonfigurasi pemicu Amazon S3 menggunakan konsol atau AWS CLI

Important

Prosedur ini mengonfigurasi bucket S3 untuk memanggil fungsi Anda setiap kali objek dibuat di bucket. Pastikan untuk mengonfigurasi ini hanya di bucket sumber. Jika fungsi Lambda Anda membuat objek dalam bucket yang sama yang memanggilnya, fungsi Anda dapat [dipanggil terus menerus](#) dalam satu loop. Hal ini dapat mengakibatkan biaya yang tidak diharapkan ditagih ke Anda Akun AWS.

Console

Untuk mengonfigurasi pemicu Amazon S3 (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda (`()EncryptPDF`).
2. Pilih Tambahkan pemicu.
3. Pilih S3.
4. Di bawah Bucket, pilih bucket sumber Anda.
5. Di bawah Jenis acara, pilih Semua objek membuat acara.

6. Di bawah Pemanggilan rekursif, pilih kotak centang untuk mengetahui bahwa tidak disarankan menggunakan bucket S3 yang sama untuk input dan output. Anda dapat mempelajari lebih lanjut tentang pola pemanggilan rekursif di Lambda dengan membaca [pola rekursif yang menyebabkan fungsi Lambda yang tidak terkendali](#) di Tanah Tanpa Server.
7. Pilih Tambahkan.

Saat Anda membuat pemacu menggunakan konsol Lambda, Lambda secara otomatis membuat [kebijakan berbasis sumber daya](#) untuk memberikan layanan yang Anda pilih izin untuk menjalankan fungsi Anda.

AWS CLI

Untuk mengonfigurasi pemacu Amazon S3 (AWS CLI)

1. [Agar bucket sumber Amazon S3 menjalankan fungsi saat menambahkan file, pertama-tama Anda harus mengonfigurasi izin untuk fungsi menggunakan kebijakan berbasis sumber daya.](#) Pernyataan kebijakan berbasis sumber daya memberikan AWS layanan izin lain untuk menjalankan fungsi Anda. Untuk memberikan izin Amazon S3 untuk menjalankan fungsi Anda, jalankan perintah berikut. CLI Pastikan untuk mengganti `source-account` parameter dengan Akun AWS ID Anda sendiri dan menggunakan nama bucket sumber Anda sendiri.

```
aws lambda add-permission --function-name EncryptPDF \  
--principal s3.amazonaws.com --statement-id s3invoke --action \  
"lambda:InvokeFunction" \  
--source-arn arn:aws:s3:::SOURCEBUCKET \  
--source-account 123456789012
```

Kebijakan yang Anda tetapkan dengan perintah ini memungkinkan Amazon S3 untuk menjalankan fungsi Anda hanya ketika tindakan dilakukan di bucket sumber Anda.

Note

Meskipun nama bucket S3 unik secara global, saat menggunakan kebijakan berbasis sumber daya, praktik terbaik adalah menentukan bahwa bucket harus milik akun Anda. Ini karena jika Anda menghapus bucket, Anda dapat membuat bucket dengan Amazon Resource Name (ARN) yang sama. Akun AWS

2. Simpan berikut ini JSON dalam file bernama `notification.json`. Saat diterapkan ke bucket sumber Anda, ini akan JSON mengonfigurasi bucket untuk mengirim notifikasi ke fungsi Lambda Anda setiap kali objek baru ditambahkan. Ganti Akun AWS nomor dan Wilayah AWS dalam fungsi Lambda ARN dengan nomor akun dan wilayah Anda sendiri.

```
{
  "LambdaFunctionConfigurations": [
    {
      "Id": "EncryptPDFEventConfiguration",
      "LambdaFunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:EncryptPDF",
      "Events": [ "s3:ObjectCreated:Put" ]
    }
  ]
}
```

3. Jalankan CLI perintah berikut untuk menerapkan pengaturan notifikasi dalam JSON file yang Anda buat ke bucket sumber Anda. Ganti `SOURCEBUCKET` dengan nama bucket sumber Anda sendiri.

```
aws s3api put-bucket-notification-configuration --bucket SOURCEBUCKET \
--notification-configuration file://notification.json
```

Untuk mempelajari lebih lanjut tentang `put-bucket-notification-configuration` perintah dan `notification-configuration` opsi, lihat [put-bucket-notification-configuration](#) di Referensi AWS CLI Perintah.

Menyebarkan sumber daya menggunakan AWS SAM

Untuk menerapkan aplikasi contoh menggunakan AWS SAM CLI, lakukan langkah-langkah berikut.

Pastikan Anda telah [menginstal versi terbaru CLI](#) dan [Docker](#) diinstal pada mesin build Anda.

1. Edit `template.yaml` file untuk menentukan nama bucket S3 Anda. Bucket S3 harus memiliki nama unik secara global yang memenuhi aturan penamaan [bucket S3](#).

Ganti nama bucket `EXAMPLE-BUCKET` dengan nama pilihan Anda yang terdiri dari huruf kecil, angka, titik (`.`), dan tanda hubung (`-`). Untuk bucket tujuan, ganti `EXAMPLE-BUCKET-encrypted` dengan `<source-bucket-name>-encrypted`, di `<source-bucket>` mana nama yang Anda pilih untuk bucket sumber Anda.

2. Jalankan perintah berikut dari direktori tempat Anda menyimpan `template.yaml`, `lambda_function.py`, dan `requirements.txt` file Anda.

```
sam build --use-container
```

Perintah ini mengumpulkan artefak build untuk aplikasi Anda dan menempatkannya dalam format dan lokasi yang tepat untuk menerapkannya. Menentukan `--use-container` opsi membangun fungsi Anda di dalam wadah Docker seperti Lambda. Kami menggunakannya di sini sehingga Anda tidak perlu menginstal Python 3.12 di mesin lokal Anda agar build berfungsi.

Selama proses build, AWS SAM cari kode fungsi Lambda di lokasi yang Anda tentukan dengan `CodeUri` properti di `template`. Dalam hal ini, kami menentukan direktori saat ini sebagai `location` (`./`).

Jika ada `requirements.txt` file, AWS SAM gunakan untuk mengumpulkan dependensi yang ditentukan. Secara default, AWS SAM buat paket deployment `.zip` dengan kode fungsi dan dependensi Anda. Anda juga dapat memilih untuk menerapkan fungsi Anda sebagai gambar kontainer menggunakan `PackageType` properti.

3. Untuk menerapkan aplikasi Anda dan membuat sumber daya Lambda dan Amazon S3 yang ditentukan dalam `template` AWS SAM Anda, jalankan perintah berikut.

```
sam deploy --guided
```

Menggunakan `--guided` tanda berarti itu AWS SAM akan menunjukkan kepada Anda petunjuk untuk memandu Anda melalui proses penerapan. Untuk penerapan ini, terima opsi default dengan menekan Enter.

Selama proses penerapan, AWS SAM buat sumber daya berikut di: Akun AWS

- Sebuah AWS CloudFormation [tumpukan](#) bernama `sam-app`
- Fungsi Lambda dengan nama `EncryptPDF`
- Dua ember S3 dengan nama yang Anda pilih saat Anda mengedit file `template.yaml` AWS SAM
- Peran IAM eksekusi untuk fungsi Anda dengan format nama `sam-app-EncryptPDFFunctionRole-2qGaapHFWOQ8`

Ketika AWS SAM selesai membuat sumber daya Anda, Anda akan melihat pesan berikut:

```
Successfully created/updated stack - sam-app in us-west-2
```

Menguji aplikasi

Untuk menguji aplikasi, Anda mengunggah PDF file ke bucket sumber, dan mengonfirmasi bahwa Lambda membuat versi file terenkripsi di bucket tujuan. Dalam contoh ini, Anda dapat menguji ini secara manual menggunakan konsol atau AWS CLI, atau dengan menggunakan skrip pengujian yang disediakan.

Untuk aplikasi produksi, Anda dapat menggunakan metode dan teknik pengujian tradisional, seperti pengujian unit, untuk mengonfirmasi berfungsinya kode fungsi Lambda Anda dengan benar. Praktik terbaik juga melakukan pengujian seperti yang ada di skrip pengujian yang disediakan yang melakukan pengujian integrasi dengan sumber daya berbasis cloud yang nyata. Pengujian integrasi di cloud mengonfirmasi bahwa infrastruktur Anda telah digunakan dengan benar dan bahwa peristiwa mengalir di antara berbagai layanan seperti yang diharapkan. Untuk mempelajari selengkapnya, lihat [Menguji fungsi tanpa server](#).

Menguji aplikasi secara manual

Anda dapat menguji fungsi Anda secara manual dengan menambahkan PDF file ke bucket sumber Amazon S3 Anda. Saat Anda menambahkan file ke bucket sumber, fungsi Lambda Anda akan dipanggil secara otomatis dan harus menyimpan versi file terenkripsi di bucket target Anda.

Console

Untuk menguji aplikasi Anda dengan mengunggah file (konsol)

1. Untuk mengunggah PDF file ke bucket S3 Anda, lakukan hal berikut:
 - a. Buka halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket sumber Anda.
 - b. Pilih Unggah.
 - c. Pilih Tambahkan file dan gunakan pemilih file untuk memilih PDF file yang ingin Anda unggah.
 - d. Pilih Buka, lalu pilih Unggah.
2. Verifikasi bahwa Lambda telah menyimpan versi terenkripsi PDF file Anda di bucket target Anda dengan melakukan hal berikut:

- a. Arahkan kembali ke halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket tujuan Anda.
- b. Di panel Objects, Anda sekarang akan melihat file dengan format nama `filename_encrypted.pdf` (di mana `filename.pdf` nama file yang Anda unggah ke bucket sumber Anda). Untuk mengunduh file terenkripsi Anda PDF, pilih file, lalu pilih Unduh.
- c. Konfirmasikan bahwa Anda dapat membuka file yang diunduh dengan kata sandi fungsi Lambda Anda melindunginya dengan `()my-secret-password`.

AWS CLI

Untuk menguji aplikasi Anda dengan mengunggah file ()AWS CLI

1. Dari direktori yang berisi PDF file yang ingin Anda unggah, jalankan CLI perintah berikut. Ganti `--bucket` parameter dengan nama bucket sumber Anda. Untuk `--body` parameter `--key` dan, gunakan nama file file pengujian Anda.

```
aws s3api put-object --bucket SOURCEBUCKET --key test.pdf --body ./test.pdf
```

2. Verifikasi bahwa fungsi Anda telah membuat versi terenkripsi dari file Anda dan menyimpannya ke bucket S3 target Anda. Jalankan CLI perintah berikut, ganti `SOURCEBUCKET-encrypted` dengan nama bucket tujuan Anda sendiri.

```
aws s3api list-objects-v2 --bucket SOURCEBUCKET-encrypted
```

Jika fungsi Anda berjalan dengan sukses, Anda akan melihat output yang mirip dengan berikut ini. Bucket target Anda harus berisi file dengan format nama `<your_test_file>_encrypted.pdf`, di `<your_test_file>` mana nama file yang Anda unggah.

```
{
  "Contents": [
    {
      "Key": "test_encrypted.pdf",
      "LastModified": "2023-06-07T00:15:50+00:00",
      "ETag": "\"7781a43e765a8301713f533d70968a1e\"",
      "Size": 2763,
      "StorageClass": "STANDARD"
    }
  ]
}
```

```
]
}
```

- Untuk mengunduh file yang disimpan Lambda di bucket tujuan Anda, jalankan perintah berikut CLI. Ganti `--bucket` parameter dengan nama bucket tujuan Anda. Untuk `--key` parameternya, gunakan nama file `<your_test_file>_encrypted.pdf`, di `<your_test_file>` mana nama file pengujian yang Anda unggah.

```
aws s3api get-object --bucket SOURCEBUCKET-encrypted --key test_encrypted.pdf
my_encrypted_file.pdf
```

Perintah ini mengunduh file ke direktori Anda saat ini dan menyimpannya sebagai `my_encrypted_file.pdf`.

- Konfirmasikan bahwa Anda dapat membuka file yang diunduh dengan kata sandi fungsi Lambda Anda melindunginya dengan `()my-secret-password`.

Menguji aplikasi dengan skrip otomatis

Untuk menguji aplikasi Anda menggunakan skrip pengujian yang disediakan, pertama-tama pastikan bahwa `pytest` modul diinstal di lingkungan lokal Anda. Anda dapat menginstal `pytest` dengan menjalankan perintah berikut:

```
pip install pytest
```

Anda juga perlu mengedit kode dalam `test_pdf_encrypt.py` file untuk mengganti nama bucket placeholder dengan nama bucket sumber dan tujuan Amazon S3 Anda. Buat perubahan berikut ke `test_pdf_encrypt.py`:

- Dalam `test_source_bucket_available` fungsinya, ganti `EXAMPLE-BUCKET` dengan nama bucket sumber Anda.
- Dalam `test_encrypted_file_in_bucket` fungsinya, ganti `EXAMPLE-BUCKET-encrypted` dengan `<source-bucket>-encrypted`, di `<source-bucket>` mana nama bucket sumber Anda.
- Dalam `cleanup` fungsi, ganti `EXAMPLE-BUCKET` dengan nama bucket sumber Anda, dan ganti `EXAMPLE-BUCKET-encrypted` dengan `#<source-bucket>-encrypted`, di `<source-bucket>` mana nama bucket sumber Anda.

Untuk menjalankan tes lakukan hal berikut:

- Simpan PDF file bernama `test.pdf` dalam direktori yang berisi `pytest.ini` file `test_pdf_encrypt.py` dan.
- Buka terminal atau program shell dan jalankan perintah berikut dari direktori yang berisi file uji.

```
pytest -s -v
```

Ketika tes selesai, Anda akan melihat output seperti berikut:

```
===== test session starts
=====
platform linux -- Python 3.12.2, pytest-7.2.2, pluggy-1.0.0 -- /usr/bin/python3
cachedir: .pytest_cache
hypothesis profile 'default' -> database=DirectoryBasedExampleDatabase('/home/pdf_encrypt_app/.hypothesis/examples')
Test order randomisation NOT enabled. Enable with --random-order or --random-order-bucket=<bucket_type>
rootdir: /home/pdf_encrypt_app, configfile: pytest.ini
plugins: anyio-3.7.1, hypothesis-6.70.0, localserver-0.7.1, random-order-1.1.0
collected 4 items

test_pdf_encrypt.py::test_source_bucket_available PASSED
test_pdf_encrypt.py::test_lambda_invoked PASSED
test_pdf_encrypt.py::test_encrypted_file_in_bucket PASSED
test_pdf_encrypt.py::test_cleanup PASSED
Deleted test.pdf from EXAMPLE-BUCKET
Deleted test_encrypted.pdf from EXAMPLE-BUCKET-encrypted

===== 4 passed in 7.32s
=====
```

Langkah selanjutnya

Sekarang Anda telah membuat aplikasi contoh ini, Anda dapat menggunakan kode yang disediakan sebagai dasar untuk membuat jenis aplikasi pemrosesan file lainnya. Ubah kode dalam `lambda_function.py` file untuk mengimplementasikan logika pemrosesan file untuk kasus penggunaan Anda.

Banyak kasus penggunaan pemrosesan file yang khas melibatkan pemrosesan gambar. Saat menggunakan Python, perpustakaan pemrosesan gambar yang paling populer seperti [bantal](#) biasanya berisi komponen C atau C ++. Untuk memastikan bahwa paket penerapan fungsi Anda kompatibel dengan lingkungan eksekusi Lambda, penting untuk menggunakan biner distribusi sumber yang benar.

Saat menerapkan sumber daya Anda AWS SAM, Anda perlu mengambil beberapa langkah ekstra untuk menyertakan distribusi sumber yang tepat dalam paket penerapan Anda. Karena AWS SAM tidak akan menginstal dependensi untuk platform yang berbeda dari mesin build Anda, menentukan distribusi sumber (.whlfile) yang benar dalam `requirements.txt` file Anda tidak akan berfungsi jika mesin build Anda menggunakan sistem operasi atau arsitektur yang berbeda dari lingkungan eksekusi Lambda. Sebagai gantinya, Anda harus melakukan salah satu hal berikut:

- Gunakan `--use-container` opsi saat menjalankansam `build`. Saat Anda menentukan opsi ini, AWS SAM unduh gambar dasar kontainer yang kompatibel dengan lingkungan eksekusi Lambda dan buat paket penerapan fungsi Anda dalam wadah Docker menggunakan gambar itu. Untuk mempelajari lebih lanjut, lihat [Membangun fungsi Lambda di dalam wadah yang disediakan](#).
- Buat sendiri paket.zip deployment fungsi Anda menggunakan biner distribusi sumber yang benar dan simpan file.zip di direktori yang Anda tentukan seperti `CodeUri` di template. AWS SAM Untuk mempelajari lebih lanjut tentang membangun paket deployment .zip untuk Python menggunakan distribusi biner, lihat dan. [the section called “Membuat paket penerapan.zip dengan dependensi”](#) [the section called “Membuat paket penerapan.zip dengan pustaka asli”](#)

Memahami konsep Lambda utama

Lambda adalah layanan komputasi berbasis peristiwa yang menjalankan instance fungsi Anda untuk memproses peristiwa. Anda dapat menjalankan fungsi Anda secara langsung menggunakan API Lambda, atau Anda dapat mengonfigurasi AWS layanan atau sumber daya untuk menjalankan fungsi Anda.

Bagian berikut menjelaskan beberapa konsep kunci fungsi Lambda, model pemrograman berbasis peristiwa, dan lingkungan fungsi Anda berjalan di dalamnya.

Konsep

- [Fungsi](#)
- [Pemicu](#)
- [Peristiwa](#)
- [Lingkungan eksekusi](#)
- [Paket deployment](#)
- [Waktu Aktif](#)
- [Lapisan](#)
- [Konkurensi](#)
- [Pengualifikasi](#)
- [Tujuan](#)

Fungsi

Fungsi adalah sumber daya yang dapat Anda panggil untuk menjalankan kode Anda di Lambda. Fungsi memiliki kode untuk memproses [peristiwa](#) yang Anda lewatkan ke fungsi atau AWS layanan lain yang dikirim ke fungsi tersebut.

Pemicu

Pemicu adalah sumber daya atau konfigurasi yang memanggil fungsi Lambda. Pemicu mencakup AWS layanan yang dapat Anda konfigurasi untuk memanggil fungsi dan pemetaan [sumber peristiwa](#). Pemetaan sumber peristiwa adalah sumber daya di Lambda yang membaca item dari

arus atau antrean dan mengaktifkan fungsi. Untuk informasi selengkapnya, silakan lihat [Memahami metode pemanggilan fungsi Lambda](#) dan [Memanggil Lambda dengan acara dari layanan lain AWS](#).

Peristiwa

Peristiwa adalah dokumen JSON berformat yang berisi data untuk fungsi Lambda untuk diproses. Runtime mengonversi peristiwa menjadi objek dan meneruskannya ke kode fungsi Anda. Saat Anda memanggil fungsi, Anda menentukan struktur dan konten peristiwa.

Example peristiwa kustom – data cuaca

```
{
  "TemperatureK": 281,
  "WindKmh": -3,
  "HumidityPct": 0.55,
  "PressureHPa": 1020
}
```

Ketika AWS layanan memanggil fungsi Anda, layanan menentukan bentuk acara.

Example acara layanan - SNS Pemberitahuan Amazon

```
{
  "Records": [
    {
      "Sns": {
        "Timestamp": "2019-01-02T12:45:07.000Z",
        "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi+tE/1+82j...65r==",
        "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
        "Message": "Hello from SNS!",
        ...
      }
    }
  ]
}
```

Untuk informasi selengkapnya tentang acara dari AWS layanan, lihat [Memanggil Lambda dengan acara dari layanan lain AWS](#).

Lingkungan eksekusi

Lingkungan eksekusi menyediakan lingkungan runtime yang aman dan terisolasi tempat Lambda mengaktifkan fungsi Anda. Lingkungan eksekusi mengelola proses dan sumber daya yang diperlukan

untuk menjalankan fungsi Anda. Lingkungan eksekusi menyediakan dukungan siklus hidup untuk runtime dan untuk [ekstensi](#) apa pun yang berkaitan dengan fungsi Anda.

Untuk informasi selengkapnya, lihat [Memahami siklus hidup lingkungan eksekusi Lambda](#).

Paket deployment

Anda men-deploy kode fungsi Lambda Anda menggunakan paket deployment. Lambda mendukung dua tipe paket deployment:

- Buat arsip file .zip yang berisi kode fungsi dan dependensi Anda. Lambda menyediakan sistem operasi dan runtime untuk fungsi Anda. Untuk informasi selengkapnya, lihat [Menyebarkan fungsi Lambda sebagai arsip file.zip](#).
- Gambar kontainer yang kompatibel dengan spesifikasi [Open Container Initiative \(OCI\)](#). Anda menambahkan kode fungsi dan dependensi ke gambar. Anda juga harus menyertakan sistem operasi dan runtime Lambda. Untuk informasi selengkapnya, lihat [Buat fungsi Lambda menggunakan gambar kontainer](#).

Waktu Aktif

Runtime menyediakan lingkungan khusus bahasa yang berjalan di lingkungan eksekusi. Runtime menyampaikan peristiwa invokasi, informasi konteks, dan respons antara Lambda dan fungsi. Anda dapat menggunakan runtime yang disediakan Lambda, atau membangun sendiri. Jika Anda mengemas kode Anda sebagai arsip file .zip, Anda harus mengonfigurasi fungsi Anda untuk menggunakan runtime yang sesuai dengan bahasa pemrograman Anda. Untuk gambar kontainer, Anda menyertakan runtime ketika Anda membangun gambar.

Untuk informasi selengkapnya, lihat [Runtime Lambda](#).

Lapisan

Lapisan Lambda adalah arsip file .zip yang dapat berisi kode tambahan atau konten lainnya. Lapisan dapat berisi pustaka, [runtime kustom](#), data, atau file konfigurasi.

Lapisan menyediakan cara yang nyaman untuk mengemas pustaka dan dependensi lain yang dapat Anda gunakan dengan fungsi Lambda Anda. Menggunakan lapisan mengurangi ukuran arsip deployment yang diunggah dan membuatnya lebih cepat untuk men-deploy kode Anda. Lapisan juga

mendukung berbagi kode dan pemisahan tanggung jawab agar Anda dapat mengiterasi lebih cepat saat menulis logika bisnis.

Anda dapat menyertakan hingga lima lapisan per fungsi. Lapisan menghitung terhadap standar [kuota ukuran deployment](#) Lambda. Ketika Anda menyertakan lapisan dalam fungsi, konten diekstrak ke direktori `/opt` di lingkungan eksekusi.

Secara default, lapisan yang Anda buat bersifat pribadi untuk AWS akun Anda. Anda dapat memilih untuk berbagi lapisan dengan akun lain atau untuk membuat lapisan menjadi publik. Jika fungsi Anda menggunakan lapisan yang diterbitkan oleh akun lain, fungsi Anda dapat terus menggunakan versi lapisan setelah dihapus, atau setelah izin Anda untuk mengakses layer dicabut. Namun, Anda tidak dapat membuat fungsi baru atau memperbarui fungsi menggunakan versi lapisan yang dihapus.

Fungsi yang di-deploy sebagai gambar kontainer tidak menggunakan lapisan. Sebaliknya, Anda mengemas runtime pilihan, pustaka, dan dependensi lainnya ke dalam kontainer gambar ketika Anda membangun gambar.

Untuk informasi selengkapnya, lihat [Lapisan Lambda](#).

Konkurensi

Konkurensi adalah jumlah permintaan yang dilayani fungsi Anda pada waktu tertentu. Ketika fungsi Anda diaktifkan, Lambda menyediakan instans untuk memproses peristiwa. Saat selesai dijalankan, kode fungsi dapat menangani permintaan lain. Jika fungsi diaktifkan kembali ketika permintaan masih diproses, instans lain disediakan, meningkatkan konkurensi fungsi tersebut.

Konkurensi tunduk pada [kuota](#) di tingkat AWS Wilayah. Anda dapat mengonfigurasi fungsi individu untuk membatasi konkurensi, atau memungkinkan mereka mencapai tingkat konkurensi tertentu. Untuk informasi selengkapnya, lihat [Mengkonfigurasi konkurensi cadangan untuk suatu fungsi](#).

Pengualifikasi

Saat Anda mengaktifkan atau melihat fungsi, Anda dapat menyertakan pengualifikasi untuk menentukan versi atau alias. Versi adalah snapshot tetap dari kode dan konfigurasi fungsi yang memiliki pengualifikasi numerik. Misalnya, `my-function:1`. Alias adalah penunjuk ke versi yang dapat diperbarui untuk memetakan ke versi berbeda, atau membagi lalu lintas di antara dua versi. Misalnya, `my-function:BLUE`. Anda dapat menggunakan versi dan alias bersama-sama untuk menyediakan antarmuka yang stabil bagi klien guna mengaktifkan fungsi Anda.

Untuk informasi selengkapnya, lihat [Kelola versi fungsi Lambda](#).

Tujuan

Tujuan adalah AWS sumber daya tempat Lambda dapat mengirim peristiwa dari pemanggilan asinkron. Anda dapat mengonfigurasi tujuan untuk acara yang gagal diproses. Beberapa layanan juga mendukung tujuan untuk acara yang berhasil diproses.

Untuk informasi selengkapnya, lihat [Menambahkan tujuan](#).

Menggunakan Lambda dengan infrastruktur sebagai kode (IaC)

Lambda menawarkan beberapa cara untuk menyebarkan kode Anda dan membuat fungsi. Misalnya, Anda dapat menggunakan konsol Lambda atau AWS Command Line Interface (AWS CLI) untuk membuat atau memperbarui fungsi Lambda secara manual. Selain opsi manual ini, AWS menawarkan sejumlah solusi untuk menerapkan fungsi Lambda dan aplikasi tanpa server menggunakan infrastruktur sebagai kode (IaC). Dengan IaC, Anda dapat menyediakan dan memelihara fungsi Lambda dan sumber daya AWS lainnya menggunakan kode alih-alih menggunakan proses dan pengaturan manual.

Sebagian besar waktu, fungsi Lambda tidak berjalan secara terpisah. Sebaliknya, mereka membentuk bagian dari aplikasi tanpa server dengan sumber daya lain seperti database, antrian, dan penyimpanan. Dengan IaC, Anda dapat mengotomatiskan proses penyebaran Anda untuk menyebarkan dan memperbarui seluruh aplikasi tanpa server dengan cepat dan berulang yang melibatkan banyak sumber daya terpisah. AWS Pendekatan ini mempercepat siklus pengembangan Anda, membuat manajemen konfigurasi lebih mudah, dan memastikan bahwa sumber daya Anda digunakan dengan cara yang sama setiap saat.

Topik

- [Alat IaC untuk Lambda](#)
- [Memulai dengan IaC untuk Lambda](#)
- [Langkah selanjutnya](#)
- [Daerah yang didukung untuk integrasi Lambda dengan Application Composer](#)

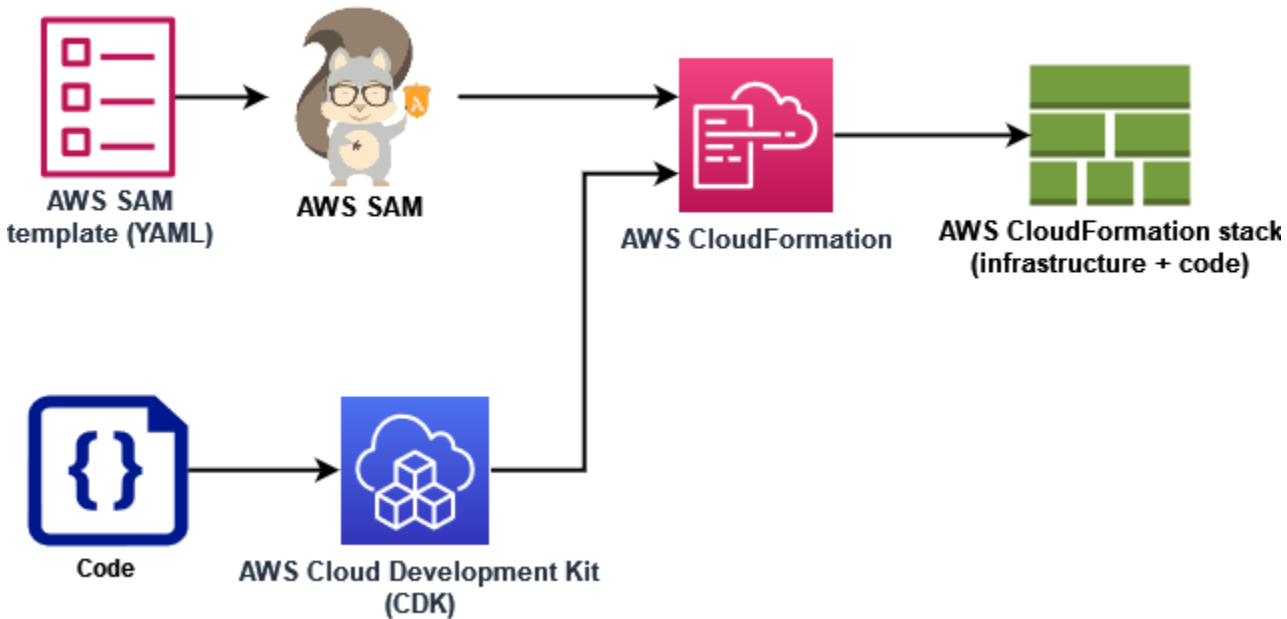
Alat IaC untuk Lambda

Untuk menyebarkan fungsi Lambda dan aplikasi tanpa server menggunakan IaC AWS, menawarkan sejumlah alat dan layanan yang berbeda.

AWS CloudFormation adalah layanan pertama yang ditawarkan oleh AWS untuk membuat dan mengkonfigurasi sumber daya cloud. Dengan AWS CloudFormation, Anda membuat templat teks untuk menentukan infrastruktur dan kode. Ketika AWS diperkenalkan lebih banyak layanan baru dan kompleksitas pembuatan AWS CloudFormation template meningkat, dua alat lebih lanjut dirilis. AWS SAM adalah kerangka kerja berbasis template lain untuk mendefinisikan aplikasi tanpa server.

AWS Cloud Development Kit (AWS CDK) Ini adalah pendekatan kode-pertama untuk mendefinisikan dan menyediakan infrastruktur menggunakan konstruksi kode dalam banyak bahasa pemrograman populer.

Dengan keduanya AWS SAM dan AWS CDK, AWS CloudFormation beroperasi di belakang layar untuk membangun dan menyebarkan infrastruktur Anda. Diagram berikut menggambarkan hubungan antara alat-alat ini, dan paragraf setelah diagram menjelaskan fitur utama mereka.



- **AWS CloudFormation-** Dengan CloudFormation Anda memodelkan dan mengatur AWS sumber daya Anda menggunakan YAML atau JSON templat yang menjelaskan sumber daya Anda dan propertinya. CloudFormation menyediakan sumber daya Anda dengan cara yang aman dan berulang, memungkinkan Anda untuk sering membangun infrastruktur dan aplikasi Anda tanpa langkah manual. Saat Anda mengubah konfigurasi, CloudFormation tentukan operasi yang tepat untuk dilakukan untuk memperbarui tumpukan Anda. CloudFormation bahkan dapat memutar kembali perubahan.
- **AWS Serverless Application Model (AWS SAM)** - AWS SAM adalah kerangka kerja sumber terbuka untuk mendefinisikan aplikasi tanpa server. AWS SAM template menggunakan sintaks singkatan untuk mendefinisikan fungsi, databaseAPIs, dan pemetaan sumber peristiwa hanya dengan beberapa baris teks () per sumber daya. YAML Selama penyebaran, AWS SAM mengubah dan memperluas sintaks menjadi AWS SAM sintaks. AWS CloudFormation Karena itu, CloudFormation sintaks apa pun dapat ditambahkan ke AWS SAM template. Ini memberikan AWS SAM semua kekuatan CloudFormation, tetapi dengan garis konfigurasi yang lebih sedikit.

- AWS Cloud Development Kit (AWS CDK)- Dengan AWS CDK, Anda mendefinisikan infrastruktur Anda menggunakan konstruksi kode dan menyediakannya melalui AWS CloudFormation. AWS CDK memungkinkan Anda untuk memodelkan infrastruktur aplikasi dengan TypeScript, Python, Java, .NET, dan Go (di Pratinjau Pengembang) menggunakan alat pengujian IDE, dan pola alur kerja yang ada. Anda mendapatkan semua manfaat AWS CloudFormation, termasuk penerapan berulang, rollback yang mudah, dan deteksi drift.

AWS juga menyediakan layanan yang dipanggil Komposer Aplikasi AWS untuk mengembangkan template IAC menggunakan antarmuka grafis sederhana. Dengan Application Composer, Anda merancang arsitektur aplikasi dengan menyeret, mengelompokkan, dan menghubungkan AWS layanan dalam kanvas visual. Application Composer kemudian membuat AWS SAM template atau AWS CloudFormation template dari desain Anda yang dapat Anda gunakan untuk menyebarkan aplikasi Anda.

Pada [the section called “Memulai dengan IAc untuk Lambda”](#) bagian di bawah ini, Anda menggunakan Application Composer untuk mengembangkan template untuk aplikasi tanpa server berdasarkan fungsi Lambda yang ada.

Memulai dengan IAc untuk Lambda

Dalam tutorial ini, Anda dapat mulai menggunakan IAc dengan Lambda dengan membuat template dari fungsi Lambda AWS SAM yang ada dan kemudian membangun aplikasi tanpa server di Application Composer dengan menambahkan sumber daya lainnya. AWS

Jika Anda lebih suka memulai dengan melakukan AWS SAM atau AWS CloudFormation tutorial untuk mempelajari cara bekerja dengan template tanpa menggunakan Application Composer, Anda akan menemukan tautan ke sumber daya lain di [the section called “Langkah selanjutnya”](#) bagian di akhir halaman ini.

Saat Anda menjalankan tutorial ini, Anda akan mempelajari beberapa konsep dasar, seperti bagaimana AWS sumber daya ditentukan AWS SAM. Anda juga akan belajar cara menggunakan Application Composer untuk membangun aplikasi tanpa server yang dapat Anda gunakan menggunakan atau. AWS SAM AWS CloudFormation

Untuk menyelesaikan tutorial ini, Anda akan melakukan langkah-langkah berikut:

- Buat contoh fungsi Lambda

- Gunakan konsol Lambda untuk melihat AWS SAM template untuk fungsi
- Ekspor konfigurasi fungsi Anda ke Komposer Aplikasi AWS dan rancang aplikasi tanpa server sederhana berdasarkan konfigurasi fungsi Anda
- Menyimpan AWS SAM template yang diperbarui yang dapat Anda gunakan sebagai dasar untuk menyebarkan aplikasi tanpa server Anda

Di [the section called “Langkah selanjutnya”](#) bagian ini, Anda akan menemukan sumber daya yang dapat Anda gunakan untuk mempelajari lebih lanjut tentang AWS SAM dan Application Composer. Sumber daya ini mencakup tautan ke tutorial yang lebih canggih yang mengajarkan Anda cara menggunakan aplikasi tanpa server. AWS SAM

Prasyarat

Dalam tutorial ini, Anda menggunakan fitur [sinkronisasi lokal](#) Application Composer untuk menyimpan file template dan kode Anda ke mesin build lokal Anda. Untuk menggunakan fitur ini, Anda memerlukan browser yang mendukung Akses Sistem FileAPI, yang memungkinkan aplikasi web membaca, menulis, dan menyimpan file di sistem file lokal Anda. Sebaiknya gunakan Google Chrome atau Microsoft Edge. Untuk informasi selengkapnya tentang Akses Sistem FileAPI, lihat [Apa itu Akses Sistem FileAPI?](#)

Buat fungsi Lambda

Pada langkah pertama ini, Anda membuat fungsi Lambda yang dapat Anda gunakan untuk menyelesaikan sisa tutorial. Untuk menjaga hal-hal sederhana, Anda menggunakan konsol Lambda untuk membuat fungsi dasar 'Hello world' menggunakan runtime Python 3.11.

Untuk membuat fungsi Lambda 'Hello world' menggunakan konsol

1. Buka [Konsol Lambda](#).
2. Pilih Buat fungsi.
3. Biarkan Penulis dari awal dipilih, dan di bawah Informasi dasar, masukkan **LambdaIaCDemo** untuk nama Fungsi.
4. Untuk Runtime, pilih Python 3.11.
5. Pilih Buat fungsi.

Lihat AWS SAM template untuk fungsi Anda

Sebelum Anda mengeksport konfigurasi fungsi Anda ke Application Composer, gunakan konsol Lambda untuk melihat konfigurasi fungsi Anda saat ini sebagai AWS SAM template. Dengan mengikuti langkah-langkah di bagian ini, Anda akan belajar tentang anatomi AWS SAM template dan cara mendefinisikan sumber daya seperti fungsi Lambda untuk mulai menentukan aplikasi tanpa server.

Untuk melihat AWS SAM template untuk fungsi Anda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang baru saja Anda buat (LambdaIaCDemo).
3. Di panel Ikhtisar fungsi, pilih Template.

Di tempat diagram yang mewakili konfigurasi fungsi Anda, Anda akan melihat AWS SAM template untuk fungsi Anda. Template akan terlihat seperti berikut ini.

```
# This AWS SAM template has been generated from your function's
# configuration. If your function has one or more triggers, note
# that the AWS resources associated with these triggers aren't fully
# specified in this template and include placeholder values. Open this template
# in AWS Application Composer or your favorite IDE and modify
# it to specify a serverless application with other AWS resources.
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
        MaximumRetryAttempts: 2
```

```
EphemeralStorage:
  Size: 512
RuntimeManagementConfig:
  UpdateRuntimeOn: Auto
SnapStart:
  ApplyOn: None
PackageType: Zip
Policies:
  Statement:
    - Effect: Allow
      Action:
        - logs:CreateLogGroup
      Resource: arn:aws:logs:us-east-1:123456789012:*
    - Effect: Allow
      Action:
        - logs:CreateLogStream
        - logs:PutLogEvents
      Resource:
        - >-
          arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
LambdaIaCDemo:*
```

Mari luangkan waktu sejenak untuk melihat YAML template untuk fungsi Anda dan memahami beberapa konsep kunci.

Template dimulai dengan deklarasi `Transform: AWS::Serverless-2016-10-31`. Deklarasi ini diperlukan karena di balik layar, AWS SAM template digunakan melalui AWS CloudFormation. Menggunakan `Transform` pernyataan mengidentifikasi template sebagai file AWS SAM template.

Setelah `Transform` deklarasi datang `Resources` bagian. Di sinilah AWS sumber daya yang ingin Anda terapkan dengan AWS SAM template Anda ditentukan. AWS SAM template dapat berisi kombinasi AWS SAM sumber daya dan sumber AWS CloudFormation daya. Ini karena selama penerapan, AWS SAM templat diperluas ke AWS CloudFormation templat, sehingga AWS CloudFormation sintaks apa pun yang valid dapat ditambahkan ke templat. AWS SAM

Saat ini, hanya ada satu sumber daya yang ditentukan di `Resources` bagian template, fungsi Lambda Anda. `LambdaIaCDemo` Untuk menambahkan fungsi Lambda ke AWS SAM template, Anda menggunakan jenis `AWS::Serverless::Function` sumber daya. Sumber daya fungsi Lambda menentukan runtime fungsi, penanganan fungsi, dan opsi konfigurasi lainnya. `Properties` Jalur ke kode sumber fungsi Anda yang AWS SAM harus digunakan untuk menyebarkan fungsi juga

didefinisikan di sini. Untuk mempelajari lebih lanjut tentang sumber daya fungsi Lambda di AWS SAM, lihat [AWS: :Serverless: :Function](#) dalam Panduan Pengembang.AWS SAM

Selain properti dan konfigurasi fungsi, template juga menentukan kebijakan AWS Identity and Access Management (IAM) untuk fungsi Anda. Kebijakan ini memberikan izin fungsi Anda untuk menulis log ke Amazon CloudWatch Logs. Saat Anda membuat fungsi di konsol Lambda, Lambda secara otomatis melampirkan kebijakan ini ke fungsi Anda. Untuk mempelajari lebih lanjut tentang menentukan IAM kebijakan untuk fungsi dalam AWS SAM template, lihat *polici*es properti di halaman [AWS: :Serverless: :Function](#) dari Panduan Pengembang.AWS SAM

Untuk mempelajari lebih lanjut tentang struktur AWS SAM templat, lihat [anatomi AWS SAM templat](#).

Gunakan Komposer Aplikasi AWS untuk mendesain aplikasi tanpa server

Untuk mulai membangun aplikasi tanpa server sederhana menggunakan AWS SAM template fungsi Anda sebagai titik awal, Anda mengekspor konfigurasi fungsi Anda ke Application Composer dan mengaktifkan mode sinkronisasi lokal Application Composer. Sinkronisasi lokal secara otomatis menyimpan kode fungsi dan AWS SAM template Anda ke mesin build lokal Anda dan membuat template tersimpan Anda tetap disinkronkan saat Anda menambahkan AWS sumber daya lain di Application Composer.

Untuk mengekspor fungsi Anda ke Application Composer

1. Di panel Ikhtisar Fungsi, pilih Ekspor ke Komposer Aplikasi.


Untuk mengekspor konfigurasi dan kode fungsi Anda ke Application Composer, Lambda membuat bucket Amazon S3 di akun Anda untuk menyimpan sementara data ini.

2. Di kotak dialog, pilih Konfirmasi dan buat proyek untuk menerima nama default untuk bucket ini dan ekspor konfigurasi dan kode fungsi Anda ke Application Composer.
3. (Opsional) Untuk memilih nama lain untuk bucket Amazon S3 yang dibuat Lambda, masukkan nama baru dan pilih Konfirmasi dan buat proyek. Nama bucket Amazon S3 harus unik secara global dan mengikuti aturan [penamaan bucket](#).

Memilih Konfirmasi dan membuat proyek membuka konsol Application Composer. Di kanvas, Anda akan melihat fungsi Lambda Anda.

4. Dari menu tarik-turun, pilih Aktifkan sinkronisasi lokal.
5. Di kotak dialog yang terbuka, pilih Pilih folder dan pilih folder di mesin build lokal Anda.
6. Pilih Aktifkan untuk mengaktifkan sinkronisasi lokal.

Untuk mengekspor fungsi Anda ke Application Composer, Anda memerlukan izin untuk menggunakan API tindakan tertentu. Jika Anda tidak dapat mengekspor fungsi Anda, lihat [the section called “Izin yang diperlukan”](#) dan pastikan Anda memiliki izin yang Anda butuhkan.

 Note

[Harga Amazon S3](#) standar berlaku untuk bucket yang dibuat Lambda saat Anda mengekspor fungsi ke Application Composer. Objek yang dimasukkan Lambda ke dalam bucket secara otomatis dihapus setelah 10 hari, tetapi Lambda tidak menghapus bucket itu sendiri. Untuk menghindari biaya tambahan yang ditambahkan ke Anda Akun AWS, ikuti petunjuk dalam [Menghapus ember setelah Anda mengekspor](#) fungsi Anda ke Application Composer. Untuk informasi selengkapnya tentang bucket Amazon S3 yang dibuat Lambda, lihat. [the section called “Komposer Aplikasi”](#)

Untuk mendesain aplikasi tanpa server Anda di Application Composer

Setelah mengaktifkan sinkronisasi lokal, perubahan yang Anda buat di Application Composer akan tercermin dalam AWS SAM template yang disimpan di mesin build lokal Anda. Anda sekarang dapat menarik dan melepas AWS sumber daya tambahan ke kanvas Application Composer untuk membangun aplikasi Anda. Dalam contoh ini, Anda menambahkan antrian SQS sederhana Amazon sebagai pemicu fungsi Lambda Anda dan tabel DynamoDB untuk fungsi untuk menulis data.

1. Tambahkan SQS pemicu Amazon ke fungsi Lambda Anda dengan melakukan hal berikut:
 - a. Di bidang pencarian di palet Sumber Daya, masukkan **SQS**.
 - b. Seret sumber daya SQS Antrian ke kanvas Anda dan posisikan di sebelah kiri fungsi Lambda Anda.
 - c. Pilih Detail, dan untuk Logical ID masukkan **LambdaIaCQueue**.
 - d. Pilih Simpan.
 - e. Hubungkan sumber daya Amazon SQS dan Lambda Anda dengan mengklik port Langganan pada kartu SQS antrian dan menyeretnya ke port sebelah kiri pada kartu fungsi Lambda. Munculnya garis antara dua sumber daya menunjukkan koneksi yang sukses. Application Composer juga menampilkan pesan di bagian bawah kanvas yang menunjukkan bahwa dua sumber daya berhasil terhubung.
2. Tambahkan tabel Amazon DynamoDB untuk fungsi Lambda Anda untuk menulis data dengan melakukan hal berikut:

- a. Di bidang pencarian di palet Sumber Daya, masukkan **DynamoDB**.
- b. Seret sumber daya DynamoDB Table ke kanvas Anda dan posisikan di sebelah kanan fungsi Lambda Anda.
- c. Pilih Detail, dan untuk Logical ID masukkan **LambdaIaCTable**.
- d. Pilih Simpan.
- e. Hubungkan tabel DynamoDB ke fungsi Lambda Anda dengan mengklik port kanan kartu fungsi Lambda dan menyeretnya ke port kiri pada kartu DynamoDB.

Sekarang Anda telah menambahkan sumber daya tambahan ini, mari kita lihat AWS SAM template yang diperbarui Application Composer telah dibuat.

Untuk melihat AWS SAM template Anda yang diperbarui

- Pada kanvas Application Composer, pilih Template untuk beralih dari tampilan kanvas ke tampilan template.

AWS SAM Template Anda sekarang harus berisi sumber daya dan properti tambahan berikut:

- SQS Antrian Amazon dengan pengenal LambdaIaCQueue

```
LambdaIaCQueue:  
  Type: AWS::SQS::Queue  
  Properties:  
    MessageRetentionPeriod: 345600
```

Saat Anda menambahkan SQS antrian Amazon menggunakan Application Composer, Application Composer menetapkan properti. `MessageRetentionPeriod` Anda juga dapat mengatur `FifoQueue` properti dengan memilih Detail pada kartu Antrian dan mencentang atau menghapus centang SQS antrian Fifo.

Untuk mengatur properti lain untuk antrian Anda, Anda dapat mengedit template secara manual untuk menambahkannya. Untuk mempelajari lebih lanjut tentang `AWS::SQS::Queue` sumber daya dan properti yang tersedia, lihat [AWS::SQS::Antrian](#) di AWS CloudFormation Panduan Pengguna.

- `Events` Properti dalam definisi fungsi Lambda Anda yang menentukan SQS antrian Amazon sebagai pemicu fungsi


```

Events:
  LambdaIaCQueue:
    Type: SQS
    Properties:
      Queue: !GetAtt LambdaIaCQueue.Arn
      BatchSize: 1

```

EventsProperti terdiri dari jenis acara dan satu set properti yang bergantung pada jenisnya. Untuk mempelajari tentang perbedaan yang dapat AWS layanan Anda konfigurasi untuk memicu fungsi Lambda dan properti yang dapat Anda atur, lihat [EventSource](#) di Panduan AWS SAM Pengembang.

- Sebuah tabel DynamoDB dengan identifier LambdaIaCTable

```

LambdaIaCTable:
  Type: AWS::DynamoDB::Table
  Properties:
    AttributeDefinitions:
      - AttributeName: id
        AttributeType: S
    BillingMode: PAY_PER_REQUEST
    KeySchema:
      - AttributeName: id
        KeyType: HASH
    StreamSpecification:
      StreamViewType: NEW_AND_OLD_IMAGES

```

Ketika Anda menambahkan tabel DynamoDB menggunakan Application Composer, Anda dapat mengatur kunci tabel Anda dengan memilih Detail pada kartu tabel DynamoDB dan mengedit nilai-nilai kunci. Application Composer juga menetapkan nilai default untuk sejumlah properti lain termasuk BillingMode danStreamViewType.

Untuk mempelajari lebih lanjut tentang properti ini dan properti lain yang dapat Anda tambahkan ke AWS SAM template Anda, lihat [AWS: :DynamoDB: :Table](#) di Panduan Pengguna.AWS CloudFormation

- IAMKebijakan baru yang memberikan izin fungsi Anda untuk melakukan CRUD operasi pada tabel DynamoDB yang Anda tambahkan.

```

Policies:

```

```
...
- DynamoDBCrudPolicy:
  TableName: !Ref LambdaIaCTable
```

AWS SAM Template akhir yang lengkap akan terlihat seperti berikut ini.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
        MaximumRetryAttempts: 2
      EphemeralStorage:
        Size: 512
      RuntimeManagementConfig:
        UpdateRuntimeOn: Auto
      SnapStart:
        ApplyOn: None
      PackageType: Zip
      Policies:
        - Statement:
            - Effect: Allow
              Action:
                - logs:CreateLogGroup
              Resource: arn:aws:logs:us-east-1:594035263019:*
            - Effect: Allow
              Action:
                - logs:CreateLogStream
                - logs:PutLogEvents
              Resource:
```

```

- arn:aws:logs:us-east-1:594035263019:log-group:/aws/lambda/
LambdaIaCDemo:*
  - DynamoDBCrudPolicy:
      TableName: !Ref LambdaIaCTable
  Events:
    LambdaIaCQueue:
      Type: SQS
      Properties:
        Queue: !GetAtt LambdaIaCQueue.Arn
        BatchSize: 1
  Environment:
    Variables:
      LAMBDAIACTABLE_TABLE_NAME: !Ref LambdaIaCTable
      LAMBDAIACTABLE_TABLE_ARN: !GetAtt LambdaIaCTable.Arn
LambdaIaCQueue:
  Type: AWS::SQS::Queue
  Properties:
    MessageRetentionPeriod: 345600
LambdaIaCTable:
  Type: AWS::DynamoDB::Table
  Properties:
    AttributeDefinitions:
      - AttributeName: id
        AttributeType: S
    BillingMode: PAY_PER_REQUEST
    KeySchema:
      - AttributeName: id
        KeyType: HASH
    StreamSpecification:
      StreamViewType: NEW_AND_OLD_IMAGES

```

Terapkan aplikasi tanpa server Anda menggunakan AWS SAM (opsional)

Jika Anda ingin menggunakan AWS SAM untuk menyebarkan aplikasi tanpa server menggunakan template yang baru saja Anda buat di Application Composer, Anda harus menginstal file terlebih dahulu. AWS SAM CLI Untuk melakukan ini, ikuti instruksi di [Instalasi AWS SAM CLI](#).

Sebelum Anda menyebarkan aplikasi Anda, Anda juga perlu memperbarui kode fungsi yang disimpan oleh Application Composer bersama dengan template Anda. Saat ini, `lambda_function.py` file yang disimpan oleh Application Composer hanya berisi kode dasar 'Hello world' yang disediakan Lambda saat Anda membuat fungsi.

Untuk memperbarui kode fungsi Anda, salin kode berikut dan tempelkan ke `lambda_function.py` file Application Composer yang disimpan ke mesin build lokal Anda. Anda menentukan direktori untuk Application Composer untuk menyimpan file ini ketika Anda mengaktifkan mode Local Sync.

Kode ini menerima pasangan nilai kunci dalam pesan dari SQS antrian Amazon yang Anda buat di Application Composer. Jika kedua kunci dan nilai adalah string, kode kemudian menggunakannya untuk menulis item ke tabel DynamoDB didefinisikan dalam template Anda.

Kode fungsi Python yang diperbarui

```
import boto3
import os
import json

# define the DynamoDB table that Lambda will connect to
tablename = os.environ['LAMBDAIACTABLE_TABLE_NAME']

# create the DynamoDB resource
dynamo = boto3.client('dynamodb')

def lambda_handler(event, context):
    # get the message out of the SQS event
    message = event['Records'][0]['body']
    data = json.loads(message)
    # write event data to DDB table
    if check_message_format(data):
        key = next(iter(data))
        value = data[key]
        dynamo.put_item(
            TableName=tablename,
            Item={
                'id': {'S': key},
                'Value': {'S': value}
            }
        )
    else:
        raise ValueError("Input data not in the correct format")

# check that the event object contains a single key value
# pair that can be written to the database
def check_message_format(message):
    if len(message) != 1:
        return False
```

```
key, value = next(iter(message.items()))

if not (isinstance(key, str) and isinstance(value, str)):
    return False

else:
    return True
```

Untuk menerapkan aplikasi tanpa server

Untuk menyebarkan aplikasi Anda menggunakan AWS SAM CLI, lakukan langkah-langkah berikut. Agar fungsi Anda dapat membangun dan menerapkan dengan benar, Python versi 3.11 harus diinstal pada mesin build Anda dan di mesin Anda. PATH

1. Jalankan perintah berikut dari direktori di mana Application Composer menyimpan `lambda_function.py` file Anda `template.yaml` dan.

```
sam build
```

Perintah ini mengumpulkan artefak build untuk aplikasi Anda dan menempatkannya dalam format dan lokasi yang tepat untuk menerapkannya.

2. Untuk menerapkan aplikasi Anda dan membuat sumber daya Lambda, SQS Amazon, dan DynamoDB yang ditentukan dalam template AWS SAM Anda, jalankan perintah berikut.

```
sam deploy --guided
```

Menggunakan `--guided` tanda berarti itu AWS SAM akan menunjukkan kepada Anda petunjuk untuk memandu Anda melalui proses penerapan. Untuk penerapan ini, terima opsi default dengan menekan Enter.

Selama proses penerapan, AWS SAM buat sumber daya berikut di: Akun AWS

- Sebuah AWS CloudFormation [tumpukan](#) bernama `sam-app`
- Fungsi Lambda dengan format nama `sam-app-LambdaIaCDemo-99VXPpYQVv1M`
- SQSAntrian Amazon dengan format nama `sam-app-LambdaIaCQueue-xL87VeKsGiIo`
- Sebuah tabel DynamoDB dengan format nama `sam-app-LambdaIaCTable-CN0S66C0VLNV`

AWS SAM juga membuat IAM peran dan kebijakan yang diperlukan sehingga fungsi Lambda Anda dapat membaca pesan dari SQS antrian Amazon dan melakukan CRUD operasi pada tabel DynamoDB.

Untuk mempelajari lebih lanjut tentang penggunaan AWS SAM untuk menyebarkan aplikasi tanpa server, lihat sumber daya di bagian ini. [the section called “Langkah selanjutnya”](#)

Menguji aplikasi yang Anda gunakan (opsional)

Untuk mengonfirmasi bahwa aplikasi tanpa server Anda diterapkan dengan benar, kirim pesan ke SQS antrian Amazon Anda yang berisi pasangan nilai kunci dan periksa apakah Lambda menulis item ke tabel DynamoDB Anda menggunakan nilai-nilai ini.

Untuk menguji aplikasi tanpa server Anda

1. Buka halaman [Antrian](#) SQS konsol Amazon dan pilih antrian yang AWS SAM dibuat dari template Anda. Namanya memiliki format `sam-app-LambdaIaCQueue-xL87VeKsGiIo`.
2. Pilih Kirim dan terima pesan dan tempel yang berikut ini JSON ke badan Pesan di bagian Kirim pesan.

```
{
  "myKey": "myValue"
}
```

3. Pilih Kirim pesan.

Mengirim pesan ke antrian menyebabkan Lambda memanggil fungsi Anda melalui pemetaan sumber peristiwa yang ditentukan dalam templat Anda. AWS SAM Untuk mengonfirmasi bahwa Lambda telah memanggil fungsi Anda seperti yang diharapkan, konfirmasi bahwa item telah ditambahkan ke tabel DynamoDB Anda.

4. Buka halaman [Tabel](#) konsol DynamoDB dan pilih tabel Anda. Namanya memiliki format `sam-app-LambdaIaCTable-CN0S66C0VLNV`.
5. Pilih Jelajahi item tabel. Di panel Item yang dikembalikan, Anda akan melihat item dengan id `myKey` dan `myValue`.

Langkah selanjutnya

Untuk mempelajari lebih lanjut tentang menggunakan Application Composer dengan AWS SAM dan AWS CloudFormation, mulailah dengan [Menggunakan Application Composer dengan AWS CloudFormation](#) dan [AWS SAM](#)

[Untuk tutorial terpandu yang digunakan AWS SAM untuk menyebarkan aplikasi tanpa server yang dirancang di Application Composer, kami juga menyarankan Anda melakukan Komposer Aplikasi AWS tutorial di Workshop Pola Tanpa Server.AWS](#)

AWS SAM menyediakan antarmuka baris perintah (CLI) yang dapat Anda gunakan dengan AWS SAM templat dan integrasi pihak ketiga yang didukung untuk membangun dan menjalankan aplikasi tanpa server Anda. Dengan itu AWS SAM CLI, Anda dapat membangun dan menerapkan aplikasi Anda, melakukan pengujian dan debugging lokal, mengonfigurasi pipeline CI/CD, dan banyak lagi. Untuk mempelajari lebih lanjut tentang menggunakan AWS SAM CLI, lihat [Memulai AWS SAM](#) di Panduan AWS Serverless Application Model Pengembang.

Untuk mempelajari cara menerapkan aplikasi tanpa server dengan AWS SAM templat menggunakan AWS CloudFormation konsol, mulailah dengan [Menggunakan AWS CloudFormation konsol di Panduan Pengguna.AWS CloudFormation](#)

Daerah yang didukung untuk integrasi Lambda dengan Application Composer

Integrasi Lambda dengan Application Composer didukung sebagai berikut: Wilayah AWS

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Mumbai)

- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Zürich)
- Eropa (Irlandia)
- Europe (London)
- Eropa (Stockholm)
- Timur Tengah (UAE)

Memahami model pemrograman Lambda

Lambda menyediakan model pemrograman yang umum untuk semua runtime. Model pemrograman mendefinisikan antarmuka antara kode Anda dan sistem Lambda. Anda memberi tahu Lambda titik masuk ke fungsi Anda dengan mendefinisikan handler dalam konfigurasi fungsi. Runtime berlalu dengan objek ke handler yang berisi acara invokasi dan konteks, seperti nama fungsi dan ID permintaan.

Setelah handler selesai memproses peristiwa pertama, runtime mengirimkan peristiwa lain. Kelas fungsi tetap di dalam memori, sehingga klien dan variabel yang dinyatakan di luar metode handler dalam kode inisialisasi dapat digunakan kembali. Untuk menghemat waktu pemrosesan pada peristiwa berikutnya, buat sumber daya yang dapat digunakan kembali seperti AWS SDK klien selama inisialisasi. Setelah diinisialisasi, setiap instans fungsi Anda dapat memproses ribuan permintaan.

Fungsi Anda juga memiliki akses ke penyimpanan lokal di direktori `/tmp`. Isi direktori tetap ada ketika lingkungan eksekusi dibekukan, menyediakan cache sementara yang dapat digunakan untuk beberapa invokasi. Untuk informasi selengkapnya, lihat [Lingkungan eksekusi Lambda](#).

Saat [AWS X-Ray pelacakan](#) diaktifkan, runtime mencatat subsegmen terpisah untuk inisialisasi dan eksekusi.

Runtime menangkap output logging dari fungsi Anda dan mengirimkannya ke Amazon CloudWatch Logs. Selain mencatat output fungsi Anda, runtime juga mencatat entri saat invokasi fungsi dimulai dan berakhir. Ini termasuk catatan laporan dengan ID permintaan, durasi yang ditagih, durasi inisialisasi, dan perincian lainnya. Jika fungsi Anda menampilkan kesalahan, runtime mengembalikan kesalahan tersebut ke pemanggil.

Note

Logging tunduk pada [kuota CloudWatch Log](#). Data log dapat hilang karena pelambatan atau, dalam beberapa kasus, ketika satu instans fungsi Anda dihentikan.

Lambda memperluas fungsi Anda dengan menjalankan instans tambahannya seiring peningkatan permintaan, dan dengan menghentikan instans seiring dengan penurunan permintaan. Model ini mengarah pada variasi dalam arsitektur aplikasi, seperti:

- Kecuali dinyatakan sebaliknya, permintaan masuk dapat diproses di luar pesanan atau bersamaan.
- Jangan mengandalkan contoh fungsi Anda yang berumur panjang, alih-alih simpan status aplikasi Anda di tempat lain.
- Gunakan penyimpanan lokal dan objek tingkat kelas untuk meningkatkan performa, tetapi jaga ukuran paket deployment Anda seminimum mungkin dan jumlah data yang Anda transfer ke lingkungan eksekusi.

Untuk pengenalan langsung model pemrograman dalam bahasa pemrograman pilihan Anda, lihat bab berikut.

- [Membangun fungsi Lambda dengan Node.js](#)
- [Membangun fungsi Lambda dengan Python](#)
- [Membangun fungsi Lambda dengan Ruby](#)
- [Membangun fungsi Lambda dengan Java](#)
- [Membangun fungsi Lambda dengan Go](#)
- [Membangun fungsi Lambda dengan C#](#)
- [Membangun fungsi Lambda dengan PowerShell](#)

Runtime Lambda

Lambda mendukung banyak bahasa melalui penggunaan runtime. Runtime menyediakan lingkungan khusus bahasa yang menyampaikan peristiwa pemanggilan, informasi konteks, dan respons antara Lambda dan fungsinya. Anda dapat menggunakan runtime yang disediakan Lambda, atau membangun sendiri.

Setiap rilis bahasa pemrograman utama memiliki runtime terpisah, dengan pengidentifikasi runtime yang unik, seperti `node.js20.x` `python3.12`. Untuk mengonfigurasi fungsi untuk menggunakan versi bahasa utama yang baru, Anda perlu mengubah pengenalan runtime. Karena AWS Lambda tidak dapat menjamin kompatibilitas mundur antara versi utama, ini adalah operasi yang digerakkan oleh pelanggan.

Untuk [fungsi yang didefinisikan sebagai image container](#), Anda memilih runtime dan distribusi Linux saat membuat image container. Untuk mengubah runtime, Anda membuat gambar kontainer baru.

Ketika Anda menggunakan arsip file `.zip` untuk paket deployment, Anda memilih runtime ketika Anda membuat fungsi. Untuk mengubah runtime, Anda dapat [memperbarui konfigurasi fungsi](#). Runtime dipasangkan dengan salah satu distribusi Amazon Linux. Lingkungan eksekusi yang mendasari menyediakan pustaka dan [variabel lingkungan](#) tambahan yang dapat Anda akses dari kode fungsi Anda.

[Lambda memanggil fungsi Anda di lingkungan eksekusi](#). Lingkungan eksekusi menyediakan lingkungan runtime yang aman dan terisolasi yang mengelola sumber daya yang diperlukan untuk menjalankan fungsi Anda. Lambda menggunakan kembali lingkungan eksekusi dari pemanggilan sebelumnya jika tersedia, atau dapat membuat lingkungan eksekusi baru.

Untuk menggunakan bahasa lain di Lambda, seperti [Go](#) atau [Rust](#), gunakan runtime khusus [OS](#). Area pelaksanaan Lambda menyediakan [antarmuka runtime](#) atas adanya event invokasi dan mengirimkan tanggapan. [Anda dapat menerapkan bahasa lain dengan menerapkan runtime kustom di samping kode fungsi Anda, atau dalam lapisan](#).

Waktu aktif yang didukung

Tabel berikut mencantumkan runtime Lambda yang didukung dan tanggal penghentian yang diproyeksikan. Setelah runtime tidak digunakan lagi, Anda masih dapat membuat dan memperbarui fungsi untuk jangka waktu terbatas. Untuk informasi selengkapnya, lihat [the section called "Penggunaan runtime setelah penghentian"](#). Tabel menyediakan tanggal yang diperkirakan saat ini

untuk penghentian runtime. Tanggal-tanggal ini disediakan untuk tujuan perencanaan dan dapat berubah sewaktu-waktu.

Runtime yang Didukung

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------|------------------|-------------------|---------------------|-------------------|-----------------------|
| Node.js 20 | nodejs20.x | Amazon Linux 2023 | | | |
| Node.js 18 | nodejs18.x | Amazon Linux 2 | | | |
| Python 3.12 | python3.12 | Amazon Linux 2023 | | | |
| Python 3.11 | python3.11 | Amazon Linux 2 | | | |
| Python 3.10 | python3.10 | Amazon Linux 2 | | | |
| Python 3.9 | python3.9 | Amazon Linux 2 | | | |
| Python 3.8 | python3.8 | Amazon Linux 2 | Okt 14, 2024 | Februari 28, 2025 | 31 Mar 2025 |
| Jawa 21 | java21 | Amazon Linux 2023 | | | |
| Jawa 17 | java17 | Amazon Linux 2 | | | |
| Java 11 | java11 | Amazon Linux 2 | | | |
| Java 8 | java8.a12 | Amazon Linux 2 | | | |

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------|------------------|-------------------|---------------------|-------------------|-----------------------|
| .NET8 | dotnet8 | Amazon Linux 2023 | | | |
| .NET6 | dotnet6 | Amazon Linux 2 | 20 Des 2024 | Februari 28, 2025 | 31 Mar 2025 |
| Ruby 3.3 | ruby3.3 | Amazon Linux 2023 | | | |
| Ruby 3.2 | ruby3.2 | Amazon Linux 2 | | | |
| Runtime Khusus OS | provided.a12023 | Amazon Linux 2023 | | | |
| Runtime Khusus OS | provided.a12 | Amazon Linux 2 | | | |

Note

Untuk wilayah baru, Lambda tidak akan mendukung runtime yang ditetapkan untuk tidak digunakan lagi dalam 6 bulan ke depan.

Lambda membuat runtime terkelola dan gambar dasar kontainer yang sesuai diperbarui dengan tambalan dan dukungan untuk rilis versi minor. Untuk informasi selengkapnya, lihat [pembaruan runtime Lambda](#).

Lambda terus mendukung bahasa pemrograman Go setelah penghentian runtime Go 1.x. Untuk informasi selengkapnya, lihat [Memigrasi AWS Lambda fungsi dari runtime Go1.x ke runtime khusus di Amazon Linux 2 di Blog Komputasi.AWS](#)

Semua runtime Lambda yang didukung mendukung arsitektur x86_64 dan arm64.

Rilis runtime baru

Lambda menyediakan runtime terkelola untuk versi bahasa baru hanya ketika rilis mencapai fase support (LTS) jangka panjang dari siklus rilis bahasa. Misalnya, untuk [siklus rilis Node.js](#), saat rilis mencapai LTS fase Aktif.

Sebelum rilis mencapai fase dukungan jangka panjang, ia tetap dalam pengembangan dan masih dapat mengalami perubahan yang melanggar. Lambda menerapkan pembaruan runtime secara otomatis secara default, sehingga melanggar perubahan pada versi runtime dapat menghentikan fungsi Anda berfungsi seperti yang diharapkan.

Lambda tidak menyediakan runtime terkelola untuk versi bahasa yang tidak dijadwalkan untuk rilis. LTS

Daftar berikut menunjukkan bulan peluncuran target untuk runtime Lambda mendatang. Tanggal-tanggal ini hanya bersifat indikatif dan dapat berubah sewaktu-waktu.

- Python 3.13 - November 2024
- Node.js 22 - November 2024

Kebijakan penghentian runtime

[Runtime Lambda](#) untuk arsip file .zip dibangun di sekitar kombinasi sistem operasi, bahasa pemrograman, dan pustaka perangkat lunak yang tunduk pada pemeliharaan dan pembaruan keamanan. Kebijakan penghentian standar Lambda adalah menghentikan runtime ketika komponen utama runtime mencapai akhir dukungan jangka panjang komunitas (LTS) dan pembaruan keamanan tidak lagi tersedia. Biasanya, ini adalah runtime bahasa, meskipun dalam beberapa kasus, runtime dapat dihentikan karena sistem operasi (OS) mencapai akhir. LTS

Setelah runtime tidak digunakan lagi, AWS mungkin tidak lagi menerapkan patch keamanan atau pembaruan ke runtime tersebut, dan fungsi yang menggunakan runtime tersebut tidak lagi memenuhi syarat untuk dukungan teknis. Runtime yang tidak digunakan lagi tersebut disediakan 'apa adanya', tanpa jaminan apa pun, dan mungkin mengandung bug, kesalahan, cacat, atau kerentanan lainnya.

Untuk mempelajari lebih lanjut tentang mengelola upgrade runtime dan penghentian, lihat bagian berikut dan [Mengelola upgrade AWS Lambda runtime](#) di Compute Blog.AWS

⚠ Important

Lambda terkadang menunda penghentian runtime Lambda untuk periode terbatas di luar akhir tanggal dukungan versi bahasa yang didukung runtime. Selama periode ini, Lambda hanya menerapkan patch keamanan ke OS runtime. Lambda tidak menerapkan patch keamanan untuk runtime bahasa pemrograman setelah mereka mencapai akhir tanggal dukungan mereka.

Model tanggung jawab bersama

Lambda bertanggung jawab untuk mengkurasi dan menerbitkan pembaruan keamanan untuk semua runtime terkelola dan gambar dasar kontainer yang didukung. Secara default, Lambda akan menerapkan pembaruan ini secara otomatis ke fungsi menggunakan runtime terkelola. Jika pengaturan pembaruan runtime otomatis default telah diubah, lihat model [tanggung jawab bersama kontrol manajemen runtime](#). Untuk fungsi yang digunakan menggunakan gambar kontainer, Anda bertanggung jawab untuk membangun kembali gambar kontainer fungsi Anda dari gambar dasar terbaru dan menerapkan kembali gambar kontainer.

Ketika runtime tidak digunakan lagi, tanggung jawab Lambda untuk memperbarui runtime terkelola dan gambar dasar kontainer berhenti. Anda bertanggung jawab untuk meningkatkan fungsi Anda untuk menggunakan runtime atau gambar dasar yang didukung.

Dalam semua kasus, Anda bertanggung jawab untuk menerapkan pembaruan pada kode fungsi Anda, termasuk dependensinya. Tanggung jawab Anda di bawah model tanggung jawab bersama dirangkum dalam tabel berikut.

| Fase siklus hidup runtime | Tanggung jawab Lambda | Tanggung jawab Anda |
|---------------------------------|---|--|
| Runtime terkelola yang didukung | <p>Berikan pembaruan runtime reguler dengan tambalan keamanan dan pembaruan lainnya.</p> <p>Menerapkan pembaruan runtime secara otomatis secara default (lihat the section called “Mode</p> | Perbarui kode fungsi Anda, termasuk dependensi, untuk mengatasi kerentanan keamanan apa pun. |

| Fase siklus hidup runtime | Tanggung jawab Lambda | Tanggung jawab Anda |
|---|--|--|
| | <p>pembaruan runtime” perilaku non-default).</p> | |
| Gambar kontainer yang didukung | Berikan pembaruan rutin ke gambar dasar kontainer dengan tambalan keamanan dan pembaruan lainnya. | <p>Perbarui kode fungsi Anda, termasuk dependensi, untuk mengatasi kerentanan keamanan apa pun.</p> <p>Buat ulang dan terapkan ulang image container Anda secara teratur menggunakan image dasar terbaru.</p> |
| Runtime terkelola mendekati penghentian | <p>Beri tahu pelanggan sebelum penghentian runtime melalui dokumentasi,, email, AWS Health Dashboard dan. Trusted Advisor</p> <p>Tanggung jawab untuk pembaruan runtime berakhir pada penghentian.</p> | <p>Pantau dokumentasi Lambda, email AWS Health Dashboard, atau informasi Trusted Advisor penghentian runtime.</p> <p>Tingkatkan fungsi ke runtime yang didukung sebelum runtime sebelumnya tidak digunakan lagi.</p> |
| Gambar kontainer mendekati penghentian | <p>Pemberitahuan penghentian tidak tersedia untuk fungsi yang menggunakan gambar kontainer.</p> <p>Tanggung jawab atas pembaruan gambar dasar kontainer berakhir dengan penghentian.</p> | Perhatikan jadwal penghentian dan tingkatkan fungsi ke gambar dasar yang didukung sebelum gambar sebelumnya tidak digunakan lagi. |

Penggunaan runtime setelah penghentian

Setelah runtime tidak digunakan lagi, AWS mungkin tidak lagi menerapkan patch keamanan atau pembaruan ke runtime tersebut, dan fungsi yang menggunakan runtime tersebut tidak lagi memenuhi syarat untuk dukungan teknis. Runtime yang tidak digunakan lagi tersebut disediakan 'apa adanya', tanpa jaminan apa pun, dan mungkin mengandung bug, kesalahan, cacat, atau kerentanan lainnya. Fungsi yang menggunakan runtime usang juga dapat mengalami penurunan kinerja atau masalah lain, seperti kedaluwarsa sertifikat, yang dapat menyebabkan mereka berhenti bekerja dengan benar.

Setidaknya selama 30 hari setelah runtime tidak digunakan lagi, Anda masih dapat membuat fungsi Lambda baru menggunakan runtime tersebut. Mulai dari 30 hari setelah penghentian, Lambda mulai memblokir pembuatan fungsi baru.

Setidaknya selama 60 hari setelah runtime tidak digunakan lagi, Anda masih dapat memperbarui kode fungsi dan konfigurasi untuk fungsi yang ada. Mulai dari 60 hari setelah penghentian, Lambda mulai memblokir pembaruan kode fungsi dan konfigurasi untuk fungsi yang ada.

Note

Untuk beberapa runtime, AWS menunda block-function-create dan block-function-update tanggal di luar 30 dan 60 hari biasa setelah penghentian. AWS telah membuat perubahan ini sebagai tanggapan atas umpan balik pelanggan untuk memberi Anda lebih banyak waktu untuk meningkatkan fungsi Anda. Lihat tabel di [the section called “Waktu aktif yang didukung”](#) dan [the section called “Waktu pengoperasian terdepresiasi”](#) untuk melihat tanggal runtime Anda.

Anda dapat memperbarui fungsi untuk menggunakan runtime yang didukung lebih baru tanpa batas waktu setelah runtime tidak digunakan lagi. Anda harus menguji apakah fungsi Anda berfungsi dengan runtime baru sebelum menerapkan perubahan runtime di lingkungan produksi, karena Anda tidak akan dapat kembali ke runtime yang tidak digunakan lagi setelah periode 60 hari berlalu. Sebaiknya gunakan [versi](#) fungsi dan [alias](#) untuk mengaktifkan penerapan yang aman dengan rollback.

Perhatikan bahwa lamanya waktu yang tepat untuk terus membuat dan memperbarui fungsi tidak tetap. Periode ini dapat bervariasi untuk setiap penghentian dan untuk yang berbeda. Wilayah AWS Tanggal nominal untuk pemblokiran pembuatan dan pembaruan fungsi disediakan di tabel Waktu

Proses yang Didukung di bagian pertama halaman ini. Lambda tidak akan mulai memblokir fungsi membuat atau memperbarui sebelum tanggal yang diberikan dalam tabel ini.

Anda dapat terus menjalankan fungsi Anda tanpa batas waktu setelah runtime tidak digunakan lagi. Namun, AWS sangat disarankan agar Anda memigrasikan fungsi ke runtime yang didukung sehingga fungsi Anda terus menerima patch keamanan dan tetap memenuhi syarat untuk mendapatkan dukungan teknis.

Menerima pemberitahuan penghentian runtime

Saat runtime mendekati tanggal penghentiannya, Lambda mengirim Anda peringatan email jika ada fungsi dalam penggunaan runtime tersebut. Akun AWS Pemberitahuan juga ditampilkan di dalam AWS Health Dashboard dan di AWS Trusted Advisor.

- Menerima pemberitahuan email:

Lambda mengirim Anda peringatan email setidaknya 180 hari sebelum runtime tidak digunakan lagi. Email ini mencantumkan LATEST versi \$ dari semua fungsi menggunakan runtime. Untuk melihat daftar lengkap versi fungsi yang terpengaruh, gunakan Trusted Advisor atau lihat [the section called “Dapatkan data tentang fungsi berdasarkan runtime”](#).

Lambda mengirimkan pemberitahuan email ke kontak akun Akun AWS utama Anda. Untuk informasi tentang melihat atau memperbarui alamat email di akun Anda, lihat [Memperbarui informasi kontak](#) di Referensi AWS Umum.

- Menerima pemberitahuan melalui AWS Health Dashboard:

Ini AWS Health Dashboard menampilkan pemberitahuan setidaknya 180 hari sebelum runtime tidak digunakan lagi. Pemberitahuan muncul di halaman kesehatan akun Anda di bawah [Pemberitahuan lain](#). Tab Sumber daya yang terpengaruh dari notifikasi mencantumkan LATEST versi \$ dari semua fungsi menggunakan runtime.

Note

Untuk melihat lengkap dan up-to-date daftar versi fungsi yang terpengaruh, gunakan Trusted Advisor atau lihat [the section called “Dapatkan data tentang fungsi berdasarkan runtime”](#).

AWS Health Dashboard notifikasi kedaluwarsa 90 hari setelah runtime yang terpengaruh tidak digunakan lagi.

- Menggunakan AWS Trusted Advisor

Trusted Advisor menampilkan pemberitahuan 180 hari sebelum runtime tidak digunakan lagi. Pemberitahuan muncul di halaman [Keamanan](#). Daftar fungsi yang terpengaruh ditampilkan di bawah AWS Lambda Functions Using Deprecated Runtimes. Daftar fungsi ini menunjukkan \$ LATEST dan versi yang diterbitkan dan diperbarui secara otomatis untuk mencerminkan status fungsi Anda saat ini.

Anda dapat mengaktifkan notifikasi email mingguan dari Trusted Advisor halaman [Preferensi Trusted Advisor](#) konsol.

Waktu pengoperasian terdepresiasi

Runtime berikut telah mencapai akhir dukungan:

Waktu pengoperasian terdepresiasi

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------------|------------------|----------------|---------------------|-------------------|-----------------------|
| Node.js 16 | nodejs16.x | Amazon Linux 2 | 12 Jun 2024 | Februari 28, 2025 | 31 Mar 2025 |
| .NET7 (hanya kontainer) | dotnet7 | Amazon Linux 2 | 14 Mei 2024 | | |
| Java 8 | java8 | Amazon Linux | 8 Jan 2024 | Februari 8, 2024 | Februari 28, 2025 |
| Jalankan 1.x | go1.x | Amazon Linux | 8 Jan 2024 | Februari 8, 2024 | Februari 28, 2025 |
| Runtime Khusus OS | provided | Amazon Linux | 8 Jan 2024 | Februari 8, 2024 | Februari 28, 2025 |

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------------|------------------|----------------|---------------------|------------------|-----------------------|
| Ruby 2.7 | ruby2.7 | Amazon Linux 2 | 7 Desember 2023 | 9 Jan 2024 | Februari 28, 2025 |
| Node.js 14 | nodejs14.x | Amazon Linux 2 | 4 Desember 2023 | 9 Jan 2024 | Februari 28, 2025 |
| Python 3.7 | python3.7 | Amazon Linux | 4 Desember 2023 | 9 Jan 2024 | Februari 28, 2025 |
| .NETInti 3.1 | dotnetcore3.1 | Amazon Linux 2 | Apr 3, 2023 | Apr 3, 2023 | 3 Mei 2023 |
| Node.js 12 | nodejs12.x | Amazon Linux 2 | 31 Mar 2023 | 31 Mar 2023 | Apr 30, 2023 |
| Python 3.6 | python3.6 | Amazon Linux | Jul 18, 2022 | Jul 18, 2022 | Agustus 29, 2022 |
| .NET5 (hanya kontainer) | dotnet5.0 | Amazon Linux 2 | 10 Mei 2022 | | |
| .NETInti 2.1 | dotnetcore2.1 | Amazon Linux | Jan 5, 2022 | Jan 5, 2022 | Apr 13, 2022 |
| Node.js 10 | nodejs10.x | Amazon Linux 2 | Juli 30, 2021 | Juli 30, 2021 | Feb 14, 2022 |
| Ruby 2.5 | ruby2.5 | Amazon Linux | Juli 30, 2021 | Juli 30, 2021 | Mar 31, 2022 |
| Python 2.7 | python2.7 | Amazon Linux | Juli 15, 2021 | Juli 15, 2021 | Mei 30, 2022 |
| Node.js 8.10 | nodejs8.10 | Amazon Linux | Mar 6, 2020 | | Mar 6, 2020 |

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|------------------|------------------|----------------|---------------------|------------------|-----------------------|
| Node.js 4.3 | nodejs4.3 | Amazon Linux | Mar 5, 2020 | | Mar 5, 2020 |
| Node.js 4.3 edge | nodejs4.3-edge | Amazon Linux | Mar 5, 2020 | | Apr 30, 2019 |
| Node.js 6.10 | nodejs6.10 | Amazon Linux | Agustus 12, 2019 | Agustus 12, 2019 | |
| .NETInti 1.0 | dotnetcore1.0 | Amazon Linux | 27 Jun 2019 | | 30 Jul 2019 |
| .NETInti 2.0 | dotnetcore2.0 | Amazon Linux | 30 Mei 2019 | | 30 Mei 2019 |
| Node.js 0.10 | nodejs | Amazon Linux | | | Okt 31, 2016 |

Dalam hampir semua kasus, end-of-life tanggal versi bahasa atau sistem operasi sudah diketahui sebelumnya. Tautan berikut memberikan end-of-life jadwal untuk setiap bahasa yang didukung Lambda sebagai runtime terkelola.

Kebijakan dukungan bahasa dan framework

- Node.js – github.com
- Python – devguide.python.org
- Ruby – www.ruby-lang.org
- Jawa — www.oracle.com dan [Corretto FAQs](#)
- Go – golang.org
- .NET— dotnet.microsoft.com

Memahami bagaimana Lambda mengelola pembaruan versi runtime

Lambda selalu memperbarui setiap runtime yang dikelola dengan pembaruan keamanan, perbaikan bug, fitur baru, peningkatan kinerja, dan dukungan untuk rilis versi minor. Pembaruan runtime ini diterbitkan sebagai versi runtime. Lambda menerapkan pembaruan runtime ke fungsi dengan memigrasikan fungsi dari versi runtime sebelumnya ke versi runtime baru.

Secara default, untuk fungsi yang menggunakan runtime terkelola, Lambda menerapkan pembaruan runtime secara otomatis. Dengan pembaruan runtime otomatis, Lambda menanggung beban operasional untuk menambal versi runtime. Bagi sebagian besar pelanggan, pembaruan otomatis adalah pilihan yang tepat. Anda dapat mengubah perilaku default ini dengan [mengonfigurasi pengaturan manajemen runtime](#).

Lambda juga menerbitkan setiap versi runtime baru sebagai gambar kontainer. Untuk memperbarui versi runtime untuk fungsi berbasis container, Anda harus [membuat image container baru dari image](#) dasar yang diperbarui dan menerapkan ulang fungsi Anda.

Setiap versi runtime dikaitkan dengan nomor versi dan ARN (Nama Sumber Daya Amazon). Nomor versi runtime menggunakan skema penomoran yang didefinisikan Lambda, terlepas dari nomor versi yang digunakan bahasa pemrograman. Versi runtime ARN adalah pengenal unik untuk setiap versi runtime. Anda dapat melihat versi runtime fungsi Anda saat ini di konsol Lambda, atau [baris INIT_START log fungsi Anda](#). ARN

Versi runtime tidak boleh disamakan dengan pengidentifikasi runtime. Setiap runtime memiliki pengenal runtime yang unik, seperti `python3.12 nodejs20.x`. Ini sesuai dengan setiap rilis bahasa pemrograman utama. Versi runtime menjelaskan versi patch dari runtime individual.

Note

ARN Untuk nomor versi runtime yang sama dapat bervariasi antara Wilayah AWS dan CPU arsitektur.

Topik

- [Mode pembaruan runtime](#)
- [Peluncuran versi runtime dua fase](#)

- [Mengonfigurasi pengaturan manajemen runtime Lambda](#)
- [Mengembalikan versi runtime Lambda](#)
- [Mengidentifikasi perubahan versi runtime Lambda](#)
- [Memahami model tanggung jawab bersama untuk manajemen runtime Lambda](#)
- [Mengontrol izin pembaruan runtime Lambda untuk aplikasi dengan kepatuhan tinggi](#)

Mode pembaruan runtime

Lambda berusaha untuk menyediakan pembaruan runtime yang kompatibel dengan fungsi yang ada. Namun, seperti halnya patching perangkat lunak, ada kasus yang jarang terjadi di mana pembaruan runtime dapat berdampak negatif pada fungsi yang ada. Misalnya, patch keamanan dapat mengekspos masalah mendasar dengan fungsi yang ada yang bergantung pada perilaku tidak aman sebelumnya. Kontrol manajemen runtime Lambda membantu mengurangi risiko dampak pada beban kerja Anda jika terjadi ketidakcocokan versi runtime yang jarang terjadi. Untuk setiap [versi fungsi](#) (\$LATEST atau versi yang diterbitkan), Anda dapat memilih salah satu mode pembaruan runtime berikut:

- Otomatis (default) - Secara otomatis memperbarui ke versi runtime terbaru dan aman menggunakan [Peluncuran versi runtime dua fase](#). Kami merekomendasikan mode ini untuk sebagian besar pelanggan sehingga Anda selalu mendapat manfaat dari pembaruan runtime.
- Pembaruan fungsi - Perbarui ke versi runtime terbaru dan aman saat Anda memperbarui fungsi Anda. Saat memperbarui fungsi, Lambda memperbarui runtime fungsi Anda ke versi runtime terbaru dan aman. Pendekatan ini menyinkronkan pembaruan runtime dengan penerapan fungsi, memberi Anda kendali atas kapan Lambda menerapkan pembaruan runtime. Dengan mode ini, Anda dapat mendeteksi dan mengurangi ketidakcocokan pembaruan runtime yang jarang terjadi lebih awal. Saat menggunakan mode ini, Anda harus memperbarui fungsi secara teratur agar runtime tetap up to date.
- Manual - Perbarui versi runtime Anda secara manual. Anda menentukan versi runtime dalam konfigurasi fungsi Anda. Fungsi ini menggunakan versi runtime ini tanpa batas waktu. Dalam kasus yang jarang terjadi di mana versi runtime baru tidak kompatibel dengan fungsi yang ada, Anda dapat menggunakan mode ini untuk memutar kembali fungsi Anda ke versi runtime sebelumnya. Sebaiknya jangan menggunakan mode Manual untuk mencoba mencapai konsistensi runtime di seluruh penerapan. Untuk informasi selengkapnya, lihat [Mengembalikan versi runtime Lambda](#).

Tanggung jawab untuk menerapkan pembaruan runtime ke fungsi Anda bervariasi sesuai dengan mode pembaruan runtime yang Anda pilih. Untuk informasi selengkapnya, lihat [Memahami model tanggung jawab bersama untuk manajemen runtime Lambda](#).

Peluncuran versi runtime dua fase

Lambda memperkenalkan versi runtime baru dengan urutan sebagai berikut:

1. Pada fase pertama, Lambda menerapkan versi runtime baru setiap kali Anda membuat atau memperbarui fungsi. Sebuah fungsi akan diperbarui ketika Anda memanggil [UpdateFunctionCode](#) atau [UpdateFunctionConfiguration](#) API operasi.
2. Pada fase kedua, Lambda memperbarui fungsi apa pun yang menggunakan mode pembaruan runtime Otomatis dan yang belum diperbarui ke versi runtime yang baru.

Durasi keseluruhan proses peluncuran bervariasi sesuai dengan beberapa faktor, termasuk tingkat keparahan patch keamanan apa pun yang termasuk dalam pembaruan runtime.

Jika Anda secara aktif mengembangkan dan menerapkan fungsi Anda, kemungkinan besar Anda akan mengambil versi runtime baru selama fase pertama. Ini menyinkronkan pembaruan runtime dengan pembaruan fungsi. Jika versi runtime terbaru berdampak negatif pada aplikasi Anda, pendekatan ini memungkinkan Anda mengambil tindakan korektif yang cepat. Fungsi yang tidak dalam pengembangan aktif masih menerima manfaat operasional dari pembaruan runtime otomatis selama fase kedua.

Pendekatan ini tidak memengaruhi fungsi yang disetel ke pembaruan Fungsi atau mode Manual. Fungsi yang menggunakan mode pembaruan Fungsi menerima pembaruan runtime terbaru hanya ketika Anda membuat atau memperbaruinya. Fungsi yang menggunakan mode Manual tidak menerima pembaruan runtime.

Lambda menerbitkan versi runtime baru secara bertahap dan bergulir. Wilayah AWS Jika fungsi Anda disetel ke mode pembaruan Otomatis atau Fungsi, kemungkinan fungsi yang diterapkan secara bersamaan ke Wilayah yang berbeda, atau pada waktu yang berbeda di Wilayah yang sama, akan mengambil versi runtime yang berbeda. Pelanggan yang memerlukan konsistensi versi runtime yang dijamin di seluruh lingkungan mereka harus [menggunakan gambar kontainer untuk menerapkan fungsi Lambda](#) mereka. Mode Manual dirancang sebagai mitigasi sementara untuk mengaktifkan rollback versi runtime jika versi runtime tidak kompatibel dengan fungsi Anda.

Mengonfigurasi pengaturan manajemen runtime Lambda

Anda dapat mengonfigurasi pengaturan manajemen runtime menggunakan konsol Lambda atau () AWS Command Line Interface .AWS CLI

Note

Anda dapat mengonfigurasi pengaturan manajemen runtime secara terpisah untuk setiap [versi fungsi](#).

Untuk mengonfigurasi cara Lambda memperbarui versi runtime Anda (konsol)

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pada tab Kode, di bawah Pengaturan runtime, pilih Edit konfigurasi manajemen runtime.
4. Di bawah Konfigurasi manajemen runtime, pilih salah satu dari berikut ini:
 - Agar fungsi Anda diperbarui ke versi runtime terbaru secara otomatis, pilih Otomatis.
 - Agar fungsi Anda diperbarui ke versi runtime terbaru saat Anda mengubah fungsi, pilih Pembaruan fungsi.
 - Agar fungsi Anda diperbarui ke versi runtime terbaru hanya ketika Anda mengubah versi runtimeARN, pilih Manual. Anda dapat menemukan versi runtime ARN di bawah konfigurasi manajemen Runtime. Anda juga dapat menemukan ARN di INIT_START baris log fungsi Anda.

Untuk informasi selengkapnya tentang opsi ini, lihat [Mode pembaruan waktu proses](#).

5. Pilih Simpan.

Untuk mengonfigurasi cara Lambda memperbarui versi runtime Anda ()AWS CLI

Untuk mengonfigurasi manajemen runtime untuk suatu fungsi, jalankan [put-runtime-management-config](#) AWS CLI perintah. Saat menggunakan Manual mode, Anda juga harus menyediakan versi ARN runtime.

```
aws lambda put-runtime-management-config \
```

```
--function-name my-function \  
--update-runtime-on Manual \  
--runtime-version-arn arn:aws:lambda:us-east-2::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{  
  "UpdateRuntimeOn": "Manual",  
  "FunctionArn": "arn:aws:lambda:us-east-2:111122223333:function:my-function",  
  "RuntimeVersionArn": "arn:aws:lambda:us-east-2::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1"  
}
```

Mengembalikan versi runtime Lambda

Jika versi runtime baru tidak kompatibel dengan fungsi yang ada, Anda dapat memutar kembali versi runtime ke versi sebelumnya. Ini membuat aplikasi Anda tetap berfungsi dan meminimalkan gangguan, memberikan waktu untuk memperbaiki ketidakcocokan sebelum kembali ke versi runtime terbaru.

Lambda tidak memaksakan batas waktu berapa lama Anda dapat menggunakan versi runtime tertentu. Namun, kami sangat menyarankan untuk memperbarui ke versi runtime terbaru sesegera mungkin untuk mendapatkan manfaat dari patch keamanan terbaru, peningkatan kinerja, dan fitur. Lambda menyediakan opsi untuk memutar kembali ke versi runtime sebelumnya hanya sebagai mitigasi sementara jika terjadi masalah kompatibilitas pembaruan runtime yang jarang terjadi. Fungsi yang menggunakan versi runtime sebelumnya untuk jangka waktu yang lama pada akhirnya dapat mengalami penurunan kinerja atau masalah, seperti kedaluwarsa sertifikat, yang dapat menyebabkan mereka berhenti bekerja dengan benar.

Anda dapat memutar kembali versi runtime dengan cara berikut:

- [Menggunakan mode pembaruan runtime Manual](#)
- [Menggunakan versi fungsi yang diterbitkan](#)

Untuk informasi selengkapnya, lihat [Memperkenalkan kontrol manajemen AWS Lambda runtime](#) di Blog AWS Compute.

Kembalikan versi runtime menggunakan mode pembaruan runtime Manual

Jika Anda menggunakan mode pembaruan versi runtime otomatis, atau menggunakan versi **\$LATEST** runtime, Anda dapat memutar kembali versi runtime menggunakan mode Manual. Untuk [versi fungsi](#) yang ingin Anda putar kembali, ubah mode pembaruan versi runtime ke Manual dan tentukan ARN versi runtime sebelumnya. Untuk informasi selengkapnya ARN tentang menemukan versi runtime sebelumnya, lihat [Mengidentifikasi perubahan versi runtime Lambda](#).

Note

Jika **\$LATEST** versi fungsi Anda dikonfigurasi untuk menggunakan mode Manual, maka Anda tidak dapat mengubah CPU arsitektur atau versi runtime yang digunakan fungsi Anda. Untuk membuat perubahan ini, Anda harus mengubah ke mode pembaruan Otomatis atau Fungsi.

Kembalikan versi runtime menggunakan versi fungsi yang diterbitkan

[Versi fungsi](#) yang diterbitkan adalah snapshot yang tidak dapat diubah dari kode **\$LATEST** fungsi dan konfigurasi pada saat Anda membuatnya. Dalam mode Otomatis, Lambda secara otomatis memperbarui versi runtime dari versi fungsi yang diterbitkan selama fase dua peluncuran versi runtime. Dalam mode pembaruan Fungsi, Lambda tidak memperbarui versi runtime dari versi fungsi yang diterbitkan.

Versi fungsi yang diterbitkan menggunakan mode pembaruan Fungsi karenanya membuat snapshot statis dari kode fungsi, konfigurasi, dan versi runtime. Dengan menggunakan mode pembaruan Fungsi dengan versi fungsi, Anda dapat menyinkronkan pembaruan runtime dengan penerapan Anda. Anda juga dapat mengoordinasikan rollback versi kode, konfigurasi, dan runtime dengan mengarahkan lalu lintas ke versi fungsi yang diterbitkan sebelumnya. Anda dapat mengintegrasikan pendekatan ini ke dalam integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD) untuk rollback otomatis sepenuhnya jika terjadi ketidakcocokan pembaruan runtime yang jarang terjadi. Saat menggunakan pendekatan ini, Anda harus memperbarui fungsi Anda secara teratur dan menerbitkan versi fungsi baru untuk mengambil pembaruan runtime terbaru. Untuk informasi selengkapnya, lihat [Memahami model tanggung jawab bersama untuk manajemen runtime Lambda](#).

Mengidentifikasi perubahan versi runtime Lambda

[Nomor versi runtime dan ARN dicatat di baris INIT_START log, yang dipancarkan Lambda CloudWatch ke Log setiap kali menciptakan lingkungan eksekusi baru](#). Karena lingkungan eksekusi menggunakan versi runtime yang sama untuk semua pemanggilan fungsi, Lambda memancarkan

INIT_START baris log hanya ketika Lambda mengeksekusi fase init. Lambda tidak memancarkan baris log ini untuk setiap pemanggilan fungsi. Lambda memancarkan baris log ke CloudWatch Log, tetapi tidak terlihat di konsol.

Example Contoh INIT _ baris START log

```
INIT_START Runtime Version: python:3.9.v14    Runtime Version ARN: arn:aws:lambda:eu-south-1::runtime:7b620fc2e66107a1046b140b9d320295811af3ad5d4c6a011fad1fa65127e9e6I
```

Daripada bekerja secara langsung dengan log, Anda dapat menggunakan [Amazon CloudWatch Contributor Insights](#) untuk mengidentifikasi transisi antar versi runtime. Aturan berikut menghitung versi runtime yang berbeda dari setiap baris INIT_START log. Untuk menggunakan aturan, ganti contoh nama grup log `/aws/lambda/*` dengan awalan yang sesuai untuk fungsi atau grup fungsi Anda.

```
{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "eventType",
        "In": [
          "INIT_START"
        ]
      }
    ],
    "Keys": [
      "runtimeVersion",
      "runtimeVersionArn"
    ]
  },
  "LogFormat": "CLF",
  "LogGroupNames": [
    "/aws/lambda/*"
  ],
  "Fields": {
    "1": "eventType",
    "4": "runtimeVersion",
```

```

    "8": "runtimeVersionArn"
  }
}

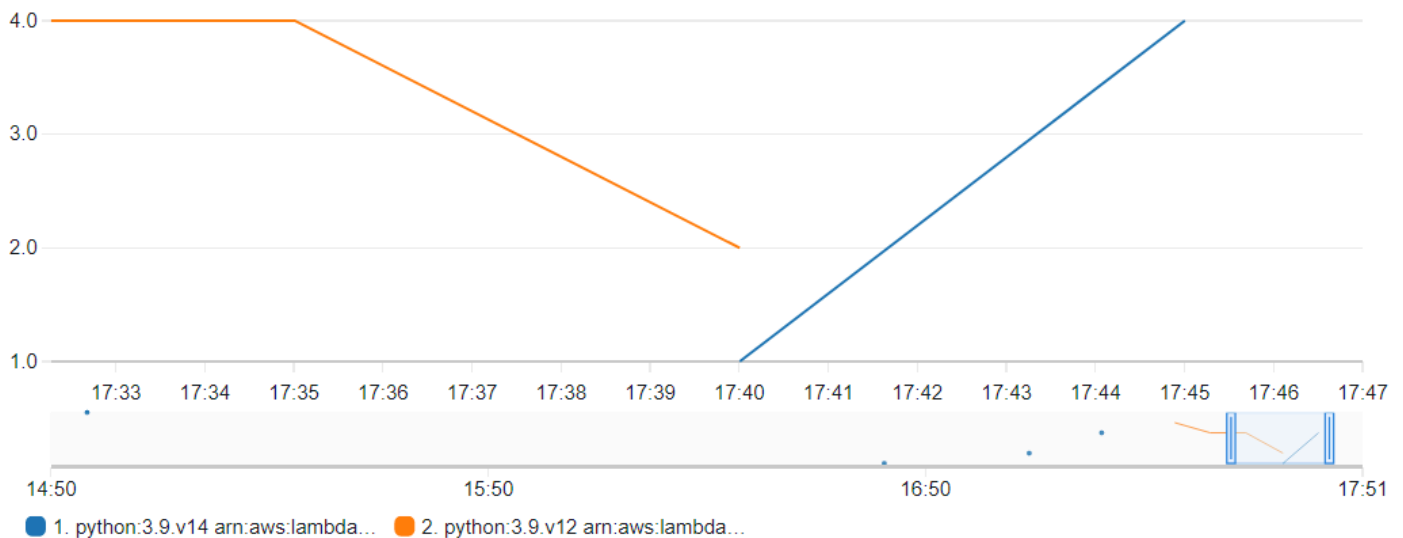
```

Laporan CloudWatch Contributor Insights berikut menunjukkan contoh transisi versi runtime seperti yang ditangkap oleh aturan sebelumnya. Baris oranye menunjukkan inisialisasi lingkungan eksekusi untuk versi runtime sebelumnya (python:3.9.v12), dan garis biru menunjukkan inisialisasi lingkungan eksekusi untuk versi runtime baru (python: 3.9.v14).

Top 2 of 2 unique contributors



2 unique contributors • No unit



Memahami model tanggung jawab bersama untuk manajemen runtime Lambda

Lambda bertanggung jawab untuk mengkurasi dan menerbitkan pembaruan keamanan untuk semua runtime terkelola dan gambar kontainer yang didukung. Tanggung jawab untuk memperbarui fungsi yang ada untuk menggunakan versi runtime terbaru bervariasi tergantung pada mode pembaruan runtime yang Anda gunakan.

Lambda bertanggung jawab untuk menerapkan pembaruan runtime ke semua fungsi yang dikonfigurasi untuk menggunakan mode Pembaruan runtime Otomatis.

Untuk fungsi yang dikonfigurasi dengan mode pembaruan runtime pembaruan Fungsi, Anda bertanggung jawab untuk memperbarui fungsi secara teratur. Lambda bertanggung jawab untuk menerapkan pembaruan runtime saat Anda melakukan pembaruan tersebut. Jika Anda tidak memperbarui fungsi Anda, maka Lambda tidak memperbarui runtime. Jika Anda tidak memperbarui

fungsi Anda secara teratur, maka kami sangat menyarankan untuk mengonfigurasinya untuk pembaruan runtime otomatis sehingga terus menerima pembaruan keamanan.

Untuk fungsi yang dikonfigurasi untuk menggunakan mode pembaruan runtime Manual, Anda bertanggung jawab untuk memperbarui fungsi agar menggunakan versi runtime terbaru. Kami sangat menyarankan Anda menggunakan mode ini hanya untuk memutar kembali versi runtime sebagai mitigasi sementara jika terjadi ketidakcocokan pembaruan runtime yang jarang terjadi. Kami juga menyarankan agar Anda mengubah ke mode Otomatis secepat mungkin untuk meminimalkan waktu di mana fungsi Anda tidak ditambal.

Jika Anda [menggunakan gambar kontainer untuk menerapkan fungsi Anda](#), Lambda bertanggung jawab untuk menerbitkan gambar dasar yang diperbarui. Dalam hal ini, Anda bertanggung jawab untuk membangun kembali image kontainer fungsi Anda dari image dasar terbaru dan menerapkan kembali image container.

Ini dirangkum dalam tabel berikut:

| Mode deployment | Tanggung jawab Lambda | Tanggung jawab pelanggan |
|--|---|--|
| Runtime terkelola, mode Otomatis | Publikasikan versi runtime baru yang berisi tambalan terbaru. Terapkan patch runtime ke fungsi yang ada. | Kembalikan ke versi runtime sebelumnya jika terjadi masalah kompatibilitas pembaruan runtime yang jarang terjadi. |
| Runtime terkelola, Mode pembaruan Fungsi | Publikasikan versi runtime baru yang berisi tambalan terbaru. | Perbarui fungsi secara teratur untuk mengambil versi runtime terbaru. Ganti fungsi ke mode Otomatis saat Anda tidak memperbarui fungsi secara teratur. Kembalikan ke versi runtime sebelumnya jika terjadi masalah kompatibilitas pembaruan runtime yang jarang terjadi. |
| Runtime terkelola, mode Manual | Publikasikan versi runtime baru yang berisi tambalan terbaru. | Gunakan mode ini hanya untuk rollback runtime sementara jika terjadi masalah kompatibilitas pembaruan runtime yang jarang terjadi. |

| Mode deployment | Tanggung jawab Lambda | Tanggung jawab pelanggan |
|------------------|--|---|
| | | Ganti fungsi ke mode pembaruan Otomatis atau Fungsi dan versi runtime terbaru sesegera mungkin. |
| Gambar kontainer | Publikasikan gambar kontainer baru yang berisi tambalan terbaru. | Menerapkan ulang fungsi secara teratur menggunakan gambar dasar kontainer terbaru untuk mengambil tambalan terbaru. |

Untuk informasi selengkapnya tentang tanggung jawab bersama AWS, lihat [Model Tanggung Jawab Bersama](#).

Mengontrol izin pembaruan runtime Lambda untuk aplikasi dengan kepatuhan tinggi

Untuk memenuhi persyaratan penambalan, pelanggan Lambda biasanya mengandalkan pembaruan runtime otomatis. Jika aplikasi Anda tunduk pada persyaratan kesegaran patch yang ketat, Anda mungkin ingin membatasi penggunaan versi runtime sebelumnya. Anda dapat membatasi kontrol manajemen runtime Lambda dengan menggunakan AWS Identity and Access Management (IAM) untuk menolak pengguna di akses AWS akun Anda ke operasi. [PutRuntimeManagementConfigAPI](#) Operasi ini digunakan untuk memilih mode pembaruan runtime untuk suatu fungsi. Menolak akses ke operasi ini menyebabkan semua fungsi default ke mode Otomatis. Anda dapat menerapkan pembatasan ini di seluruh organisasi Anda dengan menggunakan [kebijakan kontrol layanan \(SCP\)](#). Jika Anda harus memutar kembali fungsi ke versi runtime sebelumnya, Anda dapat memberikan pengecualian kebijakan case-by-case berdasarkan.

Mengambil data tentang fungsi Lambda yang menggunakan runtime usang

Saat runtime Lambda mendekati penghentian, Lambda memberi tahu Anda melalui email dan memberikan pemberitahuan di dan. AWS Health Dashboard Trusted Advisor Email dan notifikasi ini mencantumkan versi fungsi \$ LATEST menggunakan runtime. Untuk mencantumkan semua versi fungsi yang menggunakan runtime tertentu, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) atau salah satu AWS SDK.

Jika Anda memiliki sejumlah besar fungsi yang menggunakan runtime yang akan usang, Anda juga dapat menggunakan AWS CLI atau AWS SDK untuk membantu Anda memprioritaskan pembaruan ke fungsi yang paling sering dipanggil.

Lihat bagian berikut untuk mempelajari cara menggunakan AWS CLI dan AWS SDK untuk mengumpulkan data tentang fungsi yang menggunakan runtime tertentu.

Daftar versi fungsi yang menggunakan runtime tertentu

Untuk menggunakan daftar semua versi fungsi Anda yang menggunakan runtime tertentu, jalankan perintah berikut. AWS CLI Ganti `RUNTIME_IDENTIFIER` dengan nama runtime yang sudah tidak digunakan lagi dan pilih sendiri. Wilayah AWS Untuk daftar hanya versi fungsi \$LATEST, hilangkan `--function-version ALL` dari perintah.

```
aws lambda list-functions --function-version ALL --region us-east-1 --output text --query "Functions[?Runtime=='RUNTIME_IDENTIFIER'].FunctionArn"
```

Tip

Contoh perintah mencantumkan fungsi di `us-east-1` wilayah untuk tertentu Akun AWS. Anda harus mengulangi perintah ini untuk setiap wilayah di mana akun Anda memiliki fungsi dan untuk masing-masing Akun AWS.

Anda juga dapat membuat daftar fungsi yang menggunakan runtime tertentu menggunakan salah satu AWS SDK. Contoh kode berikut menggunakan V3 AWS SDK for JavaScript dan AWS SDK for Python (Boto3) untuk mengembalikan daftar fungsi ARN untuk fungsi menggunakan runtime tertentu. Kode contoh juga mengembalikan grup CloudWatch log untuk masing-masing fungsi yang terdaftar.

Anda dapat menggunakan grup log ini untuk menemukan tanggal pemanggilan terakhir untuk fungsi tersebut. Lihat bagian berikut [the section called “Mengidentifikasi fungsi yang paling umum dan paling baru dipanggil”](#) untuk informasi lebih lanjut.

Node.js

Example JavaScript kode untuk daftar fungsi menggunakan runtime tertentu

```
import { LambdaClient, ListFunctionsCommand } from "@aws-sdk/client-lambda";
const lambdaClient = new LambdaClient();

const command = new ListFunctionsCommand({
  FunctionVersion: "ALL",
  MaxItems: 50
});
const response = await lambdaClient.send(command);

for (const f of response.Functions){
  if (f.Runtime == '<your_runtime>'){ // Use the runtime id, e.g. 'nodejs18.x' or
  'python3.9'
    console.log(f.FunctionArn);
    // get the CloudWatch log group of the function to
    // use later for finding the last invocation date
    console.log(f.LoggingConfig.LogGroup);
  }
}
// If your account has more functions than the specified
// MaxItems, use the returned pagination token in the
// next request with the 'Marker' parameter
if ('NextMarker' in response){
  let paginationToken = response.NextMarker;
}
```

Python

Example Kode Python untuk mencantumkan fungsi menggunakan runtime tertentu

```
import boto3

lambda_client = boto3.client('lambda')

response = lambda_client.list_functions(
  FunctionVersion='ALL',
```

```
    MaxItems=50
)

for function in response['Functions']:
    if function['Runtime'] == '<your_runtime>': # Use the runtime id, e.g.
        'nodejs18.x' or 'python3.9'
        print(function['FunctionArn'])
        # Print the CloudWatch log group of the function
        # to use later for finding last invocation date
        print(function['LoggingConfig']['LogGroup'])

# If your account has more functions than the specified
# MaxItems, use the returned pagination token in the
# next request with the 'Marker' parameter
if 'NextMarker' in response:
    pagination_token = response['NextMarker']
```

Untuk mempelajari lebih lanjut tentang menggunakan AWS SDK untuk mencantumkan fungsi Anda menggunakan [ListFunctionstindakan](#), lihat [dokumentasi SDK](#) untuk bahasa pemrograman pilihan Anda.

Anda juga dapat menggunakan fitur Kueri AWS Config lanjutan untuk mencantumkan semua fungsi yang menggunakan runtime yang terpengaruh. Kueri ini hanya mengembalikan fungsi \$LATEST versi, tetapi Anda dapat menggabungkan kueri ke daftar fungsi di semua wilayah dan beberapa Akun AWS dengan satu perintah. Untuk mempelajari selengkapnya, lihat [Menanyakan Status AWS Auto Scaling Sumber Daya Konfigurasi Saat Ini](#) di Panduan AWS Config Pengembang.

Mengidentifikasi fungsi yang paling umum dan paling baru dipanggil

Jika Akun AWS berisi fungsi yang menggunakan runtime yang seharusnya tidak digunakan lagi, Anda mungkin ingin memprioritaskan fungsi pembaruan yang sering dipanggil atau fungsi yang baru saja dipanggil.

Jika Anda hanya memiliki beberapa fungsi, Anda dapat menggunakan konsol CloudWatch Log untuk mengumpulkan informasi ini dengan melihat aliran log fungsi Anda. [Lihat Melihat data log yang dikirim ke CloudWatch Log](#) untuk informasi selengkapnya.

Untuk melihat jumlah pemanggilan fungsi terbaru, Anda juga dapat menggunakan informasi CloudWatch metrik yang ditampilkan di konsol Lambda. Untuk melihat informasi ini, lakukan hal berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang ingin Anda lihat statistik pemanggilan.
3. Pilih tab Monitor.
4. Tetapkan periode waktu yang ingin Anda lihat statistik untuk menggunakan pemilih rentang tanggal. Pemanggilan terbaru ditampilkan di panel Pemanggilan.

Untuk akun dengan jumlah fungsi yang lebih besar, akan lebih efisien untuk mengumpulkan data ini secara terprogram menggunakan AWS CLI atau salah satu AWS SDK menggunakan tindakan API [DescribeLogStreams](#) dan [GetMetricStatistics](#).

Contoh berikut menyediakan cuplikan kode menggunakan V3 AWS SDK for JavaScript dan AWS SDK for Python (Boto3) untuk mengidentifikasi tanggal pemanggilan terakhir untuk fungsi tertentu dan untuk menentukan jumlah pemanggilan untuk fungsi tertentu dalam 14 hari terakhir.

Node.js

Example JavaScript kode untuk menemukan waktu pemanggilan terakhir untuk suatu fungsi

```
import { CloudWatchLogsClient, DescribeLogStreamsCommand } from "@aws-sdk/client-cloudwatch-logs";
const cloudWatchLogsClient = new CloudWatchLogsClient();
const command = new DescribeLogStreamsCommand({
  logGroupName: '<your_log_group_name>',
  orderBy: 'LastEventTime',
  limit: 1
});
try {
  const response = await cloudWatchLogsClient.send(command);
  const lastEventTimestamp = response.logStreams.length > 0 ?
    response.logStreams[0].lastEventTimestamp : null;
  // Convert the UNIX timestamp to a human-readable format for display
  const date = new Date(lastEventTimestamp).toLocaleDateString();
  const time = new Date(lastEventTimestamp).toLocaleTimeString();
  console.log(`${date} ${time}`);
} catch (e){
  console.error('Log group not found.')
}
```

Python

Example Kode Python untuk menemukan waktu pemanggilan terakhir untuk suatu fungsi

```
import boto3
from datetime import datetime

cloudwatch_logs_client = boto3.client('logs')

response = cloudwatch_logs_client.describe_log_streams(
    logGroupName='<your_log_group_name>',
    orderBy='LastEventTime',
    limit=1
)

try:
    if len(response['logStreams']) > 0:
        last_event_timestamp = response['logStreams'][0]['lastEventTimestamp']
        print(datetime.fromtimestamp(last_event_timestamp/1000)) # Convert timestamp
        from ms to seconds
    else:
        last_event_timestamp = None
except:
    print('Log group not found')
```

Tip

Anda dapat menemukan nama grup log fungsi Anda menggunakan operasi [ListFunctionsAPI](#). Lihat kode di [the section called “Daftar versi fungsi yang menggunakan runtime tertentu”](#) untuk contoh bagaimana melakukan ini.

Node.js

Example JavaScript kode untuk menemukan jumlah pemanggilan dalam 14 hari terakhir

```
import { CloudWatchClient, GetMetricStatisticsCommand } from "@aws-sdk/client-cloudwatch";
const cloudWatchClient = new CloudWatchClient();
const command = new GetMetricStatisticsCommand({
    Namespace: 'AWS/Lambda',
```

```

    MetricName: 'Invocations',
    StartTime: new Date(Date.now()-86400*1000*14), // 14 days ago
    EndTime: new Date(Date.now()),
    Period: 86400 * 14, // 14 days.
    Statistics: ['Sum'],
    Dimensions: [{
      Name: 'FunctionName',
      Value: '<your_function_name>'
    }]
  });
const response = await cloudWatchClient.send(command);
const invokesInLast14Days = response.Datapoints.length > 0 ?
  response.Datapoints[0].Sum : 0;

console.log('Number of invocations: ' + invokesInLast14Days);

```

Python

Example Kode Python untuk menemukan jumlah pemanggilan dalam 14 hari terakhir

```

import boto3
from datetime import datetime, timedelta

cloudwatch_client = boto3.client('cloudwatch')

response = cloudwatch_client.get_metric_statistics(
    Namespace='AWS/Lambda',
    MetricName='Invocations',
    Dimensions=[
        {
            'Name': 'FunctionName',
            'Value': '<your_function_name>'
        },
    ],
    StartTime=datetime.now() - timedelta(days=14),
    EndTime=datetime.now(),
    Period=86400 * 14, # 14 days
    Statistics=[
        'Sum'
    ]
)

if len(response['Datapoints']) > 0:

```

```
    invokes_in_last_14_days = int(response['Datapoints'][0]['Sum'])
else:
    invokes_in_last_14_days = 0

print(f'Number of invocations: {invokes_in_last_14_days}')
```

Memodifikasi lingkungan waktu pengoperasian

Anda dapat menggunakan [ekstensi internal](#) untuk memodifikasi proses waktu pengoperasian. Ekstensi internal bukan proses terpisah—ekstensi ini berjalan sebagai bagian dari proses waktu pengoperasian.

Lambda menyediakan [variabel lingkungan](#) spesifik bahasa yang dapat Anda atur untuk menambahkan opsi dan alat pada waktu pengoperasian. Lambda juga menyediakan [skrip pembungkus](#), yang memungkinkan Lambda mendelegasikan startup waktu pengoperasian ke skrip Anda. Anda dapat membuat skrip pembungkus untuk mengustomisasikan perilaku startup waktu pengoperasian.

Variabel lingkungan spesifik bahasa

Lambda mendukung cara konfigurasi saja untuk mengaktifkan kode yang akan dipramuat selama inialisasi fungsi melalui variabel lingkungan spesifik bahasa berikut:

- `JAVA_TOOL_OPTIONS`— Di Java, Lambda mendukung variabel lingkungan ini untuk mengatur variabel baris perintah tambahan di Lambda. Variabel lingkungan ini memungkinkan Anda menentukan inialisasi alat, khususnya peluncuran agen bahasa pemrograman asli atau Java menggunakan opsi `agentlib` atau `javaagent`. Untuk informasi selengkapnya, lihat [variabel `JAVA_TOOL_OPTIONS` lingkungan](#).
- `NODE_OPTIONS`- Tersedia di [runtime Node.js](#).
- `DOTNET_STARTUP_HOOKS` – Pada NET Core 3.1 dan di atas, variabel lingkungan ini menentukan jalur ke rakitan (dll) yang dapat Lambda gunakan.

Menggunakan variabel lingkungan spesifik bahasa adalah cara yang lebih disukai untuk mengatur properti startup.

Skrip pembungkus

Anda dapat membuat skrip pembungkus untuk mengustomisasikan perilaku startup waktu pengoperasian fungsi Lambda. Skrip pembungkus memungkinkan Anda mengatur parameter konfigurasi yang tidak dapat diatur melalui variabel lingkungan spesifik bahasa.

Note

Invokasi dapat gagal jika skrip pembungkus tidak berhasil memulai proses waktu pengoperasian.

[Skrip pembungkus didukung pada semua runtime Lambda asli](#). Skrip pembungkus tidak didukung pada [Runtime khusus OS](#) (keluarga provided runtime).

Saat Anda menggunakan skrip pembungkus untuk fungsi, Lambda memulai waktu pengoperasian menggunakan skrip Anda. Lambda mengirim ke skrip Anda jalur ke interpreter dan semua argumen asli untuk startup waktu pengoperasian standar. Skrip Anda dapat memperluas atau mengubah perilaku startup program. Misalnya, skrip dapat menyuntikkan dan mengubah argumen, mengatur variabel lingkungan, atau menangkap metrik, kesalahan, dan informasi diagnostik lainnya.

Anda menentukan skrip dengan mengatur nilai dari variabel lingkungan `AWS_LAMBDA_EXEC_WRAPPER` sebagai jalur sistem file dari biner atau skrip yang dapat dijalankan.

Contoh: Buat dan gunakan skrip pembungkus dengan Python 3.8

Dalam contoh berikut, Anda membuat skrip pembungkus untuk memulai interpreter Python dengan opsi `-X importtime`. Saat Anda menjalankan fungsi, Lambda membuat entri log untuk menampilkan durasi waktu impor untuk tiap impor.

Untuk membuat dan gunakan skrip pembungkus dengan Python 3.8

1. Untuk membuat skrip pembungkus, tempelkan kode berikut ke file bernama `importtime_wrapper`:

```
#!/bin/bash

# the path to the interpreter and all of the originally intended arguments
args=("$@")

# the extra options to pass to the interpreter
extra_args="-X importtime"

# insert the extra options
args=("${args[@]:0:$#-1}" "${extra_args[@]}" "${args[@]: -1}")
```



```
# start the runtime with the extra options
exec "${args[@]}"
```

2. Untuk memberi skrip izin yang dapat dijalankan, masukkan `chmod +x importtime_wrapper` dari baris perintah.
3. Terapkan skrip sebagai [Lapisan Lambda](#).
4. Buat fungsi menggunakan konsol Lambda.
 - a. Buka [konsol Lambda](#).
 - b. Pilih Buat fungsi.
 - c. Di bagian Informasi dasar, untuk Nama fungsi, masukkan **wrapper-test-function**.
 - d. Untuk Waktu pengoperasian, pilih Python 3.8.
 - e. Pilih Buat fungsi.
5. Tambahkan lapisan ke fungsi Anda.
 - a. Pilih fungsi Anda, lalu pilih Kode jika belum dipilih.
 - b. Pilih Tambahkan lapisan.
 - c. Di bagian Pilih lapisan, pilih Nama dan Versi dari lapisan kompatibel yang Anda buat sebelumnya.
 - d. Pilih Tambahkan.
6. Tambahkan kode dan variabel lingkungan ke fungsi Anda.
 - a. Dalam fungsi [editor kode](#), tempelkan kode fungsi berikut:

```
import json

def lambda_handler(event, context):
    # TODO implement
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

- b. Pilih Simpan.
- c. Pada Variabel lingkungan, pilih Edit.
- d. Pilih Tambahkan variabel lingkungan.

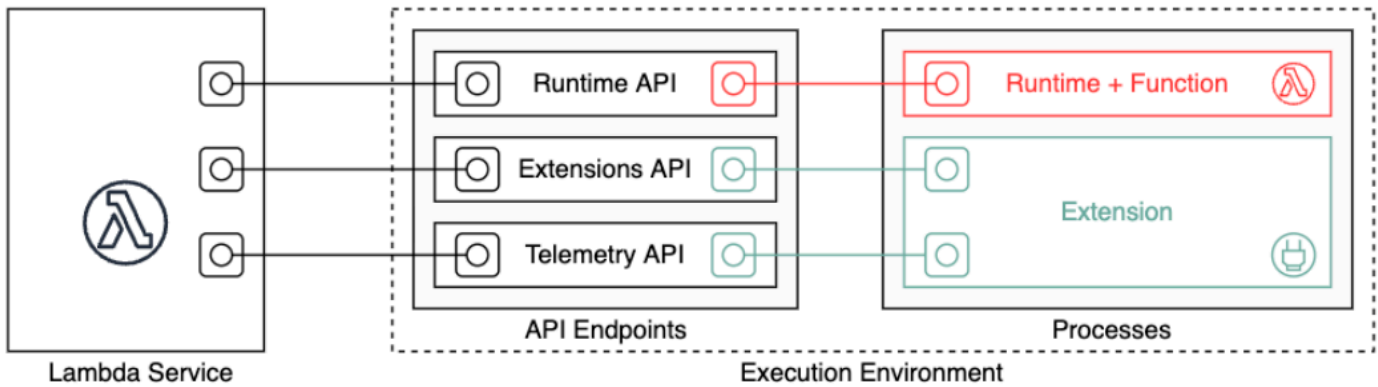
- e. Untuk Kunci, masukkan `AWS_LAMBDA_EXEC_WRAPPER`.
 - f. Untuk Nilai, masukkan `/opt/importtime_wrapper`.
 - g. Pilih Simpan.
7. Untuk menjalankan fungsi, pilih Uji.

Karena skrip pembungkus Anda memulai interpreter Python dengan opsi `-X importtime`, log menunjukkan waktu yang diperlukan untuk setiap impor. Sebagai contoh:

```
...
2020-06-30T18:48:46.780+01:00 import time: 213 | 213 | simplejson
2020-06-30T18:48:46.780+01:00 import time: 50 | 263 | simplejson.raw_json
...
```

Menggunakan runtime Lambda untuk runtime khusus API

AWS Lambda [menyediakan runtime khusus HTTP API untuk menerima acara pemanggilan dari Lambda dan mengirim data respons kembali dalam lingkungan eksekusi Lambda](#). Bagian ini berisi API referensi untuk runtime Lambda. API



API [Spesifikasi Terbuka untuk API versi runtime 2018-06-01 tersedia di runtime-api.zip](#)

Untuk membuat API permintaan URL, runtime mendapatkan API titik akhir dari variabel `AWS_LAMBDA_RUNTIME_API` lingkungan, menambahkan API versi, dan menambahkan jalur sumber daya yang diinginkan.

Example Permintaan

```
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next"
```

API metode

- [Invokasi berikutnya](#)
- [Respons invokasi](#)
- [Kesalahan inisialisasi](#)
- [Kesalahan invokasi](#)

Invokasi berikutnya

Jalur – `/runtime/invocation/next`

Metode - GET

Runtime mengirimkan pesan ini ke Lambda untuk meminta peristiwa invokasi. Badan respons berisi muatan dari pemanggilan, yang merupakan JSON dokumen yang berisi data peristiwa dari pemicu fungsi. Header respons berisi data tambahan tentang invokasi.

Header respons

- `Lambda-Runtime-Aws-Request-Id` – ID permintaan, yang mengidentifikasi permintaan pemicu invokasi fungsi.

Misalnya, `8476a536-e9f4-11e8-9739-2dfe598c3fcd`.

- `Lambda-Runtime-Deadline-Ms` – Tanggal saat fungsi berakhir, dalam milidetik waktu Unix.

Misalnya, `1542409706888`.

- `Lambda-Runtime-Invoked-Function-Arn`— Fungsi ARN Lambda, versi, atau alias yang ditentukan dalam pemanggilan.

Misalnya, `arn:aws:lambda:us-east-2:123456789012:function:custom-runtime`.

- `Lambda-Runtime-Trace-Id` – [Header pelacakan AWS X-Ray](#).

Misalnya, `Root=1-5bef4de7-ad49b0e87f6ef6c87fc2e700;Parent=9a9197af755a6419;Sampled=1`.

- `Lambda-Runtime-Client-Context`— Untuk pemanggilan dari AWS MobileSDK, data tentang aplikasi dan perangkat klien.
- `Lambda-Runtime-Cognito-Identity`— Untuk pemanggilan dari AWS PonselSDK, data tentang penyedia identitas Amazon Cognito.

Jangan atur waktu habis permintaan GET karena respons dapat tertunda. Antara saat Lambda melakukan bootstrap pada waktu pengoperasian dan saat waktu pengoperasian memiliki kejadian untuk dikembalikan, proses waktu pengoperasian mungkin dibekukan selama beberapa detik.

ID permintaan melacak invokasi di dalam Lambda. Gunakan untuk menentukan invokasi saat Anda mengirim respons.

Header pelacakan berisi ID jejak, ID induk, dan keputusan penyampelan. Jika permintaan diambil sampelnya, permintaan diambil sampelnya oleh Lambda atau layanan hulu. Waktu pengoperasian harus menetapkan `_X_AMZN_TRACE_ID` dengan nilai header. SDK X-Ray membaca ini untuk mendapatkan IDs dan menentukan apakah akan melacak permintaan.

Respons invokasi

Jalur – `/runtime/invocation/AwsRequestId/response`

Metode - POST

Setelah fungsi selesai dijalankan, runtime mengirimkan respon invokasi untuk Lambda. Untuk invokasi sinkron, Lambda mengirimkan respons ke klien.

Example permintaan berhasil

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response" -d "SUCCESS"
```

Kesalahan inisialisasi

Jika fungsi mengembalikan kesalahan atau runtime mengalami kesalahan saat inisialisasi, runtime menggunakan metode ini untuk melaporkan kesalahan ke Lambda.

Jalur – `/runtime/init/error`

Metode - POST

Header

`Lambda-Runtime-Function-Error-Type`— Jenis kesalahan yang ditemui runtime. Wajib: tidak.

Header ini terdiri dari nilai string. Lambda menerima string apa pun, tetapi kami merekomendasikan format `<category.reason>`. Sebagai contoh:

- `Runtime.NoSuchHandler`
- `Runtime.APIKeyNotFound`
- `Runtime.ConfigInvalid`
- `Runtime.UnknownReason`

Parameter tubuh

`ErrorRequest` – Informasi tentang kesalahan. Wajib: tidak.

Bidang ini adalah JSON objek dengan struktur sebagai berikut:

```
{
  errorMessage: string (text description of the error),
  errorType: string,
  stackTrace: array of strings
}
```

Perhatikan bahwa Lambda menerima nilai apa pun untuk `errorType`.

Contoh berikut menunjukkan pesan kesalahan fungsi Lambda ketika fungsi tidak dapat mengurai data peristiwa yang disediakan dalam invokasi.

Example Kesalahan fungsi

```
{
  "errorMessage" : "Error parsing event data.",
  "errorType" : "InvalidEventDataException",
  "stackTrace": [ ]
}
```

Parameter isi respons

- `StatusResponse` – String. Informasi status, dikirim dengan kode respons 202.
- `ErrorResponse` – Informasi kesalahan tambahan, dikirim dengan kode respons kesalahan. `ErrorResponse` berisi jenis kesalahan dan pesan kesalahan.

Kode respons

- 202 – Diterima
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Runtime harus segera keluar.

Example permintaan kesalahan inisialisasi

```
ERROR="{\"errorMessage\" : \"Failed to load function.\", \"errorType\" :  
  \"InvalidFunctionException\"}"  
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/init/error" -d "$ERROR" --  
header "Lambda-Runtime-Function-Error-Type: Unhandled"
```

Kesalahan invokasi

Jika fungsi mengembalikan kesalahan atau runtime mengalami kesalahan, runtime menggunakan metode ini untuk melaporkan kesalahan ke Lambda.

Jalur – `/runtime/invocation/AwsRequestId/error`

Metode - POST

Header

`Lambda-Runtime-Function-Error-Type`— Jenis kesalahan yang ditemui runtime. Wajib: tidak.

Header ini terdiri dari nilai string. Lambda menerima string apa pun, tetapi kami merekomendasikan format `<category.reason>`. Sebagai contoh:

- `Runtime.NoSuchHandler`
- `Runtime.APIKeyNotFound`
- `Runtime.ConfigInvalid`
- `Runtime.UnknownReason`

Parameter tubuh

`ErrorRequest` – Informasi tentang kesalahan. Wajib: tidak.

Bidang ini adalah JSON objek dengan struktur sebagai berikut:

```
{
  errorMessage: string (text description of the error),
  errorType: string,
  stackTrace: array of strings
}
```

Perhatikan bahwa Lambda menerima nilai apa pun untuk `errorType`.

Contoh berikut menunjukkan pesan kesalahan fungsi Lambda ketika fungsi tidak dapat mengurai data peristiwa yang disediakan dalam invokasi.

Example Kesalahan fungsi

```
{
```

```
"errorMessage" : "Error parsing event data.",  
"errorType" : "InvalidEventDataException",  
"stackTrace": [ ]  
}
```

Parameter isi respons

- **StatusResponse** – String. Informasi status, dikirim dengan kode respons 202.
- **ErrorResponse** – Informasi kesalahan tambahan, dikirim dengan kode respons kesalahan. ErrorResponse berisi jenis kesalahan dan pesan kesalahan.

Kode respons

- 202 – Diterima
- 400 – Permintaan Buruk
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Runtime harus segera keluar.

Example permintaan kesalahan

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9  
ERROR="{\"errorMessage\" : \"Error parsing event data.\", \"errorType\" :  
  \"InvalidEventDataException\"}"  
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/error"  
-d "$ERROR" --header "Lambda-Runtime-Function-Error-Type: Unhandled"
```


Kapan menggunakan runtime khusus OS Lambda

Lambda menyediakan [runtime terkelola](#) untuk Java, Python, Node.js, .NET, dan Ruby. Untuk membuat fungsi Lambda dalam bahasa pemrograman yang tidak tersedia sebagai runtime terkelola, gunakan runtime khusus OS (keluarga runtime). provided Ada tiga kasus penggunaan utama untuk runtime khusus OS:

- **Kompilasi asli ahead-of-time (AOT):** Bahasa seperti Go, Rust, dan C++ dikompilasi secara native ke biner yang dapat dieksekusi, yang tidak memerlukan runtime bahasa khusus. Bahasa-bahasa ini hanya membutuhkan lingkungan OS di mana biner yang dikompilasi dapat berjalan. Anda juga dapat menggunakan runtime khusus OS Lambda untuk menyebarkan binari yang dikompilasi dengan .NET Native AOT dan Java GraalVM Native.

Anda harus menyertakan klien antarmuka runtime dalam biner Anda. Klien antarmuka runtime memanggil [Menggunakan runtime Lambda untuk runtime khusus API](#) untuk mengambil pemanggilan fungsi dan kemudian memanggil penanganan fungsi Anda. [Lambda menyediakan klien antarmuka runtime untuk Go, .NET Native AOT, C ++, dan Rust \(eksperimental\)](#).

Anda harus mengkompilasi biner Anda untuk lingkungan Linux dan untuk arsitektur set instruksi yang sama yang Anda rencanakan untuk digunakan untuk fungsi (x86_64 atau arm64).

- **Runtime pihak ketiga:** [Anda dapat menjalankan fungsi Lambda off-the-shelf menggunakan runtime seperti Bref untuk PHP atau Swift Runtime untuk Swift. AWS Lambda](#)
- **Runtime kustom:** Anda dapat membuat runtime sendiri untuk versi bahasa atau bahasa yang Lambda tidak menyediakan runtime terkelola, seperti Node.js 19. Untuk informasi selengkapnya, lihat [Membangun runtime khusus untuk AWS Lambda](#). Ini adalah kasus penggunaan yang paling tidak umum untuk runtime khusus OS.

Lambda mendukung runtime khusus OS berikut:

Hanya OS

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------|------------------|-------------------|---------------------|------------------|-----------------------|
| Runtime Khusus OS | provided.a12023 | Amazon Linux 2023 | | | |

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------|------------------|----------------|---------------------|------------------|-----------------------|
| Runtime Khusus OS | provided.a12 | Amazon Linux 2 | | | |

Runtime Amazon Linux 2023 (`provided.a12023`) memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti `glibc`

`provided.a12023` Runtime digunakan `dnf` sebagai manajer paket, bukan `yum`, yang merupakan manajer paket default di Amazon Linux 2. Untuk informasi selengkapnya tentang perbedaan antara `provided.a12023` dan `provided.a12`, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda di Blog](#) AWS Komputasi.

Membangun runtime khusus untuk AWS Lambda

Anda dapat menerapkan AWS Lambda runtime dalam bahasa pemrograman apa pun. Runtime adalah program yang menjalankan metode handler fungsi Lambda saat fungsi tersebut dipanggil. [Anda dapat menyertakan runtime dalam paket penerapan fungsi Anda atau mendistribusikannya dalam lapisan](#). Saat Anda membuat fungsi Lambda, pilih runtime khusus [OS \(keluarga runtime\)](#).
`provided`

Note

Membuat runtime kustom adalah kasus penggunaan lanjutan. Jika Anda mencari informasi tentang kompilasi ke biner asli atau menggunakan off-the-shelf runtime pihak ketiga, lihat [Kapan menggunakan runtime khusus OS Lambda](#)

Untuk panduan tentang proses penerapan runtime kustom, lihat [Tutorial: Membangun runtime khusus](#) Anda juga dapat menjelajahi runtime khusus yang diterapkan di C++ di [aws-lambda-cppawslabs/](#) on. GitHub

Topik

- [Persyaratan](#)
- [Menerapkan streaming respons dalam runtime khusus](#)

Persyaratan

Runtime kustom harus menyelesaikan tugas inialisasi dan pemrosesan tertentu. Runtime menjalankan kode penyiapan fungsi, membaca nama handler dari variabel lingkungan, dan membaca peristiwa pemanggilan dari API runtime Lambda. Runtime meneruskan data event ke handler fungsi, dan memposting respons dari handler kembali ke Lambda.

Tugas initalisasi

Tugas inialisasi dijalankan sekali [per instans fungsi](#) untuk menyiapkan lingkungan untuk menangani invokasi.

- Ambil pengaturan – Baca variabel lingkungan untuk mendapatkan detail tentang fungsi dan lingkungan.
 - `_HANDLER` – Lokasi ke handler, dari konfigurasi fungsi. Format standar adalah *file.method*, dengan `file` adalah nama file tanpa ekstensi, dan `method` merupakan nama metode atau fungsi yang ditentukan dalam file.
 - `LAMBDA_TASK_ROOT` – Direktori yang berisi kode fungsi.
 - `AWS_LAMBDA_RUNTIME_API` – Host dan port API runtime.

Untuk daftar lengkap variabel yang tersedia, lihat [Variabel lingkungan runtime yang ditetapkan](#).

- Inialisasi fungsi – Muat file handler dan jalankan kode global atau statis yang ada di dalamnya. Fungsi harus membuat sumber daya statis seperti klien SDK dan koneksi database satu kali, dan menggunakannya kembali untuk beberapa invokasi.
- Mengatasi kesalahan – Jika terjadi kesalahan, hubungi [kesalahan inialisasi](#) API dan segera keluar.

Inialisasi diperhitungkan dalam waktu dan batas waktu eksekusi yang ditagih. Saat eksekusi memicu inialisasi instans baru dari fungsi, Anda dapat melihat waktu inialisasi dalam log dan [jejak AWS X-Ray](#).

Example log

```
REPORT RequestId: f8ac1208... Init Duration: 48.26 ms   Duration: 237.17 ms   Billed
Duration: 300 ms   Memory Size: 128 MB   Max Memory Used: 26 MB
```

Memproses tugas

Saat belajar, runtime menggunakan [antarmuka runtime Lambda](#) untuk mengelola event masuk dan melaporkan kesalahan. Setelah menyelesaikan tugas inisialisasi, runtime memproses event masuk secara berulang. Dalam kode runtime Anda, lakukan langkah berikut secara berurutan.

- Dapatkan event – Hubungi [API invokasi berikutnya](#) untuk mendapatkan event berikutnya. Badan respons berisi data event. Header respons berisi ID permintaan dan informasi lainnya.
- Sebarkan header pelacakan – Dapatkan header pelacakan X-Ray dari header `Lambda-Runtime-Trace-Id` di respons API. Tetapkan variabel lingkungan `_X_AMZN_TRACE_ID` secara lokal dengan nilai yang sama. X-Ray SDK menggunakan nilai ini untuk menghubungkan data pelacakan di antara layanan.
- Buat objek konteks – Buat objek dengan informasi konteks dari variabel lingkungan dan header dalam respons API.
- Memanggil handler fungsi – Berikan event dan objek konteks ke handler.
- Menangani respons – Hubungi [respons pemanggil](#) API untuk memposting respons dari penanggung jawab.
- Mengatasi kesalahan – Jika terjadi kesalahan, hubungi [kesalahan invokasi](#) API.
- Pembersihan – Lepaskan sumber daya yang tidak digunakan, kirim data ke layanan lain, atau lakukan tugas tambahan sebelum melanjutkan ke event berikutnya.

Entrypoint

Titik entri runtime kustom adalah file eksekusi bernama `bootstrap`. File `bootstrap` dapat menjadi runtime, atau dapat memanggil file lain yang membuat runtime. Jika root paket penyebaran Anda tidak berisi file bernama `bootstrap`, Lambda mencari file di lapisan fungsi. Jika `bootstrap` file tidak ada atau tidak dapat dieksekusi, fungsi Anda mengembalikan `Runtime.InvalidEntrypoint` kesalahan saat pemanggilan.

Berikut adalah contoh `bootstrap` file yang menggunakan versi bundel Node.js untuk menjalankan JavaScript runtime dalam file terpisah bernama `runtime.js`

Example bootstrap

```
#!/bin/sh
cd $LAMBDA_TASK_ROOT
./node-v11.1.0-linux-x64/bin/node runtime.js
```

Menerapkan streaming respons dalam runtime khusus

Untuk [fungsi streaming respons](#), titik akhir `response` dan `error` titik akhir memiliki perilaku yang sedikit dimodifikasi yang memungkinkan runtime mengalirkan sebagian respons ke klien dan mengembalikan muatan dalam potongan. Untuk informasi selengkapnya tentang perilaku tertentu, lihat berikut ini:

- `/runtime/invocation/AwsRequestId/response`— Menyebarkan `Content-Type` header dari runtime untuk dikirim ke klien. Lambda mengembalikan payload respons dalam potongan melalui HTTP/1.1 chunked transfer encoding. Stream respons dapat berukuran maksimum 20 MiB. Untuk melakukan streaming respons ke Lambda, runtime harus:
 - Atur header `Lambda-Runtime-Function-Response-Mode` HTTP ke `streaming`.
 - Atur header `Transfer-Encoding` ke `chunked`.
 - Tulis respons yang sesuai dengan spesifikasi pengkodean transfer chunked HTTP/1.1.
 - Tutup koneksi yang mendasarinya setelah berhasil menulis respons.
- `/runtime/invocation/AwsRequestId/error`— Runtime dapat menggunakan titik akhir ini untuk melaporkan kesalahan fungsi atau runtime ke Lambda, yang juga menerima header `Transfer-Encoding`. Titik akhir ini hanya dapat dipanggil sebelum runtime mulai mengirimkan respons pemanggilan.
- Laporkan kesalahan midstream menggunakan trailer kesalahan di `/runtime/invocation/AwsRequestId/response` — Untuk melaporkan kesalahan yang terjadi setelah runtime mulai menulis respons pemanggilan, runtime dapat secara opsional melampirkan header trailing HTTP bernama `Lambda-Runtime-Function-Error-Type` `Lambda-Runtime-Function-Error-Body`. Lambda memperlakukan ini sebagai respons yang berhasil dan meneruskan metadata kesalahan yang disediakan runtime kepada klien.

Note

Untuk melampirkan header tambahan, runtime harus menetapkan nilai `Trailer` header di awal permintaan HTTP. Ini adalah persyaratan dari spesifikasi pengkodean transfer chunked HTTP/1.1.

- `Lambda-Runtime-Function-Error-Type`— Jenis kesalahan yang ditemui runtime. Header ini terdiri dari nilai string. `<category.reason>` Lambda menerima string apa pun, tetapi kami merekomendasikan format. Misalnya, `Runtime.APIKeyNotFound`.

- `Lambda-Runtime-Function-Error-Body`— Informasi yang dikodekan Base64 tentang kesalahan.

Tutorial: Membangun runtime khusus

Dalam tutorial ini, Anda membuat fungsi Lambda dengan waktu pengoperasian kustom. Anda memulai dengan memasukkan waktu pengoperasian dalam paket deployment fungsi. Kemudian Anda memigrasikannya ke lapisan yang Anda kelola secara terpisah dari fungsi. Terakhir, Anda membagikan lapisan waktu pengoperasian kepada dunia dengan memperbarui kebijakan izin berbasis sumber daya.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```

Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (`\`) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa CLI perintah Bash yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh CLI perintah dalam panduan ini menggunakan pemformatan Linux. Perintah yang

menyertakan JSON dokumen inline harus diformat ulang jika Anda menggunakan Windows.
CLI

Anda memerlukan IAM peran untuk membuat fungsi Lambda. Peran memerlukan izin untuk mengirim CloudWatch log ke Log dan mengakses AWS layanan yang digunakan fungsi Anda. Jika Anda tidak memiliki peran untuk pengembangan fungsi, buatlah sekarang juga.

Untuk membuat peran eksekusi

1. Buka [halaman peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.
 - Entitas tepercaya – Lambda.
 - Izin — `AWSLambdaBasicExecutionRole`.
 - Nama peran – **lambda-role**.

`AWSLambdaBasicExecutionRoleKebijakan` ini memiliki izin yang diperlukan fungsi untuk menulis log ke CloudWatch Log.

Buat fungsi

Buat fungsi Lambda dengan waktu pengoperasian kustom. Contoh ini mencakup dua file: file runtime `bootstrap` dan function handler. Keduanya diterapkan di Bash.

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir runtime-tutorial
cd runtime-tutorial
```

2. Buat file baru bernama `bootstrap`. Ini adalah runtime khusus.

Example bootstrap

```
#!/bin/sh

set -euo pipefail
```

```
# Initialization - load function handler
source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"

# Processing
while true
do
  HEADERS="$(mktemp)"
  # Get an event. The HTTP request will block until one is received
  EVENT_DATA=$(curl -sS -LD "$HEADERS" "http://
${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

  # Extract request ID by scraping response headers received above
  REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
'[:space:]' | cut -d: -f2)

  # Run the handler function from the script
  RESPONSE=$(($echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

  # Send the response
  curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response" -d "$RESPONSE"
done
```

Waktu pengoperasian memuat skrip fungsi dari paket deployment. Runtime menggunakan dua variabel untuk menemukan skrip. `LAMBDA_TASK_ROOT` memberi tahu tempat paket diekstrak, dan `_HANDLER` mencakup nama skrip.

Setelah runtime memuat skrip fungsi, ia menggunakan runtime API untuk mengambil acara pemanggilan dari Lambda, meneruskan acara ke handler, dan memposting respons kembali ke Lambda. Untuk mendapatkan ID permintaan, runtime menyimpan header dari API respons ke file sementara, dan membaca `Lambda-Runtime-Aws-Request-Id` header dari file.

Note

Waktu pengoperasian memiliki tanggung jawab tambahan, termasuk penanganan kesalahan, dan memberikan informasi konteks kepada penangan. Untuk detailnya, lihat [Persyaratan](#).

3. Buat skrip untuk fungsi tersebut. Contoh skrip berikut mendefinisikan fungsi handler yang mengambil data peristiwa, log `stderr`, dan mengembalikannya.

Example function.sh

```
function handler () {
  EVENT_DATA=$1
  echo "$EVENT_DATA" 1>&2;
  RESPONSE="Echoing request: '$EVENT_DATA'"

  echo $RESPONSE
}
```

runtime-tutorialDirektori sekarang akan terlihat seperti ini:

```
runtime-tutorial
# bootstrap
# function.sh
```

4. Buat file dapat dijalankan dan tambahkan ke arsip file .zip. Ini adalah paket penyebaran.

```
chmod 755 function.sh bootstrap
zip function.zip function.sh bootstrap
```

5. Buat fungsi bernama bash-runtime. Untuk `--role`, masukkan peran ARN [eksekusi](#) Lambda Anda.

```
aws lambda create-function --function-name bash-runtime \
--zip-file fileb://function.zip --handler function.handler --runtime
provided.al2023 \
--role arn:aws:iam::123456789012:role/lambda-role
```

6. Memanggil fungsi.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'
response.txt --cli-binary-format raw-in-base64-out
```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat tanggapan seperti ini:

```
{
  "statusCode": 200,
  "executedVersion": "$LATEST"
}
```

7. Verifikasi responsnya.

```
cat response.txt
```

Anda akan melihat tanggapan seperti ini:

```
Echoing request: '{"text":"Hello"}'
```

Buat lapisan

Untuk memisahkan kode waktu pengoperasian dari kode fungsi, buat lapisan yang hanya berisi waktu pengoperasian. Lapisan memungkinkan Anda mengembangkan dependensi fungsi secara independen, dan dapat mengurangi penggunaan penyimpanan ketika Anda menggunakan lapisan yang sama dengan beberapa fungsi. Untuk informasi selengkapnya, lihat [Mengelola dependensi Lambda dengan lapisan](#).

1. Buat file.zip yang berisi bootstrap file.

```
zip runtime.zip bootstrap
```

2. Buat layer dengan [publish-layer-version](#) perintah.

```
aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://runtime.zip
```

Ini menciptakan versi pertama lapisan.

Perbarui fungsi

Untuk menggunakan layer runtime dalam fungsi, konfigurasi fungsi untuk menggunakan layer, dan hapus kode runtime dari fungsi.

1. Perbarui konfigurasi fungsi untuk menarik lapisan.

```
aws lambda update-function-configuration --function-name bash-runtime \  
--layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:1
```

Ini menambahkan waktu pengoperasian ke fungsi di direktori /opt. Untuk memastikan bahwa Lambda menggunakan runtime di layer, Anda harus menghapus bootstrap dari paket penerapan fungsi, seperti yang ditunjukkan dalam dua langkah berikutnya.

2. Buat file.zip yang berisi kode fungsi.

```
zip function-only.zip function.sh
```

3. Perbarui kode fungsi untuk hanya memasukkan skrip penanganan.

```
aws lambda update-function-code --function-name bash-runtime --zip-file fileb://  
function-only.zip
```

4. Panggil fungsi untuk mengonfirmasi bahwa ia berfungsi dengan layer runtime.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'  
response.txt --cli-binary-format raw-in-base64-out
```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat tanggapan seperti ini:

```
{  
  "StatusCode": 200,  
  "ExecutedVersion": "$LATEST"  
}
```

5. Verifikasi responsnya.

```
cat response.txt
```

Anda akan melihat tanggapan seperti ini:

```
Echoing request: '{"text":"Hello"}'
```

Perbarui waktu pengoperasian

1. Untuk mencatat log informasi tentang lingkungan eksekusi, perbarui skrip waktu pengoperasian ke variabel lingkungan output.

Example bootstrap

```
#!/bin/sh

set -euo pipefail

# Configure runtime to output environment variables
echo "## Environment variables:"
env

# Load function handler
source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"

# Processing
while true
do
    HEADERS="$(mktemp)"
    # Get an event. The HTTP request will block until one is received
    EVENT_DATA=$(curl -s -LD "$HEADERS" "http://
${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

    # Extract request ID by scraping response headers received above
    REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
':space:]' | cut -d: -f2)

    # Run the handler function from the script
    RESPONSE=$(echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

    # Send the response
    curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response" -d "$RESPONSE"
done
```

2. Buat file.zip yang berisi versi baru bootstrap file.

```
zip runtime.zip bootstrap
```

3. Buat versi baru dari bash-runtime layer.

```
aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://runtime.zip
```

4. Konfigurasi fungsi untuk menggunakan versi baru lapisan.

```
aws lambda update-function-configuration --function-name bash-runtime \
--layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:2
```

Bagikan lapisan

[Untuk berbagi layer dengan yang lain Akun AWS, tambahkan pernyataan izin lintas akun ke kebijakan berbasis sumber daya lapisan.](#) Jalankan [add-layer-version-permission](#) perintah dan tentukan ID akun sebagai `principal`. Dalam setiap pernyataan, Anda dapat memberikan izin ke satu akun, semua akun, atau organisasi di [AWS Organizations](#).

Contoh berikut memberikan akun 111122223333 akses ke versi 2 lapisan. bash-runtime

```
aws lambda add-layer-version-permission \
--layer-name bash-runtime \
--version-number 2 \
--statement-id xaccount \
--action lambda:GetLayerVersion \
--principal 111122223333 \
--output text
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{"Sid": "xaccount", "Effect": "Allow", "Principal":
{"AWS": "arn:aws:iam::111122223333:root"}, "Action": "lambda:GetLayerVersion", "Resource": "arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```

Izin hanya berlaku untuk satu versi lapisan. Ulangi proses ini tiap kali Anda membuat versi lapisan baru.

Bersihkan

Hapus setiap versi lapisan.

```
aws lambda delete-layer-version --layer-name bash-runtime --version-number 1  
aws lambda delete-layer-version --layer-name bash-runtime --version-number 2
```

Karena fungsi memiliki referensi ke lapisan versi 2, ia masih ada di Lambda. Fungsi terus bekerja, tetapi fungsi tidak dapat lagi dikonfigurasi untuk menggunakan versi yang dihapus. Jika Anda memodifikasi daftar lapisan pada fungsi, Anda harus menentukan versi baru atau menghilangkan lapisan yang dihapus.

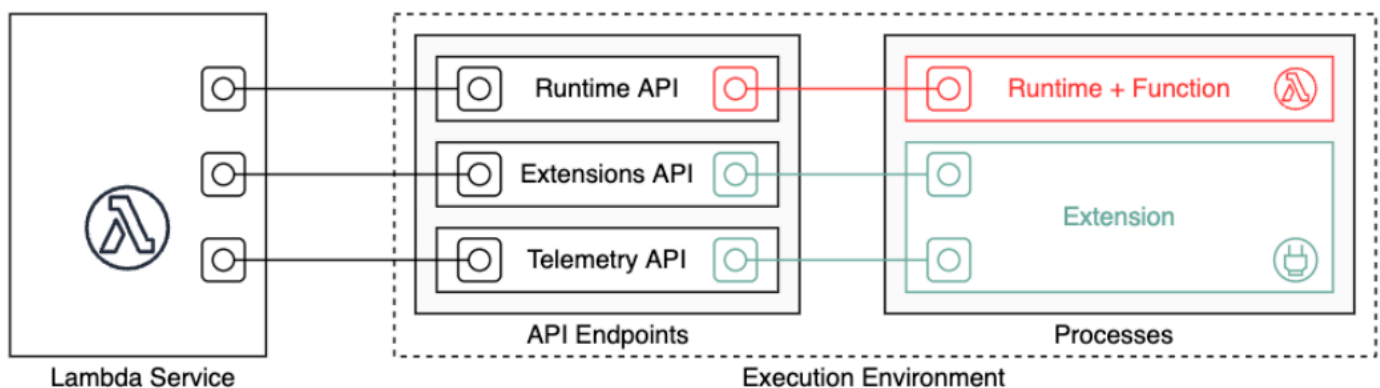
Hapus fungsi dengan perintah [hapus-fungsi](#).

```
aws lambda delete-function --function-name bash-runtime
```

Memahami siklus hidup lingkungan eksekusi Lambda

Lambda melakukan invokasi fungsi dalam lingkungan eksekusi, yang menyediakan lingkungan waktu pengoperasian yang aman dan terisolasi. Lingkungan eksekusi mengelola sumber daya yang diperlukan untuk menjalankan fungsi Anda. Lingkungan eksekusi juga menyediakan dukungan siklus hidup untuk waktu pengoperasian fungsi dan [ekstensi eksternal](#) terkait fungsi Anda.

[Runtime fungsi berkomunikasi dengan Lambda menggunakan Runtime. API Ekstensi berkomunikasi dengan Lambda menggunakan Ekstensi. API Ekstensi juga dapat menerima pesan log dan telemetry lain dari fungsi dengan menggunakan Telemetry. API](#)



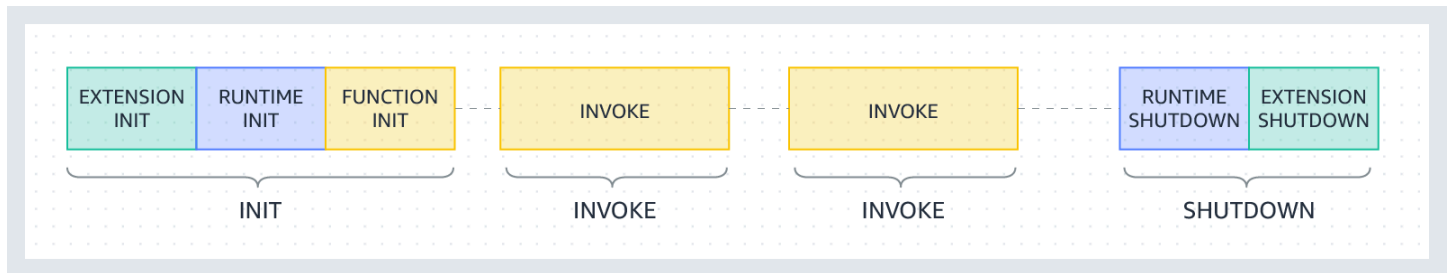
Saat membuat fungsi Lambda, Anda menentukan informasi konfigurasi, seperti jumlah memori yang tersedia dan waktu eksekusi maksimal yang diizinkan untuk fungsi Anda. Lambda menggunakan informasi ini untuk menyiapkan lingkungan eksekusi.

Waktu pengoperasian fungsi dan setiap ekstensi eksternal adalah proses yang berjalan di dalam lingkungan eksekusi. Izin, sumber daya, kredensial, dan variabel lingkungan dibagikan di antara fungsi dan ekstensi.

Topik

- [Siklus hidup lingkungan eksekusi Lambda](#)
- [Menerapkan kewarganegaraan dalam fungsi](#)

Siklus hidup lingkungan eksekusi Lambda



Setiap fase dimulai dengan kejadian yang dikirimkan Lambda ke waktu pengoperasian dan ke semua ekstensi terdaftar. Runtime dan setiap ekstensi menunjukkan penyelesaian dengan mengirimkan Next API permintaan. Lambda membekukan lingkungan eksekusi saat waktu pengoperasian dan setiap ekstensi telah selesai dan tidak ada kejadian yang tertunda.

Topik

- [Fase inisialisasi](#)
- [Kegagalan selama fase Init](#)
- [Fase pemulihan \(hanya Lambda SnapStart \)](#)
- [Fase invokasi](#)
- [Kegagalan selama fase pemanggilan](#)
- [Fase pematian](#)

Fase inisialisasi

Di fase Init, Lambda melakukan tiga tugas:

- Memulai semua ekstensi (`Extension init`)
- Melakukan bootstrap waktu pengoperasian (`Runtime init`)
- Menjalankan kode statis fungsi (`Function init`)
- Jalankan [kait beforeCheckpoint runtime apa pun \(hanya Lambda\) SnapStart](#)

InitFase berakhir ketika runtime dan semua ekstensi memberi sinyal bahwa mereka siap dengan mengirim Next API permintaan. Fase Init dibatasi 10 detik. Jika ketiga tugas tidak selesai dalam 10 detik, Lambda mencoba kembali Init fase pada saat pemanggilan fungsi pertama dengan batas waktu fungsi yang dikonfigurasi.

Ketika [Lambda SnapStart](#) diaktifkan, `Init` fase terjadi ketika Anda mempublikasikan versi fungsi. Lambda menyimpan snapshot memori dan status disk dari lingkungan eksekusi yang diinisialisasi, mempertahankan snapshot terenkripsi, dan menyimpannya dalam cache untuk akses latensi rendah. Jika Anda memiliki [hook beforeCheckpoint runtime](#), maka kode berjalan di akhir `Init` fase.

Note

Batas waktu 10 detik tidak berlaku untuk fungsi yang menggunakan konkurensi yang disediakan atau SnapStart. Untuk konkurensi dan SnapStart fungsi yang disediakan, kode inisialisasi Anda dapat berjalan hingga 15 menit. Batas waktu adalah 130 detik atau batas waktu fungsi yang dikonfigurasi (maksimum 900 detik), mana yang lebih tinggi.

Saat Anda menggunakan [konkurensi yang disediakan](#), Lambda menginisialisasi lingkungan eksekusi saat Anda mengonfigurasi pengaturan PC untuk suatu fungsi. Lambda juga memastikan bahwa lingkungan eksekusi yang diinisialisasi selalu tersedia sebelum pemanggilan. Anda mungkin melihat kesenjangan antara fase pemanggilan dan inisialisasi fungsi Anda. Bergantung pada runtime dan konfigurasi memori fungsi Anda, Anda juga dapat melihat latensi variabel pada pemanggilan pertama pada lingkungan eksekusi yang diinisialisasi.

Untuk fungsi yang menggunakan konkurensi sesuai permintaan, Lambda terkadang dapat menginisialisasi lingkungan eksekusi sebelum permintaan pemanggilan. Ketika ini terjadi, Anda juga dapat mengamati kesenjangan waktu antara fase inisialisasi dan pemanggilan fungsi Anda. Kami menyarankan Anda untuk tidak mengambil ketergantungan pada perilaku ini.

Kegagalan selama fase Init

Jika fungsi macet atau habis waktu selama `Init` fase, Lambda memancarkan informasi kesalahan di log. `INIT_REPORT`

Example — `INIT _ REPORT` log untuk batas waktu

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: timeout
```

Example — `INIT _ REPORT` log untuk kegagalan ekstensi

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: error Error Type:  
Extension.Crash
```

Jika Init fase berhasil, Lambda tidak memancarkan INIT_REPORT log [SnapStart](#)— kecuali diaktifkan. SnapStart fungsi selalu memancarkan INIT_REPORT. Untuk informasi selengkapnya, lihat [Pemantauan untuk Lambda SnapStart](#).

Fase pemulihan (hanya Lambda SnapStart)

Saat Anda pertama kali memanggil [SnapStart](#) fungsi dan saat fungsi meningkat, Lambda melanjutkan lingkungan eksekusi baru dari snapshot yang bertahan alih-alih menginisialisasi fungsi dari awal. Jika Anda memiliki [hook afterRestore\(\) runtime](#), kode berjalan di akhir Restore fase. Anda dikenakan biaya untuk durasi kait afterRestore() runtime. Runtime (JVM) harus dimuat dan kait afterRestore() runtime harus selesai dalam batas waktu tunggu (10 detik). Jika tidak, Anda akan mendapatkan SnapStartTimeoutException. Ketika Restore fase selesai, Lambda memanggil fungsi handler (the). [Fase invokasi](#)

Kegagalan selama fase Restore

Jika Restore fase gagal, Lambda memancarkan informasi kesalahan di log. RESTORE_REPORT

Example — RESTORE _ REPORT log untuk batas waktu

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: timeout
```

Example — RESTORE _ REPORT log untuk kegagalan kait runtime

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: error Error Type: Runtime.ExitError
```

Untuk informasi lebih lanjut tentang RESTORE_REPORT log, lihat [Pemantauan untuk Lambda SnapStart](#).

Fase invokasi

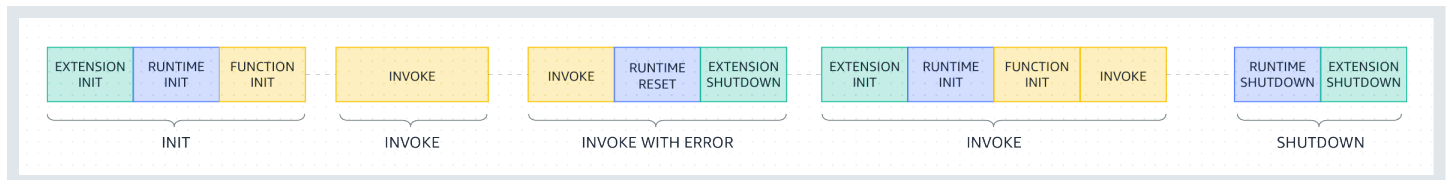
Ketika fungsi Lambda dipanggil sebagai respons terhadap permintaan NextAPI, Lambda mengirimkan Invoke acara ke runtime dan ke setiap ekstensi.

Pengaturan waktu habis fungsi membatasi durasi seluruh fase Invoke. Misalnya, jika Anda mengatur waktu fungsi habis sebagai 360 detik, fungsi dan semua ekstensi harus selesai dalam 360 detik. Perhatikan bahwa tidak ada fase pasca-invokasi yang independen. Durasi adalah jumlah semua waktu invokasi (waktu pengoperasian + ekstensi) dan tidak dihitung hingga fungsi dan semua ekstensi selesai dijalankan.

Fase pemanggilan berakhir setelah runtime dan semua ekstensi memberi sinyal bahwa mereka dilakukan dengan mengirimkan permintaan. Next API

Kegagalan selama fase pemanggilan

Jika fungsi Lambda mengalami crash atau waktu habis selama fase Invoke, Lambda mengatur ulang lingkungan eksekusi. Diagram berikut menggambarkan perilaku lingkungan eksekusi Lambda ketika ada kegagalan pemanggilan:



Pada diagram sebelumnya:

- Fase pertama adalah INIT fase, yang berjalan tanpa kesalahan.
- Fase kedua adalah INVOKE fase, yang berjalan tanpa kesalahan.
- Pada titik tertentu, misalkan fungsi Anda mengalami kegagalan pemanggilan (seperti batas waktu fungsi atau kesalahan runtime). Fase ketiga, berlabel INVOKE WITH ERROR, menggambarkan skenario ini. Ketika ini terjadi, layanan Lambda melakukan reset. Reset berperilaku seperti kejadian Shutdown. Pertama, Lambda mematikan runtime, lalu mengirimkan Shutdown acara ke setiap ekstensi eksternal terdaftar. Kejadian ini mencakup alasan untuk pematian. Jika lingkungan ini digunakan untuk pemanggilan baru, Lambda menginisialisasi ulang ekstensi dan runtime bersama dengan pemanggilan berikutnya.

Perhatikan bahwa reset Lambda tidak menghapus konten /tmp direktori sebelum fase init berikutnya. Perilaku ini konsisten dengan fase shutdown reguler.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS
Jika konfigurasi log sistem fungsi Anda disetel ke teks biasa, perubahan ini memengaruhi pesan log yang ditangkap di CloudWatch Log saat fungsi Anda mengalami kegagalan pemanggilan. Contoh berikut menunjukkan output log dalam format lama dan baru.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Example CloudWatch Keluaran log log (runtime atau ekstensi crash) - gaya lama

```
START RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Version: $LATEST
RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Error: Runtime exited without providing a reason
Runtime.ExitError
END RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1
REPORT RequestId: c3252230-c73d-49f6-8844-968c01d1e2e1 Duration: 933.59 ms Billed Duration: 934 ms Memory Size: 128 MB Max Memory Used: 9 MB
```

Example CloudWatch Keluaran log log (batas waktu fungsi) - gaya lama

```
START RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21 Version: $LATEST
2024-03-04T17:22:38.033Z b70435cc-261c-4438-b9b6-efe4c8f04b21 Task timed out after 3.00 seconds
END RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21
REPORT RequestId: b70435cc-261c-4438-b9b6-efe4c8f04b21 Duration: 3004.92 ms Billed Duration: 3000 ms Memory Size: 128 MB Max Memory Used: 33 MB Init Duration: 111.23 ms
```

Format baru untuk CloudWatch log mencakup status bidang tambahan di REPORT baris. Dalam kasus runtime atau ekstensi crash, REPORT baris juga menyertakan bidang `ErrorType`.

Example CloudWatch Keluaran log log (runtime atau ekstensi crash) - gaya baru

```
START RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd Version: $LATEST
END RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd
REPORT RequestId: 5b866fb1-7154-4af6-8078-6ef6ca4c2ddd Duration: 133.61 ms Billed Duration: 133 ms Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 80.00 ms Status: error Error Type: Runtime.ExitError
```

Example CloudWatch Keluaran log log (batas waktu fungsi) - gaya baru

```
START RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda Version: $LATEST
END RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda
REPORT RequestId: 527cb862-4f5e-49a9-9ae4-a7edc90f0fda Duration: 3016.78 ms Billed
Duration: 3016 ms Memory Size: 128 MB Max Memory Used: 31 MB Init Duration: 84.00
ms Status: timeout
```

- Fase keempat mewakili INVOKE fase segera setelah kegagalan pemanggilan. Di sini, Lambda menginisialisasi lingkungan lagi dengan menjalankan kembali fase. INIT ini disebut init yang ditekan. Ketika input yang ditekan terjadi, Lambda tidak secara eksplisit melaporkan fase tambahan di Log. INIT CloudWatch Sebagai gantinya, Anda mungkin memperhatikan bahwa durasi di REPORT baris mencakup INITdurasi INVOKEtambahan+durasi. Misalnya, Anda melihat log berikut di CloudWatch:

```
2022-12-20T01:00:00.000-08:00 START RequestId: XXX Version: $LATEST
2022-12-20T01:00:02.500-08:00 END RequestId: XXX
2022-12-20T01:00:02.500-08:00 REPORT RequestId: XXX Duration: 3022.91 ms
Billed Duration: 3000 ms Memory Size: 512 MB Max Memory Used: 157 MB
```

Dalam contoh ini, perbedaan antara stempel waktu REPORT dan START stempel waktu adalah 2,5 detik. Ini tidak cocok dengan durasi yang dilaporkan 3022,91 milliseconds, karena tidak memperhitungkan ekstra INIT (init yang ditekan) yang dilakukan Lambda. Dalam contoh ini, Anda dapat menyimpulkan bahwa INVOKE fase sebenarnya membutuhkan waktu 2,5 detik.

Untuk wawasan lebih lanjut tentang perilaku ini, Anda dapat menggunakan [Mengakses data telemetri real-time untuk ekstensi menggunakan Telemetri API](#). Telemetri API memancarkan INIT_START, INIT_RUNTIME_DONE, dan INIT_REPORT peristiwa dengan input phase=invoke setiap kali ditekan terjadi di antara fase pemanggilan.

- Fase kelima mewakili SHUTDOWN fase, yang berjalan tanpa kesalahan.

Fase pematian

Ketika Lambda akan mematikan runtime, ia mengirimkan Shutdown acara ke setiap ekstensi eksternal yang terdaftar. Ekstensi dapat menggunakan waktu ini untuk tugas pembersihan akhir. Shutdown Acara ini merupakan respons Next API atas permintaan.

Durasi: Keseluruhan fase Shutdown dibatasi hingga 2 detik. Jika waktu pengoperasian atau ekstensi tidak merespons, Lambda menghentikannya melalui sinyal (SIGKILL).

Setelah fungsi dan semua ekstensi selesai, Lambda mempertahankan lingkungan eksekusi selama beberapa waktu untuk mengantisipasi invokasi fungsi lain. Namun, Lambda menghentikan lingkungan eksekusi setiap beberapa jam untuk memungkinkan pembaruan dan pemeliharaan runtime — bahkan untuk fungsi yang dipanggil terus menerus. Anda tidak boleh berasumsi bahwa lingkungan eksekusi akan bertahan tanpa batas waktu. Untuk informasi selengkapnya, lihat [Menerapkan kewarganegaraan dalam fungsi](#).

Saat fungsinya diinvokasi lagi, Lambda mencairkan lingkungan untuk digunakan kembali. Menggunakan kembali lingkungan eksekusi memiliki implikasi berikut:

- Objek yang dinyatakan di luar metode penanganan fungsi tetap diinisialisasi, memberikan pengoptimalan tambahan ketika fungsi diinvokasi lagi. Misalnya, jika fungsi Lambda Anda menetapkan koneksi database, alih-alih menetapkan kembali koneksi, koneksi asli digunakan dalam invokasi berikutnya. Kami menyarankan Anda menambahkan logika dalam kode untuk memeriksa apakah ada koneksi sebelum membuat yang baru.
- Setiap lingkungan eksekusi menyediakan antara 512 MB dan 10.240 MB, dalam peningkatan 1-MB, ruang disk di direktori. /tmp Isi direktori tetap ada ketika lingkungan eksekusi dibekukan, menyediakan cache sementara yang dapat digunakan untuk beberapa invokasi. Anda dapat menambahkan kode tambahan untuk memeriksa apakah cache memiliki data yang Anda simpan. Untuk informasi lebih lanjut tentang batas ukuran deployment, lihat [Kuota Lambda](#).
- Proses latar belakang atau panggilan balik yang diinisialisasi fungsi Lambda Anda dan tidak selesai ketika fungsi berakhir akan dilanjutkan jika Lambda menggunakan kembali lingkungan eksekusi. Pastikan setiap proses latar belakang atau panggilan balik dalam kode Anda selesai sebelum kode tersebut ditutup.

Menerapkan kewarganegaraan dalam fungsi

Saat menulis kode fungsi Lambda Anda, perlakukan lingkungan eksekusi sebagai stateless, dengan asumsi bahwa itu hanya ada untuk satu pemanggilan. Lambda menghentikan lingkungan eksekusi setiap beberapa jam untuk memungkinkan pembaruan dan pemeliharaan runtime — bahkan untuk fungsi yang dipanggil terus menerus. Inisialisasi status apa pun yang diperlukan (misalnya, mengambil keranjang belanja dari tabel Amazon DynamoDB) saat fungsi Anda dimulai. Sebelum keluar, lakukan perubahan data permanen ke toko tahan lama seperti Amazon Simple Storage Service (Amazon S3), DynamoDB, atau Amazon Simple Queue Service (Amazon SQS). Hindari

mengandalkan struktur data yang ada, file sementara, atau status yang mencakup pemanggilan, seperti penghitung atau agregat. Ini memastikan bahwa fungsi Anda menangani setiap pemanggilan secara independen.

Mengkonfigurasi fungsi AWS Lambda

Pelajari cara mengonfigurasi kemampuan dan opsi inti untuk fungsi Lambda Anda menggunakan API Lambda atau konsol.

[Memori](#)

Pelajari bagaimana dan kapan harus meningkatkan memori fungsi.

[Penyimpanan fana](#)

Pelajari bagaimana dan kapan harus meningkatkan kapasitas penyimpanan sementara fungsi Anda.

[Batas waktu](#)

Pelajari bagaimana dan kapan harus meningkatkan nilai batas waktu fungsi Anda.

[Variabel lingkungan](#)

Anda dapat membuat kode fungsi Anda portabel dan menyimpan rahasia dari kode Anda dengan menyimpannya dalam konfigurasi fungsi Anda dengan menggunakan variabel lingkungan.

[Jaringan keluar](#)

Anda dapat menggunakan fungsi Lambda Anda dengan AWS sumber daya di Amazon. VPC Menghubungkan fungsi Anda ke sebuah VPC memungkinkan Anda mengakses sumber daya dalam subnet pribadi seperti database relasional dan cache.

[Jaringan masuk](#)

Anda dapat menggunakan VPC titik akhir antarmuka untuk menjalankan fungsi Lambda Anda tanpa melintasi internet publik.

[Sistem berkas](#)

Anda dapat menggunakan fungsi Lambda untuk memasang Amazon EFS ke direktori lokal. Sistem file memungkinkan kode fungsi Anda untuk mengakses dan memodifikasi sumber daya bersama dengan aman dan pada konkurensi tinggi.

[Alias](#)

Anda dapat mengonfigurasi klien Anda untuk memanggil versi fungsi Lambda tertentu dengan menggunakan alias, alih-alih memperbarui klien.

Versi

Dengan menerbitkan versi fungsi Anda, Anda dapat menyimpan kode dan konfigurasi Anda sebagai sumber daya terpisah yang tidak dapat diubah.

Tanda

Gunakan tag untuk mengaktifkan kontrol akses berbasis atribut (ABAC), untuk mengatur fungsi Lambda Anda, dan untuk memfilter dan menghasilkan laporan tentang fungsi Anda menggunakan AWS Cost Explorer atau layanan Billing and Cost AWS Management.

Streaming respons

Anda dapat mengonfigurasi fungsi Lambda Anda URLs untuk mengalirkan muatan respons kembali ke klien. Streaming respons dapat menguntungkan aplikasi sensitif latensi dengan meningkatkan waktu ke kinerja byte (TTFB) pertama. Ini karena Anda dapat mengirim sebagian tanggapan kembali ke klien saat tersedia. Selain itu, Anda dapat menggunakan streaming respons untuk membangun fungsi yang mengembalikan muatan yang lebih besar.

Menyebarkan fungsi Lambda sebagai arsip file.zip

Saat Anda membuat fungsi Lambda, Anda mengemas kode fungsi Anda ke dalam paket penerapan. Lambda mendukung dua tipe paket deployment: gambar kontainer dan arsip file .zip. Alur kerja untuk membuat fungsi tergantung pada jenis paket penyebaran. Untuk mengonfigurasi fungsi yang didefinisikan sebagai gambar kontainer, lihat [the section called “Gambar kontainer”](#).

Anda dapat menggunakan konsol Lambda dan Lambda API untuk membuat fungsi yang ditentukan dengan arsip file.zip. Anda juga dapat mengunggah file.zip yang diperbarui untuk mengubah kode fungsi.

Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Topik

- [Membuat fungsi](#)
- [Menggunakan editor kode konsol](#)
- [Memperbarui kode fungsi](#)
- [Mengubah runtime](#)
- [Mengubah arsitektur](#)
- [Menggunakan Lambda API](#)
- [AWS CloudFormation](#)

Membuat fungsi

Saat Anda membuat fungsi yang ditentukan dengan arsip file.zip, Anda memilih templat kode, versi bahasa, dan peran eksekusi untuk fungsi tersebut. Anda menambahkan kode fungsi Anda setelah Lambda membuat fungsi.

Untuk membuat fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih Buat fungsi.
3. Pilih Penulis dari awal atau Gunakan cetak biru untuk membuat fungsi Anda.
4. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk Nama fungsi, masukkan nama fungsi. Nama fungsi dibatasi hingga 64 karakter panjangnya.
 - b. Untuk Runtime, pilih versi bahasa yang akan digunakan untuk fungsi Anda.
 - c. (Opsional) Untuk Arsitektur, pilih arsitektur set instruksi yang akan digunakan untuk fungsi Anda. Arsitektur default adalah x86_64. Ketika Anda membangun paket deployment untuk fungsi Anda, pastikan bahwa itu kompatibel dengan [arsitektur set instruksi](#) ini.
5. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan peran yang ada.
6. (Opsional) Perluas pengaturan lanjutan. Anda dapat memilih konfigurasi penandatanganan Kode untuk fungsi tersebut. Anda juga dapat mengonfigurasi (AmazonVPC) agar fungsi dapat diakses.
7. Pilih Buat fungsi.

Lambda menciptakan fungsi baru. Anda sekarang dapat menggunakan konsol untuk menambahkan kode fungsi dan mengkonfigurasi parameter dan fitur fungsi lainnya. Untuk petunjuk penerapan kode, lihat halaman handler untuk runtime yang digunakan fungsi Anda.

Node.js

[Deploy fungsi Lambda Node.js dengan arsip file .zip](#)

Python

[Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#)

Ruby

[Deploy fungsi Lambda Ruby dengan arsip file .zip](#)

Java

[Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file](#)

Go

[Deploy fungsi Go Lambda dengan arsip file .zip](#)

C#

[Bangun dan terapkan fungsi C# Lambda dengan arsip file.zip](#)

PowerShell

[Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip](#)

Menggunakan editor kode konsol

Konsol membuat fungsi Lambda dengan satu file sumber. Untuk bahasa scripting, Anda dapat mengedit file ini dan menambahkan lebih banyak file menggunakan editor kode bawaan. Untuk menyimpan perubahan Anda, pilih Simpan. Selanjutnya, untuk menjalankan kode, pilih Uji.

Saat Anda menyimpan kode fungsi, konsol Lambda membuat paket penyebaran arsip file.zip. Saat Anda mengembangkan kode fungsi di luar konsol (menggunakan IDE), Anda perlu [membuat paket penerapan](#) untuk mengunggah kode Anda ke fungsi Lambda.

Memperbarui kode fungsi

Untuk bahasa scripting (Node.js, Python, dan Ruby), Anda dapat mengedit kode fungsi Anda di editor kode tertanam. Jika kode lebih besar dari 3MB, atau jika Anda perlu menambahkan pustaka, atau untuk bahasa yang tidak didukung editor (Java, Go, C #), Anda harus mengunggah kode fungsi Anda sebagai arsip.zip. Jika arsip file.zip lebih kecil dari 50 MB, Anda dapat mengunggah arsip file.zip dari mesin lokal Anda. Jika file lebih besar dari 50 MB, unggah file ke fungsi dari bucket Amazon S3.

Untuk mengunggah kode fungsi sebagai arsip.zip

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang akan diperbarui dan pilih tab Kode.
3. Di bagian Sumber kode, pilih Unggah dari.
4. Pilih file.zip, lalu pilih Unggah.
 - Di pemilih file, pilih versi gambar baru, pilih Buka, lalu pilih Simpan.
5. (Alternatif untuk langkah 4) Pilih lokasi Amazon S3.
 - Di kotak teks, masukkan tautan S3 URL dari arsip file.zip, lalu pilih Simpan.

Mengubah runtime

Jika Anda memperbarui konfigurasi fungsi untuk menggunakan runtime baru, Anda mungkin perlu memperbarui kode fungsi agar kompatibel dengan runtime baru. Jika Anda memperbarui konfigurasi fungsi untuk menggunakan runtime yang berbeda, Anda harus memberikan kode fungsi baru yang kompatibel dengan runtime dan arsitektur. Untuk petunjuk tentang cara membuat paket deployment untuk kode fungsi, lihat halaman handler untuk runtime yang digunakan fungsi.

Node.js 20, Python 3.12, Java 21, .NET 8, Ruby 3.3, dan gambar dasar yang lebih baru didasarkan pada gambar kontainer minimal Amazon Linux 2023. Gambar dasar sebelumnya menggunakan Amazon Linux 2. AL2023 memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti `glibc`. Untuk informasi selengkapnya, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di AWS Compute Blog.

Untuk mengubah runtime

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang akan diperbarui dan pilih tab Kode.
3. Gulir ke bawah ke bagian pengaturan Runtime, yang berada di bawah editor kode.
4. Pilih Edit.
 - a. Untuk Runtime, pilih pengenalan runtime.
 - b. Untuk Handler, tentukan nama file dan handler untuk fungsi Anda.
 - c. Untuk Arsitektur, pilih arsitektur set instruksi yang akan digunakan untuk fungsi Anda.
5. Pilih Simpan.

Mengubah arsitektur

Sebelum Anda dapat mengubah arsitektur set instruksi, Anda perlu memastikan bahwa kode fungsi Anda kompatibel dengan arsitektur target.

Jika Anda menggunakan Node.js, Python, atau Ruby dan Anda mengedit kode fungsi Anda di editor tertanam, kode yang ada dapat berjalan tanpa modifikasi.

Namun, jika Anda memberikan kode fungsi Anda menggunakan paket penyebaran arsip file.zip, Anda harus menyiapkan arsip file.zip baru yang dikompilasi dan dibangun dengan benar untuk

runtime target dan arsitektur set instruksi. Untuk instruksi, lihat halaman handler untuk runtime fungsi Anda.

Untuk mengubah arsitektur set instruksi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang akan diperbarui dan pilih tab Kode.
3. Di bawah Pengaturan waktu proses, pilih Edit.
4. Untuk Arsitektur, pilih arsitektur set instruksi yang akan digunakan untuk fungsi Anda.
5. Pilih Simpan.

Menggunakan Lambda API

Untuk membuat dan mengonfigurasi fungsi yang menggunakan arsip file.zip, gunakan API operasi berikut:

- [CreateFunction](#)
- [UpdateFunctionCode](#)
- [UpdateFunctionConfiguration](#)

AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk membuat fungsi Lambda yang menggunakan arsip file.zip. Dalam AWS CloudFormation template Anda, `AWS::Lambda::Function` sumber daya menentukan fungsi Lambda. Untuk deskripsi properti dalam `AWS::Lambda::Function` sumber daya, lihat [AWS::Lambda::Function](#) di Panduan Pengguna AWS CloudFormation

Dalam `AWS::Lambda::Function` sumber daya, atur properti berikut untuk membuat fungsi yang didefinisikan sebagai arsip file.zip:

- `AWS::Lambda::Function`
 - `PackageType` — Setel ke `Zip`.
 - `Kode` - Masukkan nama bucket Amazon S3 dan nama file.zip di dan bidang `S3Bucket` `S3Key` Untuk Node.js atau Python, Anda dapat memberikan kode sumber inline dari fungsi Lambda Anda.
 - `Runtime` - Tetapkan nilai runtime.

- **Arsitektur** - Tetapkan nilai arsitektur `arm64` untuk menggunakan prosesor AWS Graviton2. Secara default, nilai arsitektur adalah `x86_64`.

Buat fungsi Lambda menggunakan gambar kontainer

Kode AWS Lambda fungsi Anda terdiri dari skrip atau program yang dikompilasi dan dependensinya. Gunakan paket deployment untuk men-deploy fungsi kode Anda ke Lambda. Lambda mendukung dua tipe paket deployment: gambar kontainer dan arsip file .zip.

Ada tiga cara untuk membangun image kontainer untuk fungsi Lambda:

- [Menggunakan gambar AWS dasar untuk Lambda](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [kustom](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime](#) untuk bahasa Anda dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime](#) untuk bahasa Anda dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi kontainer Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Untuk membuat fungsi Lambda dari gambar kontainer, buat gambar Anda secara lokal dan unggah ke repositori Amazon Elastic Container Registry (Amazon ECR). Kemudian, tentukan repositori

URI saat Anda membuat fungsi. ECRRepository Amazon harus sama Wilayah AWS dengan fungsi Lambda. Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

Note

Lambda tidak mendukung ECR FIPS titik akhir Amazon untuk gambar kontainer. Jika repository Anda URI termasuk `ecr-fips`, Anda menggunakan titik akhir. FIPS Contoh: `111122223333.dkr.ecr-fips.us-east-1.amazonaws.com`.

Halaman ini menjelaskan jenis gambar dasar dan persyaratan untuk membuat gambar kontainer yang kompatibel dengan Lambda.

Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Topik

- [Persyaratan](#)
- [Menggunakan gambar AWS dasar untuk Lambda](#)
- [Menggunakan gambar AWS dasar khusus OS](#)
- [Menggunakan gambar AWS non-dasar](#)
- [Klien antarmuka runtime](#)
- [ECRIzin Amazon](#)
- [Siklus hidup fungsi](#)

Persyaratan

Instal [AWS Command Line Interface \(AWS CLI\) versi 2](#) dan [Docker CLI](#). Selain itu, perhatikan persyaratan berikut:

- Gambar kontainer harus mengimplementasikan file [Menggunakan runtime Lambda untuk runtime khusus API](#). [Klien antarmuka runtime AWS sumber terbuka mengimplementasikan file](#). API Anda dapat menambahkan klien antarmuka runtime untuk gambar dasar pilihan Anda untuk membuatnya kompatibel dengan Lambda.
- Gambar kontainer harus dapat berjalan pada sistem file hanya baca. Kode fungsi Anda dapat mengakses /tmp direktori yang dapat ditulis dengan penyimpanan antara 512 MB dan 10.240 MB, dengan penambahan 1-MB, penyimpanan.
- Pengguna Lambda default harus dapat membaca semua file yang diperlukan untuk menjalankan kode fungsi Anda. Lambda mengikuti praktik terbaik keamanan dengan mendefinisikan pengguna Linux default dengan izin yang paling tidak istimewa. Ini berarti Anda tidak perlu menentukan a [USER](#) di Dockerfile Anda. Verifikasi bahwa kode aplikasi Anda tidak bergantung pada file yang dibatasi pengguna Linux lain untuk berjalan.
- Lambda hanya mendukung gambar kontainer berbasis Linux.
- Lambda menyediakan gambar dasar multi-arsitektur. Namun, gambar yang Anda buat untuk fungsi Anda harus menargetkan hanya satu arsitektur. Lambda tidak mendukung fungsi yang menggunakan gambar kontainer multi-arsitektur.

Menggunakan gambar AWS dasar untuk Lambda

Anda dapat menggunakan salah satu [gambar AWS dasar](#) untuk Lambda untuk membangun gambar kontainer untuk kode fungsi Anda. Gambar dasar yang dimuat sebelumnya dengan runtime bahasa dan komponen lain yang diperlukan untuk menjalankan gambar kontainer pada Lambda. Anda menambahkan kode fungsi dan dependensi ke gambar dasar, lalu mengemasnya sebagai gambar kontainer.

AWS secara berkala memberikan pembaruan pada gambar AWS dasar untuk Lambda. [Jika Dockerfile Anda menyertakan nama gambar di FROM properti, klien Docker Anda akan menarik versi terbaru gambar dari repositori Amazon. ECR](#) Untuk menggunakan gambar dasar diperbarui, Anda harus membangun kembali gambar kontainer Anda dan [memperbarui kode fungsi](#).

Node.js 20, Python 3.12, Java 21, .NET 8, Ruby 3.3, dan gambar dasar yang lebih baru didasarkan pada gambar [kontainer minimal Amazon Linux 2023](#). Gambar dasar sebelumnya menggunakan Amazon Linux 2. AL2023 memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti. `glibc`

AL2 Gambar berbasis 023 menggunakan `microdnf` (symlinked `asdnf`) sebagai manajer paket, `bukanyum`, yang merupakan pengelola paket default di Amazon Linux 2. `microdnf` adalah

implementasi mandiri dari `dnf` Untuk daftar paket yang disertakan dalam gambar AL2 berbasis 023, lihat kolom Kontainer Minimal di Membandingkan paket yang diinstal pada Gambar Kontainer [Amazon Linux 2023](#). Untuk informasi selengkapnya tentang perbedaan antara AL2 023 dan Amazon Linux 2, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di Blog Komputasi AWS .

Note

Untuk menjalankan gambar AL2 berbasis 023 secara lokal, termasuk with AWS Serverless Application Model (AWS SAM), Anda harus menggunakan Docker versi 20.10.10 atau yang lebih baru.

Untuk membuat gambar kontainer menggunakan gambar AWS dasar, pilih instruksi untuk bahasa pilihan Anda:

- [Node.js](#)
- [TypeScript](#)(menggunakan gambar dasar Node.js)
- [Python](#)
- [Java](#)
- [Go](#)
- [.NET](#)
- [Ruby](#)

Menggunakan gambar AWS dasar khusus OS

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [kustom](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime](#) untuk bahasa Anda dalam gambar.

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|--------|-------------------|-------------------|---|-------------|
| al2023 | Runtime Khusus OS | Amazon Linux 2023 | Dockerfile untuk Runtime khusus OS aktif GitHub | |
| al2 | Runtime Khusus OS | Amazon Linux 2 | Dockerfile untuk Runtime khusus OS aktif GitHub | |

Galeri Publik Registri Kontainer Elastis Amazon: gallery.ecr.aws/lambda/provided

Menggunakan gambar AWS non-dasar

Lambda mendukung gambar apa pun yang sesuai dengan salah satu format manifes gambar berikut:

- Docker Image Manifest V2, skema 2 (digunakan dengan Docker versi 1.10 dan yang lebih baru)
- Spesifikasi Open Container Initiative (OCI) (v1.0.0 dan lebih tinggi)

Lambda mendukung ukuran gambar maksimum yang tidak terkompresi 10 GB, termasuk semua lapisan.

Note

Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime](#) untuk bahasa Anda dalam gambar.

Klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime harus memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda. AWS menyediakan klien antarmuka runtime sumber terbuka untuk bahasa berikut:

- [Node.js](#)
- [Python](#)

- [Java](#)
- [.NET](#)
- [Go](#)
- [Ruby](#)
- [Rust](#) - [Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

Jika Anda menggunakan bahasa yang tidak memiliki klien antarmuka runtime AWS yang disediakan, Anda harus membuatnya sendiri.

ECR Izin Amazon

Sebelum Anda membuat fungsi Lambda dari gambar kontainer, Anda harus membangun gambar secara lokal dan mengunggahnya ke repositori Amazon. ECR Saat Anda membuat fungsi, tentukan ECR repositori URI Amazon.

Pastikan bahwa izin untuk pengguna atau peran yang membuat fungsi termasuk `GetRepositoryPolicy` dan `SetRepositoryPolicy`.

Misalnya, gunakan IAM konsol untuk membuat peran dengan kebijakan berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
      ],
      "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world"
    }
  ]
}
```

Kebijakan ECR repositori Amazon

Untuk fungsi di akun yang sama dengan gambar penampung di Amazon ECR, Anda dapat menambahkan `ecr:BatchGetImage` dan `ecr:GetDownloadUrlForLayer` mengizinkan kebijakan ECR repositori Amazon Anda. Contoh berikut menunjukkan kebijakan minimum:

```
{
  "Sid": "LambdaECRImageRetrievalPolicy",
  "Effect": "Allow",
  "Principal": {
    "Service": "lambda.amazonaws.com"
  },
  "Action": [
    "ecr:BatchGetImage",
    "ecr:GetDownloadUrlForLayer"
  ]
}
```

Untuk informasi selengkapnya tentang izin ECR repositori Amazon, lihat [Kebijakan repositori pribadi di Panduan Pengguna Amazon Elastic Container Registry](#).

Jika ECR repositori Amazon tidak menyertakan izin ini, Lambda menambahkan `ecr:BatchGetImage` dan `ecr:GetDownloadUrlForLayer` ke izin repositori gambar kontainer. Lambda dapat menambahkan izin ini hanya jika pemanggil utama Lambda memiliki dan izin. `ecr:getRepositoryPolicy` `ecr:setRepositoryPolicy`

Untuk melihat atau mengedit izin ECR repositori Amazon Anda, ikuti petunjuk dalam [Menyetel pernyataan kebijakan repositori pribadi di Panduan Pengguna Amazon Elastic Container Registry](#).

Izin ECR lintas akun Amazon

Akun yang berbeda di wilayah yang sama dapat membuat fungsi yang menggunakan gambar kontainer yang dimiliki oleh akun Anda. Dalam contoh berikut, [kebijakan izin ECR repositori Amazon](#) Anda memerlukan pernyataan berikut untuk memberikan akses ke nomor akun 123456789012.

- **CrossAccountPermission**— Memungkinkan akun 123456789012 untuk membuat dan memperbarui fungsi Lambda yang menggunakan gambar dari repositori ini. ECR
- **LambdaECRImage CrossAccountRetrievalPolicy** - Lambda pada akhirnya akan menyetel status fungsi menjadi tidak aktif jika tidak dipanggil untuk jangka waktu yang lama. Pernyataan ini diperlukan agar Lambda dapat mengambil gambar kontainer untuk optimasi dan caching atas nama fungsi yang dimiliki oleh 123456789012.

Example — Tambahkan izin lintas akun ke repositori Anda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountPermission",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    },
    {
      "Sid": "LambdaECRImageCrossAccountRetrievalPolicy",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Condition": {
        "StringLike": {
          "aws:sourceARN": "arn:aws:lambda:us-east-1:123456789012:function:*"
        }
      }
    }
  ]
}
```

Untuk memberikan akses ke beberapa akun, Anda menambahkan akun IDs ke daftar Utama dalam `CrossAccountPermission` kebijakan dan daftar Evaluasi kondisi di `LambdaECRImageCrossAccountRetrievalPolicy`.

Jika Anda bekerja dengan beberapa akun di AWS Organisasi, sebaiknya Anda menghitung setiap ID akun dalam kebijakan izin. ECR Pendekatan ini sejalan dengan praktik terbaik AWS keamanan dalam menyetel izin sempit dalam IAM kebijakan.

Selain izin Lambda, pengguna atau peran yang membuat fungsi juga harus memiliki `BatchGetImage` dan izin `GetDownloadUrlForLayer`

Siklus hidup fungsi

Setelah Anda mengunggah gambar kontainer baru atau yang diperbarui, Lambda mengoptimalkan gambar sebelum fungsi dapat memproses pemanggilan. Proses pengoptimalan dapat memakan waktu beberapa detik. Fungsi tetap dalam status `Pending` sampai proses selesai. Fungsi selanjutnya bertransisi ke status `Active`. Sewaktu berstatus `Pending`, Anda dapat memanggil fungsi, tetapi operasi lain pada fungsi gagal. Invokasi yang terjadi saat pembaruan gambar sedang berlangsung menjalankan kode dari gambar sebelumnya.

Jika fungsi tidak dipanggil selama beberapa minggu, Lambda mengeklaim kembali versi dioptimalkan, dan fungsi bertransisi ke status `Inactive`. Untuk mengaktifkan kembali fungsinya, Anda harus memanggilnya. Lambda menolak invokasi pertama dan fungsi memasuki status `Pending` sampai Lambda mengoptimalkan kembali gambar. Fungsi kemudian kembali ke status `Active`.

Lambda secara berkala mengambil gambar kontainer terkait dari repositori Amazon ECR. Jika image kontainer yang sesuai tidak ada lagi di Amazon ECR atau izin dicabut, fungsi akan memasuki `Failed` status, dan Lambda mengembalikan kegagalan untuk pemanggilan fungsi apa pun.

Anda dapat menggunakan Lambda API untuk mendapatkan informasi tentang status fungsi. Untuk informasi selengkapnya, lihat [Status fungsi Lambda](#).

Konfigurasi memori fungsi Lambda

Lambda memberikan daya CPU sebanding dengan jumlah memori yang dikonfigurasi. Memori adalah jumlah memori yang tersedia untuk fungsi Lambda saat waktu aktif. Anda dapat menambah atau mengurangi memori dan daya CPU yang dialokasikan ke fungsi Anda menggunakan pengaturan Memori. Anda dapat mengonfigurasi memori antara 128 MB dan 10.240 MB dengan peningkatan 1-MB. Pada 1.769 MB, fungsi memiliki ekuivalensi sebesar satu vCPU (satu detik vCPU dari kredit per detik).

Halaman ini menjelaskan bagaimana dan kapan harus memperbarui pengaturan memori untuk fungsi Lambda.

Bagian-bagian

- [Menentukan pengaturan memori yang sesuai untuk fungsi Lambda](#)
- [Mengonfigurasi memori fungsi \(konsol\)](#)
- [Mengkonfigurasi memori fungsi \(\)AWS CLI](#)
- [Mengkonfigurasi memori fungsi \(\)AWS SAM](#)
- [Menerima rekomendasi memori fungsi \(konsol\)](#)

Menentukan pengaturan memori yang sesuai untuk fungsi Lambda

Memori adalah tuas utama untuk mengontrol kinerja suatu fungsi. Pengaturan default, 128 MB, adalah pengaturan serendah mungkin. Kami menyarankan Anda hanya menggunakan 128 MB untuk fungsi Lambda sederhana, seperti yang mengubah dan merutekan acara ke layanan lain AWS. Alokasi memori yang lebih tinggi dapat meningkatkan kinerja untuk fungsi yang menggunakan pustaka impor, [lapisan Lambda](#), Amazon Simple Storage Service (Amazon S3) atau Amazon Elastic File System (Amazon EFS). Menambahkan lebih banyak memori secara proporsional meningkatkan jumlah CPU, meningkatkan daya komputasi keseluruhan yang tersedia. Jika suatu fungsi adalah CPU, jaringan atau terikat memori, maka meningkatkan pengaturan memori dapat secara dramatis meningkatkan kinerjanya.

Untuk menemukan konfigurasi memori yang tepat untuk fungsi Anda, sebaiknya gunakan alat [AWS Lambda Power Tuning](#) open source. Alat ini digunakan AWS Step Functions untuk menjalankan beberapa versi bersamaan dari fungsi Lambda pada alokasi memori yang berbeda dan mengukur kinerja. Fungsi input berjalan di AWS akun Anda, melakukan panggilan HTTP langsung dan interaksi SDK, untuk mengukur kemungkinan kinerja dalam skenario produksi langsung. Anda juga dapat

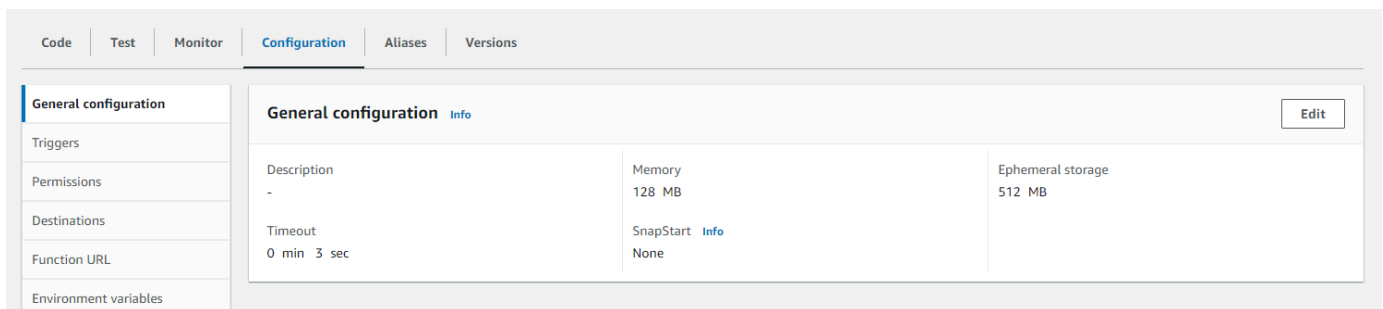
menerapkan proses CI/CD untuk menggunakan alat ini untuk secara otomatis mengukur kinerja fungsi baru yang Anda terapkan.

Mengonfigurasi memori fungsi (konsol)

Anda dapat mengonfigurasi memori fungsi Anda di konsol Lambda.

Untuk memperbarui memori fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Konfigurasi dan kemudian pilih Konfigurasi umum.



4. Di bagian Konfigurasi umum, pilih Edit.
5. Untuk Memori, tetapkan nilai dari 128 MB menjadi 10.240 MB.
6. Pilih Simpan.

Mengkonfigurasi memori fungsi ()AWS CLI

Anda dapat menggunakan [update-function-configuration](#) perintah untuk mengkonfigurasi memori fungsi Anda.

Example

```
aws lambda update-function-configuration \  
  --function-name my-function \  
  --memory-size 1024
```

Mengkonfigurasi memori fungsi ()AWS SAM

Anda dapat menggunakan [AWS Serverless Application Model](#) untuk mengkonfigurasi memori untuk fungsi Anda. Perbarui `MemorySize` properti di `template.yaml` file Anda dan kemudian jalankan [sam deploy](#).

Example `template.yaml`

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 1024
      # Other function properties...
```

Menerima rekomendasi memori fungsi (konsol)

Jika Anda memiliki izin administrator di AWS Identity and Access Management (IAM), Anda dapat memilih untuk menerima rekomendasi pengaturan memori fungsi Lambda dari AWS Compute Optimizer Untuk petunjuk cara memilih rekomendasi memori untuk akun atau organisasi Anda, lihat [Memilih akun Anda](#) di AWS Compute Optimizer Panduan Pengguna.

Note

Compute Optimizer hanya mendukung fungsi yang menggunakan arsitektur `x86_64`.

Ketika Anda telah memilih dan [fungsi Lambda Anda memenuhi persyaratan Compute Optimizer](#), Anda dapat melihat dan menerima rekomendasi memori fungsi dari Compute Optimizer di konsol Lambda dalam konfigurasi Umum.

Konfigurasi penyimpanan singkat untuk fungsi Lambda

Lambda menyediakan penyimpanan sementara untuk fungsi dalam direktori `/tmp`. Penyimpanan ini bersifat sementara dan unik untuk setiap lingkungan eksekusi. Anda dapat mengontrol jumlah penyimpanan sementara yang dialokasikan ke fungsi Anda menggunakan pengaturan penyimpanan Ephemeral. Anda dapat mengonfigurasi penyimpanan sementara antara 512 MB dan 10.240 MB, dengan peningkatan 1-MB. Semua data yang disimpan `/tmp` dienkripsi saat istirahat dengan kunci yang dikelola oleh AWS.

Halaman ini menjelaskan kasus penggunaan umum dan cara memperbarui penyimpanan sementara untuk fungsi Lambda.

Bagian-bagian

- [Kasus penggunaan umum untuk peningkatan penyimpanan sementara](#)
- [Mengkonfigurasi penyimpanan sementara \(konsol\)](#)
- [Mengkonfigurasi penyimpanan sementara \(AWS CLI\)](#)
- [Mengkonfigurasi penyimpanan sementara \(AWS SAM\)](#)

Kasus penggunaan umum untuk peningkatan penyimpanan sementara

Berikut adalah beberapa kasus penggunaan umum yang mendapat manfaat dari peningkatan penyimpanan sementara:

- Pekerjaan E xtract-transform-load (ETL): Tingkatkan penyimpanan sementara saat kode Anda melakukan komputasi menengah atau mengunduh sumber daya lain untuk menyelesaikan pemrosesan. Lebih banyak ruang sementara memungkinkan pekerjaan ETL yang lebih kompleks untuk berjalan di fungsi Lambda.
- Inferensi pembelajaran mesin (ML): Banyak tugas inferensi bergantung pada file data referensi besar, termasuk perpustakaan dan model. Dengan penyimpanan yang lebih singkat, Anda dapat mengunduh model yang lebih besar dari Amazon Simple Storage Service (Amazon S3) `/tmp` ke dan menggunakannya dalam pemrosesan Anda.
- Pemrosesan data: Untuk beban kerja yang mengunduh objek dari Amazon S3 sebagai respons terhadap peristiwa S3, `/tmp` lebih banyak ruang memungkinkan untuk menangani objek yang lebih besar tanpa menggunakan pemrosesan dalam memori. Beban kerja yang membuat PDF atau media proses juga mendapat manfaat dari penyimpanan yang lebih singkat.

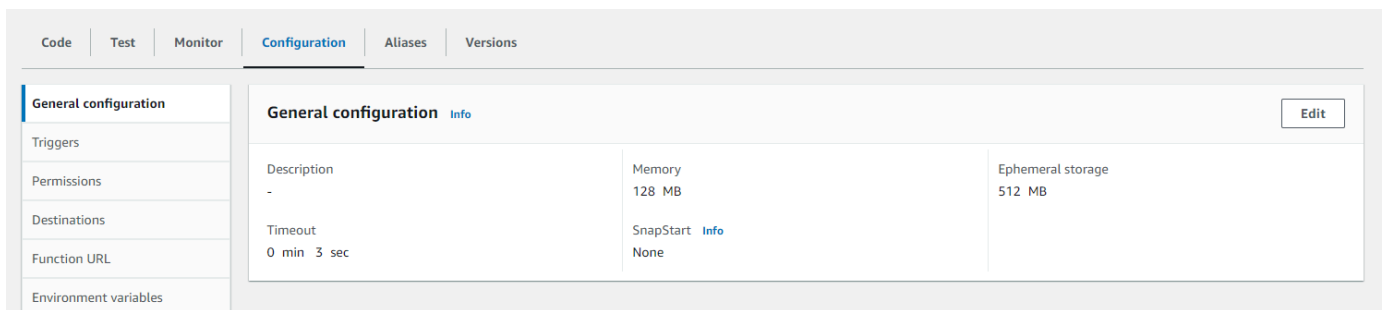
- Pemrosesan grafis: Pemrosesan gambar adalah kasus penggunaan umum untuk aplikasi berbasis Lambda. Untuk beban kerja yang memproses file TIFF besar atau citra satelit, penyimpanan yang lebih singkat memudahkan penggunaan pustaka dan melakukan perhitungan di Lambda.

Mengkonfigurasi penyimpanan sementara (konsol)

Anda dapat mengonfigurasi penyimpanan sementara di konsol Lambda.

Untuk memodifikasi penyimpanan sementara untuk suatu fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Konfigurasi dan kemudian pilih Konfigurasi umum.



4. Di bagian Konfigurasi umum, pilih Edit.
5. Untuk penyimpanan Ephemeral, tetapkan nilai antara 512 MB dan 10.240 MB, dengan peningkatan 1-MB.
6. Pilih Simpan.

Mengkonfigurasi penyimpanan sementara ()AWS CLI

Anda dapat menggunakan [update-function-configuration](#) perintah untuk mengkonfigurasi penyimpanan sementara.

Example

```
aws lambda update-function-configuration \  
  --function-name my-function \  
  --ephemeral-storage '{"Size": 1024}'
```

Mengkonfigurasi penyimpanan sementara (EphemeralStorage) AWS SAM

Anda dapat menggunakan [AWS Serverless Application Model](#) untuk mengkonfigurasi penyimpanan sementara untuk fungsi Anda. Perbarui [EphemeralStorage](#) properti di `template.yaml` file Anda dan kemudian jalankan [sam deploy](#).

Example `template.yaml`

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs20.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      # Other function properties...
```

Memilih dan mengonfigurasi arsitektur set instruksi untuk fungsi Lambda Anda

Arsitektur set instruksi dari fungsi Lambda menentukan jenis prosesor komputer yang digunakan Lambda untuk menjalankan fungsi tersebut. Lambda menyediakan pilihan arsitektur set instruksi:

- ARM arsitektur arm64 — 64-bit, untuk prosesor AWS Graviton2.
- x86_64 - arsitektur x86 64-bit, untuk prosesor berbasis x86.

Note

Arsitektur arm64 tersedia di sebagian besar Wilayah AWS. Untuk informasi selengkapnya, silakan lihat [Harga AWS Lambda](#). Dalam tabel harga memori, pilih tab Arm Price, lalu buka daftar dropdown Region untuk melihat Wilayah AWS dukungan arm64 dengan Lambda. Untuk contoh cara membuat fungsi dengan arsitektur arm64, lihat [AWS Lambda Functions Powered by AWS Graviton2 Processor](#).

Topik

- [Keuntungan menggunakan arsitektur arm64](#)
- [Persyaratan untuk migrasi ke arsitektur arm64](#)
- [Kompatibilitas kode fungsi dengan arsitektur arm64](#)
- [Cara bermigrasi ke arsitektur arm64](#)
- [Mengonfigurasi arsitektur set instruksi](#)

Keuntungan menggunakan arsitektur arm64

Fungsi Lambda yang menggunakan arsitektur arm64 (prosesor AWS Graviton2) dapat mencapai harga dan kinerja yang jauh lebih baik daripada fungsi setara yang berjalan pada arsitektur x86_64. Pertimbangkan untuk menggunakan arm64 untuk aplikasi komputasi intensif seperti komputasi kinerja tinggi, pengkodean video, dan beban kerja simulasi.

Graviton2 CPU menggunakan inti Neoverse N1 dan mendukung Armv8.2 (termasuk CRC dan ekstensi krypto) ditambah beberapa ekstensi arsitektur lainnya.

Graviton2 mengurangi waktu baca memori dengan menyediakan cache L2 per v yang lebih besar CPU, yang meningkatkan kinerja latensi backend web dan seluler, layanan mikro, dan sistem pemrosesan data. Graviton2 juga menyediakan peningkatan kinerja enkripsi dan mendukung set instruksi yang meningkatkan latensi inferensi pembelajaran mesin CPU berbasis.

[Untuk informasi lebih lanjut tentang AWS Graviton2, lihat AWS Prosesor Graviton.](#)

Persyaratan untuk migrasi ke arsitektur arm64

Saat Anda memilih fungsi Lambda untuk bermigrasi ke arsitektur arm64, untuk memastikan migrasi lancar, pastikan fungsi Anda memenuhi persyaratan berikut:

- Paket penyebaran hanya berisi komponen sumber terbuka dan kode sumber yang Anda kontrol, sehingga Anda dapat membuat pembaruan yang diperlukan untuk migrasi.
- Jika kode fungsi menyertakan dependensi pihak ketiga, setiap pustaka atau paket menyediakan versi arm64.

Kompatibilitas kode fungsi dengan arsitektur arm64

Kode fungsi Lambda Anda harus kompatibel dengan arsitektur set instruksi fungsi. Sebelum Anda memigrasikan fungsi ke arsitektur arm64, perhatikan poin-poin berikut tentang kode fungsi saat ini:

- Jika Anda menambahkan kode fungsi Anda menggunakan editor kode tertanam, kode Anda mungkin berjalan pada salah satu arsitektur tanpa modifikasi.
- Jika Anda mengunggah kode fungsi Anda, Anda harus mengunggah kode baru yang kompatibel dengan arsitektur target Anda.
- Jika fungsi Anda menggunakan lapisan, Anda harus [memeriksa setiap lapisan](#) untuk memastikan bahwa itu kompatibel dengan arsitektur baru. Jika lapisan tidak kompatibel, edit fungsi untuk mengganti versi lapisan saat ini dengan versi lapisan yang kompatibel.
- Jika fungsi Anda menggunakan ekstensi Lambda, Anda harus memeriksa setiap ekstensi untuk memastikan bahwa itu kompatibel dengan arsitektur baru.
- Jika fungsi Anda menggunakan jenis paket penyebaran gambar kontainer, Anda harus membuat image kontainer baru yang kompatibel dengan arsitektur fungsi.

Cara bermigrasi ke arsitektur arm64

Untuk memigrasikan fungsi Lambda ke arsitektur arm64, sebaiknya ikuti langkah-langkah berikut:

1. Buat daftar dependensi untuk aplikasi atau beban kerja Anda. Dependensi umum meliputi:
 - Semua pustaka dan paket yang digunakan fungsi.
 - Alat yang Anda gunakan untuk membangun, menyebarkan, dan menguji fungsi, seperti kompiler, rangkaian pengujian, integrasi berkelanjutan dan pipeline pengiriman berkelanjutan (CI/CD), alat penyediaan, dan skrip.
 - Ekstensi Lambda dan alat pihak ketiga yang Anda gunakan untuk memantau fungsi dalam produksi.
2. Untuk setiap dependensi, periksa versinya, lalu periksa apakah versi arm64 tersedia.
3. Bangun lingkungan untuk memigrasikan aplikasi Anda.
4. Bootstrap aplikasi.
5. Uji dan debug aplikasi.
6. Uji kinerja fungsi arm64. Bandingkan kinerjanya dengan versi x86_64.
7. Perbarui pipeline infrastruktur Anda untuk mendukung fungsi Lambda arm64.
8. Tahap penyebaran Anda ke produksi.

Misalnya, gunakan [konfigurasi perutean alias](#) untuk membagi lalu lintas antara versi x86 dan arm64 fungsi, dan bandingkan kinerja dan latensi.

Untuk informasi selengkapnya tentang cara membuat lingkungan kode untuk arsitektur arm64, termasuk informasi khusus bahasa untuk Java, Go, .NET, dan Python, lihat repositori [Memulai dengan AWS GitHub Graviton](#).

Mengkonfigurasi arsitektur set instruksi

Anda dapat mengonfigurasi arsitektur set instruksi untuk fungsi Lambda baru dan yang sudah ada menggunakan konsol Lambda, AWS Command Line Interface (AWS CLI), atau AWS CloudFormation. Ikuti langkah-langkah ini untuk mengubah arsitektur set instruksi untuk fungsi Lambda yang ada dari konsol.

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda konfigurasi arsitektur set instruksi.
3. Pada tab Kode utama, untuk bagian Pengaturan Runtime, pilih Edit.
4. Di bawah Arsitektur, pilih arsitektur set instruksi yang ingin digunakan oleh fungsi Anda.

5. Pilih Simpan.

Konfigurasi batas waktu fungsi Lambda

Lambda menjalankan kode Anda untuk jangka waktu tertentu sebelum waktu habis. Timeout adalah jumlah waktu maksimum dalam hitungan detik yang dapat dijalankan oleh fungsi Lambda. Nilai default untuk pengaturan ini adalah 3 detik, tetapi Anda dapat menyesuaikannya dengan penambahan 1 detik hingga nilai maksimum 900 detik (15 menit).

Halaman ini menjelaskan bagaimana dan kapan harus memperbarui pengaturan batas waktu untuk fungsi Lambda.

Bagian-bagian

- [Menentukan nilai batas waktu yang sesuai untuk fungsi Lambda](#)
- [Mengkonfigurasi batas waktu \(konsol\)](#)
- [Mengkonfigurasi batas waktu \(\)AWS CLI](#)
- [Mengkonfigurasi batas waktu \(\)AWS SAM](#)

Menentukan nilai batas waktu yang sesuai untuk fungsi Lambda

Jika nilai batas waktu mendekati durasi rata-rata suatu fungsi, ada risiko yang lebih tinggi bahwa fungsi tersebut akan habis secara tak terduga. Durasi suatu fungsi dapat bervariasi berdasarkan jumlah transfer dan pemrosesan data, dan latensi layanan apa pun yang berinteraksi dengan fungsi tersebut. Beberapa penyebab umum batas waktu meliputi:

- Unduhan dari Amazon Simple Storage Service (Amazon S3) lebih besar atau memakan waktu lebih lama dari rata-rata.
- Fungsi membuat permintaan ke layanan lain, yang membutuhkan waktu lebih lama untuk merespons.
- Parameter yang disediakan untuk suatu fungsi membutuhkan lebih banyak kompleksitas komputasi dalam fungsi, yang menyebabkan pemanggilan memakan waktu lebih lama.

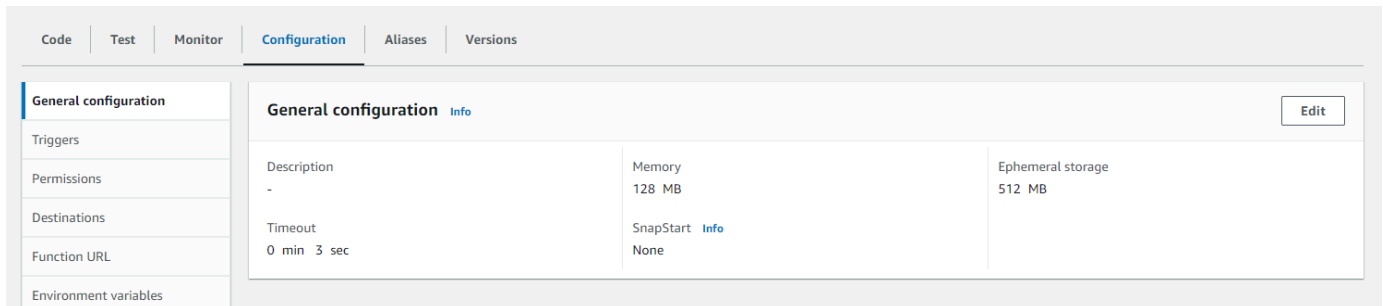
Saat menguji aplikasi Anda, pastikan pengujian Anda secara akurat mencerminkan ukuran dan kuantitas data serta nilai parameter yang realistis. Pengujian sering menggunakan sampel kecil untuk kenyamanan, tetapi Anda harus menggunakan kumpulan data di batas atas dari apa yang diharapkan secara wajar untuk beban kerja Anda.

Mengkonfigurasi batas waktu (konsol)

Anda dapat mengonfigurasi batas waktu fungsi di konsol Lambda.

Untuk memodifikasi batas waktu untuk suatu fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Konfigurasi dan kemudian pilih Konfigurasi umum.



4. Di bagian Konfigurasi umum, pilih Edit.
5. Untuk Timeout, tetapkan nilai antara 1 dan 900 detik (15 menit).
6. Pilih Simpan.

Mengkonfigurasi batas waktu ()AWS CLI

Anda dapat menggunakan [update-function-configuration](#) perintah untuk mengonfigurasi nilai batas waktu, dalam hitungan detik. Contoh perintah berikut meningkatkan batas waktu fungsi menjadi 120 detik (2 menit).

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --timeout 120
```

Mengkonfigurasi batas waktu ()AWS SAM

Anda dapat menggunakan [AWS Serverless Application Model](#) untuk mengkonfigurasi nilai batas waktu untuk fungsi Anda. Perbarui properti [Timeout](#) di `template.yaml` file Anda dan kemudian jalankan [sam deploy](#).

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'  
Transform: AWS::Serverless-2016-10-31  
Description: An AWS Serverless Application Model template describing your function.  
Resources:  
  my-function:  
    Type: AWS::Serverless::Function  
    Properties:  
      CodeUri: .  
      Description: ''  
      MemorySize: 128  
      Timeout: 120  
      # Other function properties...
```

Gunakan variabel lingkungan Lambda untuk mengonfigurasi nilai dalam kode

Anda dapat menggunakan variabel lingkungan untuk menyesuaikan perilaku fungsi Anda tanpa memperbarui kode. Variabel lingkungan adalah sepasang string yang disimpan dalam konfigurasi spesifik versi fungsi. Runtime Lambda membuat variabel lingkungan tersedia bagi kode Anda dan mengatur variabel lingkungan tambahan yang berisi informasi tentang fungsi dan permintaan invokasi.

Note

Untuk meningkatkan keamanan, sebaiknya Anda menggunakan AWS Secrets Manager variabel lingkungan untuk menyimpan kredensi database dan informasi sensitif lainnya seperti API kunci atau token otorisasi. Untuk informasi selengkapnya, lihat [Membuat dan mengelola rahasia dengan AWS Secrets Manager](#).

Variabel lingkungan tidak dievaluasi sebelum pemanggilan fungsi. Nilai apa pun yang Anda tentukan dianggap sebagai string harafiah dan tidak diperluas. Lakukan evaluasi variabel dalam kode fungsi Anda.

Anda dapat mengonfigurasi variabel lingkungan di Lambda menggunakan konsol Lambda, (), AWS Command Line Interface (AWS CLI), AWS Serverless Application Model atau menggunakan AWS SAM AWS SDK

Console

Anda menentukan variabel lingkungan pada versi fungsi yang belum dipublikasikan. Saat Anda mempublikasikan versi, variabel lingkungan dikunci untuk versi tersebut bersama dengan [pengaturan konfigurasi khusus versi](#) lainnya.

Anda membuat variabel lingkungan untuk fungsi Anda dengan mendefinisikan kunci dan nilai. Fungsi Anda menggunakan nama kunci untuk mengambil nilai variabel lingkungan.

Untuk mengatur variabel lingkungan di konsol Lambda

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih fungsi.

3. Pilih Konfigurasi, lalu pilih Variabel lingkungan.
4. Pada Variabel lingkungan, pilih Edit.
5. Pilih Tambahkan variabel lingkungan.
6. Masukkan kunci dan nilai.

Persyaratan

- Kunci dimulai dengan huruf dan setidaknya dua karakter.
 - Kunci hanya berisi huruf, angka, dan karakter garis bawah (_).
 - Kunci tidak [dicadangkan oleh Lambda](#).
 - Ukuran total semua variabel lingkungan tidak lebih dari 4 KB.
7. Pilih Simpan.

Untuk menghasilkan daftar variabel lingkungan di editor kode konsol

Anda dapat membuat daftar variabel lingkungan di editor kode Lambda. Ini adalah cara cepat untuk mereferensikan variabel lingkungan Anda saat Anda membuat kode.

1. Pilih tab Kode.
2. Pilih tab Variabel Lingkungan.
3. Pilih Alat, Tampilkan Variabel Lingkungan.

Variabel lingkungan tetap dienkripsi saat terdaftar di editor kode konsol. Jika Anda mengaktifkan pembantu enkripsi untuk enkripsi dalam perjalanan, maka pengaturan tersebut tetap tidak berubah. Untuk informasi selengkapnya, lihat [Mengamankan variabel lingkungan Lambda](#).

Daftar variabel lingkungan hanya-baca dan hanya tersedia di konsol Lambda. File ini tidak disertakan saat Anda mengunduh arsip file.zip fungsi, dan Anda tidak dapat menambahkan variabel lingkungan dengan mengunggah file ini.

AWS CLI

Contoh berikut menetapkan dua variabel lingkungan pada fungsi yang diberi nama `my-function`.

```
aws lambda update-function-configuration \
```

```
--function-name my-function \  
--environment "Variables={BUCKET=amzn-s3-demo-bucket,KEY=file.txt}"
```

Ketika Anda menerapkan variabel lingkungan dengan perintah `update-function-configuration`, seluruh isi dari struktur `Variables` digantikan. Untuk mempertahankan variabel lingkungan yang ada saat Anda menambahkan yang baru, sertakan semua nilai yang ada dalam permintaan Anda.

Untuk mendapatkan konfigurasi saat ini, gunakan perintah `get-function-configuration`.

```
aws lambda get-function-configuration \  
--function-name my-function
```

Anda akan melihat output berikut:

```
{  
  "FunctionName": "my-function",  
  "FunctionArn": "arn:aws:lambda:us-east-2:111122223333:function:my-function",  
  "Runtime": "nodejs20.x",  
  "Role": "arn:aws:iam::111122223333:role/lambda-role",  
  "Environment": {  
    "Variables": {  
      "BUCKET": "amzn-s3-demo-bucket",  
      "KEY": "file.txt"  
    }  
  },  
  "RevisionId": "0894d3c1-2a3d-4d48-bf7f-abade99f3c15",  
  ...  
}
```

Anda dapat meneruskan ID revisi dari output `get-function-configuration` sebagai parameter ke `update-function-configuration`. Ini memastikan bahwa nilai tidak berubah antara saat Anda membaca konfigurasi dan saat Anda memperbaruinya.

Untuk mengonfigurasi kunci enkripsi fungsi, atur opsi `KMSKeyARN`.

```
aws lambda update-function-configuration \  
--function-name my-function \  
--kms-key-arn arn:aws:kms:us-east-2:111122223333:key/055efbb4-xmpl-4336-  
ba9c-538c7d31f599
```


AWS SAM

Anda dapat menggunakan [AWS Serverless Application Model](#) untuk mengkonfigurasi variabel lingkungan untuk fungsi Anda. Perbarui properti [Lingkungan](#) dan [Variabel](#) dalam `template.yaml` file Anda dan kemudian jalankan [sam deploy](#).

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs18.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      Environment:
        Variables:
          BUCKET: amzn-s3-demo-bucket
          KEY: file.txt
      # Other function properties...
```

AWS SDKs

Untuk mengelola variabel lingkungan menggunakan AWS SDK, gunakan API operasi berikut.

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Untuk mempelajari lebih lanjut, lihat [AWS SDK dokumentasi](#) untuk bahasa pemrograman pilihan Anda.

Variabel lingkungan runtime yang ditetapkan

[Runtime](#) Lambda menetapkan beberapa variabel lingkungan selama inisialisasi. Sebagian besar variabel lingkungan memberikan informasi tentang fungsi atau runtime. Kunci untuk variabel lingkungan ini dicadangkan dan tidak dapat diatur dalam konfigurasi fungsi Anda.

Variabel lingkungan yang tersimpan

- `_HANDLER` – Lokasi handler dikonfigurasi pada fungsi.
- `_X_AMZN_TRACE_ID` – [Header pelacakan X-Ray](#). Variabel lingkungan ini berubah dengan setiap pemanggilan.
 - Variabel lingkungan ini tidak ditentukan untuk runtime khusus OS (keluarga runtime). `provided` Anda dapat mengatur `_X_AMZN_TRACE_ID` runtime kustom menggunakan header `Lambda-Trace-Id` respons dari file. [Invokasi berikutnya](#)
 - Untuk Java runtime versi 17 dan yang lebih baru, variabel lingkungan ini tidak digunakan. Sebaliknya, Lambda menyimpan informasi penelusuran di properti sistem. `com.amazonaws.xray.traceHeader`
- `AWS_DEFAULT_REGION`— Default Wilayah AWS di mana fungsi Lambda dijalankan.
- `AWS_REGION`— Wilayah AWS Tempat fungsi Lambda dijalankan. Jika didefinisikan, nilai ini mengesampingkan `AWS_DEFAULT_REGION`
 - Untuk informasi selengkapnya tentang penggunaan variabel Wilayah AWS lingkungan dengan AWS SDKs, lihat [AWS Wilayah](#) dalam AWS SDKs dan Panduan Referensi Alat.
- `AWS_EXECUTION_ENV`— [Pengidentifikasi runtime](#), diawali oleh `AWS_Lambda_` (misalnya, `AWS_Lambda_java8`). Variabel lingkungan ini tidak ditentukan untuk runtime khusus OS (keluarga runtime). `provided`
- `AWS_LAMBDA_FUNCTION_NAME` – Nama fungsi.
- `AWS_LAMBDA_FUNCTION_MEMORY_SIZE` – Jumlah memori yang tersedia untuk fungsi dalam MB.
- `AWS_LAMBDA_FUNCTION_VERSION` – Versi fungsi yang sedang dijalankan.
- `AWS_LAMBDA_INITIALIZATION_TYPE`— Jenis inisialisasi fungsi, yaitu, `on-demand`, `provisioned-concurrency`, atau `snap-start`. Untuk selengkapnya, lihat [Mengonfigurasi konkurensi yang disediakan atau. Meningkatkan kinerja startup dengan Lambda SnapStart](#)
- `AWS_LAMBDA_LOG_GROUP_NAME`, `AWS_LAMBDA_LOG_STREAM_NAME` — Nama grup Amazon CloudWatch Logs dan streaming untuk fungsi tersebut. [Variabel `AWS_LAMBDA_LOG_GROUP_NAME` dan `AWS_LAMBDA_LOG_STREAM_NAME` lingkungan](#) tidak tersedia dalam fungsi Lambda SnapStart .

- `AWS_ACCESS_KEY`, `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, `AWS_SESSION_TOKEN` — Kunci akses yang diperoleh dari [peran eksekusi](#) fungsi.
- `AWS_LAMBDA_RUNTIME_API`— ([Custom runtime](#)) Host dan port [runtime API](#).
- `LAMBDA_TASK_ROOT` – Jalur ke kode fungsi Lambda Anda.
- `LAMBDA_RUNTIME_DIR` – Jalur ke pustaka runtime.

Variabel lingkungan tambahan berikut ini tidak dicadangkan dan dapat diperluas dalam konfigurasi fungsi Anda.

Variabel lingkungan yang tidak dicadangkan

- `LANG` – Lokal runtime (`en_US.UTF-8`).
- `PATH` – Jalur eksekusi (`/usr/local/bin:/usr/bin:/bin:/opt/bin`).
- `LD_LIBRARY_PATH` – Jalur pustaka sistem (`/var/lang/lib:/lib64:/usr/lib64:$LAMBDA_RUNTIME_DIR:$LAMBDA_RUNTIME_DIR/lib:$LAMBDA_TASK_ROOT:$LAMBDA_TASK_ROOT/lib:/opt/lib`).
- `NODE_PATH` – ([Node.js](#)) Jalur pustaka Node.js (`/opt/nodejs/node12/node_modules:/opt/nodejs/node_modules:$LAMBDA_RUNTIME_DIR/node_modules`).
- `PYTHONPATH` – ([Python 2.7, 3.6, 3.8](#)) Jalur pustaka Python (`$LAMBDA_RUNTIME_DIR`).
- `GEM_PATH` – ([Ruby](#)) Jalur pustaka Ruby (`$LAMBDA_TASK_ROOT/vendor/bundle/ruby/2.5.0:/opt/ruby/gems/2.5.0`).
- `AWS_XRAY_CONTEXT_MISSING`— Untuk penelusuran X-Ray, Lambda mengatur ini `LOG_ERROR` untuk menghindari kesalahan runtime dari X-Ray. SDK
- `AWS_XRAY_DAEMON_ADDRESS` – Untuk pelacakan X-Ray, alamat IP dan port daemon X-Ray.
- `AWS_LAMBDA_DOTNET_PREJIT`- Untuk .NET6 dan .NET7 runtime, atur variabel ini untuk mengaktifkan atau menonaktifkan .NETpengoptimalan runtime tertentu. Nilai mencakup `always`, `never`, dan `provisioned-concurrency`. Untuk informasi selengkapnya, lihat [Mengkonfigurasi konkurensi yang disediakan untuk suatu fungsi](#).
- `TZ` – Zona waktu lingkungan (`:UTC`). Lingkungan eksekusi menggunakan NTP untuk menyinkronkan jam sistem.

Nilai sampel yang ditampilkan mencerminkan runtime terbaru. Adanya variabel tertentu atau nilainya dapat bervariasi pada runtime awal.

Contoh skenario untuk variabel lingkungan

Anda dapat menggunakan variabel lingkungan untuk menyesuaikan perilaku fungsi di lingkungan pengujian Anda dan lingkungan produksi. Misalnya, Anda dapat membuat dua fungsi dengan kode yang sama, tetapi konfigurasi yang berbeda. Satu fungsi terhubung ke basis data uji, dan fungsi lainnya terhubung ke basis data produksi. Dalam situasi ini, Anda menggunakan variabel lingkungan untuk meneruskan nama host dan detail koneksi lainnya untuk database ke fungsi.

Contoh berikut menunjukkan cara menentukan host basis data dan nama basis data sebagai variabel lingkungan.

| | | |
|--------------|---------------------------|--------|
| ENVIRONMENT | DEVELOPMENT | Remove |
| databaseHost | lambdadb | Remove |
| databaseName | rd1owwlydynm5.cuovuyfg087 | Remove |
| Key | Value | Remove |

Jika Anda ingin lingkungan pengujian Anda menghasilkan lebih banyak informasi debug daripada lingkungan produksi, Anda dapat mengatur variabel lingkungan untuk mengonfigurasi lingkungan pengujian Anda untuk menggunakan lebih banyak log verbose atau pelacakan yang lebih terperinci.

Mengamankan variabel lingkungan Lambda

Untuk mengamankan variabel lingkungan Anda, Anda dapat menggunakan enkripsi sisi server untuk melindungi data Anda saat istirahat dan enkripsi sisi klien untuk melindungi data Anda dalam perjalanan.

Note

Untuk meningkatkan keamanan database, kami sarankan Anda menggunakan AWS Secrets Manager bukan variabel lingkungan untuk menyimpan kredensi database. Untuk informasi selengkapnya, lihat [Menggunakan AWS Lambda dengan Amazon RDS](#).

Keamanan saat istirahat

Lambda selalu menyediakan enkripsi sisi server saat istirahat dengan file. AWS KMS key Secara default, Lambda menggunakan file. Kunci yang dikelola AWS Jika perilaku default ini sesuai dengan alur kerja Anda, Anda tidak perlu menyiapkan hal lain. Lambda membuat Kunci yang dikelola AWS di akun Anda dan mengelola izin untuk itu untuk Anda. AWS tidak membebankan biaya untuk menggunakan kunci ini.

Jika mau, Anda dapat memberikan kunci yang dikelola AWS KMS pelanggan sebagai gantinya. Anda dapat melakukan ini untuk memiliki kontrol atas rotasi kunci KMS atau untuk memenuhi persyaratan organisasi Anda untuk mengelola kunci KMS. Saat Anda menggunakan kunci yang dikelola pelanggan, hanya pengguna di akun Anda dengan akses ke kunci KMS yang dapat melihat atau mengelola variabel lingkungan pada fungsi tersebut.

Kunci yang dikelola pelanggan dikenakan AWS KMS biaya standar. Untuk informasi selengkapnya, lihat [harga AWS Key Management Service](#).

Keamanan dalam perjalanan

Untuk keamanan tambahan, Anda dapat mengaktifkan helper untuk enkripsi dalam perjalanan, yang memastikan bahwa variabel lingkungan Anda dienkripsi sisi klien untuk perlindungan dalam perjalanan.

Untuk mengonfigurasi enkripsi untuk variabel lingkungan Anda

1. Gunakan AWS Key Management Service (AWS KMS) untuk membuat kunci terkelola pelanggan apa pun yang digunakan Lambda untuk enkripsi sisi server dan sisi klien. Untuk informasi selengkapnya, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang.
2. Menggunakan konsol Lambda, navigasikan ke halaman Edit variabel lingkungan.
 - a. Buka [halaman Fungsi](#) di konsol Lambda.
 - b. Pilih fungsi.
 - c. Pilih Konfigurasi, lalu pilih variabel Lingkungan dari bilah navigasi kiri.
 - d. Di bagian Variabel lingkungan, pilih Edit.
 - e. Perluas Konfigurasi enkripsi.
3. (Opsional) Aktifkan pembantu enkripsi konsol untuk menggunakan enkripsi sisi klien untuk melindungi data Anda saat transit.
 - a. Di bawah Enkripsi dalam perjalanan, pilih Aktifkan pembantu untuk enkripsi saat transit.

- b. Untuk setiap variabel lingkungan yang ingin Anda aktifkan pembantu enkripsi konsol, pilih Enkripsi di sebelah variabel lingkungan.
- c. Di bawah AWS KMS key untuk mengenkripsi saat transit, pilih kunci terkelola pelanggan yang Anda buat di awal prosedur ini.
- d. Pilih Kebijakan peran eksekusi dan salin kebijakan. Kebijakan ini memberikan izin untuk peran eksekusi fungsi Anda untuk mendekripsi variabel lingkungan.

Simpan kebijakan ini untuk digunakan pada langkah terakhir prosedur ini.

- e. Tambahkan kode ke fungsi Anda yang mendekripsi variabel lingkungan. Untuk melihat contoh, pilih Dekripsi cuplikan rahasia.
4. (Opsional) Tentukan kunci terkelola pelanggan Anda untuk enkripsi saat istirahat.
 - a. Pilih Gunakan kunci utama pelanggan.
 - b. Pilih kunci yang dikelola pelanggan yang Anda buat di awal prosedur ini.
 5. Pilih Simpan.
 6. Menyiapkan izin.

Jika Anda menggunakan kunci yang dikelola pelanggan dengan enkripsi sisi server, berikan izin kepada pengguna atau peran apa pun yang Anda inginkan untuk dapat melihat atau mengelola variabel lingkungan pada fungsi tersebut. Untuk informasi selengkapnya, lihat [Mengelola izin ke kunci KMS enkripsi sisi server Anda](#).

Jika Anda mengaktifkan enkripsi sisi klien untuk keamanan dalam perjalanan, fungsi Anda memerlukan izin untuk memanggil operasi API. `kms:Decrypt` Tambahkan kebijakan yang Anda simpan sebelumnya dalam prosedur ini ke [peran eksekusi](#) fungsi.

Mengelola izin ke kunci KMS enkripsi sisi server Anda

Tidak ada AWS KMS izin yang diperlukan untuk pengguna Anda atau peran eksekusi fungsi untuk menggunakan kunci enkripsi default. Untuk menggunakan kunci yang dikelola pelanggan, Anda memerlukan izin untuk menggunakan kunci tersebut. Lambda menggunakan izin Anda untuk membuat izin pada kunci. Ini memungkinkan Lambda menggunakannya untuk enkripsi.

- `kms:ListAliases` – Untuk melihat kunci di konsol Lambda.
- `kms:CreateGrant`, `kms:Encrypt` — Untuk mengonfigurasi kunci yang dikelola pelanggan pada suatu fungsi.

- `kms:Decrypt`— Untuk melihat dan mengelola variabel lingkungan yang dienkripsi dengan kunci yang dikelola pelanggan.

Anda bisa mendapatkan izin ini dari Akun AWS atau dari kebijakan izin berbasis sumber daya kunci. `ListAliases` disediakan oleh [kebijakan terkelola untuk Lambda](#). Kebijakan kunci memberikan izin yang tersisa kepada pengguna di grup Pengguna utama.

Pengguna tanpa `Decrypt` izin masih dapat mengelola fungsi, tetapi mereka tidak dapat melihat variabel lingkungan atau mengelolanya di konsol Lambda. Untuk mencegah pengguna melihat variabel lingkungan, tambahkan pernyataan ke izin pengguna yang menolak akses ke kunci default, kunci yang dikelola pelanggan, atau semua kunci.

Example Kebijakan IAM – Menolak akses dengan ARN kunci

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-2:111122223333:key/3be10e2d-xmpl-4be4-
bc9d-0405a71945cc"
    }
  ]
}
```

Untuk detail tentang mengelola izin utama, lihat [Kebijakan utama AWS KMS di Panduan AWS Key Management Service Pengembang](#).

Mengambil variabel lingkungan Lambda

Untuk mengambil variabel lingkungan dalam kode fungsi Anda, gunakan metode standar untuk bahasa pemrograman Anda.

Node.js

```
let region = process.env.AWS_REGION
```

Python

```
import os
region = os.environ['AWS_REGION']
```

Note

Pada beberapa kasus, Anda mungkin perlu menggunakan format berikut:

```
region = os.environ.get('AWS_REGION')
```

Ruby

```
region = ENV["AWS_REGION"]
```

Java

```
String region = System.getenv("AWS_REGION");
```

Go

```
var region = os.Getenv("AWS_REGION")
```

C#

```
string region = Environment.GetEnvironmentVariable("AWS_REGION");
```

PowerShell

```
$region = $env:AWS_REGION
```

Lambda menyimpan variabel lingkungan secara aman dengan mengenkripsinya saat istirahat. Anda dapat [mengonfigurasi Lambda untuk menggunakan kunci enkripsi yang berbeda](#), mengenkripsi nilai variabel lingkungan di sisi klien, atau mengatur variabel lingkungan AWS CloudFormation dalam templat dengan [AWS Secrets Manager](#).

Memberikan fungsi Lambda akses ke sumber daya di Amazon VPC

Dengan Amazon Virtual Private Cloud (AmazonVPC), Anda dapat membuat jaringan pribadi di sumber daya host Anda Akun AWS seperti instans Amazon Elastic Compute Cloud (AmazonEC2), instans Amazon Relational Database Service (AmazonRDS), dan instans Amazon. ElastiCache Anda dapat memberikan fungsi Lambda Anda akses ke sumber daya yang dihosting di Amazon VPC dengan melampirkan fungsi Anda ke VPC melalui subnet pribadi yang berisi sumber daya. Ikuti petunjuk di bagian berikut untuk melampirkan fungsi Lambda ke Amazon VPC menggunakan konsol Lambda, AWS Command Line Interface (AWS CLI), atau AWS SAM

Note

Setiap fungsi Lambda berjalan di dalam VPC yang dimiliki dan dikelola oleh layanan Lambda. Ini VPCs dikelola secara otomatis oleh Lambda dan tidak terlihat oleh pelanggan. Mengonfigurasi fungsi Anda untuk mengakses AWS sumber daya lain di Amazon tidak VPC berpengaruh pada fungsi yang dikelola Lambda VPC yang dijalankan di dalamnya.

Bagian-bagian

- [Diperlukan izin IAM](#)
- [Melampirkan fungsi Lambda ke Amazon VPC di Anda Akun AWS](#)
- [Akses internet saat dilampirkan ke VPC](#)
- [IPv6dukungan](#)
- [Praktik terbaik untuk menggunakan Lambda dengan Amazon VPCs](#)
- [Memahami Antarmuka Jaringan Elastis Hyperplane \(\) ENIs](#)
- [Menggunakan tombol IAM kondisi untuk VPC pengaturan](#)
- [VPCtutorial](#)

Diperlukan izin IAM

Untuk melampirkan fungsi Lambda ke Amazon VPC di Anda, Akun AWS Lambda memerlukan izin untuk membuat dan mengelola antarmuka jaringan yang digunakannya untuk memberikan fungsi Anda akses ke sumber daya di VPC

Antarmuka jaringan yang dibuat Lambda dikenal sebagai Hyperplane Elastic Network Interfaces, atau Hyperplane. ENIs Untuk mempelajari lebih lanjut tentang antarmuka jaringan ini, lihat [the section called “Memahami Antarmuka Jaringan Elastis Hyperplane \(\) ENIs”](#).

Anda dapat memberikan fungsi izin yang dibutuhkan dengan melampirkan [kebijakan AWS terkelola AWSLambdaVPCAccessExecutionRole](#) ke peran eksekusi fungsi Anda. Saat Anda membuat fungsi baru di konsol Lambda dan melampirkannya ke, VPC Lambda secara otomatis menambahkan kebijakan izin ini untuk Anda.

Jika Anda lebih suka membuat kebijakan IAM izin sendiri, pastikan untuk menambahkan semua izin berikut:

- EC2: CreateNetworkInterface
- ec2: DescribeNetworkInterfaces — Tindakan ini hanya berfungsi jika diizinkan di semua sumber daya ("Resource": "*").
- EC2: DescribeSubnets
- ec2: DeleteNetworkInterface — Jika Anda tidak menentukan ID sumber daya untuk DeleteNetworkInterface dalam peran eksekusi, fungsi Anda mungkin tidak dapat mengakses VPC. Entah menentukan ID sumber daya yang unik, atau sertakan semua sumber daya IDs, misalnya, "Resource": "arn:aws:ec2:us-west-2:123456789012:*/*".
- EC2: AssignPrivateIpAddresses
- EC2: UnassignPrivateIpAddresses

Perhatikan bahwa peran fungsi Anda hanya memerlukan izin ini untuk membuat antarmuka jaringan, bukan untuk memanggil fungsi Anda. Anda masih dapat menjalankan fungsi dengan sukses saat dilampirkan ke AmazonVPC, meskipun Anda menghapus izin ini dari peran eksekusi fungsi Anda.

Untuk melampirkan fungsi Anda ke VPC, Lambda juga perlu memverifikasi sumber daya jaringan menggunakan peran IAM pengguna Anda. Pastikan peran pengguna Anda memiliki IAM izin berikut:

- EC2: DescribeSecurityGroups
- EC2: DescribeSubnets
- EC2: DescribeVpcs

Note

EC2Izin Amazon yang Anda berikan untuk peran eksekusi fungsi Anda digunakan oleh layanan Lambda untuk melampirkan fungsi Anda ke file. VPC Namun, Anda juga secara implisit memberikan izin ini ke kode fungsi Anda. Ini berarti bahwa kode fungsi Anda dapat melakukan EC2 API panggilan Amazon ini. Untuk saran tentang mengikuti praktik terbaik keamanan, lihat [the section called “Praktik terbaik keamanan”](#).

Melampirkan fungsi Lambda ke Amazon VPC di Anda Akun AWS

Lampirkan fungsi Anda ke Amazon VPC di Anda Akun AWS dengan menggunakan konsol Lambda, atau. AWS CLI AWS SAM Jika Anda menggunakan AWS CLI atau AWS SAM, atau melampirkan fungsi yang ada ke VPC menggunakan konsol Lambda, pastikan bahwa peran eksekusi fungsi Anda memiliki izin yang diperlukan yang tercantum di bagian sebelumnya.

Fungsi Lambda tidak dapat terhubung langsung ke a VPC dengan penyewaan [instans khusus](#). Untuk terhubung ke sumber daya dalam dedicatedVPC, [mengintip ke detik VPC dengan penyewaan default](#).

Lambda console

Untuk melampirkan fungsi ke Amazon VPC saat Anda membuatnya

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih Buat fungsi.
2. Di bawah Informasi Dasar, untuk Nama fungsi, masukkan nama untuk fungsi Anda.
3. Konfigurasi VPC pengaturan untuk fungsi dengan melakukan hal berikut:
 - a. Perluas Pengaturan lanjutan.
 - b. Pilih Aktifkan VPC, lalu pilih fungsi yang ingin VPC Anda lampirkan.
 - c. (Opsional) Untuk mengizinkan [IPv6lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
 - d. Pilih subnet dan grup keamanan untuk membuat antarmuka jaringan. Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok. IPv6 CIDR

Note

Untuk mengakses sumber daya privat, sambungkan fungsi Anda ke subnet privat. Jika fungsi Anda membutuhkan akses internet, lihat [the section called “Akses internet untuk VPC fungsi”](#). Menghubungkan fungsi ke subnet publik tidak memberikan akses internet atau alamat IP publik.

4. Pilih Buat fungsi.

Untuk melampirkan fungsi yang ada ke Amazon VPC

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.
2. Pilih tab Konfigurasi, lalu pilih VPC.
3. Pilih Edit.
4. Di bawah VPC, pilih Amazon tempat VPC Anda ingin melampirkan fungsi Anda.
5. (Opsional) Untuk mengizinkan [IPv6 lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
6. Pilih subnet dan grup keamanan untuk membuat antarmuka jaringan. Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok IPv6 CIDR

Note

Untuk mengakses sumber daya privat, sambungkan fungsi Anda ke subnet privat. Jika fungsi Anda membutuhkan akses internet, lihat [the section called “Akses internet untuk VPC fungsi”](#). Menghubungkan fungsi ke subnet publik tidak memberikan akses internet atau alamat IP publik.

7. Pilih Simpan.**AWS CLI**

Untuk melampirkan fungsi ke Amazon VPC saat Anda membuatnya

- Untuk membuat fungsi Lambda dan melampirkannya ke VPC, jalankan perintah berikut `CLI create-function`.

```
aws lambda create-function --function-name my-function \
--runtime nodejs20.x --handler index.js --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/lambda-role \
--vpc-config
  Ipv6AllowedForDualStack=true,SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a03
```

Tentukan subnet dan grup keamanan Anda sendiri dan atur `Ipv6AllowedForDualStack` ke `true` atau `false` sesuai dengan kasus penggunaan Anda.

Untuk melampirkan fungsi yang ada ke Amazon VPC

- Untuk melampirkan fungsi yang ada ke aVPC, jalankan CLI `update-function-configuration` perintah berikut.

```
aws lambda update-function-configuration --function-name my-function \
--vpc-config Ipv6AllowedForDualStack=true,
  SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a036,SecurityGroupIds=sg-0859123
```

Untuk melepaskan fungsi Anda dari a VPC

- Untuk melepaskan fungsi Anda dari aVPC, jalankan `update-function-configuration` CLI perintah berikut dengan daftar VPC subnet dan grup keamanan kosong.

```
aws lambda update-function-configuration --function-name my-function \
--vpc-config SubnetIds=[],SecurityGroupIds=[]
```

AWS SAM

Untuk melampirkan fungsi Anda ke VPC

- Untuk melampirkan fungsi Lambda ke AmazonVPC, tambahkan `VpcConfig` properti ke definisi fungsi Anda seperti yang ditunjukkan pada contoh template berikut. Untuk informasi selengkapnya tentang properti ini, lihat [AWS: :Lambda: :Function VpcConfig](#) di Panduan AWS CloudFormation Pengguna (AWS SAM `VpcConfig` properti diteruskan langsung ke `VpcConfig` properti sumber daya). AWS CloudFormation `AWS::Lambda::Function`

```
AWSTemplateFormatVersion: '2010-09-09'  
Transform: AWS::Serverless-2016-10-31
```

Resources:**MyFunction:**

```
Type: AWS::Serverless::Function
```

Properties:

```
CodeUri: ./lambda_function/
```

```
Handler: lambda_function.handler
```

```
Runtime: python3.12
```

VpcConfig:

```
SecurityGroupIds:
```

- !Ref MySecurityGroup

```
SubnetIds:
```

- !Ref MySubnet1

- !Ref MySubnet2

Policies:

- AWSLambdaVPCLambdaAccessExecutionRole

MySecurityGroup:

```
Type: AWS::EC2::SecurityGroup
```

Properties:

```
GroupDescription: Security group for Lambda function
```

```
VpcId: !Ref MyVPC
```

MySubnet1:

```
Type: AWS::EC2::Subnet
```

Properties:

```
VpcId: !Ref MyVPC
```

```
CidrBlock: 10.0.1.0/24
```

MySubnet2:

```
Type: AWS::EC2::Subnet
```

Properties:

```
VpcId: !Ref MyVPC
```

```
CidrBlock: 10.0.2.0/24
```

MyVPC:

```
Type: AWS::EC2::VPC
```

Properties:

```
CidrBlock: 10.0.0.0/16
```

Untuk informasi selengkapnya tentang mengonfigurasi VPC akun Anda AWS SAM, lihat [AWS:EC2:: VPC](#) di Panduan AWS CloudFormation Pengguna.

Akses internet saat dilampirkan ke VPC

Secara default, fungsi Lambda memiliki akses ke internet publik. Ketika Anda melampirkan fungsi Anda ke aVPC, itu hanya dapat mengakses sumber daya yang tersedia di dalamnya VPC. Untuk memberikan akses fungsi Anda ke internet, Anda juga perlu mengkonfigurasi VPC untuk memiliki akses internet. Untuk mempelajari selengkapnya, lihat [the section called “Akses internet untuk VPC fungsi”](#).

IPv6 dukungan

Fungsi Anda dapat terhubung ke sumber daya dalam VPC subnet dual-stack over. IPv6 Opsi ini dimatikan secara default. Untuk mengizinkan IPv6 lalu lintas keluar, gunakan konsol atau `--vpc-config Ipv6AllowedForDualStack=true` opsi dengan fungsi atau [perintah buat. update-function-configuration](#)

Note

Untuk memungkinkan IPv6 lalu lintas keluar di aVPC, semua subnet yang terhubung ke fungsi harus subnet dual-stack. Lambda tidak mendukung IPv6 koneksi keluar untuk subnet IPv6 -only di aVPC, IPv6 koneksi keluar untuk fungsi yang tidak terhubung ke VPC, atau koneksi masuk menggunakan endpoint (). IPv6 VPC AWS PrivateLink

Anda dapat memperbarui kode fungsi Anda untuk secara eksplisit terhubung ke sumber daya subnet. IPv6 Contoh Python berikut membuka soket dan menghubungkan ke server. IPv6

Example — Connect ke IPv6 server

```
def connect_to_server(event, context):
    server_address = event['host']
    server_port = event['port']
    message = event['message']
    run_connect_to_server(server_address, server_port, message)

def run_connect_to_server(server_address, server_port, message):
```

```
sock = socket.socket(socket.AF_INET6, socket.SOCK_STREAM, 0)
try:
    # Send data
    sock.connect((server_address, int(server_port), 0, 0))
    sock.sendall(message.encode())
    BUFF_SIZE = 4096
    data = b''
    while True:
        segment = sock.recv(BUFF_SIZE)
        data += segment
        # Either 0 or end of data
        if len(segment) < BUFF_SIZE:
            break
    return data
finally:
    sock.close()
```

Praktik terbaik untuk menggunakan Lambda dengan Amazon VPCs

Untuk memastikan bahwa VPC konfigurasi Lambda Anda memenuhi pedoman praktik terbaik, ikuti saran di bagian berikut.

Praktik terbaik keamanan

Untuk melampirkan fungsi Lambda Anda ke aVPC, Anda perlu memberikan peran eksekusi fungsi Anda sejumlah izin AmazonEC2. Izin ini diperlukan untuk membuat antarmuka jaringan yang digunakan fungsi Anda untuk mengakses sumber daya di VPC. Namun, izin ini juga secara implisit diberikan ke kode fungsi Anda. Ini berarti bahwa kode fungsi Anda memiliki izin untuk melakukan EC2 API panggilan Amazon ini.

Untuk mengikuti prinsip akses hak istimewa paling rendah, tambahkan kebijakan penolakan seperti contoh berikut ke peran eksekusi fungsi Anda. Kebijakan ini mencegah fungsi Anda melakukan panggilan ke Amazon EC2 APIs yang digunakan layanan Lambda untuk melampirkan fungsi Anda ke file VPC.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNetworkInterface",
```



```

        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
    ],
    "Resource": [ "*" ],
    "Condition": {
        "ArnEquals": {
            "lambda:SourceFunctionArn": [
                "arn:aws:lambda:us-west-2:123456789012:function:my_function"
            ]
        }
    }
}
]
}
}

```

AWS menyediakan [grup keamanan](#) dan [Daftar Kontrol Akses jaringan \(ACLs\)](#) untuk meningkatkan keamanan di jaringan Anda VPC. Grup keamanan mengontrol lalu lintas masuk dan keluar untuk sumber daya Anda, dan jaringan ACLs mengontrol lalu lintas masuk dan keluar untuk subnet Anda. Grup keamanan menyediakan kontrol akses yang cukup untuk sebagian besar subnet. Anda dapat menggunakan jaringan ACLs jika Anda menginginkan lapisan keamanan tambahan untuk Anda VPC. Untuk panduan umum tentang praktik terbaik keamanan saat menggunakan Amazon VPCs, lihat [Praktik terbaik keamanan untuk Anda VPC](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Praktik terbaik kinerja

Ketika Anda melampirkan fungsi Anda ke VPC, Lambda memeriksa untuk melihat apakah ada sumber daya jaringan yang tersedia (Hyperplane ENI) yang dapat digunakan untuk terhubung. Hyperplane ENIs dikaitkan dengan kombinasi tertentu dari kelompok keamanan dan VPC subnet. Jika Anda telah melampirkan satu fungsi ke aVPC, menentukan subnet dan grup keamanan yang sama saat Anda melampirkan fungsi lain berarti Lambda dapat berbagi sumber daya jaringan dan menghindari kebutuhan untuk membuat Hyperplane baru. ENI Untuk informasi selengkapnya tentang Hyperplane ENIs dan siklus hidupnya, lihat [the section called “Memahami Antarmuka Jaringan Elastis Hyperplane \(\) ENIs”](#)

Memahami Antarmuka Jaringan Elastis Hyperplane () ENIs

Hyperplane ENI adalah sumber daya terkelola yang bertindak sebagai antarmuka jaringan antara fungsi Lambda Anda dan sumber daya yang Anda inginkan untuk terhubung ke fungsi Anda.

Layanan Lambda membuat dan mengelola ini ENIs secara otomatis ketika Anda melampirkan fungsi Anda ke file VPC

Hyperplane ENIs tidak langsung terlihat oleh Anda, dan Anda tidak perlu mengkonfigurasi atau mengelolanya. Namun, mengetahui cara kerjanya dapat membantu Anda memahami perilaku fungsi Anda saat Anda melampirkannya ke fileVPC.

Pertama kali Anda melampirkan fungsi ke VPC menggunakan subnet tertentu dan kombinasi grup keamanan, Lambda membuat Hyperplane. ENI Fungsi lain di akun Anda yang menggunakan kombinasi subnet dan grup keamanan yang sama juga dapat menggunakan iniENI. Jika memungkinkan, Lambda menggunakan kembali yang ada ENIs untuk mengoptimalkan pemanfaatan sumber daya dan meminimalkan pembuatan yang baru. ENIs Setiap Hyperplane ENI mendukung hingga 65.000 koneksi/port. Jika jumlah koneksi melebihi batas ini, Lambda menskalakan jumlah secara ENIs otomatis berdasarkan lalu lintas jaringan dan persyaratan konkurensi.

Untuk fungsi baru, saat Lambda membuat HyperplaneENI, fungsi Anda tetap dalam status Pending dan Anda tidak dapat memanggилnya. Fungsi Anda beralih ke status Aktif hanya ketika Hyperplane ENI siap, yang dapat memakan waktu beberapa menit. Untuk fungsi yang ada, Anda tidak dapat melakukan operasi tambahan yang menargetkan fungsi, seperti membuat versi atau memperbarui kode fungsi, tetapi Anda dapat terus memanggil versi fungsi sebelumnya.

Note

Jika fungsi Lambda tetap mengganggu selama 30 hari, Lambda merebut kembali ENIs Hyperplane yang tidak digunakan dan menyetel status fungsi ke idle. Upaya pemanggilan berikutnya akan gagal, dan fungsi memasuki kembali status Pending sampai Lambda menyelesaikan pembuatan atau alokasi Hyperplane. ENI Untuk informasi selengkapnya tentang status fungsi Lambda, lihat. [the section called “Status fungsi”](#)

Menggunakan tombol IAM kondisi untuk VPC pengaturan

Anda dapat menggunakan kunci kondisi khusus Lambda untuk VPC pengaturan guna memberikan kontrol izin tambahan untuk fungsi Lambda Anda. Misalnya, Anda dapat mengharuskan semua fungsi di organisasi Anda terhubung ke fileVPC. Anda juga dapat menentukan subnet dan grup keamanan yang dapat dan tidak dapat digunakan oleh pengguna fungsi.

Lambda mendukung kunci kondisi berikut dalam IAM kebijakan:

- lambda: VpcIds — Izinkan atau tolak satu atau lebih VPCs.
- lambda: SubnetIds — Izinkan atau tolak satu atau lebih subnet.
- lambda: SecurityGroupIds — Izinkan atau tolak satu atau lebih grup keamanan.

API Operasi Lambda [CreateFunction](#) dan [UpdateFunctionConfiguration](#) mendukung kunci kondisi ini. Untuk informasi selengkapnya tentang menggunakan kunci kondisi dalam IAM kebijakan, lihat [Elemen IAM JSON Kebijakan: Kondisi](#) dalam Panduan IAM Pengguna.

Tip

Jika fungsi Anda sudah menyertakan VPC konfigurasi dari API permintaan sebelumnya, Anda dapat mengirim `UpdateFunctionConfiguration` permintaan tanpa VPC konfigurasi.

Contoh kebijakan dengan tombol kondisi untuk VPC pengaturan

Contoh berikut menunjukkan cara menggunakan tombol kondisi untuk VPC pengaturan. Setelah Anda membuat pernyataan kebijakan dengan batasan yang diinginkan, tambahkan pernyataan kebijakan untuk pengguna atau peran target.

Pastikan bahwa pengguna hanya menerapkan fungsi VPC -connected

Untuk memastikan bahwa semua pengguna hanya menerapkan fungsi VPC -connected, Anda dapat menolak operasi pembuatan dan pembaruan fungsi yang tidak menyertakan ID yang valid VPC.

Perhatikan bahwa VPC ID bukan parameter input untuk `UpdateFunctionConfiguration` permintaan `CreateFunction` atau. Lambda mengambil nilai VPC ID berdasarkan parameter subnet dan grup keamanan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceVPCFunction",
      "Action": [
        "lambda:CreateFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

```

    "Condition": {
      "Null": {
        "lambda:VpcIds": "true"
      }
    }
  }
]
}

```

Menolak akses pengguna ke grup tertentu VPCs, subnet, atau keamanan

Untuk menolak akses pengguna ke spesifik VPCs, gunakan `StringEquals` untuk memeriksa nilai `lambda:VpcIds` kondisi. Contoh berikut menolak akses pengguna ke `vpc-1` dan `vpc-2`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVPC",
      "Action": [
        "lambda:CreateFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "lambda:VpcIds": ["vpc-1", "vpc-2"]
        }
      }
    }
  ]
}

```

Untuk menolak akses pengguna ke subnet tertentu, gunakan `StringEquals` untuk memeriksa nilai syarat `lambda:SubnetIds`. Contoh berikut menolak akses pengguna ke `subnet-1` dan `subnet-2`.

```

{
  "Sid": "EnforceOutOfSubnet",
  "Action": [
    "lambda:CreateFunction",

```

```

    "lambda:UpdateFunctionConfiguration"
  ],
  "Effect": "Deny",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "lambda:SubnetIds": ["subnet-1", "subnet-2"]
    }
  }
}

```

Untuk menolak akses pengguna ke grup keamanan tertentu, gunakan `StringEquals` untuk memeriksa nilai syarat `lambda:SecurityGroupIds`. Contoh berikut menolak akses pengguna ke `sg-1` dan `sg-2`.

```

{
  "Sid": "EnforceOutOfSecurityGroups",
  "Action": [
    "lambda:CreateFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Effect": "Deny",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
    }
  }
}

```

Izinkan pengguna untuk membuat dan memperbarui fungsi dengan VPC pengaturan tertentu

Untuk memungkinkan pengguna mengakses spesifik VPCs, gunakan `StringEquals` untuk memeriksa nilai `lambda:VpcIds` kondisi. Contoh berikut mengizinkan pengguna mengakses `vpc-1` dan `vpc-2`.

```

{
  "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Sid": "EnforceStayInSpecificVpc",
    "Action": [
      "lambda:CreateFunction",
      "lambda:UpdateFunctionConfiguration"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "lambda:VpcIds": ["vpc-1", "vpc-2"]
      }
    }
  }
]

```

Untuk mengizinkan pengguna mengakses subnet tertentu, gunakan `StringEquals` untuk memeriksa nilai syarat `lambda:SubnetIds`. Contoh berikut mengizinkan pengguna mengakses subnet-1 dan subnet-2.

```

{
  "Sid": "EnforceStayInSpecificSubnets",
  "Action": [
    "lambda:CreateFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "lambda:SubnetIds": ["subnet-1", "subnet-2"]
    }
  }
}

```

Untuk mengizinkan pengguna mengakses grup keamanan tertentu, gunakan `StringEquals` untuk memeriksa nilai syarat `lambda:SecurityGroupIds`. Contoh berikut mengizinkan pengguna mengakses sg-1 dan sg-2.

```

{

```

```
"Sid": "EnforceStayInSpecificSecurityGroup",
"Action": [
  "lambda:CreateFunction",
  "lambda:UpdateFunctionConfiguration"
],
"Effect": "Allow",
"Resource": "*",
"Condition": {
  "ForAllValues:StringEquals": {
    "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
  }
}
]
```

VPCtutorial

Dalam tutorial berikut, Anda menghubungkan fungsi Lambda ke sumber daya di Anda. VPC

- [Tutorial: Menggunakan fungsi Lambda untuk mengakses Amazon RDS di Amazon VPC](#)
- [Tutorial: Mengonfigurasi fungsi Lambda untuk mengakses Amazon di ElastiCache Amazon VPC](#)

Aktifkan akses internet untuk fungsi VPC Lambda yang terhubung

Secara default, fungsi Lambda berjalan di Lambda-managed VPC yang memiliki akses internet. Untuk mengakses sumber daya VPC di akun Anda, Anda dapat menambahkan VPC konfigurasi ke suatu fungsi. Ini membatasi fungsi untuk sumber daya di dalamnya VPC, kecuali VPC memiliki akses internet. Halaman ini menjelaskan cara menyediakan akses internet ke fungsi Lambda yang VPC terhubung.

Saya VPC belum punya

Buat VPC

VPCAlur kerja Buat membuat semua VPC sumber daya yang diperlukan untuk fungsi Lambda untuk mengakses internet publik dari subnet pribadi, termasuk subnet, gateway, gateway internet NAT, dan entri tabel rute.

Untuk membuat VPC

1. Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di dasbor, pilih Buat VPC.
3. Agar Sumber Daya dapat dibuat, pilih, VPC dan lainnya.
4. Konfigurasi VPC
 - a. Untuk pembuatan otomatis tag Nama, masukkan nama untuk VPC
 - b. Untuk IPv4 CIDR blok, Anda dapat menyimpan saran default, atau sebagai alternatif Anda dapat memasukkan CIDR blok yang diperlukan oleh aplikasi atau jaringan Anda.
 - c. Jika aplikasi Anda berkomunikasi dengan menggunakan IPv6 alamat, pilih IPv6 CIDR blok, blok yang disediakan Amazon IPv6 CIDR.
5. Konfigurasi subnet
 - a. Untuk Jumlah Availability Zone, pilih 2. Kami merekomendasikan setidaknya dua AZs untuk ketersediaan tinggi.
 - b. Untuk Jumlah subnet publik, pilih 2.
 - c. Untuk Jumlah subnet pribadi, pilih 2.
 - d. Anda dapat menyimpan CIDR blok default untuk subnet publik, atau sebagai alternatif Anda dapat memperluas Kustomisasi blok subnet dan memasukkan CIDR blok. CIDR Untuk informasi selengkapnya, lihat [CIDR Blok subnet](#).

6. Untuk NATgateway, pilih 1 per AZ untuk meningkatkan ketahanan.
7. Untuk gateway internet Egress saja, pilih Ya jika Anda memilih untuk menyertakan blok. IPv6 CIDR
8. Untuk VPCtitik akhir, pertahankan default (S3 Gateway). Tidak ada biaya untuk opsi ini. Untuk informasi selengkapnya, lihat [Jenis VPC titik akhir untuk Amazon S3](#).
9. Untuk DNSopsi, pertahankan pengaturan default.
10. Pilih Buat VPC.

Konfigurasi fungsi Lambda

Untuk mengkonfigurasi VPC saat Anda membuat fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih Buat fungsi.
3. Di bawah Informasi Dasar, untuk Nama fungsi, masukkan nama untuk fungsi Anda.
4. Perluas Pengaturan lanjutan.
5. Pilih Aktifkan VPC, lalu pilih fileVPC.
6. (Opsional) Untuk mengizinkan [IPv6lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
7. Untuk Subnet, pilih semua subnet pribadi. Subnet pribadi dapat mengakses internet melalui NAT gateway. Menghubungkan fungsi ke subnet publik tidak memberikan akses internet.

Note

Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok. IPv6 CIDR

8. Untuk grup Keamanan, pilih grup keamanan yang memungkinkan lalu lintas keluar.
9. Pilih Buat fungsi.

Lambda secara otomatis membuat peran eksekusi dengan kebijakan

[AWSLambdaVPCAccessExecutionRole](#) AWS terkelola. Izin dalam kebijakan ini hanya diperlukan untuk membuat antarmuka jaringan elastis untuk VPC konfigurasi, bukan untuk menjalankan fungsi Anda. Untuk menerapkan izin hak istimewa paling sedikit, Anda dapat menghapus


AWSLambdaVPCAccessExecutionRolekebijakan dari peran eksekusi setelah membuat fungsi dan konfigurasi. VPC Untuk informasi selengkapnya, lihat [Diperlukan izin IAM](#).

Untuk mengkonfigurasi VPC untuk fungsi yang ada

Untuk menambahkan VPC konfigurasi ke fungsi yang ada, peran eksekusi fungsi harus memiliki [izin untuk membuat dan mengelola antarmuka jaringan elastis](#).

Kebijakan [AWSLambdaVPCAccessExecutionRole](#) AWS terkelola mencakup izin yang diperlukan. Untuk menerapkan izin hak istimewa paling sedikit, Anda dapat menghapus AWSLambdaVPCAccessExecutionRolekebijakan dari peran eksekusi setelah membuat konfigurasi. VPC

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Konfigurasi, lalu pilih VPC.
4. Di bawah VPC, pilih Edit.
5. PilihVPC.
6. (Opsional) Untuk mengizinkan [IPv6lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
7. Untuk Subnet, pilih semua subnet pribadi. Subnet pribadi dapat mengakses internet melalui NAT gateway. Menghubungkan fungsi ke subnet publik tidak memberikan akses internet.

 Note

Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok. IPv6 CIDR

8. Untuk grup Keamanan, pilih grup keamanan yang memungkinkan lalu lintas keluar.
9. Pilih Simpan.

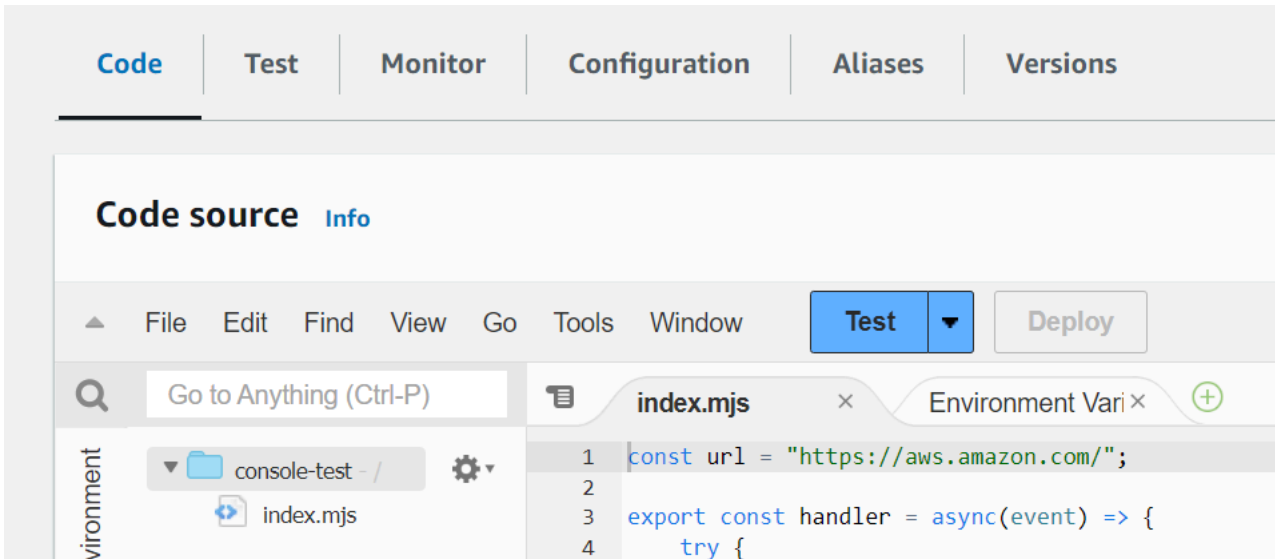
Uji fungsi

Gunakan kode contoh berikut untuk mengonfirmasi bahwa fungsi VPC -connected Anda dapat menjangkau internet publik. Jika berhasil, kode mengembalikan kode 200 status. Jika tidak berhasil, fungsi akan habis.

Node.js

Contoh ini menggunakan `fetch`, yang tersedia di `nodejs18.x` dan kemudian runtime.

1. Di panel Sumber kode di konsol Lambda, tempel kode berikut ke dalam file `index.mjs`. Fungsi membuat HTTP GET permintaan ke titik akhir publik dan mengembalikan kode HTTP respons untuk menguji apakah fungsi tersebut memiliki akses ke internet publik.

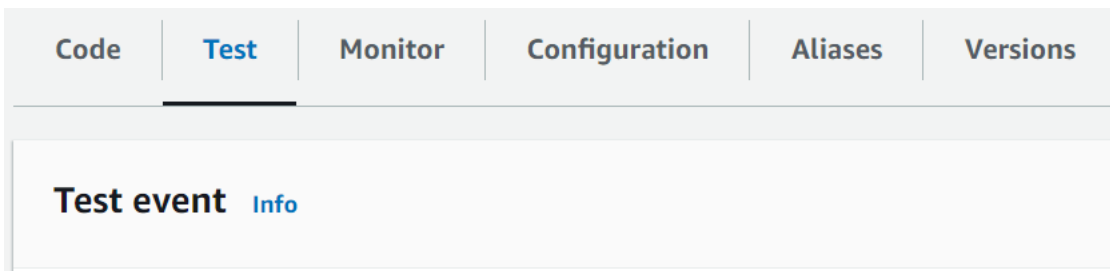


Example — HTTP permintaan dengan `async/await`

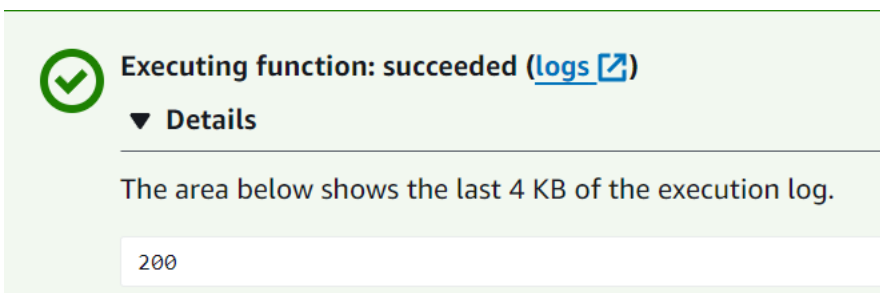
```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
  try {
    // fetch is available with Node.js 18 and later runtimes
    const res = await fetch(url);
    console.info("status", res.status);
    return res.status;
  }
  catch (e) {
    console.error(e);
    return 500;
  }
};
```

2. Pilih Deploy.
3. Pilih tab Uji.



4. Pilih Uji.
5. Fungsi mengembalikan kode 200 status. Ini berarti bahwa fungsi tersebut memiliki akses internet keluar.

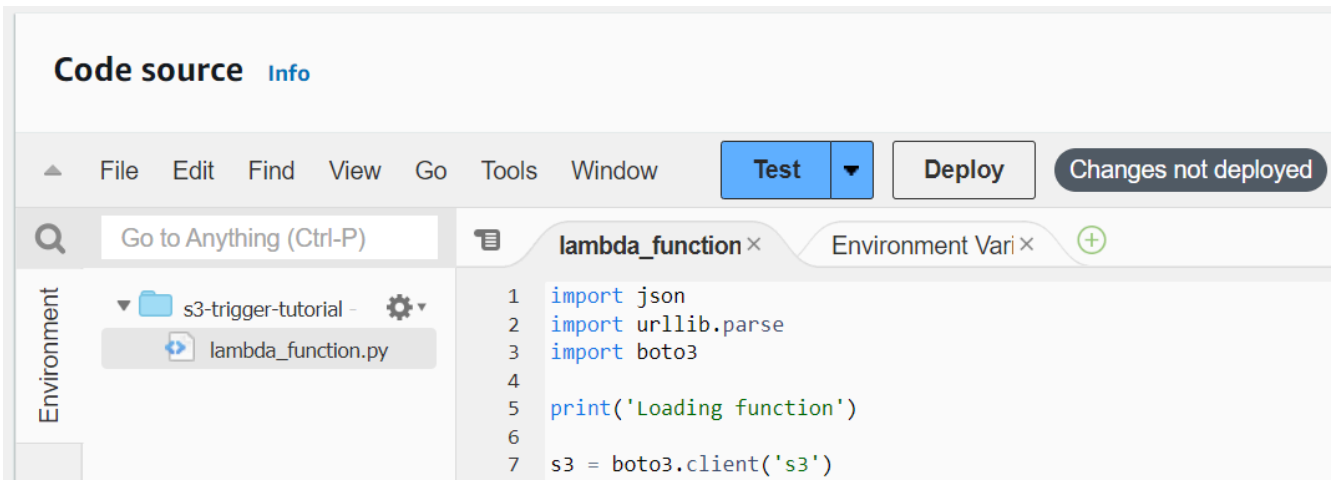


Jika fungsi tidak dapat menjangkau internet publik, Anda mendapatkan pesan kesalahan seperti ini:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12j1c-640a-8157-0249-9be825c2y110
Task timed out after 3.01 seconds"
}
```

Python

1. Di panel Sumber kode di konsol Lambda, tempel kode berikut ke dalam file `lambda_function.py`. Fungsi membuat HTTP GET permintaan ke titik akhir publik dan mengembalikan kode HTTP respons untuk menguji apakah fungsi tersebut memiliki akses ke internet publik.



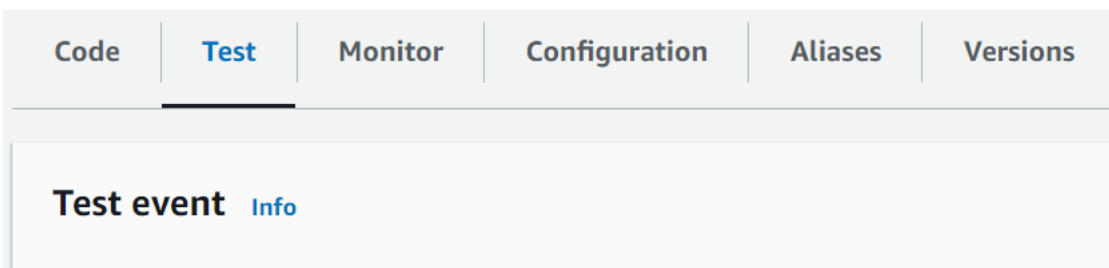
```

import urllib.request

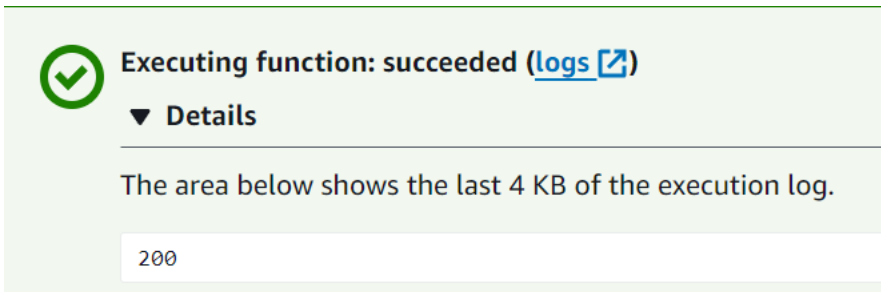
def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e

```

2. Pilih Deploy.
3. Pilih tab Uji.



4. Pilih Uji.
5. Fungsi mengembalikan kode 200 status. Ini berarti bahwa fungsi tersebut memiliki akses internet keluar.



Jika fungsi tidak dapat menjangkau internet publik, Anda mendapatkan pesan kesalahan seperti ini:

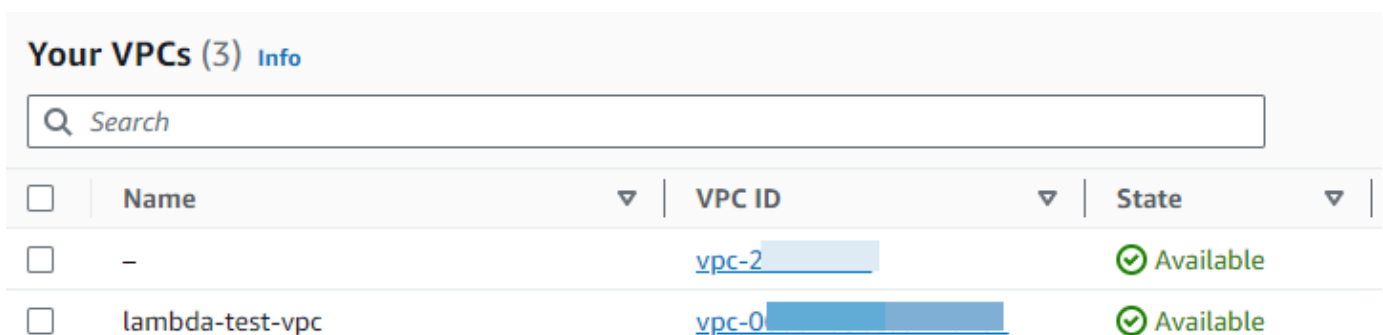
```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
Task timed out after 3.01 seconds"
}
```

Saya sudah memiliki VPC

Jika Anda sudah memiliki VPC tetapi Anda perlu mengonfigurasi akses internet publik untuk fungsi Lambda, ikuti langkah-langkah ini. Prosedur ini mengasumsikan bahwa Anda VPC memiliki setidaknya dua subnet. Jika Anda tidak memiliki dua subnet, lihat [Membuat subnet](#) di VPC Panduan Pengguna Amazon.

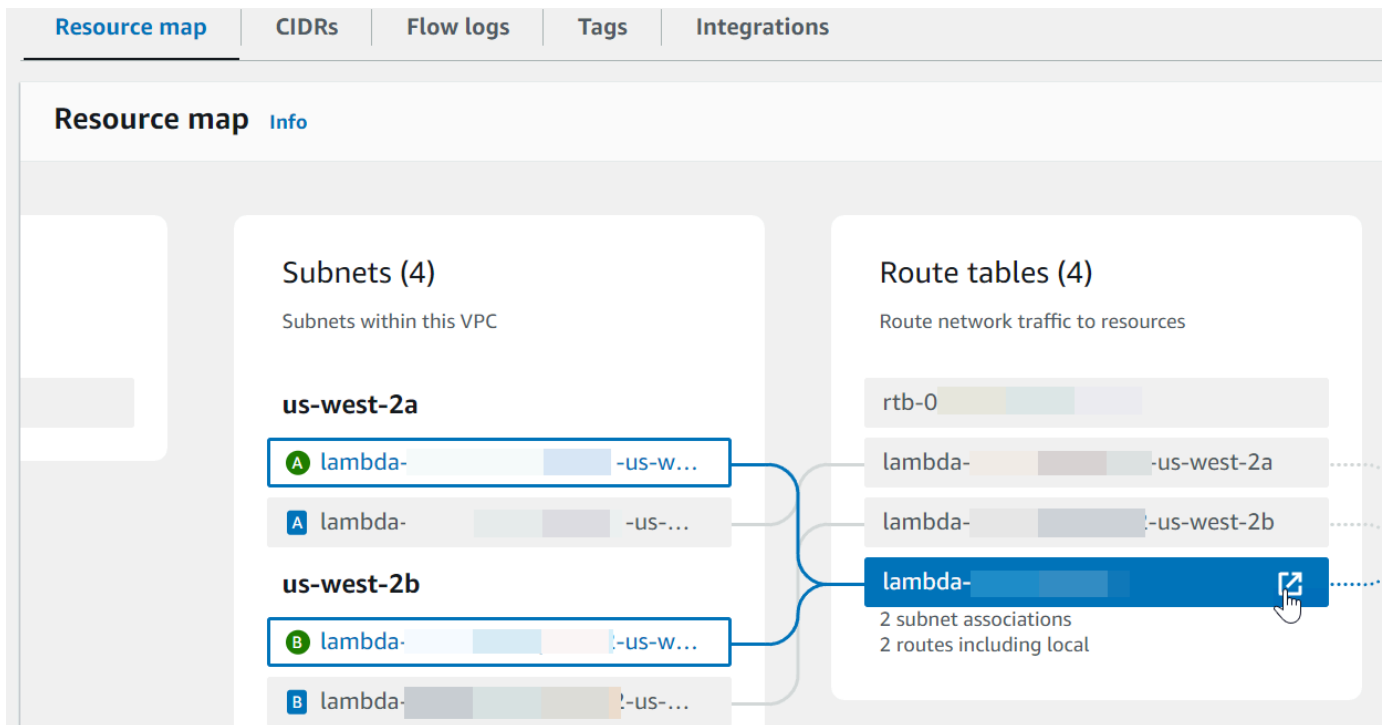
Verifikasi konfigurasi tabel rute

1. Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Pilih VPCID.



| <input type="checkbox"/> | Name | VPC ID | State |
|--------------------------|-----------------|--------|-----------|
| <input type="checkbox"/> | - | vpc-2 | Available |
| <input type="checkbox"/> | lambda-test-vpc | vpc-0 | Available |

3. Gulir ke bawah ke bagian Peta sumber daya. Perhatikan pemetaan tabel rute. Buka setiap tabel rute yang dipetakan ke subnet.



4. Gulir ke bawah ke tab Rute. Tinjau rute untuk menentukan apakah salah satu dari berikut ini benar. Masing-masing persyaratan ini harus dipenuhi oleh tabel rute terpisah.
 - Lalu lintas internet ($0.0.0.0/0$ untuk IPv4, $:::/0$ untuk IPv6) dirutekan ke gateway internet (`igw-xxxxxxxxxx`). Ini berarti bahwa subnet yang terkait dengan tabel rute adalah subnet publik.

Note

Jika subnet Anda tidak memiliki IPv6 CIDR blok, Anda hanya akan melihat IPv4 route ($0.0.0.0/0$).

Example tabel rute subnet publik

| Routes | Subnet associations | Edge associations | Route propagation | Tags |
|--|-----------------------|-------------------|-------------------|------|
| Routes (4) | | | | |
| <input type="text" value="Filter routes"/> | | | | |
| Destination | Target | Status | | |
| ::/0 | igw-0 | Active | | |
| ::/56 | local | Active | | |
| 0.0.0.0/0 | igw-0 | Active | | |
| /16 | local | Active | | |

- Lalu lintas terikat internet untuk IPv4 ($0.0.0.0/0$) dirutekan ke NAT gateway (`nat-xxxxxxxxxx`) yang terkait dengan subnet publik. Ini berarti bahwa subnet adalah subnet pribadi yang dapat mengakses internet melalui gateway. NAT

Note

Jika subnet Anda memiliki IPv6 CIDR blok, tabel rute juga harus merutekan IPv6 traffic ($::/0$) ke gateway internet () khusus egress-only. `eigw-xxxxxxxxxx` Jika subnet Anda tidak memiliki IPv6 CIDR blok, Anda hanya akan melihat IPv4 route ($0.0.0.0/0$).

Example tabel rute subnet pribadi

| Routes | Subnet associations | Edge associations | Route propagation | Tags |
|--|------------------------|-------------------|-------------------|------|
| Routes (4) | | | | |
| <input type="text" value="Filter routes"/> | | | | |
| Destination | Target | Status | | |
| ::/0 | eigw-0 | Active | | |
| ::/56 | local | Active | | |
| 0.0.0.0/0 | nat-0 | Active | | |
| /16 | local | Active | | |

- Ulangi langkah sebelumnya sampai Anda telah meninjau setiap tabel rute yang terkait dengan subnet di Anda VPC dan mengonfirmasi bahwa Anda memiliki tabel rute dengan gateway internet dan tabel rute dengan NAT gateway.

Jika Anda tidak memiliki dua tabel rute, satu dengan rute ke gateway internet dan satu dengan rute ke NAT gateway, ikuti langkah-langkah ini untuk membuat sumber daya dan entri tabel rute yang hilang.

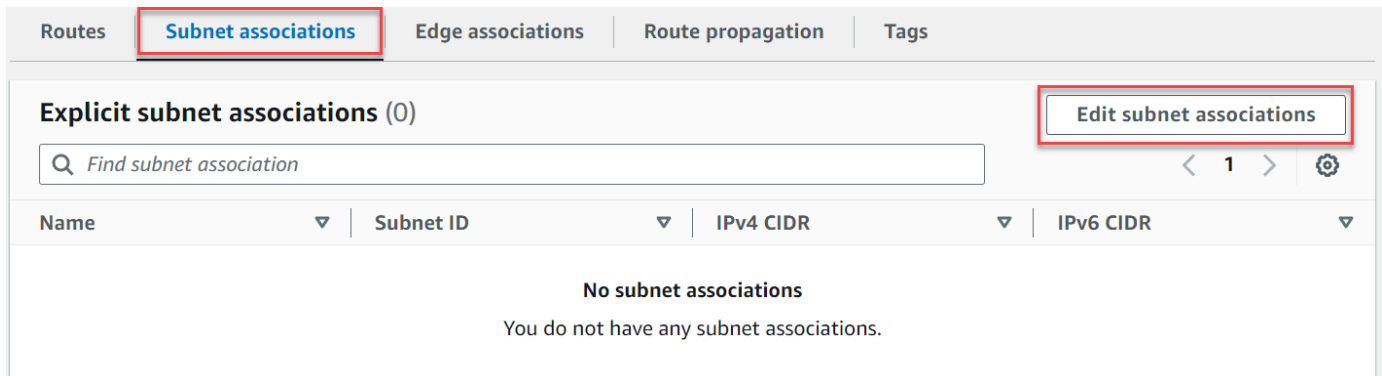
Membuat tabel rute

Ikuti langkah-langkah ini untuk membuat tabel rute dan mengaitkannya dengan subnet.

Untuk membuat tabel rute kustom menggunakan VPC konsol Amazon

- Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
- Di panel navigasi, pilih Tabel rute.
- Pilih Buat tabel rute.
- (Opsional) Untuk Nama, masukkan nama untuk tabel rute Anda.
- Untuk VPC, pilih AndaVPC.
- (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai tag.

7. Pilih Buat tabel rute.
8. Pada tab Pengaitan subnet, pilih Sunting pengaitan subnet.



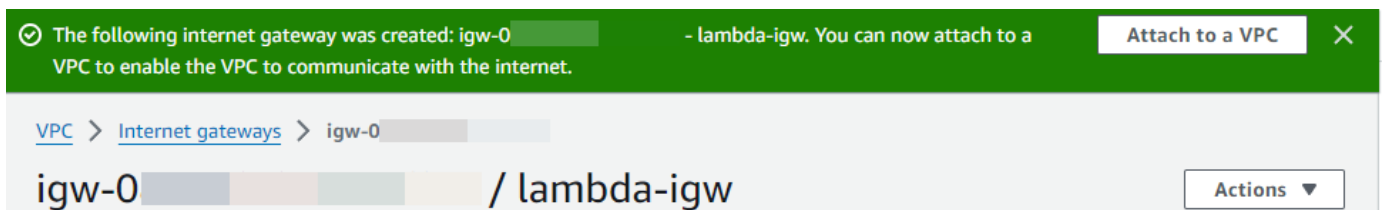
9. Pilih kotak centang untuk subnet untuk dikaitkan dengan tabel rute.
10. Pilih Simpan pengaitan.

Membuat gateway internet baru

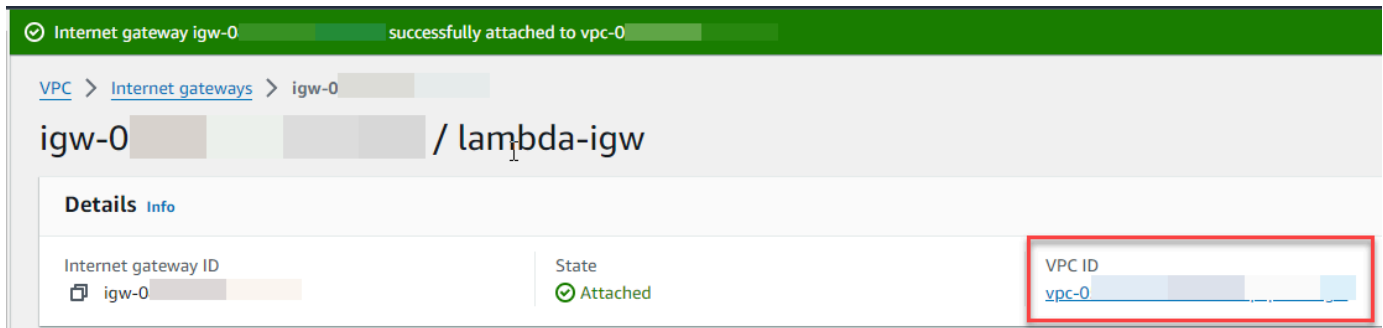
Ikuti langkah-langkah ini untuk membuat gateway internet, melampirkannya ke AndaVPC, dan menambahkannya ke tabel rute subnet publik Anda.

Untuk membuat gateway internet

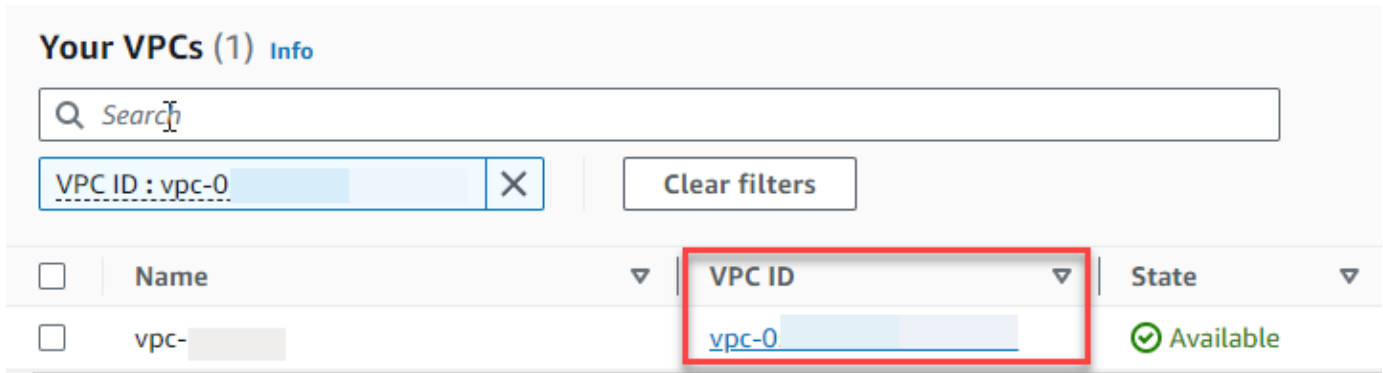
1. Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih gateway Internet.
3. Pilih Buat gateway internet.
4. (Opsional) Masukkan nama untuk gateway internet Anda.
5. (Opsional) Untuk menambahkan tag, pilih Tambahkan tag baru dan masukkan kunci tag dan nilai.
6. Pilih Buat gateway internet.
7. Pilih Lampirkan ke VPC dari spanduk di bagian atas layar, pilih yang tersediaVPC, lalu pilih Lampirkan gateway internet.



8. Pilih VPCID.



9. Pilih VPCID lagi untuk membuka halaman VPC detail.



10. Gulir ke bawah ke bagian Peta sumber daya dan kemudian pilih subnet. Detail subnet ditampilkan di tab baru.

The screenshot shows the AWS Resource map interface. At the top, there are navigation tabs: Resource map (selected), CIDRs, Flow logs, Tags, and Integrations. Below the tabs, the 'Resource map' section is active, showing a VPC and its associated subnets. The VPC is labeled 'lambda-' and has a 'Show details' link. The subnets are grouped by availability zone: 'us-west-2a' and 'us-west-2b'. Under 'us-west-2a', there are two subnets, the first of which is highlighted in blue and has a mouse cursor pointing to it. Under 'us-west-2b', there are two subnets, the first of which is highlighted in green.

11. Pilih tautan di bawah Tabel route.

The screenshot shows the AWS Subnet details page. The breadcrumb navigation is 'VPC > Subnets > subnet-'. The main heading is 'subnet-'. Below the heading, there is a 'Details' section with the following information:

| | | |
|-----------------------------------|------------------------------------|---------------------------------|
| Subnet ID subnet- | Subnet ARN arn:aws:ec2:us-west- | State Available |
| Available IPv4 addresses 4090 | IPv6 CIDR - | Availability Zone us-west-2b |
| Network border group us-west-2 | VPC | Route table rtb- |

12. Pilih ID tabel Route untuk membuka halaman detail tabel rute.

Route tables (1) Info

Find resources by attribute or tag

Route table ID : rtb-0 X Clear filters

| <input type="checkbox"/> | Name | Route table ID |
|--------------------------|------|----------------|
| <input type="checkbox"/> | - | rtb-0 |

13. Di bawah Rute, pilih Edit rute.

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both Edit routes

Filter routes

| Destination | Target | Status |
|-------------|--------|--------|
| 10.0.0.0/24 | local | Active |

14. Pilih Tambah rute, lalu masukkan $0.0.0.0/0$ di kotak Tujuan.

Edit routes

| Destination | Target | Status |
|----------------------|----------------------|--------|
| 10.0.0.0/24 | local | Active |
| <input type="text"/> | <input type="text"/> | - |

0.0.0.0/0
0.0.0.0/8
0.0.0.0/16

15. Untuk Target, pilih Internet gateway, lalu pilih gateway internet yang Anda buat sebelumnya. Jika subnet Anda memiliki IPv6 CIDR blok, Anda juga harus menambahkan rute $::/0$ ke gateway internet yang sama.

Edit routes

| Destination | Target |
|--|---|
| 10.0.0.0/24 | local |
| <input type="text" value="0.0.0.0/0"/> | <input type="text" value="local"/> |
| <input type="button" value="Add route"/> | <ul style="list-style-type: none">Carrier GatewayCore NetworkEgress Only Internet GatewayGateway Load Balancer EndpointInstanceInternet Gateway |

16. Pilih Simpan perubahan.

Buat NAT gateway

Ikuti langkah-langkah ini untuk membuat NAT gateway, mengaitkannya dengan subnet publik, dan kemudian menambahkannya ke tabel rute subnet pribadi Anda.

Untuk membuat NAT gateway dan mengaitkannya dengan subnet publik

1. Di panel navigasi, pilih NATgateway.
2. Pilih Buat NAT gateway.
3. (Opsional) Masukkan nama untuk NAT gateway Anda.
4. Untuk Subnet, pilih subnet publik di subnet Anda. VPC (Subnet publik adalah subnet yang memiliki rute langsung ke gateway internet dalam tabel rutanya.)

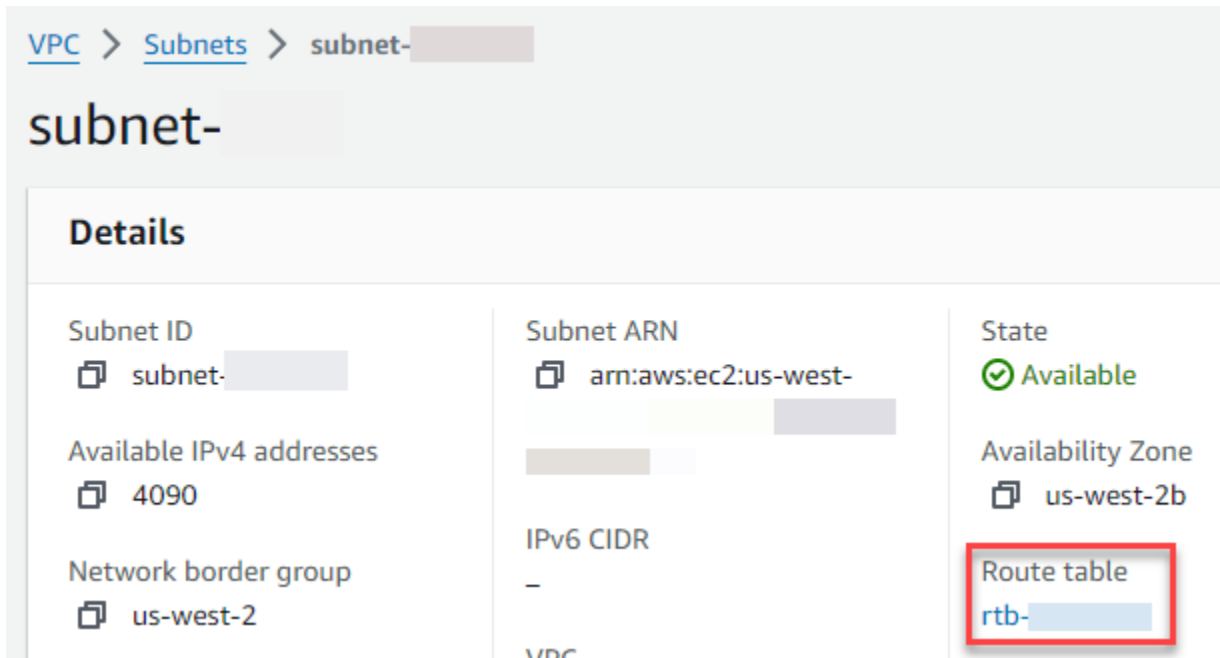
Note

NATgateway dikaitkan dengan subnet publik, tetapi entri tabel rute ada di subnet pribadi.

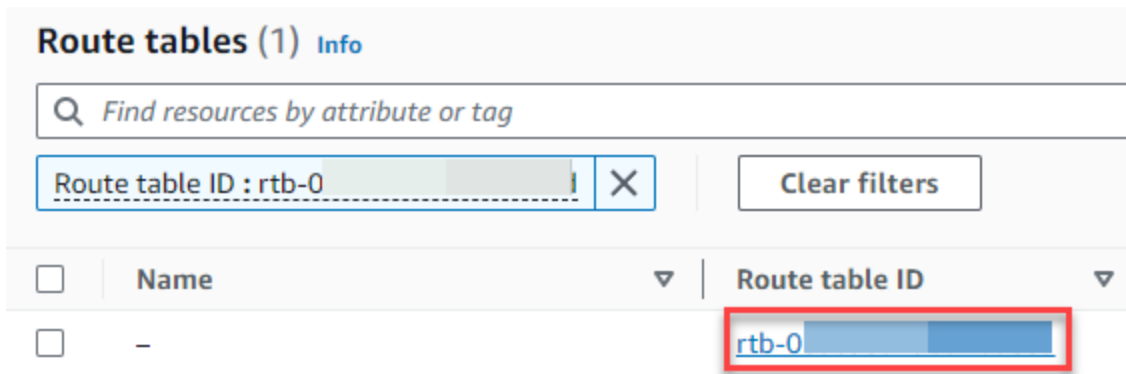
5. Untuk ID alokasi IP elastis, pilih alamat IP elastis atau pilih Alokasikan IP Elastis.
6. Pilih Buat NAT gateway.

Untuk menambahkan rute ke NAT gateway di tabel rute subnet pribadi

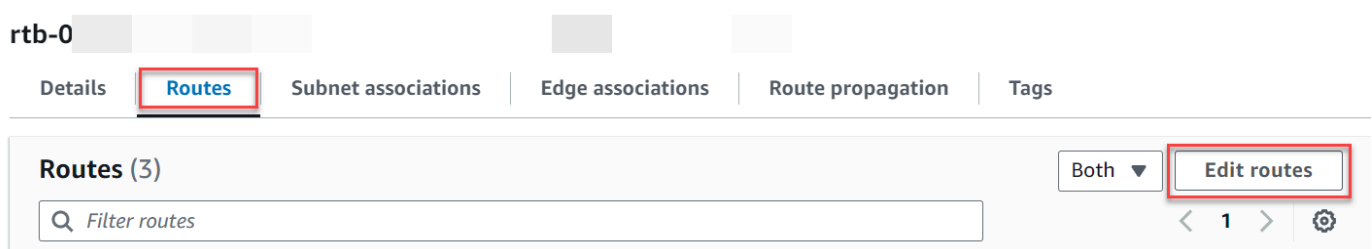
1. Di panel navigasi, pilih Pengguna.
2. Pilih subnet pribadi di AndaVPC. (Subnet pribadi adalah subnet yang tidak memiliki rute ke gateway internet di tabel rutenya.)
3. Pilih tautan di bawah Tabel rute.



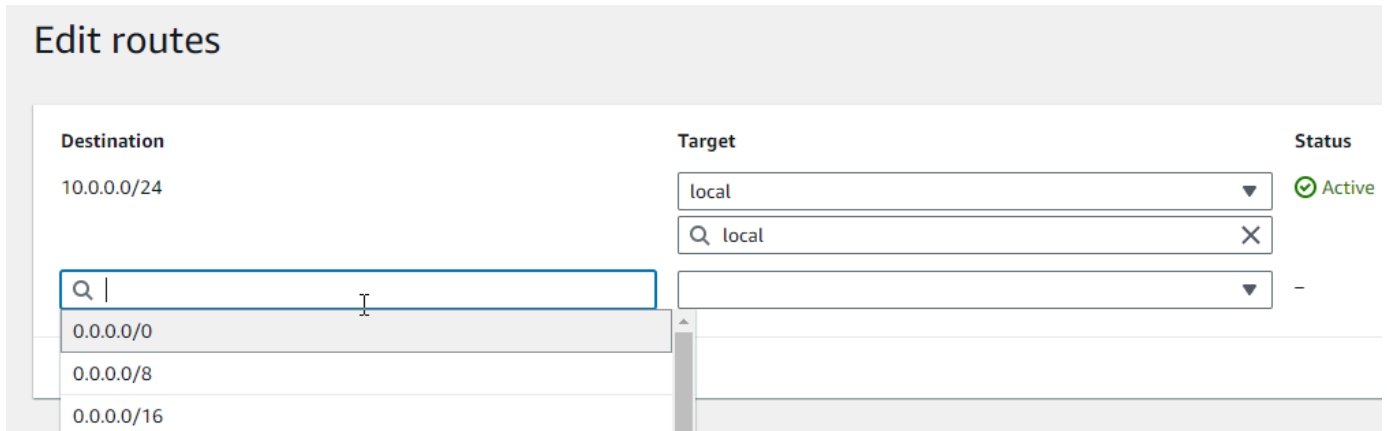
4. Pilih ID tabel Route untuk membuka halaman detail tabel rute.



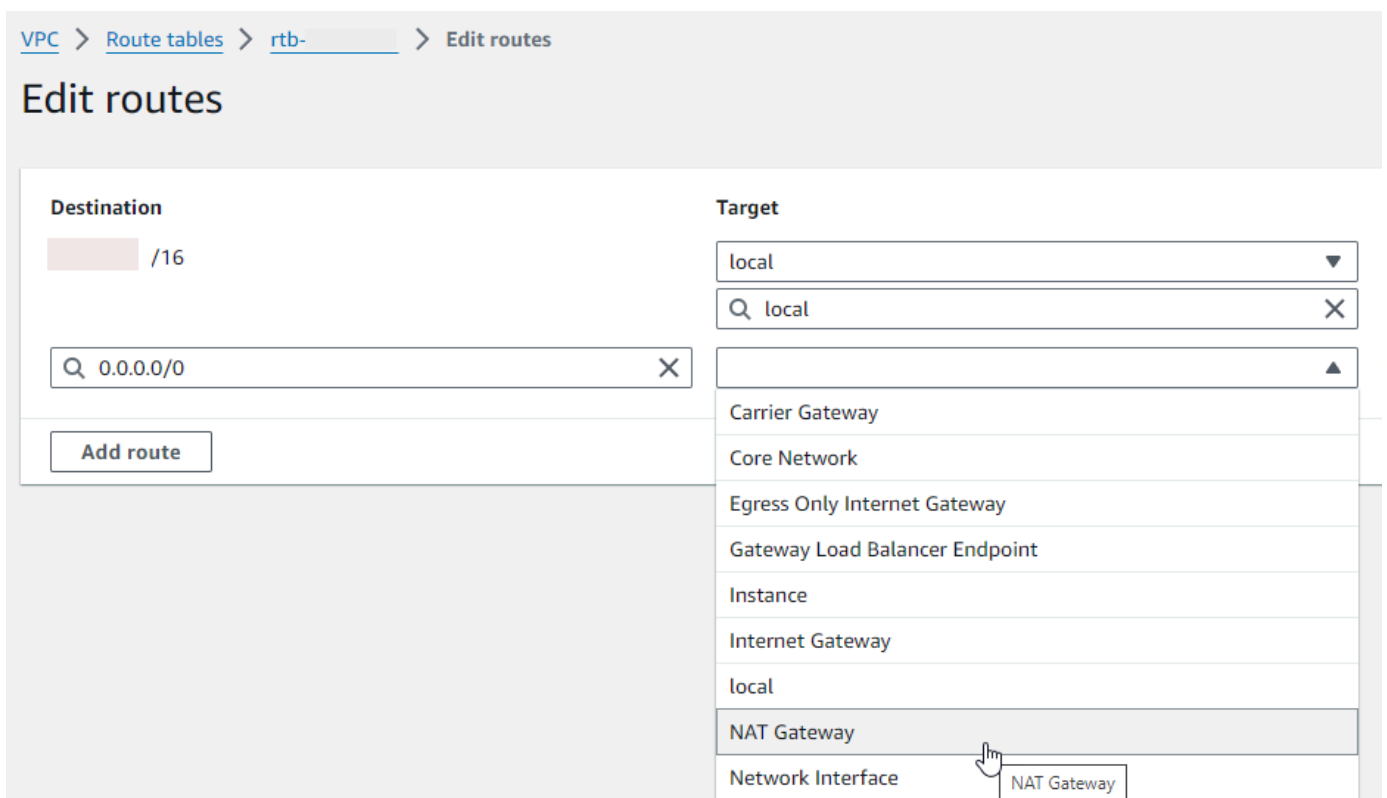
5. Gulir ke bawah dan pilih tab Rute, lalu pilih Edit rute



6. Pilih Tambah rute, lalu masukkan $0.0.0.0/0$ di kotak Tujuan.



7. Untuk Target, pilih NATgateway, lalu pilih NAT gateway yang Anda buat sebelumnya.



8. Pilih Simpan perubahan.

Buat gateway internet khusus egress (hanya) IPv6

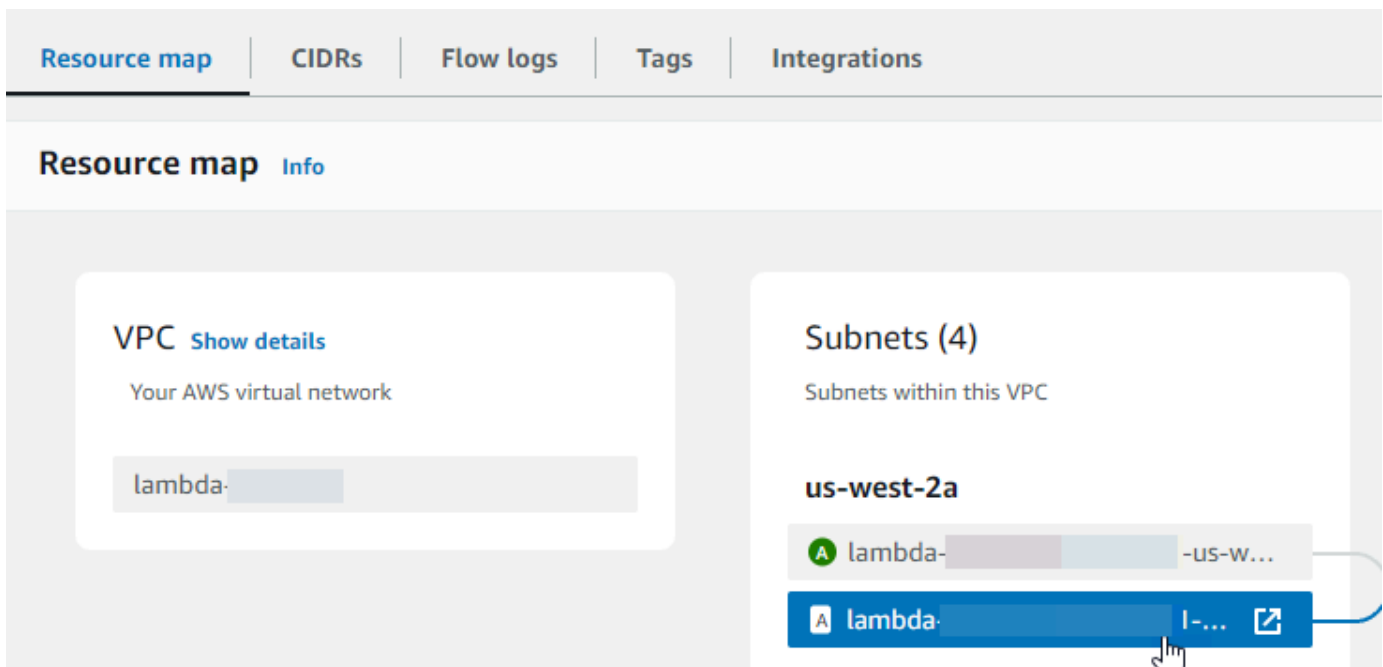
Ikuti langkah-langkah ini untuk membuat gateway internet khusus egress dan menambahkannya ke tabel rute subnet pribadi Anda.

Untuk membuat gateway internet egress-only

1. Di panel navigasi, pilih gateway internet khusus Egress.
2. Pilih Buat gateway internet hanya jalan keluar.
3. (Opsional) Masukkan nama.
4. Pilih VPC di mana untuk membuat gateway internet egress-only.
5. Pilih Buat gateway internet hanya jalan keluar.
6. Pilih tautan di bawah VPCID Terlampir.



7. Pilih tautan di bawah VPCID untuk membuka halaman VPC detail.
8. Gulir ke bawah ke bagian Peta sumber daya dan kemudian pilih subnet pribadi. (Subnet pribadi adalah subnet yang tidak memiliki rute ke gateway internet di tabel rutenya.) Detail subnet ditampilkan di tab baru.



9. Pilih tautan di bawah Tabel rute.

subnet-0 **-subnet-private1-us-west-2a**

Details

| | | |
|---|---|---|
| Subnet ID ☞ subnet- | Subnet ARN ☞ arn:aws:ec2:us-west- | State ✔ Available |
| Available IPv4 addresses ☞ 4090 | IPv6 CIDR ☞ :/64 | Availability Zone ☞ us-west-2a |
| Network border group ☞ us-west-2 | VPC vpc-0 | Route table rtb-0 west-2a |
| Default subnet No | Auto-assign public IPv4 address | Auto-assign IPv6 address |

10. Pilih ID tabel Route untuk membuka halaman detail tabel rute.

Route tables (1) Info

Find resources by attribute or tag

Route table ID : rtb-0 [X] Clear filters

| <input type="checkbox"/> | Name | Route table ID |
|--------------------------|------|----------------|
| <input type="checkbox"/> | - | rtb-0 |

11. Di bawah Rute, pilih Edit rute.

Routes (1) Both ▾ **Edit routes**

Filter routes

| Destination | Target | Status |
|-------------|--------|----------|
| 10.0.0.0/24 | local | ✔ Active |

12. Pilih Tambah rute, lalu masukkan : : /0 di kotak Tujuan.

Edit routes

| Destination | Target | Status |
|-------------|--------|----------|
| 10.0.0.0/24 | local | ✔ Active |
| 0.0.0.0/0 | local | - |
| 0.0.0.0/8 | - | - |
| 0.0.0.0/16 | - | - |

- Untuk Target, pilih Egress Only Internet Gateway, lalu pilih gateway yang Anda buat sebelumnya.

Edit routes

| Destination | Target | Status |
|-------------|------------------------------|--------|
| ::/56 | local | Active |
| 10.0.0.0/16 | local | Active |
| 0.0.0.0/0 | NAT Gateway | Active |
| ::/0 | Egress Only Internet Gateway | Active |

- Pilih Simpan perubahan.

Konfigurasi fungsi Lambda

Untuk mengkonfigurasi VPC saat Anda membuat fungsi

- Buka [halaman Fungsi](#) di konsol Lambda.
- Pilih Buat fungsi.
- Di bawah Informasi Dasar, untuk Nama fungsi, masukkan nama untuk fungsi Anda.
- Perluas Pengaturan lanjutan.
- Pilih Aktifkan VPC, lalu pilih fileVPC.
- (Opsional) Untuk mengizinkan [IPv6 lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
- Untuk Subnet, pilih semua subnet pribadi. Subnet pribadi dapat mengakses internet melalui NAT gateway. Menghubungkan fungsi ke subnet publik tidak memberikan akses internet.

Note

Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok IPv6 CIDR

- Untuk grup Keamanan, pilih grup keamanan yang memungkinkan lalu lintas keluar.

9. Pilih Buat fungsi.

Lambda secara otomatis membuat peran eksekusi dengan kebijakan [AWSLambdaVPCAccessExecutionRole](#) AWS terkelola. Izin dalam kebijakan ini hanya diperlukan untuk membuat antarmuka jaringan elastis untuk VPC konfigurasi, bukan untuk menjalankan fungsi Anda. Untuk menerapkan izin hak istimewa paling sedikit, Anda dapat menghapus [AWSLambdaVPCAccessExecutionRole](#) kebijakan dari peran eksekusi setelah membuat fungsi dan konfigurasi. VPC Untuk informasi selengkapnya, lihat [Diperlukan izin IAM](#).

Untuk mengkonfigurasi VPC untuk fungsi yang ada

Untuk menambahkan VPC konfigurasi ke fungsi yang ada, peran eksekusi fungsi harus memiliki [izin untuk membuat dan mengelola antarmuka jaringan elastis](#). Kebijakan [AWSLambdaVPCAccessExecutionRole](#) AWS terkelola mencakup izin yang diperlukan. Untuk menerapkan izin hak istimewa paling sedikit, Anda dapat menghapus [AWSLambdaVPCAccessExecutionRole](#) kebijakan dari peran eksekusi setelah membuat konfigurasi. VPC

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Konfigurasi, lalu pilih VPC.
4. Di bawah VPC, pilih Edit.
5. Pilih VPC.
6. (Opsional) Untuk mengizinkan [IPv6 lalu lintas keluar](#), pilih Izinkan lalu IPv6 lintas untuk subnet dual-stack.
7. Untuk Subnet, pilih semua subnet pribadi. Subnet pribadi dapat mengakses internet melalui NAT gateway. Menghubungkan fungsi ke subnet publik tidak memberikan akses internet.

Note

Jika Anda memilih Izinkan IPv6 lalu lintas untuk subnet dual-stack, semua subnet yang dipilih harus memiliki IPv4 CIDR blok dan blok. IPv6 CIDR

8. Untuk grup Keamanan, pilih grup keamanan yang memungkinkan lalu lintas keluar.
9. Pilih Simpan.

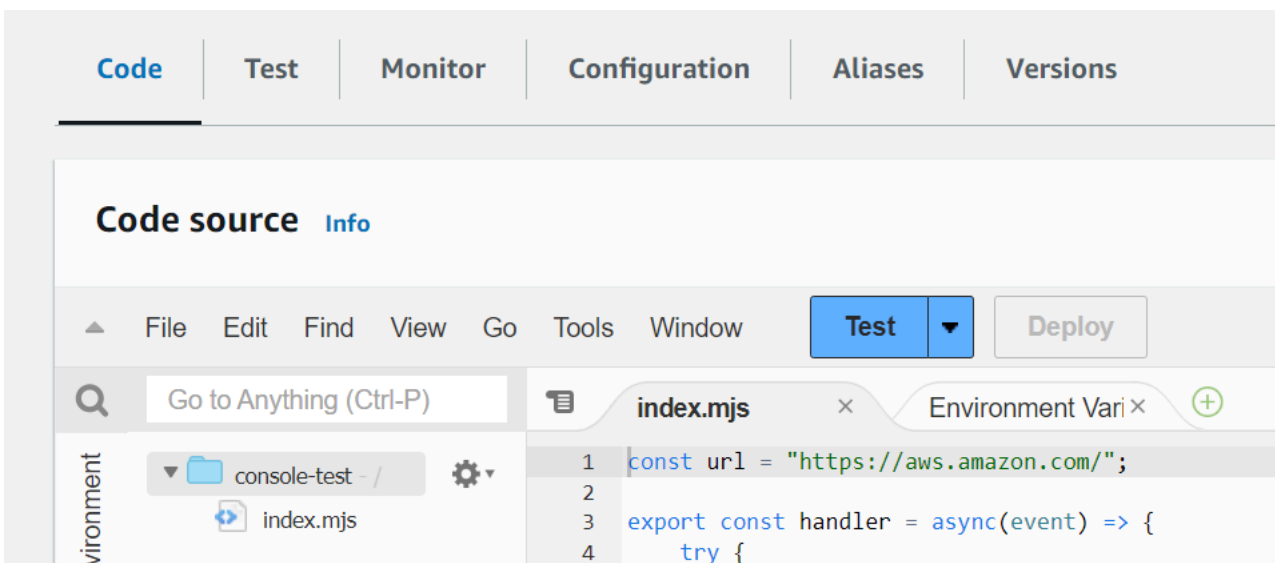
Uji fungsi

Gunakan kode contoh berikut untuk mengonfirmasi bahwa fungsi VPC -connected Anda dapat menjangkau internet publik. Jika berhasil, kode mengembalikan kode 200 status. Jika tidak berhasil, fungsi akan habis.

Node.js

Contoh ini menggunakan `fetch`, yang tersedia di `nodejs18.x` dan kemudian runtime.

1. Di panel Sumber kode di konsol Lambda, tempel kode berikut ke dalam file `index.mjs`. Fungsi membuat HTTP GET permintaan ke titik akhir publik dan mengembalikan kode HTTP respons untuk menguji apakah fungsi tersebut memiliki akses ke internet publik.



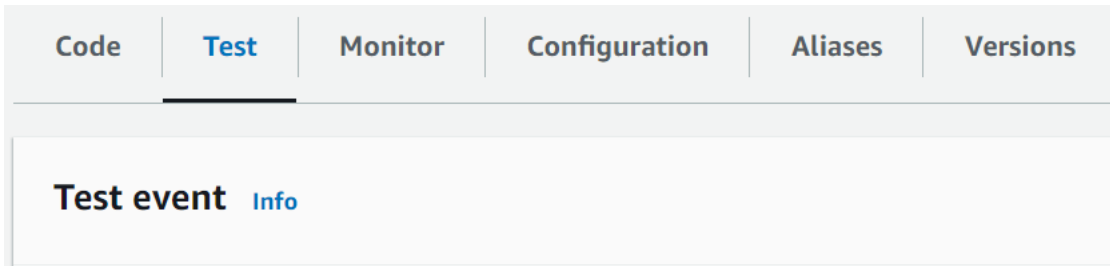
Example — HTTP permintaan dengan `async/await`

```
const url = "https://aws.amazon.com/";

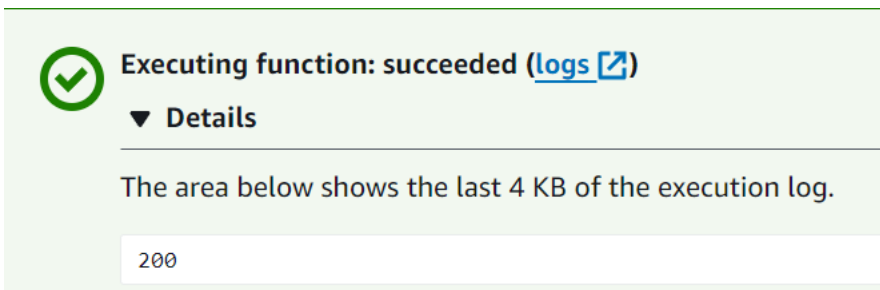
export const handler = async(event) => {
  try {
    // fetch is available with Node.js 18 and later runtimes
    const res = await fetch(url);
    console.info("status", res.status);
    return res.status;
  }
  catch (e) {
    console.error(e);
    return 500;
  }
}
```

```
}
};
```

2. Pilih Deploy.
3. Pilih tab Uji.



4. Pilih Uji.
5. Fungsi mengembalikan kode 200 status. Ini berarti bahwa fungsi tersebut memiliki akses internet keluar.

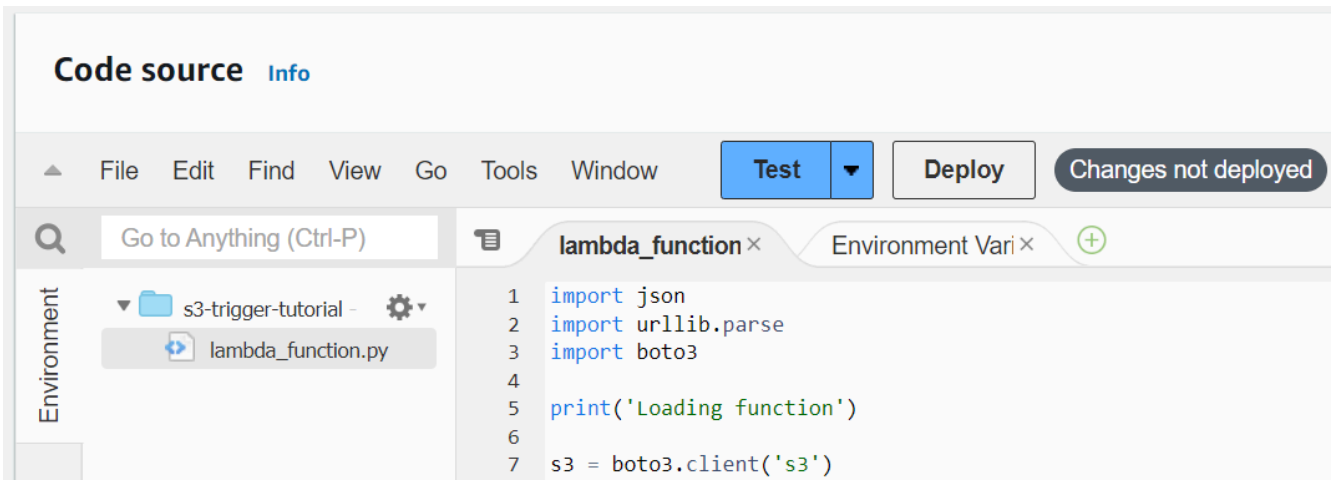


Jika fungsi tidak dapat menjangkau internet publik, Anda mendapatkan pesan kesalahan seperti ini:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
  Task timed out after 3.01 seconds"
}
```

Python

1. Di panel Sumber kode di konsol Lambda, tempel kode berikut ke dalam file `lambda_function.py`. Fungsi membuat HTTP GET permintaan ke titik akhir publik dan mengembalikan kode HTTP respons untuk menguji apakah fungsi tersebut memiliki akses ke internet publik.



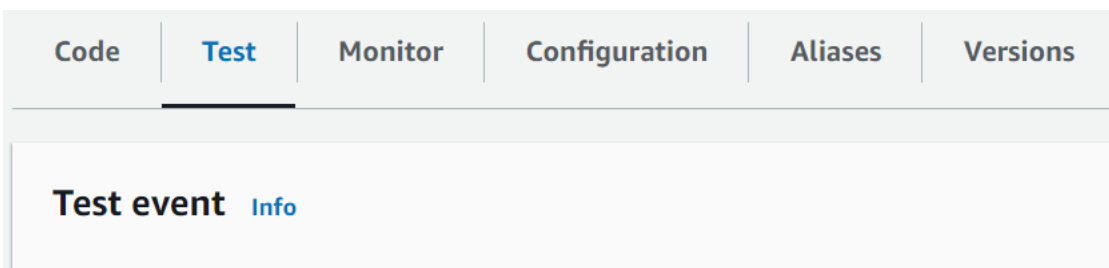
```

import urllib.request

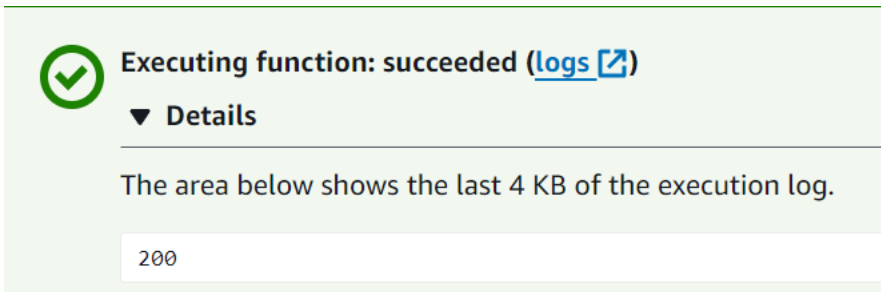
def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e

```

2. Pilih Deploy.
3. Pilih tab Uji.



4. Pilih Uji.
5. Fungsi mengembalikan kode 200 status. Ini berarti bahwa fungsi tersebut memiliki akses internet keluar.



Executing function: succeeded ([logs](#))

▼ Details

The area below shows the last 4 KB of the execution log.

200

Jika fungsi tidak dapat menjangkau internet publik, Anda mendapatkan pesan kesalahan seperti ini:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
  Task timed out after 3.01 seconds"
}
```


Menghubungkan VPC titik akhir antarmuka masuk untuk Lambda

Jika Anda menggunakan Amazon Virtual Private Cloud (AmazonVPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi antara Anda VPC dan Lambda. Anda dapat menggunakan koneksi ini untuk mengaktifkan fungsi Lambda Anda tanpa menyeberangi internet publik.

Untuk membuat koneksi pribadi antara Anda VPC dan Lambda, buat titik akhir [antarmuka VPC](#). Endpoint antarmuka didukung oleh [AWS PrivateLink](#), yang memungkinkan Anda mengakses Lambda secara pribadi APIs tanpa gateway internet, NAT perangkat, koneksi, atau VPN koneksi. AWS Direct Connect Instans di Anda VPC tidak memerlukan alamat IP publik untuk berkomunikasi dengan LambdaAPIs. Lalu lintas antara Anda VPC dan Lambda tidak meninggalkan jaringan. AWS

Setiap titik akhir antarmuka diwakili oleh satu atau lebih [antarmuka jaringan elastis](#) dalam subnet Anda. Antarmuka jaringan menyediakan alamat IP privat yang berfungsi sebagai titik masuk untuk lalu lintas ke Lambda.

Bagian

- [Pertimbangan untuk titik akhir antarmuka Lambda](#)
- [Membuat titik akhir antarmuka untuk Lambda](#)
- [Membuat kebijakan titik akhir antarmuka untuk Lambda](#)

Pertimbangan untuk titik akhir antarmuka Lambda

Sebelum menyiapkan titik akhir antarmuka untuk Lambda, pastikan untuk [meninjau properti dan batasan titik akhir Antarmuka di Panduan](#) Pengguna Amazon VPC.

Anda dapat menghubungi salah satu API operasi Lambda dari Anda. VPC Misalnya, Anda dapat menjalankan fungsi Lambda dengan memanggil dari Invoke API dalam. VPC Untuk daftar lengkap LambdaAPIs, lihat [Tindakan](#) dalam referensi Lambda. API

use1-az3 adalah Wilayah kapasitas terbatas untuk fungsi LambdaVPC. Anda tidak boleh menggunakan subnet di zona ketersediaan ini dengan fungsi Lambda Anda karena ini dapat mengakibatkan pengurangan redundansi zona jika terjadi pemadaman.

Tetap aktif untuk koneksi yang persisten

Lambda menghapus koneksi idle dari waktu ke waktu, jadi Anda harus menggunakan arahan yang tetap aktif untuk mempertahankan koneksi yang persisten. Mencoba menggunakan kembali koneksi

idle saat mengaktifkan fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi Tetap Aktif di Node.js](#) dalam AWS SDK for JavaScript Panduan Developer.

Pertimbangan Tagihan

Tidak ada biaya tambahan untuk mengakses fungsi Lambda melalui titik akhir antarmuka. Untuk informasi selengkapnya tentang harga Lambda, lihat [AWS Lambda Harga](#).

Harga standar untuk AWS PrivateLink berlaku untuk titik akhir antarmuka untuk Lambda. AWS Akun Anda ditagih untuk setiap jam, titik akhir antarmuka disediakan di setiap Availability Zone dan untuk data yang diproses melalui titik akhir antarmuka. Untuk informasi selengkapnya tentang harga titik akhir antarmuka, lihat [AWS PrivateLink harga](#).

VPC Pertimbangan Peering

Anda dapat menghubungkan yang lain VPCs ke titik akhir VPC dengan antarmuka menggunakan [VPC peering](#). VPC Peering adalah koneksi jaringan antara dua VPCs. Anda dapat membuat koneksi VPC peering antara dua Anda sendiri VPCs, atau dengan VPC AWS akun lain. VPCs Bisa juga di dua AWS wilayah yang berbeda.

Lalu lintas antara peered VPCs tetap di AWS jaringan dan tidak melintasi internet publik. Setelah VPCs di-peer, sumber daya seperti instans Amazon Elastic Compute Cloud (Amazon EC2), instans Amazon Relational Database Service (RDS Amazon), VPC atau fungsi Lambda yang diaktifkan VPCs di keduanya dapat mengakses Lambda melalui titik akhir antarmuka API yang dibuat di salah satu VPCs

Membuat titik akhir antarmuka untuk Lambda

Anda dapat membuat titik akhir antarmuka untuk Lambda menggunakan konsol VPC Amazon atau () AWS Command Line Interface .AWS CLI Untuk informasi selengkapnya, lihat [Membuat titik akhir antarmuka](#) di Panduan VPC Pengguna Amazon.

Untuk membuat titik akhir antarmuka untuk Lambda (konsol)

1. Buka [halaman Endpoints](#) dari VPC konsol Amazon.
2. Pilih Buat Titik Akhir.
3. Untuk Kategori layanan, verifikasi bahwa AWS layanan dipilih.

4. Untuk Nama Layanan, pilih `com.amazonaws.region.lambda`. Verifikasi bahwa Jenis adalah Antarmuka.
5. Pilih a VPC dan subnet.
6. Untuk mengaktifkan privat DNS untuk titik akhir antarmuka, pilih kotak centang Aktifkan DNS Nama. Kami menyarankan Anda mengaktifkan DNS nama pribadi untuk VPC AWS layanan titik akhir Anda. Ini memastikan bahwa permintaan yang menggunakan titik akhir layanan publik, seperti permintaan yang dibuat melalui AWS SDK, diselesaikan ke titik VPC akhir Anda.
7. Untuk Grup keamanan, pilih satu grup keamanan atau lebih.
8. Pilih Buat titik akhir.

Untuk menggunakan DNS opsi pribadi, Anda harus mengatur `enableDnsHostnames` dan `enableDnsSupportattributes` dari AndaVPC. Untuk informasi selengkapnya, lihat [Melihat dan memperbarui DNS dukungan untuk Anda VPC](#) di Panduan VPC Pengguna Amazon. Jika Anda mengaktifkan private DNS untuk titik akhir antarmuka, Anda dapat membuat API permintaan ke Lambda menggunakan nama DNS defaultnya untuk Wilayah, misalnya, `.lambda.us-east-1.amazonaws.com` Untuk titik akhir layanan lainnya, lihat [Titik akhir layanan dan kuota](#) di Referensi Umum AWS

Untuk informasi selengkapnya, lihat [Mengakses layanan melalui titik akhir antarmuka](#) di VPCPanduan Pengguna Amazon.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan AWS CloudFormation, lihat VPCendpoint sumber daya [AWS:EC2::](#) di AWS CloudFormation Panduan Pengguna.

Untuk membuat titik akhir antarmuka untuk Lambda (AWS CLI)

Gunakan [create-vpc-endpoint](#) perintah dan tentukan VPC ID, tipe VPC titik akhir (antarmuka), nama layanan, subnet yang akan menggunakan titik akhir, dan grup keamanan untuk dikaitkan dengan antarmuka jaringan titik akhir. Sebagai contoh:

```
aws ec2 create-vpc-endpoint
  --vpc-id vpc-ec43eb89
  --vpc-endpoint-type Interface
  --service-name com.amazonaws.us-east-1.lambda
  --subnet-id subnet-abababab
  --security-group-id sg-1a2b3c4d
```

Membuat kebijakan titik akhir antarmuka untuk Lambda

Untuk mengontrol siapa yang dapat menggunakan titik akhir antarmuka Anda dan fungsi Lambda mana yang dapat diakses pengguna, Anda dapat melampirkan kebijakan titik akhir ke titik akhir Anda. Kebijakan menentukan informasi berikut ini:

- Prinsip yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan oleh prinsip.
- Sumber daya yang dapat digunakan untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol akses ke layanan dengan VPC titik akhir](#) di Panduan VPC Pengguna Amazon.

Kebijakan titik akhir antarmuka untuk tindakan Lambda

Berikut adalah contoh kebijakan titik akhir untuk Lambda. Jika dilampirkan ke titik akhir, kebijakan ini memungkinkan MyUser pengguna untuk mengaktifkan fungsi my-function.

Note

Anda perlu memasukkan fungsi yang memenuhi syarat dan tidak memenuhi syarat ARN dalam sumber daya.

```
{
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/MyUser"
      },
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:us-east-2:123456789012:function:my-function",
        "arn:aws:lambda:us-east-2:123456789012:function:my-function:*"
      ]
    }
  ]
}
```

```
]
}
```

Mengonfigurasi akses sistem file untuk fungsi Lambda

Anda dapat mengonfigurasi fungsi untuk memasang sistem file Amazon Elastic File System (AmazonEFS) ke direktori lokal. Dengan AmazonEFS, kode fungsi Anda dapat mengakses dan memodifikasi sumber daya bersama dengan aman dan pada konkurensi tinggi.

Bagian-bagian

- [Peran eksekusi dan izin pengguna](#)
- [Mengonfigurasi sistem file dan titik akses](#)
- [Menyambung ke sistem file \(konsol\)](#)

Peran eksekusi dan izin pengguna

Jika sistem file tidak memiliki kebijakan yang dikonfigurasi pengguna AWS Identity and Access Management (IAM), EFS gunakan kebijakan default yang memberikan akses penuh ke klien mana pun yang dapat terhubung ke sistem file menggunakan target pemasangan sistem file. Jika sistem file memiliki IAM kebijakan yang dikonfigurasi pengguna, peran eksekusi fungsi Anda harus memiliki izin yang `benarelasticfilesystem`.

Izin peran eksekusi

- sistem file elastis: ClientMount
- elasticfilesystem: ClientWrite (tidak diperlukan untuk koneksi hanya-baca)

Izin ini disertakan dalam kebijakan `AmazonElasticFileSystemClientReadWriteAccesssterkelola`. Selain itu, peran eksekusi Anda harus memiliki [izin yang diperlukan untuk terhubung ke sistem file. VPC](#)

Saat Anda mengonfigurasi sistem file, Lambda menggunakan izin Anda untuk memverifikasi target pemasangan. Untuk mengonfigurasi fungsi untuk terhubung ke sistem file, pengguna Anda memerlukan izin berikut:

Izin pengguna

- sistem file elastis: DescribeMountTargets

Mengonfigurasi sistem file dan titik akses

Buat sistem file di Amazon EFS dengan target mount di setiap Availability Zone yang terhubung ke fungsi Anda. Untuk performa dan ketahanan, gunakan setidaknya dua Availability Zone. Misalnya, dalam konfigurasi sederhana Anda dapat memiliki VPC dengan dua subnet pribadi di Availability Zones terpisah. Fungsi ini terhubung ke subnet dan target pemasangan tersedia pada masing-masing subnet. Pastikan bahwa NFS lalu lintas (port 2049) diizinkan oleh kelompok keamanan yang digunakan oleh fungsi dan memasang target.

Note

Saat Anda membuat sistem file, Anda memilih mode performa yang tidak dapat diubah lagi nantinya. Mode tujuan umum memiliki latensi yang lebih rendah, dan mode Max I/O mendukung throughput maksimum yang lebih tinggi dan. IOPS Untuk bantuan memilih, lihat [EFSSkinerja Amazon](#) di Panduan Pengguna Amazon Elastic File System.

Titik akses menghubungkan setiap instans fungsi ke target pemasangan yang tepat untuk Availability Zone yang terhubung dengannya. Untuk performa terbaik, buat titik akses dengan alur non-akar, dan batasi jumlah file yang Anda buat di setiap direktori. Contoh berikut membuat direktori bernama my-function pada sistem file dan menetapkan ID pemilik menjadi 1001 dengan izin direktori standar (755).

Example konfigurasi titik akses

- Nama – files
- ID Pengguna – 1001
- ID Grup – 1001
- Jalur – /my-function
- Izin – 755
- ID pengguna pemilik – 1001
- ID pengguna grup – 1001

Saat fungsi menggunakan titik akses, fungsi diberikan ID pengguna 1001 dan memiliki akses penuh ke direktori.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna Amazon Elastic File System:

- [Membuat sumber daya untuk Amazon EFS](#)
- [Bekerja dengan pengguna, grup, dan izin](#)

Menyambung ke sistem file (konsol)

Sebuah fungsi terhubung ke sistem file melalui jaringan lokal di fileVPC. Subnet yang terhubung dengan fungsi Anda dapat berupa subnet yang sama yang berisi titik pemasangan untuk sistem file Anda, atau subnet di Availability Zone yang sama yang dapat merutekan NFS lalu lintas (port 2049) ke sistem file.

Note

Jika fungsi Anda belum terhubung ke aVPC, lihat [Memberikan fungsi Lambda akses ke sumber daya di Amazon VPC](#).

Untuk mengonfigurasi akses sistem file

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi, lalu pilih Sistem file.
4. Di bagian Sistem file, pilih Tambahkan sistem file.
5. Konfigurasi properti berikut:
 - EFSfile system — Titik akses untuk sistem file yang samaVPC.
 - Jalur pemasangan lokal – Lokasi tempat sistem file dipasang pada fungsi Lambda, memulai dengan /mnt/.

Harga

Amazon EFS mengenakan biaya untuk penyimpanan dan throughput, dengan tarif yang bervariasi menurut kelas penyimpanan. Untuk detailnya, lihat [EFSharga Amazon](#).

Lambda mengenakan biaya untuk transfer data antara VPCs Ini hanya berlaku jika fungsi Anda VPC diintip ke yang lain VPC dengan sistem file. Tarifnya sama dengan transfer EC2 data Amazon antara VPCs di Wilayah yang sama. Untuk detailnya, lihat [Harga Lambda](#).

Buat alias untuk fungsi Lambda

Anda dapat membuat alias untuk fungsi Lambda Anda. Alias Lambda adalah penunjuk ke versi fungsi yang dapat Anda perbarui. Pengguna fungsi dapat mengakses versi fungsi menggunakan alias Amazon Resource Name (ARN). Saat menerapkan versi baru, Anda dapat memperbarui alias untuk menggunakan versi baru, atau membagi lalu lintas di antara dua versi.

Console

Untuk membuat alias menggunakan konsol

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Alias, lalu pilih Buat alias.
4. Di halaman Buat alias, lakukan hal berikut:
 - a. Masukkan Nama untuk alias.
 - b. (Opsional) Masukkan Deskripsi untuk alias.
 - c. Untuk Versi, pilih versi fungsi yang ingin Anda tunjuk.
 - d. (Opsional) Untuk mengonfigurasi routing pada alias, perluas Alias tertimbang. Untuk informasi selengkapnya, lihat [Buat konfigurasi routing untuk alias Lambda](#).
 - e. Pilih Simpan.

AWS CLI

Untuk membuat alias menggunakan AWS Command Line Interface (AWS CLI), gunakan perintah [create-alias](#).

```
aws lambda create-alias \  
  --function-name my-function \  
  --name alias-name \  
  --function-version version-number \  
  --description " "
```

Untuk mengubah alias untuk mengarahkan versi baru fungsi, gunakan perintah [update-alias](#).

```
aws lambda update-alias \  
  --function-name my-function \  
  --function-version version-number \  
  --alias-name alias-name \  
  --description " "
```

```
--name alias-name \  
--function-version version-number
```

Untuk menghapus alias, gunakan perintah [delete-alias](#).

```
aws lambda delete-alias \  
--function-name my-function \  
--name alias-name
```

AWS CLI Perintah dalam langkah-langkah sebelumnya sesuai dengan operasi Lambda berikut:
API

- [CreateAlias](#)
- [UpdateAlias](#)
- [DeleteAlias](#)

Menggunakan alias Lambda dalam sumber peristiwa dan kebijakan izin

Setiap alias memiliki ARN keunikan. Alias hanya dapat menunjuk ke versi fungsi, bukan ke alias lain. Anda dapat memperbarui alias untuk menunjuk ke versi baru fungsi ini.

Sumber event seperti Amazon Simple Storage Service (Amazon S3) menginvokasi fungsi Lambda Anda. Sumber-sumber event ini mempertahankan pemetaan yang mengidentifikasi fungsi untuk diinvokasi ketika event terjadi. Jika Anda menentukan alias fungsi Lambda dalam konfigurasi pemetaan, Anda tidak perlu memperbarui pemetaan saat versi fungsi berubah. Untuk informasi selengkapnya, lihat [Bagaimana Lambda memproses catatan dari sumber acara berbasis streaming dan antrian](#).

Dalam kebijakan sumber daya, Anda dapat memberikan izin kepada sumber event untuk menggunakan fungsi Lambda Anda. Jika Anda menentukan alias ARN dalam kebijakan, Anda tidak perlu memperbarui kebijakan saat versi fungsi berubah.

Kebijakan sumber daya

Anda dapat menggunakan [kebijakan berbasis sumber daya](#) untuk memberikan layanan, sumber daya, atau akses akun ke fungsi Anda. Cakupan izin tersebut tergantung pada apakah Anda menerapkannya ke alias, versi, atau keseluruhan fungsi. Misalnya, jika Anda menggunakan nama alias (seperti `helloworld:PROD`), izin memungkinkan Anda untuk memanggil `helloworld` fungsi menggunakan alias ARN (`helloworld:PROD`).

Jika Anda mencoba memanggil fungsi tersebut tanpa alias atau versi tertentu, Anda mendapatkan kesalahan izin. Kesalahan izin ini masih terjadi meskipun Anda berupaya untuk memanggil secara langsung versi fungsi yang terkait dengan alias.

Misalnya, AWS CLI perintah berikut memberikan izin Amazon S3 untuk memanggil `PROD` alias fungsi `helloworld` saat Amazon S3 bertindak atas nama `amzn-s3-demo-bucket`

```
aws lambda add-permission \  
  --function-name helloworld \  
  --qualifier PROD \  
  --statement-id 1 \  
  --principal s3.amazonaws.com \  
  --action lambda:InvokeFunction \  
  --source-arn arn:aws:s3:::amzn-s3-demo-bucket \  
  --source-account 123456789012
```

Untuk informasi selengkapnya tentang menggunakan nama sumber daya dalam kebijakan, lihat [Menyesuaikan bagian Sumber Daya dan Ketentuan kebijakan](#).

Buat konfigurasi routing untuk alias Lambda

Gunakan konfigurasi routing pada alias untuk mengirim sebagian lalu lintas ke versi fungsi kedua. Misalnya, Anda dapat mengurangi risiko deployment versi baru dengan mengonfigurasi alias untuk mengirim sebagian besar lalu lintas ke versi yang ada, dan hanya sebagian kecil lalu lintas ke versi baru.

Lambda menggunakan model probabilistik sederhana untuk mendistribusikan lalu lintas di antara dua versi fungsi. Pada tingkat lalu lintas rendah, Anda mungkin melihat varians tinggi di antara persentase lalu lintas yang dikonfigurasi dan aktual di setiap versi. Jika fungsi Anda menggunakan konkurensi terprovisi, Anda dapat menghindari [invokasi limpahan](#) dengan mengonfigurasi jumlah yang lebih tinggi dari instans konkurensi terprovisi selama perutean alias aktif.

Anda dapat mengarahkan alias ke maksimal dua versi fungsi Lambda. Versi harus memenuhi kriteria berikut:

- Kedua versi harus memiliki [peran eksekusi](#) sama.
- Kedua versi harus memiliki konfigurasi [antrean surat mati](#) sama, atau tidak ada konfigurasi antrean surat mati.
- Kedua versi tersebut harus dipublikasikan. Alias tidak dapat menunjuk ke \$LATEST.

Console

Untuk mengkonfigurasi routing pada alias menggunakan konsol

Note

Verifikasi bahwa fungsi memiliki setidaknya dua versi yang dipublikasikan. Untuk membuat versi tambahan, ikuti petunjuk dalam [Kelola versi fungsi Lambda](#).

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Alias, lalu pilih Buat alias.

4. Di halaman Buat alias, lakukan hal berikut:
 - a. Masukkan Nama untuk alias.
 - b. (Opsional) Masukkan Deskripsi untuk alias.
 - c. Untuk Versi, pilih versi fungsi pertama yang ingin Anda tunjuk.
 - d. Perluas Alias tertimbang.
 - e. Untuk Versi tambahan, pilih versi fungsi kedua yang ingin Anda tunjuk.
 - f. Untuk Bobot (%), masukkan nilai bobot untuk fungsi. Bobot adalah persentase lalu lintas yang ditetapkan untuk versi tersebut ketika alias dipanggil. Versi pertama menerima bobot residual. Misalnya, jika Anda menentukan 10 persen ke Versi tambahan, versi pertama ditetapkan ke 90 persen secara otomatis.
 - g. Pilih Simpan.

AWS CLI

Gunakan AWS CLI perintah [create-alias](#) dan [update-alias](#) untuk mengonfigurasi bobot lalu lintas antara dua versi fungsi. Saat membuat atau memperbarui alias, Anda menentukan berat lalu lintas dalam parameter `routing-config`.

Contoh berikut membuat alias fungsi Lambda bernama `routing-alias` yang menunjuk ke versi 1 dari fungsi. Versi 2 fungsi menerima 3 persen lalu lintas. 97 persen lalu lintas yang tersisa diarahkan ke versi 1.

```
aws lambda create-alias \  
  --name routing-alias \  
  --function-name my-function \  
  --function-version 1 \  
  --routing-config AdditionalVersionWeights={"2":0.03}
```

Gunakan perintah `update-alias` untuk meningkatkan persentase lalu lintas masuk ke versi 2. Dalam contoh berikut, Anda meningkatkan lalu lintas menjadi 5 persen.

```
aws lambda update-alias \  
  --name routing-alias \  
  --function-name my-function \  
  --routing-config AdditionalVersionWeights={"2":0.05}
```

Untuk mengirimkan semua lalu lintas ke versi 2, gunakan `update-alias` untuk mengubah properti `function-version` untuk menunjuk alias ke versi 2. Perintah juga mengatur ulang konfigurasi perutean.

```
aws lambda update-alias \  
  --name routing-alias \  
  --function-name my-function \  
  --function-version 2 \  
  --routing-config AdditionalVersionWeights={}
```

AWS CLI Perintah dalam langkah-langkah sebelumnya sesuai dengan operasi Lambda berikut: API

- [CreateAlias](#)
- [UpdateAlias](#)

Menentukan versi mana yang dipanggil

Saat Anda mengonfigurasi bobot lalu lintas di antara dua versi fungsi, ada dua cara untuk menentukan versi fungsi Lambda yang sudah dipanggil:

- CloudWatch Log — Lambda secara otomatis memancarkan entri START log yang berisi ID versi yang dipanggil ke Amazon CloudWatch Logs untuk setiap pemanggilan fungsi. Berikut adalah contohnya:

```
19:44:37 START RequestId: request id Version: $version
```

Untuk invokasi alias, Lambda menggunakan dimensi `Executed Version` untuk memfilter data metrik dengan versi yang dipanggil. Untuk informasi selengkapnya, lihat [Lihat metrik untuk fungsi Lambda](#).

- Muatan respons (invokasi tersinkron) – Respons untuk invokasi fungsi tersinkron yang mencakup header `x-amz-executed-version` untuk menunjukkan versi fungsi mana yang telah dipanggil.

Kelola versi fungsi Lambda

Anda dapat menggunakan versi untuk mengelola deployment fungsi Anda. Misalnya, Anda dapat menerbitkan versi baru dari fungsi untuk uji beta tanpa memengaruhi pengguna dari versi produksi stabil. Lambda membuat versi baru fungsi Anda setiap kali Anda menerbitkan fungsi. Versi baru adalah salinan dari versi fungsi yang belum diterbitkan. Versi yang tidak dipublikasikan diberi nama \$LATEST.

Note

Untuk membuat versi baru dari fungsi Anda, Anda harus terlebih dahulu membuat perubahan pada versi yang tidak diterbitkan (\$LATEST). Perubahan ini dapat mencakup memperbarui kode atau memodifikasi pengaturan konfigurasi. Jika \$LATEST identik dengan versi yang diterbitkan sebelumnya, Anda tidak akan dapat membuat versi baru sampai Anda menerapkan perubahan ke \$LATEST.

Setelah Anda mempublikasikan versi fungsi, kode, runtime, arsitektur, memori, lapisan, dan sebagian besar pengaturan konfigurasi lainnya tidak dapat diubah. Ini berarti Anda tidak dapat mengubah pengaturan ini tanpa menerbitkan versi baru dari \$LATEST. Anda dapat mengonfigurasi item berikut untuk versi fungsi yang diterbitkan:

- [Pemicu](#)
- [Destinasi](#)
- [Konkurensi yang disediakan](#)
- [Pemanggilan asinkron](#)
- [Koneksi database dan proxy](#)

Note

Saat menggunakan [kontrol manajemen runtime](#) dengan mode Otomatis, versi runtime yang digunakan oleh versi fungsi diperbarui secara otomatis. Saat menggunakan pembaruan Fungsi atau mode Manual, versi runtime tidak diperbarui. Untuk informasi selengkapnya, lihat [the section called “Pembaruan versi runtime”](#).

Bagian-bagian

- [Membuat versi fungsi](#)
- [Menggunakan versi](#)
- [Memberi izin](#)

Membuat versi fungsi

Anda dapat mengubah kode dan pengaturan fungsi hanya pada versi fungsi yang belum diterbitkan. Saat Anda memublikasikan versi, Lambda mengunci kode dan sebagian besar pengaturan untuk mempertahankan pengalaman yang konsisten bagi pengguna versi tersebut.

Anda dapat membuat versi fungsi menggunakan konsol Lambda.

Untuk membuat versi baru fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi, lalu pilih Versi.
3. Pada halaman konfigurasi fungsi, pilih Terbitkan versi baru.
4. (Opsional) Masukkan deskripsi versi.
5. Pilih Terbitkan.

Atau, Anda dapat memublikasikan versi fungsi menggunakan [PublishVersion](#) API operasi.

AWS CLI Perintah berikut menerbitkan versi baru dari suatu fungsi. Respons mengembalikan informasi konfigurasi tentang versi baru, termasuk nomor versi dan fungsi ARN dengan akhiran versi.

```
aws lambda publish-version --function-name my-function
```

Anda akan melihat output berikut:

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:1",
  "Version": "1",
  "Role": "arn:aws:iam::123456789012:role/lambda-role",
  "Handler": "function.handler",
  "Runtime": "nodejs20.x",
  ...
}
```

```
}
```

Note

Lambda menetapkan nomor urut yang meningkat secara monoton untuk pembuatan versi. Lambda tidak pernah menggunakan kembali nomor versi, bahkan setelah Anda menghapus dan membuat ulang fungsi.

Menggunakan versi

Anda dapat mereferensikan fungsi Lambda Anda menggunakan yang memenuhi syarat ARN atau tidak memenuhi syarat. ARN

- Memenuhi syarat ARN - Fungsi ARN dengan akhiran versi. Contoh berikut mengacu pada versi 42 dari fungsi `helloworld`.

```
arn:aws:lambda:aws-region:acct-id:function:helloworld:42
```

- Tidak memenuhi syarat ARN - Fungsi ARN tanpa akhiran versi.

```
arn:aws:lambda:aws-region:acct-id:function:helloworld
```

Anda dapat menggunakan yang memenuhi syarat atau tidak memenuhi syarat ARN dalam semua API operasi yang relevan. Namun, Anda tidak dapat menggunakan unqualified ARN untuk membuat alias.

Jika Anda memutuskan untuk tidak mempublikasikan versi fungsi, Anda dapat memanggil fungsi menggunakan yang memenuhi syarat atau tidak memenuhi syarat ARN dalam pemetaan [sumber acara](#) Anda. Saat Anda memanggil fungsi menggunakan yang tidak memenuhi syarat, ARN Lambda secara implisit memanggil. `$LATEST`

Lambda menerbitkan versi fungsi baru hanya jika kode belum pernah dipublikasikan, atau jika kode telah berubah dari versi terakhir yang diterbitkan. Jika tidak ada perubahan, versi fungsi tetap pada versi publikasi terakhir.

Yang memenuhi syarat ARN untuk setiap versi fungsi Lambda adalah unik. Setelah mempublikasikan versi, Anda tidak dapat mengubah ARN atau kode fungsi.

Memberi izin

Anda dapat menggunakan [kebijakan berbasis sumber daya](#) atau [kebijakan berbasis identitas](#) untuk memberikan akses ke fungsi Anda. Ruang lingkup izin tergantung pada apakah Anda menerapkan kebijakan ke fungsi atau ke salah satu versi fungsi. Untuk informasi selengkapnya tentang nama sumber daya fungsi dalam kebijakan, lihat [Menyesuaikan bagian Sumber Daya dan Ketentuan kebijakan](#).

Anda dapat menyederhanakan pengelolaan sumber peristiwa dan AWS Identity and Access Management (IAM) kebijakan dengan menggunakan alias fungsi. Untuk informasi selengkapnya, lihat [Buat alias untuk fungsi Lambda](#).

Menggunakan tag pada fungsi Lambda

Anda dapat menandai AWS Lambda fungsi untuk mengaktifkan [kontrol akses berbasis atribut \(ABAC\)](#) dan mengaturnya berdasarkan pemilik, proyek, atau departemen. [Tag adalah pasangan nilai kunci bentuk bebas yang didukung di seluruh AWS layanan untuk digunakan di ABAC, memfilter sumber daya, dan menambahkan detail ke laporan penagihan.](#)

Tanda berlaku pada tingkat fungsi, bukan pada versi atau alias. Tag bukan bagian dari konfigurasi khusus versi yang Lambda buat snapshot saat Anda memublikasikan versi.

Bagian-bagian

- [Izin diperlukan untuk bekerja dengan tag](#)
- [Menggunakan tag dengan konsol Lambda](#)
- [Menggunakan tag dengan AWS CLI](#)
- [Persyaratan untuk tag](#)

Izin diperlukan untuk bekerja dengan tag

Berikan izin yang sesuai untuk identitas AWS Identity and Access Management (IAM) (pengguna, grup, atau peran) untuk orang yang bekerja dengan fungsi tersebut:

- `lambda: ListTags` — Ketika suatu fungsi memiliki tag, berikan izin ini kepada siapa saja yang perlu memanggil `GetFunction` atau `ListTags` menggunakannya.
- `lambda: TagResource` — Berikan izin ini kepada siapa saja yang perlu menelepon `CreateFunction` atau `TagResource`.

Untuk informasi selengkapnya, lihat [Kebijakan berbasis identitas IAM untuk Lambda](#).

Menggunakan tag dengan konsol Lambda

Anda dapat menggunakan konsol Lambda untuk membuat fungsi yang memiliki tag, menambahkan tag ke fungsi yang ada, dan memfilter fungsi berdasarkan tag yang Anda tambahkan.

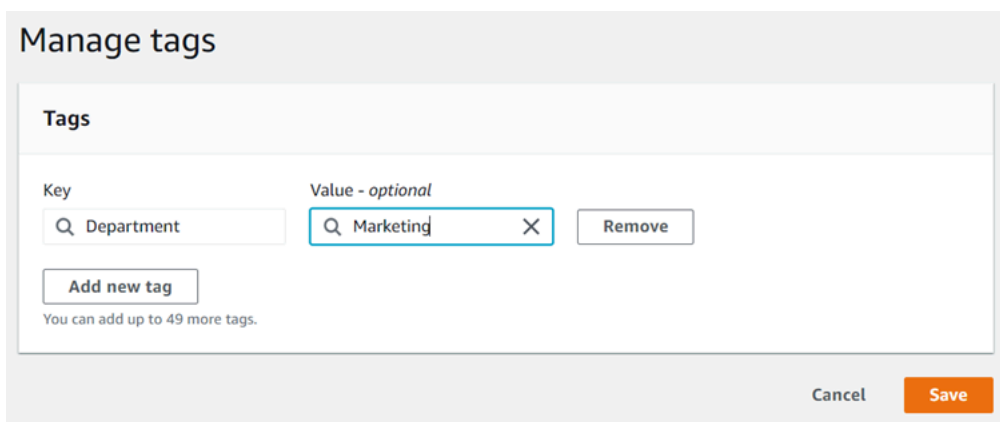
Untuk menambahkan tag saat Anda membuat fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih Buat fungsi.
3. Pilih Penulis dari awal atau gambar Kontainer.
4. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk Nama fungsi, masukkan nama fungsi. Nama fungsi dibatasi hingga 64 karakter panjangnya.
 - b. Untuk Runtime, pilih versi bahasa yang akan digunakan untuk fungsi Anda.
 - c. (Opsional) Untuk Arsitektur, pilih [arsitektur set instruksi](#) yang akan digunakan untuk fungsi Anda. Arsitektur defaultnya adalah x86_64. Ketika Anda membangun paket deployment untuk fungsi Anda, pastikan bahwa itu kompatibel dengan arsitektur set instruksi yang Anda pilih.
5. Perluas Pengaturan lanjutan, lalu pilih Aktifkan tag.
6. Pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai opsional. Untuk menambahkan lebih banyak tag, ulangi langkah ini.
7. Pilih Buat fungsi.

Untuk menambahkan tag ke fungsi yang ada

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih Konfigurasi, lalu pilih Tag.
4. Di bagian Tanda, pilih Kelola tanda.
5. Pilih Tambahkan tag baru, lalu masukkan Kunci dan Nilai opsional. Untuk menambahkan lebih banyak tag, ulangi langkah ini.

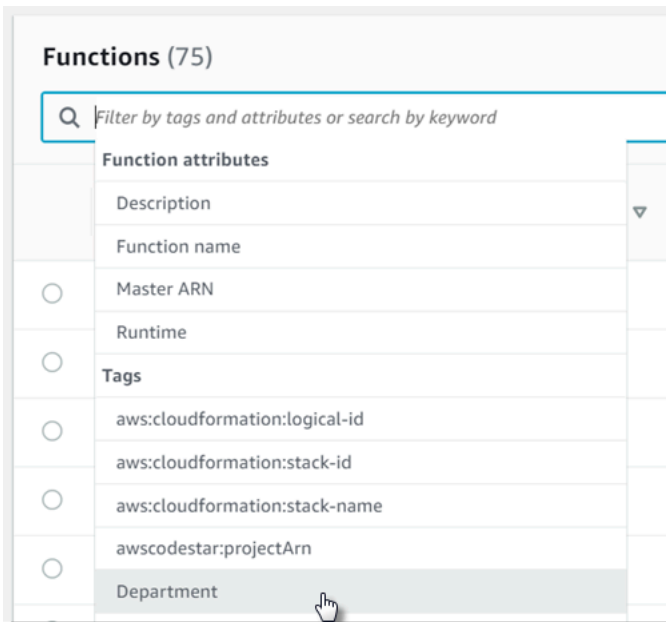


The screenshot shows a 'Manage tags' dialog box. It has a title bar 'Manage tags'. Inside, there's a section titled 'Tags'. Below this, there are two input fields: 'Key' with the value 'Department' and 'Value - optional' with the value 'Marketing'. To the right of the 'Marketing' value is a small 'X' icon and a 'Remove' button. Below these fields is an 'Add new tag' button. At the bottom of the dialog, there are 'Cancel' and 'Save' buttons. A note at the bottom left says 'You can add up to 49 more tags.'

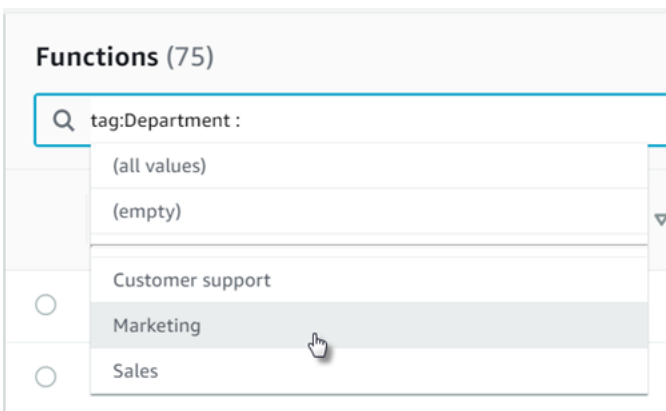
6. Pilih Simpan.

Untuk memfilter fungsi dengan tag

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih bilah pencarian untuk melihat daftar atribut fungsi dan tombol tag.



3. Pilih kunci tag untuk melihat daftar nilai yang sedang digunakan di AWS Wilayah saat ini.
4. Pilih nilai untuk melihat fungsi dengan nilai tersebut, atau pilih (semua nilai) untuk melihat semua fungsi yang memiliki tanda dengan kunci tersebut.



Bilah pencarian juga mendukung pencarian kunci tanda. Masukkan tag untuk melihat hanya daftar kunci tag, atau masukkan nama kunci untuk menemukannya dalam daftar.

Menggunakan tag dengan AWS CLI

Menambahkan dan menghapus tag

Untuk membuat fungsi Lambda baru dengan tag, gunakan `create-function` perintah dengan opsi `--tags`.

```
aws lambda create-function --function-name my-function
--handler index.js --runtime nodejs20.x \
--role arn:aws:iam::123456789012:role/lambda-role \
--tags Department=Marketing,CostCenter=1234ABCD
```

Untuk menambahkan tanda ke fungsi yang sudah ada, gunakan perintah `tag-resource`.

```
aws lambda tag-resource \
--resource arn:aws:lambda:us-east-2:123456789012:function:my-function \
--tags Department=Marketing,CostCenter=1234ABCD
```

Untuk menghapus tanda, gunakan perintah `untag-resource`.

```
aws lambda untag-resource --resource arn:aws:lambda:us-east-1:123456789012:function:my-function \
--tag-keys Department
```

Melihat tag pada suatu fungsi

Jika Anda ingin melihat tag yang diterapkan ke fungsi Lambda tertentu, Anda dapat menggunakan salah satu dari perintah berikut: AWS CLI

- [ListTags](#)— Untuk melihat daftar tag yang terkait dengan fungsi ini, sertakan ARN fungsi Lambda Anda (Nama Sumber Daya Amazon):

```
aws lambda list-tags --resource arn:aws:lambda:us-east-1:123456789012:function:my-function
```

- [GetFunction](#)— Untuk melihat daftar tag yang terkait dengan fungsi ini, sertakan nama fungsi Lambda Anda:

```
aws lambda get-function --function-name my-function
```

Fungsi penyaringan berdasarkan tag

Anda dapat menggunakan operasi AWS Resource Groups Tagging API [GetResources](#) API untuk memfilter sumber daya berdasarkan tag. `GetResources` Operasi menerima hingga 10 filter, dengan setiap filter berisi kunci tag dan hingga 10 nilai tag. `GetResources` menyediakan `ResourceType` untuk memfilter berdasarkan jenis sumber daya tertentu.

Untuk informasi selengkapnya AWS Resource Groups, lihat [Apa itu grup sumber daya?](#) di Panduan Pengguna AWS Resource Groups dan Tag.

Persyaratan untuk tag

Persyaratan berikut berlaku untuk tanda:

- Jumlah maksimum tanda per sumber daya: 50
- Panjang kunci maksimum: 128 karakter Unicode di UTF-8
- Panjang nilai maksimum: 256 karakter Unicode di UTF-8
- Kunci dan nilai tanda peka huruf besar dan kecil.
- Jangan menggunakan awalan `aws:` pada nama atau nilai tanda Anda, karena hal ini khusus untuk penggunaan AWS. Anda tidak dapat mengedit atau menghapus nama atau nilai tag dengan awalan ini. Tag dengan awalan ini tidak dihitung terhadap tag Anda per batas sumber daya.
- Jika Anda berencana untuk menggunakan skema penandaan di beberapa layanan dan sumber daya, ingatlah bahwa layanan lain mungkin memiliki batasan pada karakter yang diizinkan. Karakter yang diperbolehkan adalah: huruf, spasi, dan angka yang dapat mewakili dalam UTF-8, serta karakter berikut: `+ - = . _ : / @`.

Streaming respons untuk fungsi Lambda

Anda dapat mengonfigurasi fungsi Lambda Anda URLs untuk mengalirkan muatan respons kembali ke klien. Streaming respons dapat menguntungkan aplikasi sensitif latensi dengan meningkatkan waktu ke kinerja byte (TTFB) pertama. Ini karena Anda dapat mengirim sebagian tanggapan kembali ke klien saat tersedia. Selain itu, Anda dapat menggunakan streaming respons untuk membangun fungsi yang mengembalikan muatan yang lebih besar. Muatan aliran respons memiliki batas lunak 20 MB dibandingkan dengan batas 6 MB untuk respons buffer. Streaming respons juga berarti bahwa fungsi Anda tidak perlu sesuai dengan seluruh respons dalam memori. Untuk respons yang sangat besar, ini dapat mengurangi jumlah memori yang perlu Anda konfigurasi untuk fungsi Anda.

Kecepatan Lambda mengalirkan respons Anda tergantung pada ukuran respons. Rasio streaming untuk 6MB pertama dari respons fungsi Anda tidak dibatasi. Untuk respons yang lebih besar dari 6MB, sisa respons tunduk pada batas bandwidth. Untuk informasi lebih lanjut tentang bandwidth streaming, lihat [Batas bandwidth untuk streaming respons](#).

Respons streaming menimbulkan biaya. Untuk informasi selengkapnya, silakan lihat [Harga AWS Lambda](#).

Lambda mendukung streaming respons pada runtime terkelola Node.js. Untuk bahasa lain, Anda dapat [menggunakan runtime kustom dengan API integrasi Runtime kustom](#) untuk melakukan streaming respons atau menggunakan Adaptor Web [Lambda](#). Anda dapat melakukan streaming respons melalui [fungsi Lambda URLs](#) AWS SDK, atau menggunakan Lambda. [InvokeWithResponseStream](#) API

Note

Saat menguji fungsi Anda melalui konsol Lambda, Anda akan selalu melihat respons sebagai buffer.

Topik

- [Batas bandwidth untuk streaming respons](#)
- [Menulis fungsi Lambda yang mendukung streaming respons](#)
- [Memanggil fungsi yang diaktifkan streaming respons menggunakan fungsi Lambda URLs](#)
- [Tutorial: Membuat respons streaming fungsi Lambda dengan URL fungsi](#)

Batas bandwidth untuk streaming respons

6MB pertama dari muatan respons fungsi Anda memiliki bandwidth yang tidak dibatasi. Setelah ledakan awal ini, Lambda mengalirkan respons Anda dengan kecepatan maksimum 2. MBps. Jika respons fungsi Anda tidak pernah melebihi 6MB, maka batas bandwidth ini tidak pernah berlaku.

Note

Batas bandwidth hanya berlaku untuk payload respons fungsi Anda, dan bukan untuk akses jaringan oleh fungsi Anda.

Tingkat bandwidth yang tidak dibatasi bervariasi tergantung pada sejumlah faktor, termasuk kecepatan pemrosesan fungsi Anda. Anda biasanya dapat mengharapkan tingkat yang lebih tinggi dari 2 MBps untuk 6MB pertama dari respons fungsi Anda. Jika fungsi Anda mengalirkan respons ke tujuan di luar AWS, kecepatan streaming juga tergantung pada kecepatan koneksi internet eksternal.

Menulis fungsi Lambda yang mendukung streaming respons

Menulis handler untuk fungsi streaming respons berbeda dari pola handler biasa. Saat menulis fungsi streaming, pastikan untuk melakukan hal berikut:

- Bungkus fungsi Anda dengan `awsLambda.streamifyResponse()` dekorator yang disediakan runtime Node.js asli.
- Akhiri aliran dengan `anggun` untuk memastikan bahwa semua pemrosesan data selesai.

Mengkonfigurasi fungsi handler untuk mengalirkan respons

Untuk menunjukkan ke runtime bahwa Lambda harus mengalirkan respons fungsi Anda, Anda harus membungkus fungsi Anda dengan `streamifyResponse()` dekorator. Ini memberi tahu runtime untuk menggunakan jalur logika yang tepat untuk respons streaming dan memungkinkan fungsi untuk mengalirkan respons.

`streamifyResponse()` Dekorator menerima fungsi yang menerima parameter berikut:

- `event`— Memberikan informasi tentang acara URL pemanggilan fungsi, seperti HTTP metode, parameter kueri, dan badan permintaan.
- `responseStream`— Menyediakan aliran yang dapat ditulis.

- `context` Menyediakan metode dan properti dengan informasi tentang pemanggilan, fungsi, dan lingkungan eksekusi.

`responseStream` objeknya adalah [Node.js writableStream](#). Seperti halnya aliran seperti itu, Anda harus menggunakan `pipeline()` metode ini.

Example handler yang mendukung streaming respons

```
const pipeline = require("util").promisify(require("stream").pipeline);
const { Readable } = require('stream');

exports.echo = awslambda.streamifyResponse(async (event, responseStream, _context) => {
  // As an example, convert event to a readable stream.
  const requestStream = Readable.from(Buffer.from(JSON.stringify(event)));

  await pipeline(requestStream, responseStream);
});
```

Meskipun `responseStream` menawarkan `write()` metode untuk menulis ke aliran, kami sarankan Anda menggunakannya [pipeline\(\)](#) sedapat mungkin. Menggunakan `pipeline()` memastikan bahwa aliran yang dapat ditulis tidak kewalahan oleh aliran yang dapat dibaca lebih cepat.

Mengakhiri aliran

Pastikan Anda mengakhiri aliran dengan benar sebelum handler kembali. `pipeline()` Metode ini menangani ini secara otomatis.

Untuk kasus penggunaan lainnya, panggil `responseStream.end()` metode untuk mengakhiri aliran dengan benar. Metode ini menandakan bahwa tidak ada lagi data yang harus ditulis ke aliran. Metode ini tidak diperlukan jika Anda menulis ke aliran dengan `pipeline()` atau `pipe()`.

Example Contoh mengakhiri aliran dengan `pipeline()`

```
const pipeline = require("util").promisify(require("stream").pipeline);

exports.handler = awslambda.streamifyResponse(async (event, responseStream, _context)
=> {
  await pipeline(requestStream, responseStream);
});
```

Example Contoh mengakhiri aliran tanpa pipeline ()

```
exports.handler = awslambda.streamifyResponse(async (event, responseStream, _context)
=> {
  responseStream.write("Hello ");
  responseStream.write("world ");
  responseStream.write("from ");
  responseStream.write("Lambda!");
  responseStream.end();
});
```

Memanggil fungsi yang diaktifkan streaming respons menggunakan fungsi Lambda URLs

Note

Anda harus memanggil fungsi Anda menggunakan fungsi URL untuk mengalirkan respons.

Anda dapat memanggil fungsi yang diaktifkan streaming respons dengan mengubah mode pemanggilan fungsi Anda. URL Mode pemanggilan menentukan API operasi yang digunakan Lambda untuk menjalankan fungsi Anda. Mode pemanggilan yang tersedia adalah:

- **BUFFERED**— Ini adalah opsi default. Lambda memanggil fungsi Anda menggunakan operasi. Invoke API Hasil pemanggilan tersedia saat muatan selesai. Ukuran muatan maksimum adalah 6 MB.
- **RESPONSE_STREAM**— Memungkinkan fungsi Anda untuk mengalirkan hasil payload saat tersedia. Lambda memanggil fungsi Anda menggunakan operasi. InvokeWithResponseStream API Ukuran payload respons maksimum adalah 20 MB. Namun, Anda dapat [meminta kenaikan kuota](#).

Anda masih dapat menjalankan fungsi Anda tanpa streaming respons dengan langsung memanggil Invoke API operasi. Namun, Lambda mengalirkan semua muatan respons untuk pemanggilan yang datang melalui fungsi URL hingga Anda mengubah mode pemanggilan menjadi. BUFFERED

Console

Untuk mengatur mode pemanggilan fungsi URL (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih nama fungsi yang ingin Anda atur untuk mode pemanggilan.
3. Pilih tab Configuration, lalu pilih Function URL.
4. Pilih Edit, lalu pilih Pengaturan tambahan.
5. Di bawah mode Panggilan, pilih mode pemanggilan yang Anda inginkan.
6. Pilih Simpan.

AWS CLI

Untuk mengatur mode pemanggilan fungsi URL ()AWS CLI

```
aws lambda update-function-url-config \  
  --function-name my-function \  
  --invoke-mode RESPONSE_STREAM
```

AWS CloudFormation

Untuk mengatur mode pemanggilan fungsi URL ()AWS CloudFormation

```
MyFunctionUrl:  
  Type: AWS::Lambda::Url  
  Properties:  
    AuthType: AWS_IAM  
    InvokeMode: RESPONSE_STREAM
```

Untuk informasi selengkapnya tentang mengonfigurasi fungsiURLs, lihat Fungsi [URLsLambda](#).

Tutorial: Membuat respons streaming fungsi Lambda dengan URL fungsi

Dalam tutorial ini, Anda membuat fungsi Lambda yang didefinisikan sebagai arsip file.zip dengan titik akhir URL fungsi yang mengembalikan aliran respons. Untuk informasi selengkapnya tentang mengonfigurasi URL fungsi, lihat [Fungsi URLs](#)

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```

Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (\) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh perintah CLI dalam panduan ini menggunakan pemformatan Linux. Perintah yang menyertakan dokumen JSON sebaris harus diformat ulang jika Anda menggunakan CLI Windows.

Membuat peran eksekusi

Buat [peran eksekusi](#) yang memberikan izin kepada fungsi Lambda Anda untuk mengakses sumber daya AWS .

Untuk membuat peran eksekusi

1. Buka [halaman](#) Peran konsol AWS Identity and Access Management (IAM).
2. Pilih Buat peran.
3. Buat peran dengan properti berikut:
 - Jenis entitas tepercaya - AWS layanan
 - Kasus penggunaan - Lambda
 - Izin – AWSLambdaBasicExecutionRole

- Nama peran – **response-streaming-role**

AWSLambdaBasicExecutionRoleKebijakan ini memiliki izin yang diperlukan fungsi untuk menulis log ke Amazon CloudWatch Logs. Setelah Anda membuat peran, catat Nama Sumber Daya Amazon (ARN). Anda akan membutuhkannya di langkah berikutnya.

Buat fungsi streaming respons (AWS CLI)

Buat respons streaming fungsi Lambda dengan titik akhir URL fungsi menggunakan (). AWS Command Line Interface AWS CLI

Untuk membuat fungsi yang dapat mengalirkan respons

1. Salin contoh kode berikut ke file bernama `index.mjs`.

```
import util from 'util';
import stream from 'stream';
const { Readable } = stream;
const pipeline = util.promisify(stream.pipeline);

/* global awslambda */
export const handler = awslambda.streamifyResponse(async (event, responseStream,
  _context) => {
  const requestStream = Readable.from(Buffer.from(JSON.stringify(event)));
  await pipeline(requestStream, responseStream);
});
```

2. Buat paket deployment.

```
zip function.zip index.mjs
```

3. Buat fungsi Lambda dengan perintah `create-function`. Ganti nilai `--role` dengan peran ARN dari langkah sebelumnya.

```
aws lambda create-function \
  --function-name my-streaming-function \
  --runtime nodejs16.x \
  --zip-file fileb://function.zip \
  --handler index.handler \
  --role arn:aws:iam::123456789012:role/response-streaming-role
```

Untuk membuat URL fungsi

1. Tambahkan kebijakan berbasis sumber daya ke fungsi Anda untuk mengizinkan akses ke URL fungsi Anda. Ganti nilai `--principal` dengan Akun AWS ID Anda.

```
aws lambda add-permission \  
  --function-name my-streaming-function \  
  --action lambda:InvokeFunctionUrl \  
  --statement-id 12345 \  
  --principal 123456789012 \  
  --function-url-auth-type AWS_IAM \  
  --statement-id url
```

2. Buat titik akhir URL untuk fungsi dengan `create-function-url-config` perintah.

```
aws lambda create-function-url-config \  
  --function-name my-streaming-function \  
  --auth-type AWS_IAM \  
  --invoke-mode RESPONSE_STREAM
```

Uji titik akhir URL fungsi

Uji integrasi Anda dengan menjalankan fungsi Anda. Anda dapat membuka URL fungsi Anda di browser, atau Anda dapat menggunakan curl.

```
curl --request GET "<function_url>" --user "<key:token>" --aws-sigv4 "aws:amz:us-east-1:lambda" --no-buffer
```

URL fungsi kami menggunakan jenis `IAM_AUTH` otentikasi. Ini berarti Anda perlu menandatangani permintaan dengan kunci AWS akses dan kunci rahasia Anda. Pada perintah sebelumnya, ganti `<key:token>` dengan ID kunci AWS akses. Masukkan kunci AWS rahasia Anda saat diminta. Jika Anda tidak memiliki kunci AWS rahasia Anda, Anda dapat [menggunakan AWS kredensial sementara](#) sebagai gantinya.

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Akun AWS.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Memahami metode pemanggilan fungsi Lambda

Setelah Anda menerapkan fungsi Lambda Anda, Anda dapat memanggilmnya dengan beberapa cara:

- Konsol [Lambda — Gunakan konsol](#) Lambda untuk membuat acara pengujian dengan cepat untuk menjalankan fungsi Anda.
- The [AWS SDK](#)— Gunakan AWS SDK untuk memanggil fungsi Anda secara terprogram.
- The [Invoke](#) API — Gunakan Lambda API Invoke untuk langsung memanggil fungsi Anda.
- The [AWS Command Line Interface \(AWS CLI\)](#) — Gunakan `aws lambda invoke` AWS CLI perintah untuk langsung memanggil fungsi Anda dari baris perintah.
- [Titik akhir fungsi URL HTTP \(S\) - Gunakan fungsi URLs untuk membuat titik](#) akhir khusus HTTP (S) yang dapat Anda gunakan untuk memanggil fungsi Anda.

Semua metode ini adalah cara langsung untuk menjalankan fungsi Anda. Di Lambda, kasus penggunaan umum adalah memanggil fungsi Anda berdasarkan peristiwa yang terjadi di tempat lain dalam aplikasi Anda. Beberapa layanan dapat memanggil fungsi Lambda dengan setiap acara baru. Ini disebut [pemicu](#). Untuk layanan berbasis streaming dan antrian, Lambda memanggil fungsi dengan kumpulan catatan. Ini disebut [pemetaan sumber peristiwa](#).

Saat Anda mengaktifkan suatu fungsi, Anda dapat memilih untuk mengaktifkannya secara sinkron atau asinkron. Dengan [invokasi sinkron](#), Anda menunggu fungsi untuk memproses peristiwa dan mengirimkan respons. Dengan invokasi [asinkron](#), Lambda membuat antrean peristiwa untuk memproses dan mengembalikan respons dengan segera. [Parameter InvocationType permintaan di Invoke API](#) menentukan cara Lambda memanggil fungsi Anda. Nilai `RequestResponse` menunjukkan pemanggilan sinkron, dan nilai `Event` menunjukkan pemanggilan asinkron.

Untuk menjalankan fungsi Anda IPv6, gunakan titik akhir tumpukan [ganda](#) publik Lambda. Titik akhir dual-stack mendukung keduanya dan. IPv4 IPv6 Titik akhir dual-stack Lambda menggunakan sintaks berikut:

```
protocol://lambda.us-east-1.api.aws
```

Anda juga dapat menggunakan fungsi [Lambda URLs untuk memanggil fungsi](#). IPv6 URL Titik akhir fungsi memiliki format berikut:

```
https://url-id.lambda-url.us-east-1.on.aws
```

Jika pemanggilan fungsi menghasilkan kesalahan, untuk pemanggilan sinkron, lihat pesan kesalahan dalam respons dan coba lagi pemanggilan secara manual. [Untuk pemanggilan asinkron, Lambda menangani percobaan ulang secara otomatis dan dapat mengirim catatan pemanggilan ke tujuan.](#)

Memanggil fungsi Lambda secara sinkron

Saat Anda memanggil fungsi secara sinkron, Lambda menjalankan fungsi dan menunggu suatu respons. Ketika fungsi selesai, Lambda mengembalikan respons dari kode fungsi dengan data tambahan, seperti versi fungsi yang diaktifkan. Untuk menjalankan fungsi secara sinkron dengan AWS CLI, gunakan perintah. `invoke`

```
aws lambda invoke --function-name my-function \  
  --cli-binary-format raw-in-base64-out \  
  --payload '{ "key": "value" }' response.json
```

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

Diagram berikut menunjukkan klien yang memanggil fungsi Lambda secara sinkron. Lambda mengirimkan peristiwa tersebut secara langsung ke fungsi dan mengirimkan respons fungsi kembali ke invoker.

Synchronous Invocation



payloadIni adalah string yang berisi peristiwa dalam JSON format. Nama file tempat AWS CLI menulis respons dari fungsi adalah `response.json`. Jika fungsi mengembalikan objek atau kesalahan, badan respons adalah objek atau kesalahan dalam JSON format. Jika fungsi keluar tanpa kesalahan, badan responsnya adalah `null`.

Note

Lambda tidak menunggu ekstensi eksternal selesai sebelum mengirim respons. Ekstensi eksternal berjalan sebagai proses independen di lingkungan eksekusi dan terus berjalan setelah pemanggilan fungsi selesai. Untuk informasi selengkapnya, lihat [Menambah fungsi Lambda menggunakan ekstensi Lambda](#).

Output dari perintah, yang ditampilkan di terminal, mencakup informasi dari header di respons dari Lambda. Ini termasuk versi yang memproses peristiwa (berguna saat Anda menggunakan [alias](#)), dan kode status yang dikembalikan oleh Lambda. Jika Lambda dapat menjalankan fungsi, kode statusnya adalah 200, meskipun fungsi tersebut mengembalikan kesalahan.

Note

Untuk fungsi dengan waktu habis yang lama, klien Anda mungkin terputus selama invokasi sinkron sementara menunggu respons. Konfigurasi HTTP klien SDK, firewall, proxy, atau sistem operasi Anda untuk memungkinkan koneksi panjang dengan pengaturan batas waktu atau keep-alive.

Jika Lambda tidak dapat menjalankan fungsi, kesalahan ditampilkan di output.

```
aws lambda invoke --function-name my-function \  
  --cli-binary-format raw-in-base64-out \  
  --payload value response.json
```

Anda akan melihat output berikut:

```
An error occurred (InvalidRequestContentException) when calling the Invoke operation:  
Could not parse request body into json: Unrecognized token 'value': was expecting  
( 'true', 'false' or 'null' )  
at [Source: (byte[])"value"; line: 1, column: 11]
```

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBULQgUmVxdWVzdElk0iA4N2QwNDRiOC1mMTU0LTExZTgt0GNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvc21vb... ",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`.

Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Untuk informasi selengkapnya tentang InvokeAPI, termasuk daftar lengkap parameter, header, dan error, lihat [Memanggil](#).

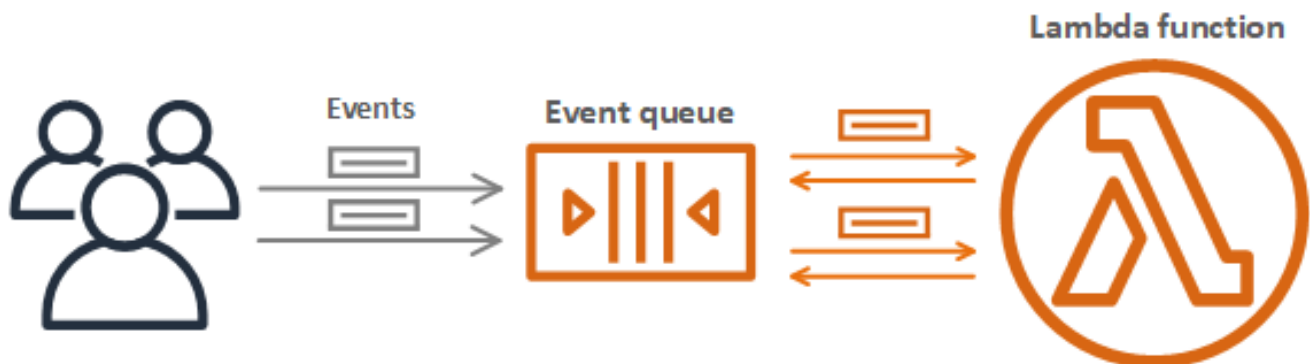
Saat Anda memanggil fungsi secara langsung, Anda dapat memeriksa respons kesalahan dan mencoba lagi. AWS CLI Dan AWS SDK juga secara otomatis mencoba lagi pada batas waktu klien, pelambatan, dan kesalahan layanan. Untuk informasi selengkapnya, lihat [Memahami perilaku coba lagi di Lambda](#).

Memanggil fungsi Lambda secara asinkron

Beberapa AWS layanan, seperti Amazon Simple Storage Service (Amazon S3) dan Amazon Simple Notification Service (SNS/Amazon), memanggil fungsi secara asinkron untuk memproses peristiwa. Anda juga dapat menjalankan fungsi Lambda secara asinkron menggunakan AWS CLI() atau salah satu AWS Command Line Interface satu fungsi. AWS SDKs Saat Anda memanggil fungsi secara asinkron, Anda tidak perlu menunggu respons dari kode fungsi tersebut. Anda menyerahkan peristiwa ke Lambda dan Lambda menangani sisanya. Anda dapat mengonfigurasi cara Lambda menangani kesalahan, dan dapat mengirim catatan pemanggilan ke sumber daya hilir seperti Amazon Simple Queue Service (Amazon) SQS atau Amazon EventBridge (EventBridge) untuk menyatukan komponen aplikasi Anda.

Diagram berikut menunjukkan klien yang mengaktifkan fungsi Lambda secara asinkron. Lambda membuat antrian peristiwa sebelum mengirimkannya ke fungsi.

Asynchronous Invocation



Untuk invokasi asinkron, Lambda menempatkan peristiwa dalam antrian dan mengembalikan respons sukses informasi tambahan. Proses terpisah membaca peristiwa dari antrian dan mengirimnya ke fungsi Anda.

Untuk menjalankan fungsi Lambda secara asinkron menggunakan AWS Command Line Interface AWS CLI() atau salah satu fungsi, setel parameter AWS SDKs ke [InvocationType](#) Event Contoh berikut menunjukkan AWS CLI perintah untuk memanggil fungsi.

```
aws lambda invoke \  
  --function-name my-function \  
  --invocation-type Event \  
  <event>
```



```
--cli-binary-format raw-in-base64-out \  
--payload '{ "key": "value" }' response.json
```

Anda akan melihat output berikut:

```
{  
  "statusCode": 202  
}
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

File output (`response.json`) tidak berisi informasi apa pun, tetapi masih dibuat saat Anda menjalankan perintah ini. Jika Lambda tidak dapat menambahkan peristiwa ke antrean, pesan kesalahan akan muncul di output perintah.

Bagaimana Lambda menangani kesalahan dan mencoba ulang dengan pemanggilan asinkron

Lambda mengelola antrian peristiwa asinkron fungsi Anda dan mencoba lagi kesalahan. Jika fungsi mengembalikan kesalahan, secara default Lambda mencoba menjalankannya dua kali lagi, dengan menunggu satu menit antara dua upaya pertama, dan dua menit antara upaya kedua dan ketiga. Kesalahan fungsi meliputi kesalahan yang dikembalikan oleh kode fungsi dan kesalahan yang dikembalikan oleh runtime fungsi, seperti waktu habis.

Apabila fungsi tidak memiliki ketersediaan konkurensi yang cukup untuk memproses semua peristiwa, permintaan tambahan akan diperlambat. Untuk kesalahan pelambatan (429) dan kesalahan sistem (seri 500), Lambda mengembalikan acara ke antrian dan mencoba menjalankan fungsi lagi hingga 6 jam secara default. Interval percobaan lagi meningkat secara eksponensial dari 1 detik setelah percobaan pertama hingga maksimum 5 menit. Jika antrian berisi banyak entri, Lambda meningkatkan interval coba lagi dan mengurangi tingkat di mana ia membaca peristiwa dari antrian.

Meskipun fungsi Anda tidak memunculkan kesalahan, fungsi dapat menerima peristiwa yang sama dari Lambda beberapa kali karena antrean itu sendiri pada akhirnya konsisten. Jika fungsi tidak dapat mengikuti peristiwa masuk, peristiwa juga dapat dihapus dari antrean tanpa dikirim ke fungsi.

Pastikan bahwa kode fungsi Anda secara rapi menangani duplikasi peristiwa, dan bahwa Anda memiliki cukup konkurensi tersedia untuk menangani semua invokasi.

Ketika antrean sangat panjang, acara baru mungkin menua sebelum Lambda memiliki kesempatan untuk mengirimnya ke fungsi Anda. Saat peristiwa kedaluwarsa atau gagal dalam semua upaya pemrosesan, Lambda menghapusnya. Anda dapat [mengonfigurasi penanganan kesalahan](#) untuk fungsi mengurangi jumlah percobaan ulang yang dilakukan Lambda, atau membuang kejadian yang tidak diproses dengan lebih cepat.

Anda juga dapat mengonfigurasi Lambda untuk mengirim catatan invokasi ke layanan lain. Lihat [Menangkap catatan pemanggilan asinkron Lambda](#) untuk mempelajari lebih lanjut.

Mengonfigurasi pengaturan penanganan kesalahan untuk pemanggilan asinkron Lambda

Gunakan pengaturan berikut untuk mengonfigurasi cara Lambda menangani kesalahan dan mencoba ulang untuk pemanggilan fungsi asinkron:

- [MaximumEventAgeInSeconds](#): Jumlah waktu maksimum, dalam hitungan detik, Lambda menyimpan peristiwa dalam antrian acara asinkron sebelum membuangnya.
- [MaximumRetryAttempts](#): Jumlah maksimum kali Lambda mencoba ulang peristiwa ketika fungsi mengembalikan kesalahan.

Gunakan konsol Lambda atau AWS CLI untuk mengonfigurasi pengaturan penanganan kesalahan pada fungsi, versi, atau alias.

Console

Untuk mengonfigurasi penanganan kesalahan

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi, lalu pilih Invokasi asinkron.
4. Di bagian Invokasi asinkron, pilih Edit.
5. Konfigurasikan pengaturan berikut.
 - Usia maksimum peristiwa – Jumlah waktu maksimum yang dimiliki Lambda untuk menyimpan acara dalam antrean peristiwa asinkron, hingga 6 jam.

- Usaha percobaan ulang – Jumlah pengulangan Lambda saat fungsi mengembalikan kesalahan, antara 0 dan 2.

6. Pilih Simpan.

AWS CLI

[Untuk mengonfigurasi pemanggilan asinkron dengan AWS CLI, gunakan perintah `put-function-event-invoke`](#) Contoh berikut mengonfigurasi fungsi dengan batas waktu peristiwa maksimum selama 1 jam dan tidak perlu percobaan ulang.

```
aws lambda put-function-event-invoke-config \  
  --function-name error \  
  --maximum-event-age-in-seconds 3600 \  
  --maximum-retry-attempts 0
```

Perintah `put-function-event-invoke-config` menimpa konfigurasi fungsi, versi, atau alias yang ada. Untuk mengonfigurasi opsi tanpa mengatur ulang yang lain, gunakan [update-function-event-invoke-config](#). Contoh berikut mengonfigurasi Lambda untuk mengirim catatan ke antrian SQS standar destination bernama saat peristiwa tidak dapat diproses.

```
aws lambda update-function-event-invoke-config \  
  --function-name my-function \  
  --destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-  
east-1:123456789012:destination"}}'
```

Anda akan melihat output berikut:

```
{  
  "LastModified": 1573686021.479,  
  "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:  
$LATEST",  
  "MaximumRetryAttempts": 0,  
  "MaximumEventAgeInSeconds": 3600,  
  "DestinationConfig": {  
    "OnSuccess": {},  
    "OnFailure": {}  
  }  
}
```

Ketika peristiwa invokasi melebihi waktu maksimum atau gagal dalam semua upaya percobaan ulang, Lambda menghapusnya. [Untuk menyimpan salinan peristiwa yang dibuang, konfigurasi tujuan acara yang gagal.](#)

Menangkap catatan pemanggilan asinkron Lambda

Lambda dapat mengirim catatan pemanggilan asinkron ke salah satu dari berikut ini. AWS layanan

- Amazon SQS — SQS Antrian standar.
- Amazon SNS — SNS Topik standar.
- AWS Lambda – Fungsi Lambda.
- Amazon EventBridge — Bus EventBridge acara.

Catatan pemanggilan berisi rincian tentang permintaan dan respons dalam JSON format. Anda dapat mengonfigurasi tujuan terpisah untuk acara yang berhasil diproses, dan acara yang gagal dalam semua upaya pemrosesan. Atau, Anda dapat mengonfigurasi SQS antrian Amazon standar atau SNS topik Amazon standar sebagai antrian huruf mati untuk acara yang dibuang. Untuk antrian dead-letter, Lambda hanya mengirimkan konten acara, tanpa perincian tentang responsnya.

Jika Lambda tidak dapat mengirim catatan ke tujuan yang telah Anda konfigurasi, Lambda akan mengirimkan `DestinationDeliveryFailures` metrik ke Amazon. CloudWatch Hal ini dapat terjadi jika konfigurasi Anda menyertakan jenis tujuan yang tidak didukung, seperti SQS FIFO antrian Amazon atau topik Amazon SNSFIFO. Kesalahan pengiriman juga dapat terjadi karena kesalahan izin dan batas ukuran. Untuk informasi selengkapnya tentang metrik pemanggilan Lambda, lihat.

[Metrik invokasi](#)

Note

Untuk mencegah fungsi memicu, Anda dapat mengatur konkurensi cadangan fungsi ke nol. [Saat Anda menyetel konkurensi cadangan ke nol untuk fungsi yang dipanggil secara asinkron, Lambda mulai mengirim peristiwa baru ke antrian huruf mati yang dikonfigurasi atau tujuan peristiwa yang sedang gagal, tanpa mencoba lagi.](#) Untuk memproses peristiwa yang dikirim saat konkurensi cadangan disetel ke nol, Anda harus menggunakan peristiwa dari antrian surat mati atau tujuan acara yang gagal.

Menambahkan tujuan

Untuk menyimpan catatan pemanggilan asinkron, tambahkan tujuan ke fungsi Anda. Anda dapat memilih untuk mengirim pemanggilan yang berhasil atau gagal ke tujuan. Setiap fungsi dapat memiliki beberapa tujuan, sehingga Anda dapat mengonfigurasi tujuan terpisah untuk acara yang berhasil dan gagal. Setiap catatan yang dikirim ke tujuan adalah JSON dokumen dengan rincian tentang doa. Seperti pengaturan penanganan kesalahan, Anda dapat mengonfigurasi tujuan pada fungsi, versi fungsi, atau alias.

Note

[Anda juga dapat menyimpan catatan pemanggilan gagal untuk jenis pemetaan sumber peristiwa berikut: Amazon Kinesis, Amazon DynamoDB, ApacheKafka yang dikelola sendiri, dan Amazon. MSK](#)

Tabel berikut mencantumkan tujuan yang didukung untuk catatan pemanggilan asinkron. Agar Lambda berhasil mengirim catatan ke tujuan yang Anda pilih, pastikan [peran eksekusi](#) fungsi Anda juga berisi izin yang relevan. Tabel juga menjelaskan bagaimana setiap tipe tujuan menerima catatan JSON pemanggilan.

| Jenis tujuan | Izin yang diperlukan | Format khusus tujuan JSON |
|-------------------|--------------------------------------|--|
| SQSAntrian Amazon | persegi: SendMessage | Lambda melewati catatan doa sebagai ke tujuan. Message |
| SNSTopik Amazon | SNS: Publikasikan | Lambda melewati catatan doa sebagai ke tujuan. Message |
| Fungsi Lambda | InvokeFunction | Lambda meneruskan catatan pemanggilan sebagai muatan ke fungsi. |
| EventBridge | peristiwa: PutEvents | <ul style="list-style-type: none"> Lambda melewati catatan pemanggilan seperti dalam panggilan. <code>detail PutEvents</code> |

| Jenis tujuan | Izin yang diperlukan | Format khusus tujuan JSON |
|--------------|----------------------|---|
| | | <ul style="list-style-type: none"> • Nilai untuk bidang <code>source</code> acara adalah <code>Lambda</code>. • Nilai untuk bidang <code>detail-type</code> acara adalah “Hasil Pemanggilan Fungsi Lambda - Sukses” atau “Hasil Pemanggilan Fungsi Lambda - Kegagalan”. • Bidang <code>resource</code> acara berisi fungsi dan tujuan Amazon Resource Names (ARNs). • Untuk bidang acara lainnya, lihat EventBridge Acara Amazon. |

Langkah-langkah berikut menjelaskan cara mengonfigurasi tujuan untuk suatu fungsi menggunakan konsol Lambda dan AWS CLI

Console

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambahkan tujuan.
4. Untuk Sumber, pilih Invokasi asinkron.
5. Untuk Kondisi, pilih dari opsi berikut:
 - Kegagalan – Kirimkan catatan saat peristiwa gagal dalam semua upaya pemrosesan atau melebihi waktu maksimum.
 - Sukses – Kirimkan catatan saat fungsi berhasil memproses invokasi asinkron.
6. Untuk Jenis tujuan, pilih jenis sumber daya yang menerima catatan invokasi.
7. Untuk Tujuan, pilih sumber daya.
8. Pilih Simpan.

AWS CLI

Untuk mengkonfigurasi tujuan menggunakan AWS CLI, jalankan perintah [update-function-event-invoke-config](#). Contoh berikut mengonfigurasi Lambda untuk mengirim catatan ke antrian SQS standar `destination` bernama saat peristiwa tidak dapat diproses.

```
aws lambda update-function-event-invoke-config \  
  --function-name my-function \  
  --destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-  
east-1:123456789012:destination"}}'
```

Ketika pemanggilan cocok dengan kondisi, Lambda mengirimkan [JSONdokumen dengan](#) rincian tentang pemanggilan ke tujuan. Contoh berikut menunjukkan catatan invokasi untuk peristiwa yang gagal dalam tiga upaya pemrosesan karena kesalahan fungsi.

Example rekaman invokasi

```
{  
  "version": "1.0",  
  "timestamp": "2019-11-14T18:16:05.568Z",  
  "requestContext": {  
    "requestId": "e4b46cbf-b738-xmpl-8880-a18cdf61200e",  
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function:  
$LATEST",  
    "condition": "RetriesExhausted",  
    "approximateInvokeCount": 3  
  },  
  "requestPayload": {  
    "ORDER_IDS": [  
      "9e07af03-ce31-4ff3-xmpl-36dce652cb4f",  
      "637de236-e7b2-464e-xmpl-baf57f86bb53",  
      "a81ddca6-2c35-45c7-xmpl-c3a03a31ed15"  
    ]  
  },  
  "responseContext": {  
    "statusCode": 200,  
    "executedVersion": "$LATEST",  
    "functionError": "Unhandled"  
  },  
  "responsePayload": {  
    "errorMessage": "RequestId: e4b46cbf-b738-xmpl-8880-a18cdf61200e Process exited  
before completing request"  
  }  
}
```

```
}  
}  
}
```

Catatan invokasi berisi perincian tentang peristiwa, respons, dan alasan mengapa catatan dikirim.

Menelusuri permintaan ke tujuan

Anda dapat menggunakan AWS X-Ray untuk melihat tampilan terhubung dari setiap permintaan saat antrian, diproses oleh fungsi Lambda, dan diteruskan ke layanan tujuan. Saat Anda mengaktifkan penelusuran X-Ray untuk fungsi atau layanan yang memanggil fungsi, Lambda menambahkan header X-Ray ke permintaan dan meneruskan header ke layanan tujuan. Jejak dari layanan hulu secara otomatis ditautkan ke jejak dari fungsi Lambda hilir dan layanan tujuan, menciptakan end-to-end tampilan seluruh aplikasi. Untuk informasi lebih lanjut tentang penelusuran, lihat [Visualisasikan pemanggilan fungsi Lambda menggunakan AWS X-Ray](#).

Menambahkan antrian huruf mati

Sebagai alternatif untuk [tujuan kegagalan](#), Anda dapat mengonfigurasi fungsi Anda dengan antrian dead-letter untuk menyimpan kejadian yang telah dihapus untuk pemrosesan lebih lanjut. Antrian dead-letter juga berfungsi sama seperti tujuan kegagalan dalam kondisi di mana ini digunakan saat suatu kejadian gagal dalam semua upaya pemrosesan atau kedaluwarsa tanpa diproses. Namun, Anda hanya dapat menambah atau menghapus antrian huruf mati di tingkat fungsi. Versi fungsi menggunakan pengaturan antrian huruf mati yang sama dengan versi yang tidak dipublikasikan (\$). LATEST Tujuan kegagalan juga mendukung target tambahan dan mencakup perincian tentang respons fungsi dalam catatan invokasi.

Untuk memproses ulang peristiwa dalam antrian huruf mati, Anda dapat mengaturnya sebagai sumber [peristiwa untuk](#) fungsi Lambda Anda. Atau, Anda dapat mengambil acara secara manual.

Anda dapat memilih antrian SQS standar Amazon atau topik SNS standar Amazon untuk antrian surat mati Anda. FIFO antrian dan SNS FIFO topik Amazon tidak didukung.

- [SQS Antrian Amazon](#) — Antrian menyimpan peristiwa yang gagal hingga diambil. Pilih antrian SQS standar Amazon jika Anda mengharapkan satu entitas, seperti fungsi Lambda CloudWatch atau alarm, untuk memproses peristiwa yang gagal. Untuk informasi selengkapnya, lihat [Menggunakan Lambda dengan Amazon SQS](#).
- [SNS Topik Amazon](#) — Sebuah topik menyampaikan peristiwa yang gagal ke satu atau beberapa tujuan. Pilih topik SNS standar Amazon jika Anda mengharapkan beberapa entitas bertindak atas peristiwa yang gagal. Misalnya, Anda dapat mengonfigurasi topik untuk mengirim peristiwa

ke alamat email, fungsi Lambda, dan/atau titik akhir. HTTP Untuk informasi selengkapnya, lihat [Memanggil fungsi Lambda dengan notifikasi Amazon SNS](#).

Untuk mengirim acara ke antrean atau topik, fungsi Anda memerlukan izin tambahan. Tambahkan kebijakan dengan [izin yang diperlukan](#) ke [peran eksekusi](#) fungsi Anda.

Jika antrean atau topik target dienkripsi dengan kunci yang dikelola pelanggan, peran eksekusi juga harus menjadi pengguna dalam [kebijakan berbasis sumber daya](#) kunci.

Setelah membuat target dan memperbarui peran eksekusi fungsi Anda, tambahkan antrean dead-letter ke fungsi Anda. Anda dapat mengonfigurasi beberapa fungsi untuk mengirimkan peristiwa ke target yang sama.

Console

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi, lalu pilih Invokasi asinkron.
4. Di bagian Invokasi asinkron, pilih Edit.
5. Atur layanan antrian Dead-letter ke Amazon atau SQS Amazon. SNS
6. Pilih antrean atau topik target.
7. Pilih Simpan.

AWS CLI

Untuk mengkonfigurasi antrian huruf mati dengan AWS CLI, gunakan perintah. [update-function-configuration](#)

```
aws lambda update-function-configuration \  
  --function-name my-function \  
  --dead-letter-config TargetArn=arn:aws:sns:us-east-1:123456789012:my-topic
```

Lambda mengirimkan peristiwa ke antrean surat mati sebagaimana adanya, dengan informasi tambahan dalam atribut. Anda dapat menggunakan informasi ini untuk mengidentifikasi kesalahan yang dikembalikan fungsi, atau untuk menghubungkan peristiwa dengan log atau jejak AWS X-Ray .

Atribut pesan antrean surat mati

- RequestID (String) – ID permintaan invokasi. Permintaan IDs muncul dalam log fungsi. Anda juga dapat menggunakan X-Ray SDK untuk merekam ID permintaan pada atribut dalam jejak. Kemudian, Anda dapat mencari jejak berdasarkan ID permintaan di konsol X-Ray.
- ErrorCode(Nomor) — Kode HTTP status.
- ErrorMessage(String) - 1 KB pertama dari pesan kesalahan.

Jika Lambda tidak dapat mengirim pesan ke antrean huruf mati, Lambda akan menghapus acara dan memancarkan metrik. [DeadLetterErrors](#) Ini dapat terjadi karena kurangnya izin, atau jika ukuran total pesan melebihi batasan untuk antrean atau topik target. Misalnya, katakan bahwa SNS notifikasi Amazon dengan ukuran tubuh mendekati 256 KB memicu fungsi yang menghasilkan kesalahan. Dalam hal ini, data peristiwa yang SNS ditambahkan Amazon, dikombinasikan dengan atribut yang ditambahkan Lambda, dapat menyebabkan pesan melebihi ukuran maksimum yang diizinkan dalam antrian huruf mati.

Jika Anda menggunakan Amazon SQS sebagai sumber peristiwa, konfigurasi antrian huruf mati di SQS antrian Amazon itu sendiri dan bukan pada fungsi Lambda. Untuk informasi selengkapnya, lihat [Menggunakan Lambda dengan Amazon SQS](#).

Bagaimana Lambda memproses catatan dari sumber acara berbasis streaming dan antrian

Pemetaan sumber peristiwa adalah sumber daya Lambda yang membaca item dari layanan berbasis streaming dan antrian dan memanggil fungsi dengan kumpulan catatan. Layanan berikut menggunakan pemetaan sumber peristiwa untuk menjalankan fungsi Lambda:

- [Amazon DocumentDB \(dengan kompatibilitas MongoDB\) \(Amazon DocumentDB\)](#)
- [Amazon DynamoDB](#)
- [Amazon Kinesis](#)
- [Amazon MQ](#)
- [Amazon Managed Streaming for Apache Kafka \(Amazon\) MSK](#)
- [Apache Kafka yang dikelola sendiri](#)
- [Layanan Antrian Sederhana Amazon \(AmazonSQS\)](#)

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Bagaimana pemetaan sumber peristiwa berbeda dari pemicu langsung

Beberapa AWS layanan dapat langsung memanggil fungsi Lambda menggunakan pemicu. Layanan ini mendorong peristiwa ke Lambda, dan fungsi segera dipanggil saat peristiwa yang ditentukan terjadi. Pemicu cocok untuk peristiwa diskrit dan pemrosesan waktu nyata. Saat Anda [membuat pemicu menggunakan konsol Lambda, konsol](#) berinteraksi dengan AWS layanan terkait untuk mengonfigurasi pemberitahuan peristiwa pada layanan tersebut. Pemicunya sebenarnya disimpan dan dikelola oleh layanan yang menghasilkan peristiwa, bukan oleh Lambda. Berikut adalah beberapa contoh layanan yang menggunakan pemicu untuk menjalankan fungsi Lambda:

- Amazon Simple Storage Service (Amazon S3): Memanggil fungsi saat objek dibuat, dihapus, atau dimodifikasi dalam bucket. Untuk informasi selengkapnya, lihat [Tutorial: Menggunakan pemicu Amazon S3 untuk memanggil fungsi Lambda](#).
- Amazon Simple Notification Service (Amazon SNS): Memanggil fungsi saat pesan dipublikasikan ke suatu SNS topik. Untuk informasi selengkapnya, lihat [Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service](#).
- Amazon API Gateway: Memanggil fungsi saat API permintaan dibuat ke titik akhir tertentu. Untuk informasi selengkapnya, lihat [Memanggil fungsi Lambda menggunakan titik akhir Amazon Gateway API](#).

Pemetaan sumber peristiwa adalah sumber daya Lambda yang dibuat dan dikelola dalam layanan Lambda. Pemetaan sumber peristiwa dirancang untuk memproses data streaming volume tinggi atau pesan dari antrian. Memproses catatan dari aliran atau antrian dalam batch lebih efisien daripada memproses catatan secara individual.

Perilaku batching

Secara default, pemetaan sumber peristiwa mengumpulkan catatan bersama menjadi satu muatan yang dikirim Lambda ke fungsi Anda. Untuk menyempurnakan perilaku batching, Anda dapat mengonfigurasi jendela batching ([MaximumBatchingWindowInSeconds](#)) dan ukuran batch ([BatchSize](#)). Jendela batching adalah jumlah waktu maksimum untuk mengumpulkan catatan ke dalam satu muatan. Ukuran batch adalah jumlah maksimum catatan dalam satu batch. Lambda memanggil fungsi Anda ketika salah satu dari tiga kriteria berikut terpenuhi:

- Jendela batching mencapai nilai maksimumnya. Perilaku jendela batching default bervariasi tergantung pada sumber peristiwa tertentu.
 - Untuk sumber peristiwa Kinesis, DynamoDB, dan SQS Amazon: Jendela batching default adalah 0 detik. Ini berarti Lambda memanggil fungsi Anda segera setelah catatan tersedia. Untuk mengatur jendela batching, konfigurasi `MaximumBatchingWindowInSeconds`. Anda dapat mengatur parameter ini ke nilai apa pun dari 0 hingga 300 detik dengan penambahan 1 detik. Jika Anda mengonfigurasi jendela batching, jendela berikutnya dimulai segera setelah pemanggilan fungsi sebelumnya selesai.
 - Untuk AmazonMSK, sumber acara Apache Kafka, Amazon MQ, dan Amazon DocumentDB yang dikelola sendiri: Jendela batching default adalah 500 ms. Anda dapat mengonfigurasi `MaximumBatchingWindowInSeconds` ke nilai apa pun dari 0 detik hingga 300 detik dengan penambahan detik. Jendela batching dimulai segera setelah rekor pertama tiba.

Note

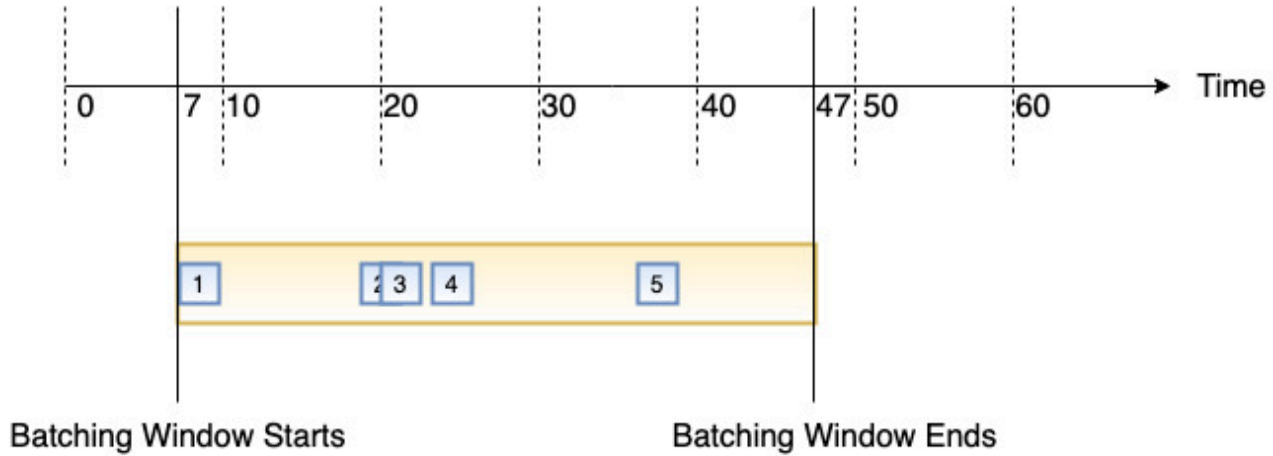
Karena Anda hanya dapat mengubah `MaximumBatchingWindowInSeconds` dalam beberapa detik, Anda tidak dapat kembali ke jendela batching default 500 ms setelah Anda mengubahnya. Untuk mengembalikan jendela batching default, Anda harus membuat pemetaan sumber peristiwa baru.

- Ukuran batch terpenuhi. Ukuran batch minimum adalah 1. Ukuran batch default dan maksimum bergantung pada sumber acara. Untuk detail tentang nilai-nilai ini, lihat [Batch Sizes](#) spesifikasi untuk `CreateEventSourceMapping` API operasi.
- Ukuran payload mencapai [6 MB](#). Anda tidak dapat mengubah batas ini.

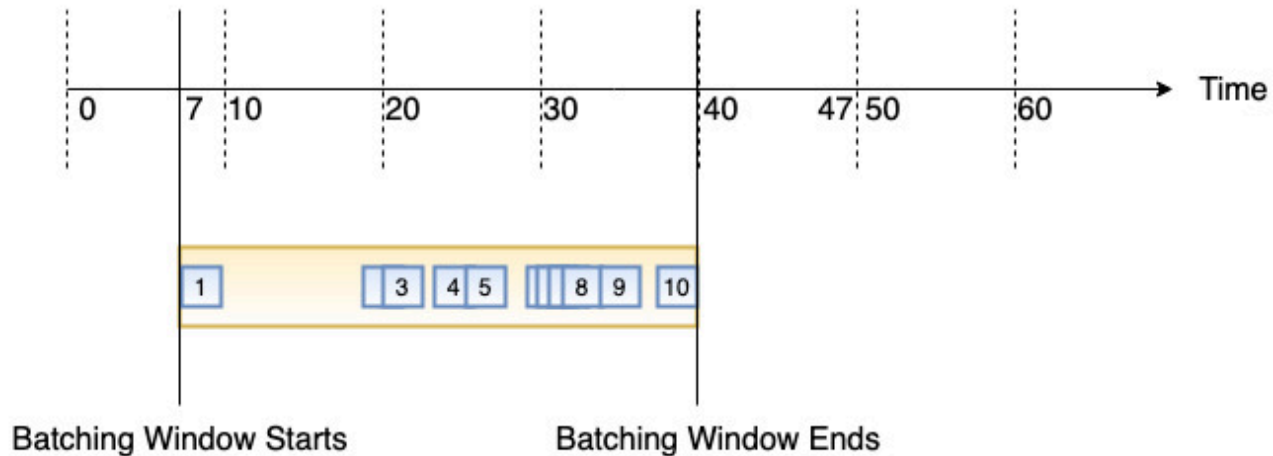
Diagram berikut menggambarkan ketiga kondisi ini. Misalkan jendela batching dimulai pada $t = 7$ detik. Dalam skenario pertama, jendela batching mencapai maksimum 40 detik pada $t = 47$ detik setelah mengumpulkan 5 catatan. Dalam skenario kedua, ukuran batch mencapai 10 sebelum jendela batching berakhir, sehingga jendela batching berakhir lebih awal. Dalam skenario ketiga, ukuran muatan maksimum tercapai sebelum jendela batching berakhir, sehingga jendela batching berakhir lebih awal.

Max Batching Window = 40 Seconds
Max Batch Size = 10
Max Batch Size in Bytes = 6 MB

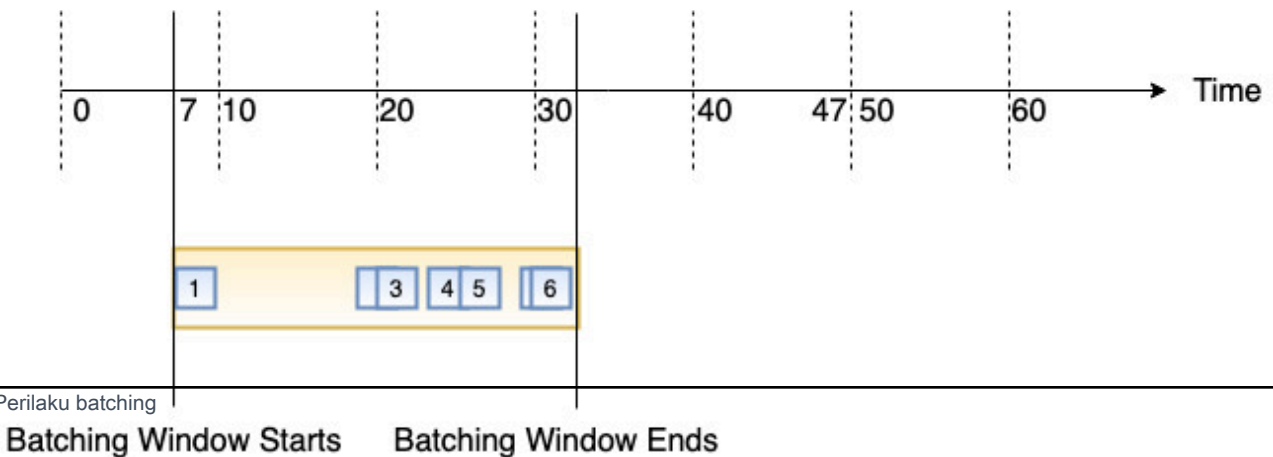
(1) Batching Window Expires



(2) Batching Size is reached



(3) Batch Size in bytes is reached



Kami menyarankan Anda menguji dengan ukuran batch dan rekaman yang berbeda sehingga frekuensi polling dari setiap sumber acara disetel ke seberapa cepat fungsi Anda dapat menyelesaikan tugasnya. [CreateEventSourceMapping](#) BatchSize Parameter mengontrol jumlah maksimum catatan yang dapat dikirim ke fungsi Anda dengan setiap pemanggilan. Ukuran batch yang lebih besar sering kali dapat menyerap overhead secara lebih efisien di serangkaian catatan yang lebih besar, sehingga meningkatkan throughput Anda.

Lambda tidak menunggu [ekstensi](#) yang dikonfigurasi selesai sebelum mengirim batch berikutnya untuk diproses. Dengan kata lain, ekstensi Anda dapat terus berjalan saat Lambda memproses kumpulan catatan berikutnya. Hal ini dapat menyebabkan masalah pembatasan jika Anda melanggar pengaturan atau [batasan konkurensi](#) akun Anda. Untuk mendeteksi apakah ini merupakan masalah potensial, pantau fungsi Anda dan periksa apakah Anda melihat [metrik konkurensi](#) yang lebih tinggi dari yang diharapkan untuk pemetaan sumber peristiwa Anda. Karena waktu yang singkat di antara pemanggilan, Lambda mungkin secara singkat melaporkan penggunaan konkurensi yang lebih tinggi daripada jumlah pecahan. Ini bisa benar bahkan untuk fungsi Lambda tanpa ekstensi.

Secara default, jika fungsi Anda mengembalikan kesalahan, pemetaan sumber peristiwa memproses ulang seluruh batch hingga fungsi berhasil, atau item dalam batch kedaluwarsa. Untuk memastikan pemrosesan dalam urutan, pemetaan sumber peristiwa menghentikan pemrosesan untuk pecahan yang terpengaruh hingga kesalahan teratasi. Untuk sumber aliran (DynamoDB dan Kinesis), Anda dapat mengonfigurasi jumlah maksimum kali Lambda mencoba ulang saat fungsi Anda mengembalikan kesalahan. Kesalahan layanan atau pembatasan di mana batch tidak mencapai fungsi Anda tidak diperhitungkan dalam upaya coba lagi. Anda juga dapat mengonfigurasi pemetaan sumber peristiwa untuk mengirim catatan pemanggilan ke [tujuan](#) saat membuang kumpulan peristiwa.

API pemetaan sumber kejadian

Untuk mengelola sumber peristiwa dengan [AWS Command Line Interface \(AWS CLI\)](#) atau [AWS SDK](#), Anda dapat menggunakan API operasi berikut:

- [CreateEventSourceMapping](#)
- [ListEventSourceMappings](#)
- [GetEventSourceMapping](#)
- [UpdateEventSourceMapping](#)
- [DeleteEventSourceMapping](#)

Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Misalnya, Anda dapat menambahkan filter sehingga fungsi Anda hanya memproses SQS pesan Amazon yang berisi parameter data tertentu. Pemfilteran acara hanya berfungsi dengan pemetaan sumber peristiwa tertentu. Anda dapat menambahkan filter ke pemetaan sumber peristiwa untuk layanan berikut: AWS

- Amazon DynamoDB
- Amazon Kinesis Data Streams
- Amazon MQ
- Amazon Managed Streaming for Apache Kafka (Amazon) MSK
- Apache Kafka yang dikelola sendiri
- Layanan Antrian Sederhana Amazon (AmazonSQS)

Untuk informasi spesifik tentang pemfilteran dengan sumber peristiwa tertentu, lihat [the section called “Menggunakan filter dengan berbeda AWS layanan”](#). Lambda tidak mendukung pemfilteran acara untuk Amazon DocumentDB.

Secara default, Anda dapat menentukan hingga lima filter berbeda untuk pemetaan sumber peristiwa tunggal. Filter Anda secara logis ORed bersama-sama. Jika rekaman dari sumber acara memenuhi satu atau beberapa filter Anda, Lambda menyertakan catatan di acara berikutnya yang dikirim ke fungsi Anda. Jika tidak ada filter Anda yang puas, Lambda membuang catatan tersebut.

Note

Jika Anda perlu menentukan lebih dari lima filter untuk sumber peristiwa, Anda dapat meminta peningkatan kuota hingga 10 filter untuk setiap sumber peristiwa. Jika Anda mencoba menambahkan lebih banyak filter daripada yang diizinkan kuota saat ini, Lambda akan menampilkan kesalahan saat Anda mencoba membuat sumber acara.

Topik

- [Memahami dasar-dasar penyaringan acara](#)
- [Menangani catatan yang tidak memenuhi kriteria filter](#)
- [Filter sintaks aturan](#)

- [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#)
- [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(\)AWS CLI](#)
- [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(\)AWS SAM](#)
- [Enkripsi kriteria filter](#)
- [Menggunakan filter dengan berbeda AWS layanan](#)

Memahami dasar-dasar penyaringan acara

Objek filter criteria (`FilterCriteria`) adalah struktur yang terdiri dari daftar filter (`Filters`). Setiap filter adalah struktur yang mendefinisikan pola penyaringan peristiwa (`Pattern`). Pola adalah representasi string dari aturan JSON filter. Struktur suatu `FilterCriteria` objek adalah sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"Metadata1\": [ rule1 ], \"data\": { \"Data1\": [ rule2 ] } }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```
{
  "Metadata1": [ rule1 ],
  "data": {
    "Data1": [ rule2 ]
  }
}
```

Pola filter Anda dapat mencakup properti metadata, properti data, atau keduanya. Parameter metadata yang tersedia dan format parameter data bervariasi sesuai dengan AWS layanan yang bertindak sebagai sumber peristiwa. Misalnya, misalkan pemetaan sumber peristiwa Anda menerima catatan berikut dari SQS antrian Amazon:

```
{
  "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
```

```

"receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
"body": "{\n \"City\": \"Seattle\",\n \"State\": \"WA\",\n \"Temperature\": \"46\"\n}",
"attributes": {
  "ApproximateReceiveCount": "1",
  "SentTimestamp": "1545082649183",
  "SenderId": "AIDAIENQZJOL023YVJ4V0",
  "ApproximateFirstReceiveTimestamp": "1545082649185"
},
"messageAttributes": {},
"md5ofBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
"eventSource": "aws:sqs",
"eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
"awsRegion": "us-east-2"
}

```

- Properti metadata adalah bidang yang berisi informasi tentang peristiwa yang membuat catatan. Dalam contoh SQS catatan Amazon, properti metadata menyertakan bidang seperti `messageID`, `eventSourceArn`, dan `awsRegion`
- Properti data adalah bidang catatan yang berisi data dari aliran atau antrian Anda. Dalam contoh SQS peristiwa Amazon, kunci untuk bidang data adalah `body`, dan properti data adalah bidang `CityState`, dan `Temperature`.

Berbagai jenis sumber acara menggunakan nilai kunci yang berbeda untuk bidang datanya. Untuk memfilter properti data, pastikan Anda menggunakan kunci yang benar dalam pola filter Anda. Untuk daftar kunci pemfilteran data, dan untuk melihat contoh pola filter untuk setiap yang didukung AWS layanan, lihat. [Menggunakan filter dengan berbeda AWS layanan](#)

Pemfilteran acara dapat menangani penyaringan multi-level JSON. Misalnya, pertimbangkan fragmen catatan berikut dari aliran DynamoDB:

```

"dynamodb": {
  "Keys": {
    "ID": {
      "S": "ABCD"
    }
    "Number": {
      "N": "1234"
    }
  },
  ...
}

```

Misalkan Anda hanya ingin memproses catatan tersebut di mana nilai kunci sortir `Number` adalah `4567`. Dalam hal ini, `FilterCriteria` objek Anda akan terlihat seperti ini:

```
{
  "Filters": [
    {
      "Pattern": "{ \"dynamodb\": { \"Keys\": { \"Number\": { \"N\":
[ \"4567\" ] } } } }]"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```
{
  "dynamodb": {
    "Keys": {
      "Number": {
        "N": [ "4567" ]
      }
    }
  }
}
```

Menangani catatan yang tidak memenuhi kriteria filter

Cara Lambda menangani catatan yang tidak memenuhi kriteria filter Anda tergantung pada sumber acara.

- Untuk Amazon SQS, jika pesan tidak memenuhi kriteria filter Anda, Lambda secara otomatis menghapus pesan dari antrian. Anda tidak perlu menghapus pesan-pesan ini secara manual di AmazonSQS.
- Untuk Kinesis dan DynamoDB, setelah kriteria filter Anda mengevaluasi sebuah record, iterator stream akan melewati catatan ini. Jika catatan tidak memenuhi kriteria filter Anda, Anda tidak perlu menghapus catatan secara manual dari sumber acara Anda. Setelah periode retensi, Kinesis dan DynamoDB secara otomatis menghapus catatan lama ini. Jika Anda ingin catatan dihapus lebih cepat, lihat [Mengubah Periode Retensi Data](#).
- Untuk Amazon MSK, Apache Kafka yang dikelola sendiri, dan pesan Amazon MQ, Lambda menghapus pesan yang tidak cocok dengan semua bidang yang disertakan dalam filter. Untuk

Amazon MSK dan Apache Kafka yang dikelola sendiri, Lambda melakukan offset untuk pesan yang cocok dan tak tertandingi setelah berhasil menjalankan fungsi. Untuk Amazon MQ, Lambda mengakui pesan yang cocok setelah berhasil menjalankan fungsi, dan mengakui pesan yang tak tertandingi saat memfilternya.

Filter sintaks aturan

Untuk aturan filter, Lambda mendukung EventBridge aturan Amazon dan menggunakan sintaks yang sama seperti EventBridge. Untuk informasi selengkapnya, lihat [pola EventBridge acara Amazon](#) di Panduan EventBridge Pengguna Amazon.

Berikut ini adalah ringkasan dari semua operator perbandingan yang tersedia untuk pemfilteran acara Lambda.

| Operator perbandingan | Contoh | Sintaks aturan |
|-----------------------------|---|---|
| Kosong | UserID adalah kosong | "userId": [null] |
| Kosong | LastName kosong | "LastName": [""] |
| Setara | Namanya adalah "Alice" | "Name": ["Alice"] |
| Sama dengan (abaikan kasus) | Namanya adalah "Alice" | "Name": [{"equals-ignore-case": "alice"}] |
| Dan | Lokasi adalah "New York" dan Hari adalah "Senin" | "Lokasi": ["New York"], "Hari": ["Senin"] |
| Atau | PaymentType adalah "Kredit" atau "Debit" | "PaymentType": ["Kredit", "Debit"] |
| Atau (beberapa bidang) | Lokasi adalah "New York", atau Hari adalah "Senin". | "\$or": [{"Lokasi": ["New York"]}, {"Hari": ["Senin"]}] |
| Bukan | Cuaca hanyalah "Hujan" | "Weather": [{"anything-but": ["Hujan"]}] |
| Numerik (sama dengan) | Harga 100 | "Harga": [{"numerik": ["=", 100]}] |

| Operator perbandingan | Contoh | Sintaks aturan |
|-----------------------|--|---|
| Numerik (rentang) | Harga lebih dari 10, dan kurang dari atau sama dengan 20 | "Harga": [{"numerik": [">", 10, "<=", 20]}] |
| Exists | ProductName ada | "ProductName": [{"exists": true}] |
| Tidak ada | ProductName tidak ada | "ProductName": [{"exists": false}] |
| Dimulai dengan | Wilayah ada di AS | "Region": [{"prefix": "us-"}] |
| Ends with | FileName diakhiri dengan ekstensi.png. | "FileName": [{"akhiran": ".png"}] |

Note

Seperti EventBridge, untuk string, Lambda menggunakan pencocokan character-by-character yang tepat tanpa case folding atau normalisasi string lainnya. Untuk angka, Lambda juga menggunakan representasi string. Sebagai contoh, 300, 300,0, dan 3,0e2 dianggap tidak sama.

Perhatikan bahwa operator Exists hanya bekerja pada node daun di sumber acara AndaJSON. Itu tidak cocok dengan node perantara. Misalnya, dengan berikut iniJSON, pola filter tidak `{ "person": { "address": [{ "exists": true }] } }` akan menemukan kecocokan karena "address" merupakan simpul perantara.

```
{
  "person": {
    "name": "John Doe",
    "age": 30,
    "address": {
      "street": "123 Main St",
      "city": "Anytown",
      "country": "USA"
    }
  }
}
```

```
}
}
```

Melampirkan kriteria filter ke pemetaan sumber peristiwa (konsol)

Ikuti langkah-langkah ini untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter menggunakan konsol Lambda.

Untuk membuat pemetaan sumber acara baru dengan kriteria filter (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi untuk membuat pemetaan sumber peristiwa.
3. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.
4. Untuk konfigurasi Trigger, pilih jenis pemicu yang mendukung pemfilteran peristiwa. Untuk daftar layanan yang didukung, lihat daftar di awal halaman ini.
5. Perluas Pengaturan tambahan.
6. Di bawah Kriteria filter, pilih Tambah, lalu tentukan dan masukkan filter Anda. Misalnya, Anda dapat memasukkan yang berikut ini.

```
{ "Metadata" : [ 1, 2 ] }
```

Ini menginstruksikan Lambda untuk memproses hanya catatan di mana Metadata a bidang sama dengan 1 atau 2. Anda dapat terus memilih Tambah untuk menambahkan lebih banyak filter hingga jumlah maksimum yang diizinkan.

7. Setelah selesai menambahkan filter, pilih Simpan.

Saat Anda memasukkan kriteria filter menggunakan konsol, Anda hanya memasukkan pola filter dan tidak perlu memberikan tanda kutip Pattern kunci atau escape. Pada langkah 6 dari instruksi sebelumnya, { "Metadata" : [1, 2] } sesuai dengan yang berikut ini. FilterCriteria

```
{
  "Filters": [
    {
      "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
    }
  ]
}
```

Setelah membuat pemetaan sumber acara di konsol, Anda dapat melihat format `FilterCriteria` dalam detail pemicu. Untuk lebih banyak contoh pembuatan filter acara menggunakan konsol, lihat [Menggunakan filter dengan berbeda AWS layanan](#).

Melampirkan kriteria filter ke pemetaan sumber peristiwa ()AWS CLI

Misalkan Anda ingin pemetaan sumber peristiwa memiliki yang berikut: `FilterCriteria`

```
{
  "Filters": [
    {
      "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
    }
  ]
}
```

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ] }"}]}'
```

[create-event-source-mapping](#) Perintah ini membuat pemetaan sumber SQS peristiwa Amazon baru untuk fungsi `my-function` dengan yang ditentukan `FilterCriteria`.

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ] }"}]}'
```

Perhatikan bahwa untuk memperbarui pemetaan sumber peristiwa, Anda memerlukannya `UUID`. Anda bisa mendapatkan `UUID` dari [list-event-source-mappings](#) panggilan. Lambda juga mengembalikan `UUID` respons. [create-event-source-mapping](#) CLI

Untuk menghapus kriteria filter dari sumber peristiwa, Anda dapat menjalankan [update-event-source-mapping](#) perintah berikut dengan `FilterCriteria` objek kosong.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria "{}"
```

Untuk lebih banyak contoh pembuatan filter acara menggunakan AWS CLI, lihat [Menggunakan filter dengan berbeda AWS layanan](#).

Melampirkan kriteria filter ke pemetaan sumber peristiwa (AWS SAM)

Misalkan Anda ingin mengonfigurasi sumber acara AWS SAM untuk menggunakan kriteria filter berikut:

```
{
  "Filters": [
    {
      "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
    }
  ]
}
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber acara Anda, masukkan cuplikan berikut ke dalam YAML templat untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{"Metadata": [1, 2]}'
```

Untuk informasi selengkapnya tentang membuat dan mengonfigurasi AWS SAM templat untuk pemetaan sumber peristiwa, lihat [EventSource](#) bagian Panduan AWS SAM Pengembang. Untuk lebih banyak contoh pembuatan filter acara menggunakan AWS SAM templat, lihat [Menggunakan filter dengan berbeda AWS layanan](#).

Enkripsi kriteria filter

Secara default, Lambda tidak mengenkripsi objek kriteria filter Anda. Untuk kasus penggunaan di mana Anda dapat menyertakan informasi sensitif dalam objek kriteria filter Anda, Anda dapat menggunakan [KMSkunci](#) Anda sendiri untuk mengenkripsinya.

Setelah mengenkripsi objek kriteria filter, Anda dapat melihat versi teks biasa menggunakan panggilan. [GetEventSourceMapping](#) API Anda harus memiliki `kms:Decrypt` izin untuk dapat berhasil melihat kriteria filter dalam teks biasa.

Note

Jika objek kriteria filter Anda dienkripsi, Lambda menyunting nilai `FilterCriteria` bidang dalam respons panggilan. [ListEventSourceMappings](#) Sebaliknya, bidang ini ditampilkan sebagai `null`. Untuk melihat nilai sebenarnya dari `FilterCriteria`, gunakan [GetEventSourceMapping](#) API.

Untuk melihat nilai yang didekripsi `FilterCriteria` di konsol, pastikan IAM peran Anda berisi izin untuk. [GetEventSourceMapping](#)

Anda dapat menentukan KMS kunci Anda sendiri melalui konsol, API/CLI, atau AWS CloudFormation.

Untuk mengenkripsi kriteria filter dengan KMS kunci milik pelanggan (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih Tambahkan pemicu. Jika Anda sudah memiliki pemicu yang ada, pilih tab Konfigurasi, lalu pilih Pemicu. Pilih pemicu yang ada, dan pilih Edit.
3. Pilih kotak centang di samping Enkripsi dengan kunci terkelola KMS pelanggan.
4. Untuk Pilih kunci KMS enkripsi terkelola pelanggan, pilih kunci aktif yang ada atau buat kunci baru. Bergantung pada operasinya, Anda memerlukan beberapa atau semua izin berikut: `kms:DescribeKey`, `kms:GenerateDataKey`, dan `kms:Decrypt`. Gunakan kebijakan KMS kunci untuk memberikan izin ini.

Jika Anda menggunakan KMS kunci Anda sendiri, API operasi berikut harus diizinkan dalam [kebijakan kunci](#):

- `kms:Decrypt`— Harus diberikan kepada kepala layanan Lambda regional (`lambda.AWS_region.amazonaws.com`). Ini memungkinkan Lambda untuk mendekripsi data dengan kunci ini. KMS
- Untuk mencegah [masalah wakil lintas layanan yang membingungkan](#), kebijakan kunci menggunakan kunci kondisi `aws:SourceArn` global. Nilai `aws:SourceArn` kunci yang benar adalah sumber daya pemetaan sumber peristiwa, sehingga Anda dapat menambahkan ini ke kebijakan hanya setelah Anda mengetahuinya. ARN ARN Lambda juga meneruskan

`aws:lambda:EventSourceArn` kunci `aws:lambda:FunctionArn` dan dan nilainya masing-masing dalam [konteks enkripsi](#) saat membuat permintaan dekripsi ke KMS. Nilai-nilai ini harus sesuai dengan kondisi yang ditentukan dalam kebijakan kunci agar permintaan dekripsi berhasil. Anda tidak perlu menyertakan `EventSourceArn` sumber acara Kafka yang dikelola sendiri karena mereka tidak memiliki `EventSourceArn`.

- `kms:Decrypt`— Juga harus diberikan kepada kepala sekolah yang bermaksud menggunakan kunci untuk melihat kriteria filter teks biasa dalam [GetEventSourceMapping](#) atau panggilan [DeleteEventSourceMappingAPI](#).
- `kms:DescribeKey`— Memberikan rincian kunci yang dikelola pelanggan untuk memungkinkan prinsipal yang ditentukan untuk menggunakan kunci.
- `kms:GenerateDataKey`— Memberikan izin bagi Lambda untuk menghasilkan kunci data untuk mengenkripsi kriteria filter, atas nama prinsipal yang ditentukan (enkripsi amplop).

Anda dapat menggunakan AWS CloudTrail untuk melacak AWS KMS permintaan yang dibuat Lambda atas nama Anda. Untuk contoh CloudTrail peristiwa, lihat [????](#).

Kami juga merekomendasikan menggunakan tombol [kms:ViaService](#) kondisi untuk membatasi penggunaan KMS kunci untuk permintaan dari Lambda saja. Nilai kunci ini adalah kepala layanan Lambda regional (`()lambda.AWS_region.amazonaws.com`). Berikut ini adalah contoh kebijakan kunci yang memberikan semua izin yang relevan:

Example AWS KMS kebijakan kunci

```
{
  "Version": "2012-10-17",
  "Id": "example-key-policy-1",
  "Statement": [
    {
      "Sid": "Allow Lambda to decrypt using the key",
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.us-east-1.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals" : {
```

```

        "aws:SourceArn": [
            "arn:aws:lambda:us-east-1:123456789012:event-source-
mapping:<esm_uuid>"
        ]
    },
    "StringEquals": {
        "kms:EncryptionContext:aws:lambda:FunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:test-function",
        "kms:EncryptionContext:aws:lambda:EventSourceArn": "arn:aws:sqs:us-
east-1:123456789012:test-queue"
    }
}
},
{
    "Sid": "Allow actions by an AWS account on the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
    },
    "Action": "kms:*",
    "Resource": "*"
},
{
    "Sid": "Allow use of the key to specific roles",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/ExampleRole"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals" : {
            "kms:ViaService": "lambda.us-east-1.amazonaws.com"
        }
    }
}
]
}

```

Untuk menggunakan KMS kunci Anda sendiri untuk mengenkripsi kriteria filter, Anda juga dapat menggunakan [CreateEventSourceMapping](#) AWS CLI perintah berikut. Tentukan KMS kunci ARN dengan `--kms-key-arn` bendera.

```
aws lambda create-event-source-mapping --function-name my-function \
  --maximum-batching-window-in-seconds 60 \
  --event-source-arn arn:aws:sqs:us-east-1:123456789012:my-queue \
  --filter-criteria "{\"filters\": [{\"pattern\": \"{\\\"a\\\": [\\\"1\\\", \\\"2\\\"]}\" }]}\" \
  --kms-key-arn arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-  
ba9c-538c7d31f599
```

Jika Anda memiliki pemetaan sumber peristiwa yang ada, gunakan [UpdateEventSourceMapping](#) AWS CLI perintah sebagai gantinya. Tentukan KMS kunci ARN dengan `--kms-key-arn` bendera.

```
aws lambda update-event-source-mapping --function-name my-function \
  --maximum-batching-window-in-seconds 60 \
  --event-source-arn arn:aws:sqs:us-east-1:123456789012:my-queue \
  --filter-criteria "{\"filters\": [{\"pattern\": \"{\\\"a\\\": [\\\"1\\\", \\\"2\\\"]}\" }]}\" \
  --kms-key-arn arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-  
ba9c-538c7d31f599
```

Operasi ini menimpa KMS kunci apa pun yang telah ditentukan sebelumnya. Jika Anda menentukan `--kms-key-arn` bendera bersama dengan argumen kosong, Lambda berhenti menggunakan KMS kunci Anda untuk mengenkripsi kriteria filter. Sebaliknya, Lambda default kembali menggunakan kunci milik Amazon.

Untuk menentukan KMS kunci Anda sendiri dalam AWS CloudFormation templat, gunakan `KMSKeyArn` properti jenis `AWS::Lambda::EventSourceMapping` sumber daya. Misalnya, Anda dapat menyisipkan cuplikan berikut ke dalam YAML template untuk sumber acara Anda.

```
MyEventSourceMapping:
  Type: AWS::Lambda::EventSourceMapping
  Properties:
    ...
    FilterCriteria:
      Filters:
        - Pattern: '{"a": [1, 2]}'
      KMSKeyArn: "arn:aws:kms:us-east-1:123456789012:key/055efbb4-xmpl-4336-  
ba9c-538c7d31f599"
    ...
```

Untuk dapat melihat kriteria filter terenkripsi Anda dalam teks biasa dalam [DeleteEventSourceMapping](#) API panggilan [GetEventSourceMapping](#) atau, Anda harus memiliki izin. `kms:Decrypt`

Mulai 6 Agustus 2024, `FilterCriteria` bidang tidak lagi muncul di AWS CloudTrail log dari [CreateEventSourceMapping](#) [UpdateEventSourceMapping](#), dan [DeleteEventSourceMapping](#) API memanggil jika fungsi Anda tidak menggunakan pemfilteran peristiwa. Jika fungsi Anda menggunakan pemfilteran peristiwa, `FilterCriteria` bidang akan muncul sebagai empty (`{}`). Anda masih dapat melihat kriteria filter Anda dalam teks biasa dalam respons [GetEventSourceMapping](#) API panggilan jika Anda memiliki `kms:Decrypt` izin untuk kunci yang benar.

Contoh entri CloudTrail log untuk `DeleteEventSourceMapping` Buat/Perbarui/panggilan

Dalam AWS CloudTrail contoh entri log berikut untuk `CreateEventSourceMapping` panggilan, `FilterCriteria` muncul sebagai empty (`{}`) karena fungsi menggunakan pemfilteran peristiwa. Ini adalah kasus bahkan jika `FilterCriteria` objek berisi kriteria filter yang valid yang fungsi Anda gunakan secara aktif. Jika fungsi tidak menggunakan pemfilteran peristiwa, tidak CloudTrail akan menampilkan `FilterCriteria` bidang sama sekali dalam entri log.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI23456789EXAMPLE:user1",
    "arn": "arn:aws:sts::123456789012:assumed-role/Example/example-role",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI987654321EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/User1",
        "accountId": "123456789012",
        "userName": "User1"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-05-09T20:35:01Z",
        "mfaAuthenticated": "false"
      }
    }
  },
}
```

```
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2024-05-09T21:05:41Z",
  "eventSource": "lambda.amazonaws.com",
  "eventName": "CreateEventSourceMapping20150331",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "eventSourceArn": "arn:aws:sqs:us-east-2:123456789012:example-queue",
    "functionName": "example-function",
    "enabled": true,
    "batchSize": 10,
    "filterCriteria": {},
    "kMSKeyArn": "arn:aws:kms:us-east-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "scalingConfig": {},
    "maximumBatchingWindowInSeconds": 0,
    "sourceAccessConfigurations": []
  },
  "responseElements": {
    "uUID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEaaaaa",
    "batchSize": 10,
    "maximumBatchingWindowInSeconds": 0,
    "eventSourceArn": "arn:aws:sqs:us-east-2:123456789012:example-queue",
    "filterCriteria": {},
    "kMSKeyArn": "arn:aws:kms:us-east-2:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:example-
function",
    "lastModified": "May 9, 2024, 9:05:41 PM",
    "state": "Creating",
    "stateTransitionReason": "USER_INITIATED",
    "functionResponseTypes": [],
    "eventSourceMappingArn": "arn:aws:lambda:us-east-2:123456789012:event-source-
mapping:a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbbb"
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
```

```
"sessionCredentialFromConsole": "true"
}
```

Menggunakan filter dengan berbeda AWS layanan

Berbagai jenis sumber acara menggunakan nilai kunci yang berbeda untuk bidang datanya. Untuk memfilter properti data, pastikan Anda menggunakan kunci yang benar dalam pola filter Anda. Tabel berikut memberikan kunci penyaringan untuk setiap didukung AWS layanan.

| AWS layanan | Kunci penyaringan |
|------------------------------------|-------------------|
| DynamoDB | dynamodb |
| Kinesis | data |
| Amazon MQ | data |
| Amazon MSK | value |
| Apache Kafka yang dikelola sendiri | value |
| Amazon SQS | body |

Bagian berikut memberikan contoh pola filter untuk berbagai jenis sumber peristiwa. Mereka juga memberikan definisi format data masuk yang didukung dan format bodi pola filter untuk setiap layanan yang didukung.

- [the section called “Penyaringan acara”](#)
- [the section called “Penyaringan acara”](#)
- [the section called “Penyaringan acara”](#)
- [the section called “Penyaringan acara”](#)
- [the section called “Penyaringan acara”](#)
- [the section called “Penyaringan acara”](#)

Menguji fungsi Lambda di konsol

Anda dapat menguji fungsi Lambda di konsol dengan menjalankan fungsi Anda dengan peristiwa pengujian. Peristiwa pengujian adalah input JSON ke fungsi Anda. Jika fungsi Anda tidak memerlukan input, acara dapat berupa dokumen kosong ({}).

Saat Anda menjalankan pengujian di konsol, Lambda secara sinkron memanggil fungsi Anda dengan peristiwa pengujian. Fungsi runtime mengubah acara JSON menjadi objek dan meneruskannya ke metode handler kode Anda untuk diproses.

Buat acara pengujian

Sebelum Anda dapat menguji di konsol, Anda perlu membuat acara pengujian pribadi atau dapat dibagikan.

Memanggil fungsi dengan acara pengujian

Untuk menguji suatu fungsi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda uji.
3. Pilih tab Uji.
4. Di bawah Acara uji, pilih Buat acara baru atau Edit acara tersimpan, lalu pilih acara tersimpan yang ingin Anda gunakan.
5. Opsional - pilih Template untuk acara JSON.
6. Pilih Uji.
7. Untuk meninjau hasil pengujian, di bawah Hasil eksekusi, perluas Detail.

Untuk menjalankan fungsi Anda tanpa menyimpan peristiwa pengujian Anda, pilih Uji sebelum menyimpan. Ini menciptakan peristiwa pengujian yang belum disimpan yang dipertahankan Lambda hanya selama sesi berlangsung.

Anda juga dapat mengakses peristiwa pengujian yang disimpan dan belum disimpan di tab Kode. Dari sana, pilih Uji, lalu pilih acara pengujian Anda.

Membuat acara pengujian pribadi

Acara pengujian pribadi hanya tersedia untuk pembuat acara, dan tidak memerlukan izin tambahan untuk digunakan. Anda dapat membuat dan menyimpan hingga 10 acara pengujian pribadi per fungsi.

Untuk membuat acara pengujian pribadi

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda uji.
3. Pilih tab Uji.
4. Di bawah acara Uji, lakukan hal berikut:
 - a. Pilih Template.
 - b. Masukkan Nama untuk tes.
 - c. Di kotak entri teks, masukkan acara uji JSON.
 - d. Di bawah Pengaturan berbagi acara, pilih Pribadi.
5. Pilih Simpan perubahan.

Anda juga dapat membuat acara pengujian baru di tab Kode. Dari sana, pilih Test, Configure test event.

Membuat acara uji yang dapat dibagikan

Peristiwa pengujian yang dapat dibagikan adalah peristiwa pengujian yang dapat Anda bagikan dengan pengguna lain di AWS akun yang sama. Anda dapat mengedit peristiwa pengujian yang dapat dibagikan pengguna lain dan menjalankan fungsi Anda dengannya.

Lambda menyimpan peristiwa pengujian yang dapat dibagikan sebagai skema dalam registri skema [Amazon EventBridge \(CloudWatch Acara\) bernama](#) `lambda-testevent-schemas`. Karena Lambda menggunakan registri ini untuk menyimpan dan memanggil acara pengujian yang dapat dibagikan yang Anda buat, kami menyarankan Anda untuk tidak mengedit registri ini atau membuat registri menggunakan nama tersebut. `lambda-testevent-schemas`

Untuk melihat, membagikan, dan mengedit peristiwa pengujian yang dapat dibagikan, Anda harus memiliki izin untuk semua operasi API [registri skema EventBridge \(CloudWatch Acara\)](#) berikut:

- [schemas.CreateRegistry](#)

- [schemas.CreateSchema](#)
- [schemas.DeleteSchema](#)
- [schemas.DeleteSchemaVersion](#)
- [schemas.DescribeRegistry](#)
- [schemas.DescribeSchema](#)
- [schemas.GetDiscoveredSchema](#)
- [schemas.ListSchemaVersions](#)
- [schemas.UpdateSchema](#)

Perhatikan bahwa menyimpan pengeditan yang dilakukan pada peristiwa pengujian yang dapat dibagikan menimpa peristiwa itu.

Jika Anda tidak dapat membuat, mengedit, atau melihat peristiwa pengujian yang dapat dibagikan, periksa apakah akun Anda memiliki izin yang diperlukan untuk operasi ini. Jika Anda memiliki izin yang diperlukan tetapi masih tidak dapat mengakses peristiwa pengujian yang dapat dibagikan, periksa [kebijakan berbasis sumber daya](#) yang mungkin membatasi akses ke registri (Peristiwa).

EventBridge CloudWatch

Untuk membuat acara pengujian yang dapat dibagikan

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda uji.
3. Pilih tab Uji.
4. Di bawah acara Uji, lakukan hal berikut:
 - a. Pilih Template.
 - b. Masukkan Nama untuk tes.
 - c. Di kotak entri teks, masukkan acara uji JSON.
 - d. Di bawah Pengaturan berbagi acara, pilih Dapat dibagikan.
5. Pilih Simpan perubahan.

i Gunakan acara pengujian yang dapat dibagikan dengan AWS Serverless Application Model. Anda dapat menggunakan AWS SAM untuk memanggil acara pengujian yang dapat dibagikan. Lihat [sam remote test-event](#) di [Panduan AWS Serverless Application Model Pengembang](#)

Menghapus skema acara uji yang dapat dibagikan

Saat Anda menghapus peristiwa pengujian yang dapat dibagikan, Lambda menghapusnya dari `lambda-testevent-schemas` registri. Jika Anda menghapus peristiwa pengujian terakhir yang dapat dibagikan dari registri, Lambda menghapus registri.

Jika Anda menghapus fungsi, Lambda tidak menghapus skema peristiwa pengujian yang dapat dibagikan terkait. Anda harus membersihkan sumber daya ini secara manual dari [konsol EventBridge \(CloudWatch Acara\)](#).

Status fungsi Lambda

Lambda menyertakan bidang status dalam konfigurasi fungsi untuk semua fungsi untuk menunjukkan kapan fungsi Anda siap untuk dipanggil. `Status` memberikan informasi tentang status fungsi saat ini, termasuk apakah Anda berhasil menjalankan fungsi tersebut. Status fungsi tidak mengubah perilaku pemanggilan fungsi atau bagaimana fungsi Anda menjalankan kode. Status fungsi meliputi:

- **Pending**— Setelah Lambda membuat fungsi, ia menetapkan status ke pending. Saat dalam status tertunda, Lambda mencoba membuat atau mengonfigurasi sumber daya untuk fungsi tersebut, seperti sumber daya VPC atau EFS. Lambda tidak memanggil fungsi selama status tertunda. Setiap pemanggilan atau tindakan API lainnya yang beroperasi pada fungsi akan gagal.
- **Active**— Fungsi Anda bertransisi ke status aktif setelah Lambda menyelesaikan konfigurasi dan penyediaan sumber daya. Fungsi hanya dapat berhasil dipanggil saat aktif.
- **Failed**— Menunjukkan bahwa konfigurasi atau penyediaan sumber daya mengalami kesalahan.
- **Inactive**— Sebuah fungsi menjadi tidak aktif ketika sudah mengganggu cukup lama bagi Lambda untuk merebut kembali sumber daya eksternal yang dikonfigurasi untuknya. Saat Anda mencoba memanggil fungsi yang tidak aktif, pemanggilan gagal dan Lambda menyetel fungsi ke status tertunda hingga sumber daya fungsi dibuat ulang. Jika Lambda gagal membuat ulang sumber daya, fungsi kembali ke status tidak aktif. Jika fungsi Anda macet dalam keadaan tidak aktif, lihat fungsi `StatusCode` dan `StatusCodeReason` atribut untuk pemecahan masalah lebih lanjut. Anda mungkin perlu menyelesaikan kesalahan apa pun dan menerapkan kembali fungsi Anda untuk mengembalikannya ke status aktif.

Jika Anda menggunakan alur kerja otomatisasi berbasis SDK atau memanggil API layanan Lambda secara langsung, pastikan Anda memeriksa status fungsi sebelum pemanggilan untuk memverifikasi bahwa fungsi tersebut aktif. Anda dapat melakukan ini dengan tindakan Lambda API [GetFunction](#), atau dengan mengonfigurasi pelayan menggunakan SDK for [AWS Java](#) 2.0.

```
aws lambda get-function --function-name my-function --query 'Configuration.[State, LastUpdateStatus]'
```

Anda akan melihat output berikut:

```
[  
  "Active",  
  "Successful"
```

]

Operasi berikut gagal saat pembuatan fungsi tertunda:

- [Memohon](#)
- [UpdateFunctionCode](#)
- [UpdateFunctionConfiguration](#)
- [PublishVersion](#)

Status fungsi saat memperbarui

Lambda menyediakan konteks tambahan untuk fungsi yang menjalani pembaruan dengan `LastUpdateStatus` atribut, yang dapat memiliki status berikut:

- `InProgress`— Pembaruan sedang terjadi pada fungsi yang ada. Saat pembaruan fungsi sedang berlangsung, pemanggilan masuk ke kode dan konfigurasi fungsi sebelumnya.
- `Successful`— Pembaruan telah selesai. Setelah Lambda menyelesaikan pembaruan, ini tetap disetel hingga pembaruan lebih lanjut.
- `Failed`— Pembaruan fungsi telah gagal. Lambda membatalkan pembaruan dan kode serta konfigurasi fungsi sebelumnya tetap tersedia.

Example

Berikut ini adalah hasil dari `get-function-configuration` fungsi yang menjalani pembaruan.

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
  "Runtime": "nodejs20.x",
  "VpcConfig": {
    "SubnetIds": [
      "subnet-071f712345678e7c8",
      "subnet-07fd123456788a036",
      "subnet-0804f77612345cacf"
    ],
    "SecurityGroupIds": [
      "sg-085912345678492fb"
    ]
  },
}
```

```
    "VpcId": "vpc-08e1234569e011e83"  
  },  
  "State": "Active",  
  "LastUpdateStatus": "InProgress",  
  ...  
}
```

[FunctionConfiguration](#) memiliki dua atribut lain, `LastUpdateStatusReason` dan `LastUpdateStatusReasonCode`, untuk membantu memecahkan masalah dengan memperbarui.

Operasi berikut gagal saat pembaruan asinkron sedang berlangsung:

- [UpdateFunctionCode](#)
- [UpdateFunctionConfiguration](#)
- [PublishVersion](#)
- [TagResource](#)

Memahami perilaku coba lagi di Lambda

Ketika Anda memanggil fungsi secara langsung, Anda menentukan strategi untuk menangani kesalahan yang terkait dengan kode fungsi Anda. Lambda tidak secara otomatis mencoba lagi jenis kesalahan ini atas nama Anda. Untuk mencoba lagi, Anda dapat memanggil ulang fungsi secara manual, mengirim peristiwa yang gagal ke antrian untuk debugging, atau mengabaikan kesalahan. Kode fungsi Anda mungkin telah berjalan sepenuhnya, sebagian, atau tidak sama sekali. Jika Anda mencoba lagi, pastikan bahwa kode fungsi Anda dapat menangani kejadian yang sama beberapa kali tanpa menyebabkan transaksi duplikat atau efek samping yang tidak diinginkan lainnya.

Saat Anda mengaktifkan suatu fungsi secara tidak langsung, Anda perlu menyadari perilaku dari invoker dan layanan apa pun yang dihadapi permintaan selama pelaksanaannya. Ini termasuk skenario berikut.

- **Invokasi asinkron** – Lambda mencoba kembali kesalahan fungsi dua kali. Jika fungsi tidak memiliki kapasitas yang cukup untuk menangani semua permintaan yang masuk, peristiwa mungkin menunggu dalam antrian selama berjam-jam untuk dikirim ke fungsi. Anda dapat mengonfigurasi antrian dead-letter di fungsi untuk menangkap peristiwa yang tidak berhasil diproses. Untuk informasi selengkapnya, lihat [Memanggil fungsi Lambda secara asinkron](#).
- **Pemetaan sumber peristiwa** – Pemetaan sumber peristiwa yang membaca dari aliran mencoba kembali seluruh batch item. Kesalahan berulang memblokir pemrosesan shard berdampak hingga kesalahan diselesaikan atau item kedaluwarsa. Untuk mendeteksi shard yang terhambat, Anda dapat memantau metrik [Usia Iterator](#).

Untuk pemetaan sumber peristiwa yang membaca dari antrian, Anda menentukan lama waktu antara percobaan ulang dan destinasi untuk peristiwa yang gagal dengan mengonfigurasi waktu habis tampilan dan kebijakan redrive pada antrian sumber. Untuk informasi selengkapnya, lihat [Bagaimana Lambda memproses catatan dari sumber acara berbasis streaming dan antrian](#) dan topik khusus layanan di bawah [Memanggil Lambda dengan acara dari layanan lain AWS](#).

- **AWS layanan** — AWS layanan dapat memanggil fungsi Anda secara sinkron atau [asinkron](#). Untuk invokasi sinkron, layanan memutuskan apakah akan mencoba kembali. Misalnya, operasi batch Amazon S3 mencoba kembali operasi jika fungsi Lambda mengembalikan kode respons `TemporaryFailure`. Layanan yang meminta proxy dari pengguna atau klien hulu mungkin memiliki strategi coba lagi atau dapat menyampaikan respons kesalahan kembali ke pemohon. Misalnya, API Gateway selalu menyampaikan respons kesalahan kembali ke pemohon.

Untuk pemanggilan asinkron, logika coba lagi sama terlepas dari sumber pemanggilannya.

Secara default, Lambda mencoba ulang pemanggilan asinkron yang gagal hingga dua kali. Untuk informasi selengkapnya, lihat [Bagaimana Lambda menangani kesalahan dan mencoba ulang dengan pemanggilan asinkron](#).

- Akun dan klien lain – Saat Anda memberikan akses ke akun lain, Anda dapat menggunakan [kebijakan berbasis sumber daya](#) untuk membatasi layanan atau sumber daya yang dapat mereka konfigurasi untuk mengaktifkan fungsi Anda. Untuk melindungi fungsi Anda dari kelebihan beban, pertimbangkan untuk meletakkan API lapisan di depan fungsi Anda dengan [Amazon API Gateway](#).

Untuk membantu Anda mengatasi kesalahan dalam aplikasi Lambda, Lambda terintegrasi dengan layanan seperti Amazon dan CloudWatch AWS X-Ray Anda dapat menggunakan kombinasi log, metrik, alarm, dan penelusuran untuk mendeteksi dan mengidentifikasi masalah dengan cepat dalam kode fungsi API, atau sumber daya lain yang mendukung aplikasi Anda. Untuk informasi selengkapnya, lihat [Pemantauan dan pemecahan masalah fungsi Lambda](#).

Gunakan deteksi loop rekursif Lambda untuk mencegah loop tak terbatas

Saat Anda mengonfigurasi fungsi Lambda untuk menampilkan ke layanan atau sumber daya yang sama yang memanggil fungsi, dimungkinkan untuk membuat loop rekursif tak terbatas. Misalnya, fungsi Lambda mungkin menulis pesan ke antrian Amazon Simple Queue Service (AmazonSQS), yang kemudian memanggil fungsi yang sama. Pemanggilan ini menyebabkan fungsi untuk menulis pesan lain ke antrian, yang pada gilirannya memanggil fungsi lagi.

Loop rekursif yang tidak disengaja dapat mengakibatkan biaya tak terduga ditagih ke Anda. Akun AWS Loop juga dapat menyebabkan Lambda [menskalakan](#) dan menggunakan semua konkurensi akun Anda yang tersedia. Untuk membantu mengurangi dampak loop yang tidak disengaja, Lambda mendeteksi jenis loop rekursif tertentu segera setelah terjadi. Secara default, ketika Lambda mendeteksi loop rekursif, Lambda menghentikan fungsi Anda dipanggil dan memberi tahu Anda. Jika desain Anda sengaja menggunakan pola rekursif, Anda dapat mengubah konfigurasi default fungsi untuk memungkinkannya dipanggil secara rekursif. Untuk informasi selengkapnya, lihat [the section called “Mengizinkan fungsi Lambda berjalan dalam loop rekursif”](#).

Bagian-bagian

- [Memahami deteksi loop rekursif](#)
- [Didukung AWS layanan dan SDKs](#)
- [Pemberitahuan loop rekursif](#)
- [Menanggapi notifikasi deteksi loop rekursif](#)
- [Mengizinkan fungsi Lambda berjalan dalam loop rekursif](#)
- [Wilayah yang didukung untuk deteksi loop rekursif Lambda](#)

Memahami deteksi loop rekursif

Deteksi loop rekursif di Lambda bekerja dengan melacak peristiwa. Lambda adalah layanan komputasi berbasis peristiwa yang menjalankan kode fungsi Anda saat peristiwa tertentu terjadi. Misalnya, saat item ditambahkan ke topik SQS antrian Amazon atau Amazon Simple Notification Service (AmazonSNS). Lambda meneruskan peristiwa ke fungsi Anda sebagai JSON objek, yang berisi informasi tentang perubahan status sistem. Ketika suatu peristiwa menyebabkan fungsi Anda berjalan, ini disebut pemanggilan.

Untuk mendeteksi loop rekursif, Lambda [AWS X-Ray](#) menggunakan header penelusuran. Ketika [AWS layanan mendukung deteksi loop rekursif](#) mengirim peristiwa ke Lambda, peristiwa tersebut secara otomatis dianotasi dengan metadata. Saat fungsi Lambda Anda menulis salah satu peristiwa ini ke peristiwa lain yang didukung AWS layanan menggunakan [versi yang didukung AWS SDK](#), fungsi Lambda akan memperbarui metadata ini. Metadata yang diperbarui mencakup hitungan berapa kali acara telah memanggil fungsi.

Note

Anda tidak perlu mengaktifkan penelusuran aktif X-Ray agar fitur ini berfungsi. Deteksi loop rekursif diaktifkan secara default untuk semua AWS pelanggan. Tidak ada biaya untuk menggunakan fitur ini.

Rantai permintaan adalah urutan pemanggilan Lambda yang disebabkan oleh peristiwa pemicu yang sama. Misalnya, bayangkan SQS antrian Amazon memanggil fungsi Lambda Anda. Fungsi Lambda Anda kemudian mengirim peristiwa yang diproses kembali ke SQS antrean Amazon yang sama, yang memanggil fungsi Anda lagi. Dalam contoh ini, setiap pemanggilan fungsi Anda berada dalam rantai permintaan yang sama.

Jika fungsi Anda dipanggil sekitar 16 kali dalam rantai permintaan yang sama, maka Lambda secara otomatis menghentikan pemanggilan fungsi berikutnya dalam rantai permintaan tersebut dan memberi tahu Anda. Jika fungsi Anda dikonfigurasi dengan beberapa pemicu, maka pemanggilan dari pemicu lain tidak terpengaruh.

Note

Meskipun `maxReceiveCount` pengaturan pada kebijakan redrive antrian sumber lebih tinggi dari 16, perlindungan rekursi Lambda tidak SQS mencegah Amazon mencoba ulang pesan setelah loop rekursif terdeteksi dan dihentikan. Ketika Lambda mendeteksi loop rekursif dan menjatuhkan pemanggilan berikutnya, ia mengembalikan a `RecursiveInvocationException` ke pemetaan sumber peristiwa. Ini meningkatkan `receiveCount` nilai pada pesan. Lambda terus mencoba lagi pesan, dan terus memblokir pemanggilan fungsi, hingga SQS Amazon menentukan bahwa terlampaui dan mengirim pesan `maxReceiveCount` ke antrian huruf mati yang dikonfigurasi.

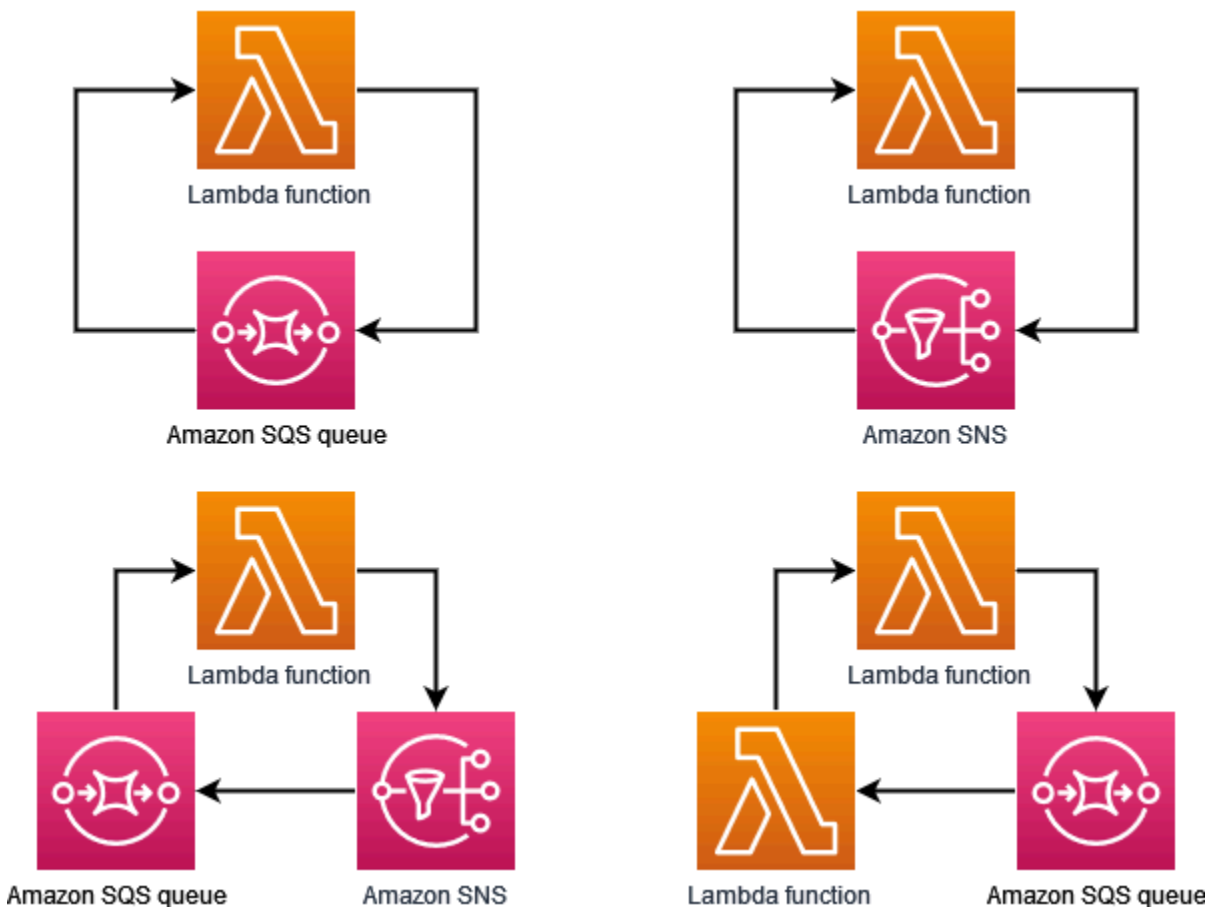
Jika Anda memiliki [tujuan yang gagal](#) atau [antrean huruf mati yang](#) dikonfigurasi untuk fungsi Anda, maka Lambda juga mengirimkan acara dari pemanggilan yang dihentikan ke antrean tujuan atau surat mati Anda. Saat mengonfigurasi antrian tujuan atau huruf mati untuk fungsi Anda, pastikan untuk tidak menggunakan topik Amazon SNS atau SQS antrian Amazon yang juga digunakan fungsi Anda sebagai pemicu peristiwa atau pemetaan sumber peristiwa. Jika Anda mengirim peristiwa ke sumber daya yang sama yang memanggil fungsi Anda, maka Anda dapat membuat loop rekursif lain.

Didukung AWS layanan dan SDKs

Lambda hanya dapat mendeteksi loop rekursif yang menyertakan dukungan tertentu. AWS layanan Agar loop rekursif terdeteksi, fungsi Anda juga harus menggunakan salah satu yang didukung AWS SDKs.

Didukung AWS layanan

Lambda saat ini mendeteksi loop rekursif antara fungsi Anda, Amazon, SQS dan Amazon. SNS Lambda juga mendeteksi loop yang hanya terdiri dari fungsi Lambda, yang dapat memanggil satu sama lain secara sinkron atau asinkron. Diagram berikut menunjukkan beberapa contoh loop yang dapat dideteksi Lambda:



Ketika yang lain AWS layanan seperti Amazon DynamoDB atau Amazon Simple Storage Service (Amazon S3) merupakan bagian dari loop, Lambda saat ini tidak dapat mendeteksi dan menghentikannya.

Karena Lambda saat ini hanya mendeteksi loop rekursif yang melibatkan Amazon dan SQS AmazonSNS, masih mungkin loop yang melibatkan yang lain AWS layanan dapat mengakibatkan penggunaan fungsi Lambda Anda yang tidak diinginkan.

Untuk mencegah tagihan tak terduga yang ditagih ke Anda Akun AWS, kami sarankan Anda mengonfigurasi [CloudWatchalarm Amazon](#) untuk mengingatkan Anda tentang pola penggunaan yang tidak biasa. Misalnya, Anda dapat mengonfigurasi CloudWatch untuk memberi tahu Anda tentang lonjakan dalam konkurensi atau pemanggilan fungsi Lambda. Anda juga dapat mengonfigurasi [alarm penagihan](#) untuk memberi tahu Anda saat pengeluaran di akun melebihi ambang batas yang Anda tentukan. Atau, Anda dapat menggunakannya [AWS Cost Anomaly Detection](#) untuk mengingatkan Anda tentang pola penagihan yang tidak biasa.

Didukung AWS SDKs

Agar Lambda dapat mendeteksi loop rekursif, fungsi Anda harus menggunakan salah satu SDK versi berikut atau yang lebih tinggi:

| Waktu Aktif | AWS SDKVersi minimum yang diperlukan |
|--------------------|--------------------------------------|
| Node.js | 2.1147.0 (versi 2) SDK |
| | 3.105.0 (SDKversi 3) |
| Python | 1.24.46 (Boto3) |
| | 1.27.46 (botocore) |
| Java 8 dan Java 11 | 2.17.135 |
| Jawa 17 | 2.20.81 |
| Jawa 21 | 2.21.24 |
| .NET | 3.7.293.0 |
| Ruby | 3.134.0 |

| | |
|-------------|--------------------------------------|
| Waktu Aktif | AWS SDKVersi minimum yang diperlukan |
| PHP | 3.232.0 |
| Go | SDKV2 (gunakan versi terbaru) |

Beberapa runtime Lambda seperti Python dan Node.js menyertakan versi file. AWS SDK Jika SDK versi yang disertakan dalam runtime fungsi Anda lebih rendah dari minimum yang diperlukan, maka Anda dapat menambahkan versi yang didukung SDK ke paket [penerapan](#) fungsi Anda. Anda juga dapat menambahkan SDK versi yang didukung ke fungsi Anda menggunakan lapisan [Lambda](#). Untuk daftar yang SDKs disertakan dengan setiap runtime Lambda, lihat. [Runtime Lambda](#)

Pemberitahuan loop rekursif

Ketika Lambda menghentikan loop rekursif, Anda menerima pemberitahuan melalui [AWS Health Dashboard](#) dan melalui email. Anda juga dapat menggunakan CloudWatch metrik untuk memantau jumlah pemanggilan rekursif yang dihentikan Lambda.

AWS Health Dashboard pemberitahuan

[Ketika Lambda menghentikan pemanggilan rekursif, akan AWS Health Dashboard menampilkan pemberitahuan di halaman kesehatan akun Anda, di bawah Terbuka dan masalah terbaru.](#)

Perhatikan bahwa ini dapat memakan waktu hingga tiga jam setelah Lambda menghentikan pemanggilan rekursif sebelum pemberitahuan ini ditampilkan. Untuk informasi selengkapnya tentang melihat peristiwa akun di AWS Health Dashboard, lihat [Memulai dengan Dasbor AWS Kesehatan — Kesehatan akun Anda](#) di Panduan Pengguna AWS Kesehatan.

Peringatan email

Saat Lambda pertama kali menghentikan pemanggilan rekursif fungsi Anda, Lambda mengirimkan peringatan email kepada Anda. Lambda mengirim maksimal satu email setiap 24 jam untuk setiap fungsi di Anda. Akun AWS Setelah Lambda mengirimkan pemberitahuan email, Anda tidak akan menerima email lagi untuk fungsi itu selama 24 jam lagi, bahkan jika Lambda menghentikan pemanggilan rekursif lebih lanjut dari fungsi tersebut. Perhatikan bahwa ini dapat memakan waktu hingga tiga jam setelah Lambda menghentikan pemanggilan rekursif sebelum Anda menerima peringatan email ini.

Lambda mengirimkan peringatan email loop rekursif ke kontak akun utama Anda Akun AWS dan kontak operasi alternatif Anda. Untuk informasi tentang melihat atau memperbarui alamat email di akun Anda, lihat [Memperbarui informasi kontak](#) di Referensi AWS Umum.

CloudWatch Metrik Amazon

[CloudWatch Metrik](#) `RecursiveInvocationsDropped` mencatat jumlah pemanggilan fungsi yang dihentikan Lambda karena fungsi Anda telah dipanggil lebih dari 16 kali dalam satu rantai permintaan. Lambda memancarkan metrik ini segera setelah menghentikan pemanggilan rekursif. Untuk melihat metrik ini, ikuti petunjuk untuk [Melihat metrik di CloudWatch konsol](#) dan pilih metrik `RecursiveInvocationsDropped`.

Menanggapi notifikasi deteksi loop rekursif

Ketika fungsi Anda dipanggil lebih dari 16 kali oleh peristiwa pemicu yang sama, Lambda menghentikan pemanggilan fungsi berikutnya untuk acara tersebut untuk memutus loop rekursif. Untuk mencegah terulangnya loop rekursif yang rusak Lambda, lakukan hal berikut:

- Kurangi [konkurensi](#) fungsi Anda yang tersedia menjadi nol, yang membatasi semua pemanggilan future.
- Hapus atau nonaktifkan pemicu atau pemetaan sumber peristiwa yang menjalankan fungsi Anda.
- Identifikasi dan perbaiki cacat kode yang menulis peristiwa kembali ke AWS sumber daya yang menjalankan fungsi Anda. Sebuah sumber umum cacat terjadi ketika Anda menggunakan variabel untuk menentukan sumber peristiwa fungsi dan target. Periksa apakah Anda tidak menggunakan nilai yang sama untuk kedua variabel.

Selain itu, jika sumber peristiwa untuk fungsi Lambda Anda adalah SQS antrian Amazon, pertimbangkan untuk [mengonfigurasi antrian huruf mati pada antrean](#) sumber.

Note

Pastikan Anda mengonfigurasi antrean surat gagal di antrean sumber, bukan di fungsi Lambda. Antrean surat gagal yang dikonfigurasi di fungsi digunakan untuk [antrean invokasi asinkron](#) fungsi, bukan untuk antrean sumber kejadian.

Jika sumber acara adalah SNS topik Amazon, pertimbangkan untuk menambahkan [tujuan yang gagal](#) untuk fungsi Anda.

Untuk mengurangi konkurensi fungsi Anda yang tersedia menjadi nol (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Anda.
3. Pilih Throttle.
4. Di kotak dialog Throttle your function, pilih Confirm.

Untuk menghapus pemicu atau pemetaan sumber peristiwa untuk fungsi Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Anda.
3. Pilih tab Konfigurasi, lalu pilih Pemicu.
4. Di bawah Pemicu, pilih pemicu atau pemetaan sumber peristiwa yang ingin Anda hapus, lalu pilih Hapus.
5. Di kotak dialog Hapus pemicu, pilih Hapus.

Untuk menonaktifkan pemetaan sumber peristiwa untuk fungsi Anda (AWS CLI)

1. Untuk menemukan UUID pemetaan sumber peristiwa yang ingin Anda nonaktifkan, jalankan [list-event-source-mappings](#) perintah AWS Command Line Interface (AWS CLI).

```
aws lambda list-event-source-mappings
```

2. Untuk menonaktifkan pemetaan sumber peristiwa, jalankan AWS CLI [update-event-source-mapping](#) perintah berikut.

```
aws lambda update-event-source-mapping --function-name MyFunction \  
--uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --no-enabled
```

Mengizinkan fungsi Lambda berjalan dalam loop rekursif

Jika desain Anda sengaja menggunakan loop rekursif, Anda dapat mengonfigurasi fungsi Lambda untuk memungkinkannya dipanggil secara rekursif. Kami menyarankan Anda menghindari penggunaan loop rekursif dalam desain Anda. Kesalahan implementasi dapat menyebabkan pemanggilan rekursif menggunakan semua konkurensi Anda Akun AWS yang tersedia dan biaya tak terduga yang ditagih ke akun Anda.

⚠ Important

Jika Anda menggunakan loop rekursif, perlakukan dengan hati-hati. Menerapkan best practice guard rail untuk meminimalkan risiko kesalahan implementasi. Untuk mempelajari lebih lanjut tentang praktik terbaik untuk menggunakan pola rekursif, lihat Pola [rekursif yang menyebabkan fungsi Lambda yang tidak terkendali](#) di Tanah Tanpa Server.

Anda dapat mengonfigurasi fungsi untuk memungkinkan loop rekursif menggunakan konsol Lambda, AWS Command Line Interface AWS CLI(), dan [PutFunctionRecursionConfig](#) API. Anda juga dapat mengonfigurasi pengaturan deteksi loop rekursif fungsi di AWS SAM dan AWS CloudFormation.

Secara default, Lambda mendeteksi dan mengakhiri loop rekursif. Kecuali desain Anda sengaja menggunakan loop rekursif, kami menyarankan Anda untuk tidak mengubah konfigurasi default fungsi Anda.

Perhatikan bahwa saat Anda mengonfigurasi fungsi untuk mengizinkan loop rekursif, [CloudWatch metrik](#) `RecursiveInvocationsDropped` tidak dipancarkan.

Console

Untuk memungkinkan fungsi berjalan dalam loop rekursif (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Anda untuk membuka halaman detail fungsi.
3. Pilih tab Konfigurasi, lalu pilih Konkurensi dan deteksi rekursi.
4. Selain deteksi loop rekursif, pilih Edit.
5. Pilih Izinkan loop rekursif.
6. Pilih Simpan.

AWS CLI

Anda dapat menggunakan [PutFunctionRecursionConfig](#) API untuk memungkinkan fungsi Anda dipanggil dalam loop rekursif. Tentukan `Allow` untuk parameter loop rekursif. Misalnya, Anda dapat memanggil ini API dengan `put-function-recursion-config` AWS CLI perintah:

```
aws lambda put-function-recursion-config --function-name yourFunctionName --  
recursive-loop Allow
```


Anda dapat mengubah konfigurasi fungsi Anda kembali ke pengaturan default sehingga Lambda menghentikan loop rekursif saat mendeteksi mereka. Edit konfigurasi fungsi Anda menggunakan konsol Lambda atau. AWS CLI

Console

Untuk mengkonfigurasi fungsi sehingga loop rekursif dihentikan (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Anda untuk membuka halaman detail fungsi.
3. Pilih tab Konfigurasi, lalu pilih Konkurensi dan deteksi rekursi.
4. Selain deteksi loop rekursif, pilih Edit.
5. Pilih Hentikan loop rekursif.
6. Pilih Simpan.

AWS CLI

Anda dapat menggunakan [PutFunctionRecursionConfig](#) API untuk mengonfigurasi fungsi Anda sehingga Lambda mengakhiri loop rekursif saat mendeteksi mereka. Tentukan `Terminate` untuk parameter loop rekursif. Misalnya, Anda dapat memanggil ini API dengan `put-function-recursion-config` AWS CLI perintah:

```
aws lambda put-function-recursion-config --function-name yourFunctionName --recursive-loop Terminate
```

Wilayah yang didukung untuk deteksi loop rekursif Lambda

Deteksi loop rekursif Lambda didukung sebagai berikut. Wilayah AWS

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)

- Asia Pasifik (Mumbai)
- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Milan)
- Eropa (Paris)
- Eropa (Stockholm)
- Timur Tengah (Bahrain)
- Amerika Selatan (Sao Paulo)

Membuat dan mengelola fungsi Lambda URLs

Fungsi URL adalah titik akhir khusus HTTP (S) untuk fungsi Lambda Anda. Anda dapat membuat dan mengonfigurasi fungsi URL melalui konsol Lambda atau Lambda. API Saat Anda membuat fungsiURL, Lambda secara otomatis menghasilkan URL titik akhir yang unik untuk Anda. Setelah Anda membuat fungsiURL, URL titik akhirnya tidak pernah berubah. URLTitik akhir fungsi memiliki format berikut:

```
https://<url-id>.lambda-url.<region>.on.aws
```

Note

Fungsi tidak URLs didukung sebagai berikut Wilayah AWS: Asia Pasifik (Hyderabad) (), Asia Pasifik (Melbourneap-south-2) (), Asia Pasifik (Malaysiaap-southeast-4) (), Kanada Barat (Calgaryap-southeast-5) (), Eropa (Spanyolca-west-1) (), Eropa (Zuricheu-south-2) (), Israel (Tel Aviveu-central-2) (), dan Timur Tengah (il-central-1) (). UAE me-central-1

Fungsi URLs adalah dual stack-enabled, mendukung dan. IPv4 IPv6 Setelah Anda mengkonfigurasi fungsi URL untuk fungsi Anda, Anda dapat memanggil fungsi Anda melalui titik akhir HTTP (S) melalui browser web, curl, Postman, atau klien apa pun. HTTP

Note

Anda dapat mengakses fungsi Anda hanya URL melalui Internet publik. Sementara fungsi Lambda mendukung AWS PrivateLink, fungsi URLs tidak.

Fungsi Lambda URLs menggunakan [kebijakan berbasis sumber daya](#) untuk keamanan dan kontrol akses. Fungsi URLs juga mendukung opsi konfigurasi berbagi sumber daya lintas asal (CORS).

Anda dapat menerapkan fungsi URLs ke alias fungsi apa pun, atau ke versi fungsi yang \$LATEST tidak dipublikasikan. Anda tidak dapat menambahkan fungsi URL ke versi fungsi lainnya.

Bagian berikut menunjukkan cara membuat dan mengelola fungsi URL menggunakan konsol Lambda, AWS CLI, dan template AWS CloudFormation

Topik

- [Membuat fungsi URL \(konsol\)](#)
- [Membuat fungsi URL \(AWS CLI\)](#)
- [Menambahkan fungsi URL ke CloudFormation template](#)
- [Berbagi sumber daya lintas asal \(\) CORS](#)
- [Fungsi pelambatan URLs](#)
- [Menonaktifkan fungsi URLs](#)
- [Menghapus fungsi URLs](#)
- [Kontrol akses ke URL fungsi Lambda](#)
- [Memanggil fungsi Lambda URLs](#)
- [Memantau URL fungsi Lambda](#)
- [Tutorial: Membuat fungsi Lambda dengan URL fungsi](#)

Membuat fungsi URL (konsol)

Ikuti langkah-langkah ini untuk membuat fungsi URL menggunakan konsol.

Untuk membuat fungsi URL untuk fungsi yang ada (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda URL buat fungsinya.
3. Pilih tab Configuration, lalu pilih Function URL.
4. Pilih Buat fungsiURL.
5. Untuk jenis Auth, pilih AWS_ IAM atau NONE. Untuk informasi selengkapnya tentang URL otentikasi fungsi, lihat [Kontrol akses](#).
6. (Opsional) Pilih Konfigurasi berbagi sumber daya lintas asal (CORS), lalu konfigurasi CORS pengaturan untuk fungsi URL Anda. Untuk informasi lebih lanjut tentang CORS, lihat [Berbagi sumber daya lintas asal \(\) CORS](#).
7. Pilih Simpan.

Ini menciptakan fungsi URL untuk versi fungsi Anda \$LATEST yang tidak dipublikasikan. Fungsi ini URL muncul di bagian Ikhtisar fungsi konsol.

Untuk membuat fungsi URL untuk alias yang ada (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi dengan alias yang ingin Anda URL buat fungsinya.
3. Pilih tab Alias, lalu pilih nama alias yang ingin Anda buat fungsinyaURL.
4. Pilih tab Configuration, lalu pilih Function URL.
5. Pilih Buat fungsiURL.
6. Untuk jenis Auth, pilih AWS_ IAM atau NONE. Untuk informasi selengkapnya tentang URL otentikasi fungsi, lihat[Kontrol akses](#).
7. (Opsional) Pilih Konfigurasi berbagi sumber daya lintas asal (CORS), lalu konfigurasi CORS pengaturan untuk fungsi URL Anda. Untuk informasi lebih lanjut tentangCORS, lihat[Berbagi sumber daya lintas asal \(\) CORS](#).
8. Pilih Simpan.

Ini menciptakan fungsi URL untuk alias fungsi Anda. Fungsi URL muncul di bagian ikhtisar Fungsi konsol untuk alias Anda.

Untuk membuat fungsi baru dengan fungsi URL (konsol)

Untuk membuat fungsi baru dengan fungsi URL (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih Buat fungsi.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda, seperti**my-function**.
 - b. Untuk Runtime, pilih runtime bahasa yang Anda inginkan, seperti Node.js 18.x.
 - c. Untuk Arsitektur, pilih x86_64 atau arm64.
 - d. Perluas Izin, lalu pilih apakah akan membuat peran eksekusi baru atau menggunakan yang sudah ada.
4. Perluas Pengaturan lanjutan, lalu pilih Fungsi URL.
5. Untuk jenis Auth, pilih AWS_ IAM atau NONE. Untuk informasi selengkapnya tentang URL otentikasi fungsi, lihat[Kontrol akses](#).
6. (Opsional) Pilih Konfigurasi berbagi sumber daya lintas asal (CORS). Dengan memilih opsi ini selama pembuatan fungsi, fungsi Anda URL mengizinkan permintaan dari semua asal secara

default. Anda dapat mengedit CORS pengaturan untuk fungsi Anda URL setelah membuat fungsi. Untuk informasi lebih lanjut tentang CORS, lihat [Berbagi sumber daya lintas asal \(\) CORS](#).

7. Pilih Buat fungsi.

Ini menciptakan fungsi baru dengan fungsi URL untuk versi fungsi yang \$LATEST tidak dipublikasikan. Fungsi ini URL muncul di bagian Ikhtisar fungsi konsol.

Membuat fungsi URL (AWS CLI)

Untuk membuat fungsi URL untuk fungsi Lambda yang ada menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut:

```
aws lambda create-function-url-config \  
  --function-name my-function \  
  --qualifier prod \ // optional  
  --auth-type AWS_IAM  
  --cors-config {AllowOrigins="https://example.com"} // optional
```

Ini menambahkan fungsi URL ke **prod** qualifier untuk fungsi **my-function** tersebut. Untuk informasi selengkapnya tentang parameter konfigurasi ini, lihat [CreateFunctionUrlConfig](#) di API referensi.

Note

Untuk membuat fungsi URL melalui AWS CLI, fungsi tersebut harus sudah ada.

Menambahkan fungsi URL ke CloudFormation template

Untuk menambahkan `AWS::Lambda::Url` sumber daya ke AWS CloudFormation template Anda, gunakan sintaks berikut:

JSON

```
{  
  "Type" : "AWS::Lambda::Url",  
  "Properties" : {  
    "AuthType" : String,  
    "Cors" : Cors,  
    "Qualifier" : String,
```

```

    "TargetFunctionArn" : String
  }
}

```

YAML

```

Type: AWS::Lambda::Url
Properties:
  AuthType: String
  Cors:
    Cors
  Qualifier: String
  TargetFunctionArn: String

```

Parameter

- (Wajib) `AuthType` — Mendefinisikan jenis otentikasi untuk fungsi Anda. URL Nilai yang mungkin adalah salah satu `AWS_IAM` atau `NONE`. Untuk membatasi akses ke pengguna yang diautentikasi saja, setel ke `AWS_IAM` Untuk mem-bypass IAM otentikasi dan memungkinkan setiap pengguna untuk membuat permintaan ke fungsi Anda, atur ke `NONE`
- (Opsional) `Cors` - Mendefinisikan [CORSpengaturan](#) untuk fungsi URL Anda. `Cors` Untuk menambah `AWS::Lambda::Url` sumber daya Anda CloudFormation, gunakan sintaks berikut.

Example `AWS::Lambda::Url.Cors ()` JSON

```

{
  "AllowCredentials" : Boolean,
  "AllowHeaders" : [ String, ... ],
  "AllowMethods" : [ String, ... ],
  "AllowOrigins" : [ String, ... ],
  "ExposeHeaders" : [ String, ... ],
  "MaxAge" : Integer
}

```

Example `AWS::Lambda::Url.Cors ()` YAML

```

AllowCredentials: Boolean
AllowHeaders:
  - String
AllowMethods:

```

```

- String
AllowOrigins:
- String
ExposeHeaders:
- String
MaxAge: Integer

```

- (Opsional) **Qualifier** — Nama alias.
- (Wajib) **TargetFunctionArn** - Nama atau Nama Sumber Daya Amazon (ARN) dari fungsi Lambda. Format nama yang valid meliputi yang berikut:
 - Nama fungsi - my-function
 - Fungsi ARN - arn:aws:lambda:us-west-2:123456789012:function:my-function
 - Sebagian ARN — 123456789012:function:my-function

Berbagi sumber daya lintas asal () CORS

Untuk menentukan cara asal yang berbeda dapat mengakses fungsi Anda URL, gunakan [berbagi sumber daya lintas asal \(CORS\)](#). Sebaiknya konfigurasi CORS jika Anda bermaksud memanggil fungsi Anda URL dari domain yang berbeda. Lambda mendukung CORS header berikut untuk fungsi. URLs

| CORSsundulan | CORSproperti konfigurasi | Contoh nilai |
|--|--------------------------|--|
| Access-Control-Allow-Origin | AllowOrigins | *(izinkan semua asal) https://www.example.com http://localhost:60905 |
| Access-Control-Allow-Methods | AllowMethods | GET, POST, DELETE, * |
| Access-Control-Allow-Header | AllowHeaders | Date, Keep-Alive , X-Custom-Header |
| Access-Control-Expose-Header | ExposeHeaders | Date, Keep-Alive , X-Custom-Header |

| CORSsundulan | CORSproperti konfigurasi | Contoh nilai |
|--|--------------------------|------------------|
| Access-Control-Allow-Credentials | AllowCredentials | TRUE |
| Akses-Kontrol-Max-Age | MaxAge | 5 (default), 300 |

Saat Anda mengonfigurasi CORS fungsi URL menggunakan konsol Lambda atau, AWS CLI Lambda secara otomatis menambahkan CORS header ke semua respons melalui fungsi tersebut. URL Atau, Anda dapat menambahkan CORS header secara manual ke respons fungsi Anda. Jika ada header yang bertentangan, perilaku yang diharapkan tergantung pada jenis permintaan:

- Untuk permintaan preflight seperti OPTIONS permintaan, CORS header yang dikonfigurasi pada fungsi URL diutamakan. Lambda hanya mengembalikan CORS header ini dalam respons.
- Untuk permintaan non-preflight seperti GET atau POST permintaan, Lambda mengembalikan CORS header yang dikonfigurasi pada fungsiURL, serta header yang dikembalikan oleh CORS fungsi. Hal ini dapat mengakibatkan duplikat CORS header dalam respon. Anda mungkin melihat kesalahan yang mirip dengan berikut ini: `The 'Access-Control-Allow-Origin' header contains multiple values '*', *', but only one is allowed.`

Secara umum, kami sarankan untuk mengonfigurasi semua CORS pengaturan pada fungsiURL, daripada mengirim CORS header secara manual dalam respons fungsi.

Fungsi pelambatan URLs

Throttling membatasi tingkat permintaan proses fungsi Anda. Ini berguna dalam banyak situasi, seperti mencegah fungsi Anda membebani sumber daya hilir secara berlebihan, atau menangani lonjakan permintaan yang tiba-tiba.

Anda dapat membatasi laju permintaan yang diproses fungsi Lambda Anda melalui fungsi URL dengan mengonfigurasi konkurensi cadangan. Konkurensi cadangan membatasi jumlah pemanggilan bersamaan maksimum untuk fungsi Anda. Tingkat permintaan maksimum fungsi Anda per detik (RPS) setara dengan 10 kali konkurensi cadangan yang dikonfigurasi. Misalnya, jika Anda mengonfigurasi fungsi Anda dengan konkurensi cadangan 100, maka maksimumnya RPS adalah 1.000.

Setiap kali konkurensi fungsi Anda melebihi konkurensi cadangan, fungsi Anda URL mengembalikan kode HTTP 429 status. Jika fungsi Anda menerima permintaan yang melebihi RPS maksimum 10x berdasarkan konkurensi cadangan yang dikonfigurasi, Anda juga menerima kesalahan HTTP429. Untuk informasi selengkapnya tentang konkurensi cadangan, lihat [Mengkonfigurasi konkurensi cadangan untuk suatu fungsi](#).

Menonaktifkan fungsi URLs

Dalam keadaan darurat, Anda mungkin ingin menolak semua lalu lintas ke fungsi URL Anda. Untuk menonaktifkan fungsi AndaURL, atur konkurensi cadangan ke nol. Ini membatasi semua permintaan ke fungsi AndaURL, menghasilkan respons HTTP 429 status. Untuk mengaktifkan kembali fungsi AndaURL, hapus konfigurasi konkurensi cadangan, atau atur konfigurasi ke jumlah yang lebih besar dari nol.

Menghapus fungsi URLs

Saat Anda menghapus suatu fungsiURL, Anda tidak dapat memulihkannya. Membuat fungsi baru URL akan menghasilkan URL alamat yang berbeda.

Note

Jika Anda menghapus fungsi URL dengan jenis autentikasiNONE, Lambda tidak secara otomatis menghapus kebijakan berbasis sumber daya terkait. Jika Anda ingin menghapus kebijakan ini, Anda harus melakukannya secara manual.

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi.
3. Pilih tab Configuration, lalu pilih Function URL.
4. Pilih Hapus.
5. Masukkan kata hapus ke dalam bidang untuk mengonfirmasi penghapusan.
6. Pilih Hapus.

Note

Saat Anda menghapus fungsi yang memiliki fungsiURL, Lambda secara asinkron menghapus fungsi tersebut. URL Jika Anda segera membuat fungsi baru dengan nama yang sama di

akun yang sama, ada kemungkinan fungsi asli URL akan dipetakan ke fungsi baru alih-alih dihapus.

Kontrol akses ke URL fungsi Lambda

Anda dapat mengontrol akses ke URL fungsi Lambda menggunakan AuthType parameter yang dikombinasikan dengan kebijakan [berbasis sumber daya yang dilampirkan ke fungsi spesifik](#) Anda. Konfigurasi kedua komponen ini menentukan siapa yang dapat memanggil atau melakukan tindakan administratif lainnya pada URL fungsi Anda.

AuthTypeParameter menentukan cara Lambda mengautentikasi atau mengotorisasi permintaan ke URL fungsi Anda. Saat Anda mengonfigurasi URL fungsi Anda, Anda harus menentukan salah satu AuthType opsi berikut:

- **AWS_IAM**— Lambda menggunakan AWS Identity and Access Management (IAM) untuk mengautentikasi dan mengotorisasi permintaan berdasarkan kebijakan identitas kepala sekolah IAM dan kebijakan berbasis sumber daya fungsi. Pilih opsi ini jika Anda hanya ingin pengguna dan peran yang diautentikasi untuk memanggil fungsi Anda melalui URL fungsi.
- **NONE**— Lambda tidak melakukan otentikasi apa pun sebelum menjalankan fungsi Anda. Namun, kebijakan berbasis sumber daya fungsi Anda selalu berlaku dan harus memberikan akses publik sebelum URL fungsi Anda dapat menerima permintaan. Pilih opsi ini untuk mengizinkan akses publik yang tidak diautentikasi ke URL fungsi Anda.

Selain ituAuthType, Anda juga dapat menggunakan kebijakan berbasis sumber daya untuk memberikan izin kepada orang lain Akun AWS untuk menjalankan fungsi Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan kebijakan berbasis sumber daya di Lambda IAM](#).

Untuk wawasan tambahan tentang keamanan, Anda dapat menggunakan AWS Identity and Access Management Access Analyzer untuk mendapatkan analisis komprehensif tentang akses eksternal ke URL fungsi Anda. IAM Access Analyzer juga memantau izin baru atau yang diperbarui pada fungsi Lambda Anda untuk membantu Anda mengidentifikasi izin yang memberikan akses publik dan lintas akun. IAM Access Analyzer gratis digunakan untuk pelanggan mana pun AWS . Untuk memulai dengan IAM Access Analyzer, lihat [Menggunakan AWS IAM Access Analyzer](#).

Halaman ini berisi contoh kebijakan berbasis sumber daya untuk kedua jenis autentikasi, dan juga cara membuat kebijakan ini menggunakan [AddPermission](#) operasi API atau konsol Lambda. Untuk

informasi tentang cara memanggil URL fungsi setelah menyiapkan izin, lihat. [Memanggil fungsi Lambda URLs](#)

Topik

- [Menggunakan tipe AWS_IAM autentikasi](#)
- [Menggunakan tipe NONE autentikasi](#)
- [Tata kelola dan kontrol akses](#)

Menggunakan tipe **AWS_IAM** autentikasi

Jika Anda memilih jenis `AWS_IAM` autentikasi, pengguna yang perlu memanggil URL fungsi Lambda Anda harus memiliki izin. `lambda:InvokeFunctionUrl` Bergantung pada siapa yang membuat permintaan pemanggilan, Anda mungkin harus memberikan izin ini menggunakan kebijakan berbasis sumber daya.

Jika prinsipal yang membuat permintaan Akun AWS sama dengan URL fungsi, maka prinsipal harus memiliki **`lambda:InvokeFunctionUrl`** izin dalam kebijakan [berbasis identitas mereka](#), [atau memiliki izin yang diberikan kepada mereka dalam kebijakan berbasis sumber daya fungsi](#). Dengan kata lain, kebijakan berbasis sumber daya bersifat opsional jika pengguna sudah memiliki `lambda:InvokeFunctionUrl` izin dalam kebijakan berbasis identitas mereka. Evaluasi kebijakan mengikuti aturan yang diuraikan dalam [Menentukan apakah permintaan diizinkan atau ditolak dalam akun](#).

Jika prinsipal yang membuat permintaan berada di akun yang berbeda, maka prinsipal harus memiliki kebijakan berbasis identitas yang memberi mereka **`lambda:InvokeFunctionUrl`** izin dan izin yang diberikan kepada mereka dalam kebijakan berbasis sumber daya pada fungsi yang mereka coba panggil. Dalam kasus lintas akun ini, evaluasi kebijakan mengikuti aturan yang diuraikan dalam [Menentukan apakah permintaan lintas akun diperbolehkan](#).

Sebagai contoh interaksi lintas akun, kebijakan berbasis sumber daya berikut memungkinkan example peran Akun AWS 444455556666 untuk memanggil URL fungsi yang terkait dengan fungsi: `my-function`

Example fungsi URL kebijakan pemanggilan lintas akun

```
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": {  
      "AWS": "arn:aws:iam::444455556666:role/example"  
    },  
    "Action": "lambda:InvokeFunctionUrl",  
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",  
    "Condition": {  
      "StringEquals": {  
        "lambda:FunctionUrlAuthType": "AWS_IAM"  
      }  
    }  
  }  
]
```

Anda dapat membuat pernyataan kebijakan ini melalui konsol dengan mengikuti langkah-langkah berikut:

Untuk memberikan izin pemanggilan URL ke akun lain (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda berikan izin pemanggilan URL.
3. Pilih tab Konfigurasi, lalu pilih Izin.
4. Di bawah Kebijakan berbasis sumber daya, pilih Tambahkan izin.
5. Pilih URL Fungsi.
6. Untuk jenis Auth, pilih AWS_IAM.
7. (Opsional) Untuk ID Pernyataan, masukkan ID pernyataan untuk pernyataan kebijakan Anda.
8. Untuk Principal, masukkan ID akun atau Nama Sumber Daya Amazon (ARN) pengguna atau peran yang ingin Anda berikan izin. Misalnya: **444455556666**.
9. Pilih Simpan.

Atau, Anda dapat membuat pernyataan kebijakan ini menggunakan perintah [add-permission](#) AWS Command Line Interface (AWS CLI) berikut:

```
aws lambda add-permission --function-name my-function \  
  --statement-id example0-cross-account-statement \  
  --
```

```
--action lambda:InvokeFunctionUrl \  
--principal 444455556666 \  
--function-url-auth-type AWS_IAM
```

Pada contoh sebelumnya, nilai kunci `lambda:FunctionUrlAuthType` kondisi adalah `AWS_IAM`. Kebijakan ini hanya mengizinkan akses jika jenis autentikasi URL fungsi Anda juga `AWS_IAM`.

Menggunakan tipe **NONE** autentikasi

Important

Ketika jenis autentikasi URL fungsi Anda `NONE` dan Anda memiliki kebijakan berbasis sumber daya yang memberikan akses publik, setiap pengguna yang tidak diautentikasi dengan URL fungsi Anda dapat memanggil fungsi Anda.

Dalam beberapa kasus, Anda mungkin ingin URL fungsi Anda menjadi publik. Misalnya, Anda mungkin ingin menyajikan permintaan yang dibuat langsung dari browser web. Untuk mengizinkan akses publik ke URL fungsi Anda, pilih jenis `NONE` autentikasi.

Jika Anda memilih jenis `NONE` autentikasi, Lambda tidak menggunakan IAM untuk mengautentikasi permintaan ke URL fungsi Anda. Namun, pengguna masih harus memiliki `lambda:InvokeFunctionUrl` izin agar berhasil memanggil URL fungsi Anda. Anda dapat memberikan `lambda:InvokeFunctionUrl` izin menggunakan kebijakan berbasis sumber daya berikut:

Example kebijakan pemanggilan URL fungsi untuk semua prinsip yang tidak diautentikasi

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "lambda:InvokeFunctionUrl",  
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",  
      "Condition": {  
        "StringEquals": {  
          "lambda:FunctionUrlAuthType": "NONE"  
        }  
      }  
    }  
  ]  
}
```

```
    }  
  }  
]  
}
```

Note

Saat Anda membuat URL fungsi dengan jenis autentikasi NONE melalui konsol atau AWS Serverless Application Model (AWS SAM), Lambda secara otomatis membuat pernyataan kebijakan berbasis sumber daya sebelumnya untuk Anda. Jika kebijakan sudah ada, atau pengguna atau peran yang membuat aplikasi tidak memiliki izin yang sesuai, Lambda tidak akan membuatnya untuk Anda. Jika Anda menggunakan AWS CLI, AWS CloudFormation, atau Lambda API secara langsung, Anda harus menambahkan `lambda:InvokeFunctionUrl` izin sendiri. Ini membuat fungsi Anda publik. Selain itu, jika Anda menghapus URL fungsi dengan jenis autentikasi NONE, Lambda tidak secara otomatis menghapus kebijakan berbasis sumber daya terkait. Jika Anda ingin menghapus kebijakan ini, Anda harus melakukannya secara manual.

Dalam pernyataan ini, nilai kunci `lambda:FunctionUrlAuthType` kondisi adalah `NONE`. Pernyataan kebijakan ini mengizinkan akses hanya jika jenis autentikasi URL fungsi Anda juga `NONE`.

Jika kebijakan berbasis sumber daya fungsi tidak memberikan `lambda:invokeFunctionUrl` izin, pengguna akan mendapatkan kode kesalahan 403 Forbidden saat mereka mencoba memanggil URL fungsi Anda, meskipun URL fungsi menggunakan jenis autentikasi. `NONE`

Tata kelola dan kontrol akses

Selain izin pemanggilan URL fungsi, Anda juga dapat mengontrol akses pada tindakan yang digunakan untuk mengonfigurasi URL fungsi. Lambda mendukung tindakan kebijakan IAM berikut untuk URL fungsi:

- `lambda:InvokeFunctionUrl`— Memanggil fungsi Lambda menggunakan URL fungsi.
- `lambda:CreateFunctionUrlConfig`— Buat URL fungsi dan atur `AuthType`.
- `lambda:UpdateFunctionUrlConfig`— Perbarui konfigurasi URL fungsi dan `AuthType`.
- `lambda:GetFunctionUrlConfig`— Lihat detail URL fungsi.
- `lambda:ListFunctionUrlConfigs`— Daftar konfigurasi URL fungsi.

- `lambda:DeleteFunctionUrlConfig`— Hapus URL fungsi.

Note

Konsol Lambda mendukung penambahan izin hanya untuk `lambda:InvokeFunctionUrl`. Untuk semua tindakan lainnya, Anda harus menambahkan izin menggunakan Lambda API atau AWS CLI.

Untuk mengizinkan atau menolak akses URL fungsi ke AWS entitas lain, sertakan tindakan ini dalam kebijakan IAM. Misalnya, kebijakan berikut memberikan `example` peran dalam Akun AWS 444455556666 izin untuk memperbarui URL fungsi untuk fungsi **my-function** di akun. 123456789012

Example kebijakan URL fungsi lintas akun

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/example"
      },
      "Action": "lambda:UpdateFunctionUrlConfig",
      "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function"
    }
  ]
}
```

Kunci syarat

Untuk kontrol akses berbutir halus atas URL fungsi Anda, gunakan kunci kondisi. Lambda mendukung satu tombol kondisi tambahan untuk URL fungsi: `FunctionUrlAuthType`. `FunctionUrlAuthTypeKunci` mendefinisikan nilai enum yang menjelaskan jenis autentikasi yang digunakan URL fungsi Anda. Nilai dapat berupa `AWS_IAM` atau `NONE`, salah satu.

Anda dapat menggunakan kunci kondisi ini dalam kebijakan yang terkait dengan fungsi Anda. Misalnya, Anda mungkin ingin membatasi siapa yang dapat membuat perubahan konfigurasi pada

URL fungsi Anda. Untuk menolak semua UpdateFunctionUrlConfig permintaan ke fungsi apa pun dengan jenis autentikasi URLNONE, Anda dapat menentukan kebijakan berikut:

Example kebijakan URL fungsi dengan penolakan eksplisit

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "lambda:UpdateFunctionUrlConfig"
      ],
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
      "Condition": {
        "StringEquals": {
          "lambda:FunctionUrlAuthType": "NONE"
        }
      }
    }
  ]
}
```

Untuk memberikan example peran dalam Akun AWS 444455556666 izin untuk membuat CreateFunctionUrlConfig dan UpdateFunctionUrlConfig permintaan pada fungsi dengan jenis autentikasi URLAWS_IAM, Anda dapat menentukan kebijakan berikut:

Example kebijakan URL fungsi dengan izin eksplisit

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/example"
      },
      "Action": [
        "lambda:CreateFunctionUrlConfig",
        "lambda:UpdateFunctionUrlConfig"
      ],
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
    }
  ]
}
```

```
        "Condition": {
            "StringEquals": {
                "lambda:FunctionUrlAuthType": "AWS_IAM"
            }
        }
    ]
}
```

Anda juga dapat menggunakan kunci kondisi ini dalam [kebijakan kontrol layanan](#) (SCP). Gunakan SCP untuk mengelola izin di seluruh organisasi di AWS Organizations Misalnya, untuk menolak pengguna membuat atau memperbarui URL fungsi yang menggunakan apa pun selain jenis AWS_IAM autentikasi, gunakan kebijakan kontrol layanan berikut:

Example fungsi URL SCP dengan penolakan eksplisit

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "lambda:CreateFunctionUrlConfig",
        "lambda:UpdateFunctionUrlConfig"
      ],
      "Resource": "arn:aws:lambda:*:123456789012:function:*",
      "Condition": {
        "StringNotEquals": {
          "lambda:FunctionUrlAuthType": "AWS_IAM"
        }
      }
    }
  ]
}
```

Memanggil fungsi Lambda URLs

Fungsi URL adalah titik akhir khusus HTTP (S) untuk fungsi Lambda Anda. Anda dapat membuat dan mengonfigurasi fungsi URL melalui konsol Lambda atau Lambda. API Saat Anda membuat fungsiURL, Lambda secara otomatis menghasilkan URL titik akhir yang unik untuk Anda. Setelah Anda membuat fungsiURL, URL titik akhirnya tidak pernah berubah. URL titik akhir fungsi memiliki format berikut:

```
https://<url-id>.lambda-url.<region>.on.aws
```

Note

Fungsi tidak URLs didukung sebagai berikut Wilayah AWS: Asia Pasifik (Hyderabad) (), Asia Pasifik (Melbourneap-south-2) (), Asia Pasifik (Malaysiaap-southeast-4) (), Kanada Barat (Calgaryap-southeast-5) (), Eropa (Spanyolca-west-1) (), Eropa (Zuricheu-south-2) (), Israel (Tel Aviveu-central-2) (), dan Timur Tengah (il-central-1) (). UAE me-central-1

Fungsi URLs adalah dual stack-enabled, mendukung dan. IPv4 IPv6 Setelah mengonfigurasi fungsi AndaURL, Anda dapat memanggil fungsi Anda melalui titik akhir HTTP (S) melalui browser web, curl, Postman, atau klien apa pun. HTTP Untuk menjalankan fungsiURL, Anda harus memiliki `lambda:InvokeFunctionUrl` izin. Untuk informasi selengkapnya, lihat [Kontrol akses](#).

Topik

- [Dasar-dasar URL pemanggilan fungsi](#)
- [Muatan permintaan dan respons](#)

Dasar-dasar URL pemanggilan fungsi

Jika fungsi Anda URL menggunakan jenis `AWS_IAM` autentikasi, Anda harus menandatangani setiap HTTP permintaan menggunakan [AWS Signature Version 4 \(SigV4\)](#). Alat seperti [awscurl](#), [Postman](#), dan [AWS SiGv4 Proxy menawarkan cara bawaan untuk menandatangani permintaan Anda dengan SiGv4](#).

Jika Anda tidak menggunakan alat untuk menandatangani HTTP permintaan ke fungsi AndaURL, Anda harus menandatangani setiap permintaan secara manual menggunakan SigV4. Saat

fungsi Anda URL menerima permintaan, Lambda juga menghitung tanda tangan SigV4.

Lambda memproses permintaan hanya jika tanda tangan cocok. Untuk petunjuk tentang cara menandatangani permintaan Anda secara manual dengan SigV4, lihat [Menandatangani AWS permintaan dengan Tanda Tangan Versi 4](#) di Referensi Umum Amazon Web Services Panduan.

Jika fungsi Anda URL menggunakan jenis NONE autentikasi, Anda tidak perlu menandatangani permintaan menggunakan SigV4. Anda dapat menjalankan fungsi Anda menggunakan browser web, curl, Postman, atau klien apa pun. HTTP

Untuk menguji GET permintaan sederhana ke fungsi Anda, gunakan browser web. Misalnya, jika fungsi URL Anda `https://abcdefg.lambda-url.us-east-1.on.aws`, dan dibutuhkan dalam parameter `stringmessage`, permintaan Anda URL bisa terlihat seperti ini:

```
https://abcdefg.lambda-url.us-east-1.on.aws/?message>HelloWorld
```

Untuk menguji HTTP permintaan lain, seperti POST permintaan, Anda dapat menggunakan alat seperti curl. Misalnya, jika Anda ingin menyertakan beberapa JSON data dalam POST permintaan ke fungsi Anda URL, Anda dapat menggunakan perintah curl berikut:

```
curl -v 'https://abcdefg.lambda-url.us-east-1.on.aws/?message>HelloWorld' \  
-H 'content-type: application/json' \  
-d '{ "example": "test" }'
```

Muatan permintaan dan respons

Saat klien memanggil fungsi Anda URL, Lambda memetakan permintaan ke objek peristiwa sebelum meneruskannya ke fungsi Anda. Respons fungsi Anda kemudian dipetakan ke HTTP respons yang dikirim Lambda kembali ke klien melalui fungsi tersebut. URL

Format peristiwa permintaan dan respons mengikuti skema yang sama dengan format [payload Amazon API Gateway versi 2.0](#).

Minta format muatan

Muatan permintaan memiliki struktur sebagai berikut:

```
{  
  "version": "2.0",  
  "routeKey": "$default",  
  "rawPath": "/my/path",  
  "rawQueryString": "parameter1=value1&parameter1=value2&parameter2=value",
```

```
"cookies": [
  "cookie1",
  "cookie2"
],
"headers": {
  "header1": "value1",
  "header2": "value1,value2"
},
"queryStringParameters": {
  "parameter1": "value1,value2",
  "parameter2": "value"
},
"requestContext": {
  "accountId": "123456789012",
  "apiId": "<urlid>",
  "authentication": null,
  "authorizer": {
    "iam": {
      "accessKey": "AKIA...",
      "accountId": "111122223333",
      "callerId": "AIDA...",
      "cognitoIdentity": null,
      "principalOrgId": null,
      "userArn": "arn:aws:iam::111122223333:user/example-user",
      "userId": "AIDA..."
    }
  },
  "domainName": "<url-id>.lambda-url.us-west-2.on.aws",
  "domainPrefix": "<url-id>",
  "http": {
    "method": "POST",
    "path": "/my/path",
    "protocol": "HTTP/1.1",
    "sourceIp": "123.123.123.123",
    "userAgent": "agent"
  },
  "requestId": "id",
  "routeKey": "$default",
  "stage": "$default",
  "time": "12/Mar/2020:19:03:58 +0000",
  "timeEpoch": 1583348638390
},
"body": "Hello from client!",
"pathParameters": null,
```

```

"isBase64Encoded": false,
"stageVariables": null
}

```

| Parameter | Deskripsi | Contoh |
|----------------|--|--|
| version | Versi format payload untuk acara ini. Fungsi Lambda URLs saat ini mendukung format payload versi 2.0 . | 2.0 |
| routeKey | Fungsi URLs tidak menggunakan parameter ini. Lambda menetapkan ini \$default sebagai placeholder. | \$default |
| rawPath | Jalur permintaan. Misalnya, jika URL permintaannya <code>https://{url-id}.lambda-url.{region}.on.aws/example/test/demo</code> , maka nilai jalur mentah adalah <code>/example/test/demo</code> . | /example/test/demo |
| rawQueryString | String mentah yang berisi parameter string query permintaan. Karakter yang didukung termasuk <code>a-zA-Z,0-9,.,_,-,%,&=, dan+</code> . | "?parameter1=value1¶meter2=value2" |
| cookies | Array yang berisi semua cookie yang dikirim sebagai bagian dari permintaan. | ["Cookie_1=Value_1", "Cookie_2=Value_2"] |
| headers | Daftar header permintaan, disajikan sebagai pasangan kunci-nilai. | {"header1": "value1", "header2": "value2"} |

| Parameter | Deskripsi | Contoh |
|--|--|-------------------------------|
| <code>queryStringParameters</code> | Parameter kueri untuk permintaan. Misalnya, jika URL permintaannya <code>https://{url-id}.lambda-url.{region}.on.aws/example?name=Jane</code> , maka <code>queryStringParameters</code> nilainya adalah JSON objek dengan kunci dari <code>name</code> dan nilai <code>Jane</code> . | <code>{"name": "Jane"}</code> |
| <code>requestContext</code> | Objek yang berisi informasi tambahan tentang permintaan, seperti <code>requestId</code> , waktu permintaan, dan identitas penelepon jika diotorisasi melalui AWS Identity and Access Management (IAM). | |
| <code>requestContext.accountId</code> | Akun AWS ID pemilik fungsi. | <code>"123456789012"</code> |
| <code>requestContext.apiId</code> | ID fungsi URL. | <code>"33anwqw8fj"</code> |
| <code>requestContext.authentication</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda mengatur ini ke <code>null</code> . | <code>null</code> |
| <code>requestContext.authorizer</code> | Objek yang berisi informasi tentang identitas pemanggil, jika fungsi URL menggunakan jenis <code>AWS_IAM auth</code> . Jika tidak, Lambda menyetel ini ke <code>null</code> . | |

| Parameter | Deskripsi | Contoh |
|--|---|---|
| <code>requestContext.authorizer.iam.accessKey</code> | Kunci akses identitas penelepon. | "AKIAIOSFODNN7EXAMPLE" |
| <code>requestContext.authorizer.iam.accountId</code> | Akun AWS ID identitas penelepon. | "111122223333" |
| <code>requestContext.authorizer.iam.callerId</code> | ID (ID pengguna) pemanggil. | "AIDACKCEVSQ6C2EXAMPLE" |
| <code>requestContext.authorizer.iam.cognitoIdentity</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda menyetel ini ke <code>null</code> atau mengecualikan ini dari. JSON | <code>null</code> |
| <code>requestContext.authorizer.iam.principalOrgId</code> | ID organisasi utama yang terkait dengan identitas penelepon. | "AIDACKCEVSQORGEXAMPLE" |
| <code>requestContext.authorizer.iam.userArn</code> | Nama Sumber Daya Amazon pengguna (ARN) dari identitas pemanggil. | "arn:aws:iam::111122223333:user/example-user" |
| <code>requestContext.authorizer.iam.userId</code> | ID pengguna dari identitas pemanggil. | "AIDACOSFODNN7EXAMPLE2" |
| <code>requestContext.domainName</code> | Nama domain dari fungsi tersebutURL. | "<url-id>.lambda-url.us-west-2.on.aws" |
| <code>requestContext.domainPrefix</code> | Awalan domain dari fungsi URL tersebut. | "<url-id>" |
| <code>requestContext.http</code> | Objek yang berisi rincian tentang HTTP permintaan. | |

| Parameter | Deskripsi | Contoh |
|--|--|---|
| <code>requestContext.http.method</code> | HTTPMetode yang digunakan dalam permintaan ini. Nilai yang valid termasuk GET, POST, PUT, HEAD, OPTIONS, PATCH, dan DELETE. | GET |
| <code>requestContext.http.path</code> | Jalur permintaan. Misalnya, jika URL permintaannya <code>https://{url-id}.lambda-url.{region}.on.aws/example/test/demo</code> , maka nilai jalurnya adalah <code>/example/test/demo</code> . | <code>/example/test/demo</code> |
| <code>requestContext.http.protocol</code> | Protokol permintaan. | HTTP/1.1 |
| <code>requestContext.http.sourceIp</code> | Alamat IP sumber dari TCP koneksi langsung membuat permintaan. | 123.123.123.123 |
| <code>requestContext.http.userAgent</code> | Nilai header permintaan User-Agent. | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Gecko/20100101 Firefox/42.0 |
| <code>requestContext.requestId</code> | ID permintaan pemanggilan. Anda dapat menggunakan ID ini untuk melacak log pemanggilan yang terkait dengan fungsi Anda. | e1506fd5-9e7b-434f-bd42-4f8fa224b599 |

| Parameter | Deskripsi | Contoh |
|---------------------------------------|---|---|
| <code>requestContext.routeKey</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda menetapkan ini <code>\$default</code> sebagai placeholder. | <code>\$default</code> |
| <code>requestContext.stage</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda menetapkan ini <code>\$default</code> sebagai placeholder. | <code>\$default</code> |
| <code>requestContext.time</code> | Stempel waktu permintaan. | <code>"07/Sep/2021:22:50:22 +0000"</code> |
| <code>requestContext.timeEpoch</code> | Stempel waktu permintaan, dalam waktu zaman Unix. | <code>"1631055022677"</code> |
| <code>body</code> | Tubuh permintaan. Jika jenis konten permintaan adalah biner, isi dikodekan base64. | <code>{"key1": "value1", "key2": "value2"}</code> |
| <code>pathParameters</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda menyetel ini ke <code>null</code> atau mengecualikan ini dari. JSON | <code>null</code> |
| <code>isBase64Encoded</code> | TRUE jika bodinya adalah muatan biner dan dikodekan base64. FALSE jika tidak. | <code>FALSE</code> |
| <code>stageVariables</code> | Fungsi URLs tidak menggunakan parameter ini. Lambda menyetel ini ke <code>null</code> atau mengecualikan ini dari. JSON | <code>null</code> |

Format payload respon

Saat fungsi Anda mengembalikan respons, Lambda mem-parsing respons dan mengubahnya menjadi respons. HTTP Muatan respons fungsi memiliki format berikut:

```
{
  "statusCode": 201,
  "headers": {
    "Content-Type": "application/json",
    "My-Custom-Header": "Custom Value"
  },
  "body": "{ \"message\": \"Hello, world!\" }",
  "cookies": [
    "Cookie_1=Value1; Expires=21 Oct 2021 07:48 GMT",
    "Cookie_2=Value2; Max-Age=78000"
  ],
  "isBase64Encoded": false
}
```

Lambda menyimpulkan format respons untuk Anda. Jika fungsi Anda mengembalikan valid JSON dan tidak mengembalikan `statusCode`, Lambda mengasumsikan hal berikut:

- `statusCode` adalah `200`.
- `content-type` adalah `application/json`.
- `body` adalah respon fungsi.
- `isBase64Encoded` adalah `false`.

Contoh berikut menunjukkan bagaimana output fungsi Lambda Anda memetakan ke payload respons, dan bagaimana payload respons memetakan respons ke respons akhir. HTTP Ketika klien memanggil fungsi Anda URL, mereka melihat HTTP responsnya.

Contoh output untuk respon string

| Keluaran fungsi Lambda | Output respons yang ditafsirkan | HTTPrespon (apa yang dilihat klien) |
|------------------------|---------------------------------|--|
| "Hello, world!" | { "statusCode": 200, | HTTP/2 200 date: Wed, 08 Sep 2021 18:02:24 GMT |

| Keluaran fungsi Lambda | Output respons yang ditafsirkan | HTTPrespon (apa yang dilihat klien) |
|------------------------|---|--|
| | <pre> "body": "Hello, world!", "headers": { "content-type": "application/json" }, "isBase64Encoded": false } </pre> | <pre> content-type: applicati on/json content-length: 15 "Hello, world!" </pre> |

Contoh keluaran untuk JSON respons

| Keluaran fungsi Lambda | Output respons yang ditafsirkan | HTTPrespon (apa yang dilihat klien) |
|---|---|--|
| <pre> { "message": "Hello, world!" } </pre> | <pre> { "statusCode": 200, "body": { "message": "Hello, world!" }, "headers": { "content-type": "application/json" }, "isBase64Encoded": false } </pre> | <pre> HTTP/2 200 date: Wed, 08 Sep 2021 18:02:24 GMT content-type: applicati on/json content-length: 34 { "message": "Hello, world!" } </pre> |

Contoh keluaran untuk respons kustom

| Keluaran fungsi Lambda | Output respons yang ditafsirkan | HTTPrespon (apa yang dilihat klien) |
|------------------------|---------------------------------|-------------------------------------|
| <pre> { </pre> | <pre> { </pre> | <pre> HTTP/2 201 </pre> |

| Keluaran fungsi Lambda | Output respons yang ditafsirkan | HTTPrespon (apa yang dilihat klien) |
|---|---|--|
| <pre> "statusCode": 201, "headers": { "Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false } </pre> | <pre> "statusCode": 201, "headers": { "Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false } </pre> | <pre> date: Wed, 08 Sep 2021 18:02:24 GMT content-type: applicati on/json content-length: 27 my-custom-header: Custom Value { "message": "Hello, world!" } </pre> |

Cookie

Untuk mengembalikan cookie dari fungsi Anda, jangan menambahkan set-cookie header secara manual. Sebagai gantinya, sertakan cookie di objek payload respons Anda. Lambda secara otomatis menafsirkan ini dan menambahkannya sebagai set-cookie header dalam HTTP respons Anda, seperti pada contoh berikut.

| Keluaran fungsi Lambda | HTTPrespon (apa yang dilihat klien) |
|--|---|
| <pre> { "statusCode": 201, "headers": { "Content-Type": "application/ json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "cookies": [</pre> | <pre> HTTP/2 201 date: Wed, 08 Sep 2021 18:02:24 GMT content-type: application/json content-length: 27 my-custom-header: Custom Value set-cookie: Cookie_1=Value2; Expires=21 Oct 2021 07:48 GMT set-cookie: Cookie_2=Value2; Max- Age=78000 { "message": "Hello, world!" } </pre> |

Keluaran fungsi Lambda

```
    "Cookie_1=Value1; Expires=21
    Oct 2021 07:48 GMT",
    "Cookie_2=Value2; Max-Age=7
    8000"
  ],
  "isBase64Encoded": false
}
```

HTTPrespon (apa yang dilihat klien)

```
}
```

Memantau URL fungsi Lambda

Anda dapat menggunakan AWS CloudTrail dan Amazon CloudWatch untuk memantau URL fungsi Anda.

Topik

- [Memantau URL fungsi dengan CloudTrail](#)
- [CloudWatch metrik untuk URL fungsi](#)

Memantau URL fungsi dengan CloudTrail

Untuk URL fungsi, Lambda secara otomatis mendukung pencatatan operasi API berikut sebagai peristiwa CloudTrail dalam file log:

- [CreateFunctionUrlConfig](#)
- [UpdateFunctionUrlConfig](#)
- [DeleteFunctionUrlConfig](#)
- [GetFunctionUrlConfig](#)
- [ListFunctionUrlConfigs](#)

Setiap entri log berisi informasi tentang identitas penelepon, kapan permintaan dibuat, dan detail lainnya. Anda dapat melihat semua acara dalam 90 hari terakhir dengan melihat riwayat CloudTrail Acara Anda. Untuk menyimpan catatan 90 hari terakhir, Anda dapat membuat jejak.

Secara default, CloudTrail tidak mencatat `InvokeFunctionUrl` permintaan, yang dianggap peristiwa data. Namun, Anda dapat mengaktifkan login peristiwa data CloudTrail. Untuk informasi lebih lanjut, lihat [Peristiwa Pencatatan Data untuk Pelacakan](#) dalam AWS CloudTrail Panduan Pengguna.

CloudWatch metrik untuk URL fungsi

Lambda mengirimkan metrik agregat tentang permintaan URL fungsi ke CloudWatch. Dengan metrik ini, Anda dapat memantau URL fungsi, membuat dasbor, dan mengonfigurasi alarm di konsol. CloudWatch

URL fungsi mendukung metrik pemanggilan berikut. Kami merekomendasikan untuk melihat metrik ini dengan Sum statistik.

- `UrlRequestCount`— Jumlah permintaan yang dibuat untuk URL fungsi ini.
- `Url4xxCount`— Jumlah permintaan yang mengembalikan kode status HTTP 4XX. Kode seri 4XX menunjukkan kesalahan sisi klien, seperti permintaan buruk.
- `Url5xxCount`— Jumlah permintaan yang mengembalikan kode status HTTP 5XX. Kode seri 5XX menunjukkan kesalahan sisi server, seperti kesalahan fungsi dan batas waktu.

URL fungsi juga mendukung metrik kinerja berikut. Kami merekomendasikan untuk melihat metrik ini dengan Average atau Max statistik.

- `UrlRequestLatency`— Waktu antara ketika URL fungsi menerima permintaan dan ketika URL fungsi mengembalikan respons.

Masing-masing metrik pemanggilan dan kinerja ini mendukung dimensi berikut:

- `FunctionName`— Lihat metrik agregat untuk URL fungsi yang ditetapkan ke versi fungsi yang `$LATEST` tidak dipublikasikan, atau ke alias fungsi mana pun. Misalnya, `hello-world-function`.
- `Resource`— Lihat metrik untuk URL fungsi tertentu. Ini didefinisikan oleh nama fungsi, bersama dengan versi fungsi yang `$LATEST` tidak dipublikasikan atau salah satu alias fungsi. Misalnya, `hello-world-function:$LATEST`.
- `ExecutedVersion`— Lihat metrik untuk URL fungsi tertentu berdasarkan versi yang dieksekusi. Anda dapat menggunakan dimensi ini terutama untuk melacak URL fungsi yang ditetapkan ke versi yang `$LATEST` tidak dipublikasikan.

Tutorial: Membuat fungsi Lambda dengan URL fungsi

Dalam tutorial ini, Anda membuat fungsi Lambda didefinisikan sebagai arsip file.zip dengan titik akhir URL fungsi publik yang mengembalikan produk dari dua angka. Untuk informasi selengkapnya tentang mengonfigurasi URL fungsi, lihat [Fungsi URLs](#)

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```

Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (\) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh perintah CLI dalam panduan ini menggunakan pemformatan Linux. Perintah yang menyertakan dokumen JSON sebaris harus diformat ulang jika Anda menggunakan CLI Windows.

Membuat peran eksekusi

Buat [peran eksekusi](#) yang memberikan izin kepada fungsi Lambda Anda untuk mengakses sumber daya AWS .

Untuk membuat peran eksekusi

1. Buka [halaman Peran](#) konsol AWS Identity and Access Management (IAM).
2. Pilih Buat peran.
3. Untuk jenis entitas Tepercaya pilih AWS layanan, lalu untuk kasus Penggunaan, pilih Lambda.
4. Pilih Berikutnya.
5. Di panel Kebijakan izin, masukkan **AWSLambdaBasicExecutionRole** di kotak pencarian.
6. Pilih kotak centang di sebelah kebijakan AWSLambdaBasicExecutionRole AWS terkelola, lalu pilih Berikutnya.
7. Masukkan nama **lambda-url-role** Peran, lalu pilih Buat peran.

AWSLambdaBasicExecutionRoleKebijakan ini memiliki izin yang diperlukan fungsi untuk menulis log ke Amazon CloudWatch Logs. Kemudian dalam tutorial, Anda akan memerlukan Amazon Resource Name (ARN) peran untuk membuat fungsi Lambda Anda.

Untuk menemukan ARN peran eksekusi Anda

1. Buka [halaman Peran](#) konsol AWS Identity and Access Management (IAM).
2. Pilih peran yang baru saja Anda buat (lambda-url-role).
3. Di panel Ringkasan, salin ARN.

Buat fungsi Lambda dengan URL fungsi (arsip file.zip)

Buat fungsi Lambda dengan titik akhir URL fungsi menggunakan arsip file.zip.

Untuk membuat fungsi

1. Salin contoh kode berikut ke file bernama `index.js`.

Example index.js

```
exports.handler = async (event) => {
  let body = JSON.parse(event.body);
  const product = body.num1 * body.num2;
  const response = {
    statusCode: 200,
    body: "The product of " + body.num1 + " and " + body.num2 + " is " +
product,
```

```
};  
return response;  
};
```

2. Buat paket deployment.

```
zip function.zip index.js
```

3. Buat fungsi Lambda dengan perintah `create-function`. Pastikan untuk mengganti peran ARN dengan ARN dari peran eksekusi Anda sendiri yang Anda salin sebelumnya dalam tutorial.

```
aws lambda create-function \  
  --function-name my-url-function \  
  --runtime nodejs18.x \  
  --zip-file fileb://function.zip \  
  --handler index.handler \  
  --role arn:aws:iam::123456789012:role/lambda-url-role
```

4. Tambahkan kebijakan berbasis sumber daya ke fungsi Anda yang memberikan izin untuk mengizinkan akses publik ke URL fungsi Anda.

```
aws lambda add-permission \  
  --function-name my-url-function \  
  --action lambda:InvokeFunctionUrl \  
  --principal "*" \  
  --function-url-auth-type "NONE" \  
  --statement-id url
```

5. Buat titik akhir URL untuk fungsi dengan `create-function-url-config` perintah.

```
aws lambda create-function-url-config \  
  --function-name my-url-function \  
  --auth-type NONE
```

Uji titik akhir URL fungsi

Panggil fungsi Lambda Anda dengan memanggil titik akhir URL fungsi Anda menggunakan klien HTTP seperti curl atau Postman.

```
curl 'https://abcdefg.lambda-url.us-east-1.on.aws/' \  
-H 'Content-Type: application/json' \  

```

```
-d '{"num1": "10", "num2": "10"}'
```

Anda akan melihat output berikut:

```
The product of 10 and 10 is 100
```

Buat fungsi Lambda dengan URL fungsi () CloudFormation

Anda juga dapat membuat fungsi Lambda dengan titik akhir URL fungsi menggunakan tipe. AWS CloudFormation `AWS::Lambda::Url`

```
Resources:
  MyUrlFunction:
    Type: AWS::Lambda::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs18.x
      Role: arn:aws:iam::123456789012:role/lambda-url-role
      Code:
        ZipFile: |
          exports.handler = async (event) => {
            let body = JSON.parse(event.body);
            const product = body.num1 * body.num2;
            const response = {
              statusCode: 200,
              body: "The product of " + body.num1 + " and " + body.num2 + " is " +
product,
            };
            return response;
          };
      Description: Create a function with a URL.
  MyUrlFunctionPermissions:
    Type: AWS::Lambda::Permission
    Properties:
      FunctionName: !Ref MyUrlFunction
      Action: lambda:InvokeFunctionUrl
      Principal: "*"
      FunctionUrlAuthType: NONE
  MyFunctionUrl:
    Type: AWS::Lambda::Url
    Properties:
      TargetFunctionArn: !Ref MyUrlFunction
```

```
AuthType: NONE
```

Buat fungsi Lambda dengan URL fungsi ()AWS SAM

Anda juga dapat membuat fungsi Lambda yang dikonfigurasi dengan URL fungsi menggunakan AWS Serverless Application Model ()AWS SAM.

```
ProductFunction:
  Type: AWS::Serverless::Function
  Properties:
    CodeUri: function/.
    Handler: index.handler
    Runtime: nodejs18.x
    AutoPublishAlias: live
    FunctionUrlConfig:
      AuthType: NONE
```

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Memahami penskalaan fungsi Lambda

Konkurensi adalah jumlah permintaan dalam penerbangan yang ditangani oleh AWS Lambda fungsi Anda pada saat yang bersamaan. Untuk setiap permintaan bersamaan, Lambda menyediakan instance terpisah dari lingkungan eksekusi Anda. Saat fungsi Anda menerima lebih banyak permintaan, Lambda secara otomatis menangani penskalaan jumlah lingkungan eksekusi hingga Anda mencapai batas konkurensi akun Anda. Secara default, Lambda menyediakan akun Anda dengan batas konkurensi total 1.000 eksekusi bersamaan di semua fungsi dalam file. Wilayah AWS Untuk mendukung kebutuhan akun spesifik Anda, Anda dapat [meminta peningkatan kuota](#) dan mengonfigurasi kontrol konkurensi tingkat fungsi sehingga fungsi penting Anda tidak mengalami pelambatan.

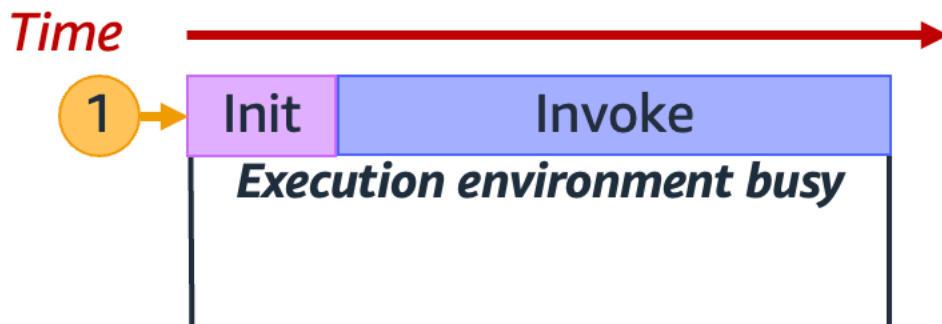
Topik ini menjelaskan konsep konkurensi dan penskalaan fungsi di Lambda. Pada akhir topik ini, Anda akan dapat memahami cara menghitung konkurensi, memvisualisasikan dua opsi kontrol konkurensi utama (dicadangkan dan disediakan), memperkirakan pengaturan kontrol konkurensi yang sesuai, dan melihat metrik untuk pengoptimalan lebih lanjut.

Bagian-bagian

- [Memahami dan memvisualisasikan konkurensi](#)
- [Menghitung konkurensi untuk suatu fungsi](#)
- [Memahami konkurensi cadangan dan konkurensi yang disediakan](#)
- [Memahami konkurensi dan permintaan per detik](#)
- [Kuota konkurensi](#)
- [Mengkonfigurasi konkurensi cadangan untuk suatu fungsi](#)
- [Mengkonfigurasi konkurensi yang disediakan untuk suatu fungsi](#)
- [Perilaku penskalaan Lambda](#)
- [Memantau konkurensi](#)

Memahami dan memvisualisasikan konkurensi

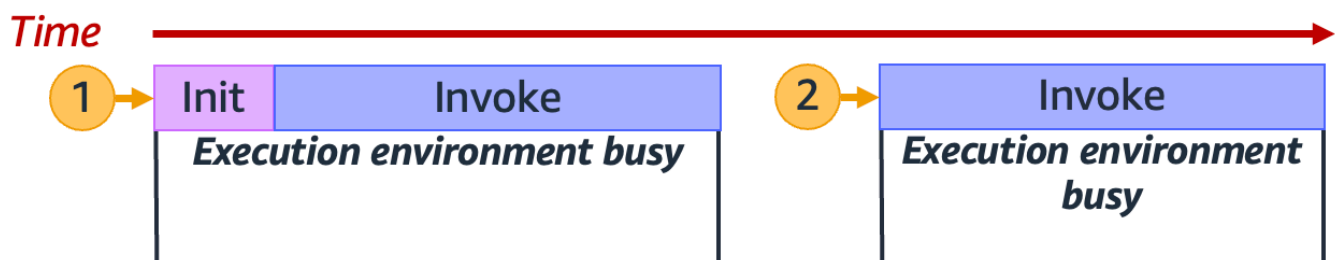
[Lambda memanggil fungsi Anda di lingkungan eksekusi yang aman dan terisolasi. Untuk menangani permintaan, Lambda harus terlebih dahulu menginisialisasi lingkungan eksekusi \(fase Init\), sebelum menggunakannya untuk memanggil fungsi Anda \(fase Invoke\):](#)

**Note**

Durasi Init dan Invoke yang sebenarnya dapat bervariasi tergantung pada banyak faktor, seperti runtime yang Anda pilih dan kode fungsi Lambda. Diagram sebelumnya tidak dimaksudkan untuk mewakili proporsi yang tepat dari durasi fase Init dan Invoke.

Diagram sebelumnya menggunakan persegi panjang untuk mewakili lingkungan eksekusi tunggal. Ketika fungsi Anda menerima permintaan pertamanya (diwakili oleh lingkaran kuning dengan label 1), Lambda membuat lingkungan eksekusi baru dan menjalankan kode di luar handler utama Anda selama fase Init. Kemudian, Lambda menjalankan kode handler utama fungsi Anda selama fase Invoke. Selama seluruh proses ini, lingkungan eksekusi ini sibuk dan tidak dapat memproses permintaan lainnya.

Ketika Lambda selesai memproses permintaan pertama, lingkungan eksekusi ini kemudian dapat memproses permintaan tambahan untuk fungsi yang sama. Untuk permintaan berikutnya, Lambda tidak perlu menginisialisasi ulang lingkungan.

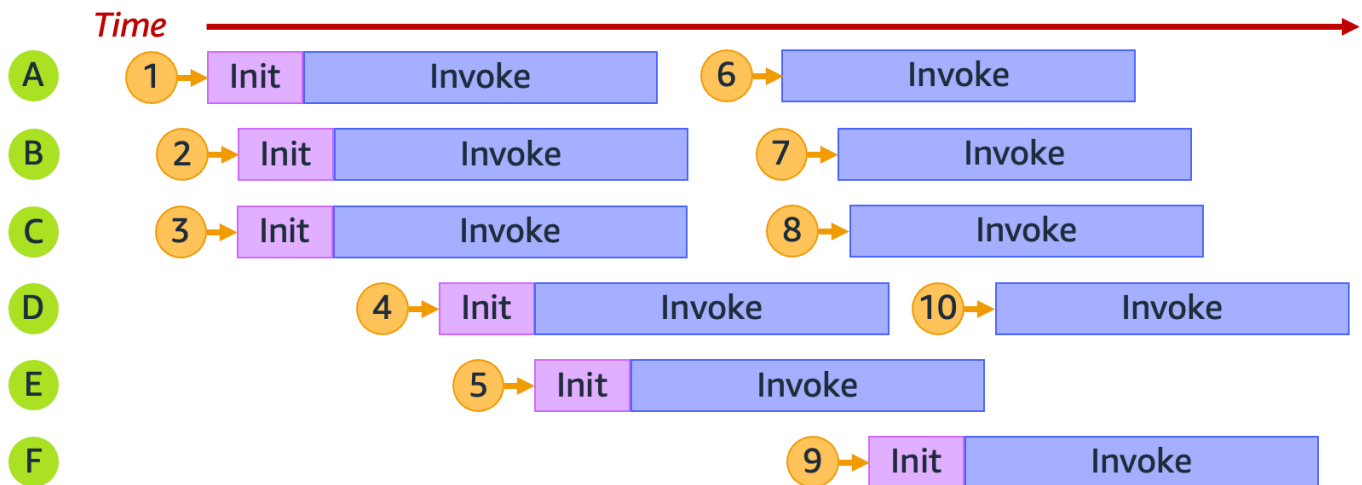


Pada diagram sebelumnya, Lambda menggunakan kembali lingkungan eksekusi untuk menangani permintaan kedua (diwakili oleh lingkaran kuning dengan label). 2

Sejauh ini, kami hanya berfokus pada satu contoh lingkungan eksekusi Anda (yaitu, konkurensi 1). Dalam praktiknya, Lambda mungkin perlu menyediakan beberapa instance lingkungan eksekusi secara paralel untuk menangani semua permintaan yang masuk. Ketika fungsi Anda menerima permintaan baru, salah satu dari dua hal dapat terjadi:

- Jika instance lingkungan eksekusi pra-inisialisasi tersedia, Lambda menggunakannya untuk memproses permintaan.
- Jika tidak, Lambda membuat instance lingkungan eksekusi baru untuk memproses permintaan.

Misalnya, mari kita jelajahi apa yang terjadi ketika fungsi Anda menerima 10 permintaan:



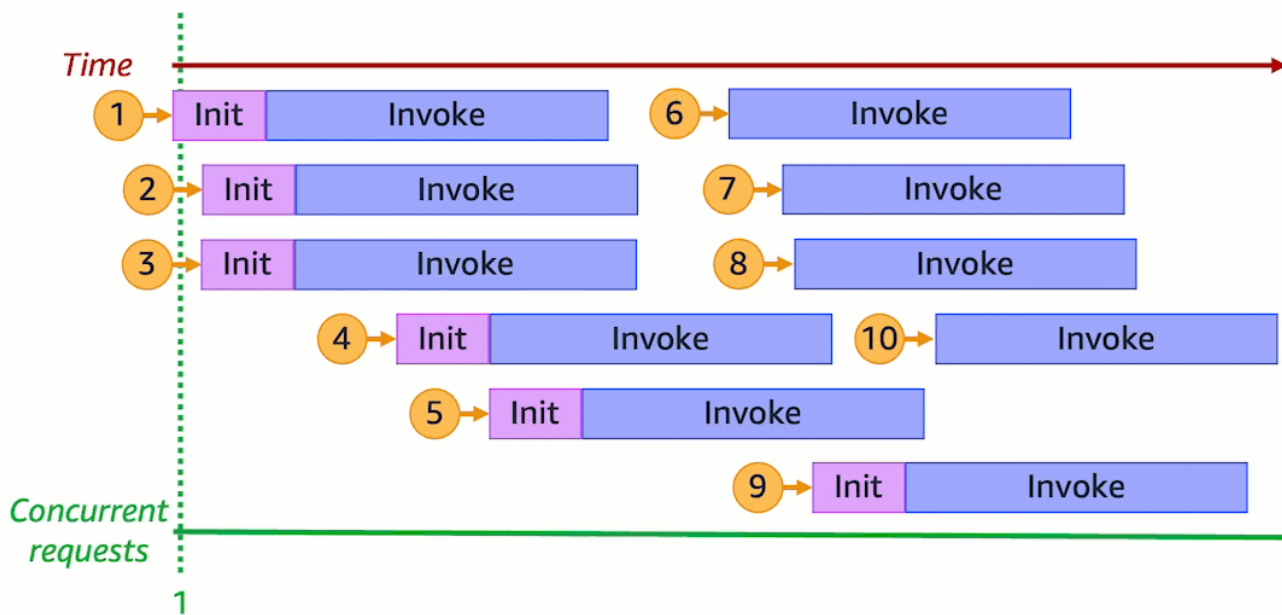
Dalam diagram sebelumnya, setiap bidang horizontal mewakili contoh lingkungan eksekusi tunggal (diberi label dari A melalui F). Inilah cara Lambda menangani setiap permintaan:

| Permintaan | Perilaku Lambda | Penalaran |
|------------|-----------------------------|--|
| 1 | Ketentuan lingkungan baru A | Ini adalah permintaan pertama; tidak ada instance lingkungan eksekusi yang tersedia. |

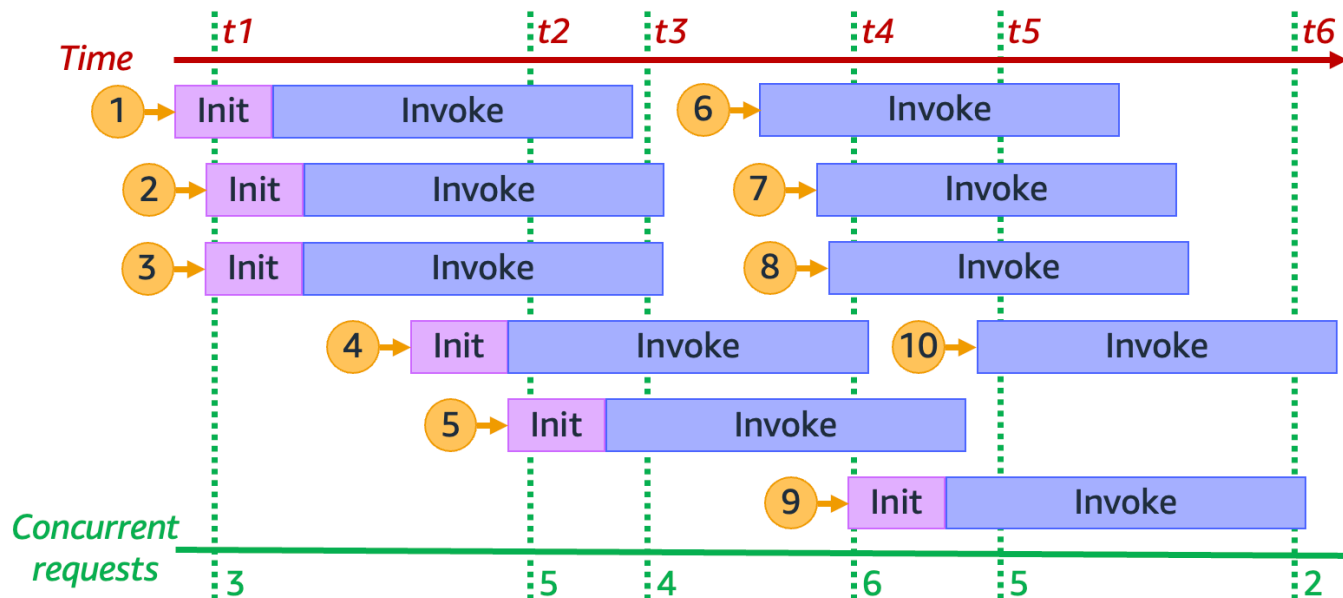
| Permintaan | Perilaku Lambda | Penalaran |
|------------|----------------------------------|--|
| 2 | Ketentuan lingkungan baru B | Lingkungan eksekusi yang ada misalnya A sibuk. |
| 3 | Ketentuan lingkungan baru C | Instans lingkungan eksekusi yang ada A dan B keduanya sibuk. |
| 4 | Ketentuan lingkungan baru D | Instans lingkungan eksekusi yang ada A, B, dan C semuanya sibuk. |
| 5 | Ketentuan lingkungan baru E | Contoh lingkungan eksekusi yang ada A, B, C, dan D semuanya sibuk. |
| 6 | Menggunakan kembali lingkungan A | Lingkungan eksekusi instance A telah selesai memproses permintaan 1 dan sekarang tersedia. |
| 7 | Menggunakan kembali lingkungan B | Contoh lingkungan eksekusi B telah selesai memproses permintaan 2 dan sekarang tersedia. |
| 8 | Menggunakan kembali lingkungan C | Contoh lingkungan eksekusi C telah selesai memproses permintaan 3 dan sekarang tersedia. |
| 9 | Ketentuan lingkungan baru F | Contoh lingkungan eksekusi yang ada A, B, C, D, dan E semuanya sibuk. |

| Permintaan | Perilaku Lambda | Penalaran |
|------------|----------------------------------|--|
| 10 | Menggunakan kembali lingkungan D | Contoh lingkungan eksekusi D telah selesai memproses permintaan 4 dan sekarang tersedia. |

Saat fungsi Anda menerima lebih banyak permintaan bersamaan, Lambda meningkatkan jumlah instance lingkungan eksekusi sebagai respons. Animasi berikut melacak jumlah permintaan bersamaan dari waktu ke waktu:



Dengan membekukan animasi sebelumnya pada enam titik waktu yang berbeda, kita mendapatkan diagram berikut:



Pada diagram sebelumnya, kita dapat menggambar garis vertikal kapan saja dan menghitung jumlah lingkungan yang memotong garis ini. Ini memberi kita jumlah permintaan bersamaan pada saat itu. Misalnya, pada waktu t_1 , ada tiga lingkungan aktif yang melayani tiga permintaan bersamaan. Jumlah maksimum permintaan bersamaan dalam simulasi ini terjadi pada waktu t_4 , ketika ada enam lingkungan aktif yang melayani enam permintaan bersamaan.

Untuk meringkas, konkurensi fungsi Anda adalah jumlah permintaan bersamaan yang ditangani secara bersamaan. Menanggapi peningkatan konkurensi fungsi Anda, Lambda menyediakan lebih banyak instance lingkungan eksekusi untuk memenuhi permintaan permintaan.

Menghitung konkurensi untuk suatu fungsi

Secara umum, konkurensi suatu sistem adalah kemampuan untuk memproses lebih dari satu tugas secara bersamaan. Di Lambda, konkurensi adalah jumlah permintaan dalam penerbangan yang ditangani fungsi Anda secara bersamaan. Cara cepat dan praktis untuk mengukur konkurensi fungsi Lambda adalah dengan menggunakan rumus berikut:

$$\text{Concurrency} = (\text{average requests per second}) * (\text{average request duration in seconds})$$

Konkurensi berbeda dari permintaan per detik. Misalnya, fungsi Anda menerima rata-rata 100 permintaan per detik. Jika durasi permintaan rata-rata adalah satu detik, maka memang benar bahwa konkurensi juga 100:

$$\text{Concurrency} = (100 \text{ requests/second}) * (1 \text{ second/request}) = 100$$

Namun, jika durasi permintaan rata-rata adalah 500 ms, maka konkurensi adalah 50:

$$\text{Concurrency} = (100 \text{ requests/second}) * (0.5 \text{ second/request}) = 50$$

Apa arti konkurensi 50 dalam praktik? Jika durasi permintaan rata-rata adalah 500 ms, maka Anda dapat menganggap instance fungsi Anda mampu menangani dua permintaan per detik. Kemudian, dibutuhkan 50 instance fungsi Anda untuk menangani beban 100 permintaan per detik. Konkurensi 50 berarti bahwa Lambda harus menyediakan 50 instance lingkungan eksekusi untuk menangani beban kerja ini secara efisien tanpa pembatasan apa pun. Berikut cara mengekspresikan ini dalam bentuk persamaan:

$$\text{Concurrency} = (100 \text{ requests/second}) / (2 \text{ requests/second}) = 50$$

Jika fungsi Anda menerima dua kali lipat jumlah permintaan (200 permintaan per detik), tetapi hanya membutuhkan separuh waktu untuk memproses setiap permintaan (250 ms), maka konkurensi masih 50:

$$\text{Concurrency} = (200 \text{ requests/second}) * (0.25 \text{ second/request}) = 50$$

Uji pemahaman Anda tentang konkurensi

Misalkan Anda memiliki fungsi yang membutuhkan, rata-rata, 200 ms untuk dijalankan. Selama beban puncak, Anda mengamati 5.000 permintaan per detik. Apa konkurensi fungsi Anda selama beban puncak?

Jawaban

Durasi fungsi rata-rata adalah 200 ms, atau 0,2 detik. Dengan menggunakan rumus konkurensi, Anda dapat memasukkan angka untuk mendapatkan konkurensi 1.000:

$$\text{Concurrency} = (5,000 \text{ requests/second}) * (0.2 \text{ seconds/request}) = 1,000$$

Atau, durasi fungsi rata-rata 200 ms berarti bahwa fungsi Anda dapat memproses 5 permintaan per detik. Untuk menangani beban kerja 5.000 permintaan per detik, Anda memerlukan 1.000 instance lingkungan eksekusi. Jadi, konkurensi adalah 1.000:

$$\text{Concurrency} = (5,000 \text{ requests/second}) / (5 \text{ requests/second}) = 1,000$$

Memahami konkurensi cadangan dan konkurensi yang disediakan

Secara default, akun Anda memiliki batas konkurensi 1.000 eksekusi bersamaan di semua fungsi di Wilayah. Fungsi Anda berbagi kumpulan 1.000 konkurensi ini berdasarkan permintaan. Fungsi Anda mengalami pelambatan (yaitu, mereka mulai menghapus permintaan) jika Anda kehabisan konkurensi yang tersedia.

Beberapa fungsi Anda mungkin lebih penting daripada yang lain. Akibatnya, Anda mungkin ingin mengonfigurasi pengaturan konkurensi untuk memastikan bahwa fungsi penting mendapatkan konkurensi yang mereka butuhkan. Ada dua jenis kontrol konkurensi yang tersedia: konkurensi cadangan dan konkurensi yang disediakan.

- Gunakan konkurensi cadangan untuk memesan sebagian dari konkurensi akun Anda untuk suatu fungsi. Ini berguna jika Anda tidak ingin fungsi lain mengambil semua konkurensi tanpa syarat yang tersedia.
- Gunakan konkurensi yang disediakan untuk menginisialisasi sejumlah instance lingkungan untuk suatu fungsi. Ini berguna untuk mengurangi latensi start dingin.

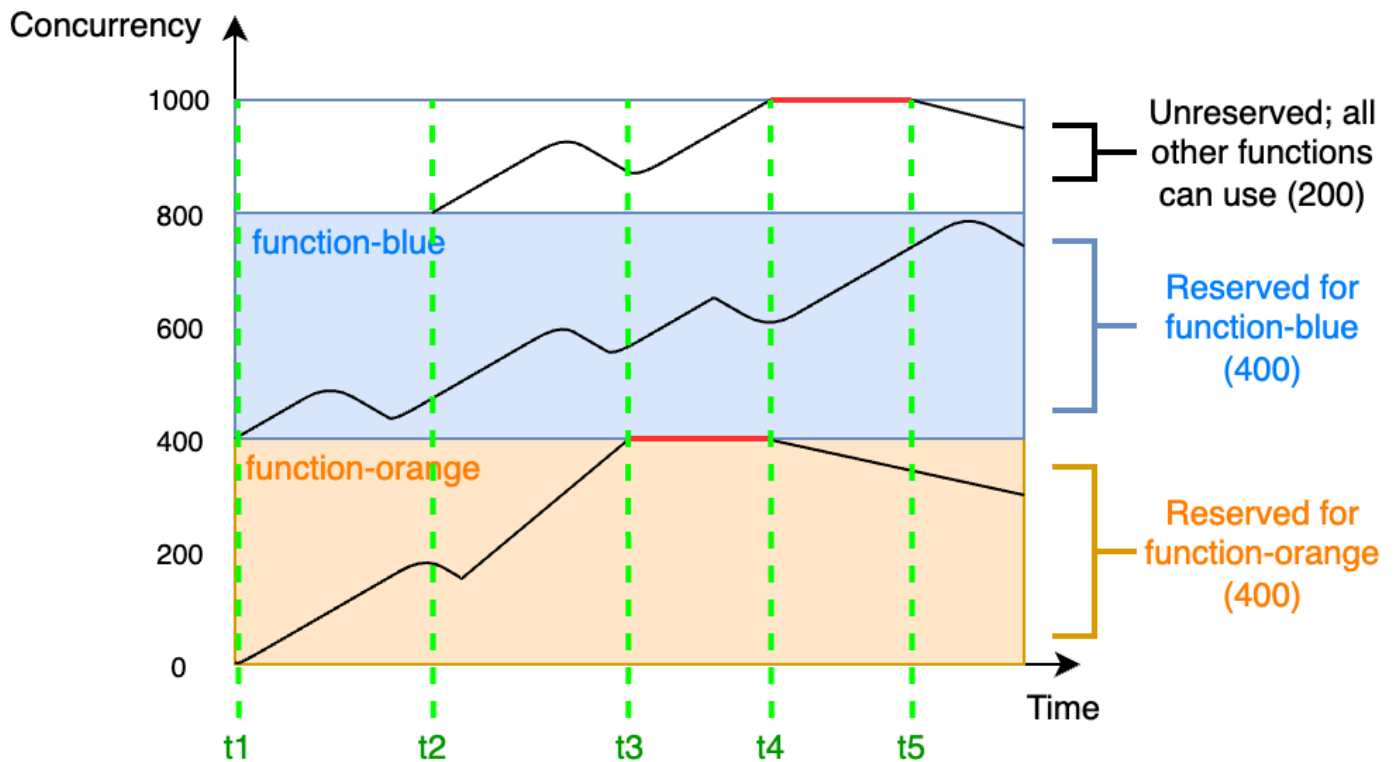
Konkurensi terpesan

Jika Anda ingin menjamin bahwa sejumlah konkurensi tersedia untuk fungsi Anda kapan saja, gunakan konkurensi cadangan.

Konkurensi cadangan adalah jumlah maksimum instance bersamaan yang ingin Anda alokasikan ke fungsi Anda. Saat Anda mendedikasikan konkurensi cadangan ke suatu fungsi, tidak ada fungsi lain yang dapat menggunakan konkurensi itu. Dengan kata lain, pengaturan konkurensi cadangan dapat memengaruhi kumpulan konkurensi yang tersedia untuk fungsi lain. Fungsi yang tidak memiliki konkurensi cadangan berbagi kumpulan konkurensi tanpa syarat yang tersisa.

Mengkonfigurasi jumlah konkurensi cadangan terhadap batas konkurensi akun Anda secara keseluruhan. Tidak ada biaya untuk mengonfigurasi konkurensi terpesan untuk fungsi.

Untuk lebih memahami konkurensi cadangan, pertimbangkan diagram berikut:



Dalam diagram ini, batas konkurensi akun Anda untuk semua fungsi di Wilayah ini berada pada batas default 1.000. Misalkan Anda memiliki dua fungsi penting, `function-blue` dan `function-orange`, yang secara rutin mengharapkan untuk mendapatkan volume pemanggilan yang tinggi. Anda memutuskan untuk memberikan 400 unit konkurensi cadangan ke `function-blue`, dan 400 unit konkurensi cadangan untuk `function-orange`. Dalam contoh ini, semua fungsi lain di akun Anda harus membagikan 200 unit konkurensi tanpa syarat yang tersisa.

Diagram memiliki lima poin menarik:

- Di `t1`, keduanya `function-orange` dan `function-blue` mulai menerima permintaan. Setiap fungsi mulai menggunakan bagian yang dialokasikan dari unit konkurensi cadangan.
- Di `t2`, `function-orange` dan `function-blue` terus menerima lebih banyak permintaan. Pada saat yang sama, Anda menerapkan beberapa fungsi Lambda lainnya, yang mulai menerima permintaan. Anda tidak mengalokasikan konkurensi cadangan untuk fungsi-fungsi lain ini. Mereka mulai menggunakan 200 unit konkurensi tanpa syarat yang tersisa.
- Pada `t3`, `function-orange` mencapai konkurensi maks 400. Meskipun ada konkurensi yang tidak digunakan di tempat lain di akun Anda, `function-orange` tidak dapat mengaksesnya. Garis

merah menunjukkan bahwa `function-orange` sedang mengalami pelambatan, dan Lambda dapat membatalkan permintaan.

- Pada `Padat4`, `function-orange` mulai menerima lebih sedikit permintaan dan tidak lagi melambat. Namun, fungsi Anda yang lain mengalami lonjakan lalu lintas dan mulai melambat. Meskipun ada konkurensi yang tidak digunakan di tempat lain di akun Anda, fungsi-fungsi lain ini tidak dapat mengaksesnya. Garis merah menunjukkan bahwa fungsi Anda yang lain mengalami pelambatan.
- Pada `Padat5`, fungsi lain mulai menerima lebih sedikit permintaan dan tidak lagi melambat.

Dari contoh ini, perhatikan bahwa `reserving concurrency` memiliki efek sebagai berikut:

- Fungsi Anda dapat menskalakan secara independen dari fungsi lain di akun Anda. Semua fungsi akun Anda di Wilayah yang sama yang tidak memiliki konkurensi cadangan berbagi kumpulan konkurensi tanpa syarat. Tanpa konkurensi cadangan, fungsi lain berpotensi menggunakan semua konkurensi Anda yang tersedia. Ini mencegah fungsi penting meningkat jika diperlukan.
- Fungsi Anda tidak dapat skala di luar kendali. Konkurensi cadangan membatasi konkurensi maksimum fungsi Anda. Ini berarti bahwa fungsi Anda tidak dapat menggunakan konkurensi yang dicadangkan untuk fungsi lain, atau konkurensi dari kumpulan yang tidak dipesan. Anda dapat memesan konkurensi untuk mencegah fungsi Anda menggunakan semua konkurensi yang tersedia di akun Anda, atau membebani sumber daya hilir yang berlebihan.
- Anda mungkin tidak dapat menggunakan semua konkurensi akun Anda yang tersedia. Reservasi konkurensi diperhitungkan terhadap batas konkurensi akun Anda, tetapi ini juga berarti bahwa fungsi lain tidak dapat menggunakan potongan konkurensi cadangan itu. Jika fungsi Anda tidak menggunakan semua konkurensi yang Anda pesan untuk itu, Anda secara efektif membuang-buang konkurensi itu. Ini bukan masalah kecuali fungsi lain di akun Anda bisa mendapatkan keuntungan dari konkurensi yang terbuang.

Untuk mempelajari cara mengelola setelan konkurensi cadangan untuk fungsi Anda, lihat [Mengkonfigurasi konkurensi cadangan untuk suatu fungsi](#).

Konkurensi terprovisi

Anda menggunakan konkurensi cadangan untuk menentukan jumlah maksimum lingkungan eksekusi yang dicadangkan untuk fungsi Lambda. Namun, tidak satu pun dari lingkungan ini yang diinisialisasi sebelumnya. Akibatnya, pemanggilan fungsi Anda mungkin memakan waktu lebih lama karena Lambda harus terlebih dahulu menginisialisasi lingkungan baru sebelum dapat menggunakannya untuk memanggil fungsi Anda. Ketika Lambda harus menginisialisasi lingkungan baru untuk

melaksanakan doa, ini dikenal sebagai awal yang dingin. Untuk mengurangi start dingin, Anda dapat menggunakan konkurensi yang disediakan.

Konkurensi yang disediakan adalah jumlah lingkungan eksekusi pra-inisialisasi yang ingin Anda alokasikan ke fungsi Anda. Jika Anda menyetel konkurensi yang disediakan pada suatu fungsi, Lambda menginisialisasi jumlah lingkungan eksekusi tersebut sehingga mereka siap untuk segera merespons permintaan fungsi.

Note

Menggunakan konkurensi yang disediakan menimbulkan biaya tambahan ke akun Anda. Jika Anda bekerja dengan runtime Java 11 atau Java 17, Anda juga dapat menggunakan SnapStart Lambda untuk mengurangi masalah start dingin tanpa biaya tambahan. SnapStart menggunakan snapshot cache dari lingkungan eksekusi Anda untuk meningkatkan kinerja startup secara signifikan. Anda tidak dapat menggunakan keduanya SnapStart dan konkurensi yang disediakan pada versi fungsi yang sama. Untuk informasi selengkapnya tentang SnapStart fitur, batasan, dan Wilayah yang didukung, lihat [Meningkatkan kinerja startup dengan Lambda SnapStart](#).

Saat menggunakan konkurensi yang disediakan, Lambda masih mendaur ulang lingkungan eksekusi di latar belakang. Namun, pada waktu tertentu, Lambda selalu memastikan bahwa jumlah lingkungan pra-inisialisasi sama dengan nilai setelah konkurensi yang disediakan fungsi Anda. Perilaku ini berbeda dari konkurensi cadangan, di mana Lambda dapat sepenuhnya mengakhiri lingkungan setelah periode tidak aktif. Diagram berikut mengilustrasikan hal ini dengan membandingkan siklus hidup lingkungan eksekusi tunggal saat Anda mengonfigurasi fungsi menggunakan konkurensi cadangan dibandingkan dengan konkurensi yang disediakan.

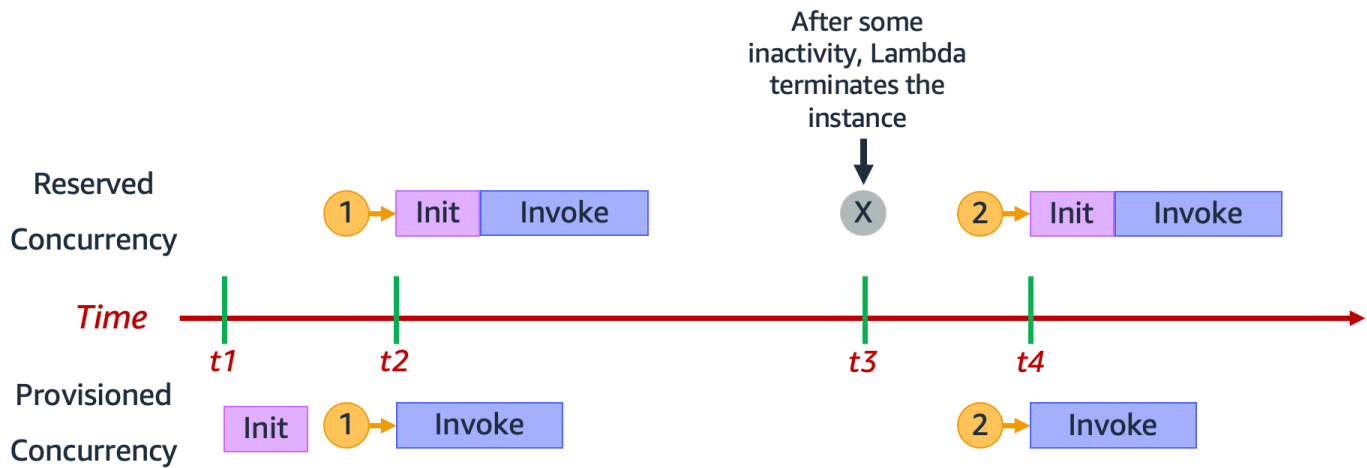
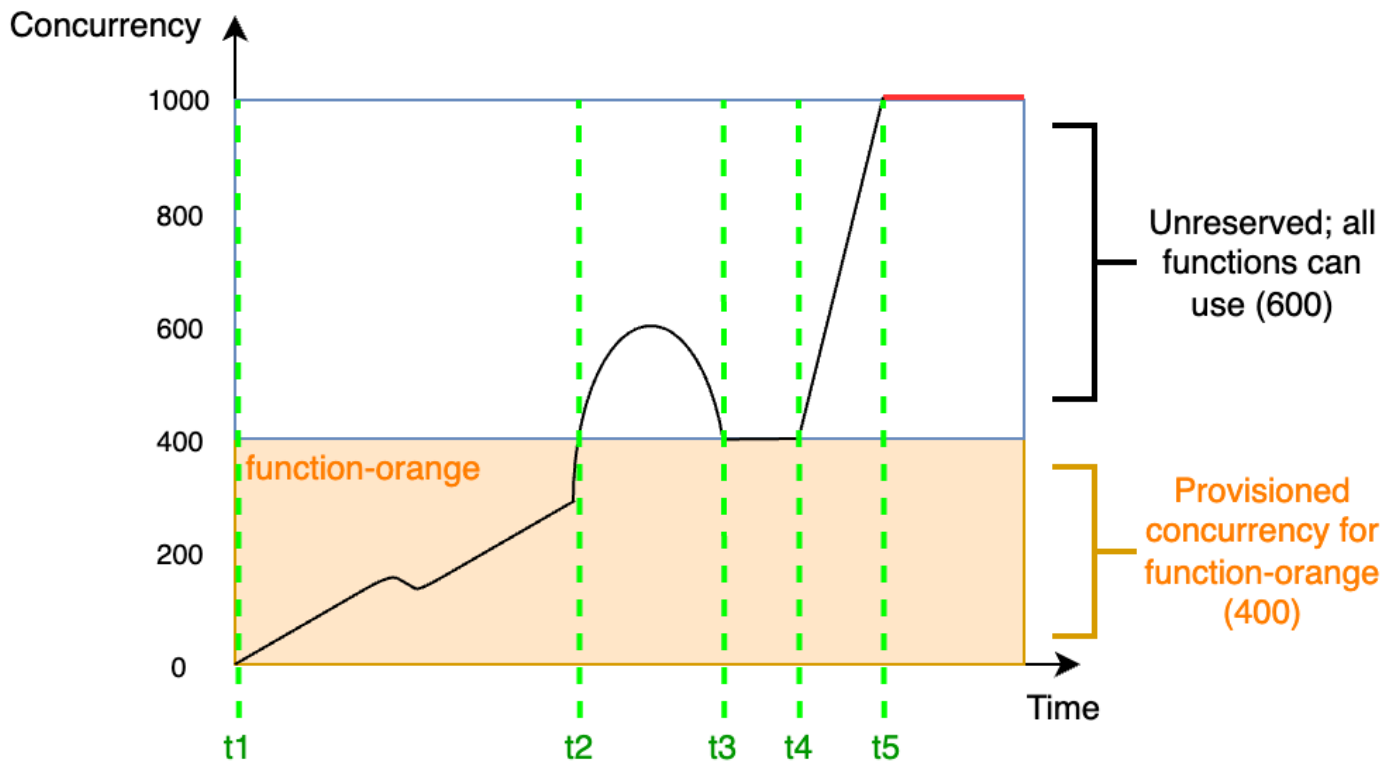


Diagram memiliki empat tempat menarik:

| Waktu | Konkurensi terpesan | Konkurensi terprovisi |
|-------|--|--|
| t1 | Tidak ada yang terjadi. | Lambda melakukan pra-inisialisasi instance lingkungan eksekusi. |
| t2 | Permintaan 1 masuk. Lambda harus menginisialisasi instance lingkungan eksekusi baru. | Permintaan 1 masuk. Lambda menggunakan instance lingkungan pra-inisialisasi. |
| t3 | Setelah beberapa tidak aktif, Lambda menghentikan instance lingkungan aktif. | Tidak ada yang terjadi. |
| t4 | Permintaan 2 masuk. Lambda harus menginisialisasi instance lingkungan eksekusi baru. | Permintaan 2 masuk. Lambda menggunakan instance lingkungan pra-inisialisasi. |

Untuk lebih memahami konkurensi yang disediakan, pertimbangkan diagram berikut:



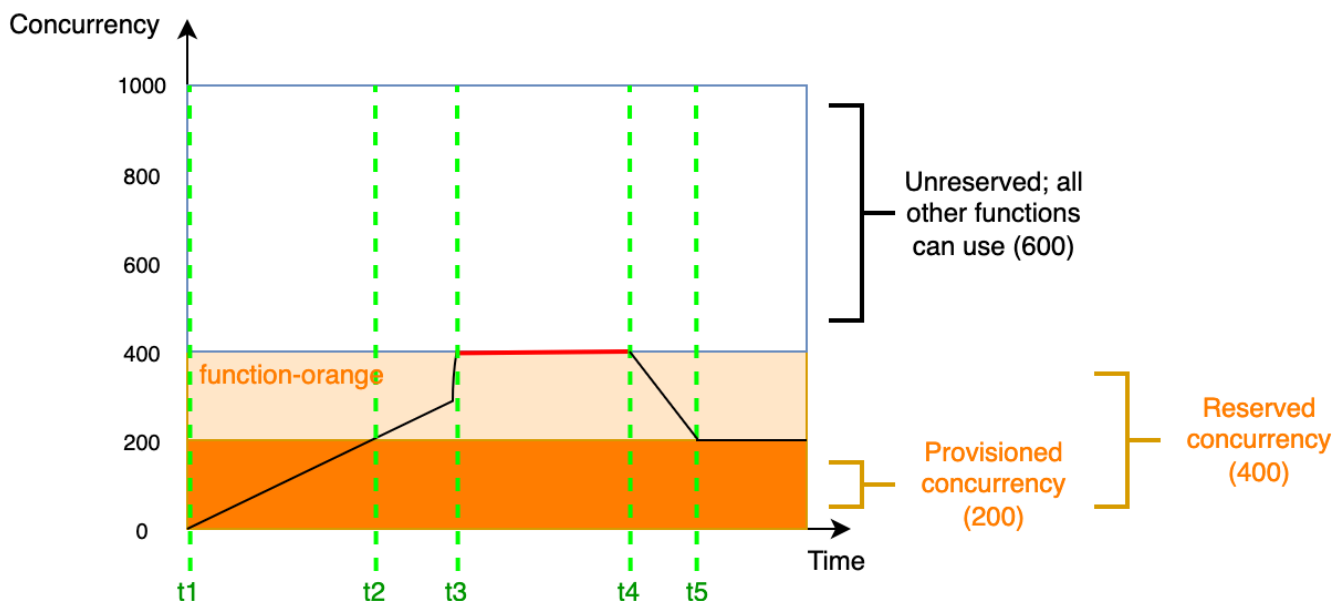
Dalam diagram ini, Anda memiliki batas konkurensi akun 1.000. Anda memutuskan untuk memberikan 400 unit konkurensi yang disediakan ke `function-orange`. Semua fungsi di akun Anda, termasuk `function-orange`, dapat menggunakan sisa 600 unit konkurensi tanpa syarat.

Diagram memiliki lima poin menarik:

- Pada `t1`, `function-orange` mulai menerima permintaan. Karena Lambda memiliki 400 instance lingkungan eksekusi yang telah diinisialisasi sebelumnya, `function-orange` siap untuk pemanggilan segera.
- Pada `t2`, `function-orange` mencapai 400 permintaan bersamaan. Akibatnya, `function-orange` kehabisan konkurensi yang disediakan. Namun, karena masih ada konkurensi tanpa syarat yang tersedia, Lambda dapat menggunakan ini untuk menangani permintaan tambahan `function-orange` (tidak ada pembatasan). Lambda harus membuat instance baru untuk melayani permintaan ini, dan fungsi Anda mungkin mengalami latensi start dingin.
- Pada `t3`, `function-orange` kembali ke 400 permintaan bersamaan setelah lonjakan lalu lintas singkat. Lambda sekali lagi dapat menangani semua permintaan tanpa latensi start dingin.

- Dit4, fungsi di akun Anda mengalami ledakan lalu lintas. Burst ini dapat berasal dari `function-orange` atau fungsi lain di akun Anda. Lambda menggunakan konkurensi tanpa syarat untuk menangani permintaan ini.
- Dit5, fungsi di akun Anda mencapai batas konkurensi maksimum 1.000, dan mengalami pelambatan.

Contoh sebelumnya dianggap hanya konkurensi yang disediakan. Dalam praktiknya, Anda dapat mengatur konkurensi yang disediakan dan konkurensi cadangan pada suatu fungsi. Anda dapat melakukan ini jika Anda memiliki fungsi yang menangani beban pemanggilan yang konsisten pada hari kerja, tetapi secara rutin melihat lonjakan lalu lintas pada akhir pekan. Dalam hal ini, Anda dapat menggunakan konkurensi yang disediakan untuk menetapkan jumlah dasar lingkungan untuk menangani permintaan selama hari kerja, dan menggunakan konkurensi cadangan untuk menangani lonjakan akhir pekan. Pertimbangkan diagram berikut:



Dalam diagram ini, misalkan Anda mengonfigurasi 200 unit konkurensi yang disediakan dan 400 unit konkurensi cadangan untuk `function-orange`. Karena Anda mengonfigurasi konkurensi cadangan, `function-orange` tidak dapat menggunakan salah satu dari 600 unit konkurensi tanpa syarat.

Diagram ini memiliki lima poin menarik:

- **Padat1**, `function-orange` mulai menerima permintaan. Karena Lambda memiliki 200 instance lingkungan eksekusi yang telah diinisialisasi sebelumnya, `function-orange` siap untuk pemanggilan segera.
- **Dit2**, `function-orange` menggunakan semua konkurensi yang disediakan. `function-orange` dapat terus melayani permintaan menggunakan konkurensi cadangan, tetapi permintaan ini mungkin mengalami latensi awal yang dingin.
- **Padat3**, `function-orange` mencapai 400 permintaan bersamaan. Akibatnya, `function-orange` menggunakan semua konkurensi yang dicadangkan. Karena `function-orange` tidak dapat menggunakan konkurensi tanpa syarat, permintaan mulai melambat.
- **Padat4**, `function-orange` mulai menerima lebih sedikit permintaan, dan tidak lagi throttle.
- **Padat5**, `function-orange` turun ke 200 permintaan bersamaan, sehingga semua permintaan kembali dapat menggunakan konkurensi yang disediakan (yaitu, tidak ada latensi start dingin).

[Baik konkurensi cadangan maupun konkurensi yang disediakan dihitung terhadap batas konkurensi akun Anda dan kuota Regional.](#) Dengan kata lain, mengalokasikan konkurensi yang dicadangkan dan disediakan dapat memengaruhi kumpulan konkurensi yang tersedia untuk fungsi lain. Mengonfigurasi konkurensi yang disediakan menimbulkan biaya ke Anda. Akun AWS

Note

Jika jumlah konkurensi yang disediakan pada versi dan alias fungsi ditambahkan ke konkurensi cadangan fungsi, maka semua pemanggilan berjalan pada konkurensi yang disediakan. Konfigurasi ini juga memiliki efek membatasi versi fungsi yang tidak dipublikasikan (\$LATEST), yang mencegahnya dijalankan. Anda tidak dapat mengalokasikan lebih banyak konkurensi terprovisi dari konkurensi terpesan untuk fungsi.

Untuk mengelola setelan konkurensi yang disediakan untuk fungsi Anda, lihat [Mengkonfigurasi konkurensi yang disediakan untuk suatu fungsi](#) Untuk mengotomatiskan penskalaan konkurensi yang disediakan berdasarkan jadwal atau pemanfaatan aplikasi, lihat [Menggunakan Application Auto Scaling untuk mengotomatiskan manajemen konkurensi yang disediakan](#)

Bagaimana Lambda mengalokasikan konkurensi yang disediakan

Konkurensi yang disediakan tidak langsung online setelah Anda mengonfigurasinya. Lambda mulai mengalokasikan konkurensi terprovisi setelah satu atau dua menit persiapan. Untuk setiap fungsi,

Lambda dapat menyediakan hingga 6.000 lingkungan eksekusi setiap menit, terlepas dari itu. Wilayah AWS Ini persis sama dengan [tingkat penskalaan konkurensi untuk fungsi](#).

Saat Anda mengirimkan permintaan untuk mengalokasikan konkurensi yang disediakan, Anda tidak dapat mengakses salah satu lingkungan tersebut hingga Lambda benar-benar selesai mengalokasikannya. Misalnya, jika Anda meminta 5.000 konkurensi yang disediakan, tidak ada permintaan yang dapat menggunakan konkurensi yang disediakan hingga Lambda benar-benar selesai mengalokasikan 5.000 lingkungan eksekusi.

Membandingkan konkurensi cadangan dan konkurensi yang disediakan

Tabel berikut merangkum dan membandingkan konkurensi yang dicadangkan dan disediakan.

| Topik | Konkurensi terpesan | Konkurensi terprovisi |
|----------------------|---|---|
| Definisi | Jumlah maksimum instance lingkungan eksekusi untuk fungsi Anda. | Tetapkan jumlah instance lingkungan eksekusi yang telah disediakan sebelumnya untuk fungsi Anda. |
| Perilaku penyediaan | Lambda menyediakan instans baru berdasarkan permintaan. | Instans pra-ketentuan Lambda (yaitu, sebelum fungsi Anda mulai menerima permintaan). |
| Perilaku awal dingin | Latensi start dingin dimungkinkan, karena Lambda harus membuat instance baru sesuai permintaan. | Latensi start dingin tidak dimungkinkan, karena Lambda tidak harus membuat instance sesuai permintaan. |
| Perilaku melambat | Fungsi dibatasi ketika batas konkurensi cadangan tercapai. | <p>Jika konkurensi cadangan tidak disetel: fungsi menggunakan konkurensi tanpa syarat saat batas konkurensi yang disediakan tercapai.</p> <p>Jika set konkurensi cadangan: fungsi dibatasi saat batas konkurensi cadangan tercapai.</p> |

| Topik | Konkurensi terpesan | Konkurensi terprovisi |
|-------------------------------------|--|--|
| Perilaku default jika tidak disetel | Fungsi menggunakan konkurensi tanpa syarat yang tersedia di akun Anda. | Lambda tidak menyediakan instan apa pun terlebih dahulu. Sebaliknya, jika konkurensi cadangan tidak disetel: fungsi menggunakan konkurensi tanpa syarat yang tersedia di akun Anda. Jika set konkurensi cadangan: fungsi menggunakan konkurensi cadangan. |
| Harga | Tidak ada biaya tambahan. | Mengalami biaya tambahan. |

Memahami konkurensi dan permintaan per detik

Seperti disebutkan di bagian sebelumnya, konkurensi berbeda dari permintaan per detik. Ini adalah perbedaan yang sangat penting untuk dibuat ketika bekerja dengan fungsi yang memiliki durasi permintaan rata-rata kurang dari 100 ms.

Di semua fungsi di akun Anda, Lambda memberlakukan batas permintaan per detik yang sama dengan 10 kali konkurensi akun Anda. Misalnya, karena batas konkurensi akun default adalah 1.000, fungsi di akun Anda dapat menangani maksimum 10.000 permintaan per detik.

Misalnya, pertimbangkan fungsi dengan durasi permintaan rata-rata 50 ms. Pada 20.000 permintaan per detik, inilah konkurensi fungsi ini:

$$\text{Concurrency} = (20,000 \text{ requests/second}) * (0.05 \text{ second/request}) = 1,000$$

Berdasarkan hasil ini, Anda mungkin berharap bahwa batas konkurensi akun 1.000 cukup untuk menangani beban ini. Namun, karena batas 10.000 permintaan per detik, fungsi Anda hanya dapat menangani 10.000 permintaan per detik dari total 20.000 permintaan. Fungsi ini mengalami pelambatan.

Pelajarannya adalah Anda harus mempertimbangkan konkurensi dan permintaan per detik saat mengonfigurasi pengaturan konkurensi untuk fungsi Anda. Dalam hal ini, Anda perlu meminta

konkurensi akun limit meningkat menjadi 2.000, karena ini akan meningkatkan total permintaan per detik batas menjadi 20.000.

Note

Berdasarkan batas permintaan per detik ini, tidak benar untuk mengatakan bahwa setiap lingkungan eksekusi Lambda hanya dapat menangani maksimum 10 permintaan per detik. Alih-alih mengamati beban pada setiap lingkungan eksekusi individu, Lambda hanya mempertimbangkan keseluruhan konkurensi dan permintaan keseluruhan per detik saat menghitung kuota Anda.

Uji pemahaman Anda tentang konkurensi (fungsi sub-100 ms)

Misalkan Anda memiliki fungsi yang membutuhkan, rata-rata, 20 ms untuk dijalankan. Selama beban puncak, Anda mengamati 30.000 permintaan per detik. Apa konkurensi fungsi Anda selama beban puncak?

Jawaban

Durasi fungsi rata-rata adalah 20 ms, atau 0,02 detik. Dengan menggunakan rumus konkurensi, Anda dapat memasukkan angka untuk mendapatkan konkurensi 600:

$$\text{Concurrency} = (30,000 \text{ requests/second}) * (0.02 \text{ seconds/request}) = 600$$

Secara default, batas konkurensi akun 1.000 tampaknya cukup untuk menangani beban ini. Namun, batas permintaan per detik 10.000 tidak cukup untuk menangani 30.000 permintaan per detik yang masuk. Untuk sepenuhnya mengakomodasi 30.000 permintaan, Anda perlu meminta peningkatan batas konkurensi akun menjadi 3.000 atau lebih tinggi.

Batas permintaan per detik berlaku untuk semua kuota di Lambda yang melibatkan konkurensi.

[Dengan kata lain, ini berlaku untuk fungsi on-demand sinkron, fungsi yang menggunakan konkurensi yang disediakan, dan perilaku penskalaan konkurensi.](#) Misalnya, berikut adalah beberapa skenario di mana Anda harus mempertimbangkan dengan cermat batas konkurensi dan permintaan per detik Anda:

- Fungsi yang menggunakan konkurensi sesuai permintaan dapat mengalami peningkatan ledakan 500 konkurensi setiap 10 detik, atau 5.000 permintaan per detik setiap 10 detik, mana yang terjadi lebih dulu.

- Misalkan Anda memiliki fungsi yang memiliki alokasi konkurensi yang disediakan 10. Fungsi ini tumpah ke konkurensi sesuai permintaan setelah 10 konkurensi atau 100 permintaan per detik, mana yang terjadi lebih dulu.

Kuota konkurensi

Lambda menetapkan kuota untuk jumlah total konkurensi yang dapat Anda gunakan di semua fungsi di Wilayah. Kuota ini ada pada dua tingkatan:

- Pada tingkat akun, fungsi Anda dapat memiliki hingga 1.000 unit konkurensi secara default. Untuk meningkatkan batas ini, lihat [Meminta peningkatan kuota pada Panduan Pengguna Service Quotas](#).
- Pada tingkat fungsi, Anda dapat memesan hingga 900 unit konkurensi di semua fungsi Anda secara default. Terlepas dari total batas konkurensi akun Anda, Lambda selalu mencadangkan 100 unit konkurensi untuk fungsi Anda yang tidak secara eksplisit mencadangkan konkurensi. Misalnya, jika Anda meningkatkan batas konkurensi akun Anda menjadi 2.000, maka Anda dapat memesan hingga 1.900 unit konkurensi di tingkat fungsi.
- Pada tingkat akun dan tingkat fungsi, Lambda juga memberlakukan batas permintaan per detik sebesar 10 kali kuota konkurensi yang sesuai. [Misalnya, ini berlaku untuk konkurensi tingkat akun, fungsi yang menggunakan konkurensi sesuai permintaan, fungsi yang menggunakan konkurensi yang ditentukan, dan perilaku penskalaan konkurensi](#). Untuk informasi selengkapnya, lihat [the section called “Memahami konkurensi dan permintaan per detik”](#).

Untuk memeriksa kuota konkurensi tingkat akun Anda saat ini, gunakan AWS Command Line Interface (AWS CLI) untuk menjalankan perintah berikut:

```
aws lambda get-account-settings
```

Anda akan melihat output yang terlihat seperti berikut:

```
{
  "AccountLimit": {
    "TotalCodeSize": 80530636800,
    "CodeSizeUnzipped": 262144000,
    "CodeSizeZipped": 52428800,
    "ConcurrentExecutions": 1000,
    "UnreservedConcurrentExecutions": 900
  }
}
```



```
  },
  "AccountUsage": {
    "TotalCodeSize": 410759889,
    "FunctionCount": 8
  }
}
```

`ConcurrentExecutions` adalah total kuota konkurensi tingkat akun Anda.

`UnreservedConcurrentExecutions` adalah jumlah konkurensi cadangan yang masih dapat Anda alokasikan ke fungsi Anda.

Saat fungsi Anda menerima lebih banyak permintaan, Lambda secara otomatis meningkatkan jumlah lingkungan eksekusi untuk menangani permintaan ini hingga akun Anda mencapai kuota konkurensinya. Namun, untuk melindungi dari penskalaan berlebih sebagai respons terhadap ledakan lalu lintas yang tiba-tiba, Lambda membatasi seberapa cepat fungsi Anda dapat menskalakan. Tingkat penskalaan konkurensi ini adalah tingkat maksimum di mana fungsi di akun Anda dapat menskalakan sebagai respons terhadap peningkatan permintaan. (Artinya, seberapa cepat Lambda dapat membuat lingkungan eksekusi baru.) Tingkat penskalaan konkurensi berbeda dari batas konkurensi tingkat akun, yang merupakan jumlah total konkurensi yang tersedia untuk fungsi Anda.

Di masing-masing Wilayah AWS, dan untuk setiap fungsi, tingkat penskalaan konkurensi Anda adalah 1.000 instance lingkungan eksekusi setiap 10 detik (atau 10.000 permintaan per detik setiap 10 detik). Dengan kata lain, setiap 10 detik, Lambda dapat mengalokasikan paling banyak 1.000 instance lingkungan eksekusi tambahan, atau mengakomodasi 10.000 permintaan tambahan per detik, ke setiap fungsi Anda.

Biasanya, Anda tidak perlu khawatir tentang batasan ini. Tingkat penskalaan Lambda cukup untuk sebagian besar kasus penggunaan.

Yang penting, tingkat penskalaan konkurensi adalah batas tingkat fungsi. Ini berarti bahwa setiap fungsi di akun Anda dapat menskalakan secara independen dari fungsi lainnya.

Untuk informasi selengkapnya tentang perilaku penskalaan, lihat [Perilaku penskalaan Lambda](#).

Mengkonfigurasi konkurensi cadangan untuk suatu fungsi

Di Lambda, [konkurensi](#) adalah jumlah permintaan dalam penerbangan yang saat ini ditangani oleh fungsi Anda. Ada dua tipe kontrol konkurensi yang tersedia:

- **Konkurensi cadangan** - Ini mewakili jumlah maksimum instans bersamaan yang dialokasikan ke fungsi Anda. Ketika fungsi sudah memiliki konkurensi terpesan, tidak ada fungsi lain yang dapat menggunakan konkurensi tersebut. Konkurensi cadangan berguna untuk memastikan bahwa fungsi Anda yang paling penting selalu memiliki konkurensi yang cukup untuk menangani permintaan yang masuk. Mengkonfigurasi konkurensi cadangan untuk suatu fungsi tidak menimbulkan biaya tambahan.
 - **Konkurensi yang disediakan** — Ini adalah jumlah lingkungan eksekusi pra-inisialisasi yang dialokasikan untuk fungsi Anda. Lingkungan eksekusi ini siap merespons segera permintaan fungsi yang masuk. Konkurensi yang disediakan berguna untuk mengurangi latensi start dingin untuk fungsi. Mengkonfigurasi konkurensi yang disediakan menimbulkan biaya tambahan untuk Anda.
- Akun AWS

Topik ini merinci cara mengelola dan mengonfigurasi konkurensi cadangan. Untuk gambaran konseptual dari dua jenis kontrol konkurensi ini, lihat Konkurensi cadangan [dan konkurensi yang disediakan](#). Untuk informasi tentang mengonfigurasi konkurensi yang disediakan, lihat [the section called “Mengonfigurasi konkurensi yang tersedia”](#)

Note

Fungsi Lambda yang ditautkan ke pemetaan sumber peristiwa Amazon MQ memiliki konkurensi maksimum default. Untuk Apache Active MQ, jumlah maksimum instans bersamaan adalah 5. Untuk Rabbit MQ, jumlah maksimum instans bersamaan adalah 1. Menyetel konkurensi cadangan atau yang disediakan untuk fungsi Anda tidak mengubah batasan ini. Untuk meminta peningkatan konkurensi maksimum default saat menggunakan Amazon MQ, hubungi [AWS Support](#)

Bagian-bagian

- [Mengonfigurasi konkurensi terpesan](#)
- [Memperkirakan secara akurat konkurensi cadangan yang diperlukan untuk suatu fungsi](#)

Mengonfigurasi konkurensi terpesan

Anda dapat mengonfigurasi pengaturan konkurensi cadangan untuk suatu fungsi menggunakan konsol Lambda atau Lambda. API

Untuk mencadangkan konkurensi untuk fungsi (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang ingin Anda pesan konkurensi.
3. Pilih Konfigurasi, lalu pilih Konkurensi.
4. Dalam Konkurensi, pilih Edit.
5. Pilih Pesan konkurensi. Masukkan jumlah konkurensi yang dipesan untuk fungsi tersebut.
6. Pilih Simpan.

Anda dapat melakukan reservasi hingga nilai konkurensi akun Unreserved dikurangi 100. 100 unit konkurensi yang tersisa adalah untuk fungsi yang tidak menggunakan konkurensi cadangan. Misalnya, jika akun Anda memiliki batas konkurensi 1.000, Anda tidak dapat memesan semua 1.000 unit konkurensi ke satu fungsi.


Edit concurrency

Concurrency

Unreserved account concurrency: 0

Use unreserved account concurrency

Reserve concurrency

 The unreserved account concurrency can't go below 100.

Cancel Save

Pemesanan konkurensi untuk suatu fungsi memengaruhi kumpulan konkurensi yang tersedia untuk fungsi lain. Misalnya, jika Anda memesan 100 unit konkurensi untuk `function-a`, fungsi lain di akun

Anda harus berbagi 900 unit konkurensi yang tersisa, bahkan jika `function-a` tidak menggunakan semua 100 unit konkurensi cadangan.

Untuk sengaja membatasi fungsi, atur konkurensi cadangannya ke 0. Ini menghentikan fungsi Anda dari memproses peristiwa apa pun hingga Anda menghapus batasnya.

Untuk mengonfigurasi konkurensi cadangan dengan API Lambda, gunakan operasi berikut. API

- [PutFunctionConcurrency](#)
- [GetFunctionConcurrency](#)
- [DeleteFunctionConcurrency](#)

Misalnya, untuk mengonfigurasi konkurensi cadangan dengan AWS Command Line Interface (CLI), gunakan `put-function-concurrency` perintah. Perintah berikut menyimpan 100 unit konkurensi untuk fungsi bernama `my-function`:

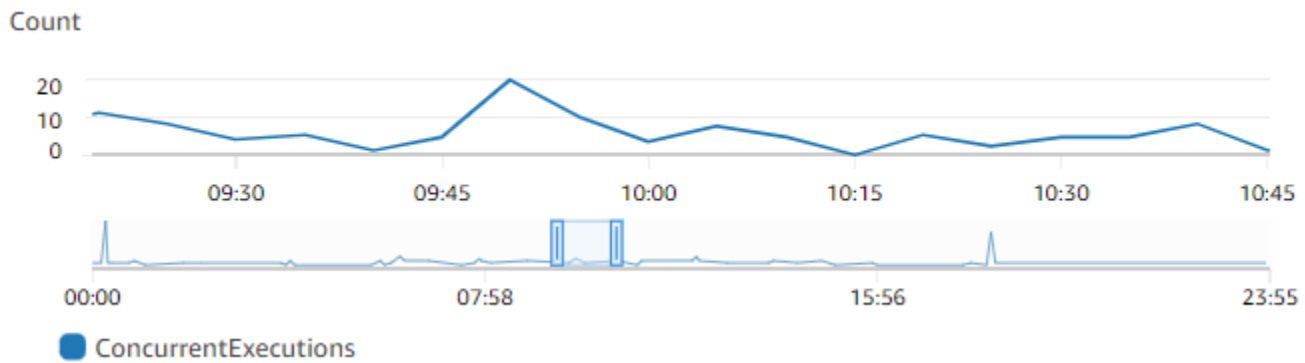
```
aws lambda put-function-concurrency --function-name my-function \  
--reserved-concurrent-executions 100
```

Anda akan melihat output yang terlihat seperti berikut:

```
{  
  "ReservedConcurrentExecutions": 100  
}
```

Memperkirakan secara akurat konkurensi cadangan yang diperlukan untuk suatu fungsi

[Jika fungsi Anda saat ini melayani lalu lintas, Anda dapat dengan mudah melihat metrik konkurensi menggunakan CloudWatch metrik.](#) Secara khusus, `ConcurrentExecutions` metrik menunjukkan jumlah pemanggilan bersamaan untuk setiap fungsi di akun Anda.



Grafik sebelumnya menunjukkan bahwa fungsi ini melayani rata-rata 5 hingga 10 permintaan bersamaan pada waktu tertentu, dan memuncak pada 20 permintaan pada hari biasa. Misalkan ada banyak fungsi lain di akun Anda. Jika fungsi ini sangat penting untuk aplikasi Anda dan Anda tidak ingin membatalkan permintaan apa pun, gunakan angka yang lebih besar dari atau sama dengan 20 sebagai pengaturan konkurensi cadangan Anda.

Atau, ingatlah bahwa Anda juga dapat [menghitung konkurensi](#) menggunakan rumus berikut:

$$\text{Concurrency} = (\text{average requests per second}) * (\text{average request duration in seconds})$$

Mengalikan permintaan rata-rata per detik dengan durasi permintaan rata-rata dalam hitungan detik memberi Anda perkiraan kasar tentang berapa banyak konkurensi yang perlu Anda pesan. Anda dapat memperkirakan permintaan rata-rata per detik menggunakan `Invocation` metrik, dan durasi permintaan rata-rata dalam detik menggunakan `Duration` metrik. Lihat [Lihat metrik untuk fungsi Lambda](#) untuk detail selengkapnya.

Anda juga harus terbiasa dengan kendala throughput hulu dan hilir Anda. Sementara fungsi Lambda berskala mulus dengan beban, dependensi hulu dan hilir mungkin tidak memiliki kemampuan throughput yang sama. Jika Anda perlu membatasi seberapa tinggi skala fungsi Anda, konfigurasi konkurensi cadangan pada fungsi Anda.

Mengkonfigurasi konkurensi yang disediakan untuk suatu fungsi

Di Lambda, [konkurensi](#) adalah jumlah permintaan dalam penerbangan yang saat ini ditangani oleh fungsi Anda. Ada dua tipe kontrol konkurensi yang tersedia:

- **Konkurensi cadangan** - Ini mewakili jumlah maksimum instans bersamaan yang dialokasikan ke fungsi Anda. Ketika fungsi sudah memiliki konkurensi terpesan, tidak ada fungsi lain yang dapat menggunakan konkurensi tersebut. Konkurensi cadangan berguna untuk memastikan bahwa fungsi Anda yang paling penting selalu memiliki konkurensi yang cukup untuk menangani permintaan yang masuk. Mengkonfigurasi konkurensi cadangan untuk suatu fungsi tidak menimbulkan biaya tambahan.
- **Konkurensi yang disediakan** — Ini adalah jumlah lingkungan eksekusi pra-inisialisasi yang dialokasikan untuk fungsi Anda. Lingkungan eksekusi ini siap merespons segera permintaan fungsi yang masuk. Konkurensi yang disediakan berguna untuk mengurangi latensi start dingin untuk fungsi. Mengkonfigurasi konkurensi yang disediakan menimbulkan biaya tambahan untuk Anda. Akun AWS

Topik ini merinci cara mengelola dan mengonfigurasi konkurensi yang disediakan. Untuk gambaran konseptual dari dua jenis kontrol konkurensi ini, lihat Konkurensi cadangan [dan konkurensi yang disediakan](#). Untuk informasi selengkapnya tentang mengonfigurasi konkurensi cadangan, lihat [the section called “Mengonfigurasi konkurensi terpesan”](#)

Note

Fungsi Lambda yang ditautkan ke pemetaan sumber peristiwa Amazon MQ memiliki konkurensi maksimum default. Untuk Apache Active MQ, jumlah maksimum instans bersamaan adalah 5. Untuk Rabbit MQ, jumlah maksimum instans bersamaan adalah 1. Menyetel konkurensi cadangan atau yang disediakan untuk fungsi Anda tidak mengubah batasan ini. Untuk meminta peningkatan konkurensi maksimum default saat menggunakan Amazon MQ, hubungi AWS Support

Bagian-bagian

- [Mengonfigurasi konkurensi yang tersedia](#)
- [Memperkirakan konkurensi yang disediakan secara akurat untuk suatu fungsi](#)
- [Mengoptimalkan kode fungsi saat menggunakan konkurensi yang disediakan](#)

- [Menggunakan variabel lingkungan untuk melihat dan mengontrol perilaku konkurensi yang disediakan](#)
- [Memahami perilaku pencatatan dan penagihan dengan konkurensi yang disediakan](#)
- [Menggunakan Application Auto Scaling untuk mengotomatiskan manajemen konkurensi yang disediakan](#)

Mengonfigurasi konkurensi yang tersedia

Anda dapat mengonfigurasi pengaturan konkurensi yang disediakan untuk suatu fungsi menggunakan konsol Lambda atau Lambda API

Untuk mengalokasikan konkurensi yang disediakan untuk fungsi (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang ingin Anda alokasikan konkurensi yang disediakan.
3. Pilih Konfigurasi, lalu pilih Konkurensi.
4. Dalam Konfigurasi konkurensi terprovisi, pilih Tambah konfigurasi.
5. Pilih jenis qualifier, dan alias atau versi.

Note

Anda tidak dapat menggunakan konkurensi yang disediakan dengan LATEST versi \$ dari fungsi apa pun.

Jika fungsi Anda memiliki sumber peristiwa, pastikan bahwa sumber peristiwa menunjuk ke alias atau versi fungsi yang benar. Jika tidak, fungsi Anda tidak akan menggunakan lingkungan konkurensi yang disediakan.


6. Masukkan nomor di bawah Konkurensi yang disediakan. Lambda memberikan perkiraan biaya bulanan.
7. Pilih Simpan.

Anda dapat mengonfigurasi hingga konkurensi akun Unreserved di akun Anda, minus 100. 100 unit konkurensi yang tersisa adalah untuk fungsi yang tidak menggunakan konkurensi cadangan. Misalnya, jika akun Anda memiliki batas konkurensi 1.000, dan Anda belum menetapkan konkurensi cadangan atau ketentuan apa pun ke fungsi lainnya, Anda dapat mengonfigurasi maksimum 900 unit konkurensi yang disediakan untuk satu fungsi.


Provisioned concurrency

To enable your function to scale without fluctuations in latency, use provisioned concurrency. You can use Application Auto Scaling to automatically adjust provisioned concurrency to maintain a configured target utilization. Provisioned concurrency runs continually and has separate pricing for concurrency and execution duration. [Learn more](#) 

\$0.00 per month in addition to pricing for duration and requests. [Pricing](#) 

 The maximum allowed provisioned concurrency is 900, based on the unreserved concurrency available (1000) minus the minimum unreserved account concurrency (100).

900 available

 Please correct the errors above.

Mengonfigurasi konkurensi yang disediakan untuk suatu fungsi berdampak pada kumpulan konkurensi yang tersedia untuk fungsi lain. Misalnya, jika Anda mengonfigurasi 100 unit konkurensi yang disediakan untuk `function-a`, fungsi lain di akun Anda harus berbagi 900 unit konkurensi yang tersisa. Ini benar bahkan jika `function-a` tidak menggunakan semua 100 unit.

Dimungkinkan untuk mengalokasikan konkurensi cadangan dan konkurensi yang disediakan untuk fungsi yang sama. Dalam kasus seperti itu, konkurensi yang disediakan tidak dapat melebihi konkurensi yang dicadangkan.

Batasan ini meluas ke versi fungsi. Konkurensi maksimum yang disediakan yang dapat Anda tetapkan ke versi fungsi tertentu adalah konkurensi cadangan fungsi dikurangi konkurensi yang disediakan pada versi fungsi lainnya.

Untuk mengonfigurasi konkurensi yang disediakan dengan LambdaAPI, gunakan operasi berikut. API

- [PutProvisionedConcurrencyConfig](#)
- [GetProvisionedConcurrencyConfig](#)
- [ListProvisionedConcurrencyConfigs](#)
- [DeleteProvisionedConcurrencyConfig](#)

Misalnya, untuk mengonfigurasi konkurensi yang disediakan dengan AWS Command Line Interface (CLI), gunakan perintah `put-provisioned-concurrency-config`. Perintah berikut mengalokasikan 100 unit konkurensi yang disediakan untuk BLUE alias fungsi bernama: `my-function`

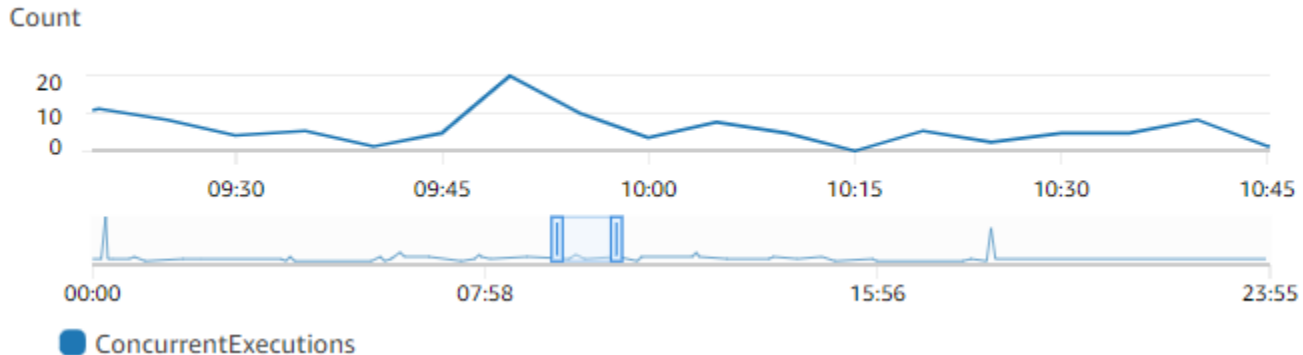

```
aws lambda put-provisioned-concurrency-config --function-name my-function \  
--qualifier BLUE \  
--provisioned-concurrent-executions 100
```

Anda akan melihat output yang terlihat seperti berikut:

```
{  
  "Requested ProvisionedConcurrentExecutions": 100,  
  "Allocated ProvisionedConcurrentExecutions": 0,  
  "Status": "IN_PROGRESS",  
  "LastModified": "2023-01-21T11:30:00+0000"  
}
```

Memperkirakan konkurensi yang disediakan secara akurat untuk suatu fungsi

[Anda dapat melihat metrik konkurensi fungsi aktif apa pun menggunakan CloudWatch metrik.](#) Secara khusus, `ConcurrentExecutions` metrik menunjukkan jumlah pemanggilan bersamaan untuk fungsi di akun Anda.



Grafik sebelumnya menunjukkan bahwa fungsi ini melayani rata-rata 5 hingga 10 permintaan bersamaan pada waktu tertentu, dan memuncak pada 20 permintaan. Misalkan ada banyak fungsi lain di akun Anda. Jika fungsi ini sangat penting untuk aplikasi Anda dan Anda memerlukan respons latensi rendah pada setiap pemanggilan, konfigurasi setidaknya 20 unit konkurensi yang disediakan.

Ingatlah bahwa Anda juga dapat [menghitung konkurensi](#) menggunakan rumus berikut:

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

Untuk memperkirakan berapa banyak konkurensi yang Anda butuhkan, kalikan permintaan rata-rata per detik dengan durasi permintaan rata-rata dalam hitungan detik. Anda dapat memperkirakan permintaan rata-rata per detik menggunakan `Invocation` metrik, dan durasi permintaan rata-rata dalam detik menggunakan `Duration` metrik.

Saat mengonfigurasi konkurensi yang disediakan, Lambda menyarankan untuk menambahkan buffer 10% di atas jumlah konkurensi yang biasanya dibutuhkan fungsi Anda. Misalnya, jika fungsi Anda biasanya memuncak pada 200 permintaan bersamaan, setel konkurensi yang disediakan ke 220 (200 permintaan bersamaan + 10% = 220 konkurensi yang disediakan).

Mengoptimalkan kode fungsi saat menggunakan konkurensi yang disediakan

Jika Anda menggunakan konkurensi yang disediakan, pertimbangkan untuk merestrukturisasi kode fungsi Anda untuk mengoptimalkan latensi rendah. Untuk fungsi yang menggunakan konkurensi yang disediakan, Lambda menjalankan kode inisialisasi apa pun, seperti memuat pustaka dan membuat instance klien, selama waktu alokasi. Oleh karena itu, disarankan untuk memindahkan sebanyak mungkin inisialisasi di luar penanganan fungsi utama untuk menghindari dampak latensi selama pemanggilan fungsi aktual. Sebaliknya, menginisialisasi pustaka atau membuat instance klien dalam kode pengendali utama Anda berarti fungsi Anda harus menjalankan ini setiap kali dipanggil (ini terjadi terlepas dari apakah Anda menggunakan konkurensi yang disediakan).

Untuk pemanggilan sesuai permintaan, Lambda mungkin perlu menjalankan ulang kode inisialisasi Anda setiap kali fungsi Anda mengalami awal yang dingin. Untuk fungsi tersebut, Anda dapat memilih untuk menunda inisialisasi kemampuan tertentu sampai fungsi Anda membutuhkannya. Misalnya, pertimbangkan alur kontrol berikut untuk handler Lambda:

```
def handler(event, context):
    ...
    if ( some_condition ):
        // Initialize CLIENT_A to perform a task
    else:
        // Do nothing
```

Pada contoh sebelumnya, alih-alih menginisialisasi `CLIENT_A` di luar handler utama, pengembang menginisiasiasinya dalam pernyataan `if`. Dengan melakukan ini, Lambda menjalankan kode ini hanya jika `some_condition` terpenuhi. Jika Anda menginisialisasi `CLIENT_A` di luar penanganan utama, Lambda menjalankan kode itu di setiap awal yang dingin. Ini dapat meningkatkan latensi keseluruhan.

Menggunakan variabel lingkungan untuk melihat dan mengontrol perilaku konkurensi yang disediakan

Dimungkinkan bagi fungsi Anda untuk menggunakan semua konkurensi yang disediakan. Lambda menggunakan instans sesuai permintaan untuk menangani kelebihan lalu lintas. Untuk menentukan jenis inisialisasi Lambda yang digunakan untuk lingkungan tertentu, periksa nilai variabel lingkungan. `AWS_LAMBDA_INITIALIZATION_TYPE` Variabel ini memiliki dua nilai yang mungkin: `provisioned-concurrency` atau `on-demand`. Nilai `AWS_LAMBDA_INITIALIZATION_TYPE` tidak dapat diubah dan tetap konstan sepanjang masa hidup lingkungan. Untuk memeriksa nilai variabel lingkungan dalam kode fungsi Anda, lihat [???](#).

Jika Anda menggunakan .NET6 atau .NET7 runtime, Anda dapat mengonfigurasi variabel `AWS_LAMBDA_DOTNET_PREJIT` lingkungan untuk meningkatkan latensi fungsi, bahkan jika mereka tidak menggunakan konkurensi yang disediakan. Itu. NETruntime menggunakan kompilasi dan inisialisasi malas untuk setiap pustaka yang dipanggil kode Anda untuk pertama kalinya. Akibatnya, pemanggilan pertama fungsi Lambda mungkin memakan waktu lebih lama dari yang berikutnya. Untuk mengurangi ini, Anda dapat memilih salah satu dari tiga nilai untuk `AWS_LAMBDA_DOTNET_PREJIT`

- `ProvisionedConcurrency`: Lambda melakukan ahead-of-time JIT kompilasi untuk semua lingkungan menggunakan konkurensi yang disediakan. Ini adalah nilai default.
- `Always`: Lambda melakukan ahead-of-time JIT kompilasi untuk setiap lingkungan, meskipun fungsinya tidak menggunakan konkurensi yang disediakan.
- `Never`: Lambda menonaktifkan ahead-of-time JIT kompilasi untuk semua lingkungan.

Memahami perilaku pencatatan dan penagihan dengan konkurensi yang disediakan

Untuk lingkungan konkurensi yang disediakan, kode inisialisasi fungsi Anda berjalan selama alokasi, dan secara berkala saat Lambda mendaur ulang instance lingkungan Anda. Anda dapat melihat waktu inisialisasi di log dan [jejak](#) setelah instance lingkungan memproses permintaan. Penting untuk dicatat bahwa Lambda menagih Anda untuk inisialisasi meskipun instance lingkungan tidak pernah memproses permintaan. Konkurensi yang disediakan berjalan terus menerus dan menimbulkan penagihan terpisah dari biaya inisialisasi dan pemanggilan. Untuk detail selengkapnya, lihat [AWS Lambda Harga](#).

Selain itu, saat Anda mengonfigurasi fungsi Lambda dengan konkurensi yang disediakan, Lambda melakukan pra-inisialisasi lingkungan eksekusi tersebut sehingga tersedia sebelum permintaan pemanggilan fungsi. Namun, fungsi Anda menerbitkan log pemanggilan CloudWatch hanya ketika fungsi tersebut benar-benar dipanggil. Oleh karena itu, [bidang Init Duration](#) muncul di baris REPORT log dari pemanggilan fungsi pertama, meskipun inisialisasi terjadi sebelumnya. Ini tidak berarti fungsi mengalami awal yang dingin.

Menggunakan Application Auto Scaling untuk mengotomatiskan manajemen konkurensi yang disediakan

Anda dapat menggunakan Application Auto Scaling untuk mengelola konkurensi yang disediakan sesuai jadwal atau berdasarkan pemanfaatan. Jika fungsi Anda menerima pola lalu lintas yang dapat diprediksi, gunakan penskalaan terjadwal. Jika Anda ingin fungsi Anda mempertahankan persentase pemanfaatan tertentu, gunakan kebijakan penskalaan pelacakan target.

Penskalaan terjadwal

Dengan Application Auto Scaling, Anda dapat mengatur jadwal penskalaan Anda sendiri sesuai dengan perubahan beban yang dapat diprediksi. Untuk informasi dan contoh selengkapnya, lihat [Penskalaan terjadwal untuk Application Auto Scaling](#) di Panduan Pengguna Application Auto Scaling, [AWS Lambda dan Scheduling Provisioned Concurrency](#) untuk penggunaan puncak berulang di Blog Komputasi. AWS

Pelacakan target

Dengan pelacakan target, Application Auto Scaling membuat dan mengelola serangkaian CloudWatch alarm berdasarkan cara Anda menentukan kebijakan penskalaan Anda. Ketika alarm ini diaktifkan, Application Auto Scaling secara otomatis menyesuaikan jumlah lingkungan yang dialokasikan menggunakan konkurensi yang disediakan. Gunakan pelacakan target untuk aplikasi yang tidak memiliki pola lalu lintas yang dapat diprediksi.

Untuk menskalakan konkurensi yang disediakan menggunakan pelacakan target, gunakan operasi Application Auto PutScalingPolicy Scaling RegisterScalableTarget dan Application. API Misalnya, jika Anda menggunakan AWS Command Line Interface (CLI), ikuti langkah-langkah berikut:

1. Daftarkan alias fungsi sebagai target penskalaan. Contoh berikut mendaftarkan BLUE alias fungsi bernama: `my-function`

```
aws application-autoscaling register-scalable-target --service-namespace lambda \
```

```
--resource-id function:my-function:BLUE --min-capacity 1 --max-capacity 100 \
--scalable-dimension lambda:function:ProvisionedConcurrency
```

2. Terapkan kebijakan penskalaan ke target. Contoh berikut mengonfigurasi Application Auto Scaling untuk menyesuaikan konfigurasi konkurensi yang disediakan untuk alias agar pemanfaatan tetap mendekati 70 persen, tetapi Anda dapat menerapkan nilai apa pun antara 10% dan 90%.

```
aws application-autoscaling put-scaling-policy \
  --service-namespace lambda \
  --scalable-dimension lambda:function:ProvisionedConcurrency \
  --resource-id function:my-function:BLUE \
  --policy-name my-policy \
  --policy-type TargetTrackingScaling \
  --target-tracking-scaling-policy-configuration '{ "TargetValue":
0.7, "PredefinedMetricSpecification": { "PredefinedMetricType":
"LambdaProvisionedConcurrencyUtilization" } }'
```

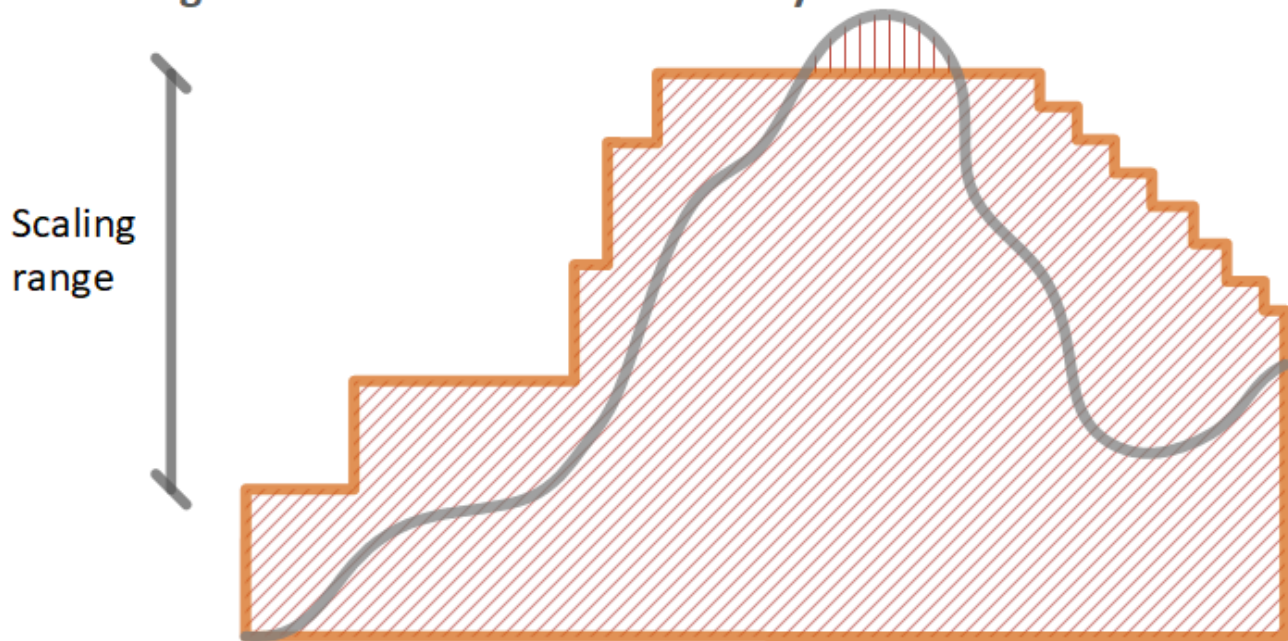
Anda akan melihat output seperti ini:

```
{
  "PolicyARN": "arn:aws:autoscaling:us-
east-2:123456789012:scalingPolicy:12266dbb-1524-xmpl-a64e-9a0a34b996fa:resource/lambda/
function:my-function:BLUE:policyName/my-policy",
  "Alarms": [
    {
      "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7",
      "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7"
    },
    {
      "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66",
      "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66"
    }
  ]
}
```





Application Auto Scaling membuat dua alarm masuk. CloudWatch Alarm pertama terpicu ketika pemanfaatan konkurensi yang disediakan secara konsisten melebihi 70%. Jika hal ini terjadi, Application Auto Scaling mengalokasikan lebih banyak konkurensi terprovisi untuk mengurangi penggunaan. Alarm kedua terpicu ketika pemanfaatan secara konsisten kurang dari 63% (90 persen dari target 70%). Jika hal ini terjadi, Application Auto Scaling mengurangi konkurensi terprovisi alias.

Dalam contoh berikut, fungsi menskalakan antara jumlah konkurensi terprovisi minimum dan maksimum berdasarkan penggunaan.

Autoscaling with Provisioned Concurrency



Legenda

-  Instans fungsi
-  Permintaan terbuka
-  Konkurensi terprovisi
-  Konkurensi standar

Ketika jumlah permintaan terbuka meningkat, Application Auto Scaling meningkatkan konkurensi yang disediakan dalam langkah-langkah besar hingga mencapai maksimum yang dikonfigurasi. Setelah ini, fungsi dapat terus menskalakan pada konkurensi standar tanpa syarat jika Anda belum mencapai batas konkurensi akun Anda. Saat pemanfaatan turun dan tetap rendah, Application Auto Scaling mengurangi konkurensi yang disediakan dalam langkah-langkah periodik yang lebih kecil.

Kedua alarm Application Auto Scaling menggunakan statistik rata-rata secara default. Fungsi yang mengalami semburan lalu lintas cepat mungkin tidak memicu alarm ini. Misalnya, misalkan fungsi Lambda Anda dijalankan dengan cepat (yaitu 20-100 ms) dan lalu lintas Anda datang dalam ledakan cepat. Dalam hal ini, jumlah permintaan melebihi konkurensi yang disediakan yang dialokasikan selama burst. Namun, Application Auto Scaling membutuhkan beban burst untuk bertahan setidaknya selama 3 menit untuk menyediakan lingkungan tambahan. Selain itu, kedua CloudWatch alarm memerlukan 3 titik data yang mencapai rata-rata target untuk mengaktifkan kebijakan penskalaan otomatis. Jika fungsi Anda mengalami ledakan lalu lintas yang cepat, menggunakan statistik Maksimum alih-alih statistik Rata-rata dapat lebih efektif dalam menskalakan konkurensi yang disediakan untuk meminimalkan start dingin.

Untuk informasi selengkapnya tentang kebijakan penskalaan pelacakan target, lihat [Kebijakan penskalaan pelacakan target untuk Application Auto Scaling](#).

Perilaku penskalaan Lambda

Saat fungsi Anda menerima lebih banyak permintaan, Lambda secara otomatis meningkatkan jumlah lingkungan eksekusi untuk menangani permintaan ini hingga akun Anda mencapai kuota konkurensinya. Namun, untuk melindungi dari penskalaan berlebih sebagai respons terhadap ledakan lalu lintas yang tiba-tiba, Lambda membatasi seberapa cepat fungsi Anda dapat menskalakan. Tingkat penskalaan konkurensi ini adalah tingkat maksimum di mana fungsi di akun Anda dapat menskalakan sebagai respons terhadap peningkatan permintaan. (Artinya, seberapa cepat Lambda dapat membuat lingkungan eksekusi baru.) Tingkat penskalaan konkurensi berbeda dari batas konkurensi tingkat akun, yang merupakan jumlah total konkurensi yang tersedia untuk fungsi Anda.

Tingkat penskalaan konkurensi

Di masing-masing Wilayah AWS, dan untuk setiap fungsi, tingkat penskalaan konkurensi Anda adalah 1.000 instance lingkungan eksekusi setiap 10 detik (atau 10.000 permintaan per detik setiap 10 detik). Dengan kata lain, setiap 10 detik, Lambda dapat mengalokasikan paling banyak 1.000 instance lingkungan eksekusi tambahan, atau mengakomodasi 10.000 permintaan tambahan per detik, ke setiap fungsi Anda.

Biasanya, Anda tidak perlu khawatir tentang batasan ini. Tingkat penskalaan Lambda cukup untuk sebagian besar kasus penggunaan.

Yang penting, tingkat penskalaan konkurensi adalah batas tingkat fungsi. Ini berarti bahwa setiap fungsi di akun Anda dapat menskalakan secara independen dari fungsi lainnya.

Note

Dalam praktiknya, Lambda melakukan upaya terbaik untuk mengisi ulang tingkat penskalaan konkurensi Anda secara terus menerus dari waktu ke waktu, bukan dalam satu isi ulang 1.000 unit setiap 10 detik.

Lambda tidak memperoleh bagian yang tidak terpakai dari tingkat penskalaan konkurensi Anda. Ini berarti bahwa setiap saat, tingkat penskalaan Anda selalu maksimum 1.000 unit konkurensi. Misalnya, jika Anda tidak menggunakan 1.000 unit konkurensi yang tersedia dalam interval 10 detik, Anda tidak akan memperoleh 1.000 unit tambahan dalam interval 10 detik berikutnya. Tingkat penskalaan konkurensi Anda masih 1.000 dalam interval 10 detik berikutnya.

Selama fungsi Anda terus menerima peningkatan jumlah permintaan, maka Lambda menskalakan pada tingkat tercepat yang tersedia untuk Anda, hingga batas konkurensi akun Anda. Anda dapat membatasi jumlah konkurensi yang dapat digunakan oleh masing-masing fungsi dengan [mengonfigurasi konkurensi cadangan](#). Jika permintaan masuk lebih cepat dari skala fungsi Anda, atau jika fungsi Anda berada pada konkurensi maksimum, maka permintaan tambahan gagal dengan kesalahan pelambatan (429 kode status).

Memantau konkurensi

Lambda memancarkan metrik CloudWatch Amazon untuk membantu Anda memantau konkurensi fungsi Anda. Topik ini menjelaskan metrik ini dan cara menafsirkannya.

Bagian-bagian

- [Metrik konkurensi umum](#)
- [Metrik konkurensi terprovisi](#)
- [Bekerja dengan ClaimedAccountConcurrency metrik](#)

Metrik konkurensi umum

Gunakan metrik berikut untuk memantau konkurensi fungsi Lambda Anda. Granularitas untuk setiap metrik adalah 1 menit.

- **ConcurrentExecutions**— Jumlah pemanggilan bersamaan aktif pada titik waktu tertentu. Lambda memancarkan metrik ini untuk semua fungsi, versi, dan alias. Untuk fungsi apa pun di konsol Lambda, Lambda menampilkan grafik **ConcurrentExecutions** secara native di tab Pemantauan, di bawah Metrik. Lihat metrik ini menggunakan MAX.
- **UnreservedConcurrentExecutions**— Jumlah pemanggilan bersamaan aktif yang menggunakan konkurensi tanpa syarat. Lambda memancarkan metrik ini di semua fungsi di suatu wilayah. Lihat metrik ini menggunakan MAX.
- **ClaimedAccountConcurrency**— Jumlah konkurensi yang tidak tersedia untuk pemanggilan sesuai permintaan. **ClaimedAccountConcurrency** sama dengan **UnreservedConcurrentExecutions** ditambah jumlah konkurensi yang dialokasikan (yaitu total konkurensi cadangan ditambah total konkurensi yang disediakan). Jika **ClaimedAccountConcurrency** melebihi batas konkurensi akun Anda, Anda dapat [meminta batas konkurensi akun yang lebih tinggi](#). Lihat metrik ini menggunakan MAX. Untuk informasi selengkapnya, lihat [Bekerja dengan ClaimedAccountConcurrency metrik](#).

Metrik konkurensi terprovisi

Gunakan metrik berikut untuk memantau fungsi Lambda menggunakan konkurensi yang disediakan. Granularitas untuk setiap metrik adalah 1 menit.

- **ProvisionedConcurrentExecutions**— Jumlah instance lingkungan eksekusi yang secara aktif memproses pemanggilan pada konkurensi yang disediakan. Lambda memancarkan metrik ini untuk setiap versi fungsi dan alias dengan konkurensi yang disediakan yang dikonfigurasi. Lihat metrik ini menggunakan MAX.

ProvisionedConcurrentExecution tidak sama dengan jumlah total konkurensi yang disediakan yang Anda alokasikan. Misalnya, Anda mengalokasikan 100 unit konkurensi yang disediakan ke versi fungsi. Selama menit tertentu, jika paling banyak 50 dari 100 lingkungan eksekusi tersebut menangani pemanggilan secara bersamaan, maka nilai **MAX(ProvisionedConcurrentExecutions)** adalah 50.

- **ProvisionedConcurrentInvocations**— Berapa kali Lambda memanggil kode fungsi Anda menggunakan konkurensi yang disediakan. Lambda memancarkan metrik ini untuk setiap versi fungsi dan alias dengan konkurensi yang disediakan yang dikonfigurasi. Lihat metrik ini menggunakan SUM.

ProvisionedConcurrentInvocations berbeda dari **ProvisionedConcurrentExecutions** yang **ProvisionedConcurrentInvocations** menghitung jumlah total pemanggilan, sementara **ProvisionedConcurrentExecutions** menghitung jumlah lingkungan aktif. Untuk memahami perbedaan ini, pertimbangkan skenario berikut:



Dalam contoh ini, misalkan Anda menerima 1 doa per menit, dan setiap pemanggilan membutuhkan waktu 2 menit untuk menyelesaikannya. Setiap bar horisontal oranye mewakili satu permintaan. Misalkan Anda mengalokasikan 10 unit konkurensi yang disediakan untuk fungsi ini, sehingga setiap permintaan berjalan pada konkurensi yang disediakan.

Di antara menit 0 dan 1, Request 1 masuk. Pada menit 1, nilai untuk `MAX(ProvisionedConcurrentExecutions)` adalah 1, karena paling banyak 1 lingkungan eksekusi aktif selama beberapa menit terakhir. Nilai untuk `SUM(ProvisionedConcurrentInvocations)` juga 1, karena 1 permintaan baru masuk selama beberapa menit terakhir.

Di antara menit 1 dan 2, Request 2 masuk, dan Request 1 terus berjalan. Pada menit 2, nilai untuk `MAX(ProvisionedConcurrentExecutions)` adalah 2, karena paling banyak 2 lingkungan eksekusi aktif selama beberapa menit terakhir. Namun, nilai untuk `SUM(ProvisionedConcurrentInvocations)` adalah 1, karena hanya 1 permintaan baru yang masuk selama beberapa menit terakhir. Perilaku metrik ini berlanjut hingga akhir contoh.

- `ProvisionedConcurrencySpilloverInvocations`— Berapa kali Lambda memanggil fungsi Anda pada konkurensi standar (reserved atau unreserved) saat semua konkurensi yang disediakan sedang digunakan. Lambda memancarkan metrik ini untuk setiap versi fungsi dan alias dengan konkurensi yang disediakan yang dikonfigurasi. Lihat metrik ini menggunakan `SUM`. Nilai `ProvisionedConcurrentInvocations` + `ProvisionedConcurrencySpilloverInvocations` harus sama dengan jumlah total pemanggilan fungsi (yaitu `Invocations` metrik).

`ProvisionedConcurrencyUtilization`— Persentase konkurensi yang disediakan yang digunakan (yaitu nilai `ProvisionedConcurrentExecutions` dibagi dengan jumlah total konkurensi yang disediakan yang dialokasikan). Lambda memancarkan metrik ini untuk setiap versi fungsi dan alias dengan konkurensi yang disediakan yang dikonfigurasi. Lihat metrik ini menggunakan `MAX`.

Misalnya, Anda menyediakan 100 unit konkurensi yang disediakan ke versi fungsi. Selama menit tertentu, jika paling banyak 60 dari 100 lingkungan eksekusi tersebut menangani pemanggilan secara bersamaan, maka nilai `MAX(ProvisionedConcurrentExecutions)` adalah 60, dan nilai `MAX(ProvisionedConcurrentUtilization)` adalah 0,6.

Nilai tinggi untuk `ProvisionedConcurrencySpilloverInvocations` mungkin menunjukkan bahwa Anda perlu mengalokasikan konkurensi tambahan yang disediakan untuk fungsi Anda. Atau, Anda dapat [mengonfigurasi Application Auto Scaling untuk menangani penskalaan otomatis konkurensi yang disediakan berdasarkan ambang batas yang telah ditentukan sebelumnya](#).

Sebaliknya, nilai rendah secara konsisten untuk `ProvisionedConcurrencyUtilization` dapat menunjukkan bahwa Anda mengalokasikan konkurensi yang disediakan secara berlebihan untuk fungsi Anda.

Bekerja dengan **ClaimedAccountConcurrency** metrik

Lambda menggunakan `ClaimedAccountConcurrency` metrik untuk menentukan berapa banyak konkurensi akun Anda tersedia untuk pemanggilan sesuai permintaan. Lambda menghitung `ClaimedAccountConcurrency` menggunakan rumus berikut:

$$\text{ClaimedAccountConcurrency} = \text{UnreservedConcurrentExecutions} + (\text{allocated concurrency})$$

`UnreservedConcurrentExecutions` adalah jumlah pemanggilan bersamaan aktif yang menggunakan konkurensi tanpa syarat. Konkurensi yang dialokasikan adalah jumlah dari dua bagian berikut (diganti sebagai “konkurensi cadangan” dan RC PC sebagai “konkurensi yang disediakan”):

- Total RC di semua fungsi di suatu Wilayah.
- Total PC di semua fungsi di Wilayah yang menggunakan PC, tidak termasuk fungsi yang digunakan RC.

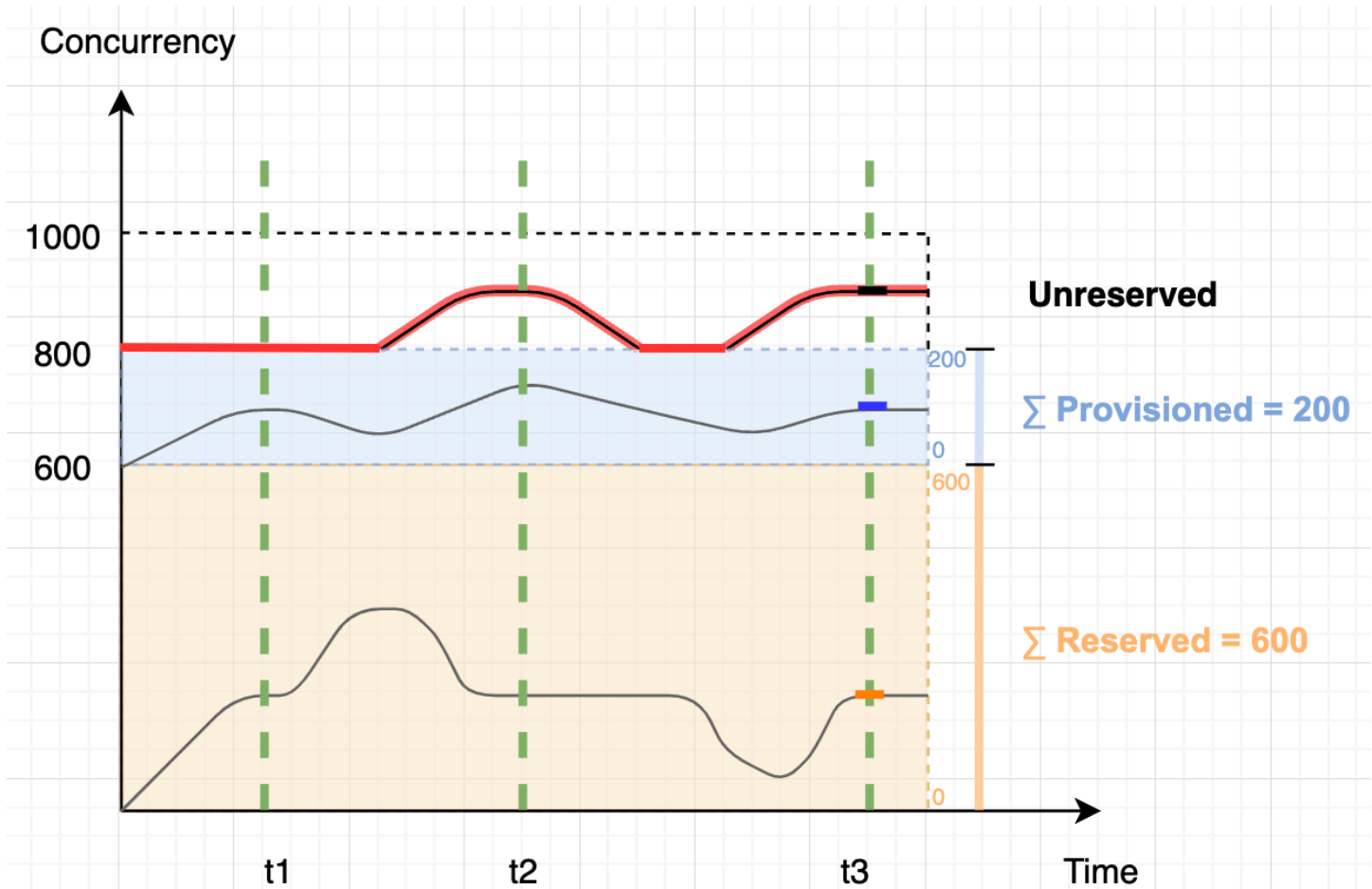
Note

Anda tidak dapat mengalokasikan PC lebih dari RC untuk suatu fungsi. Dengan demikian, fungsi selalu RC lebih besar dari atau sama dengan fungsinya PC. Untuk menghitung kontribusi konkurensi yang dialokasikan untuk fungsi-fungsi tersebut dengan keduanya PC dan, RC Lambda hanya mempertimbangkan RC, yang merupakan maksimum dari keduanya.

Lambda menggunakan `ClaimedAccountConcurrency` metrik, bukan `ConcurrentExecutions`, untuk menentukan berapa banyak konkurensi yang tersedia untuk pemanggilan sesuai permintaan. Meskipun `ConcurrentExecutions` metrik berguna untuk melacak jumlah pemanggilan bersamaan yang aktif, metrik tidak selalu mencerminkan ketersediaan konkurensi Anda yang sebenarnya. Ini karena Lambda juga mempertimbangkan konkurensi cadangan dan konkurensi yang disediakan untuk menentukan ketersediaan.

Sebagai ilustrasi `ClaimedAccountConcurrency`, pertimbangkan skenario di mana Anda mengonfigurasi banyak konkurensi cadangan dan konkurensi yang disediakan di seluruh fungsi Anda

yang sebagian besar tidak digunakan. Dalam contoh berikut, asumsikan bahwa batas konkurensi akun Anda adalah 1.000, dan Anda memiliki dua fungsi utama di akun Anda: `function-orange` dan `function-blue`. Anda mengalokasikan 600 unit konkurensi cadangan untuk `function-orange` dan mengalokasikan 200 unit konkurensi yang disediakan untuk `function-blue`. Misalkan seiring waktu, Anda menerapkan fungsi tambahan dan mengamati pola lalu lintas berikut:



Pada diagram sebelumnya, garis hitam menunjukkan penggunaan konkurensi aktual dari waktu ke waktu, dan garis merah menunjukkan nilai dari waktu `ClaimedAccountConcurrency` ke waktu. Sepanjang skenario `ClaimedAccountConcurrency` ini, minimal 800, meskipun pemanfaatan konkurensi aktual rendah di seluruh fungsi Anda. Ini karena Anda mengalokasikan total 800 unit konkurensi untuk `function-orange` dan `function-blue`. Dari perspektif Lambda, Anda telah “mengklaim” konkurensi ini untuk digunakan, sehingga Anda secara efektif hanya memiliki 200 unit konkurensi yang tersisa untuk fungsi lain.

Untuk skenario ini, konkurensi yang dialokasikan adalah 800 dalam rumus. `ClaimedAccountConcurrency` Kita kemudian dapat memperoleh nilai `ClaimedAccountConcurrency` pada berbagai titik dalam diagram:

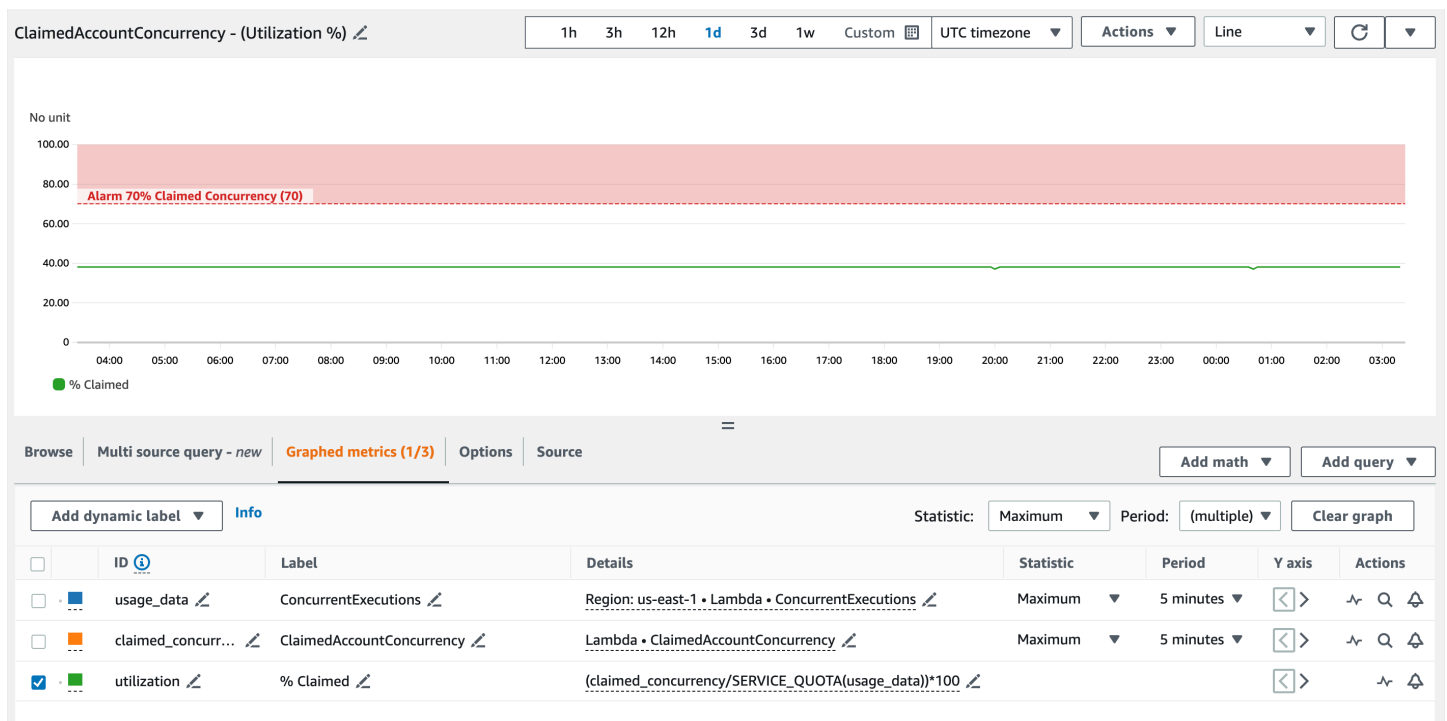
- Padat1, ClaimedAccountConcurrency adalah 800 (800 + 0UnreservedConcurrentExecutions).
- Padat2, ClaimedAccountConcurrency adalah 900 (800 + 100UnreservedConcurrentExecutions).
- Padat3, ClaimedAccountConcurrency lagi 900 (800 + 100UnreservedConcurrentExecutions).

Menyiapkan **ClaimedAccountConcurrency** metrik di CloudWatch

Lambda memancarkan metrik di. ClaimedAccountConcurrency CloudWatch Gunakan metrik ini bersama dengan nilai SERVICE_QUOTA(ConcurrentExecutions) untuk mendapatkan persentase pemanfaatan konkurensi di akun Anda, seperti yang ditunjukkan dalam rumus berikut:

$$\text{Utilization} = (\text{ClaimedAccountConcurrency} / \text{SERVICE_QUOTA}(\text{ConcurrentExecutions})) * 100\%$$

Screenshot berikut menggambarkan bagaimana Anda dapat membuat grafik rumus ini. CloudWatch `claim_utilization` Garis hijau mewakili pemanfaatan konkurensi dalam akun ini, yaitu sekitar 40%:



Tangkapan layar sebelumnya juga menyertakan CloudWatch alarm yang masuk ke ALARM status ketika pemanfaatan konkurensi melebihi 70%. Anda dapat menggunakan

`ClaimedAccountConcurrency` metrik bersama dengan alarm serupa untuk secara proaktif menentukan kapan Anda mungkin perlu meminta batas konkurensi akun yang lebih tinggi.

Membangun fungsi Lambda dengan Node.js

Anda dapat menjalankan JavaScript kode dengan Node.js di AWS Lambda. Lambda menyediakan [runtime](#) untuk Node.js yang menjalankan kode Anda untuk memproses peristiwa. Kode Anda berjalan di lingkungan yang menyertakan AWS SDK for JavaScript, dengan kredensial dari peran AWS Identity and Access Management (IAM) yang Anda kelola. Untuk mempelajari lebih lanjut tentang SDK versi yang disertakan dengan runtime Node.js, lihat [the section called “Versi termasuk runtime SDK”](#).

Lambda mendukung runtime Node.js berikut.

Node.js

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|------------|------------------|-------------------|---------------------|------------------|-----------------------|
| Node.js 20 | nodejs20.x | Amazon Linux 2023 | | | |
| Node.js 18 | nodejs18.x | Amazon Linux 2 | | | |

Note

Node.js 18 dan runtime yang lebih baru digunakan AWS SDK untuk JavaScript v3. Untuk memigrasikan fungsi dari runtime sebelumnya, ikuti [lokakarya migrasi](#) di GitHub Untuk informasi lebih lanjut tentang AWS SDK untuk JavaScript versi 3, lihat [Modular AWS SDK untuk JavaScript posting blog yang sekarang tersedia secara umum](#).

Untuk membuat fungsi Node.js

1. Buka [Konsol Lambda](#).
2. Pilih Buat fungsi.
3. Konfigurasi pengaturan berikut:
 - Nama fungsi: Masukkan nama untuk fungsi tersebut.
 - Runtime: Pilih Node.js 20.x.

4. Pilih Buat fungsi.
5. Untuk mengonfigurasi peristiwa uji, pilih Uji.
6. Untuk Nama peristiwa, masukkan **test**.
7. Pilih Simpan perubahan.
8. Untuk mengaktifkan fungsi, pilih Uji.

Konsol membuat fungsi Lambda dengan satu file sumber bernama `index.js` atau `index.mjs`. Anda dapat mengedit file ini dan menambahkan lebih banyak file di editor kode bawaan. Untuk menyimpan perubahan Anda, pilih Simpan. Selanjutnya, untuk menjalankan kode, pilih Uji.

`index.mjs`File `index.js` or mengekspor fungsi bernama `handler` yang mengambil objek acara dan objek konteks. Ini adalah [fungsi handler](#) yang dipanggil Lambda saat fungsi tersebut dipanggil. Waktu habis fungsi Node.js mendapatkan peristiwa invokasi dari Lambda dan meneruskannya ke handler. Dalam konfigurasi fungsi, nilai handler adalah `index.handler`.

Saat Anda menyimpan kode fungsi, konsol Lambda membuat paket penyebaran arsip file.zip. Saat Anda mengembangkan kode fungsi di luar konsol (menggunakan IDE), Anda perlu [membuat paket penerapan](#) untuk mengunggah kode Anda ke fungsi Lambda.

Runtime fungsi meneruskan objek konteks ke handler, selain peristiwa invokasi. [Objek konteks](#) berisi informasi tambahan tentang lingkungan invokasi, fungsi, dan eksekusi. Informasi selengkapnya tersedia dari variabel lingkungan.

Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log. Fungsi runtime mengirimkan detail tentang setiap pemanggilan ke Log. CloudWatch Detail tersebut menyampaikan [log yang dihasilkan fungsi Anda](#) selama invokasi. Jika fungsi mengembalikan kesalahan, Lambda memformat kesalahan dan mengembalikannya ke pemanggil.

Topik

- [Inisialisasi Node.js](#)
- [Versi termasuk runtime SDK](#)
- [Menggunakan keep-alive untuk koneksi TCP](#)
- [Pemuatan sertifikat CA](#)
- [Tentukan penanganan fungsi Lambda di Node.js](#)
- [Deploy fungsi Lambda Node.js dengan arsip file .zip](#)
- [Deploy fungsi Lambda Node.js dengan gambar kontainer](#)

- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Node.js](#)
- [Log dan pantau fungsi Node.js Lambda](#)
- [Menginstrumentasi kode Node.js di AWS Lambda](#)

Inisialisasi Node.js

Node.js memiliki model loop peristiwa unik yang menyebabkan perilaku inisialisasi berbeda dari runtime lainnya. Secara khusus, Node.js menggunakan model I/O non-pemblokiran yang mendukung operasi asinkron. Model ini memungkinkan Node.js bekerja secara efisien untuk sebagian besar beban kerja. Misalnya, jika fungsi Node.js membuat panggilan jaringan, permintaan tersebut dapat ditetapkan sebagai operasi asinkron dan ditempatkan ke dalam antrian panggilan balik. Fungsi ini dapat terus memproses operasi lain dalam tumpukan panggilan utama tanpa diblokir dengan menunggu panggilan jaringan kembali. Setelah panggilan jaringan selesai, callback dijalankan dan kemudian dihapus dari antrian callback.

Beberapa tugas inisialisasi dapat berjalan secara asinkron. Tugas asinkron ini tidak dijamin untuk menyelesaikan eksekusi sebelum pemanggilan. Misalnya, kode yang membuat panggilan jaringan untuk mengambil parameter dari AWS Parameter Store mungkin tidak lengkap pada saat Lambda menjalankan fungsi handler. Akibatnya, variabel mungkin nol selama pemanggilan. Untuk menghindari hal ini, pastikan bahwa variabel dan kode asinkron lainnya sepenuhnya diinisialisasi sebelum melanjutkan dengan logika bisnis inti fungsi lainnya.

Atau, Anda dapat menunjuk kode fungsi Anda sebagai modul ES, memungkinkan Anda untuk menggunakan `await` di tingkat atas file, di luar lingkup penanganan fungsi Anda. [Saat Anda melakukannya `await Promise`, kode inisialisasi asinkron selesai sebelum pemanggilan handler, memaksimalkan efektivitas konkurensi yang disediakan dalam mengurangi latensi start dingin.](#) Untuk informasi selengkapnya dan contoh, lihat [Menggunakan modul ES Node.js dan menunggu tingkat atas](#). AWS Lambda

Menunjuk penanganan fungsi sebagai modul ES

Secara default, Lambda memperlakukan file dengan `.js` akhiran sebagai modul CommonJS. Secara opsional, Anda dapat menunjuk kode Anda sebagai modul ES. Anda dapat melakukan ini dengan dua cara: menentukan `type as module` dalam `package.json` file fungsi, atau dengan menggunakan ekstensi nama `.mjs` file. Pada pendekatan pertama, kode fungsi Anda memperlakukan semua `.js` file sebagai modul ES, sedangkan dalam skenario kedua, hanya file yang Anda tentukan `.mjs` adalah modul ES. Anda dapat mencampur modul ES dan modul

CommonJS dengan menamainya `.mjs` dan `.cjs` masing-masing, karena `.mjs` file selalu modul ES dan `.cjs` file selalu modul CommonJS.

Lambda mencari folder dalam variabel `NODE_PATH` lingkungan saat memuat modul ES. Anda dapat memuat AWS SDK yang disertakan dalam runtime menggunakan `import` pernyataan modul ES. Anda juga dapat memuat modul ES dari [lapisan](#).

Versi termasuk runtime SDK

Versi yang AWS SDK disertakan dalam runtime Node.js bergantung pada versi runtime dan versi Anda. Wilayah AWS Untuk menemukan versi yang SDK disertakan dalam runtime yang Anda gunakan, buat fungsi Lambda dengan kode berikut.

Note

Contoh kode yang ditunjukkan di bawah ini untuk Node.js versi 18 ke atas menggunakan format CommonJS. Jika Anda membuat fungsi di konsol Lambda, pastikan untuk mengganti nama file yang berisi kode menjadi `index.js`

Example Node.js 18 dan di atas

```
const { version } = require("@aws-sdk/client-s3/package.json");

exports.handler = async () => ({ version });
```

Ini mengembalikan respons dalam format berikut:

```
{
  "version": "3.462.0"
}
```

Menggunakan keep-alive untuk koneksi TCP

HTTPSAgen Node.jsHTTP/default membuat TCP koneksi baru untuk setiap permintaan baru. Untuk menghindari biaya membangun koneksi baru, Anda dapat menggunakan `keepAlive: true` untuk menggunakan kembali koneksi yang digunakan oleh fungsi Anda menggunakan AWS SDK for

JavaScript. Keep-alive dapat mengurangi waktu permintaan untuk fungsi Lambda yang melakukan beberapa panggilan menggunakan API SDK

Dalam AWS SDK for JavaScript 3.x, yang disertakan dalam runtime Lambda `nodejs18.x` dan yang lebih baru, keep-alive diaktifkan secara default. Untuk menonaktifkan keep-alive, lihat [Menggunakan kembali koneksi dengan keep-alive di Node.js dalam](#) for 3.x Developer Guide. AWS SDK JavaScript Untuk informasi selengkapnya tentang penggunaan keep-alive, lihat [HTTP keep-alive aktif secara default di modular AWS SDK untuk JavaScript di Blog Alat](#) Pengembang. AWS

Pemuatan sertifikat CA

Untuk versi runtime Node.js hingga Node.js 18, Lambda secara otomatis memuat sertifikat CA (otoritas sertifikat) khusus Amazon untuk memudahkan Anda membuat fungsi yang berinteraksi dengan layanan lain. AWS Misalnya, Lambda menyertakan RDS sertifikat Amazon yang diperlukan untuk memvalidasi [sertifikat identitas server](#) yang diinstal pada database Amazon Anda. RDS Perilaku ini dapat memiliki dampak kinerja selama start dingin.

Dimulai dengan Node.js 20, Lambda tidak lagi memuat sertifikat CA tambahan secara default. Runtime Node.js 20 berisi file sertifikat dengan semua sertifikat Amazon CA terletak di `/var/runtime/ca-cert.pem`. Untuk memulihkan perilaku yang sama dari Node.js 18 dan runtime sebelumnya, setel [variabel `NODE_EXTRA_CA_CERTS` lingkungan](#) ke `/var/runtime/ca-cert.pem`.

Untuk kinerja yang optimal, kami sarankan untuk menggabungkan hanya sertifikat yang Anda butuhkan dengan paket penerapan Anda dan memuatnya melalui variabel `NODE_EXTRA_CA_CERTS` lingkungan. File sertifikat harus terdiri dari satu atau lebih root tepercaya atau sertifikat CA perantara dalam PEM format. Misalnya, untuk RDS, sertakan sertifikat yang diperlukan di samping kode Anda sebagai `certificates/rds.pem`. Kemudian, muat sertifikat dengan menyetel `NODE_EXTRA_CA_CERTS` ke `/var/task/certificates/rds.pem`.

Tentukan penanganan fungsi Lambda di Node.js

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Topik

- [Dasar-dasar penanganan Node.js](#)
- [Penamaan](#)
- [Menggunakan async/await](#)
- [Menggunakan callback](#)
- [Praktik terbaik kode untuk fungsi Lambda Node.js](#)

Dasar-dasar penanganan Node.js

Contoh fungsi berikut mencatat isi dari [objek acara](#) dan mengembalikan lokasi log.

Note

Halaman ini menunjukkan contoh penanganan modul CommonJS dan ES. Untuk mempelajari tentang perbedaan antara kedua jenis handler ini, lihat [Menunjuk penanganan fungsi sebagai modul ES](#).

ES module handler

Example

```
export const handler = async (event, context) => {
  console.log("EVENT: \n" + JSON.stringify(event, null, 2));
  return context.logStreamName;
};
```

CommonJS module handler

Example

```
exports.handler = async function (event, context) {
```

```
console.log("EVENT: \n" + JSON.stringify(event, null, 2));
return context.logStreamName;
};
```

Saat Anda mengonfigurasi fungsi, nilai pengaturan handler adalah nama file dan nama metode handler yang diekspor, dipisahkan oleh titik. Default di konsol dan untuk contoh dalam panduan ini adalah `index.handler`. Hal ini menunjukkan metode handler yang diekspor dari file `index.js`.

Runtime meneruskan argumen ke metode handler. Argumen pertama adalah objek event, yang berisi informasi dari invoker. Invoker meneruskan informasi ini sebagai string yang JSON diformat - saat memanggil [Invoke](#), dan runtime mengubahnya menjadi objek. Ketika AWS layanan memanggil fungsi Anda, struktur acara [bervariasi menurut layanan](#).

Argumen kedua adalah [objek konteks](#), yang berisi informasi tentang lingkungan invokasi, fungsi, dan eksekusi. Pada contoh sebelumnya, fungsi mendapatkan nama [alur log](#) dari objek konteks dan mengembalikannya ke invoker.

Anda juga dapat menggunakan argumen callback, yang merupakan fungsi yang dapat Anda panggil di penanganan non-async untuk mengirim respons. Kami menyarankan Anda menggunakan `async/await` alih-alih callback. `Async/await` memberikan peningkatan keterbacaan, penanganan kesalahan, dan efisiensi. Untuk informasi selengkapnya tentang perbedaan antara `async/await` dan callback, lihat [Menggunakan callback](#)

Penamaan

Saat Anda mengonfigurasi fungsi, nilai pengaturan handler adalah nama file dan nama metode handler yang diekspor, dipisahkan oleh titik. Default untuk fungsi yang dibuat di konsol dan untuk contoh dalam panduan ini adalah `index.handler`. Ini menunjukkan handler metode yang diekspor dari `index.mjs` file `index.js` atau.

Jika Anda membuat fungsi di konsol menggunakan nama file atau nama pengendali fungsi yang berbeda, Anda harus mengedit nama handler default.

Untuk mengubah nama fungsi handler (konsol)

1. Buka halaman [Fungsi](#) di konsol Lambda dan pilih fungsi Anda.
2. Pilih tab Kode.
3. Gulir ke bawah ke panel pengaturan Runtime dan pilih Edit.

4. Di Handler, masukkan nama baru untuk handler fungsi Anda.
5. Pilih Simpan.

Menggunakan async/await

Jika kode Anda melakukan tugas asinkron, gunakan pola `async/await` untuk memastikan bahwa handler selesai berjalan. `Async/await` adalah cara ringkas dan mudah dibaca untuk menulis kode asinkron di Node.js, tanpa perlu panggilan balik bersarang atau janji rantai. Dengan `async/await`, Anda dapat menulis kode yang berbunyi seperti kode sinkron, sambil tetap asinkron dan tidak memblokir.

`async` Kata kunci menandai fungsi sebagai asinkron, dan `await` kata kunci menjeda eksekusi fungsi sampai a diselesaikan. `Promise`

Note

Pastikan untuk menunggu acara asinkron selesai. Jika fungsi kembali sebelum peristiwa `async` selesai, fungsi mungkin gagal atau menyebabkan perilaku tak terduga dalam aplikasi Anda. Ini bisa terjadi ketika `forEach` loop berisi peristiwa `async`. `forEachloop` mengharapkan panggilan sinkron. Untuk informasi selengkapnya, lihat [Array.prototype.forEach\(\)](#) dalam dokumentasi Mozilla.

ES module handler

Example — HTTP permintaan dengan async/await

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
  try {
    // fetch is available in Node.js 18 and later runtimes
    const res = await fetch(url);
    console.info("status", res.status);
    return res.status;
  }
  catch (e) {
    console.error(e);
    return 500;
  }
}
```



```
    }  
};
```

CommonJS module handler

Example — HTTP permintaan dengan async/await

```
const https = require("https");  
let url = "https://aws.amazon.com/";  
  
exports.handler = async function (event) {  
  let statusCode;  
  await new Promise(function (resolve, reject) {  
    https.get(url, (res) => {  
      statusCode = res.statusCode;  
      resolve(statusCode);  
    }).on("error", (e) => {  
      reject(Error(e));  
    });  
  });  
  console.log(statusCode);  
  return statusCode;  
};
```

Contoh berikutnya menggunakan async/await untuk mencantumkan bucket Amazon Simple Storage Service Anda.

Note

Sebelum menggunakan contoh ini, pastikan peran eksekusi fungsi Anda memiliki izin baca Amazon S3.

ES module handler

Example — AWS SDK v3 dengan async/await

Contoh ini menggunakan [AWS SDK for JavaScript v3](#), yang tersedia di nodejs18.x dan kemudian runtime.

```
import {S3Client, ListBucketsCommand} from '@aws-sdk/client-s3';
```

```
const s3 = new S3Client({region: 'us-east-1'});

export const handler = async(event) => {
  const data = await s3.send(new ListBucketsCommand({}));
  return data.Buckets;
};
```

CommonJS module handler

Example — AWS SDK v3 dengan async/await

Contoh ini menggunakan [AWS SDK for JavaScript v3](#), yang tersedia di `nodejs18.x` dan kemudian runtime.

```
const { S3Client, ListBucketsCommand } = require('@aws-sdk/client-s3');
const s3 = new S3Client({ region: 'us-east-1' });

exports.handler = async (event) => {
  const data = await s3.send(new ListBucketsCommand({}));
  return data.Buckets;
};
```

Menggunakan callback

Kami menyarankan Anda menggunakan [async/await](#) untuk mendeklarasikan fungsi handler alih-alih menggunakan callback. Async/await adalah pilihan yang lebih baik karena beberapa alasan:

- **Keterbacaan:** Kode async/await lebih mudah dibaca dan dipahami daripada kode panggilan balik, yang dapat dengan cepat menjadi sulit untuk diikuti dan menghasilkan neraka panggilan balik.
- **Debugging dan penanganan kesalahan:** Debugging kode berbasis callback bisa jadi sulit. Tumpukan panggilan bisa menjadi sulit untuk diikuti dan kesalahan dapat dengan mudah ditelan. Dengan async/await, Anda dapat menggunakan blok coba/tangkap untuk menangani kesalahan.
- **Efisiensi:** Callback sering memerlukan peralihan di antara bagian-bagian kode yang berbeda. Async/await dapat mengurangi jumlah sakelar konteks, menghasilkan kode yang lebih efisien.

Saat Anda menggunakan callback di handler Anda, fungsi terus dijalankan hingga [loop peristiwa](#) kosong atau fungsi habis waktu. Respons tidak dikirimkan ke invoker hingga semua tugas loop peristiwa selesai. Jika waktu fungsi habis, kesalahan akan dikembalikan. Anda

dapat mengonfigurasi runtime untuk mengirim respons segera dengan menyetel [konteks. `callbackWaitsForEmptyEventLoop`](#) untuk palsu.

Fungsi panggilan balik memiliki dua argumen: `Error` dan respons. Objek respons harus kompatibel dengan `JSON.stringify`.

Contoh fungsi berikut memeriksa URL dan mengembalikan kode status ke invoker.

ES module handler

Example — HTTP permintaan dengan panggilan balik

```
import https from "https";
let url = "https://aws.amazon.com/";

export function handler(event, context, callback) {
  https.get(url, (res) => {
    callback(null, res.statusCode);
  }).on("error", (e) => {
    callback(Error(e));
  });
}
```

CommonJS module handler

Example — HTTP permintaan dengan panggilan balik

```
const https = require("https");
let url = "https://aws.amazon.com/";

exports.handler = function (event, context, callback) {
  https.get(url, (res) => {
    callback(null, res.statusCode);
  }).on("error", (e) => {
    callback(Error(e));
  });
};
```

Dalam contoh berikutnya, respons dari Amazon S3 dikembalikan ke pemanggil segera setelah tersedia. Waktu habis pada loop peristiwa dibekukan, dan terus berjalan pada saat fungsi diaktifkan berikutnya.

Note

Sebelum menggunakan contoh ini, pastikan peran eksekusi fungsi Anda memiliki izin baca Amazon S3.

ES module handler

Example - AWS SDK v3 dengan `callbackWaitsFor EmptyEventLoop`

Contoh ini menggunakan [AWS SDK for JavaScript v3](#), yang tersedia di `nodejs18.x` dan kemudian runtime.

```
import AWS from "@aws-sdk/client-s3";
const s3 = new AWS.S3({});

export const handler = function (event, context, callback) {
  context.callbackWaitsForEmptyEventLoop = false;
  s3.listBuckets({}, callback);
  setTimeout(function () {
    console.log("Timeout complete.");
  }, 5000);
};
```

CommonJS module handler

Example - AWS SDK v3 dengan `callbackWaitsFor EmptyEventLoop`

Contoh ini menggunakan [AWS SDK for JavaScript v3](#), yang tersedia di `nodejs18.x` dan kemudian runtime.

```
const AWS = require("@aws-sdk/client-s3");
const s3 = new AWS.S3({});

exports.handler = function (event, context, callback) {
  context.callbackWaitsForEmptyEventLoop = false;
  s3.listBuckets({}, callback);
  setTimeout(function () {
    console.log("Timeout complete.");
  }, 5000);
};
```

Praktik terbaik kode untuk fungsi Lambda Node.js

Patuhi panduan dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji. Dalam Node.js, ini mungkin terlihat seperti:

```
exports.myHandler = function(event, context, callback) {
  var foo = event.foo;
  var bar = event.bar;
  var result = MyLambdaFunction (foo, bar);

  callback(null, result);
}

function MyLambdaFunction (foo, bar) {
  // MyLambdaFunction logic here
}
```

- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk runtime Node.js dan Python, ini termasuk file. AWS SDKs Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi.
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Deploy fungsi Lambda Node.js dengan arsip file .zip

Kode AWS Lambda fungsi Anda terdiri dari file.js atau .mjs yang berisi kode handler fungsi Anda, bersama dengan paket dan modul tambahan yang bergantung pada kode Anda. Untuk menyebarkan kode fungsi ini ke Lambda, Anda menggunakan paket penerapan. Paket ini dapat berupa arsip file.zip atau gambar kontainer. Untuk informasi selengkapnya tentang penggunaan gambar kontainer dengan Node.js, lihat [Menerapkan fungsi Lambda Node.js dengan gambar kontainer](#).

[Untuk membuat paket penyebaran Anda sebagai arsip file.zip, Anda dapat menggunakan utilitas arsip file.zip bawaan alat baris perintah Anda, atau utilitas file.zip lainnya seperti 7zip.](#) Contoh yang ditampilkan di bagian berikut mengasumsikan Anda menggunakan zip alat baris perintah di lingkungan Linux atau macOS. Untuk menggunakan perintah yang sama di Windows, Anda dapat [menginstal Windows Subsystem untuk Linux untuk](#) mendapatkan versi Windows terintegrasi dari Ubuntu dan Bash.

Perhatikan bahwa Lambda menggunakan izin POSIX file, jadi Anda mungkin perlu [mengatur izin untuk folder paket penyebaran](#) sebelum membuat arsip file.zip.

Topik

- [Dependensi runtime di Node.js](#)
- [Membuat paket penerapan.zip tanpa dependensi](#)
- [Membuat paket penerapan.zip dengan dependensi](#)
- [Membuat layer Node.js untuk dependensi Anda](#)
- [Jalur pencarian ketergantungan dan pustaka yang disertakan runtime](#)
- [Membuat dan memperbarui fungsi Lambda Node.js menggunakan file.zip](#)

Dependensi runtime di Node.js

Untuk fungsi Lambda yang menggunakan runtime Node.js, dependensi dapat berupa modul Node.js apa pun. Runtime Node.js mencakup sejumlah pustaka umum, serta versi. AWS SDK for JavaScript Runtime node.js16.x Lambda mencakup versi 2.x dari file. SDK Versi runtime node.js18.x dan yang lebih baru termasuk versi 3 dari versi. SDK Untuk menggunakan versi 2 dari versi SDK with runtime node.js18.x dan yang lebih baru, tambahkan SDK ke paket penyebaran file.zip Anda. Jika runtime yang Anda pilih menyertakan versi yang SDK Anda gunakan, Anda tidak perlu menyertakan SDK pustaka dalam file.zip Anda. Untuk mengetahui versi mana yang SDK disertakan dalam runtime yang Anda gunakan, lihat [the section called “Versi termasuk runtime SDK”](#).

Lambda memperbarui SDK pustaka secara berkala di runtime Node.js untuk menyertakan fitur terbaru dan peningkatan keamanan. Lambda juga menerapkan patch keamanan dan pembaruan ke pustaka lain yang termasuk dalam runtime. Untuk memiliki kontrol penuh atas dependensi dalam paket Anda, Anda dapat menambahkan versi pilihan Anda dari setiap dependensi yang disertakan runtime ke paket penerapan Anda. Misalnya, jika Anda ingin menggunakan versi tertentu dari SDK for JavaScript, Anda dapat memasukkannya ke dalam file.zip Anda sebagai dependensi. Untuk informasi selengkapnya tentang menambahkan dependensi yang disertakan runtime ke file.zip Anda, lihat.

[Jalur pencarian ketergantungan dan pustaka yang disertakan runtime](#)

Di bawah [model tanggung jawab AWS bersama](#), Anda bertanggung jawab atas pengelolaan dependensi apa pun dalam paket penerapan fungsi Anda. Ini termasuk menerapkan pembaruan dan patch keamanan. Untuk memperbarui dependensi dalam paket penerapan fungsi Anda, pertama buat file.zip baru dan kemudian unggah ke Lambda. Lihat [Membuat paket penerapan.zip dengan dependensi](#) dan [Membuat dan memperbarui fungsi Lambda Node.js menggunakan file.zip](#) untuk informasi lebih lanjut.

Membuat paket penerapan.zip tanpa dependensi

Jika kode fungsi Anda tidak memiliki dependensi kecuali pustaka yang disertakan dalam runtime Lambda, file.zip Anda hanya berisi `index.mjs` file `index.js` atau dengan kode handler fungsi Anda. Gunakan utilitas zip pilihan Anda untuk membuat file.zip dengan `index.mjs` file `index.js` atau Anda di root. Jika file yang berisi kode handler Anda tidak berada di root file.zip Anda, Lambda tidak akan dapat menjalankan kode Anda.

Untuk mempelajari cara menerapkan file.zip Anda untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada, lihat. [Membuat dan memperbarui fungsi Lambda Node.js menggunakan file.zip](#)

Membuat paket penerapan.zip dengan dependensi

[Jika kode fungsi Anda bergantung pada paket atau modul yang tidak disertakan dalam runtime Lambda Node.js, Anda dapat menambahkan dependensi ini ke file.zip dengan kode fungsi Anda atau menggunakan lapisan Lambda.](#) Petunjuk di bagian ini menunjukkan cara memasukkan dependensi Anda ke dalam paket penerapan.zip Anda. Untuk petunjuk tentang cara memasukkan dependensi Anda dalam lapisan, lihat. [the section called “Membuat layer Node.js untuk dependensi Anda”](#)

Contoh CLI perintah berikut membuat file.zip bernama `my_deployment_package.zip` berisi `index.mjs` file `index.js` or dengan kode handler fungsi Anda dan dependensinya. Dalam contoh, Anda menginstal dependensi menggunakan manajer paket npm.

Untuk membuat paket deployment

1. Arahkan ke direktori proyek yang berisi file kode `index.mjs` sumber `index.js` atau Anda. Dalam contoh ini, direktori diberi nama `my_function`.

```
cd my_function
```

2. Instal pustaka yang diperlukan fungsi Anda di `node_modules` direktori menggunakan `npm install` perintah. Dalam contoh ini Anda menginstal file AWS X-Ray SDK for Node.js.

```
npm install aws-xray-sdk
```

Ini menciptakan struktur folder yang mirip dengan berikut ini:

```
~/my_function
### index.mjs
### node_modules
    ### async
    ### async-listener
    ### atomic-batcher
    ### aws-sdk
    ### aws-xray-sdk
    ### aws-xray-sdk-core
```

Anda juga dapat menambahkan modul khusus yang Anda buat sendiri ke paket penyebaran Anda. Buat direktori di bawah `node_modules` dengan nama modul Anda dan simpan paket tertulis kustom Anda di sana.

3. Buat `file.zip` yang berisi isi folder proyek Anda di root. Gunakan opsi `r` (rekursif) untuk memastikan zip mengompresi subfolder.

```
zip -r my_deployment_package.zip .
```

Membuat layer Node.js untuk dependensi Anda

Instruksi di bagian ini menunjukkan cara memasukkan dependensi Anda dalam lapisan. Untuk petunjuk tentang cara menyertakan dependensi Anda dalam paket penerapan, lihat [the section called "Membuat paket penerapan.zip dengan dependensi"](#)

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam `/opt` direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, PATH variabel sudah menyertakan jalur folder tertentu dalam direktori `/opt`. Untuk memastikan bahwa PATH variabel mengambil konten lapisan Anda, file `layer.zip` Anda harus memiliki dependensi di jalur folder berikut:

- `nodejs/node_modules`
- `nodejs/node16/node_modules` (`NODE_PATH`)
- `nodejs/node18/node_modules` (`NODE_PATH`)
- `nodejs/node20/node_modules` (`NODE_PATH`)

Misalnya, struktur file `layer.zip` Anda mungkin terlihat seperti berikut:

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

Selain itu, Lambda secara otomatis mendeteksi pustaka apa pun di `/opt/lib` direktori, dan binari apa pun di direktori `/opt/bin`. Untuk memastikan bahwa Lambda menemukan konten layer Anda dengan benar, Anda juga dapat membuat layer dengan struktur berikut:

```
custom-layer.zip
# lib
  | lib_1
  | lib_2
# bin
  | bin_1
  | bin_2
```

Setelah Anda mengemas layer Anda, lihat [the section called “Membuat dan menghapus lapisan”](#) dan [the section called “Menambahkan lapisan”](#) untuk menyelesaikan setup layer Anda.

Jalur pencarian ketergantungan dan pustaka yang disertakan runtime

Runtime Node.js mencakup sejumlah pustaka umum, serta versi. AWS SDK for JavaScript Jika Anda ingin menggunakan versi yang berbeda dari pustaka yang disertakan runtime, Anda dapat melakukannya dengan menggabungkannya dengan fungsi Anda atau dengan menambahkannya sebagai dependensi dalam paket penerapan Anda. Misalnya, Anda dapat menggunakan versi yang berbeda SDK dengan menambahkannya ke paket penerapan.zip Anda. Anda juga dapat memasukkannya ke dalam [lapisan Lambda untuk fungsi](#) Anda.

Saat Anda menggunakan `require` pernyataan `import` atau dalam kode Anda, runtime Node.js akan mencari direktori di `NODE_PATH` jalur hingga menemukan modul. Secara default, lokasi pertama pencarian runtime adalah direktori tempat paket deployment .zip Anda didekompresi dan dipasang (`./var/task`). Jika Anda menyertakan versi pustaka yang disertakan runtime dalam paket penerapan, versi ini akan lebih diutamakan daripada versi yang disertakan dalam runtime. Dependensi dalam paket penerapan Anda juga lebih diutamakan daripada dependensi dalam lapisan.

Saat Anda menambahkan dependensi ke lapisan, Lambda mengekstrak ini `/opt/nodejs/nodexx/node_modules` ke `nodexx` mana mewakili versi runtime yang Anda gunakan. Di jalur pencarian, direktori ini lebih diutamakan daripada direktori yang berisi pustaka yang disertakan runtime (`./var/lang/lib/node_modules`). Oleh karena itu, pustaka di lapisan fungsi lebih diutamakan daripada versi yang disertakan dalam runtime.

Anda dapat melihat jalur pencarian lengkap untuk fungsi Lambda Anda dengan menambahkan baris kode berikut.

```
console.log(process.env.NODE_PATH)
```

Anda juga dapat menambahkan dependensi di folder terpisah di dalam paket.zip Anda. Misalnya, Anda dapat menambahkan modul kustom ke folder dalam paket.zip Anda yang dipanggil `common`. Ketika paket.zip Anda didekompresi dan dipasang, folder ini ditempatkan di dalam direktori `./var/task`. Untuk menggunakan dependensi dari folder dalam paket deployment .zip Anda dalam kode Anda, gunakan `const { } = require()` pernyataan `import { } from` atau, tergantung pada apakah Anda menggunakan CJS atau ESM resolusi modul. Sebagai contoh:

```
import { myModule } from './common'
```

Jika Anda menggabungkan kode Anda dengan `esbuild`, `rollup`, atau serupa, dependensi yang digunakan oleh fungsi Anda dibundel bersama dalam satu atau beberapa file. Kami merekomendasikan menggunakan metode ini untuk menjual dependensi bila memungkinkan. Dibandingkan dengan menambahkan dependensi ke paket penerapan Anda, bundling kode Anda menghasilkan peningkatan kinerja karena pengurangan operasi I/O.

Membuat dan memperbarui fungsi Lambda Node.js menggunakan file.zip

Setelah Anda membuat paket.zip deployment, Anda dapat menggunakannya untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada. Anda dapat menerapkan paket.zip Anda menggunakan konsol Lambda, the, AWS Command Line Interface dan Lambda. API Anda juga dapat

membuat dan memperbarui fungsi Lambda menggunakan AWS Serverless Application Model (AWS SAM) dan AWS CloudFormation

Ukuran maksimum untuk paket.zip deployment untuk Lambda adalah 250 MB (unzip). Perhatikan bahwa batas ini berlaku untuk ukuran gabungan semua file yang Anda unggah, termasuk lapisan Lambda apa pun.

Runtime Lambda membutuhkan izin untuk membaca file dalam paket deployment Anda. Dalam notasi oktal izin Linux, Lambda membutuhkan 644 izin untuk file yang tidak dapat dieksekusi (rw-r--r--) dan 755 izin () untuk direktori dan file yang dapat dieksekusi. rwxr-xr-x

Di Linux dan macOS, gunakan `chmod` perintah untuk mengubah izin file pada file dan direktori dalam paket penyebaran Anda. Misalnya, untuk memberikan file yang dapat dieksekusi izin yang benar, jalankan perintah berikut.

```
chmod 755 <filepath>
```

Untuk mengubah izin file di Windows, lihat [Mengatur, Melihat, Mengubah, atau Menghapus Izin pada Objek](#) dalam dokumentasi Microsoft Windows.

Membuat dan memperbarui fungsi dengan file.zip menggunakan konsol

Untuk membuat fungsi baru, Anda harus terlebih dahulu membuat fungsi di konsol, lalu mengunggah arsip.zip Anda. Untuk memperbarui fungsi yang ada, buka halaman untuk fungsi Anda, lalu ikuti prosedur yang sama untuk menambahkan file.zip Anda yang diperbarui.

Jika file.zip Anda kurang dari 50MB, Anda dapat membuat atau memperbarui fungsi dengan mengunggah file langsung dari mesin lokal Anda. Untuk file.zip yang lebih besar dari 50MB, Anda harus mengunggah paket Anda ke bucket Amazon S3 terlebih dahulu. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS Management Console, lihat [Memulai Amazon S3](#). Untuk mengunggah file menggunakan AWS CLI, lihat [Memindahkan objek](#) di Panduan AWS CLI Pengguna.

Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Untuk membuat fungsi baru (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih Buat Fungsi.
2. Pilih Tulis dari awal.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda.
 - b. Untuk Runtime, pilih runtime yang ingin Anda gunakan.
 - c. (Opsional) Untuk Arsitektur, pilih arsitektur set instruksi untuk fungsi Anda. Arsitektur defaultnya adalah x86_64. Pastikan bahwa paket deployment .zip untuk fungsi Anda kompatibel dengan arsitektur set instruksi yang Anda pilih.
4. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan yang sudah ada.
5. Pilih Buat fungsi. Lambda menciptakan fungsi dasar 'Hello world' menggunakan runtime yang Anda pilih.

Untuk mengunggah arsip.zip dari mesin lokal Anda (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih file.zip.
5. Untuk mengunggah file.zip, lakukan hal berikut:
 - a. Pilih Unggah, lalu pilih file.zip Anda di pemilih file.
 - b. Pilih Buka.
 - c. Pilih Simpan.

Untuk mengunggah arsip.zip dari bucket Amazon S3 (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip baru.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih lokasi Amazon S3.

5. Rekatkan tautan Amazon S3 URL dari file.zip Anda dan pilih Simpan.

Memperbarui fungsi file.zip menggunakan editor kode konsol

Untuk beberapa fungsi dengan paket penyebaran.zip, Anda dapat menggunakan editor kode bawaan konsol Lambda untuk memperbarui kode fungsi Anda secara langsung. Untuk menggunakan fitur ini, fungsi Anda harus memenuhi kriteria berikut:

- Fungsi Anda harus menggunakan salah satu runtime bahasa yang ditafsirkan (Python, Node.js, atau Ruby)
- Paket penerapan fungsi Anda harus lebih kecil dari 3MB.

Kode fungsi untuk fungsi dengan paket penerapan gambar kontainer tidak dapat diedit langsung di konsol.

Untuk memperbarui kode fungsi menggunakan editor kode konsol

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih file kode sumber Anda dan edit di editor kode terintegrasi.
4. Setelah selesai mengedit kode, pilih Deploy untuk menyimpan perubahan dan memperbarui fungsi Anda.

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CLI

Anda dapat menggunakan [AWS CLI](#) untuk membuat fungsi baru atau memperbarui yang sudah ada menggunakan file.zip. Gunakan [create-function](#) dan [update-function-code](#) perintah untuk menyebarkan paket.zip Anda. Jika file.zip Anda lebih kecil dari 50MB, Anda dapat mengunggah paket.zip dari lokasi file di mesin build lokal Anda. Untuk file yang lebih besar, Anda harus mengunggah paket.zip Anda dari bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Note

Jika Anda mengunggah file.zip dari bucket Amazon S3 menggunakan AWS CLI bucket, bucket harus berada di lokasi Wilayah AWS yang sama dengan fungsi Anda.

Untuk membuat fungsi baru menggunakan file.zip dengan AWS CLI, Anda harus menentukan yang berikut:

- Nama fungsi Anda (`--function-name`)
- Runtime (`--runtime`) fungsi Anda
- Amazon Resource Name (ARN) dari [peran eksekusi](#) fungsi Anda (`--role`)
- Nama metode handler dalam kode fungsi Anda (`--handler`)

Anda juga harus menentukan lokasi file.zip Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda create-function --function-name myFunction \  
--runtime nodejs20.x --handler index.handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi seperti `--code` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `S3ObjectVersion` parameter untuk objek berversi.

```
aws lambda create-function --function-name myFunction \  
--runtime nodejs20.x --handler index.handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--code S3Bucket=amzn-s3-demo-  
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Untuk memperbarui fungsi yang ada menggunakan CLI, Anda menentukan nama fungsi Anda menggunakan `--function-name` parameter. Anda juga harus menentukan lokasi file.zip yang ingin Anda gunakan untuk memperbarui kode fungsi Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda update-function-code --function-name myFunction \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi `--s3-key` dan seperti `--s3-bucket` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `--s3-object-version` parameter untuk objek berversi.

```
aws lambda update-function-code --function-name myFunction \  
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject  
Version
```

Membuat dan memperbarui fungsi dengan file.zip menggunakan Lambda API

Untuk membuat dan memperbarui fungsi menggunakan arsip file.zip, gunakan API operasi berikut:

- [CreateFunction](#)
- [UpdateFunctionCode](#)

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS SAM

The AWS Serverless Application Model (AWS SAM) adalah toolkit yang membantu merampingkan proses membangun dan menjalankan aplikasi tanpa server. AWS Anda menentukan sumber daya untuk aplikasi Anda dalam JSON template YAML atau dan menggunakan antarmuka baris AWS SAM perintah (AWS SAM CLI) untuk membangun, mengemas, dan menyebarkan aplikasi Anda. Saat Anda membuat fungsi Lambda dari AWS SAM template, AWS SAM secara otomatis membuat paket penerapan .zip atau gambar kontainer dengan kode fungsi Anda dan dependensi apa pun yang Anda tentukan. Untuk mempelajari lebih lanjut cara menggunakan AWS SAM untuk membangun dan menerapkan fungsi Lambda, [lihat Memulai](#) di Panduan AWS SAMAWS Serverless Application Model Pengembang.

Anda juga dapat menggunakan AWS SAM untuk membuat fungsi Lambda menggunakan arsip file.zip yang ada. Untuk membuat fungsi Lambda menggunakan AWS SAM, Anda dapat menyimpan file.zip di bucket Amazon S3 atau di folder lokal di mesin build Anda. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS SAM template Anda, `AWS::Serverless::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- diatur ke `Zip`
- `CodeUri`- diatur ke kode fungsi Amazon S3URI, jalur ke folder lokal, atau objek [FunctionCode](#)
- `Runtime`- Setel ke runtime yang Anda pilih

Dengan AWS SAM, jika file.zip Anda lebih besar dari 50MB, Anda tidak perlu mengunggahnya ke bucket Amazon S3 terlebih dahulu. AWS SAM dapat mengunggah paket.zip hingga ukuran maksimum yang diizinkan 250MB (unzip) dari lokasi di mesin build lokal Anda.

Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS SAM, lihat [AWS::Serverless::Function](#) dalam Panduan Pengembang.AWS SAM

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk membuat fungsi Lambda menggunakan arsip file.zip. Untuk membuat fungsi Lambda dari file.zip, Anda harus terlebih dahulu mengunggah file Anda ke bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS CloudFormation template Anda, `AWS::Lambda::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- Setel ke `Zip`
- `Code`- Masukkan nama bucket Amazon S3 dan nama file.zip di dan bidang `S3Bucket` `S3Key`
- `Runtime`- Setel ke runtime yang Anda pilih

File.zip yang AWS CloudFormation menghasilkan tidak boleh melebihi 4MB. Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS CloudFormation, lihat [AWS::Lambda::Function](#) di Panduan Pengguna.AWS CloudFormation

Deploy fungsi Lambda Node.js dengan gambar kontainer

Ada tiga cara untuk membangun image container untuk fungsi Lambda Node.js:

- [Menggunakan gambar AWS dasar untuk Node.js](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [khusus](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Node.js](#) dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Node.js](#) dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi kontainer Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

Topik

- [AWS gambar dasar untuk Node.js](#)
- [Menggunakan gambar AWS dasar untuk Node.js](#)

- [Menggunakan gambar dasar alternatif dengan klien antarmuka runtime](#)

AWS gambar dasar untuk Node.js

AWS menyediakan gambar dasar berikut untuk Node.js:

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|-------|----------------|-------------------|---|-------------|
| 20 | Node.js 20 | Amazon Linux 2023 | Dockerfile untuk Node.js 20 di GitHub | |
| 18 | Node.js 18 | Amazon Linux 2 | Dockerfile untuk Node.js 18 di GitHub | |

ECR [Repositori Amazon: gallery.ecr.aws/lambda/nodejs](https://gallery.ecr.aws/lambda/nodejs)

Gambar dasar Node.js 20 dan yang lebih baru didasarkan pada [gambar kontainer minimal Amazon Linux 2023](#). Gambar dasar sebelumnya menggunakan Amazon Linux 2. AL2023 memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti `glibc`

AL2 Gambar berbasis 023 menggunakan `microdnf` (symlinked `asdnf`) sebagai manajer paket, bukannya `yum`, yang merupakan pengelola paket default di Amazon Linux 2. `microdnf` adalah implementasi mandiri dari `dnf` Untuk daftar paket yang disertakan dalam gambar AL2 berbasis 023, lihat kolom Kontainer Minimal di Membandingkan paket yang diinstal pada Gambar Kontainer [Amazon Linux 2023](#). Untuk informasi selengkapnya tentang perbedaan antara AL2 023 dan Amazon Linux 2, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di Blog Komputasi AWS .

Note

Untuk menjalankan gambar AL2 berbasis 023 secara lokal, termasuk with AWS Serverless Application Model (AWS SAM), Anda harus menggunakan Docker versi 20.10.10 atau yang lebih baru.

Menggunakan gambar AWS dasar untuk Node.js

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#) (versi minimum 20.10.10 untuk Node.js 20 dan gambar dasar yang lebih baru)
- Node.js

Membuat gambar dari gambar dasar

Untuk membuat gambar kontainer dari gambar AWS dasar untuk Node.js

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Buat proyek Node.js baru dengannpm. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekanEnter.

```
npm init
```

3. Buat file baru bernamaindex.js. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

```
exports.handler = async (event) => {
  const response = {
    statusCode: 200,
    body: JSON.stringify('Hello from Lambda!'),
  };
  return response;
};
```

4. Jika fungsi Anda bergantung pada pustaka selain AWS SDK for JavaScript, gunakan [npm](#) untuk menambahkannya ke paket Anda.
5. Buat Dockerfile baru dengan konfigurasi berikut:

- Atur FROM properti ke [URL gambar dasar](#).
- Gunakan COPY perintah untuk menyalin kode fungsi dan dependensi runtime ke {LAMBDA_TASK_ROOT}, variabel lingkungan yang ditentukan [Lambda](#).
- Atur CMD argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/nodejs:20

# Copy function code
COPY index.js ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
of the Dockerfile)
CMD [ "index.handler" ]
```

6. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

1. Mulai gambar Docker dengan perintah `docker run`. Dalam contoh ini, `docker-image` adalah nama gambar dan test tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

2. Dari jendela terminal baru, posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d  
'{"payload": "hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/  
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

3. Dapatkan ID kontainer.

```
docker ps
```

4. Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECRRepository Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repository Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:


```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositori URI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan gambar dasar alternatif dengan klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda.

Instal [klien antarmuka runtime Node.js](#) menggunakan manajer paket npm:

```
npm install aws-lambda-ric
```

Anda juga dapat mengunduh [klien antarmuka runtime Node.js](#) dari GitHub. Klien antarmuka runtime mendukung versi Node.js berikut:

- 14.x
- 16.x
- 18.x
- 20.x

Contoh berikut menunjukkan bagaimana membangun image container untuk Node.js menggunakan image AWS non-base. Contoh Dockerfile menggunakan gambar buster dasar. Dockerfile menyertakan klien antarmuka runtime.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#)
- Node.js

Membuat gambar dari gambar dasar alternatif

Untuk membuat gambar kontainer dari gambar AWS non-dasar

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Buat proyek Node.js baru dengan npm. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan Enter.

```
npm init
```

3. Buat file baru bernama `index.js`. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

Example Penangan CommonJS

```
exports.handler = async (event) => {
  const response = {
    statusCode: 200,
    body: JSON.stringify('Hello from Lambda!'),
  };
  return response;
};
```

4. Buat Dockerfile baru. Dockerfile berikut menggunakan gambar buster dasar bukan gambar [AWS dasar](#). Dockerfile menyertakan [klien antarmuka runtime](#), yang membuat gambar kompatibel

dengan Lambda. Dockerfile menggunakan build [multi-tahap](#). Tahap pertama membuat image build, yang merupakan lingkungan Node.js standar tempat dependensi fungsi diinstal. Tahap kedua menciptakan gambar yang lebih ramping yang mencakup kode fungsi dan dependensinya. Ini mengurangi ukuran gambar akhir.

- Atur FROM properti ke pengenalan gambar dasar.
- Gunakan COPY perintah untuk menyalin kode fungsi dan dependensi runtime.
- Atur ENTRYPOINT ke modul yang Anda inginkan untuk menjalankan wadah Docker saat dimulai. Dalam hal ini, modul adalah klien antarmuka runtime.
- Atur CMD argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
# Define custom function directory
ARG FUNCTION_DIR="/function"

FROM node:20-buster as build-image

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Install build dependencies
RUN apt-get update && \
    apt-get install -y \
    g++ \
    make \
    cmake \
    unzip \
    libcurl4-openssl-dev

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

WORKDIR ${FUNCTION_DIR}
```

```
# Install Node.js dependencies
RUN npm install

# Install the runtime interface client
RUN npm install aws-lambda-ric

# Grab a fresh slim copy of the image to reduce the final size
FROM node:20-buster-slim

# Required for Node runtimes which use npm@8.6.0+ because
# by default npm writes logs under /home/.npm and Lambda fs is read-only
ENV NPM_CONFIG_CACHE=/tmp/.npm

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT ["/usr/local/bin/npm", "aws-lambda-ric"]
# Pass the name of the function handler as an argument to the runtime
CMD [index.handler]
```

5. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar secara lokal. Anda dapat [membangun emulator ke dalam gambar Anda](#) atau menggunakan prosedur berikut untuk menginstalnya di mesin lokal Anda.

Untuk menginstal dan menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Dari direktori proyek Anda, jalankan perintah berikut untuk mengunduh emulator antarmuka runtime (arsitektur x86-64) dari GitHub dan menginstalnya di mesin lokal Anda.

Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \  
  curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-  
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \  
  chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Untuk menginstal emulator arm64, ganti GitHub repositori URL di perintah sebelumnya dengan yang berikut:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/  
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"  
if (-not (Test-Path $dirPath)) {  
  New-Item -Path $dirPath -ItemType Directory  
}  
  
$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/  
releases/latest/download/aws-lambda-rie"  
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"  
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Untuk menginstal emulator arm64, ganti `$downloadLink` dengan yang berikut ini:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/  
download/aws-lambda-rie-arm64
```

2. Mulai gambar Docker dengan perintah docker run. Perhatikan hal berikut:

- `docker-image` adalah nama gambar dan test tag.
- `/usr/local/bin/npx aws-lambda-ric index.handler` adalah ENTRYPOINT diikuti oleh CMD dari Dockerfile Anda.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
9000:8080 \
  --entrypoint /aws-lambda/aws-lambda-rie \
  docker-image:test \
  /usr/local/bin/npx aws-lambda-ric index.handler
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
/usr/local/bin/npx aws-lambda-ric index.handler
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

3. Posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan Invoke-WebRequest perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{} ' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

4. Dapatkan ID kontainer.

```
docker ps
```

5. Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.

- Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
- Ganti `111122223333` dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECRRepositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.

4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repository URI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Node.js

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Metode konteks

- `getRemainingTimeInMillis()` – Mengembalikan jumlah milidetik yang tersisa sebelum waktu eksekusi habis.

Properti konteks

- `functionName` – Nama fungsi Lambda.
- `functionVersion` – [Versi](#) fungsi.
- `invokedFunctionArn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `memoryLimitInMB` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `awsRequestId` – Pengidentifikasi permintaan invokasi.
- `logGroupName` – Grup log untuk fungsi.
- `logStreamName` – Aliran log untuk instans fungsi.
- `identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
 - `cognitoIdentityId` – Identitas Amazon Cognito terautentikasi.
 - `cognitoIdentityPoolId` – Kumpulan identitas Amazon Cognito yang mengesahkan invokasi.
- `clientContext` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
 - `client.installation_id`
 - `client.app_title`
 - `client.app_version_name`
 - `client.app_version_code`
 - `client.app_package_name`

- `env.platform_version`
 - `env.platform`
 - `env.make`
 - `env.model`
 - `env.locale`
 - Custom – Nilai kustom yang ditetapkan oleh aplikasi klien.
- `callbackWaitsForEmptyEventLoop` – Atur ke salah untuk mengirimkan jawaban segera saat [panggilan balik](#) berjalan, alih-alih menunggu loop peristiwa Node.js kosong. Jika ini salah, semua peristiwa yang belum selesai akan terus berjalan selama invokasi berikutnya.

Contoh fungsi berikut mencatat informasi konteks dan mengembalikan lokasi log.

Example `index.js` file

```
exports.handler = async function(event, context) {
  console.log('Remaining time: ', context.getRemainingTimeInMillis())
  console.log('Function name: ', context.functionName)
  return context.logStreamName
}
```

Log dan pantau fungsi Node.js Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda dan mengirim log ke Amazon CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap invokasi ke pengaliran log, dan menyampaikan log serta output lain dari kode fungsi Anda. Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Halaman ini menjelaskan cara menghasilkan keluaran log dari kode fungsi Lambda Anda, dan mengakses log menggunakan AWS Command Line Interface, konsol Lambda, atau konsol CloudWatch

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Menggunakan kontrol logging lanjutan Lambda dengan Node.js](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)

Membuat fungsi yang mengembalikan log

Untuk menghasilkan log dari kode fungsi, Anda dapat menggunakan metode di [objek konsol](#), atau pustaka pencatatan yang menulis ke `stdout` atau `stderr`. Contoh berikut mencatat nilai variabel lingkungan dan objek peristiwa.

Example index.js file – Pencatatan

```
exports.handler = async function(event, context) {
  console.log("ENVIRONMENT VARIABLES\n" + JSON.stringify(process.env, null, 2))
  console.info("EVENT\n" + JSON.stringify(event, null, 2))
  console.warn("Event not processed.")
  return context.logStreamName
}
```

Example format log

```
START RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Version: $LATEST
```

```

2019-06-07T19:11:20.562Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO ENVIRONMENT
  VARIABLES
  {
    "AWS_LAMBDA_FUNCTION_VERSION": "$LATEST",
    "AWS_LAMBDA_LOG_GROUP_NAME": "/aws/lambda/my-function",
    "AWS_LAMBDA_LOG_STREAM_NAME": "2019/06/07/[$LATEST]e6f4a0c4241adcd70c262d34c0bbc85c",
    "AWS_EXECUTION_ENV": "AWS_Lambda_nodejs12.x",
    "AWS_LAMBDA_FUNCTION_NAME": "my-function",
    "PATH": "/var/lang/bin:/usr/local/bin:/usr/bin:/bin:/opt/bin",
    "NODE_PATH": "/opt/nodejs/node10/node_modules:/opt/nodejs/node_modules:/var/runtime/
node_modules",
    ...
  }
2019-06-07T19:11:20.563Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO EVENT
  {
    "key": "value"
  }
2019-06-07T19:11:20.564Z c793869b-ee49-115b-a5b6-4fd21e8dedac WARN Event not processed.
END RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac
REPORT RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Duration: 128.83 ms Billed
  Duration: 200 ms Memory Size: 128 MB Max Memory Used: 74 MB Init Duration: 166.62 ms
XRAY TraceId: 1-5d9d007f-0a8c7fd02xmpl480aed55ef0 SegmentId: 3d752xmpl1bbe37e Sampled:
  true

```

Runtime Node.js mencatat baris START, END, dan REPORT untuk setiap invokasi. Ini menambahkan stempel waktu, ID permintaan, dan tingkat log ke setiap entri yang dicatat oleh fungsi. Baris laporan memberikan perincian berikut.

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.

- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Anda dapat melihat log di konsol Lambda, di konsol CloudWatch Log, atau dari baris perintah.

Menggunakan kontrol logging lanjutan Lambda dengan Node.js

Untuk memberi Anda kontrol lebih besar atas bagaimana log fungsi Anda ditangkap, diproses, dan digunakan, Anda dapat mengonfigurasi opsi logging berikut untuk runtime Node.js yang didukung:

- Format log - pilih antara teks biasa dan format JSON terstruktur untuk log fungsi Anda
- Tingkat log - untuk log dalam format JSON, pilih tingkat detail log yang dikirim Lambda ke CloudWatch Amazon, seperti ERROR, DEBUG, atau INFO
- Grup log - pilih grup CloudWatch log yang dikirimkan oleh fungsi Anda

Untuk informasi selengkapnya tentang opsi pencatatan ini, dan petunjuk tentang cara mengonfigurasi fungsi Anda untuk menggunakannya, lihat [the section called “Konfigurasi log fungsi”](#).

Untuk menggunakan format log dan opsi tingkat log dengan fungsi Lambda Node.js Anda, lihat panduan di bagian berikut.

Menggunakan log JSON terstruktur dengan Node.js

Jika Anda memilih JSON untuk format log fungsi Anda, Lambda akan mengirim output log menggunakan metode `console.trace`, `console.debug`, `console.log`, `console.info`, `console.error`, `console.warn` dan CloudWatch ke sebagai JSON terstruktur. Setiap objek log JSON berisi setidaknya empat pasangan nilai kunci dengan kunci berikut:

- "timestamp"- waktu pesan log dihasilkan
- "level"- tingkat log yang ditetapkan untuk pesan
- "message"- isi pesan log
- "requestId"- ID permintaan unik untuk pemanggilan fungsi

Bergantung pada metode logging yang digunakan fungsi Anda, objek JSON ini mungkin juga berisi pasangan kunci tambahan. Misalnya, jika fungsi Anda menggunakan `console` metode untuk mencatat objek kesalahan menggunakan beberapa argumen, objek JSON akan berisi pasangan nilai kunci tambahan dengan kunci `errorMessage`, `errorType`, dan `stackTrace`.

Jika kode Anda sudah menggunakan pustaka logging lain, seperti Powertools for AWS Lambda, untuk menghasilkan log terstruktur JSON, Anda tidak perlu membuat perubahan apa pun. Lambda tidak menyandikan dua kali log apa pun yang sudah dikodekan JSON, sehingga log aplikasi fungsi Anda akan terus ditangkap seperti sebelumnya.

Untuk informasi selengkapnya tentang penggunaan paket Powertools for AWS Lambda logging guna membuat log terstruktur JSON di runtime Node.js, lihat [the section called "Pencatatan log"](#)

Contoh keluaran log yang diformat JSON

Contoh berikut menunjukkan bagaimana berbagai keluaran log yang dihasilkan menggunakan `console` metode dengan argumen tunggal dan ganda ditangkap di CloudWatch Log saat Anda menyetel format log fungsi Anda ke JSON.

Contoh pertama menggunakan `console.error` metode untuk menampilkan string sederhana.

Example Kode pencatatan Node.js

```
export const handler = async (event) => {
  console.error("This is a warning message");
  ...
}
```

Example Catatan log JSON

```
{
  "timestamp": "2023-11-01T00:21:51.358Z",
  "level": "ERROR",
  "message": "This is a warning message",
  "requestId": "93f25699-2cbf-4976-8f94-336a0aa98c6f"
}
```

Anda juga dapat menampilkan pesan log terstruktur yang lebih kompleks menggunakan argumen tunggal atau ganda dengan `console` metode. Dalam contoh berikutnya, Anda gunakan `console.log` untuk menampilkan dua pasangan nilai kunci menggunakan argumen tunggal. Perhatikan bahwa "message" bidang dalam objek JSON yang dikirim Lambda CloudWatch ke Log tidak dirangkai.

Example Kode pencatatan Node.js

```
export const handler = async (event) => {
```

```
console.log({data: 12.3, flag: false});
...
}
```

Example Catatan log JSON

```
{
  "timestamp": "2023-12-08T23:21:04.664Z",
  "level": "INFO",
  "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
  "message": {
    "data": 12.3,
    "flag": false
  }
}
```

Dalam contoh berikutnya, Anda kembali menggunakan `console.log` metode untuk membuat output log. Kali ini, metode ini mengambil dua argumen, peta yang berisi dua pasangan nilai kunci dan string pengidentifikasi. Perhatikan bahwa dalam kasus ini, karena Anda telah memberikan dua argumen, Lambda membuat stringifikasi bidang. "message"

Example Kode pencatatan Node.js

```
export const handler = async (event) => {
  console.log('Some object - ', {data: 12.3, flag: false});
  ...
}
```

Example Catatan log JSON

```
{
  "timestamp": "2023-12-08T23:21:04.664Z",
  "level": "INFO",
  "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
  "message": "Some object - { data: 12.3, flag: false }"
}
```

Lambda menetapkan output yang dihasilkan menggunakan INFO tingkat `logconsole.log`.

Contoh terakhir menunjukkan bagaimana objek kesalahan dapat output ke CloudWatch Log menggunakan `console` metode. Perhatikan bahwa ketika Anda mencatat objek kesalahan

menggunakan beberapa argumen, Lambda menambahkan bidang `errorMessage`, `errorType`, dan `stackTrace` ke output log.

Example Kode pencatatan Node.js

```
export const handler = async (event) => {
  let e1 = new ReferenceError("some reference error");
  let e2 = new SyntaxError("some syntax error");
  console.log(e1);
  console.log("errors logged - ", e1, e2);
};
```

Example Catatan log JSON

```
{
  "timestamp": "2023-12-08T23:21:04.632Z",
  "level": "INFO",
  "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
  "message": {
    "errorType": "ReferenceError",
    "errorMessage": "some reference error",
    "stackTrace": [
      "ReferenceError: some reference error",
      "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
      "    at Runtime.handleOnceNonStreaming (file:///var/runtime/index.mjs:1173:29)"
    ]
  }
}

{
  "timestamp": "2023-12-08T23:21:04.646Z",
  "level": "INFO",
  "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
  "message": "errors logged - ReferenceError: some reference error
\n    at Runtime.handler (file:///var/task/index.mjs:3:12)\n    at
Runtime.handleOnceNonStreaming
(file:///var/runtime/index.mjs:1173:29) SyntaxError: some syntax
error\n    at Runtime.handler (file:///var/task/index.mjs:4:12)\n    at
Runtime.handleOnceNonStreaming
(file:///var/runtime/index.mjs:1173:29)",
  "errorType": "ReferenceError",
  "errorMessage": "some reference error",
```

```
"stackTrace": [
  "ReferenceError: some reference error",
  "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
  "    at Runtime.handleOnceNonStreaming (file:///var/runtime/index.mjs:1173:29)"
]
```

Saat mencatat beberapa jenis kesalahan, bidang `errorMessage`, `errorType`, dan `stackTrace` diekstraksi dari jenis kesalahan pertama yang diberikan ke `console` metode.

Menggunakan pustaka klien format metrik tertanam (EMF) dengan log JSON terstruktur

AWS menyediakan pustaka klien sumber terbuka untuk Node.js yang dapat Anda gunakan untuk membuat log [format metrik tertanam](#) (EMF). Jika Anda memiliki fungsi yang ada yang menggunakan pustaka ini dan Anda mengubah format log fungsi Anda ke JSON, CloudWatch mungkin tidak lagi mengenali metrik yang dipancarkan oleh kode Anda.

Jika kode Anda saat ini memancarkan log EMF secara langsung menggunakan `console.log` atau dengan menggunakan Powertools for AWS Lambda (TypeScript), juga tidak CloudWatch akan dapat mengurai ini jika Anda mengubah format log fungsi Anda menjadi JSON.

Important

Untuk memastikan bahwa log EMF fungsi Anda terus diurai dengan benar CloudWatch, perbarui [EMF](#) dan [Powertools Anda untuk AWS Lambda](#) pustaka ke versi terbaru.

Jika beralih ke format log JSON, kami juga menyarankan Anda melakukan pengujian untuk memastikan kompatibilitas dengan metrik tertanam fungsi Anda. Jika kode Anda memancarkan log EMF secara langsung menggunakan `console.log`, ubah kode Anda untuk menampilkan metrik tersebut secara langsung `stdout` seperti yang ditunjukkan pada contoh kode berikut.

Example kode yang memancarkan metrik tertanam ke **stdout**

```
process.stdout.write(JSON.stringify(
  {
    "_aws": {
      "Timestamp": Date.now(),
```

```
    "CloudWatchMetrics": [{
      "Namespace": "lambda-function-metrics",
      "Dimensions": [["functionVersion"]],
      "Metrics": [{
        "Name": "time",
        "Unit": "Milliseconds",
        "StorageResolution": 60
      }]
    }]
  },
  "functionVersion": "$LATEST",
  "time": 100,
  "requestId": context.awsRequestId
}
) + "\n")
```

Menggunakan penyaringan tingkat log dengan Node.js

AWS Lambda Untuk memfilter log aplikasi Anda sesuai dengan tingkat lognya, fungsi Anda harus menggunakan log berformat JSON. Anda dapat mencapai ini dengan dua cara:

- Buat output log menggunakan metode konsol standar dan konfigurasi fungsi Anda untuk menggunakan pemformatan log JSON. AWS Lambda kemudian memfilter output log Anda menggunakan pasangan nilai kunci "level" di objek JSON yang dijelaskan dalam [the section called "Menggunakan log JSON terstruktur dengan Node.js"](#) Untuk mempelajari cara mengonfigurasi format log fungsi Anda, lihat [the section called "Konfigurasi log fungsi"](#).
- Gunakan pustaka atau metode logging lain untuk membuat log terstruktur JSON dalam kode Anda yang menyertakan pasangan nilai kunci "level" yang menentukan tingkat keluaran log. Misalnya, Anda dapat menggunakan Powertools AWS Lambda untuk menghasilkan keluaran log terstruktur JSON dari kode Anda. Lihat [the section called "Pencatatan log"](#) untuk mempelajari lebih lanjut tentang menggunakan Powertools dengan runtime Node.js.

Agar Lambda dapat memfilter log fungsi Anda, Anda juga harus menyertakan pasangan nilai "timestamp" kunci dalam keluaran log JSON Anda. Waktu harus ditentukan dalam format stempel waktu [RFC 3339](#) yang valid. Jika Anda tidak menyediakan stempel waktu yang valid, Lambda akan menetapkan log INFO level dan menambahkan stempel waktu untuk Anda.

Ketika Anda mengonfigurasi fungsi Anda untuk menggunakan pemfilteran tingkat log, Anda memilih tingkat log yang ingin Anda kirim AWS Lambda ke CloudWatch Log dari opsi berikut:

| Tingkat log | Penggunaan standar |
|-----------------------|--|
| TRACE (paling detail) | Informasi paling halus yang digunakan untuk melacak jalur eksekusi kode Anda |
| AWAKUTU | Informasi terperinci untuk debugging sistem |
| INFO | Pesan yang merekam operasi normal fungsi Anda |
| PERINGATAN | Pesan tentang potensi kesalahan yang dapat menyebabkan perilaku tak terduga jika tidak ditangani |
| ERROR | Pesan tentang masalah yang mencegah kode berfungsi seperti yang diharapkan |
| FATAL (paling detail) | Pesan tentang kesalahan serius yang menyebabkan aplikasi berhenti berfungsi |

Lambda mengirimkan log dari level yang dipilih dan lebih rendah ke CloudWatch. Misalnya, jika Anda mengonfigurasi level log WARN, Lambda akan mengirim log yang sesuai dengan level WARN, ERROR, dan FATAL.

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, kami sarankan untuk menginstrumentasi fungsi Anda dengan AWS X-Ray. X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBULQgUmVxdWVzdElk0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzVlNGZiMjEgVmVyc2l1vb...",
  "ExecutedVersion": "$LATEST"
```

```
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \  
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --  
decode
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST  
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-  
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0\"", ask/lib:/opt/lib",  
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed  
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15 detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`.

Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
{
  "events": [
    {
      "timestamp": 1559763003171,
      "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
      "ingestionTime": 1559763003309
    },
    {
      "timestamp": 1559763003173,
```

```

      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\$LATEST\",
\r ...",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
    "ingestionTime": 1559763018353
  }
],
"nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}

```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Menginstrumentasi kode Node.js di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari dua SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK for Node.js](#)— An SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh. AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray. SDKs](#)

Bagian-bagian

- [Menggunakan ADOT untuk menginstruksikan fungsi Node.js Anda](#)
- [Menggunakan X-Ray SDK untuk instrumen fungsi Node.js Anda](#)
- [Mengaktifkan penelusuran dengan konsol Lambda](#)
- [Mengaktifkan penelusuran dengan Lambda API](#)
- [Mengaktifkan penelusuran dengan AWS CloudFormation](#)
- [Menafsirkan jejak X-Ray](#)

- [Menyimpan dependensi runtime dalam lapisan \(X-Ray\) SDK](#)

Menggunakan ADOT untuk menginstruksikan fungsi Node.js Anda

ADOT menyediakan [lapisan](#) Lambda yang dikelola sepenuhnya yang mengemas semua yang Anda butuhkan untuk mengumpulkan data telemetri menggunakan file. OTEL SDK Dengan menggunakan lapisan ini, Anda dapat menginstruksikan fungsi Lambda Anda tanpa harus memodifikasi kode fungsi apa pun. Anda juga dapat mengonfigurasi lapisan Anda untuk melakukan inisialisasi kustom. OTEL Untuk informasi selengkapnya, lihat [Konfigurasi khusus untuk ADOT Kolektor di Lambda](#) dalam dokumentasi. ADOT

Untuk runtime Node.js, Anda dapat menambahkan layer Lambda AWS terkelola ADOT untuk Javascript untuk menginstruksikan fungsi Anda secara otomatis. Untuk petunjuk rinci tentang cara menambahkan layer ini, lihat [AWS Distro untuk OpenTelemetry Lambda JavaScript Support](#) untuk ADOT dalam dokumentasi.

Menggunakan X-Ray SDK untuk instrumen fungsi Node.js Anda

Untuk merekam detail tentang panggilan yang dilakukan oleh fungsi Lambda Anda ke sumber daya lain dalam aplikasi Anda, Anda juga dapat menggunakan. AWS X-Ray SDK for Node.js Untuk mendapatkan SDK, tambahkan `aws-xray-sdk-core` paket ke dependensi aplikasi Anda.

Example [kosong-nodejs/package.json](#)

```
{
  "name": "blank-nodejs",
  "version": "1.0.0",
  "private": true,
  "devDependencies": {
    "jest": "29.7.0"
  },
  "dependencies": {
    "@aws-sdk/client-lambda": "3.345.0",
    "aws-xray-sdk-core": "3.5.3"
  },
  "scripts": {
    "test": "jest"
  }
}
```

Untuk instrumen AWS SDK klien di [AWS SDK for JavaScript v3](#), bungkus instance klien dengan `captureAWSv3Client` metode.

Example [blank-nodejs/function/index.js](#) - Menelusuri klien AWS SDK

```
const AWSXRay = require('aws-xray-sdk-core');
const { LambdaClient, GetAccountSettingsCommand } = require('@aws-sdk/client-lambda');

// Create client outside of handler to reuse
const lambda = AWSXRay.captureAWSv3Client(new LambdaClient());

// Handler
exports.handler = async function(event, context) {
  event.Records.forEach(record => {
    ...
  })
}
```

Runtime Lambda menetapkan beberapa variabel lingkungan untuk mengkonfigurasi X-Ray. SDK Misalnya, Lambda mengatur `AWS_XRAY_CONTEXT_MISSING LOG_ERROR` untuk menghindari melempar kesalahan runtime dari X-Ray. SDK Untuk menetapkan strategi yang hilang dalam konteks khusus, timpa variabel lingkungan dalam konfigurasi fungsi Anda agar tidak memiliki nilai, lalu Anda dapat menetapkan konteks yang tidak memiliki strategi yang terprogram.

Example Kode inisialisasi contoh

```
const AWSXRay = require('aws-xray-sdk-core');

// Configure the context missing strategy to do nothing
AWSXRay.setContextMissingStrategy(() => {});
```

Untuk informasi selengkapnya, lihat [the section called “Mengonfigurasi variabel lingkungan”](#).

Setelah Anda menambahkan dependensi yang benar dan membuat perubahan kode yang diperlukan, aktifkan penelusuran dalam konfigurasi fungsi Anda melalui konsol Lambda atau. API

Mengaktifkan penelusuran dengan konsol Lambda

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

Mengaktifkan penelusuran dengan Lambda API

Konfigurasikan penelusuran pada fungsi Lambda Anda dengan AWS CLI AWS SDK atau, gunakan operasi berikut API:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \  
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Lambda::Function  
    Properties:  
      TracingConfig:  
        Mode: Active
```

...

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Menafsirkan jejak X-Ray

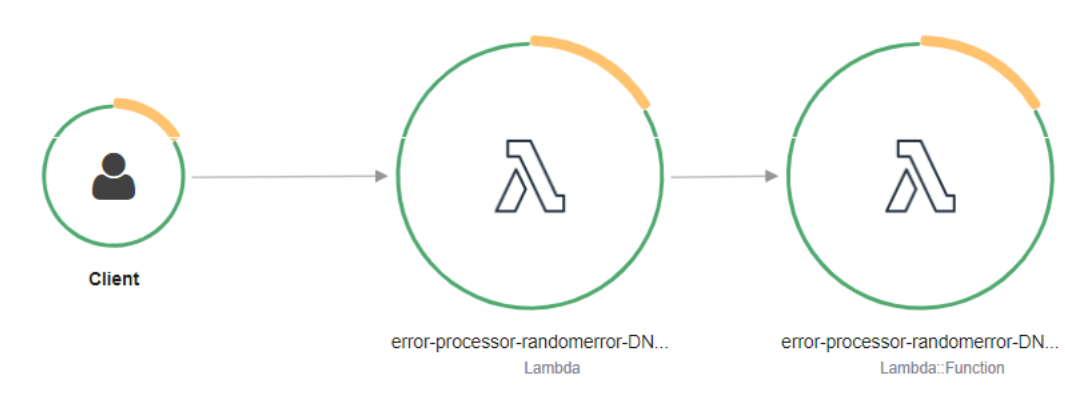
Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch

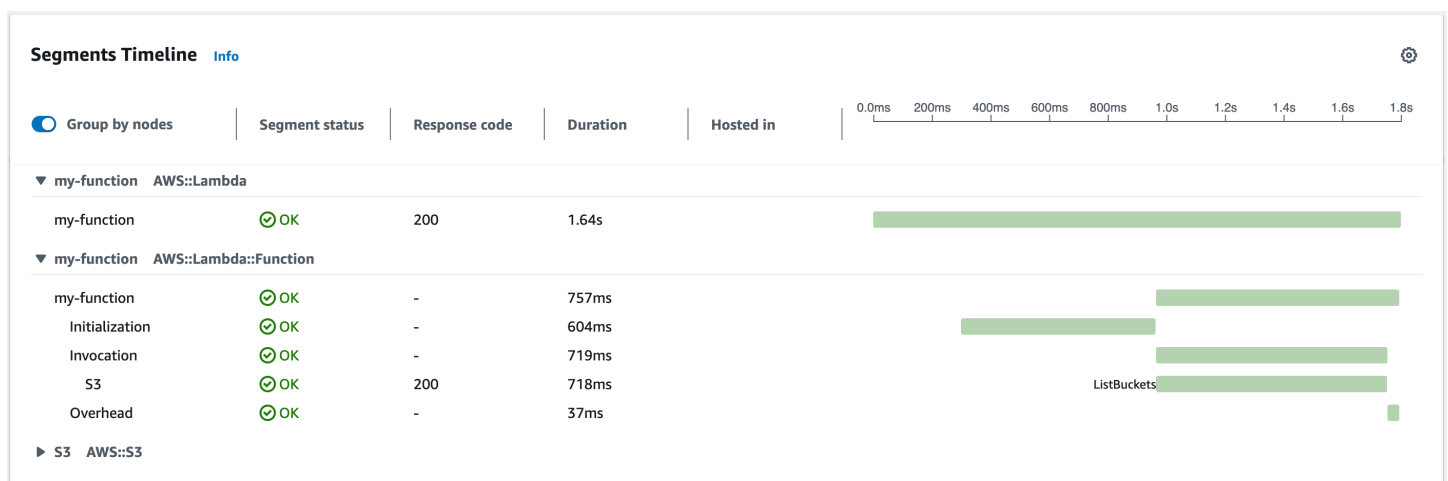


X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyortir dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal `usul`. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. `Invocation` Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat [the section called “Memahami jejak X-Ray”](#)

Anda juga dapat HTTP menginstrumentasikan klien, merekam SQL kueri, dan membuat subsegmen khusus dengan anotasi dan metadata. Untuk informasi selengkapnya, lihat [AWS X-Ray SDK for Node.js](#) di Panduan AWS X-Ray Pengembang.

Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-

Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi selengkapnya, lihat [harga AWS X-Ray](#).

Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK

Jika Anda menggunakan X-Ray SDK untuk instrumen AWS SDK klien kode fungsi Anda, paket penyebaran Anda bisa menjadi cukup besar. [Untuk menghindari mengunggah dependensi runtime setiap kali Anda memperbarui kode fungsi, paketkan X-Ray di SDK lapisan Lambda.](#)

Contoh berikut menunjukkan `AWS::Serverless::LayerVersion` sumber daya yang menyimpan file AWS X-Ray SDK for Node.js.

Example [template.yml](#) – Lapisan dependensi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
        ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-nodejs-lib
      Description: Dependencies for the blank sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - nodejs16.x
```

Dengan konfigurasi ini, Anda memperbarui lapisan pustaka hanya jika Anda mengubah dependensi runtime Anda. Karena paket penerapan fungsi hanya berisi kode Anda, ini dapat membantu mengurangi waktu upload.

Membuat lapisan untuk dependensi memerlukan perubahan build untuk membuat arsip lapisan sebelum deployment. Untuk contoh pekerjaan, lihat contoh aplikasi [blank-nodejs](#).

Membangun fungsi Lambda dengan TypeScript

Anda dapat menggunakan runtime Node.js untuk menjalankan TypeScript kode di AWS Lambda. Karena Node.js tidak menjalankan TypeScript kode secara asli, Anda harus terlebih dahulu mentranspile TypeScript kode Anda menjadi JavaScript. Kemudian, gunakan JavaScript file untuk menyebarkan kode fungsi Anda ke Lambda. Kode Anda berjalan di lingkungan yang menyertakan AWS SDK for JavaScript, dengan kredensial dari peran AWS Identity and Access Management (IAM) yang Anda kelola. Untuk mempelajari lebih lanjut tentang SDK versi yang disertakan dengan runtime Node.js, lihat [the section called “Versi termasuk runtime SDK”](#).

Lambda mendukung runtime Node.js berikut.

Node.js

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|------------|------------------|-------------------|---------------------|------------------|-----------------------|
| Node.js 20 | nodejs20.x | Amazon Linux 2023 | | | |
| Node.js 18 | nodejs18.x | Amazon Linux 2 | | | |

Topik

- [Menyiapkan lingkungan TypeScript pengembangan](#)
- [Tentukan penanganan fungsi Lambda di TypeScript](#)
- [Terapkan TypeScript kode yang ditranspilasikan di Lambda dengan arsip file.zip](#)
- [Terapkan TypeScript kode yang ditranspilasikan di Lambda dengan gambar wadah](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi TypeScript](#)
- [Log dan pantau fungsi TypeScript Lambda](#)
- [Menelusuri TypeScript kode di AWS Lambda](#)

Menyiapkan lingkungan TypeScript pengembangan

Gunakan lingkungan pengembangan terintegrasi lokal (IDE), editor teks, atau [AWS Cloud9](#) untuk menulis kode TypeScript fungsi Anda. Anda tidak dapat membuat TypeScript kode di konsol Lambda.

[Untuk mentranspile TypeScript kode Anda, siapkan kompiler seperti esbuild atau TypeScript compiler \(tsc\) Microsoft, yang dibundel dengan distribusi TypeScript](#) Anda dapat menggunakan [AWS Serverless Application Model \(AWS SAM\)](#) atau [AWS Cloud Development Kit \(AWS CDK\)](#) untuk menyederhanakan pembuatan dan penerapan kode TypeScript . Kedua alat menggunakan esbuild untuk mentranspile TypeScript kode ke dalam. JavaScript

Saat menggunakan esbuild, pertimbangkan hal berikut:

- Ada beberapa [TypeScript peringatan](#).
- Anda harus mengonfigurasi pengaturan TypeScript transpilasi agar sesuai dengan runtime Node.js yang Anda rencanakan untuk digunakan. Untuk informasi selengkapnya, lihat [Target](#) dalam dokumentasi esbuild. [Untuk contoh file tsconfig.json yang menunjukkan cara menargetkan versi Node.js tertentu yang didukung oleh Lambda, lihat repositori TypeScript GitHub](#)
- esbuild tidak melakukan pemeriksaan tipe. Untuk memeriksa jenis, gunakan tsc kompiler. Jalankan `tsc -noEmit` atau tambahkan "noEmit" parameter ke file tsconfig.json Anda, seperti yang ditunjukkan pada contoh berikut. Ini mengkonfigurasi tsc untuk tidak memancarkan file JavaScript . Setelah memeriksa jenis, gunakan esbuild untuk mengonversi TypeScript file menjadi JavaScript.

Example tsconfig.json

```
{
  "compilerOptions": {
    "target": "es2020",
    "strict": true,
    "preserveConstEnums": true,
    "noEmit": true,
    "sourceMap": false,
    "module": "commonjs",
    "moduleResolution": "node",
    "esModuleInterop": true,
    "skipLibCheck": true,
    "forceConsistentCasingInFileNames": true,
    "isolatedModules": true,
  }
}
```

```
  },  
  "exclude": ["node_modules", "**/*.test.ts"]  
}
```

Tentukan penanganan fungsi Lambda di TypeScript

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Topik

- [Dasar-dasar penanganan TypeScript](#)
- [Menggunakan async/await](#)
- [Menggunakan callback](#)
- [Menggunakan tipe untuk objek acara](#)
- [Praktik terbaik kode untuk fungsi Lambda TypeScript](#)

Dasar-dasar penanganan TypeScript

Example TypeScript pawang

Fungsi contoh ini mencatat isi objek acara dan mengembalikan lokasi log. Perhatikan hal berikut:

- Sebelum menggunakan kode ini dalam fungsi Lambda, Anda harus menambahkan paket [@types / aws-lambda](#) sebagai dependensi pengembangan. Paket ini berisi definisi tipe untuk Lambda. Ketika `@types/aws-lambda` diinstal, `import` pernyataan (`import ... from 'aws-lambda'`) mengimpor definisi tipe. Itu tidak mengimpor `aws-lambda` NPM paket, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori DefinitelyTyped GitHub
- Handler dalam contoh ini adalah modul ES dan harus ditunjuk seperti itu di `package.json` file Anda atau dengan menggunakan ekstensi `.mjs` file. Untuk informasi lebih lanjut, lihat [Menunjuk penanganan fungsi sebagai modul ES](#).

```
import { Handler } from 'aws-lambda';

export const handler: Handler = async (event, context) => {
  console.log('EVENT: \n' + JSON.stringify(event, null, 2));
  return context.logStreamName;
};
```

Runtime meneruskan argumen ke metode handler. Argumen pertama adalah objek event, yang berisi informasi dari invoker. Invoker meneruskan informasi ini sebagai string yang JSON diformat - saat memanggil [Invoke](#), dan runtime mengubahnya menjadi objek. Ketika AWS layanan memanggil fungsi Anda, struktur acara [bervariasi menurut layanan](#). Dengan TypeScript, kami sarankan menggunakan anotasi tipe untuk objek acara. Untuk informasi selengkapnya, lihat [Menggunakan tipe untuk objek acara](#).

Argumen kedua adalah [objek konteks](#), yang berisi informasi tentang lingkungan invokasi, fungsi, dan eksekusi. Pada contoh sebelumnya, fungsi mendapatkan nama [alur log](#) dari objek konteks dan mengembalikannya ke invoker.

Anda juga dapat menggunakan argumen callback, yang merupakan fungsi yang dapat Anda panggil di penanganan non-async untuk mengirim respons. Kami menyarankan Anda menggunakan `async/await` alih-alih callback. `Async/await` memberikan peningkatan keterbacaan, penanganan kesalahan, dan efisiensi. Untuk informasi selengkapnya tentang perbedaan antara `async/await` dan callback, lihat [Menggunakan callback](#)

Menggunakan `async/await`

Jika kode Anda melakukan tugas asinkron, gunakan pola `async/await` untuk memastikan bahwa handler selesai berjalan. `Async/await` adalah cara ringkas dan mudah dibaca untuk menulis kode asinkron di Node.js, tanpa perlu panggilan balik bersarang atau janji rantai. Dengan `async/await`, Anda dapat menulis kode yang berbunyi seperti kode sinkron, sambil tetap asinkron dan tidak memblokir.

`async` Kata kunci menandai fungsi sebagai asinkron, dan `await` kata kunci menjeda eksekusi fungsi sampai a diselesaikan. `Promise`

Example TypeScript fungsi — asinkron

Contoh ini menggunakan `fetch`, yang tersedia di `nodejs18.x` runtime. Perhatikan hal berikut:

- Sebelum menggunakan kode ini dalam fungsi Lambda, Anda harus menambahkan paket [@types/aws-lambda](#) sebagai dependensi pengembangan. Paket ini berisi definisi tipe untuk Lambda. Ketika `@types/aws-lambda` diinstal, `import` pernyataan (`import ... from 'aws-lambda'`) mengimpor definisi tipe. Itu tidak mengimpor `aws-lambda` NPM paket, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub

- Handler dalam contoh ini adalah modul ES dan harus ditunjuk seperti itu di package.json file Anda atau dengan menggunakan ekstensi .mjs file. Untuk informasi lebih lanjut, lihat [Menunjuk penanganan fungsi sebagai modul ES](#).

```
import { APIGatewayProxyEvent, APIGatewayProxyResult } from 'aws-lambda';
const url = 'https://aws.amazon.com/';
export const lambdaHandler = async (event: APIGatewayProxyEvent):
  Promise<APIGatewayProxyResult> => {
  try {
    // fetch is available with Node.js 18
    const res = await fetch(url);
    return {
      statusCode: res.status,
      body: JSON.stringify({
        message: await res.text(),
      }),
    };
  } catch (err) {
    console.log(err);
    return {
      statusCode: 500,
      body: JSON.stringify({
        message: 'some error happened',
      }),
    };
  }
};
```

Menggunakan callback

Kami menyarankan Anda menggunakan [async/await](#) untuk mendeklarasikan fungsi handler alih-alih menggunakan callback. Async/await adalah pilihan yang lebih baik karena beberapa alasan:

- Keterbacaan: Kode async/await lebih mudah dibaca dan dipahami daripada kode panggilan balik, yang dapat dengan cepat menjadi sulit untuk diikuti dan menghasilkan neraka panggilan balik.
- Debugging dan penanganan kesalahan: Debugging kode berbasis callback bisa jadi sulit. Tumpukan panggilan bisa menjadi sulit untuk diikuti dan kesalahan dapat dengan mudah ditelan. Dengan async/await, Anda dapat menggunakan blok coba/tangkap untuk menangani kesalahan.
- Efisiensi: Callback sering memerlukan peralihan di antara bagian-bagian kode yang berbeda. Async/await dapat mengurangi jumlah sakelar konteks, menghasilkan kode yang lebih efisien.

Saat Anda menggunakan callback di handler Anda, fungsi terus dijalankan hingga [loop peristiwa](#) kosong atau fungsi habis waktu. Respons tidak dikirimkan ke invoker hingga semua tugas loop peristiwa selesai. Jika waktu fungsi habis, kesalahan akan dikembalikan. Anda dapat mengonfigurasi runtime untuk mengirim respons segera dengan menyetel [konteks.callbackWaitsForEmptyEventLoop](#) untuk palsu.

Fungsi panggilan balik memiliki dua argumen: `Error` dan respons. Objek respons harus kompatibel dengan `JSON.stringify`.

Example TypeScript fungsi dengan callback

Fungsi sampel ini menerima peristiwa dari Amazon API Gateway, mencatat peristiwa dan objek konteks, lalu mengembalikan respons ke API Gateway. Perhatikan hal berikut:

- Sebelum menggunakan kode ini dalam fungsi Lambda, Anda harus menambahkan paket [@types/aws-lambda](#) sebagai dependensi pengembangan. Paket ini berisi definisi tipe untuk Lambda. Ketika `@types/aws-lambda` diinstal, `import` pernyataan (`import ... from 'aws-lambda'`) mengimpor definisi tipe. Itu tidak mengimpor `aws-lambda` NPM paket, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub
- Handler dalam contoh ini adalah modul ES dan harus ditunjuk seperti itu di `package.json` file Anda atau dengan menggunakan ekstensi `.mjs` file. Untuk informasi lebih lanjut, lihat [Menunjuk penanganan fungsi sebagai modul ES](#).

```
import { Context, APIGatewayProxyCallback, APIGatewayEvent } from 'aws-lambda';

export const lambdaHandler = (event: APIGatewayEvent, context: Context, callback:
  APIGatewayProxyCallback): void => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  callback(null, {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  });
};
```

Menggunakan tipe untuk objek acara

Kami menyarankan agar Anda tidak menggunakan tipe [apa pun](#) untuk argumen handler dan tipe pengembalian karena Anda kehilangan kemampuan untuk memeriksa tipe. [Sebagai gantinya, buat acara menggunakan AWS Serverless Application Model CLI perintah `sam local generate-event`, atau gunakan definisi sumber terbuka dari paket `@types/aws-lambda`.](#)

Menghasilkan acara menggunakan perintah `sam local generate-event`

1. Buat acara proxy Amazon Simple Storage Service (Amazon S3).

```
sam local generate-event s3 put >> S3PutEvent.json
```

2. Gunakan [utilitas quicktype](#) untuk menghasilkan definisi tipe dari file S3 PutEvent .json.

```
npm install -g quicktype
quicktype S3PutEvent.json -o S3PutEvent.ts
```

3. Gunakan jenis yang dihasilkan dalam kode Anda.

```
import { S3PutEvent } from './S3PutEvent';

export const lambdaHandler = async (event: S3PutEvent): Promise<void> => {
  event.Records.map((record) => console.log(record.s3.object.key));
};
```

Membuat acara menggunakan definisi sumber terbuka dari paket `@types/aws-lambda`

1. Tambahkan paket [@types/aws-lambda](#) sebagai dependensi pengembangan.

```
npm install -D @types/aws-lambda
```

2. Gunakan jenis dalam kode Anda.

```
import { S3Event } from "aws-lambda";

export const lambdaHandler = async (event: S3Event): Promise<void> => {
  event.Records.map((record) => console.log(record.s3.object.key));
};
```

Praktik terbaik kode untuk fungsi Lambda TypeScript

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji. Dalam Node.js, ini mungkin terlihat seperti:

```
exports.myHandler = function(event, context, callback) {
  var foo = event.foo;
  var bar = event.bar;
  var result = MyLambdaFunction (foo, bar);

  callback(null, result);
}

function MyLambdaFunction (foo, bar) {
  // MyLambdaFunction logic here
}
```

- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk runtime Node.js dan Python, ini termasuk file. AWS SDKs Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi.
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Terapkan TypeScript kode yang ditranspilasikan di Lambda dengan arsip file.zip

Sebelum Anda dapat menerapkan TypeScript kode ke AWS Lambda, Anda perlu mentranspilasikannya menjadi JavaScript. Halaman ini menjelaskan tiga cara untuk membangun dan menyebarkan TypeScript kode ke Lambda dengan arsip file.zip:

- [Menggunakan AWS Serverless Application Model \(AWS SAM\)](#)
- [Menggunakan AWS Cloud Development Kit \(AWS CDK\)](#)
- [Menggunakan AWS Command Line Interface \(AWS CLI\) dan esbuild](#)

AWS SAM dan AWS CDK menyederhanakan fungsi membangun dan menyebarkan TypeScript. [Spesifikasi AWS SAM template](#) menyediakan sintaks sederhana dan bersih untuk menggambarkan fungsi Lambda, API, izin, konfigurasi, dan peristiwa yang membentuk aplikasi tanpa server Anda. Ini [AWS CDK](#) memungkinkan Anda membangun aplikasi yang andal, terukur, dan hemat biaya di cloud dengan kekuatan ekspresif yang cukup besar dari bahasa pemrograman. AWS CDK ini ditujukan untuk AWS pengguna yang cukup hingga sangat berpengalaman. Baik esbuild AWS CDK dan AWS SAM use untuk mentranspile TypeScript kode menjadi JavaScript.

Menggunakan AWS SAM untuk menyebarkan TypeScript kode ke Lambda

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World menggunakan TypeScript aplikasi Hello World. AWS SAM Aplikasi ini mengimplementasikan backend API dasar. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Ketika Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda dipanggil. Fungsi mengembalikan hello world pesan.

Note

AWS SAM menggunakan esbuild untuk membuat fungsi Lambda Node.js TypeScript dari kode. Dukungan esbuild saat ini dalam pratinjau publik. Selama pratinjau publik, dukungan esbuild mungkin mengalami perubahan yang tidak kompatibel ke belakang.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#)
- Node.js 18.x

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan TypeScript template Hello World.

```
sam init --app-template hello-world-typescript --name sam-app --package-type Zip --runtime nodejs18.x
```

2. [\(Opsional\) Aplikasi sampel mencakup konfigurasi untuk alat yang umum digunakan, seperti ESLint untuk linting kode dan Jest untuk pengujian unit.](#) Untuk menjalankan perintah lint dan test:

```
cd sam-app/hello-world
npm install
npm run lint
npm run test
```

3. Bangun aplikasi.

```
cd sam-app
sam build
```

4. Terapkan aplikasi.

```
sam deploy --guided
```

5. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, respons dengan `Enter`.
6. Output menunjukkan titik akhir untuk REST API. Buka titik akhir di browser untuk menguji fungsinya. Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Menggunakan TypeScript kode AWS CDK untuk menyebarkan ke Lambda

Ikuti langkah-langkah di bawah ini untuk membangun dan menerapkan TypeScript aplikasi sampel menggunakan aplikasi. AWS CDK Aplikasi ini mengimplementasikan backend API dasar. Ini terdiri dari titik akhir API Gateway dan fungsi Lambda. Ketika Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda dipanggil. Fungsi mengembalikan `hello world` pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS CLI versi 2](#)
- [AWS CDK versi 2](#)
- Node.js 18.x
- [Baik Docker atau esbuild](#)

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world  
cd hello-world
```

2. Inisialisasi aplikasi.


```
cdk init app --language typescript
```

3. Tambahkan paket [@types/aws-lambda](#) sebagai dependensi pengembangan. Paket ini berisi definisi tipe untuk Lambda.

```
npm install -D @types/aws-lambda
```

4. Buka direktori `lib`. Anda akan melihat file bernama `hello-world-stack.ts`. Buat dua file baru di direktori ini: `hello-world.function.ts` dan `hello-world.ts`.

5. Buka `hello-world.function.ts` dan tambahkan kode berikut ke file. Ini adalah kode untuk fungsi Lambda.

 Note

`importPernyataan` mengimpor definisi tipe dari [@types /aws-lambda](#). Itu tidak mengimpor paket `aws-lambda` NPM, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
  Promise<APIGatewayProxyResult> => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

6. Buka `hello-world.ts` dan tambahkan kode berikut ke file. Ini berisi [NodejsFunction konstruksi](#), yang menciptakan fungsi Lambda, dan konstruksi, [LambdaRestApi yang](#) membuat REST API.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function');
    new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
  }
}
```


NodejsFunctionKonstruk mengasumsikan hal berikut secara default:

- Penangan fungsi Anda dipanggil handler.
- File.ts yang berisi kode fungsi (hello-world.function.ts) berada di direktori yang sama dengan file.ts yang berisi konstruksi (hello-world.ts). Konstruk menggunakan ID konstruksi (“hello-world”) dan nama file penangan Lambda (“fungsi”) untuk menemukan kode fungsi. Misalnya, jika kode fungsi Anda ada dalam file bernama hello-world.my-function.ts, file hello-world.ts harus mereferensikan kode fungsi seperti ini:

```
const helloFunction = new NodejsFunction(this, 'my-function');
```

Anda dapat mengubah perilaku ini dan mengonfigurasi parameter esbuild lainnya. Untuk informasi selengkapnya, lihat [Mengonfigurasi esbuild](#) di referensi AWS CDK API.

7. Buka hello-world-stack.ts. Ini adalah kode yang mendefinisikan [AWS CDK tumpukan](#) Anda. Ganti kode dengan yang berikut:

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

8. dari hello-world direktori yang berisi cdk.json file Anda, terapkan aplikasi Anda.

```
cdk deploy
```

9. AWS CDK Membangun dan mengemas fungsi Lambda menggunakan esbuild, lalu menerapkan fungsi tersebut ke runtime Lambda. Output menunjukkan titik akhir untuk REST API. Buka titik akhir di browser untuk menguji fungsinya. Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

Menggunakan AWS CLI dan esbuild untuk menyebarkan TypeScript kode ke Lambda

Contoh berikut menunjukkan cara mentranspile dan menyebarkan kode TypeScript ke Lambda menggunakan esbuild dan. esbuild menghasilkan satu file dengan semua AWS CLI dependensi. JavaScript Ini adalah satu-satunya file yang perlu Anda tambahkan ke arsip.zip.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS CLI versi 2](#)
- Node.js 18.x
- [Peran eksekusi](#) untuk fungsi Lambda
- Untuk pengguna Windows, utilitas file zip seperti [7zip](#).

Menyebarkan fungsi sampel

1. Pada mesin lokal Anda, buat direktori proyek untuk fungsi baru Anda.
2. Buat proyek Node.js baru dengan npm atau manajer paket pilihan Anda.

```
npm init
```

3. Tambahkan paket [@types/aws-lambda](#) dan [esbuild](#) sebagai dependensi pengembangan. `@types/aws-lambda` Paket berisi definisi tipe untuk Lambda.

```
npm install -D @types/aws-lambda esbuild
```

4. Buat file baru bernama `index.ts`. Tambahkan kode berikut ke file baru. Ini adalah kode untuk fungsi Lambda. Fungsi mengembalikan `hello world` pesan. Fungsi ini tidak membuat sumber daya API Gateway apa pun.

Note

`importPernyataan` mengimpor definisi tipe dari [@types /aws-lambda](#). Itu tidak mengimpor paket `aws-lambda` NPM, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
  Promise<APIGatewayProxyResult> => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

5. Tambahkan skrip build ke file `package.json`. Ini mengonfigurasi `esbuild` untuk secara otomatis membuat paket penyebaran.zip. Untuk informasi selengkapnya, lihat [Membuat skrip](#) di dokumentasi `esbuild`.

Linux and MacOS

```
"scripts": {
  "prebuild": "rm -rf dist",
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
  target=es2020 --outfile=dist/index.js",
  "postbuild": "cd dist && zip -r index.zip index.js*"
},
```

Windows

Dalam contoh ini, "postbuild" perintah menggunakan utilitas [7zip](#) untuk membuat file.zip Anda. Gunakan utilitas zip Windows pilihan Anda sendiri dan modifikasi perintah seperlunya.

```
"scripts": {
  "prebuild": "del /q dist",
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --target=es2020 --outfile=dist/index.js",
  "postbuild": "cd dist && 7z a -tzip index.zip index.js*"
},
```

6. Bangun paketnya.

```
npm run build
```

7. Buat fungsi Lambda menggunakan paket.zip deployment. Ganti teks yang disorot dengan Amazon Resource Name (ARN) dari peran [eksekusi](#) Anda.

```
aws lambda create-function --function-name hello-world --runtime "nodejs18.x" --role arn:aws:iam::123456789012:role/lambda-ex --zip-file "fileb://dist/index.zip" --handler index.handler
```

8. [Jalankan acara uji](#) untuk mengonfirmasi bahwa fungsi mengembalikan respons berikut. Jika Anda ingin menjalankan fungsi ini menggunakan API Gateway, [buat dan konfigurasi REST API](#).

```
{
  "statusCode": 200,
  "body": "{\"message\":\"hello world\"}"
}
```

Terapkan TypeScript kode yang ditranspilasikan di Lambda dengan gambar wadah

Anda dapat menerapkan TypeScript kode Anda ke AWS Lambda fungsi sebagai [gambar container](#) Node.js. AWS menyediakan [gambar dasar](#) untuk Node.js untuk membantu Anda membangun image container. Gambar dasar ini dimuat sebelumnya dengan runtime bahasa dan komponen lain yang diperlukan untuk menjalankan gambar di Lambda. AWS menyediakan Dockerfile untuk setiap gambar dasar untuk membantu membangun gambar container Anda.

Jika Anda menggunakan image basis komunitas atau perusahaan pribadi, Anda harus [menambahkan Node.js runtime interface client \(RIC\)](#) ke image dasar agar kompatibel dengan Lambda.

Lambda menyediakan emulator antarmuka runtime untuk pengujian lokal. Gambar AWS dasar untuk Node.js menyertakan emulator antarmuka runtime. Jika Anda menggunakan gambar dasar alternatif, seperti gambar Alpine Linux atau Debian, Anda dapat [membangun emulator ke dalam gambar Anda](#) atau [menginstalnya di mesin lokal Anda](#).

Menggunakan image dasar Node.js untuk membangun dan mengemas kode TypeScript fungsi

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#)
- Node.js 20.x

Membuat gambar dari gambar dasar

Untuk membuat gambar dari gambar AWS dasar untuk Lambda

1. Pada mesin lokal Anda, buat direktori proyek untuk fungsi baru Anda.
2. Buat proyek Node.js baru dengan npm atau manajer paket pilihan Anda.

```
npm init
```

3. Tambahkan paket [@types /aws-lambda](#) dan [esbuild](#) sebagai dependensi pengembangan. `@types/aws-lambda` Paket berisi definisi tipe untuk Lambda.

```
npm install -D @types/aws-lambda esbuild
```

4. Tambahkan [skrip build](#) ke `package.json` file.

```
"scripts": {
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --target=es2020 --outfile=dist/index.js"
}
```

5. Buat file baru bernama `index.ts`. Tambahkan kode contoh berikut ke file baru. Ini adalah kode untuk fungsi Lambda. Fungsi mengembalikan `hello world` pesan.

Note

`import` Pernyataan mengimpor definisi tipe dari [@types /aws-lambda](#). Itu tidak mengimpor `aws-lambda` NPM paket, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
  Promise<APIGatewayProxyResult> => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

6. Buat Dockerfile baru dengan konfigurasi berikut:

- Atur `FROM` properti ke URI gambar dasar.

- Atur argumen CMD untuk menentukan handler fungsi Lambda.

Contoh berikut Dockerfile menggunakan build multi-tahap. Langkah pertama mentransformasikan TypeScript kode ke dalam JavaScript. Langkah kedua menghasilkan gambar kontainer yang hanya berisi JavaScript file dan dependensi produksi.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/nodejs:20 as builder
WORKDIR /usr/app
COPY package.json index.ts ./
RUN npm install
RUN npm run build

FROM public.ecr.aws/lambda/nodejs:20
WORKDIR ${LAMBDA_TASK_ROOT}
COPY --from=builder /usr/app/dist/* ./
CMD ["index.handler"]
```

7. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

1. Mulai gambar Docker dengan perintah `docker run`. Dalam contoh ini, `docker-image` adalah nama gambar dan `test` tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

2. Dari jendela terminal baru, posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d  
'{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/  
invocations" -Method Post -Body '{}' -ContentType "application/json"
```


Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

3. Dapatkan ID kontainer.

```
docker ps
```

4. Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECRRepository Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repository Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoriURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhirURI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di AmazonECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi TypeScript

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Metode konteks

- `getRemainingTimeInMillis()` – Mengembalikan jumlah milidetik yang tersisa sebelum waktu eksekusi habis.

Properti konteks

- `functionName` – Nama fungsi Lambda.
- `functionVersion` – [Versi](#) fungsi.
- `invokedFunctionArn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `memoryLimitInMB` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `awsRequestId` – Pengidentifikasi permintaan invokasi.
- `logGroupName` – Grup log untuk fungsi.
- `logStreamName` – Aliran log untuk instans fungsi.
- `identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
 - `cognitoIdentityId` – Identitas Amazon Cognito terautentikasi.
 - `cognitoIdentityPoolId` – Kumpulan identitas Amazon Cognito yang mengesahkan invokasi.
- `clientContext` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
 - `client.installation_id`
 - `client.app_title`
 - `client.app_version_name`
 - `client.app_version_code`
 - `client.app_package_name`

- `env.platform_version`
 - `env.platform`
 - `env.make`
 - `env.model`
 - `env.locale`
 - Custom – Nilai kustom yang ditetapkan oleh aplikasi klien.
- `callbackWaitsForEmptyEventLoop` – Atur ke salah untuk mengirimkan jawaban segera saat [panggilan balik](#) berjalan, alih-alih menunggu loop peristiwa Node.js kosong. Jika ini salah, semua peristiwa yang belum selesai akan terus berjalan selama invokasi berikutnya.

Anda dapat menggunakan paket [@types /aws-lambda](#) npm untuk bekerja dengan objek konteks.

Example file `index.ts`

Contoh fungsi berikut mencatat informasi konteks dan mengembalikan lokasi log.

Note

Sebelum menggunakan kode ini dalam fungsi Lambda, Anda harus menambahkan paket [@types /aws-lambda](#) sebagai dependensi pengembangan. Paket ini berisi definisi tipe untuk Lambda. Ketika `@types/aws-lambda` diinstal, `import` pernyataan (`import ... from 'aws-lambda'`) mengimpor definisi tipe. Itu tidak mengimpor `aws-lambda` NPM paket, yang merupakan alat pihak ketiga yang tidak terkait. Untuk informasi selengkapnya, lihat [aws-lambda](#) di repositori. DefinitelyTyped GitHub

```
import { Context } from 'aws-lambda';
export const lambdaHandler = async (event: string, context: Context): Promise<string>
=> {
  console.log('Remaining time: ', context.getRemainingTimeInMillis());
  console.log('Function name: ', context.functionName);
  return context.logStreamName;
};
```

Log dan pantau fungsi TypeScript Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda dan mengirim entri log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap pemanggilan dan output lainnya dari kode fungsi Anda ke aliran log. Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Untuk mengeluarkan log dari kode fungsi Anda, Anda dapat menggunakan metode pada [objek konsol](#). Untuk pencatatan yang lebih rinci, Anda dapat menggunakan pustaka logging apa pun yang menulis ke `stdout` atau `stderr`.

Bagian-bagian

- [Menggunakan alat logging dan pustaka](#)
- [Menggunakan Powertools for AWS Lambda \(TypeScript\) dan AWS SAM untuk logging terstruktur](#)
- [Menggunakan Powertools for AWS Lambda \(TypeScript\) dan AWS CDK untuk logging terstruktur](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)

Menggunakan alat logging dan pustaka

[Powertools for AWS Lambda \(TypeScript\)](#) adalah toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang. [Utilitas Logger menyediakan logger](#) yang dioptimalkan Lambda yang mencakup informasi tambahan tentang konteks fungsi di semua fungsi Anda dengan output terstruktur sebagai JSON. Gunakan utilitas ini untuk melakukan hal berikut:

- Tangkap bidang kunci dari konteks Lambda, cold start, dan struktur logging output sebagai JSON
- Log peristiwa pemanggilan Lambda saat diinstruksikan (dinonaktifkan secara default)
- Cetak semua log hanya untuk persentase pemanggilan melalui pengambilan sampel log (dinonaktifkan secara default)
- Tambahkan kunci tambahan ke log terstruktur kapan saja
- Gunakan pemformat log kustom (Bring Your Own Formatter) untuk mengeluarkan log dalam struktur yang kompatibel dengan RFC Logging organisasi Anda

Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS SAM untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh TypeScript aplikasi Hello World dengan modul [Powertools for AWS Lambda \(TypeScript\)](#) terintegrasi menggunakan modul. AWS SAM Aplikasi ini mengimplementasikan backend API dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan `hello world` pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Node.js 18.x atau yang lebih baru
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75](#) atau yang lebih baru. Jika Anda memiliki versi CLI yang lebih lama, lihat [Memutakhirkan AWS SAM CLI. AWS SAM](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan TypeScript template Hello World.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs18.x
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan URL aplikasi yang digunakan:

```
aws cloudformation describe-stacks --stack-name sam-app --query
'Stacks[0].Outputs[?OutputKey=='HelloWorldApi'].OutputValue' --output text
```

6. Memanggil titik akhir API:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name sam-app
```

Output log terlihat seperti ini:

```
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.552000
START RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Version: $LATEST
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.594000
2022-08-31T09:33:10.557Z 70693159-7e94-4102-a2af-98a6343fb8fb
INFO {"_aws":{"Timestamp":1661938390556,"CloudWatchMetrics":
[{"Namespace":"sam-app","Dimensions":[["service"]],"Metrics":
[{"Name":"ColdStart","Unit":"Count"}]}]},"service":"helloWorld","ColdStart":1}
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.595000
2022-08-31T09:33:10.595Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
{"level":"INFO","message":"This is an INFO log - sending HTTP 200 - hello world
response","service":"helloWorld","timestamp":"2022-08-31T09:33:10.594Z"}
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.655000
2022-08-31T09:33:10.655Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
{"_aws":{"Timestamp":1661938390655,"CloudWatchMetrics":[{"Namespace":"sam-
app","Dimensions":[["service"]],"Metrics":[]]}]},"service":"helloWorld"}
```

```
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.754000 END
RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.754000
REPORT RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Duration: 201.55 ms Billed
Duration: 202 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration: 252.42
ms
XRAY TraceId: 1-630f2ad5-1de22b6d29a658a466e7ecf5 SegmentId: 567c116658fbf11a
Sampled: true
```

- Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Mengelola retensi log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log tanpa batas waktu, hapus grup log, atau konfigurasi periode retensi setelah itu secara CloudWatch otomatis menghapus log. Untuk mengatur penyimpanan log, tambahkan yang berikut ini ke AWS SAM templat Anda:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS CDK untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh TypeScript aplikasi Hello World dengan modul [Powertools for AWS Lambda \(TypeScript\)](#) terintegrasi menggunakan modul. AWS CDK Aplikasi ini mengimplementasikan backend API dasar dan

menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan `hello world` pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Node.js 18.x atau yang lebih baru
- [AWS CLI versi 2](#)
- [AWS CDK versi 2](#)
- [AWS SAM CLI versi 1.75](#) atau yang lebih baru. Jika Anda memiliki versi CLI yang lebih lama, lihat [Memutakhirkan AWS SAM CLI. AWS SAM](#)

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world
cd hello-world
```

2. Inisialisasi aplikasi.

```
cdk init app --language typescript
```

3. Tambahkan paket [@types /aws-lambda](#) sebagai dependensi pengembangan.

```
npm install -D @types/aws-lambda
```

4. Instal utilitas Powertools [Logger](#).

```
npm install @aws-lambda-powertools/logger
```

5. Buka direktori `lib`. Anda akan melihat file bernama `hello-world-stack.ts`. Buat dua file baru di direktori ini: `hello-world.function.ts` dan `hello-world.ts`.
6. Buka `hello-world.function.ts` dan tambahkan kode berikut ke file. Ini adalah kode untuk fungsi Lambda.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Logger } from '@aws-lambda-powertools/logger';
const logger = new Logger();

export const handler = async (event: APIGatewayEvent, context: Context):
Promise<APIGatewayProxyResult> => {
  logger.info('This is an INFO log - sending HTTP 200 - hello world response');
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

7. Buka `hello-world.ts` dan tambahkan kode berikut ke file. Ini berisi [NodejsFunction konstruksi](#), yang membuat fungsi Lambda, mengonfigurasi variabel lingkungan untuk Powertools, dan menetapkan retensi log menjadi satu minggu. Ini juga mencakup [LambdaRestApi konstruksi](#), yang menciptakan REST API.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { RetentionDays } from 'aws-cdk-lib/aws-logs';
import { CfnOutput } from 'aws-cdk-lib';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        Powertools_SERVICE_NAME: 'helloWorld',
        LOG_LEVEL: 'INFO',
      },
      logRetention: RetentionDays.ONE_WEEK,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}
```

```
});  
}  
}
```

8. Buka `hello-world-stack.ts`. Ini adalah kode yang mendefinisikan [AWS CDK tumpukan](#) Anda. Ganti kode dengan yang berikut ini:

```
import { Stack, StackProps } from 'aws-cdk-lib';  
import { Construct } from 'constructs';  
import { HelloWorld } from './hello-world';  
  
export class HelloWorldStack extends Stack {  
  constructor(scope: Construct, id: string, props?: StackProps) {  
    super(scope, id, props);  
    new HelloWorld(this, 'hello-world');  
  }  
}
```

9. Kembali ke direktori proyek.

```
cd hello-world
```

10. Men-deploy aplikasi Anda.

```
cdk deploy
```

11. Dapatkan URL aplikasi yang digunakan:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query  
'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

12. Memanggil titik akhir API:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

13. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name HelloWorldStack
```

Output log terlihat seperti ini:

```
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.047000
  START RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Version: $LATEST
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.050000 {
  "level": "INFO",
  "message": "This is an INFO log - sending HTTP 200 - hello world response",
  "service": "helloWorld",
  "timestamp": "2022-08-31T14:48:37.048Z",
  "xray_trace_id": "1-630f74c4-2b080cf77680a04f2362bcf2"
}
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.082000 END
  RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.082000
  REPORT RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Duration: 34.60 ms Billed
  Duration: 35 ms Memory Size: 128 MB Max Memory Used: 57 MB Init Duration: 173.48
  ms
```

- Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
cdk destroy
```

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (/aws/lambda/ ***your-function-name***).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, kami sarankan untuk menginstrumentasi fungsi Anda dengan [AWS X-Ray](#). X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Menelusuri TypeScript kode di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari tiga SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK untuk Node.js](#) — An SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.
- [Powertools for AWS Lambda \(TypeScript\)](#) — Toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh. AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray. SDKs](#)

Bagian-bagian

- [Menggunakan Powertools for AWS Lambda \(TypeScript\) dan AWS SAM untuk tracing](#)
- [Menggunakan Powertools for AWS Lambda \(TypeScript\) dan AWS CDK for tracing](#)
- [Menafsirkan jejak X-Ray](#)

Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS SAM untuk tracing

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh TypeScript aplikasi Hello World dengan modul [Powertools for AWS Lambda \(TypeScript\)](#) terintegrasi menggunakan modul. AWS SAM Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan `hello world` pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Node.js 18.x atau yang lebih baru
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan file. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan TypeScript template Hello World.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs18.x --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name sam-app --query  
'Stacks[0].Outputs[?OutputKey=='HelloWorldApi'].OutputValue' --output text
```

6. Memanggil titik API akhir:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

```
XRay Event [revision 1] at (2023-01-31T11:29:40.527000) with id  
(1-11a2222-111a222222cb33de3b95daf9) and duration (0.483s)  
- 0.425s - sam-app/Prod [HTTP: 200]  
- 0.422s - Lambda [HTTP: 200]  
- 0.406s - sam-app-HelloWorldFunction-XYZv11a1bcde [HTTP: 200]  
- 0.172s - sam-app-HelloWorldFunction-XYZv11a1bcde  
- 0.179s - Initialization  
- 0.112s - Invocation  
- 0.052s - ## app.lambdaHandler  
- 0.001s - ### MySubSegment  
- 0.059s - Overhead
```

8. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Menggunakan Powertools for AWS Lambda (TypeScript) dan AWS CDK for tracing

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh TypeScript aplikasi Hello World dengan modul [Powertools for AWS Lambda \(TypeScript\)](#) terintegrasi menggunakan modul. AWS CDK Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan `hello world` pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Node.js 18.x atau yang lebih baru
- [AWS CLI versi 2](#)
- [AWS CDK versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan file. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS Cloud Development Kit (AWS CDK)

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world
```

```
cd hello-world
```

2. Inisialisasi aplikasi.

```
cdk init app --language typescript
```

3. Tambahkan paket [@types /aws-lambda](#) sebagai dependensi pengembangan.

```
npm install -D @types/aws-lambda
```

4. Instal utilitas Powertools [Tracer](#).

```
npm install @aws-lambda-powertools/tracer
```

5. Buka direktori lib. Anda akan melihat file bernama hello-world-stack.ts. Buat dua file baru di direktori ini: hello-world.function.ts dan hello-world.ts.

6. Buka hello-world.function.ts dan tambahkan kode berikut ke file. Ini adalah kode untuk fungsi Lambda.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Tracer } from '@aws-lambda-powertools/tracer';
const tracer = new Tracer();

export const handler = async (event: APIGatewayEvent, context: Context):
  Promise<APIGatewayProxyResult> => {
  // Get facade segment created by Lambda
  const segment = tracer.getSegment();

  // Create subsegment for the function and set it as active
  const handlerSegment = segment.addNewSubsegment(`## ${process.env._HANDLER}`);
  tracer.setSegment(handlerSegment);

  // Annotate the subsegment with the cold start and serviceName
  tracer.annotateColdStart();
  tracer.addServiceNameAnnotation();

  // Add annotation for the awsRequestId
  tracer.putAnnotation('awsRequestId', context.awsRequestId);
  // Create another subsegment and set it as active
  const subsegment = handlerSegment.addNewSubsegment('### MySubSegment');
  tracer.setSegment(subsegment);
  let response: APIGatewayProxyResult = {
```

```

    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  });
// Close subsegments (the Lambda one is closed automatically)
subsegment.close(); // (### MySubSegment)
handlerSegment.close(); // (## index.handler)

// Set the facade segment as active again (the one created by Lambda)
tracer.setSegment(segment);
return response;
};

```

7. Buka `hello-world.ts` dan tambahkan kode berikut ke file. Ini berisi [NodejsFunction konstruksi](#), yang membuat fungsi Lambda, mengonfigurasi variabel lingkungan untuk Powertools, dan menetapkan retensi log menjadi satu minggu. Ini juga termasuk [LambdaRestApi konstruksi](#), yang menciptakan REST API

```

import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { CfnOutput } from 'aws-cdk-lib';
import { Tracing } from 'aws-cdk-lib/aws-lambda';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        POWERTOOLS_SERVICE_NAME: 'helloWorld',
      },
      tracing: Tracing.ACTIVE,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}

```

8. Buka `hello-world-stack.ts`. Ini adalah kode yang mendefinisikan [AWS CDK tumpukan](#) Anda. Ganti kode dengan yang berikut ini:

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

9. Men-deploy aplikasi Anda.

```
cd ..
cdk deploy
```

10. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

11. Memanggil titik API akhir:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

12. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

```
XRay Event [revision 1] at (2023-01-31T11:50:06.997000) with id
(1-11a2222-111a222222cb33de3b95daf9) and duration (0.449s)
- 0.350s - HelloWorldStack-helloworldfunction111A2BCD-XYZv11a1bcde [HTTP: 200]
```

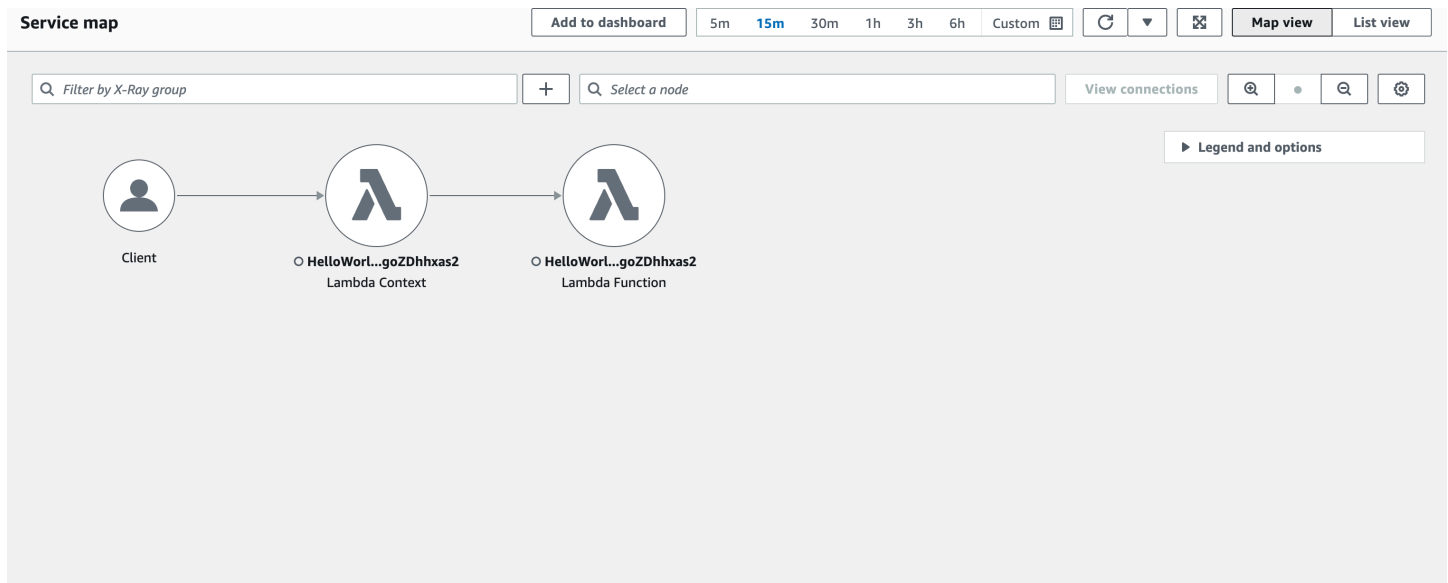
```
- 0.157s - HelloWorldStack-helloworldfunction111A2BCD-XYZv11a1bcde
- 0.169s - Initialization
- 0.058s - Invocation
  - 0.055s - ## index.handler
    - 0.000s - ### MySubSegment
- 0.099s - Overhead
```

13. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
cdk destroy
```

Menafsirkan jejak X-Ray

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Peta jejak X-Ray](#) memberikan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan jejak dari aplikasi sampel:



Membangun fungsi Lambda dengan Python

Anda bisa menjalankan kode Python di AWS Lambda. Lambda menyediakan [runtime](#) untuk Python yang menjalankan kode Anda untuk memproses peristiwa. Kode Anda berjalan di lingkungan yang menyertakan SDK untuk Python (Boto3), dengan kredensi dari peran AWS Identity and Access Management (IAM) yang Anda kelola. Untuk mempelajari lebih lanjut tentang SDK versi yang disertakan dengan runtime Python, lihat. [the section called “Versi yang disertakan runtime SDK”](#)

Lambda mendukung runtime Python berikut.

Python

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------|------------------|-------------------|---------------------|-------------------|-----------------------|
| Python 3.12 | python3.12 | Amazon Linux 2023 | | | |
| Python 3.11 | python3.11 | Amazon Linux 2 | | | |
| Python 3.10 | python3.10 | Amazon Linux 2 | | | |
| Python 3.9 | python3.9 | Amazon Linux 2 | | | |
| Python 3.8 | python3.8 | Amazon Linux 2 | Okt 14, 2024 | Februari 28, 2025 | Mar 31, 2025 |

Untuk membuat fungsi Python

1. Buka [Konsol Lambda](#).
2. Pilih Buat fungsi.
3. Konfigurasi pengaturan berikut:
 - Nama fungsi: Masukkan nama untuk fungsi tersebut.
 - Runtime: Pilih Python 3.12.

4. Pilih Buat fungsi.
5. Untuk mengonfigurasi peristiwa uji, pilih Uji.
6. Untuk Nama peristiwa, masukkan **test**.
7. Pilih Simpan perubahan.
8. Untuk mengaktifkan fungsi, pilih Uji.

Konsol membuat fungsi Lambda dengan satu file sumber bernama `lambda_function`. Anda dapat mengedit file ini dan menambahkan lebih banyak file di editor kode bawaan. Untuk menyimpan perubahan Anda, pilih Simpan. Selanjutnya, untuk menjalankan kode, pilih Uji.

Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log. Fungsi runtime mengirimkan detail tentang setiap pemanggilan ke Log. CloudWatch Detail tersebut menyampaikan [log yang dihasilkan fungsi Anda](#) selama invokasi. Jika fungsi mengembalikan kesalahan, Lambda memformat kesalahan dan mengembalikannya ke pemanggil.

Topik

- [Versi yang disertakan runtime SDK](#)
- [Format respons](#)
- [Shutdown anggun untuk ekstensi](#)
- [Tentukan penanganan fungsi Lambda dengan Python](#)
- [Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#)
- [Deploy fungsi Lambda Python dengan gambar kontainer](#)
- [Bekerja dengan lapisan untuk fungsi Lambda Python](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Python](#)
- [Log dan pantau fungsi Python Lambda](#)
- [AWS Lambdapengujian fungsi dengan Python](#)
- [Menginstrumentasi kode Python di AWS Lambda](#)

Versi yang disertakan runtime SDK

Versi yang AWS SDK disertakan dalam runtime Python tergantung pada versi runtime dan versi Anda. Wilayah AWS Untuk menemukan versi yang SDK disertakan dalam runtime yang Anda gunakan, buat fungsi Lambda dengan kode berikut.

```
import boto3
import botocore

def lambda_handler(event, context):
    print(f'boto3 version: {boto3.__version__}')
    print(f'botocore version: {botocore.__version__}')
```

Format respons

Dalam Python 3.12 dan runtime Python yang lebih baru, fungsi mengembalikan karakter Unicode sebagai bagian dari responsnya. JSON Runtime Python sebelumnya mengembalikan urutan yang diloloskan untuk karakter Unicode dalam tanggapan. Misalnya, dalam Python 3.11, jika Anda mengembalikan string Unicode seperti "こんにちは", itu lolos dari karakter Unicode dan mengembalikan "\ u3053\ u3093\ u306b\ u3061\ u306f". Runtime Python 3.12 mengembalikan yang asli "". こんにちは

Menggunakan respons Unicode mengurangi ukuran respons Lambda, membuatnya lebih mudah untuk memasukkan respons yang lebih besar ke dalam ukuran muatan maksimum 6 MB untuk fungsi sinkron. Pada contoh sebelumnya, versi escaped adalah 32 byte — dibandingkan dengan 17 byte dengan string Unicode.

Saat Anda meningkatkan ke Python 3.12, Anda mungkin perlu menyesuaikan kode Anda untuk memperhitungkan format respons baru. Jika pemanggil mengharapkan Unicode lolos, Anda harus menambahkan kode ke fungsi kembali untuk melarikan diri dari Unicode secara manual, atau menyesuaikan pemanggil untuk menangani pengembalian Unicode.

Shutdown anggun untuk ekstensi

[Python 3.12 dan runtime Python yang lebih baru menawarkan kemampuan shutdown anggun yang ditingkatkan untuk fungsi dengan ekstensi eksternal.](#) Ketika Lambda mematikan lingkungan eksekusi, Lambda mengirimkan SIGTERM sinyal ke runtime dan kemudian SHUTDOWN acara ke setiap ekstensi eksternal terdaftar. Anda dapat menangkap SIGTERM sinyal dalam fungsi Lambda Anda dan membersihkan sumber daya seperti koneksi database yang dibuat oleh fungsi tersebut.

Untuk mempelajari lebih lanjut tentang siklus hidup lingkungan eksekusi, lihat. [Memahami siklus hidup lingkungan eksekusi Lambda](#) Untuk contoh cara menggunakan shutdown anggun dengan ekstensi, lihat Repositori [AWS Sampel GitHub](#) .

Tentukan penanganan fungsi Lambda dengan Python

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Anda dapat menggunakan sintaksis umum berikut ketika membuat handler fungsi di Python:

```
def handler_name(event, context):  
    ...  
    return some_value
```

Topik

- [Penamaan](#)
- [Cara kerjanya](#)
- [Mengembalikan nilai](#)
- [Contoh](#)
- [Praktik terbaik kode untuk fungsi Lambda Python](#)

Penamaan

Nama handler fungsi Lambda yang ditentukan pada saat Anda membuat fungsi Lambda berasal dari berikut ini:

- Nama file tempat fungsi handler Lambda berada.
- Nama fungsi handler Python.

Handler fungsi dapat berupa nama apa saja; Namun, nama default di konsol Lambda adalah `lambda_function.lambda_handler`. Nama handler fungsi ini mencerminkan nama fungsi (`lambda_handler`) dan file tempat kode handler disimpan (`lambda_function.py`).

Jika Anda membuat fungsi di konsol menggunakan nama file atau nama pengendali fungsi yang berbeda, Anda harus mengedit nama handler default.

Untuk mengubah nama fungsi handler (konsol)

1. Buka halaman [Fungsi](#) di konsol Lambda dan pilih fungsi Anda.

2. Pilih tab Kode.
3. Gulir ke bawah ke panel pengaturan Runtime dan pilih Edit.
4. Di Handler, masukkan nama baru untuk handler fungsi Anda.
5. Pilih Simpan.

Cara kerjanya

Ketika Lambda memanggil handler fungsi Anda, [Runtime Lambda](#) meneruskan dua argumen ke handler fungsi:

- Argumen pertama adalah [objek peristiwa](#). Peristiwa adalah dokumen JSON berformat yang berisi data untuk fungsi Lambda untuk diproses. [Runtime Lambda](#) mengonversi peristiwa menjadi objek dan menyampaikannya ke kode fungsi Anda. Ini biasanya dari jenis `dict` Python. Ini juga dapat bertipe `list`, `str`, `int`, `float`, atau `NoneType`.

Objek peristiwa berisi informasi dari layanan invokasi. Saat Anda mengaktifkan fungsi, Anda menentukan struktur dan konten peristiwa. Ketika AWS layanan memanggil fungsi Anda, layanan mendefinisikan struktur acara. Untuk informasi selengkapnya tentang acara dari AWS layanan, lihat [Memanggil Lambda dengan acara dari layanan lain AWS](#).

- Argumen kedua adalah [objek konteks](#). Objek konteks diteruskan ke fungsi Anda dengan Lambda saat runtime. Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan lingkungan runtime.

Mengembalikan nilai

Handler dapat mengembalikan nilai secara opsional. Apa yang terjadi pada nilai yang dikembalikan tergantung pada [jenis pemanggilan](#) dan [layanan](#) yang memanggil fungsi. Sebagai contoh:

- Jika Anda menggunakan jenis `RequestResponse` pemanggilan, seperti [Memanggil fungsi Lambda secara sinkron](#), AWS Lambda mengembalikan hasil panggilan fungsi Python ke klien yang menjalankan fungsi Lambda (sebagai HTTP respons terhadap permintaan pemanggilan, diserialisasikan ke dalam). JSON Misalnya, konsol AWS Lambda menggunakan tipe invokasi `RequestResponse`, jadi ketika Anda melakukan invokasi fungsi menggunakan konsol, konsol akan menampilkan nilai yang dikembalikan.
- Jika penanganan mengembalikan objek yang tidak dapat diserialkan `json.dumps`, waktu pengoperasian akan mengembalikan kesalahan.

- Jika penanganan mengembalikan None, sebagaimana fungsi Python tanpa pernyataan `return` yang dilakukan secara implisit, hasil waktu pengoperasian akan mengembalikan `null`.
- Jika Anda menggunakan tipe Event pemanggilan (pemanggilan [asinkron](#)), [nilainya akan dibuang](#).

Note

Dalam Python 3.9 dan rilis yang lebih baru, Lambda menyertakan pemanggilan dalam `requestId` respons kesalahan.

Contoh

Bagian berikut menunjukkan contoh fungsi Python yang dapat Anda gunakan dengan Lambda. Jika Anda menggunakan konsol Lambda untuk membuat fungsi, Anda tidak perlu melampirkan [file arsip .zip](#) untuk menjalankan fungsi di bagian ini. Fungsi ini menggunakan pustaka Python standar yang disertakan dengan runtime Lambda yang Anda pilih. Untuk informasi selengkapnya, lihat [???](#).

Mengembalikan pesan

Contoh berikut menunjukkan fungsi yang disebut `lambda_handler`. Fungsi ini menerima input pengguna dari nama depan dan belakang, serta mengembalikan pesan yang berisi data dari peristiwa yang diterima sebagai input.

```
def lambda_handler(event, context):
    message = 'Hello {} {}!'.format(event['first_name'], event['last_name'])
    return {
        'message' : message
    }
```

Anda dapat menggunakan data peristiwa berikut untuk memanggil fungsi:

```
{
  "first_name": "John",
  "last_name": "Smith"
}
```

Respons menunjukkan data peristiwa yang diteruskan sebagai input:

```
{
  "message": "Hello John Smith!"
}
```

Menguraikan respons

Contoh berikut menunjukkan fungsi yang disebut `lambda_handler`. Fungsi ini menggunakan data peristiwa yang diteruskan oleh Lambda pada saat runtime. Ini [mem-parsing variabel lingkungan](#) yang `AWS_REGION` dikembalikan dalam JSON respons.

```
import os
import json

def lambda_handler(event, context):
    json_region = os.environ['AWS_REGION']
    return {
        "statusCode": 200,
        "headers": {
            "Content-Type": "application/json"
        },
        "body": json.dumps({
            "Region ": json_region
        })
    }
```

Anda dapat menggunakan data peristiwa berikut untuk memanggil fungsi:

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```

Runtime Lambda menetapkan beberapa variabel lingkungan selama permulaan. Untuk informasi selengkapnya tentang variabel lingkungan yang dikembalikan dalam respons saat runtime, lihat [Gunakan variabel lingkungan Lambda untuk mengonfigurasi nilai dalam kode](#).

Fungsi dalam contoh ini tergantung pada respon yang berhasil (in200) dari `InvokeAPI`. Untuk informasi selengkapnya tentang API status Panggilan, lihat Sintaks [Respons Panggilan](#).

Mengembalikan perhitungan

Contoh berikut menunjukkan fungsi yang disebut `lambda_handler`. Fungsi ini menerima input pengguna dan mengembalikan perhitungan kepada pengguna. Untuk informasi selengkapnya tentang contoh ini, lihat [aws-doc-sdk-examples GitHub repositori](#).

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):
    ...
    result = None
    action = event.get('action')
    if action == 'increment':
        result = event.get('number', 0) + 1
        logger.info('Calculated result of %s', result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {'result': result}
    return response
```

Anda dapat menggunakan data peristiwa berikut untuk memanggil fungsi:

```
{
  "action": "increment",
  "number": 3
}
```

Praktik terbaik kode untuk fungsi Lambda Python

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji. Misalnya, di Python, ini mungkin terlihat seperti:

```
def lambda_handler(event, context):
    foo = event['foo']
```

```
bar = event['bar']

result = my_lambda_function(foo, bar)

def my_lambda_function(foo, bar):
    // MyLambdaFunction logic here
```

- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk runtime Node.js dan Python, ini termasuk file. AWS SDKs Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.
 - Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
 - Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi.
 - Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.
- Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.
- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).

- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Bekerja dengan arsip file.zip untuk fungsi Python Lambda

Kode AWS Lambda fungsi Anda terdiri dari file.py yang berisi kode handler fungsi Anda, bersama dengan paket dan modul tambahan yang bergantung pada kode Anda. Untuk menyebarkan kode fungsi ini ke Lambda, Anda menggunakan paket penerapan. Paket ini dapat berupa arsip file.zip atau gambar kontainer. Untuk informasi selengkapnya tentang penggunaan gambar kontainer dengan Python, lihat [Menerapkan fungsi Lambda Python](#) dengan gambar kontainer.

[Untuk membuat paket penyebaran Anda sebagai arsip file.zip, Anda dapat menggunakan utilitas arsip file.zip bawaan alat baris perintah Anda, atau utilitas file.zip lainnya seperti 7zip.](#) Contoh yang ditampilkan di bagian berikut mengasumsikan Anda menggunakan zip alat baris perintah di lingkungan Linux atau macOS. Untuk menggunakan perintah yang sama di Windows, Anda dapat [menginstal Windows Subsystem untuk Linux untuk](#) mendapatkan versi Windows terintegrasi dari Ubuntu dan Bash.

Perhatikan bahwa Lambda menggunakan izin POSIX file, jadi Anda mungkin perlu [mengatur izin untuk folder paket penyebaran](#) sebelum membuat arsip file.zip.

Topik

- [Dependensi runtime dengan Python](#)
- [Membuat paket penerapan.zip tanpa dependensi](#)
- [Membuat paket penerapan.zip dengan dependensi](#)
- [Jalur pencarian ketergantungan dan pustaka yang disertakan runtime](#)
- [Menggunakan folder `__pycache__`](#)
- [Membuat paket penerapan.zip dengan pustaka asli](#)
- [Membuat dan memperbarui fungsi Lambda Python menggunakan file.zip](#)

Dependensi runtime dengan Python

Untuk fungsi Lambda yang menggunakan runtime Python, dependensi dapat berupa paket atau modul Python apa pun. [Ketika Anda menerapkan fungsi Anda menggunakan arsip.zip, Anda dapat menambahkan dependensi ini ke file.zip Anda dengan kode fungsi Anda atau menggunakan lapisan Lambda.](#) Lapisan adalah file.zip terpisah yang dapat berisi kode tambahan dan konten lainnya. Untuk mempelajari lebih lanjut tentang menggunakan layer Lambda dengan Python, lihat [the section called “Lapisan”](#)

Runtime Lambda Python mencakup dan dependensinya. AWS SDK for Python (Boto3) Lambda menyediakan SDK dalam runtime untuk skenario penerapan di mana Anda tidak dapat menambahkan dependensi Anda sendiri. Skenario ini termasuk membuat fungsi di konsol menggunakan editor kode bawaan atau menggunakan fungsi inline in AWS Serverless Application Model (AWS SAM) atau AWS CloudFormation template.

Lambda secara berkala memperbarui pustaka di runtime Python untuk menyertakan pembaruan terbaru dan patch keamanan. Jika fungsi Anda menggunakan versi Boto3 yang SDK disertakan dalam runtime tetapi paket penerapan Anda menyertakan SDK dependensi, ini dapat menyebabkan masalah ketidaksejajaran versi. Misalnya, paket penerapan Anda dapat menyertakan urllib3 SDK dependensi. Saat Lambda memperbarui SDK dalam runtime, masalah kompatibilitas antara versi baru runtime dan versi urllib3 dalam paket penerapan Anda dapat menyebabkan fungsi Anda gagal.

Important

Untuk mempertahankan kontrol penuh atas dependensi Anda dan untuk menghindari kemungkinan masalah ketidaksejajaran versi, kami sarankan Anda menambahkan semua dependensi fungsi Anda ke paket penerapan Anda, meskipun versinya disertakan dalam runtime Lambda. Ini termasuk Boto3SDK.

Untuk mengetahui versi Python (Boto3) mana yang disertakan dalam runtime yang Anda gunakan, lihat. SDK [the section called “Versi yang disertakan runtime SDK”](#)

Di bawah [model tanggung jawab AWS bersama](#), Anda bertanggung jawab atas pengelolaan dependensi apa pun dalam paket penerapan fungsi Anda. Ini termasuk menerapkan pembaruan dan patch keamanan. Untuk memperbarui dependensi dalam paket penerapan fungsi Anda, pertama buat file.zip baru dan kemudian unggah ke Lambda. Lihat [Membuat paket penerapan.zip dengan dependensi](#) dan [Membuat dan memperbarui fungsi Lambda Python menggunakan file.zip](#) untuk informasi lebih lanjut.

Membuat paket penerapan.zip tanpa dependensi

Jika kode fungsi Anda tidak memiliki dependensi, file.zip Anda hanya berisi file.py dengan kode handler fungsi Anda. Gunakan utilitas zip pilihan Anda untuk membuat file.zip dengan file.py Anda di root. Jika file.py tidak berada di root file.zip Anda, Lambda tidak akan dapat menjalankan kode Anda.

Untuk mempelajari cara menerapkan file.zip Anda untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada, lihat. [Membuat dan memperbarui fungsi Lambda Python menggunakan file.zip](#)

Membuat paket penerapan.zip dengan dependensi

Jika kode fungsi Anda bergantung pada paket atau modul tambahan, Anda dapat menambahkan dependensi ini ke file.zip Anda dengan kode fungsi Anda atau [menggunakan lapisan Lambda](#). Petunjuk di bagian ini menunjukkan cara memasukkan dependensi Anda ke dalam paket penerapan.zip Anda. Agar Lambda menjalankan kode Anda, file.py yang berisi kode handler Anda dan semua dependensi fungsi Anda harus diinstal di root file.zip.

Misalkan kode fungsi Anda disimpan dalam file bernama `lambda_function.py`. Contoh CLI perintah berikut membuat file.zip bernama `my_deployment_package.zip` berisi kode fungsi Anda dan dependensinya. Anda dapat menginstal dependensi Anda langsung ke folder di direktori proyek Anda atau menggunakan lingkungan virtual Python.

Untuk membuat paket penyebaran (direktori proyek)

1. Arahkan ke direktori proyek yang berisi file kode `lambda_function.py` sumber Anda. Dalam contoh ini, direktori diberi nama `my_function`.

```
cd my_function
```

2. Buat direktori baru bernama paket di mana Anda akan menginstal dependensi Anda.

```
mkdir package
```

Perhatikan bahwa untuk paket penyebaran.zip, Lambda mengharapkan kode sumber Anda dan semua dependensinya berada di root file.zip. Namun, menginstal dependensi langsung di direktori proyek Anda dapat memperkenalkan sejumlah besar file dan folder baru dan membuat navigasi di sekitar Anda sulit. IDE Anda membuat package direktori terpisah di sini untuk menjaga dependensi Anda terpisah dari kode sumber Anda.

3. Instal dependensi Anda di direktori. `package` Contoh di bawah ini menginstal Boto3 dari Python Package SDK Index menggunakan pip. Jika kode fungsi Anda menggunakan paket Python yang telah Anda buat sendiri, simpan di direktori. `package`

```
pip install --target ./package boto3
```

4. Buat file.zip dengan pustaka yang diinstal di root.

```
cd package
zip -r ../my_deployment_package.zip .
```

Ini menghasilkan file `my_deployment_package.zip` di direktori proyek Anda.

5. Tambahkan file `lambda_function.py` ke root file.zip

```
cd ..
zip my_deployment_package.zip lambda_function.py
```

File.zip Anda harus memiliki struktur direktori datar, dengan kode handler fungsi Anda dan semua folder dependensi Anda diinstal di root sebagai berikut.

```
my_deployment_package.zip
|- bin
|  |-jp.py
|- boto3
|  |-compat.py
|  |-data
|  |-docs
...
|- lambda_function.py
```

Jika file.py yang berisi kode handler fungsi Anda tidak berada di root file.zip Anda, Lambda tidak akan dapat menjalankan kode Anda.

Untuk membuat paket penyebaran (lingkungan virtual)

1. Buat dan aktifkan lingkungan virtual di direktori proyek Anda. Dalam contoh ini direktori proyek diberi nama `my_function`.

```
~$ cd my_function
~/my_function$ python3.12 -m venv my_virtual_env
~/my_function$ source ./my_virtual_env/bin/activate
```

2. Instal pustaka yang Anda butuhkan menggunakan pip. Contoh berikut menginstal Boto3 SDK

```
(my_virtual_env) ~/my_function$ pip install boto3
```

- Gunakan `pip show` untuk menemukan lokasi di lingkungan virtual Anda di mana pip telah menginstal dependensi Anda.

```
(my_virtual_env) ~/my_function$ pip show <package_name>
```

Folder tempat pip menginstal pustaka Anda dapat diberi nama atau `site-packages` `dist-packages` Folder ini mungkin terletak di `lib64/python3.x` direktori `lib/python3.x` or (di mana `python3.x` mewakili versi Python yang Anda gunakan).

- Nonaktifkan lingkungan virtual

```
(my_virtual_env) ~/my_function$ deactivate
```

- Arahkan ke direktori yang berisi dependensi yang Anda instal dengan pip dan buat file.zip di direktori proyek Anda dengan dependensi yang diinstal di root. Dalam contoh ini, pip telah menginstal dependensi Anda di direktori `my_virtual_env/lib/python3.12/site-packages`

```
~/my_function$ cd my_virtual_env/lib/python3.12/site-packages
~/my_function/my_virtual_env/lib/python3.12/site-packages$ zip -r ../../../../
my_deployment_package.zip .
```

- Arahkan ke root direktori proyek Anda di mana file.py yang berisi kode handler Anda berada dan tambahkan file itu ke root paket.zip Anda. Dalam contoh ini, file kode fungsi Anda diberi nama `lambda_function.py`.

```
~/my_function/my_virtual_env/lib/python3.12/site-packages$ cd ../../../../
~/my_function$ zip my_deployment_package.zip lambda_function.py
```

Jalur pencarian ketergantungan dan pustaka yang disertakan runtime

Saat Anda menggunakan `import` pernyataan dalam kode Anda, runtime Python mencari direktori di jalur pencariannya hingga menemukan modul atau paket. Secara default, lokasi pertama pencarian runtime adalah direktori tempat paket deployment .zip Anda didekompresi dan dipasang (`./var/task`). Jika Anda menyertakan versi pustaka yang disertakan runtime dalam paket penerapan, versi Anda akan lebih diutamakan daripada versi yang disertakan dalam runtime. Dependensi dalam paket penerapan Anda juga lebih diutamakan daripada dependensi dalam lapisan.

Saat Anda menambahkan dependensi ke lapisan, Lambda mengekstrak ini `/opt/python/lib/python3.x/site-packages` ke (`python3.x` di mana mewakili versi runtime yang Anda gunakan) atau `/opt/python` Di jalur pencarian, direktori ini lebih diutamakan daripada direktori yang berisi pustaka yang disertakan runtime dan pustaka yang diinstal pip (dan) `/var/runtime /var/lang/lib/python3.x/site-packages` Oleh karena itu, pustaka di lapisan fungsi lebih diutamakan daripada versi yang disertakan dalam runtime.

Note

Dalam runtime terkelola Python 3.11 dan image dasar, AWS SDK dan dependensinya diinstal di direktori `/var/lang/lib/python3.11/site-packages`

Anda dapat melihat jalur pencarian lengkap untuk fungsi Lambda Anda dengan menambahkan cuplikan kode berikut.

```
import sys

search_path = sys.path
print(search_path)
```

Note

Karena dependensi dalam paket atau lapisan penerapan Anda lebih diutamakan daripada pustaka yang disertakan runtime, ini dapat menyebabkan masalah ketidaksejajaran versi jika Anda menyertakan SDK dependensi seperti `urllib3` dalam paket Anda tanpa menyertakan juga SDK. Jika Anda menerapkan versi dependensi Boto3 Anda sendiri, Anda juga harus menerapkan Boto3 sebagai dependensi dalam paket penerapan Anda. Kami menyarankan Anda mengemas semua dependensi fungsi Anda, meskipun versinya disertakan dalam runtime.

Anda juga dapat menambahkan dependensi di folder terpisah di dalam paket.zip Anda. Misalnya, Anda dapat menambahkan versi Boto3 SDK ke folder dalam paket.zip Anda yang disebut `common`. Ketika paket.zip Anda didekompresi dan dipasang, folder ini ditempatkan di dalam direktori `/var/task` Untuk menggunakan dependensi dari folder dalam paket deployment .zip Anda dalam kode Anda, gunakan pernyataan `import from` Misalnya, untuk menggunakan versi Boto3 dari folder bernama `common` dalam paket.zip Anda, gunakan pernyataan berikut.

```
from common import boto3
```

Menggunakan folder `__pycache__`

Kami menyarankan agar Anda tidak menyertakan `__pycache__` folder dalam paket penerapan fungsi Anda. Bytecode Python yang dikompilasi pada mesin build dengan arsitektur atau sistem operasi yang berbeda mungkin tidak kompatibel dengan lingkungan eksekusi Lambda.

Membuat paket penerapan.zip dengan pustaka asli

Jika fungsi Anda hanya menggunakan paket dan modul Python murni, Anda dapat menggunakan `pip install` perintah untuk menginstal dependensi Anda pada mesin build lokal mana pun dan membuat file.zip Anda. Banyak pustaka Python populer, termasuk NumPy dan Panda, bukan Python murni dan berisi kode yang ditulis dalam C atau C++. Saat menambahkan pustaka yang berisi kode C/C++ ke paket penerapan, Anda harus membuat paket dengan benar untuk memastikan bahwa paket tersebut kompatibel dengan lingkungan eksekusi Lambda.

Sebagian besar paket yang tersedia di Indeks Paket Python ([PyPI](#)) tersedia sebagai “roda” (file.whl). File WHL adalah jenis ZIP file yang berisi distribusi yang dibangun dengan binari pra-kompilasi untuk sistem operasi tertentu dan arsitektur set instruksi. Untuk membuat paket penyebaran Anda kompatibel dengan Lambda, Anda menginstal roda untuk sistem operasi Linux dan arsitektur set instruksi fungsi Anda.

Beberapa paket mungkin hanya tersedia sebagai distribusi sumber. Untuk paket-paket ini, Anda perlu mengkompilasi dan membangun komponen C/C++ sendiri.

Untuk melihat distribusi apa yang tersedia untuk paket yang Anda butuhkan, lakukan hal berikut:

1. Cari nama paket di halaman [utama Python Package Index](#).
2. Pilih versi paket yang ingin Anda gunakan.
3. Pilih Unduh file.

Bekerja dengan distribusi yang dibangun (roda)

Untuk mengunduh roda yang kompatibel dengan Lambda, Anda menggunakan opsi `pip --platform`.

Jika fungsi Lambda Anda menggunakan arsitektur set instruksi x86_64, jalankan `pip install` perintah berikut untuk menginstal roda yang kompatibel di direktori Anda. Ganti `--python 3.x` dengan versi runtime Python yang Anda gunakan.

```
pip install \  
--platform manylinux2014_x86_64 \  
--target=package \  
--implementation cp \  
--python-version 3.x \  
--only-binary=:all: --upgrade \  
<package_name>
```

Jika fungsi Anda menggunakan arsitektur set instruksi arm64, jalankan perintah berikut. Ganti `--python 3.x` dengan versi runtime Python yang Anda gunakan.

```
pip install \  
--platform manylinux2014_aarch64 \  
--target=package \  
--implementation cp \  
--python-version 3.x \  
--only-binary=:all: --upgrade \  
<package_name>
```

Bekerja dengan distribusi sumber

Jika paket Anda hanya tersedia sebagai distribusi sumber, Anda perlu membuat pustaka C/C++ sendiri. Untuk membuat paket Anda kompatibel dengan lingkungan eksekusi Lambda, Anda perlu membangunnya di lingkungan yang menggunakan sistem operasi Amazon Linux 2 yang sama. Anda dapat melakukan ini dengan membangun paket Anda dalam instance Amazon EC2 Linux.

Untuk mempelajari cara meluncurkan dan menyambung ke instans Amazon EC2 Linux, lihat [Tutorial: Memulai instans Amazon EC2 Linux](#) di Panduan EC2 Pengguna Amazon untuk Instans Linux.

Membuat dan memperbarui fungsi Lambda Python menggunakan file.zip

Setelah Anda membuat paket.zip deployment, Anda dapat menggunakannya untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada. Anda dapat menerapkan paket.zip Anda menggunakan konsol Lambda, the, AWS Command Line Interface dan Lambda. API Anda juga dapat membuat dan memperbarui fungsi Lambda menggunakan AWS Serverless Application Model (AWS SAM) dan. AWS CloudFormation

Ukuran maksimum untuk paket.zip deployment untuk Lambda adalah 250 MB (unzip). Perhatikan bahwa batas ini berlaku untuk ukuran gabungan semua file yang Anda unggah, termasuk lapisan Lambda apa pun.

Runtime Lambda membutuhkan izin untuk membaca file dalam paket deployment Anda. Dalam notasi oktal izin Linux, Lambda membutuhkan 644 izin untuk file yang tidak dapat dieksekusi (rw-r - r--) dan 755 izin () untuk direktori dan file yang dapat dieksekusi. rwxr-xr-x

Di Linux dan macOS, gunakan `chmod` perintah untuk mengubah izin file pada file dan direktori dalam paket penyebaran Anda. Misalnya, untuk memberikan file yang dapat dieksekusi izin yang benar, jalankan perintah berikut.

```
chmod 755 <filepath>
```

Untuk mengubah izin file di Windows, lihat [Mengatur, Melihat, Mengubah, atau Menghapus Izin pada Objek](#) dalam dokumentasi Microsoft Windows.

Membuat dan memperbarui fungsi dengan file.zip menggunakan konsol

Untuk membuat fungsi baru, Anda harus terlebih dahulu membuat fungsi di konsol, lalu mengunggah arsip.zip Anda. Untuk memperbarui fungsi yang ada, buka halaman untuk fungsi Anda, lalu ikuti prosedur yang sama untuk menambahkan file.zip Anda yang diperbarui.

Jika file.zip Anda kurang dari 50MB, Anda dapat membuat atau memperbarui fungsi dengan mengunggah file langsung dari mesin lokal Anda. Untuk file.zip yang lebih besar dari 50MB, Anda harus mengunggah paket Anda ke bucket Amazon S3 terlebih dahulu. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS Management Console, lihat [Memulai Amazon S3](#). Untuk mengunggah file menggunakan AWS CLI, lihat [Memindahkan objek](#) di Panduan AWS CLI Pengguna.

Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Untuk membuat fungsi baru (konsol)

1. Buka [halaman Functions](#) dari konsol Lambda dan pilih Create Function.

2. Pilih Tulis dari awal.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda.
 - b. Untuk Runtime, pilih runtime yang ingin Anda gunakan.
 - c. (Opsional) Untuk Arsitektur, pilih arsitektur set instruksi untuk fungsi Anda. Arsitektur default adalah x86_64. Pastikan bahwa paket deployment .zip untuk fungsi Anda kompatibel dengan arsitektur set instruksi yang Anda pilih.
4. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan yang sudah ada.
5. Pilih Buat fungsi. Lambda menciptakan fungsi dasar 'Hello world' menggunakan runtime yang Anda pilih.

Untuk mengunggah arsip.zip dari mesin lokal Anda (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih file.zip.
5. Untuk mengunggah file.zip, lakukan hal berikut:
 - a. Pilih Unggah, lalu pilih file.zip Anda di pemilih file.
 - b. Pilih Buka.
 - c. Pilih Simpan.

Untuk mengunggah arsip.zip dari bucket Amazon S3 (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip baru.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih lokasi Amazon S3.
5. Rekatkan tautan Amazon S3 URL dari file.zip Anda dan pilih Simpan.

Memperbarui fungsi file.zip menggunakan editor kode konsol

Untuk beberapa fungsi dengan paket penyebaran.zip, Anda dapat menggunakan editor kode bawaan konsol Lambda untuk memperbarui kode fungsi Anda secara langsung. Untuk menggunakan fitur ini, fungsi Anda harus memenuhi kriteria berikut:

- Fungsi Anda harus menggunakan salah satu runtime bahasa yang ditafsirkan (Python, Node.js, atau Ruby)
- Paket penerapan fungsi Anda harus lebih kecil dari 3MB.

Kode fungsi untuk fungsi dengan paket penerapan gambar kontainer tidak dapat diedit langsung di konsol.

Untuk memperbarui kode fungsi menggunakan editor kode konsol

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih file kode sumber Anda dan edit di editor kode terintegrasi.
4. Setelah selesai mengedit kode, pilih Deploy untuk menyimpan perubahan dan memperbarui fungsi Anda.

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CLI

Anda dapat menggunakan [AWS CLI](#) untuk membuat fungsi baru atau memperbarui yang sudah ada menggunakan file.zip. Gunakan [create-function](#) dan [update-function-code](#) perintah untuk menyebarkan paket.zip Anda. Jika file.zip Anda lebih kecil dari 50MB, Anda dapat mengunggah paket.zip dari lokasi file di mesin build lokal Anda. Untuk file yang lebih besar, Anda harus mengunggah paket.zip Anda dari bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Note

Jika Anda mengunggah file.zip dari bucket Amazon S3 menggunakan AWS CLI, bucket harus berada di lokasi yang Wilayah AWS sama dengan fungsi Anda.

Untuk membuat fungsi baru menggunakan file.zip dengan AWS CLI, Anda harus menentukan yang berikut:

- Nama fungsi Anda (`--function-name`)
- Runtime (`--runtime`) fungsi Anda
- Amazon Resource Name (ARN) dari [peran eksekusi](#) fungsi Anda (`--role`)
- Nama metode handler dalam kode fungsi Anda (`--handler`)

Anda juga harus menentukan lokasi file.zip Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda create-function --function-name myFunction \  
--runtime python3.12 --handler lambda_function.lambda_handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi seperti `--code` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `S3ObjectVersion` parameter untuk objek berversi.

```
aws lambda create-function --function-name myFunction \  
--runtime python3.12 --handler lambda_function.lambda_handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--code S3Bucket=amzn-s3-demo-  
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Untuk memperbarui fungsi yang ada menggunakan CLI, Anda menentukan nama fungsi Anda menggunakan `--function-name` parameter. Anda juga harus menentukan lokasi file.zip yang ingin Anda gunakan untuk memperbarui kode fungsi Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda update-function-code --function-name myFunction \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi `--s3-key` dan seperti `--s3-bucket` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `--s3-object-version` parameter untuk objek berversi.

```
aws lambda update-function-code --function-name myFunction \  
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject  
Version
```

Membuat dan memperbarui fungsi dengan file.zip menggunakan Lambda API

Untuk membuat dan memperbarui fungsi menggunakan arsip file.zip, gunakan API operasi berikut:

- [CreateFunction](#)
- [UpdateFunctionCode](#)

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS SAM

The AWS Serverless Application Model (AWS SAM) adalah toolkit yang membantu merampingkan proses membangun dan menjalankan aplikasi tanpa server. AWS Anda menentukan sumber daya untuk aplikasi Anda dalam JSON template YAML atau dan menggunakan antarmuka baris AWS SAM perintah (AWS SAM CLI) untuk membangun, mengemas, dan menyebarkan aplikasi Anda. Saat Anda membuat fungsi Lambda dari AWS SAM template, AWS SAM secara otomatis membuat paket penerapan .zip atau gambar kontainer dengan kode fungsi Anda dan dependensi apa pun yang Anda tentukan. Untuk mempelajari lebih lanjut cara menggunakan AWS SAM untuk membangun dan menerapkan fungsi Lambda, [lihat Memulai](#) di Panduan AWS SAMAWS Serverless Application Model Pengembang.

Anda juga dapat menggunakan AWS SAM untuk membuat fungsi Lambda menggunakan arsip file.zip yang ada. Untuk membuat fungsi Lambda menggunakan AWS SAM, Anda dapat menyimpan file.zip di bucket Amazon S3 atau di folder lokal di mesin build Anda. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS SAM template Anda, `AWS::Serverless::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- diatur ke `Zip`
- `CodeUri`- diatur ke kode fungsi Amazon S3URI, jalur ke folder lokal, atau objek [FunctionCode](#)
- `Runtime`- Setel ke runtime yang Anda pilih

Dengan AWS SAM, jika file.zip Anda lebih besar dari 50MB, Anda tidak perlu mengunggahnya ke bucket Amazon S3 terlebih dahulu. AWS SAM dapat mengunggah paket.zip hingga ukuran maksimum yang diizinkan 250MB (unzip) dari lokasi di mesin build lokal Anda.

Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS SAM, lihat [AWS: :Serverless: :Function](#) dalam Panduan Pengembang.AWS SAM

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk membuat fungsi Lambda menggunakan arsip file.zip. Untuk membuat fungsi Lambda dari file.zip, Anda harus terlebih dahulu mengunggah file Anda ke bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Untuk runtime Node.js dan Python, Anda juga dapat memberikan kode sumber inline di template Anda. AWS CloudFormation AWS CloudFormation kemudian buat file.zip yang berisi kode Anda saat Anda membangun fungsi Anda.

Menggunakan file.zip yang ada

Dalam AWS CloudFormation template Anda, `AWS::Lambda::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- Setel ke `Zip`
- `Code`- Masukkan nama bucket Amazon S3 dan nama file.zip di dan bidang `S3Bucket` `S3Key`
- `Runtime`- Setel ke runtime yang Anda pilih

Membuat file.zip dari kode sebaris

Anda dapat mendeklarasikan fungsi sederhana yang ditulis dengan Python atau Node.js inline dalam template. AWS CloudFormation Karena kode disematkan di YAML atauJSON, Anda tidak dapat menambahkan dependences eksternal apa pun ke paket penerapan Anda. Ini berarti fungsi Anda harus menggunakan versi AWS SDK yang disertakan dalam runtime. Persyaratan template, seperti harus melarikan diri dari karakter tertentu, juga mempersulit penggunaan pemeriksaan IDE sintaks dan fitur penyelesaian kode Anda. Ini berarti bahwa template Anda mungkin memerlukan pengujian tambahan. Karena keterbatasan ini, mendeklarasikan fungsi inline paling cocok untuk kode yang sangat sederhana yang tidak sering berubah.

Untuk membuat file.zip dari kode inline untuk runtime Node.js dan Python, atur properti berikut di sumber daya template Anda: `AWS::Lambda::Function`

- `PackageType`- Setel ke `Zip`
- `Code`- Masukkan kode fungsi Anda di `ZipFile` bidang
- `Runtime`- Setel ke runtime yang Anda pilih

File.zip yang AWS CloudFormation menghasilkan tidak boleh melebihi 4MB. Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS CloudFormation, lihat [AWS::Lambda::Function](#) di Panduan Pengguna.AWS CloudFormation

Deploy fungsi Lambda Python dengan gambar kontainer

Ada tiga cara untuk membangun image kontainer untuk fungsi Lambda Python:

- [Menggunakan gambar AWS dasar untuk Python](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [kustom](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan klien [antarmuka runtime untuk Python](#) dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan klien [antarmuka runtime untuk Python](#) dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi kontainer Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

Topik

- [AWS gambar dasar untuk Python](#)
- [Menggunakan gambar AWS dasar untuk Python](#)

- [Menggunakan gambar dasar alternatif dengan klien antarmuka runtime](#)

AWS gambar dasar untuk Python

AWS menyediakan gambar dasar berikut untuk Python:

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|-------|----------------|-------------------|---|--------------|
| 3.12 | Python 3.12 | Amazon Linux 2023 | Dockerfile untuk Python 3.12 aktif GitHub | |
| 3.11 | Python 3.11 | Amazon Linux 2 | Dockerfile untuk Python 3.11 aktif GitHub | |
| 3.10 | Python 3.10 | Amazon Linux 2 | Dockerfile untuk Python 3.10 aktif GitHub | |
| 3.9 | Python 3.9 | Amazon Linux 2 | Dockerfile untuk Python 3.9 aktif GitHub | |
| 3.8 | Python 3.8 | Amazon Linux 2 | Dockerfile untuk Python 3.8 aktif GitHub | Okt 14, 2024 |

ECR [Repositori Amazon: gallery.ecr.aws/lambda/python](https://gallery.ecr.aws/lambda/python)

Python 3.12 dan gambar dasar yang lebih baru didasarkan pada gambar kontainer minimal [Amazon Linux 2023](#). Gambar dasar Python 3.8-3.11 didasarkan pada gambar Amazon Linux 2. AL2 Gambar berbasis 023 memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti `glibc`

AL2 Gambar berbasis 023 menggunakan `microdnf` (symlinked `asdnf`) sebagai manajer paket, bukannya `yum`, yang merupakan pengelola paket default di Amazon Linux 2. `microdnf` adalah implementasi mandiri dari `dnf` Untuk daftar paket yang disertakan dalam gambar AL2 berbasis 023, lihat kolom Kontainer Minimal di Membandingkan paket yang diinstal pada Gambar Kontainer [Amazon Linux 2023](#). Untuk informasi selengkapnya tentang perbedaan antara AL2 023 dan Amazon Linux 2, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di Blog Komputasi AWS .

Note

Untuk menjalankan gambar AL2 berbasis 023 secara lokal, termasuk with AWS Serverless Application Model (AWS SAM), Anda harus menggunakan Docker versi 20.10.10 atau yang lebih baru.

Jalur pencarian ketergantungan di gambar dasar

Saat Anda menggunakan `import` pernyataan dalam kode Anda, runtime Python mencari direktori di jalur pencariannya hingga menemukan modul atau paket. Secara default, runtime mencari `{LAMBDA_TASK_ROOT}` direktori terlebih dahulu. Jika Anda menyertakan versi pustaka yang disertakan runtime dalam gambar Anda, versi Anda akan lebih diutamakan daripada versi yang disertakan dalam runtime.

Langkah-langkah lain di jalur pencarian bergantung pada versi gambar dasar Lambda untuk Python yang Anda gunakan:

- Python 3.11 dan yang lebih baru: Pustaka yang disertakan runtime dan pustaka yang diinstal pip diinstal di direktori. `/var/lang/lib/python3.11/site-packages` Direktori ini lebih diutamakan `/var/runtime` di jalur pencarian. Anda dapat mengganti SDK dengan menggunakan pip untuk menginstal versi yang lebih baru. Anda dapat menggunakan pip untuk memverifikasi bahwa runtime yang disertakan SDK dan dependensinya kompatibel dengan paket apa pun yang Anda instal.
- Python 3.8-3.10: Pustaka yang disertakan runtime diinstal di direktori. `/var/runtime` Pustaka yang diinstal PIP diinstal di direktori. `/var/lang/lib/python3.x/site-packages /var/runtime` Direktori lebih diutamakan `/var/lang/lib/python3.x/site-packages` di jalur pencarian.

Anda dapat melihat jalur pencarian lengkap untuk fungsi Lambda Anda dengan menambahkan cuplikan kode berikut.

```
import sys

search_path = sys.path
print(search_path)
```

Menggunakan gambar AWS dasar untuk Python

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#) (versi minimum 20.10.10 untuk Python 3.12 dan gambar dasar yang lebih baru)
- Python

Membuat gambar dari gambar dasar

Untuk membuat gambar kontainer dari gambar AWS dasar untuk Python

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Buat file baru bernam `lambda_function.py`. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

Example Fungsi Python

```
import sys
def handler(event, context):
    return 'Hello from AWS Lambda using Python' + sys.version + '!!'
```

3. Buat file baru bernam `requirements.txt`. Jika Anda menggunakan kode fungsi sampel dari langkah sebelumnya, Anda dapat membiarkan file kosong karena tidak ada dependensi. Jika tidak, daftarkan setiap pustaka yang diperlukan. Misalnya, inilah tampilan `requirements.txt` Anda jika fungsi Anda menggunakan AWS SDK for Python (Boto3):

Example requirements.txt

```
boto3
```

4. Buat Dockerfile baru dengan konfigurasi berikut:

- Atur FROM properti ke [URL gambar dasar](#).

- Gunakan COPY perintah untuk menyalin kode fungsi dan dependensi runtime ke `{LAMBDA_TASK_ROOT}`, variabel lingkungan yang ditentukan [Lambda](#).
- Atur CMD argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/python:3.12

# Copy requirements.txt
COPY requirements.txt ${LAMBDA_TASK_ROOT}

# Install the specified packages
RUN pip install -r requirements.txt

# Copy function code
COPY lambda_function.py ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
of the Dockerfile)
CMD [ "lambda_function.handler" ]
```

5. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

1. Mulai gambar Docker dengan perintah `docker run`. Dalam contoh ini, `docker-image` adalah nama gambar dan test tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

2. Dari jendela terminal baru, posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload": "hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

3. Dapatkan ID kontainer.

```
docker ps
```

4. Gunakan perintah [docker kill](#) untuk menghentikan kontainer. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.

- Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
- Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECRRepository Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repository Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:


```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositori URI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output dari fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan gambar dasar alternatif dengan klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda.

Instal [klien antarmuka runtime untuk Python](#) menggunakan manajer paket pip:

```
pip install awslambdaric
```

Anda juga dapat mengunduh klien [antarmuka runtime Python](#) dari GitHub

Contoh berikut menunjukkan bagaimana membangun image container untuk Python menggunakan gambar AWS non-dasar. Contoh Dockerfile menggunakan gambar dasar Python resmi. Dockerfile menyertakan klien antarmuka runtime untuk Python.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

- [Docker](#)
- Python

Membuat gambar dari gambar dasar alternatif

Untuk membuat gambar kontainer dari gambar AWS non-dasar

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Buat file baru bernamalambda_function.py. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

Example Fungsi Python

```
import sys
def handler(event, context):
    return 'Hello from AWS Lambda using Python' + sys.version + '!'
```

3. Buat file baru bernamarequirements.txt. Jika Anda menggunakan kode fungsi sampel dari langkah sebelumnya, Anda dapat membiarkan file kosong karena tidak ada dependensi. Jika tidak, daftarkan setiap pustaka yang diperlukan. Misalnya, inilah tampilan requirements.txt Anda jika fungsi Anda menggunakan AWS SDK for Python (Boto3):

Example requirements.txt

```
boto3
```

4. Buat Dockerfile baru. [Dockerfile berikut menggunakan gambar dasar Python resmi, bukan gambar dasar.AWS](#) Dockerfile menyertakan [klien antarmuka runtime](#), yang membuat gambar kompatibel dengan Lambda. Contoh berikut Dockerfile menggunakan build [multi-tahap](#).
 - Atur FROM properti ke gambar dasar.
 - Atur ENTRYPOINT ke modul yang Anda inginkan untuk menjalankan wadah Docker saat dimulai. Dalam hal ini, modul adalah klien antarmuka runtime.
 - Atur CMD ke penanganan fungsi Lambda.

Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
# Define custom function directory
ARG FUNCTION_DIR="/function"

FROM python:3.12 as build-image

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

# Install the function's dependencies
RUN pip install \
    --target ${FUNCTION_DIR} \
        awslambdaric

# Use a slim version of the base Python image to reduce the final image size
FROM python:3.12-slim

# Include global arg in this stage of the build
ARG FUNCTION_DIR
# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/local/bin/python", "-m", "awslambdaric" ]
# Pass the name of the function handler as an argument to the runtime
CMD [ "lambda_function.handler" ]
```

5. Buat image Docker dengan perintah [docker build](#). Contoh berikut menamai gambar `docker-image` dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar secara lokal. Anda dapat [membangun emulator ke dalam gambar Anda](#) atau menggunakan prosedur berikut untuk menginstalnya di mesin lokal Anda.

Untuk menginstal dan menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Dari direktori proyek Anda, jalankan perintah berikut untuk mengunduh emulator antarmuka runtime (arsitektur x86-64) dari GitHub dan menginstalnya di mesin lokal Anda.

Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \  
  curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-  
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \  
  chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Untuk menginstal emulator arm64, ganti GitHub repositori URL di perintah sebelumnya dengan yang berikut:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/  
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Untuk menginstal emulator arm64, ganti `$downloadLink` dengan yang berikut ini:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Mulai gambar Docker dengan perintah `docker run`. Perhatikan hal berikut:

- `docker-image` adalah nama gambar dan test tag.
- `/usr/local/bin/python -m awslambdarc lambda_function.handler` adalah ENTRYPOINT diikuti oleh CMD dari Dockerfile Anda.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
    /usr/local/bin/python -m awslambdarc lambda_function.handler
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/local/bin/python -m awslambdarc lambda_function.handler
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

3. Posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

4. Dapatkan ID kontainer.

```
docker ps
```

5. Gunakan perintah [docker kill](#) untuk menghentikan kontainer. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{  
  "repository": {
```



```

    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}

```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhirURI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoryURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.

7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output dari fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Untuk contoh cara membuat gambar Python dari gambar dasar Alpine, lihat [Dukungan gambar kontainer untuk Lambda](#) di Blog AWS .

Bekerja dengan lapisan untuk fungsi Lambda Python

[Lapisan Lambda](#) adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi. Membuat layer melibatkan tiga langkah umum:

1. Package konten layer Anda. Ini berarti membuat arsip file.zip yang berisi dependensi yang ingin Anda gunakan dalam fungsi Anda.
2. Buat layer di Lambda.
3. Tambahkan layer ke fungsi Anda.

Topik ini berisi langkah-langkah dan panduan tentang cara mengemas dan membuat lapisan Lambda Python dengan dependensi pustaka eksternal dengan benar.

Topik

- [Prasyarat](#)
- [Kompatibilitas lapisan Python dengan Amazon Linux](#)
- [Jalur lapisan untuk runtime Python](#)
- [Mengemas konten lapisan](#)
- [Membuat layer](#)
- [Menambahkan layer ke fungsi Anda](#)
- [Bekerja dengan distribusi manylinux roda](#)

Prasyarat

Untuk mengikuti langkah-langkah di bagian ini, Anda harus memiliki yang berikut:

- [Python 3.11 dan penginstal paket pip](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Sepanjang topik ini, kami mereferensikan [layer-python](#) contoh aplikasi pada repositori awsdocs GitHub . Aplikasi ini berisi skrip yang mengunduh dependensi dan menghasilkan lapisan. Aplikasi ini juga berisi fungsi terkait yang menggunakan dependensi dari lapisan. Setelah membuat layer, Anda dapat menerapkan dan memanggil fungsi yang sesuai untuk memverifikasi bahwa semuanya

berfungsi dengan baik. Karena Anda menggunakan runtime Python 3.11 untuk fungsi, lapisan juga harus kompatibel dengan Python 3.11.

Dalam aplikasi `layer-python` sampel, ada dua contoh:

- Contoh pertama melibatkan pengemasan [requests](#) perpustakaan menjadi lapisan Lambda. `layer`/Direktori berisi skrip untuk menghasilkan lapisan. `function`/Direktori berisi fungsi sampel untuk membantu menguji bahwa lapisan berfungsi. Sebagian besar tutorial ini berjalan melalui cara membuat dan mengemas lapisan ini.
- Contoh kedua melibatkan pengemasan [numpy](#) perpustakaan menjadi lapisan Lambda. `layer-numpy`/Direktori berisi skrip untuk menghasilkan lapisan. `function-numpy`/Direktori berisi fungsi sampel untuk membantu menguji bahwa lapisan berfungsi. Untuk contoh cara membuat dan mengemas lapisan ini, lihat [the section called “Bekerja dengan distribusi manylinux roda”](#).

Kompatibilitas lapisan Python dengan Amazon Linux

Langkah pertama untuk membuat layer adalah untuk menggabungkan semua konten layer Anda ke dalam arsip file.zip. Karena fungsi Lambda berjalan di [Amazon Linux](#), konten layer Anda harus dapat dikompilasi dan dibangun di lingkungan Linux.

Dalam Python, sebagian besar paket tersedia sebagai [roda](#) (.whlfile) selain distribusi sumber. Setiap roda adalah jenis distribusi yang dibangun yang mendukung kombinasi spesifik dari versi Python, sistem operasi, dan set instruksi mesin.

Roda berguna untuk memastikan bahwa lapisan Anda kompatibel dengan Amazon Linux. Saat Anda mengunduh dependensi Anda, unduh roda universal jika memungkinkan. (Secara default, `pip` pasang roda universal jika tersedia.) Roda universal berisi any sebagai tag platform, yang menunjukkan bahwa itu kompatibel dengan semua platform, termasuk Amazon Linux.

Dalam contoh berikut, Anda mengemas `requests` pustaka ke dalam lapisan Lambda. `requests` Perpustakaan adalah contoh paket yang tersedia sebagai roda universal.

Tidak semua paket Python didistribusikan sebagai roda universal. Misalnya, [numpy](#) memiliki beberapa distribusi roda, masing-masing mendukung serangkaian platform yang berbeda. Untuk paket seperti itu, unduh `manylinux` distribusi untuk memastikan kompatibilitas dengan Amazon Linux. Untuk petunjuk terperinci tentang cara mengemas lapisan tersebut, lihat [the section called “Bekerja dengan distribusi manylinux roda”](#).

Dalam kasus yang jarang terjadi, paket Python mungkin tidak tersedia sebagai roda. Jika hanya [distribusi sumber](#) (sdist) yang ada, maka kami sarankan untuk menginstal dan mengemas dependensi Anda di lingkungan [Docker berdasarkan image](#) wadah dasar [Amazon Linux](#) 2023. Kami juga merekomendasikan pendekatan ini jika Anda ingin menyertakan pustaka kustom Anda sendiri yang ditulis dalam bahasa lain seperti C/C++. Pendekatan ini meniru lingkungan eksekusi Lambda di Docker, dan memastikan bahwa dependensi paket non-Python Anda kompatibel dengan Amazon Linux.

Jalur lapisan untuk runtime Python

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam `/opt` direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, `PATH` variabel sudah menyertakan jalur folder tertentu dalam direktori `/opt`. Untuk memastikan bahwa `PATH` variabel mengambil konten lapisan Anda, file `layer.zip` Anda harus memiliki dependensi di jalur folder berikut:

- `python`
- `python/lib/python3.x/site-packages`

Misalnya, file `layer.zip` yang dihasilkan yang Anda buat dalam tutorial ini memiliki struktur direktori berikut:

```
layer_content.zip
# python
  # lib
    # python3.11
      # site-packages
        # requests
        # <other_dependencies> (i.e. dependencies of the requests package)
        # ...
```

[requests](#) Perpustakaan terletak dengan benar di `python/lib/python3.11/site-packages` direktori. Ini memastikan bahwa Lambda dapat menemukan pustaka selama pemanggilan fungsi.

Mengemas konten lapisan

Dalam contoh ini, Anda mengemas `requests` pustaka Python dalam file `layer.zip`. Selesaikan langkah-langkah berikut untuk menginstal dan mengemas konten lapisan.

Untuk menginstal dan mengemas konten lapisan Anda

1. Kloning [aws-lambda-developer-guide GitHub repo](#), yang berisi kode sampel yang Anda butuhkan di direktori. `sample-apps/layer-python`

```
git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
```

2. Arahkan ke `layer` direktori aplikasi `layer-python` sampel. Direktori ini berisi skrip yang Anda gunakan untuk membuat dan mengemas lapisan dengan benar.

```
cd aws-lambda-developer-guide/sample-apps/layer-python/layer
```

3. Periksa [requirements.txt](#) file. File ini mendefinisikan dependensi yang ingin Anda sertakan dalam lapisan, yaitu perpustakaan. `requests` Anda dapat memperbarui file ini untuk menyertakan dependensi apa pun yang ingin Anda sertakan dalam lapisan Anda sendiri.

Example requirements.txt

```
requests==2.31.0
```

4. Pastikan Anda memiliki izin untuk menjalankan kedua skrip.

```
chmod 744 1-install.sh && chmod 744 2-package.sh
```

5. Jalankan [1-install.sh](#) skrip menggunakan perintah berikut:

```
./1-install.sh
```

Script ini digunakan venv untuk membuat lingkungan virtual Python bernama. `create_layer` Kemudian menginstal semua dependensi yang diperlukan dalam direktori. `create_layer/lib/python3.11/site-packages`

Example 1-install.sh

```
python3.11 -m venv create_layer
source create_layer/bin/activate
pip install -r requirements.txt
```

6. Jalankan [2-package.sh](#) skrip menggunakan perintah berikut:

```
./2-package.sh
```

Script ini menyalin isi dari `create_layer/lib` direktori ke direktori baru bernama `python`. Kemudian zip isi `python` direktori ke dalam file bernama `layer_content.zip`. Ini adalah file.zip untuk layer Anda. Anda dapat membuka zip file dan memverifikasi bahwa itu berisi struktur file yang benar, seperti yang ditunjukkan pada [the section called “Jalur lapisan untuk runtime Python”](#) bagian.

Example 2-package.sh

```
mkdir python
cp -r create_layer/lib python/
zip -r layer_content.zip python
```

Membuat layer

Di bagian ini, Anda mengambil `layer_content.zip` file yang Anda buat di bagian sebelumnya dan mengunggahnya sebagai lapisan Lambda. Anda dapat mengunggah layer menggunakan AWS Management Console atau Lambda API melalui AWS Command Line Interface (AWS CLI). Saat Anda mengunggah file layer .zip Anda, dalam [PublishLayerVersion](#) AWS CLI perintah berikut, tentukan `python3.11` sebagai runtime yang kompatibel dan `arm64` sebagai arsitektur yang kompatibel.

```
aws lambda publish-layer-version --layer-name python-requests-layer \
  --zip-file fileb://layer_content.zip \
  --compatible-runtimes python3.11 \
  --compatible-architectures "arm64"
```

Dari tanggapan, perhatikan `LayerVersionArn`, yang terlihat seperti `arn:aws:lambda:us-east-1:123456789012:layer:python-requests-layer:1`. Anda akan memerlukan Amazon Resource Name (ARN) ini di langkah berikutnya dari tutorial ini, ketika Anda menambahkan layer ke fungsi Anda.

Menambahkan layer ke fungsi Anda

Di bagian ini, Anda menerapkan contoh fungsi Lambda yang menggunakan `requests` pustaka dalam kode fungsinya, lalu Anda melampirkan layer. Untuk menerapkan fungsi, Anda memerlukan

file. [the section called “Peran eksekusi \(izin untuk fungsi untuk mengakses sumber daya lain\)”](#) Jika Anda tidak memiliki peran eksekusi yang ada, ikuti langkah-langkah di bagian yang dapat dilipat.

(Opsional) Buat peran eksekusi

Untuk membuat peran eksekusi

1. Buka [halaman peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.
 - Entitas tepercaya – Lambda.
 - Izin — AWSLambdaBasicExecutionRole.
 - Nama peran – **lambda-role**.

AWSLambdaBasicExecutionRoleKebijakan ini memiliki izin yang diperlukan fungsi untuk menulis log ke CloudWatch Log.

[Kode fungsi](#) Lambda mengimpor `requests` perpustakaan, membuat HTTP permintaan sederhana, dan kemudian mengembalikan kode status dan badan.

```
import requests

def lambda_handler(event, context):
    print(f"Version of requests library: {requests.__version__}")
    request = requests.get('https://api.github.com/')
    return {
        'statusCode': request.status_code,
        'body': request.text
    }
```

Untuk menyebarkan fungsi Lambda

1. Buka direktori `function/` tersebut. Jika saat ini Anda berada di `layer/` direktori, maka jalankan perintah berikut:

```
cd ../function
```

2. Buat paket penyebaran `file.zip` menggunakan perintah berikut:

```
zip my_deployment_package.zip lambda_function.py
```

3. Menyebarkan fungsi. Dalam AWS CLI perintah berikut, ganti `--role` parameter dengan peran eksekusi AndaARN:

```
aws lambda create-function --function-name python_function_with_layer \  
  --runtime python3.11 \  
  --architectures "arm64" \  
  --handler lambda_function.lambda_handler \  
  --role arn:aws:iam::123456789012:role/lambda-role \  
  --zip-file fileb://my_deployment_package.zip
```

4. Selanjutnya, pasang layer ke fungsi Anda. Dalam AWS CLI perintah berikut, ganti `--layers` parameter dengan versi layer ARN yang Anda catat sebelumnya:

```
aws lambda update-function-configuration --function-name python_function_with_layer \  
  \  
  --cli-binary-format raw-in-base64-out \  
  --layers "arn:aws:lambda:us-east-1:123456789012:layer:python-requests-layer:1"
```

5. Terakhir, coba panggil fungsi Anda menggunakan AWS CLI perintah berikut:

```
aws lambda invoke --function-name python_function_with_layer \  
  --cli-binary-format raw-in-base64-out \  
  --payload '{ "key": "value" }' response.json
```

Anda akan melihat output seperti ini:

```
{  
  "StatusCode": 200,  
  "ExecutedVersion": "$LATEST"  
}
```

`response.json` File output berisi rincian tentang respon.

(Opsional) Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus layer Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih layer yang Anda buat.
3. Pilih Hapus, lalu pilih Hapus lagi.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Bekerja dengan distribusi **manylinux** roda

Terkadang, paket yang ingin Anda sertakan sebagai dependensi tidak akan memiliki roda universal (khususnya, tidak memiliki any tag platform). Dalam hal ini, unduh roda yang mendukung manylinux sebagai gantinya. Ini memastikan bahwa pustaka lapisan Anda kompatibel dengan Amazon Linux.

[numpy](#) adalah salah satu paket yang tidak memiliki roda universal. Jika Anda ingin menyertakan numpy paket di layer Anda, maka Anda dapat menyelesaikan langkah-langkah contoh berikut untuk menginstal dan mengemas layer Anda dengan benar.

Untuk menginstal dan mengemas konten lapisan Anda

1. Kloning [aws-lambda-developer-guide GitHub repo](#), yang berisi kode sampel yang Anda butuhkan di direktori. `sample-apps/layer-python`

```
git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
```

2. Arahkan ke `layer-numpy` direktori aplikasi `layer-python` sampel. Direktori ini berisi skrip yang Anda gunakan untuk membuat dan mengemas lapisan dengan benar.

```
cd aws-lambda-developer-guide/sample-apps/layer-python/layer-numpy
```

3. Periksa [requirements.txt](#) file. File ini mendefinisikan dependensi yang ingin Anda sertakan dalam lapisan Anda, yaitu perpustakaan. `numpy` Di sini, Anda menentukan URL distribusi `manylinux` roda yang kompatibel dengan Python 3.11, Amazon Linux, dan set instruksi `six86_64`:

Example requirements.txt

```
https://files.pythonhosted.org/packages/3a/d0/edc009c27b406c4f9cbc79274d6e46d634d139075492ad055e3d68445925/numpy-1.26.4-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl
```

4. Pastikan Anda memiliki izin untuk menjalankan kedua skrip.

```
chmod 744 1-install.sh && chmod 744 2-package.sh
```

5. Jalankan [1-install.sh](#) skrip menggunakan perintah berikut:

```
./1-install.sh
```

Script ini digunakan `venv` untuk membuat lingkungan virtual Python bernama. `create_layer` Kemudian menginstal semua dependensi yang diperlukan dalam direktori. `create_layer/lib/python3.11/site-packages` `pip` Perintah berbeda dalam hal ini, karena Anda harus menentukan `--platform` tag sebagai `manylinux2014_x86_64`. Ini memberitahu `pip` untuk menginstal `manylinux` roda yang benar, bahkan jika mesin lokal Anda menggunakan `macOS` atau `Windows`.

Example 1-install.sh

```
python3.11 -m venv create_layer
source create_layer/bin/activate
pip install -r requirements.txt --platform=manylinux2014_x86_64 --only-binary=:all:
--target ./create_layer/lib/python3.11/site-packages
```

6. Jalankan [2-package.sh](#) skrip menggunakan perintah berikut:

```
./2-package.sh
```

Script ini menyalin isi dari `create_layer/lib` direktori ke direktori baru bernama `python`. Kemudian zip isi `python` direktori ke dalam file bernama `layer_content.zip`. Ini adalah file.zip untuk layer Anda. Anda dapat membuka zip file dan memverifikasi bahwa itu berisi struktur file yang benar seperti yang ditunjukkan pada [the section called “Jalur lapisan untuk runtime Python”](#) bagian.

Example 2-package.sh

```
mkdir python
cp -r create_layer/lib python/
zip -r layer_content.zip python
```

Untuk mengunggah layer ini ke Lambda, gunakan perintah berikut: [PublishLayerVersion](#) AWS CLI

```
aws lambda publish-layer-version --layer-name python-numpy-layer \
  --zip-file fileb://layer_content.zip \
  --compatible-runtimes python3.11 \
  --compatible-architectures "x86_64"
```

Dari tanggapan, perhatikan `LayerVersionArn`, yang terlihat seperti `arn:aws:lambda:us-east-1:123456789012:layer:python-numpy-layer:1`. Untuk memverifikasi bahwa lapisan Anda berfungsi seperti yang diharapkan, gunakan fungsi Lambda di `function-numpy` direktori.

Untuk menyebarkan fungsi Lambda

1. Buka direktori `function-numpy/` tersebut. Jika saat ini Anda berada di `layer-numpy/` direktori, maka jalankan perintah berikut:

```
cd ../function-numpy
```

2. Tinjau [kode fungsi](#). Fungsi mengimpor `numpy` perpustakaan, membuat `numpy` array sederhana, dan kemudian mengembalikan kode status dummy dan body.

```
import json
import numpy as np

def lambda_handler(event, context):

    x = np.arange(15, dtype=np.int64).reshape(3, 5)
```

```
print(x)

return {
    'statusCode': 200,
    'body': json.dumps('Hello from Lambda!')}
}
```

3. Buat paket penyebaran file.zip menggunakan perintah berikut:

```
zip my_deployment_package.zip lambda_function.py
```

4. Menyebarkan fungsi. Dalam AWS CLI perintah berikut, ganti `--role` parameter dengan peran eksekusi AndaARN:

```
aws lambda create-function --function-name python_function_with_numpy \
    --runtime python3.11 \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::123456789012:role/lambda-role \
    --zip-file fileb://my_deployment_package.zip
```

5. Selanjutnya, pasang layer ke fungsi Anda. Dalam AWS CLI perintah berikut, ganti `--layers` parameter dengan versi layer AndaARN:

```
aws lambda update-function-configuration --function-name python_function_with_numpy \
    --cli-binary-format raw-in-base64-out \
    --layers "arn:aws:lambda:us-east-1:123456789012:layer:python-requests-layer:1"
```

6. Terakhir, coba panggil fungsi Anda menggunakan AWS CLI perintah berikut:

```
aws lambda invoke --function-name python_function_with_numpy \
    --cli-binary-format raw-in-base64-out \
    --payload '{"key": "value"}' response.json
```

Anda akan melihat output seperti ini:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
```

Anda dapat memeriksa log fungsi untuk memverifikasi bahwa kode mencetak numpy array ke standar keluar.

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Python

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan eksekusi. Untuk informasi selengkapnya tentang bagaimana objek konteks diteruskan ke handler fungsi, lihat [Tentukan penanganan fungsi Lambda dengan Python](#).

Metode konteks

- `get_remaining_time_in_millis` – Mengembalikan jumlah milidetik yang tersisa sebelum waktu eksekusi habis.

Properti konteks

- `function_name` – Nama fungsi Lambda.
- `function_version` – [Versi](#) fungsi.
- `invoked_function_arn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `memory_limit_in_mb` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `aws_request_id` – Pengidentifikasi permintaan invokasi.
- `log_group_name` – Grup log untuk fungsi.
- `log_stream_name` – Aliran log untuk instans fungsi.
- `identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
 - `cognito_identity_id` – Identitas Amazon Cognito terautentikasi.
 - `cognito_identity_pool_id` – Kumpulan identitas Amazon Cognito yang mengesahkan invokasi.
- `client_context` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
 - `client.installation_id`
 - `client.app_title`
 - `client.app_version_name`
 - `client.app_version_code`

- `client.app_package_name`
- `custom – dict` nilai khusus yang diatur oleh aplikasi klien seluler.
- `env`— Sebuah `dict` informasi lingkungan yang disediakan oleh AWS SDK.

Contoh berikut menunjukkan fungsi penanganan yang mencatat informasi konteks.

Example handler.py

```
import time

def lambda_handler(event, context):
    print("Lambda function ARN:", context.invoked_function_arn)
    print("CloudWatch log stream name:", context.log_stream_name)
    print("CloudWatch log group name:", context.log_group_name)
    print("Lambda Request ID:", context.aws_request_id)
    print("Lambda function memory limits in MB:", context.memory_limit_in_mb)
    # We have added a 1 second delay so you can see the time remaining in
    get_remaining_time_in_millis.
    time.sleep(1)
    print("Lambda time remaining in MS:", context.get_remaining_time_in_millis())
```

Selain opsi yang tercantum di atas, Anda juga dapat menggunakan AWS X-Ray SDK [Menginstrumentasi kode Python di AWS Lambda](#) untuk mengidentifikasi jalur kode kritis, melacak kinerjanya, dan menangkap data untuk dianalisis.

Log dan pantau fungsi Python Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda dan mengirim entri log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap pemanggilan dan output lainnya dari kode fungsi Anda ke aliran log. Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Untuk mengeluarkan log dari kode fungsi Anda, Anda dapat menggunakan [logging](#) modul bawaan. Untuk entri yang lebih rinci, Anda dapat menggunakan pustaka logging apa pun yang menulis ke `stdout` atau `stderr`.

Mencetak ke log

Untuk mengirim output dasar ke log, Anda dapat menggunakan `print` metode dalam fungsi Anda. Contoh berikut mencatat nilai-nilai grup CloudWatch log Log dan aliran, dan objek acara.

Perhatikan bahwa jika fungsi Anda mengeluarkan log menggunakan pernyataan `print` Python, Lambda hanya dapat mengirim output CloudWatch log ke Log dalam format teks biasa. Untuk menangkap log di JSON terstruktur, Anda perlu menggunakan pustaka logging yang didukung. Untuk informasi selengkapnya, lihat [the section called “Menggunakan kontrol logging lanjutan Lambda dengan Python”](#).

Example `lambda_function.py`

```
import os
def lambda_handler(event, context):
    print('## ENVIRONMENT VARIABLES')
    print(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    print(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    print('## EVENT')
    print(event)
```

Example output log

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
/aws/lambda/my-function
2023/08/31/[$LATEST]3893xmpl17fac4485b47bb75b671a283c
## EVENT
{'key': 'value'}
```

```
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Duration: 15.74 ms Billed
Duration: 16 ms Memory Size: 128 MB Max Memory Used: 56 MB Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmpl1f1fb44f07bc535a1 SegmentId: 07f5xmpl2d1f6f85
Sampled: true
```

Runtime Python melakukan log baris START, END, dan REPORT untuk setiap invokasi. REPORTBaris tersebut mencakup data berikut:

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Menggunakan pustaka logging

Untuk log yang lebih detail, gunakan modul [logging](#) di pustaka standar, atau pustaka logging pihak ketiga mana pun yang menulis ke `stdout` atau `stderr`.

Untuk runtime Python yang didukung, Anda dapat memilih apakah log yang dibuat menggunakan `logging` modul standar ditangkap dalam teks biasa atau JSON. Untuk mempelajari selengkapnya, lihat [the section called “Menggunakan kontrol logging lanjutan Lambda dengan Python”](#).

Saat ini, format log default untuk semua runtime Python adalah teks biasa. Contoh berikut menunjukkan bagaimana output log yang dibuat menggunakan `logging` modul standar ditangkap dalam teks biasa di CloudWatch Log.

```
import os
```

```
import logging
logger = logging.getLogger()
logger.setLevel("INFO")

def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES')
    logger.info(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    logger.info(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    logger.info('## EVENT')
    logger.info(event)
```

Output dari logger mencakup tingkat log, stempel waktu, dan ID permintaan.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO] 2023-08-31T22:12:58.534Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 ##
ENVIRONMENT VARIABLES
[INFO] 2023-08-31T22:12:58.534Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 /aws/
lambda/my-function
[INFO] 2023-08-31T22:12:58.534Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 2023/01/31/
[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d
[INFO] 2023-08-31T22:12:58.535Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 ## EVENT
[INFO] 2023-08-31T22:12:58.535Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 {'key':
'value'}
END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Duration: 2.75 ms Billed
Duration: 3 ms Memory Size: 128 MB Max Memory Used: 56 MB Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl7c2534a87870b4370 SegmentId: 073cxmpl3e442861
Sampled: true
```

Note

Ketika format log fungsi Anda disetel ke teks biasa, pengaturan tingkat log default untuk runtime Python adalah WARN. Ini berarti bahwa Lambda hanya mengirimkan output log dari level WARN dan lebih rendah ke Log. CloudWatch Untuk mengubah tingkat log default, gunakan `logging.setLevel()` metode Python seperti yang ditunjukkan dalam kode contoh ini. Jika Anda menyetel format log fungsi Anda ke JSON, sebaiknya Anda mengonfigurasi level log fungsi Anda menggunakan Lambda Advanced Logging Controls dan bukan dengan menyetel level log dalam kode. Untuk mempelajari selengkapnya, lihat [the section called “Menggunakan penyaringan tingkat log dengan Python”](#)

Menggunakan kontrol logging lanjutan Lambda dengan Python

Untuk memberi Anda kontrol lebih besar atas bagaimana log fungsi Anda ditangkap, diproses, dan digunakan, Anda dapat mengonfigurasi opsi logging berikut untuk runtime Lambda Python yang didukung:

- Format log - pilih antara teks biasa dan format JSON terstruktur untuk log fungsi Anda
- Tingkat log - untuk log dalam format JSON, pilih tingkat detail log yang dikirim Lambda ke CloudWatch Amazon, seperti ERROR, DEBUG, atau INFO
- Grup log - pilih grup CloudWatch log fungsi Anda mengirim log ke

Untuk informasi selengkapnya tentang opsi pencatatan ini, dan petunjuk tentang cara mengonfigurasi fungsi Anda untuk menggunakannya, lihat [the section called “Konfigurasi log fungsi”](#).

Untuk mempelajari lebih lanjut tentang menggunakan format log dan opsi tingkat log dengan fungsi Lambda Python Anda, lihat panduan di bagian berikut.

Menggunakan log JSON terstruktur dengan Python

Jika Anda memilih JSON untuk format log fungsi Anda, Lambda akan mengirim keluaran log oleh pustaka CloudWatch logging standar Python ke JSON terstruktur. Setiap objek log JSON berisi setidaknya empat pasangan nilai kunci dengan kunci berikut:

- "timestamp"- waktu pesan log dihasilkan
- "level"- tingkat log yang ditetapkan untuk pesan
- "message"- isi pesan log
- "requestId"- ID permintaan unik untuk pemanggilan fungsi

Logging Pustaka Python juga dapat menambahkan pasangan nilai kunci tambahan seperti "logger" ke objek JSON ini.

Contoh di bagian berikut menunjukkan bagaimana output log yang dihasilkan menggunakan pustaka logging Python ditangkap CloudWatch di Log saat Anda mengonfigurasi format log fungsi Anda sebagai JSON.

Perhatikan bahwa jika Anda menggunakan `print` metode untuk menghasilkan output log dasar seperti yang dijelaskan dalam [the section called “Mencetak ke log”](#), Lambda akan menangkap output ini sebagai teks biasa, bahkan jika Anda mengonfigurasi format logging fungsi Anda sebagai JSON.

Output log JSON standar menggunakan pustaka logging Python

Contoh cuplikan kode dan keluaran log berikut menunjukkan bagaimana output log standar yang dihasilkan menggunakan logging pustaka Python ditangkap di CloudWatch Log saat format log fungsi Anda disetel ke JSON.

Example Kode pencatatan Python

```
import logging
logger = logging.getLogger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example Catatan log JSON

```
{
  "timestamp": "2023-10-27T19:17:45.586Z",
  "level": "INFO",
  "message": "Inside the handler function",
  "logger": "root",
  "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Mencatat parameter tambahan di JSON

Ketika format log fungsi Anda diatur ke JSON, Anda juga dapat mencatat parameter tambahan dengan pustaka logging Python standar dengan menggunakan kata kunci untuk extra meneruskan kamus Python ke output log.

Example Kode pencatatan Python

```
import logging

def lambda_handler(event, context):
    logging.info(
        "extra parameters example",
        extra={"a": "b", "b": [3]},
    )
```

Example Catatan log JSON

```
{
  "timestamp": "2023-11-02T15:26:28Z",
  "level": "INFO",
  "message": "extra parameters example",
  "logger": "root",
  "requestId": "3dbd5759-65f6-45f8-8d7d-5bdc79a3bd01",
  "a": "b",
  "b": [
    3
  ]
}
```

Pengecualian logging di JSON

Cuplikan kode berikut menunjukkan bagaimana pengecualian Python ditangkap dalam output log fungsi Anda saat Anda mengonfigurasi format log sebagai JSON. Perhatikan bahwa output log yang dihasilkan menggunakan `logging.exception` ditetapkan ERROR tingkat log.

Example Kode pencatatan Python

```
import logging

def lambda_handler(event, context):
    try:
        raise Exception("exception")
    except:
        logging.exception("msg")
```

Example Catatan log JSON

```
{
  "timestamp": "2023-11-02T16:18:57Z",
  "level": "ERROR",
  "message": "msg",
  "logger": "root",
  "stackTrace": [
    " File \"./var/task/lambda_function.py\", line 15, in lambda_handler\n    raise\nException(\"exception\")\n"
  ],
}
```

```
"errorType": "Exception",
"errorMessage": "exception",
"requestId": "3f9d155c-0f09-46b7-bdf1-e91dab220855",
"location": "/var/task/lambda_function.py:lambda_handler:17"
}
```

Log terstruktur JSON dengan alat logging lainnya

Jika kode Anda sudah menggunakan pustaka logging lain, seperti Powertools for AWS Lambda, untuk menghasilkan log terstruktur JSON, Anda tidak perlu membuat perubahan apa pun. AWS Lambda tidak menyandikan dua kali log apa pun yang sudah dikodekan JSON. Bahkan jika Anda mengonfigurasi fungsi Anda untuk menggunakan format log JSON, output logging Anda muncul CloudWatch dalam struktur JSON yang Anda tentukan.

Contoh berikut menunjukkan bagaimana output log yang dihasilkan menggunakan Powertools untuk AWS Lambda paket ditangkap di CloudWatch Log. Format output log ini sama apakah konfigurasi logging fungsi Anda diatur ke JSON atau TEXT. Untuk informasi selengkapnya tentang penggunaan Powertools untuk AWS Lambda, lihat [the section called “Menggunakan Powertools untuk AWS Lambda \(Python\) AWS SAM dan untuk logging terstruktur”](#) dan [the section called “Menggunakan Powertools untuk AWS Lambda \(Python\) AWS CDK dan untuk logging terstruktur”](#)

Example Cuplikan kode logging Python (menggunakan Powertools untuk) AWS Lambda

```
from aws_lambda_powertools import Logger

logger = Logger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example Catatan log JSON (menggunakan Powertools untuk) AWS Lambda

```
{
  "level": "INFO",
  "location": "lambda_handler:7",
  "message": "Inside the handler function",
  "timestamp": "2023-10-31 22:38:21,010+0000",
  "service": "service_undefined",
  "xray_trace_id": "1-654181dc-65c15d6b0fecbdd1531ecb30"
}
```


Menggunakan penyaringan tingkat log dengan Python

Dengan mengonfigurasi penyaringan tingkat log, Anda dapat memilih untuk mengirim hanya log dari tingkat logging tertentu atau lebih rendah ke Log. CloudWatch Untuk mempelajari cara mengonfigurasi pemfilteran tingkat log untuk fungsi Anda, lihat [the section called “Pemfilteran tingkat log”](#)

AWS Lambda Untuk memfilter log aplikasi Anda sesuai dengan tingkat lognya, fungsi Anda harus menggunakan log berformat JSON. Anda dapat mencapai ini dengan dua cara:

- Buat output log menggunakan pustaka logging Python standar dan konfigurasi fungsi Anda untuk menggunakan pemformatan log JSON. AWS Lambda kemudian memfilter output log Anda menggunakan pasangan nilai kunci “level” di objek JSON yang dijelaskan dalam [the section called “Menggunakan log JSON terstruktur dengan Python”](#) Untuk mempelajari cara mengonfigurasi format log fungsi Anda, lihat [the section called “Konfigurasi log fungsi”](#).
- Gunakan pustaka atau metode logging lain untuk membuat log terstruktur JSON dalam kode Anda yang menyertakan pasangan nilai kunci “level” yang menentukan tingkat keluaran log. Misalnya, Anda dapat menggunakan Powertools AWS Lambda untuk menghasilkan output log terstruktur JSON dari kode Anda.

Anda juga dapat menggunakan pernyataan cetak untuk menampilkan objek JSON yang berisi pengenalan tingkat log. Pernyataan cetak berikut menghasilkan output diformat JSON di mana tingkat log diatur ke INFO. AWS Lambda akan mengirim objek JSON ke CloudWatch Log jika level logging fungsi Anda diatur ke INFO, DEBUG, atau TRACE.

```
print({'msg':"My log message", "level":"info"})
```

Agar Lambda dapat memfilter log fungsi Anda, Anda juga harus menyertakan pasangan nilai “timestamp” kunci dalam keluaran log JSON Anda. Waktu harus ditentukan dalam format stempel waktu [RFC 3339](#) yang valid. Jika Anda tidak menyediakan stempel waktu yang valid, Lambda akan menetapkan log INFO level dan menambahkan stempel waktu untuk Anda.

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, sebaiknya instrumentasi fungsi Anda dengan AWS X-Ray X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log dengan AWS CLI

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBUIQgUmVxdWVzdElk0iA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2l1vb...",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0\"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15

detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
```

```

"events": [
  {
    "timestamp": 1559763003171,
    "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
    "ingestionTime": 1559763003309
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n$LATEST\n",
\r ...",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
    "ingestionTime": 1559763018353
  }
],
"nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}

```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Menggunakan alat logging dan pustaka lainnya

[Powertools for AWS Lambda \(Python\)](#) adalah toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang. [Utilitas Logger menyediakan logger](#) yang dioptimalkan Lambda yang mencakup informasi tambahan tentang konteks fungsi di semua fungsi Anda dengan output terstruktur sebagai JSON. Gunakan utilitas ini untuk melakukan hal berikut:

- Tangkap bidang kunci dari konteks Lambda, cold start, dan struktur logging output sebagai JSON
- Log peristiwa pemanggilan Lambda saat diinstruksikan (dininaktifkan secara default)
- Cetak semua log hanya untuk persentase pemanggilan melalui pengambilan sampel log (dininaktifkan secara default)
- Tambahkan kunci tambahan ke log terstruktur kapan saja
- Gunakan pemformat log kustom (Bring Your Own Formatter) untuk mengeluarkan log dalam struktur yang kompatibel dengan Logging RFC organisasi Anda

Menggunakan Powertools untuk AWS Lambda (Python) AWS SAM dan untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Python dengan [Powertools terintegrasi untuk](#) modul Python menggunakan aplikasi. AWS SAM Aplikasi ini mengimplementasikan backend API dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan hello world pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Python 3.9
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75](#) atau yang lebih baru. Jika Anda memiliki versi CLI yang lebih lama, lihat [Memutakhirkan AWS SAM CLI. AWS SAM](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan template Hello World Python.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type Zip --runtime python3.9 --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena `HelloWorldFunction` mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan URL aplikasi yang digunakan:

```
aws cloudformation describe-stacks --stack-name sam-app --query 'Stacks[0].Outputs[?OutputKey=='HelloWorldApi`'].OutputValue' --output text
```

6. Memanggil titik akhir API:

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name sam-app
```

Output log terlihat seperti ini:

```

2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
 2023-02-03T14:59:50.371000 INIT_START Runtime Version:
 python:3.9.v16 Runtime Version ARN: arn:aws:lambda:us-
 east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.112000
 START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
  "message": "Hello world API - HTTP 200",
  "timestamp": "2023-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYt0c9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYt0c9j",
  "function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
  "correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
  "xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  }
}
]

```



```

    },
    "function_name": "sam-app>HelloWorldFunction-YBg8yfYt0c9j",
    "service": "Powertools>HelloWorld",
    "ColdStart": [
      1.0
    ]
  }
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "HelloWorldInvocations",
            "Unit": "Count"
          }
        ]
      }
    ]
  }
},
"service": "Powertools>HelloWorld",
>HelloWorldInvocations": [
  1.0
]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000 END
RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000
REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Duration: 16.33 ms
Billed Duration: 17 ms Memory Size: 128 MB Max Memory Used: 64 MB Init
Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299 SegmentId: 3c5d18d735a1ced0
Sampled: true

```

8. Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Mengelola retensi log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log tanpa batas waktu, hapus grup log, atau konfigurasi periode retensi setelah itu secara CloudWatch otomatis menghapus log. Untuk mengatur penyimpanan log, tambahkan yang berikut ini ke AWS SAM templat Anda:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Menggunakan Powertools untuk AWS Lambda (Python) AWS CDK dan untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Python dengan [Powertools terintegrasi untuk modul AWS Lambda \(Python\)](#) menggunakan modul. AWS CDK Aplikasi ini mengimplementasikan backend API dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan pesan hello world.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Python 3.9
- [AWS CLI versi 2](#)

- [AWS CDK versi 2](#)
- [AWS SAM CLI versi 1.75](#) atau yang lebih baru. Jika Anda memiliki versi CLI yang lebih lama, lihat [Memutakhirkan AWS SAM CLI. AWS SAM](#)

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world  
cd hello-world
```

2. Inisialisasi aplikasi.

```
cdk init app --language python
```

3. Instal dependensi Python.

```
pip install -r requirements.txt
```

4. Buat direktori `lambda_function` di bawah folder `root`.

```
mkdir lambda_function  
cd lambda_function
```

5. Buat file `app.py` dan tambahkan kode berikut ke file. Ini adalah kode untuk fungsi Lambda.

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver  
from aws_lambda_powertools.utilities.typing import LambdaContext  
from aws_lambda_powertools.logging import correlation_paths  
from aws_lambda_powertools import Logger  
from aws_lambda_powertools import Tracer  
from aws_lambda_powertools import Metrics  
from aws_lambda_powertools.metrics import MetricUnit  
  
app = APIGatewayRestResolver()  
tracer = Tracer()  
logger = Logger()  
metrics = Metrics(namespace="PowertoolsSample")  
  
@app.get("/hello")  
@tracer.capture_method
```

```
def hello():
    # adding custom metrics
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
        value=1)

    # structured log
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
# Adding tracer
# See: https://docs.powertools.aws.dev/lambda-python/latest/core/tracer/
@tracer.capture_lambda_handler
# ensures metrics are flushed upon request completion/failure and capturing
# ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Buka direktori `hello_world`. Anda akan melihat file bernama `hello_world_stack.py`.

```
cd ..
cd hello_world
```

7. Buka `hello_world_stack.py` dan tambahkan kode berikut ke file. Ini berisi [Konstruktor Lambda](#), yang membuat fungsi Lambda, mengonfigurasi variabel lingkungan untuk Powertools dan menetapkan retensi log ke satu minggu, dan [Konstruktor ApiGatewayv 1](#), yang membuat REST API.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):
```

```
def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
    super().__init__(scope, construct_id, **kwargs)

    # Powertools Lambda Layer
    powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
        self,
        id="lambda-powertools",
        # At the moment we wrote this example, the aws_lambda_python_alpha CDK
        # constructor is in Alpha, so we use layer to make the example simpler
        # See https://docs.aws.amazon.com/cdk/api/v2/python/
        aws_cdk.aws_lambda_python_alpha/README.html
        # Check all Powertools layers versions here: https://
        docs.powertools.aws.dev/lambda-python/latest/#lambda-layer
        layer_version_arn=f"arn:aws:lambda:
{self.region}:017000801446:layer:AWSLambdaPowertoolsPythonV2:21"
    )

    function = lambda_.Function(self,
        'sample-app-lambda',
        runtime=lambda_.Runtime.PYTHON_3_9,
        layers=[powertools_layer],
        code = lambda_.Code.from_asset("./lambda_function/"),
        handler="app.lambda_handler",
        memory_size=128,
        timeout=Duration.seconds(3),
        architecture=lambda_.Architecture.X86_64,
        environment={
            "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
            "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
            "LOG_LEVEL": "INFO"
        }
    )

    apigw = apigwv1.RestApi(self, "PowertoolsAPI",
        deploy_options=apigwv1.StageOptions(stage_name="dev"))

    hello_api = apigw.root.add_resource("hello")
    hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
        proxy=True))

    CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Men-deploy aplikasi Anda.

```
cd ..
cdk deploy
```

9. Dapatkan URL aplikasi yang digunakan:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Memanggil titik akhir API:

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

11. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name HelloWorldStack
```

Output log terlihat seperti ini:

```
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
2023-02-03T14:59:50.371000 INIT_START Runtime Version:
python:3.9.v16 Runtime Version ARN: arn:aws:lambda:us-
east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.112000
START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
  "message": "Hello world API - HTTP 200",
  "timestamp": "2023-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYt0c9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYt0c9j",
```

```

"function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
"correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
"xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "function_name": "sam-app>HelloWorldFunction-YBg8yfYt0c9j",
  "service": "Powertools>HelloWorld",
  "ColdStart": [
    1.0
  ]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
          ]
        ],
        "Metrics": [
          {

```

```
        "Name": "HelloWorldInvocations",
        "Unit": "Count"
    }
]
},
"service": "PowertoolsHelloWorld",
"HelloWorldInvocations": [
    1.0
]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000 END
RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000
REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be    Duration: 16.33 ms
Billed Duration: 17 ms    Memory Size: 128 MB    Max Memory Used: 64 MB    Init
Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299    SegmentId: 3c5d18d735a1ced0
Sampled: true
```

12. Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
cdk destroy
```


AWS Lambdapengujian fungsi dengan Python

Note

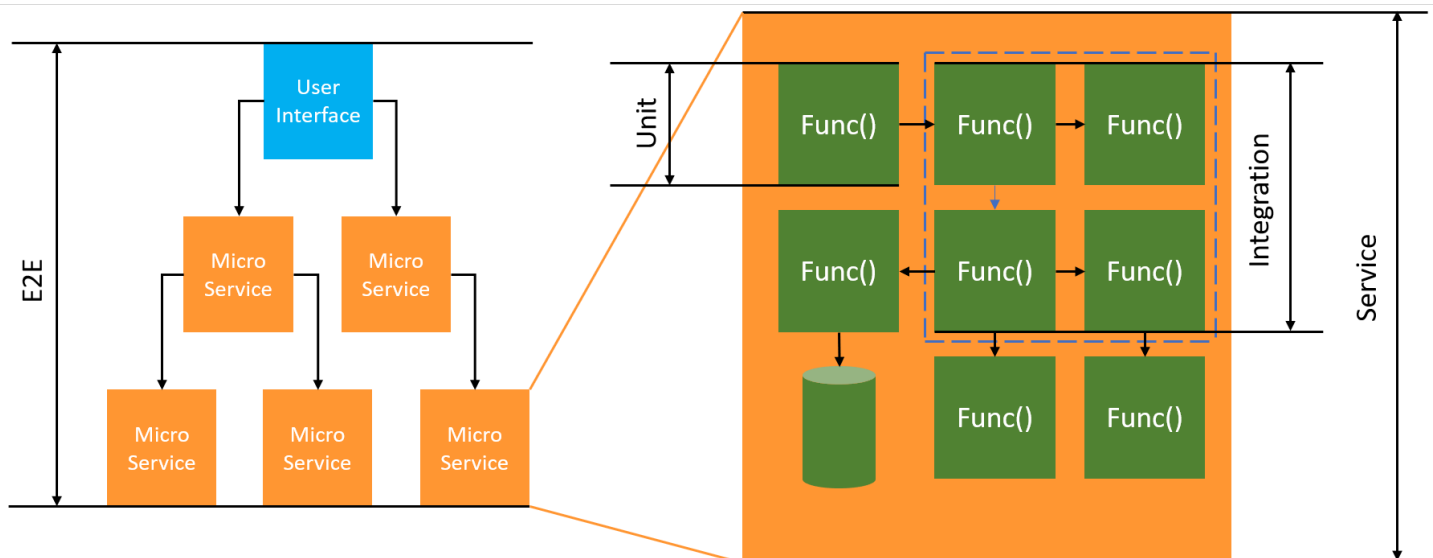
Lihat bagian [Fungsi pengujian](#) untuk pengenalan lengkap tentang teknik dan praktik terbaik untuk menguji solusi tanpa server.

Menguji fungsi tanpa server menggunakan jenis dan teknik pengujian tradisional, tetapi Anda juga harus mempertimbangkan pengujian aplikasi tanpa server secara keseluruhan. Pengujian berbasis cloud akan memberikan ukuran kualitas yang paling akurat dari fungsi dan aplikasi tanpa server Anda.

Arsitektur aplikasi tanpa server mencakup layanan terkelola yang menyediakan fungsionalitas aplikasi penting melalui panggilan API. Untuk alasan ini, siklus pengembangan Anda harus menyertakan pengujian otomatis yang memverifikasi fungsionalitas saat fungsi dan layanan Anda berinteraksi.

Jika Anda tidak membuat pengujian berbasis cloud, Anda dapat mengalami masalah karena perbedaan antara lingkungan lokal dan lingkungan yang diterapkan. Proses integrasi berkelanjutan Anda harus menjalankan pengujian terhadap serangkaian sumber daya yang disediakan di cloud sebelum mempromosikan kode Anda ke lingkungan penerapan berikutnya, seperti QA, Staging, atau Production.

Lanjutkan membaca panduan singkat ini untuk mempelajari strategi pengujian untuk aplikasi tanpa server, atau kunjungi [repositori Sampel Uji Tanpa Server](#) untuk menyelami contoh-contoh praktis, khusus untuk bahasa dan runtime pilihan Anda.



Untuk pengujian tanpa server, Anda masih akan menulis unit, integrasi, dan end-to-end pengujian.

- Tes unit - Tes yang dijalankan terhadap blok kode yang terisolasi. Misalnya, memverifikasi logika bisnis untuk menghitung biaya pengiriman yang diberikan item dan tujuan tertentu.
- Tes integrasi - Tes yang melibatkan dua atau lebih komponen atau layanan yang berinteraksi, biasanya di lingkungan cloud. Misalnya, memverifikasi fungsi memproses peristiwa dari antrian.
- End-to-end tes - Tes yang memverifikasi perilaku di seluruh aplikasi. Misalnya, memastikan infrastruktur diatur dengan benar dan bahwa peristiwa mengalir antar layanan seperti yang diharapkan untuk merekam pesanan pelanggan.

Menguji aplikasi tanpa server Anda

Anda biasanya akan menggunakan campuran pendekatan untuk menguji kode aplikasi tanpa server Anda, termasuk pengujian di cloud, pengujian dengan tiruan, dan kadang-kadang menguji dengan emulator.

Pengujian di cloud

Pengujian di cloud sangat berharga untuk semua fase pengujian, termasuk pengujian unit, pengujian integrasi, dan end-to-end pengujian. Anda menjalankan pengujian terhadap kode yang diterapkan di cloud dan berinteraksi dengan layanan berbasis cloud. Pendekatan ini memberikan ukuran kualitas kode Anda yang paling akurat.

Cara mudah untuk men-debug fungsi Lambda Anda di cloud adalah melalui konsol dengan acara pengujian. Peristiwa pengujian adalah input JSON ke fungsi Anda. Jika fungsi Anda tidak

memerlukan input, acara dapat berupa dokumen (`{}`) JSON kosong. Konsol menyediakan contoh peristiwa untuk berbagai integrasi layanan. Setelah membuat acara di konsol, Anda dapat membagikannya dengan tim Anda untuk membuat pengujian lebih mudah dan konsisten.

Note

[Menguji fungsi di konsol](#) adalah cara cepat untuk memulai, tetapi mengotomatiskan siklus pengujian Anda memastikan kualitas aplikasi dan kecepatan pengembangan.

Alat pengujian

Alat dan teknik ada untuk mempercepat loop umpan balik pengembangan. Misalnya, [AWSSAM Accelerate](#) dan [mode tontonan AWS CDK](#) mengurangi waktu yang diperlukan untuk memperbarui lingkungan cloud.

[Moto](#) adalah pustaka Python untuk mengejek AWS layanan dan sumber daya, sehingga Anda dapat menguji fungsi Anda dengan sedikit atau tanpa modifikasi menggunakan dekorator untuk mencegat dan mensimulasikan respons.

Fitur validasi [Powertools for \(AWS LambdaPython\)](#) menyediakan dekorator sehingga Anda dapat memvalidasi peristiwa input dan respons output dari fungsi Python Anda.

Untuk informasi lebih lanjut, baca posting blog [Unit Testing Lambda dengan Python](#) dan Mock Services. AWS

Untuk mengurangi latensi yang terkait dengan iterasi penerapan cloud, lihat Mode tontonan Accelerate, [AWSCloud Development Kit \(CDK\) AWS Serverless Application Model \(AWSAWSSAM\)](#). Alat-alat ini memantau infrastruktur dan kode Anda untuk perubahan. Mereka bereaksi terhadap perubahan ini dengan membuat dan menerapkan pembaruan tambahan secara otomatis ke lingkungan cloud Anda.

Contoh yang menggunakan alat ini tersedia di repositori kode [Sampel Uji Python](#).

Menginstrumentasi kode Python di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari tiga SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK for Python](#)— An SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.
- [Powertools for AWS Lambda \(Python\)](#) - Toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang untuk pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh. AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray](#). SDKs

Bagian-bagian

- [Menggunakan Powertools untuk AWS Lambda \(Python\) AWS SAM dan untuk melacak](#)
- [Menggunakan Powertools untuk AWS Lambda \(Python\) dan AWS CDK untuk melacak](#)
- [Menggunakan ADOT untuk instrumen fungsi Python Anda](#)
- [Menggunakan X-Ray SDK untuk instrumen fungsi Python Anda](#)

- [Mengaktifkan penelusuran dengan konsol Lambda](#)
- [Mengaktifkan penelusuran dengan Lambda API](#)
- [Mengaktifkan penelusuran dengan AWS CloudFormation](#)
- [Menafsirkan jejak X-Ray](#)
- [Menyimpan dependensi runtime dalam lapisan \(X-Ray\) SDK](#)

Menggunakan Powertools untuk AWS Lambda (Python) AWS SAM dan untuk melacak

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Python dengan [Powertools terintegrasi untuk modul AWS Lambda \(Python\)](#) menggunakan modul. AWS SAM Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan pesan hello world.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Python 3.9
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan file. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan template Hello World Python.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type Zip --runtime python3.9 --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena `HelloWorldFunction` mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name sam-app --query  
'Stacks[0].Outputs[?OutputKey=='HelloWorldApi'].OutputValue' --output text
```

6. Memanggil titik API akhir:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

```
New XRay Service Graph  
Start time: 2023-02-03 14:59:50+00:00  
End time: 2023-02-03 14:59:50+00:00  
Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYt0c9j -  
Edges: [1]  
Summary_statistics:  
  - total requests: 1  
  - ok count(2XX): 1  
  - error count(4XX): 0
```

```

- fault count(5XX): 0
- total response time: 0.924
Reference Id: 1 - AWS::Lambda::Function - sam-app>HelloWorldFunction-YBg8yfYt0c9j
- Edges: []
Summary_statistics:
- total requests: 1
- ok count(2XX): 1
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0.016
Reference Id: 2 - client - sam-app>HelloWorldFunction-YBg8yfYt0c9j - Edges: [0]
Summary_statistics:
- total requests: 0
- ok count(2XX): 0
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0

```

```

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
(1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
- 0.924s - sam-app>HelloWorldFunction-YBg8yfYt0c9j [HTTP: 200]
- 0.016s - sam-app>HelloWorldFunction-YBg8yfYt0c9j
- 0.739s - Initialization
- 0.016s - Invocation
- 0.013s - ## lambda_handler
- 0.000s - ## app.hello
- 0.000s - Overhead

```

8. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Menggunakan Powertools untuk AWS Lambda (Python) dan AWS CDK untuk melacak

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Python dengan [Powertools terintegrasi untuk modul AWS Lambda \(Python\)](#) menggunakan modul. AWS CDK Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan pesan hello world.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Python 3.9
- [AWS CLI versi 2](#)
- [AWS CDK versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan file. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world  
cd hello-world
```

2. Inisialisasi aplikasi.

```
cdk init app --language python
```

3. Instal dependensi Python.

```
pip install -r requirements.txt
```

4. Buat direktori lambda_function di bawah folder root.

```
mkdir lambda_function
```



```
cd lambda_function
```

5. Buat file `app.py` dan tambahkan kode berikut ke file. Ini adalah kode untuk fungsi Lambda.

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools import Logger
from aws_lambda_powertools import Tracer
from aws_lambda_powertools import Metrics
from aws_lambda_powertools.metrics import MetricUnit

app = APIGatewayRestResolver()
tracer = Tracer()
logger = Logger()
metrics = Metrics(namespace="PowertoolsSample")

@app.get("/hello")
@tracer.capture_method
def hello():
    # adding custom metrics
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
                      value=1)

    # structured log
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
# Adding tracer
# See: https://docs.powertools.aws.dev/lambda-python/latest/core/tracer/
@tracer.capture_lambda_handler
# ensures metrics are flushed upon request completion/failure and capturing
# ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Buka direktori `hello_world`. Anda akan melihat file bernama `hello_world_stack.py`.

```
cd ..
cd hello_world
```

7. Buka `hello_world_stack.py` dan tambahkan kode berikut ke file. [Ini berisi Konstruktor Lambda, yang membuat fungsi Lambda, mengonfigurasi variabel lingkungan untuk Powertools dan menetapkan retensi log ke satu minggu, dan Konstruktor 1, yang membuat file. ApiGatewayv REST API](#)

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        # Powertools Lambda Layer
        powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
            self,
            id="lambda-powertools",
            # At the moment we wrote this example, the aws_lambda_python_alpha CDK
            # constructor is in Alpha, o we use layer to make the example simpler
            # See https://docs.aws.amazon.com/cdk/api/v2/python/
            aws_cdk.aws_lambda_python_alpha/README.html
            # Check all Powertools layers versions here: https://
            docs.powertools.aws.dev/lambda-python/latest/#lambda-layer
            layer_version_arn=f"arn:aws:lambda:
{self.region}:017000801446:layer:AWSLambdaPowertoolsPythonV2:21"
        )

        function = lambda_.Function(self,
            'sample-app-lambda',
            runtime=lambda_.Runtime.PYTHON_3_9,
            layers=[powertools_layer],
            code = lambda_.Code.from_asset("./lambda_function/"),
            handler="app.lambda_handler",
```

```
        memory_size=128,
        timeout=Duration.seconds(3),
        architecture=lambda_.Architecture.X86_64,
        environment={
            "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
            "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
            "LOG_LEVEL": "INFO"
        }
    )

    apigw = apigwv1.RestApi(self, "PowertoolsAPI",
        deploy_options=apigwv1.StageOptions(stage_name="dev"))

    hello_api = apigw.root.add_resource("hello")
    hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
        proxy=True))

    CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Men-deploy aplikasi Anda.

```
cd ..
cdk deploy
```

9. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Memanggil titik API akhir:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message": "hello world"}
```

11. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

New XRay Service Graph

Start time: 2023-02-03 14:59:50+00:00

End time: 2023-02-03 14:59:50+00:00

Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYt0c9j - Edges: [1]

Summary_statistics:

- total requests: 1
- ok count(2XX): 1
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0.924

Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYt0c9j

- Edges: []

Summary_statistics:

- total requests: 1
- ok count(2XX): 1
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0.016

Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYt0c9j - Edges: [0]

Summary_statistics:

- total requests: 0
- ok count(2XX): 0
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)

- 0.924s - sam-app-HelloWorldFunction-YBg8yfYt0c9j [HTTP: 200]
- 0.016s - sam-app-HelloWorldFunction-YBg8yfYt0c9j
- 0.739s - Initialization
- 0.016s - Invocation
 - 0.013s - ## lambda_handler
 - 0.000s - ## app.hello
- 0.000s - Overhead

12. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
cdk destroy
```

Menggunakan ADOT untuk instrumen fungsi Python Anda

ADOT menyediakan [lapisan](#) Lambda yang dikelola sepenuhnya yang mengemas semua yang Anda butuhkan untuk mengumpulkan data telemetri menggunakan file. OTEL SDK Dengan menggunakan lapisan ini, Anda dapat menginstruksikan fungsi Lambda Anda tanpa harus memodifikasi kode fungsi apa pun. Anda juga dapat mengonfigurasi lapisan Anda untuk melakukan inisialisasi kustom. OTEL Untuk informasi selengkapnya, lihat [Konfigurasi khusus untuk ADOT Kolektor di Lambda](#) dalam dokumentasi. ADOT

Untuk runtime Python, Anda dapat menambahkan layer AWS Lambda terkelola untuk ADOT Python untuk secara otomatis instrumen fungsi Anda. Lapisan ini berfungsi untuk arsitektur arm64 dan x86_64. Untuk petunjuk rinci tentang cara menambahkan layer ini, lihat [AWS Distro untuk OpenTelemetry Lambda Support for ADOT Python](#) dalam dokumentasi.

Menggunakan X-Ray SDK untuk instrumen fungsi Python Anda

Untuk merekam detail tentang panggilan yang dilakukan oleh fungsi Lambda Anda ke sumber daya lain dalam aplikasi Anda, Anda juga dapat menggunakan. AWS X-Ray SDK for Python Untuk mendapatkan SDK, tambahkan `aws-xray-sdk` paket ke dependensi aplikasi Anda.

Example [requirements.txt](#)

```
jsonpickle==1.3
aws-xray-sdk==2.4.3
```

Dalam kode fungsi Anda, Anda dapat instrumen AWS SDK klien dengan menambal `boto3` perpustakaan dengan `aws_xray_sdk.core` modul.

Example [fungsi - Menelusuri klien AWS SDK](#)

```
import boto3
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

logger = logging.getLogger()
logger.setLevel(logging.INFO)
patch_all()

client = boto3.client('lambda')
```

```
client.get_account_settings()

def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES\r' + jsonpickle.encode(dict(**os.environ)))
    ...
```

Setelah Anda menambahkan dependensi yang benar dan membuat perubahan kode yang diperlukan, aktifkan penelusuran dalam konfigurasi fungsi Anda melalui konsol Lambda atau API

Mengaktifkan penelusuran dengan konsol Lambda

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

Mengaktifkan penelusuran dengan Lambda API

Konfigurasi penelusuran pada fungsi Lambda Anda dengan AWS CLI AWS SDK atau, gunakan operasi berikut API:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \
```

```
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

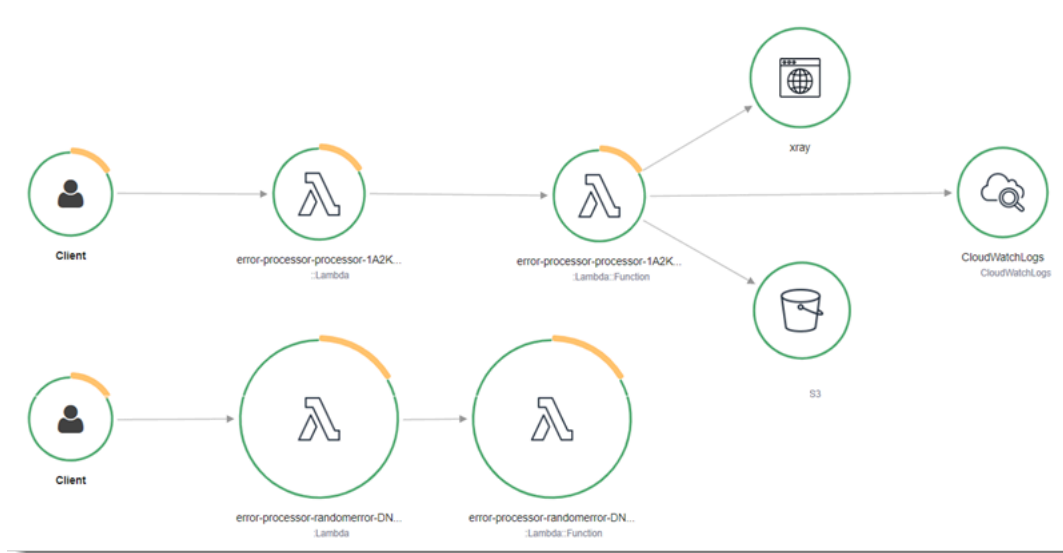
```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Menafsirkan jejak X-Ray

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses

kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch



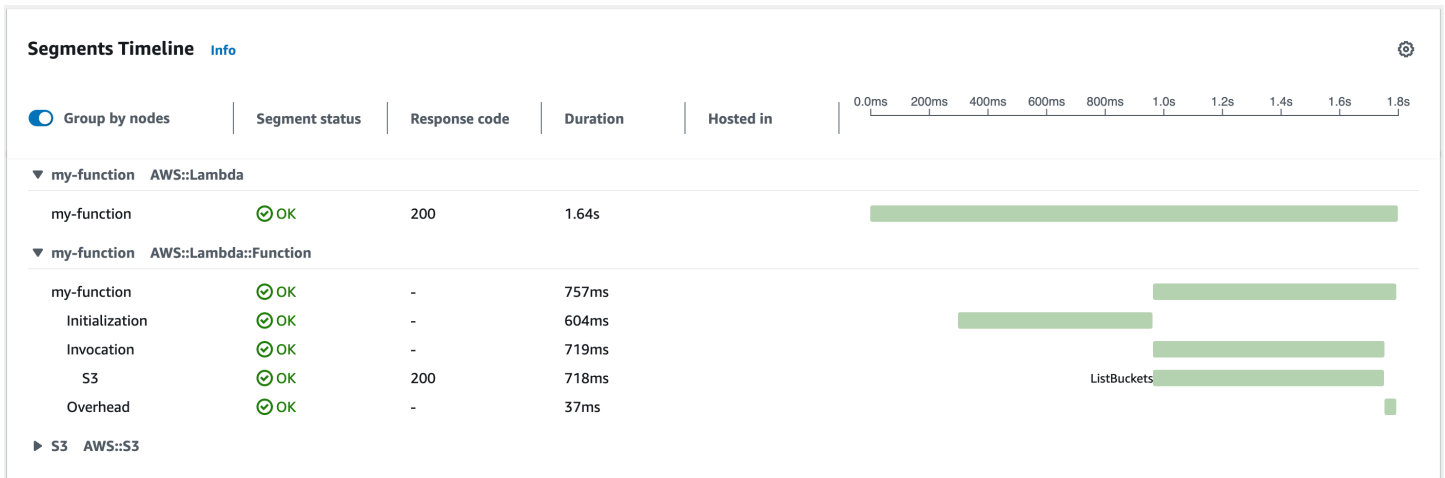
X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal AWS : : Lambda

dan yang lainnya memiliki asal usul. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat [the section called “Memahami jejak X-Ray”](#)

Anda juga dapat HTTP menginstrumentasikan klien, merekam SQL kueri, dan membuat subsegmen khusus dengan anotasi dan metadata. Untuk informasi selengkapnya, lihat [AWS X-Ray SDK for Python](#) di Panduan AWS X-Ray Pengembang.

Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi selengkapnya, lihat [harga AWS X-Ray](#).

Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK

Jika Anda menggunakan X-Ray SDK untuk instrumen AWS SDK klien kode fungsi Anda, paket penyebaran Anda bisa menjadi cukup besar. [Untuk menghindari mengunggah dependensi runtime setiap kali Anda memperbarui kode fungsi, paketkan X-Ray di SDK lapisan Lambda.](#)

Contoh berikut menunjukkan `AWS::Serverless::LayerVersion` sumber daya yang menyimpan file AWS X-Ray SDK for Python.

Example [template.yml](#) – Lapisan dependensi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
        ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-python-lib
      Description: Dependencies for the blank-python sample app.
```

```
ContentUri: package/.  
CompatibleRuntimes:  
- python3.8
```

Dengan konfigurasi ini, Anda memperbarui lapisan pustaka hanya jika Anda mengubah dependensi runtime Anda. Karena paket penerapan fungsi hanya berisi kode Anda, ini dapat membantu mengurangi waktu upload.

Membuat lapisan untuk dependensi memerlukan perubahan build untuk membuat arsip lapisan sebelum deployment. Untuk contoh pekerjaan, lihat aplikasi sampel [blank-python](#).

Membangun fungsi Lambda dengan Ruby

Anda dapat menjalankan kode Ruby di AWS Lambda. Lambda menyediakan [runtime](#) untuk Ruby yang menjalankan kode Anda untuk memproses peristiwa. Kode Anda berjalan di lingkungan yang menyertakan AWS SDK for Ruby, dengan kredensi dari peran AWS Identity and Access Management (IAM) yang Anda kelola. Untuk mempelajari lebih lanjut tentang SDK versi yang disertakan dengan runtime Ruby, lihat [the section called “Versi yang disertakan runtime SDK”](#)

Lambda mendukung runtime Ruby berikut.

Ruby

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|----------|------------------|-------------------|---------------------|------------------|-----------------------|
| Ruby 3.3 | ruby3.3 | Amazon Linux 2023 | | | |
| Ruby 3.2 | ruby3.2 | Amazon Linux 2 | | | |

Untuk membuat fungsi Ruby

1. Buka [Konsol Lambda](#).
2. Pilih Buat fungsi.
3. Konfigurasi pengaturan berikut:
 - Nama fungsi: Masukkan nama untuk fungsi tersebut.
 - Runtime: Pilih Ruby 3.2.
4. Pilih Buat fungsi.
5. Untuk mengonfigurasi peristiwa uji, pilih Uji.
6. Untuk Nama peristiwa, masukkan **test**.
7. Pilih Simpan perubahan.
8. Untuk mengaktifkan fungsi, pilih Uji.

Konsol membuat fungsi Lambda dengan satu file sumber bernama `lambda_function.rb`. Anda dapat mengedit file ini dan menambahkan lebih banyak file di editor kode bawaan. Untuk menyimpan perubahan Anda, pilih Simpan. Selanjutnya, untuk menjalankan kode, pilih Uji.

File `lambda_function.rb` mengekspor fungsi bernama `lambda_handler` yang menerima objek peristiwa dan objek konteks. Ini adalah [fungsi handler](#) yang dipanggil Lambda saat fungsi tersebut dipanggil. Fungsi waktu habis Ruby mendapatkan peristiwa invokasi dari Lambda dan meneruskannya ke handler. Dalam konfigurasi fungsi, nilai handler adalah `lambda_function.lambda_handler`.

Saat Anda menyimpan kode fungsi, konsol Lambda membuat paket penyebaran arsip file.zip. Saat Anda mengembangkan kode fungsi di luar konsol (menggunakan IDE), Anda perlu [membuat paket penerapan](#) untuk mengunggah kode Anda ke fungsi Lambda.

Runtime fungsi meneruskan objek konteks ke handler, selain peristiwa invokasi. [Objek konteks](#) berisi informasi tambahan tentang lingkungan invokasi, fungsi, dan eksekusi. Informasi selengkapnya tersedia dari variabel lingkungan.

Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log. Fungsi runtime mengirimkan detail tentang setiap pemanggilan ke Log. CloudWatch Detail tersebut menyampaikan [log yang dihasilkan fungsi Anda](#) selama invokasi. Jika fungsi mengembalikan kesalahan, Lambda memformat kesalahan dan mengembalikannya ke pemanggil.

Topik

- [Versi yang disertakan runtime SDK](#)
- [Mengaktifkan Ruby JIT Lainnya \(\) YJIT](#)
- [Tentukan penanganan fungsi Lambda di Ruby](#)
- [Deploy fungsi Lambda Ruby dengan arsip file .zip](#)
- [Deploy fungsi Ruby Lambda dengan gambar kontainer](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Ruby](#)
- [Log dan pantau fungsi Ruby Lambda](#)
- [Menginstrumentasi kode Ruby di AWS Lambda](#)

Versi yang disertakan runtime SDK

Versi yang AWS SDK disertakan dalam runtime Ruby tergantung pada versi runtime dan versi Anda. Wilayah AWS The AWS SDK for Ruby dirancang untuk menjadi modular dan dipisahkan oleh AWS

layanan. Untuk menemukan nomor versi permata layanan tertentu yang disertakan dalam runtime yang Anda gunakan, buat fungsi Lambda dengan kode dalam format berikut. Ganti `aws-sdk-s3` dan `Aws::S3` dengan nama permata layanan yang digunakan kode Anda.

```
require 'aws-sdk-s3'

def lambda_handler(event:, context:)
  puts "Service gem version: #{Aws::S3::GEM_VERSION}"
  puts "Core version: #{Aws::CORE_GEM_VERSION}"
end
```

Mengaktifkan Ruby JIT Lainnya () YJIT

Runtime Ruby 3.2 mendukung [YJIT](#), kompiler Ruby yang ringan dan minimalis. JIT YJIT memberikan kinerja yang jauh lebih tinggi, tetapi juga menggunakan lebih banyak memori daripada penerjemah Ruby. YJIT direkomendasikan untuk beban kerja Ruby on Rails.

YJIT tidak diaktifkan secara default. Untuk mengaktifkan fungsi Ruby 3.2, atur variabel `RUBY_YJIT_ENABLE` lingkungan ke 1. Untuk mengonfirmasi bahwa YJIT diaktifkan, cetak hasil `RubyVM::YJIT.enabled?` metode.

Example — Konfirmasikan bahwa YJIT diaktifkan

```
puts(RubyVM::YJIT.enabled?())
# => true
```

Tentukan penanganan fungsi Lambda di Ruby

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Topik

- [Dasar-dasar penanganan Ruby](#)
- [Praktik terbaik kode untuk fungsi Ruby Lambda](#)

Dasar-dasar penanganan Ruby

Dalam contoh berikut, file `function.rb` menentukan metode handler bernama `handler`. Fungsi handler mengambil dua objek sebagai input dan mengembalikan JSON dokumen.

Example `function.rb`

```
require 'json'

def handler(event:, context:)
  { event: JSON.generate(event), context: JSON.generate(context.inspect) }
end
```

Dalam konfigurasi fungsi Anda, pengaturan `handler` memberi tahu Lambda tempat untuk menemukan penanganan. Untuk contoh sebelumnya, nilai yang benar untuk pengaturan ini adalah **`function.handler`**. Ini mencakup dua nama yang dipisahkan oleh titik: nama file dan metode handler.

Anda juga dapat menentukan metode penanganan dalam kelas. Contoh berikut mendefinisikan metode penanganan bernama `process` pada kelas bernama `Handler` dalam modul bernama `LambdaFunctions`.

Example `source.rb`

```
module LambdaFunctions
  class Handler
    def self.process(event:, context:)
      "Hello!"
    end
  end
end
```

```
end
end
end
```

Dalam hal ini, pengaturan penanganan adalah **`source.LambdaFunctions::Handler.process`**.

Dua objek yang diterima handler adalah kejadian dan konteks invokasi. Kejadian tersebut adalah objek Ruby yang berisi muatan yang disediakan oleh pelaku invokasi. Jika payload adalah JSON dokumen, objek acara adalah hash Ruby. Jika tidak, objek kejadiannya adalah string. [Objek konteks](#) memiliki metode dan properti yang menyediakan informasi tentang invokasi, fungsi, dan lingkungan eksekusi.

Penangan fungsi dijalankan setiap kali fungsi Lambda Anda diinvokasi. Kode statis di luar penanganan dijalankan satu kali per instans fungsi. Jika handler Anda menggunakan sumber daya seperti SDK klien dan koneksi database, Anda dapat membuatnya di luar metode handler untuk menggunakannya kembali untuk beberapa pemanggilan.

Setiap instans fungsi Anda dapat memproses beberapa kejadian invokasi, tetapi hanya memproses satu kejadian dalam satu waktu. Jumlah instans yang memproses kejadian pada waktu tertentu adalah konkurensi fungsi Anda. Untuk informasi lebih lanjut tentang lingkungan eksekusi Lambda, lihat [Memahami siklus hidup lingkungan eksekusi Lambda](#).

Praktik terbaik kode untuk fungsi Ruby Lambda

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji. Misalnya, di Ruby, ini mungkin terlihat seperti:

```
def lambda_handler(event:, context:)
  foo = event['foo']
  bar = event['bar']

  result = my_lambda_function(foo:, bar:)
end

def my_lambda_function(foo:, bar:)
  // MyLambdaFunction logic here
```



```
end
```

- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk runtime Ruby, ini termasuk AWS SDK Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi. Untuk fungsi yang ditulis di Ruby, hindari mengunggah seluruh AWS SDK pustaka sebagai bagian dari paket penerapan Anda. Sebaliknya, secara selektif bergantung pada permata yang mengambil komponen yang SDK Anda butuhkan (misalnya permata DynamoDB atau Amazon SDK S3).
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.

- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Deploy fungsi Lambda Ruby dengan arsip file .zip

Kode AWS Lambda fungsi Anda terdiri dari file.rb yang berisi kode handler fungsi Anda, bersama dengan dependensi tambahan (permata) yang bergantung pada kode Anda. Untuk menyebarkan kode fungsi ini ke Lambda, Anda menggunakan paket penerapan. Paket ini dapat berupa arsip file.zip atau gambar kontainer. Untuk informasi selengkapnya tentang penggunaan gambar kontainer dengan Ruby, lihat [Menerapkan fungsi Ruby Lambda](#) dengan gambar kontainer.

[Untuk membuat paket penyebaran Anda sebagai arsip file.zip, Anda dapat menggunakan utilitas arsip file.zip bawaan alat baris perintah Anda, atau utilitas file.zip lainnya seperti 7zip.](#) Contoh yang ditampilkan di bagian berikut mengasumsikan Anda menggunakan zip alat baris perintah di lingkungan Linux atau macOS. Untuk menggunakan perintah yang sama di Windows, Anda dapat [menginstal Windows Subsystem untuk Linux untuk](#) mendapatkan versi Windows terintegrasi dari Ubuntu dan Bash.

Perhatikan bahwa Lambda menggunakan izin POSIX file, jadi Anda mungkin perlu [mengatur izin untuk folder paket penyebaran](#) sebelum membuat arsip file.zip.

Perintah contoh di bagian berikut menggunakan utilitas [Bundler](#) untuk menambahkan dependensi ke paket penyebaran Anda. Untuk menginstal bundler, jalankan perintah berikut.

```
gem install bundler
```

Bagian-bagian

- [Dependensi di Ruby](#)
- [Membuat paket penerapan.zip tanpa dependensi](#)
- [Membuat paket penerapan.zip dengan dependensi](#)
- [Membuat layer Ruby untuk dependensi Anda](#)
- [Membuat paket penerapan.zip dengan pustaka asli](#)
- [Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip](#)

Dependensi di Ruby

Untuk fungsi Lambda yang menggunakan runtime Ruby, dependensi dapat berupa permata Ruby apa pun. Ketika Anda menerapkan fungsi Anda menggunakan arsip.zip, Anda dapat menambahkan dependensi ini ke file.zip Anda dengan kode fungsi Anda atau menggunakan lapisan Lambda.

Lapisan adalah file.zip terpisah yang dapat berisi kode tambahan dan konten lainnya. Untuk mempelajari lebih lanjut tentang menggunakan layer Lambda, lihat. [Lapisan Lambda](#)

Runtime Ruby termasuk. AWS SDK for Ruby Jika fungsi Anda menggunakan SDK, Anda tidak perlu menggabungkannya dengan kode Anda. Namun, untuk mempertahankan kontrol penuh atas dependensi Anda, atau menggunakan versi tertentu dari dependensi SDK, Anda dapat menambahkannya ke paket penerapan fungsi Anda. Anda dapat menyertakan SDK dalam file.zip Anda, atau menambahkannya menggunakan lapisan Lambda. Dependensi di file.zip Anda atau di lapisan Lambda lebih diutamakan daripada versi yang disertakan dalam runtime. Untuk mengetahui versi Ruby mana yang SDK disertakan dalam versi runtime Anda, lihat. [the section called “Versi yang disertakan runtime SDK”](#)

Di bawah [model tanggung jawab AWS bersama](#), Anda bertanggung jawab atas pengelolaan dependensi apa pun dalam paket penerapan fungsi Anda. Ini termasuk menerapkan pembaruan dan patch keamanan. Untuk memperbarui dependensi dalam paket penerapan fungsi Anda, pertama buat file.zip baru dan kemudian unggah ke Lambda. Lihat [Membuat paket penerapan.zip dengan dependensi](#) dan [Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip](#) untuk informasi lebih lanjut.

Membuat paket penerapan.zip tanpa dependensi

Jika kode fungsi Anda tidak memiliki dependensi, file.zip Anda hanya berisi file.rb dengan kode handler fungsi Anda. Gunakan utilitas zip pilihan Anda untuk membuat file.zip dengan file.rb Anda di root. Jika file.rb tidak berada di root file.zip Anda, Lambda tidak akan dapat menjalankan kode Anda.

Untuk mempelajari cara menerapkan file.zip Anda untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada, lihat. [Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip](#)

Membuat paket penerapan.zip dengan dependensi

[Jika kode fungsi Anda bergantung pada permata Ruby tambahan, Anda dapat menambahkan dependensi ini ke file.zip Anda dengan kode fungsi Anda atau menggunakan lapisan Lambda.](#) Petunjuk di bagian ini menunjukkan cara memasukkan dependensi dalam paket penerapan.zip Anda. Untuk petunjuk tentang cara memasukkan dependensi Anda dalam lapisan, lihat. [the section called “Membuat layer Ruby untuk dependensi Anda”](#)

Misalkan kode fungsi Anda disimpan dalam file bernama `lambda_function.rb` di direktori proyek Anda. Contoh CLI perintah berikut membuat file.zip bernama `my_deployment_package.zip` berisi kode fungsi Anda dan dependensinya.

Untuk membuat paket deployment

1. Di direktori proyek Anda, buat a Gemfile untuk menentukan dependensi Anda di.

```
bundle init
```

2. Menggunakan editor teks pilihan Anda, edit Gemfile untuk menentukan dependensi fungsi Anda. Misalnya, untuk menggunakan TZInfo permata, edit Anda Gemfile agar terlihat seperti berikut ini.

```
source "https://rubygems.org"  
gem "tzinfo"
```

3. Jalankan perintah berikut untuk menginstal permata yang ditentukan Gemfile dalam direktori proyek Anda. Perintah ini ditetapkan vendor/bundle sebagai jalur default untuk instalasi permata.

```
bundle config set --local path 'vendor/bundle' && bundle install
```

Anda akan melihat output seperti yang berikut ini.

```
Fetching gem metadata from https://rubygems.org/.....  
Resolving dependencies...  
Using bundler 2.4.13  
Fetching tzinfo 2.0.6  
Installing tzinfo 2.0.6  
...
```

Note

Untuk menginstal permata secara global lagi nanti, jalankan perintah berikut.

```
bundle config set --local system 'true'
```

4. Buat arsip file.zip yang berisi lambda_function.rb file dengan kode handler fungsi Anda dan dependensi yang Anda instal pada langkah sebelumnya.

```
zip -r my_deployment_package.zip lambda_function.rb vendor
```

Anda akan melihat output seperti yang berikut ini.

```
adding: lambda_function.rb (deflated 37%)
  adding: vendor/ (stored 0%)
  adding: vendor/bundle/ (stored 0%)
  adding: vendor/bundle/ruby/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/build_info/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/cache/ (stored 0%)
  adding: vendor/bundle/ruby/3.2.0/cache/aws-eventstream-1.0.1.gem (deflated 36%)
...
```

Membuat layer Ruby untuk dependensi Anda

Instruksi di bagian ini menunjukkan kepada Anda bagaimana memasukkan dependensi Anda dalam lapisan. Untuk petunjuk tentang cara menyertakan dependensi Anda dalam paket penerapan Anda, lihat [the section called “Membuat paket penerapan.zip dengan dependensi”](#)

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam `/opt` direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, `PATH` variabel sudah menyertakan jalur folder tertentu dalam direktori `/opt` Untuk memastikan bahwa `PATH` variabel mengambil konten lapisan Anda, file `layer.zip` Anda harus memiliki dependensi di jalur folder berikut:

- `ruby/gems/2.7.0` (`GEM_PATH`)
- `ruby/lib` (`RUBYLIB`)

Misalnya, struktur file `layer.zip` Anda mungkin terlihat seperti berikut:

```
json.zip
# ruby/gems/2.7.0/
  | build_info
  | cache
  | doc
  | extensions
  | gems
  | # json-2.1.0
# specifications
  # json-2.1.0.gemspec
```

Selain itu, Lambda secara otomatis mendeteksi pustaka apa pun di `/opt/lib` direktori, dan binari apa pun di direktori `/opt/bin`. Untuk memastikan bahwa Lambda menemukan konten layer Anda dengan benar, Anda juga dapat membuat layer dengan struktur berikut:

```
custom-layer.zip
# lib
  | lib_1
  | lib_2
# bin
  | bin_1
  | bin_2
```

Setelah Anda mengemas layer Anda, lihat [the section called “Membuat dan menghapus lapisan”](#) dan [the section called “Menambahkan lapisan”](#) untuk menyelesaikan setup layer Anda.

Membuat paket penerapan.zip dengan pustaka asli

Banyak permata Ruby umum seperti `nokogiri`, `nio4r`, dan `mysql` berisi ekstensi asli yang ditulis dalam C. Ketika Anda menambahkan pustaka yang berisi kode C ke paket penyebaran Anda, Anda harus membangun paket Anda dengan benar untuk memastikan bahwa itu kompatibel dengan lingkungan eksekusi Lambda.

Untuk aplikasi produksi, kami sarankan untuk membangun dan menerapkan kode Anda menggunakan AWS Serverless Application Model (AWS SAM). AWS SAM Gunakan `sam build --use-container` opsi untuk membangun fungsi Anda di dalam wadah Docker seperti Lambda. Untuk mempelajari lebih lanjut AWS SAM cara menggunakan kode fungsi, lihat [Membangun aplikasi](#) di Panduan AWS SAM Pengembang.

Untuk membuat paket penerapan.zip yang berisi permata dengan ekstensi asli tanpa menggunakan AWS SAM, Anda dapat menggunakan container untuk menggabungkan dependensi Anda di lingkungan yang sama dengan lingkungan runtime Lambda Ruby. Untuk menyelesaikan langkah-langkah ini, Anda harus menginstal Docker di mesin build Anda. Untuk mempelajari lebih lanjut tentang menginstal Docker, lihat [Menginstal Docker Engine](#).

Untuk membuat paket penyebaran.zip dalam wadah Docker

1. Buat folder di mesin build lokal Anda untuk menyimpan wadah Anda. Di dalam folder itu, buat file bernama `dockerfile` dan tempel kode berikut ke dalamnya.

```
FROM public.ecr.aws/sam/build-ruby3.2:latest-x86_64
```

```
RUN gem update bundler  
CMD "/bin/bash"
```

2. Di dalam folder yang Anda `dockerfile` buat, jalankan perintah berikut untuk membuat wadah Docker.

```
docker build -t awsruby32 .
```

3. Arahkan ke direktori proyek yang berisi `.rb` file dengan kode handler fungsi Anda dan `Gemfile` menentukan dependensi fungsi Anda. Dari dalam direktori itu, jalankan perintah berikut untuk memulai wadah Lambda Ruby.

Linux/macOS

```
docker run --rm -it -v $PWD:/var/task -w /var/task awsruby32
```

Note

Di macOS, Anda mungkin melihat peringatan yang memberi tahu Anda bahwa platform gambar yang diminta tidak cocok dengan platform host yang terdeteksi. Abaikan peringatan ini.

Windows PowerShell

```
docker run --rm -it -v ${pwd}:var/task -w /var/task awsruby32
```

Saat wadah Anda dimulai, Anda akan melihat prompt bash.

```
bash-4.2#
```

4. Konfigurasi utilitas bundel untuk menginstal permata yang ditentukan `Gemfile` dalam `vendor/bundle` direktori lokal Anda dan instal dependensi Anda.

```
bash-4.2# bundle config set --local path 'vendor/bundle' && bundle install
```

5. Buat paket deployment `.zip` dengan kode fungsi Anda dan dependensinya. Dalam contoh ini, file yang berisi kode handler fungsi Anda diberi nama `lambda_function.rb`.


```
bash-4.2# zip -r my_deployment_package.zip lambda_function.rb vendor
```

6. Keluar dari wadah dan kembali ke direktori proyek lokal Anda.

```
bash-4.2# exit
```

Anda sekarang dapat menggunakan paket penyebaran file.zip untuk membuat atau memperbarui fungsi Lambda Anda. Lihat [Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip](#)

Membuat dan memperbarui fungsi Ruby Lambda menggunakan file.zip

Setelah Anda membuat paket.zip deployment, Anda dapat menggunakannya untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada. Anda dapat menerapkan paket.zip Anda menggunakan konsol Lambda, the, AWS Command Line Interface dan Lambda. API Anda juga dapat membuat dan memperbarui fungsi Lambda menggunakan AWS Serverless Application Model (AWS SAM) dan. AWS CloudFormation

Ukuran maksimum untuk paket.zip deployment untuk Lambda adalah 250 MB (unzip). Perhatikan bahwa batas ini berlaku untuk ukuran gabungan semua file yang Anda unggah, termasuk lapisan Lambda apa pun.

Runtime Lambda membutuhkan izin untuk membaca file dalam paket deployment Anda. Dalam notasi oktal izin Linux, Lambda membutuhkan 644 izin untuk file yang tidak dapat dieksekusi (rw-r - r--) dan 755 izin () untuk direktori dan file yang dapat dieksekusi. rwxr-xr-x

Di Linux dan macOS, gunakan chmod perintah untuk mengubah izin file pada file dan direktori dalam paket penyebaran Anda. Misalnya, untuk memberikan file yang dapat dieksekusi izin yang benar, jalankan perintah berikut.

```
chmod 755 <filepath>
```

Untuk mengubah izin file di Windows, lihat [Mengatur, Melihat, Mengubah, atau Menghapus Izin pada Objek](#) dalam dokumentasi Microsoft Windows.

Membuat dan memperbarui fungsi dengan file.zip menggunakan konsol

Untuk membuat fungsi baru, Anda harus terlebih dahulu membuat fungsi di konsol, lalu mengunggah arsip.zip Anda. Untuk memperbarui fungsi yang ada, buka halaman untuk fungsi Anda, lalu ikuti prosedur yang sama untuk menambahkan file.zip Anda yang diperbarui.

Jika file.zip Anda kurang dari 50MB, Anda dapat membuat atau memperbarui fungsi dengan mengunggah file langsung dari mesin lokal Anda. Untuk file.zip yang lebih besar dari 50MB, Anda harus mengunggah paket Anda ke bucket Amazon S3 terlebih dahulu. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS Management Console, lihat [Memulai Amazon S3](#). Untuk mengunggah file menggunakan AWS CLI, lihat [Memindahkan objek](#) di Panduan AWS CLI Pengguna.

Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Untuk membuat fungsi baru (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih Buat Fungsi.
2. Pilih Tulis dari awal.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda.
 - b. Untuk Runtime, pilih runtime yang ingin Anda gunakan.
 - c. (Opsional) Untuk Arsitektur, pilih arsitektur set instruksi untuk fungsi Anda. Arsitektur defaultnya adalah x86_64. Pastikan bahwa paket deployment .zip untuk fungsi Anda kompatibel dengan arsitektur set instruksi yang Anda pilih.
4. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan yang sudah ada.
5. Pilih Buat fungsi. Lambda menciptakan fungsi dasar 'Hello world' menggunakan runtime yang Anda pilih.

Untuk mengunggah arsip.zip dari mesin lokal Anda (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih file.zip.
5. Untuk mengunggah file.zip, lakukan hal berikut:
 - a. Pilih Unggah, lalu pilih file.zip Anda di pemilih file.
 - b. Pilih Buka.
 - c. Pilih Simpan.

Untuk mengunggah arsip.zip dari bucket Amazon S3 (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip baru.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih lokasi Amazon S3.
5. Rekatkan tautan Amazon S3 URL dari file.zip Anda dan pilih Simpan.

Memperbarui fungsi file.zip menggunakan editor kode konsol

Untuk beberapa fungsi dengan paket penyebaran.zip, Anda dapat menggunakan editor kode bawaan konsol Lambda untuk memperbarui kode fungsi Anda secara langsung. Untuk menggunakan fitur ini, fungsi Anda harus memenuhi kriteria berikut:

- Fungsi Anda harus menggunakan salah satu runtime bahasa yang ditafsirkan (Python, Node.js, atau Ruby)
- Paket penerapan fungsi Anda harus lebih kecil dari 3MB.

Kode fungsi untuk fungsi dengan paket penerapan gambar kontainer tidak dapat diedit langsung di konsol.

Untuk memperbarui kode fungsi menggunakan editor kode konsol

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.

2. Pilih tab Kode.
3. Di panel Sumber kode, pilih file kode sumber Anda dan edit di editor kode terintegrasi.
4. Setelah selesai mengedit kode, pilih Deploy untuk menyimpan perubahan dan memperbarui fungsi Anda.

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CLI

Anda dapat menggunakan [AWS CLI](#) untuk membuat fungsi baru atau memperbarui yang sudah ada menggunakan file.zip. Gunakan [create-function](#) dan [update-function-code](#) perintah untuk menyebarkan paket.zip Anda. Jika file.zip Anda lebih kecil dari 50MB, Anda dapat mengunggah paket.zip dari lokasi file di mesin build lokal Anda. Untuk file yang lebih besar, Anda harus mengunggah paket.zip Anda dari bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Note

Jika Anda mengunggah file.zip dari bucket Amazon S3 menggunakan AWS CLI bucket, bucket harus berada di lokasi Wilayah AWS yang sama dengan fungsi Anda.

Untuk membuat fungsi baru menggunakan file.zip dengan AWS CLI, Anda harus menentukan yang berikut:

- Nama fungsi Anda (`--function-name`)
- Runtime (`--runtime`) fungsi Anda
- Amazon Resource Name (ARN) dari [peran eksekusi](#) fungsi Anda (`--role`)
- Nama metode handler dalam kode fungsi Anda (`--handler`)

Anda juga harus menentukan lokasi file.zip Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda create-function --function-name myFunction \  
--runtime ruby3.2 --handler lambda_function.lambda_handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi seperti `--code` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `S3ObjectVersion` parameter untuk objek berversi.

```
aws lambda create-function --function-name myFunction \  
--runtime ruby3.2 --handler lambda_function.lambda_handler \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--code S3Bucket=amzn-s3-demo-  
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Untuk memperbarui fungsi yang ada menggunakan CLI, Anda menentukan nama fungsi Anda menggunakan `--function-name` parameter. Anda juga harus menentukan lokasi file.zip yang ingin Anda gunakan untuk memperbarui kode fungsi Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda update-function-code --function-name myFunction \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi `--s3-key` dan seperti `--s3-bucket` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `--s3-object-version` parameter untuk objek berversi.

```
aws lambda update-function-code --function-name myFunction \  
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject  
Version
```

Membuat dan memperbarui fungsi dengan file.zip menggunakan Lambda API

Untuk membuat dan memperbarui fungsi menggunakan arsip file.zip, gunakan API operasi berikut:

- [CreateFunction](#)
- [UpdateFunctionCode](#)

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS SAM

The AWS Serverless Application Model (AWS SAM) adalah toolkit yang membantu merampingkan proses membangun dan menjalankan aplikasi tanpa server. AWS Anda menentukan sumber daya

untuk aplikasi Anda dalam JSON template YAML atau dan menggunakan antarmuka baris AWS SAM perintah (AWS SAM CLI) untuk membangun, mengemas, dan menyebarkan aplikasi Anda. Saat Anda membuat fungsi Lambda dari AWS SAM template, AWS SAM secara otomatis membuat paket penerapan .zip atau gambar kontainer dengan kode fungsi Anda dan dependensi apa pun yang Anda tentukan. Untuk mempelajari lebih lanjut cara menggunakan AWS SAM untuk membangun dan menerapkan fungsi Lambda, [lihat Memulai](#) di Panduan AWS SAM AWS Serverless Application Model Pengembang.

Anda juga dapat menggunakan AWS SAM untuk membuat fungsi Lambda menggunakan arsip file.zip yang ada. Untuk membuat fungsi Lambda menggunakan AWS SAM, Anda dapat menyimpan file.zip di bucket Amazon S3 atau di folder lokal di mesin build Anda. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS SAM template Anda, `AWS::Serverless::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- diatur ke `Zip`
- `CodeUri`- diatur ke kode fungsi Amazon S3URI, jalur ke folder lokal, atau objek [FunctionCode](#)
- `Runtime`- Setel ke runtime yang Anda pilih

Dengan AWS SAM, jika file.zip Anda lebih besar dari 50MB, Anda tidak perlu mengunggahnya ke bucket Amazon S3 terlebih dahulu. AWS SAM dapat mengunggah paket.zip hingga ukuran maksimum yang diizinkan 250MB (unzip) dari lokasi di mesin build lokal Anda.

Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS SAM, lihat [AWS::Serverless::Function](#) dalam Panduan Pengembang AWS SAM

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk membuat fungsi Lambda menggunakan arsip file.zip. Untuk membuat fungsi Lambda dari file.zip, Anda harus terlebih dahulu mengunggah file Anda ke bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS CloudFormation template Anda, `AWS::Lambda::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- Setel ke `Zip`
- `Code`- Masukkan nama bucket Amazon S3 dan nama file.zip di dan bidang `S3Bucket` `S3Key`
- `Runtime`- Setel ke runtime yang Anda pilih

File.zip yang AWS CloudFormation menghasilkan tidak boleh melebihi 4MB. Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS CloudFormation, lihat [AWS: :Lambda: :Function](#) di Panduan Pengguna.AWS CloudFormation

Deploy fungsi Ruby Lambda dengan gambar kontainer

Ada tiga cara untuk membangun image container untuk fungsi Ruby Lambda:

- [Menggunakan gambar AWS dasar untuk Ruby](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [khusus](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Ruby](#) dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Ruby](#) dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi kontainer Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

Topik

- [AWS gambar dasar untuk Ruby](#)
- [Menggunakan gambar AWS dasar untuk Ruby](#)

- [Menggunakan gambar dasar alternatif dengan klien antarmuka runtime](#)

AWS gambar dasar untuk Ruby

AWS menyediakan gambar dasar berikut untuk Ruby:

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|-------|----------------|-------------------|---|-------------|
| 3.3 | Ruby 3.3 | Amazon Linux 2023 | Dockerfile untuk Ruby 3.3 di GitHub | |
| 3.2 | Ruby 3.2 | Amazon Linux 2 | Dockerfile untuk Ruby 3.2 di GitHub | |

ECR [Repositori Amazon: gallery.ecr.aws/lambda/ruby](https://gallery.ecr.aws/lambda/ruby)

Menggunakan gambar AWS dasar untuk Ruby

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#)
- Ruby

Membuat gambar dari gambar dasar

Untuk membuat gambar kontainer untuk Ruby

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Buat file baru bernama `Gemfile`. Di sinilah Anda mencantumkan RubyGems paket yang diperlukan aplikasi Anda. AWS SDK for Ruby Tersedia dari RubyGems. Anda harus memilih

permata AWS layanan tertentu untuk dipasang. Misalnya, untuk menggunakan [permata Ruby untuk Lambda](#), Gemfile Anda akan terlihat seperti ini:

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

Atau, permata [aws-sdk](#) berisi setiap permata layanan yang tersedia. AWS Permata ini sangat besar. Kami menyarankan Anda menggunakannya hanya jika Anda bergantung pada banyak AWS layanan.

3. [Instal dependensi yang ditentukan dalam Gemfile menggunakan bundle install.](#)

```
bundle install
```

4. Buat file baru bernamalambda_function.rb. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

Example Fungsi Ruby

```
module LambdaFunction
  class Handler
    def self.process(event:, context:)
      "Hello from Lambda!"
    end
  end
end
```

5. Buat Dockerfile baru. Berikut ini adalah contoh Dockerfile yang menggunakan gambar [AWS dasar](#). Dockerfiles ini menggunakan konfigurasi berikut:

- Atur FROM properti ke URI gambar dasar.
- Gunakan COPY perintah untuk menyalin kode fungsi dan dependensi runtime ke{LAMBDA_TASK_ROOT}, variabel lingkungan yang ditentukan [Lambda](#).
- Atur CMD argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/ruby:3.2

# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set the CMD to your handler (could also be done as a parameter override outside
of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Buat image Docker dengan perintah [docker build](#). Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

1. Mulai gambar Docker dengan perintah `docker run`. Dalam contoh ini, `docker-image` adalah nama gambar dan test tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

2. Dari jendela terminal baru, posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload": "hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload": "hello world!"}' -ContentType "application/json"
```

3. Dapatkan ID kontainer.

```
docker ps
```

- Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

- Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

- Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
```

```
"registryId": "111122223333",
"repositoryName": "hello-world",
"repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
"createdAt": "2023-03-09T10:39:01+00:00",
"imageTagMutability": "MUTABLE",
"imageScanningConfiguration": {
  "scanOnPush": true
},
"encryptionConfiguration": {
  "encryptionType": "AES256"
}
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repository URI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.

7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan gambar dasar alternatif dengan klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda.

Instal [klien antarmuka runtime Lambda untuk Ruby](#) menggunakan pengelola paket.org: RubyGems

```
gem install aws_lambda_riic
```

Anda juga dapat mengunduh [klien antarmuka runtime Ruby](#) dari GitHub. Klien antarmuka runtime mendukung Ruby versi 2.5.x hingga 2.7.x.

Contoh berikut menunjukkan bagaimana membangun image container untuk Ruby menggunakan gambar AWS non-dasar. Contoh Dockerfile menggunakan gambar dasar Ruby resmi. Dockerfile menyertakan klien antarmuka runtime.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [Docker](#)
- Ruby

Membuat gambar dari gambar dasar alternatif

Untuk membuat gambar kontainer untuk Ruby menggunakan gambar dasar alternatif

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example  
cd example
```


2. Buat file baru bernama `Gemfile`. Di sinilah Anda mencantumkan RubyGems paket yang diperlukan aplikasi Anda. AWS SDK for Ruby Tersedia dari RubyGems. Anda harus memilih permata AWS layanan tertentu untuk dipasang. Misalnya, untuk menggunakan [permata Ruby untuk Lambda](#), Gemfile Anda akan terlihat seperti ini:

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

Atau, permata [aws-sdk](#) berisi setiap permata layanan yang tersedia. AWS Permata ini sangat besar. Kami menyarankan Anda menggunakannya hanya jika Anda bergantung pada banyak AWS layanan.

3. [Instal dependensi yang ditentukan dalam Gemfile menggunakan bundle install.](#)

```
bundle install
```

4. Buat file baru bernama `lambda_function.rb`. Anda dapat menambahkan kode fungsi contoh berikut ke file untuk pengujian, atau menggunakan kode Anda sendiri.

Example Fungsi Ruby

```
module LambdaFunction
  class Handler
    def self.process(event:, context:)
      "Hello from Lambda!"
    end
  end
end
```

5. Buat Dockerfile baru. [Dockerfile berikut menggunakan gambar dasar Ruby alih-alih gambar dasar.AWS](#) Dockerfile menyertakan [klien antarmuka runtime untuk Ruby](#), yang membuat gambar kompatibel dengan Lambda. Atau, Anda dapat menambahkan klien antarmuka runtime ke Gemfile aplikasi Anda.

- Atur FROM properti ke gambar dasar Ruby.
- Buat direktori untuk kode fungsi dan variabel lingkungan yang menunjuk ke direktori itu. Dalam contoh ini, direktorinya adalah `/var/task`, yang mencerminkan lingkungan eksekusi Lambda. Namun, Anda dapat memilih direktori apa pun untuk kode fungsi karena Dockerfile tidak menggunakan gambar AWS dasar.

- Atur ENTRYPOINT ke modul yang Anda inginkan untuk menjalankan wadah Docker saat dimulai. Dalam hal ini, modul adalah klien antarmuka runtime.
- Atur CMD argumen ke penanganan fungsi Lambda.

Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM ruby:2.7

# Install the runtime interface client for Ruby
RUN gem install aws_lambda_riic

# Add the runtime interface client to the PATH
ENV PATH="/usr/local/bundle/bin:${PATH}"

# Create a directory for the Lambda function
ENV LAMBDA_TASK_ROOT=/var/task
RUN mkdir -p ${LAMBDA_TASK_ROOT}
WORKDIR ${LAMBDA_TASK_ROOT}

# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "aws_lambda_riic" ]

# Set the CMD to your handler (could also be done as a parameter override outside
of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar `docker-image` dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar secara lokal. Anda dapat [membangun emulator ke dalam gambar Anda](#) atau menggunakan prosedur berikut untuk menginstalnya di mesin lokal Anda.

Untuk menginstal dan menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Dari direktori proyek Anda, jalankan perintah berikut untuk mengunduh emulator antarmuka runtime (arsitektur x86-64) dari GitHub dan menginstalnya di mesin lokal Anda.

Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \  
  curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-  
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \  
  chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Untuk menginstal emulator arm64, ganti GitHub repositori URL di perintah sebelumnya dengan yang berikut:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/  
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Untuk menginstal emulator arm64, ganti `$downloadLink` dengan yang berikut ini:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Mulai gambar Docker dengan perintah `docker run`. Perhatikan hal berikut:

- `docker-image` adalah nama gambar dan test tag.
- `aws_lambda_rie lambda_function.LambdaFunction::Handler.process` adalah ENTRYPOINT diikuti oleh CMD dari Dockerfile Anda.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
    aws_lambda_rie lambda_function.LambdaFunction::Handler.process
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    aws_lambda_rie lambda_function.LambdaFunction::Handler.process
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

3. Posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

4. Dapatkan ID kontainer.

```
docker ps
```

5. Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{  
  "repository": {
```

```

    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}

```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoryURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.

7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.


```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Ruby

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Metode konteks

- `get_remaining_time_in_millis` – Mengembalikan jumlah milidetik yang tersisa sebelum waktu eksekusi habis.

Properti konteks

- `function_name` – Nama fungsi Lambda.
- `function_version` – [Versi](#) fungsi.
- `invoked_function_arn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `memory_limit_in_mb` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `aws_request_id` – Pengidentifikasi permintaan invokasi.
- `log_group_name` – Grup log untuk fungsi.
- `log_stream_name` – Aliran log untuk instans fungsi.
- `deadline_ms`— Tanggal saat eksekusi berakhir, dalam milidetik waktu Unix.
- `identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
- `client_context`— (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.

Log dan pantau fungsi Ruby Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda dan mengirim log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap invokasi ke pengaliran log, dan menyampaikan log serta output lain dari kode fungsi Anda. Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Halaman ini menjelaskan cara menghasilkan keluaran log dari kode fungsi Lambda Anda, dan mengakses log menggunakan AWS Command Line Interface, konsol Lambda, atau konsol CloudWatch

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)
- [Bekerja dengan pustaka logger Ruby](#)

Membuat fungsi yang mengembalikan log

Untuk menghasilkan log dari kode fungsi, Anda dapat menggunakan pernyataan `puts`, atau pustaka pencatatan apa pun yang menulis ke `stdout` atau `stderr`. Contoh berikut mencatat nilai variabel lingkungan dan objek peristiwa.

Example `lambda_function.rb`

```
# lambda_function.rb

def handler(event:, context:)
  puts "## ENVIRONMENT VARIABLES"
  puts ENV.to_a
  puts "## EVENT"
  puts event.to_a
end
```

Example format log

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
  'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]3893xmpl7fac4485b47bb75b671a283c',
  'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})
## EVENT
{'key': 'value'}
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Duration: 15.74 ms Billed
  Duration: 16 ms Memory Size: 128 MB Max Memory Used: 56 MB Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmplf1fb44f07bc535a1 SegmentId: 07f5xmpl2d1f6f85
  Sampled: true
```

Waktu pengoperasian Ruby melakukan log baris START, END, dan REPORT untuk setiap invokasi. Baris laporan memberikan perincian berikut.

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Untuk log yang lebih rinci, gunakan file [the section called “Bekerja dengan pustaka logger Ruby”](#).

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, sebaiknya instrumentasi fungsi Anda dengan AWS X-Ray X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBUIQgUmVxdWVzdE1k0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzV1NGZiMjEgVmVyc2l1vb...",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0\"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15

detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
```

```

"events": [
  {
    "timestamp": 1559763003171,
    "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
    "ingestionTime": 1559763003309
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n$LATEST\n",
\r ...",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
    "ingestionTime": 1559763018353
  }
],
"nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}

```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Bekerja dengan pustaka logger Ruby

[Pustaka logger](#) Ruby mengembalikan log yang disederhanakan yang mudah dibaca. Gunakan utilitas logger untuk menampilkan informasi rinci, pesan, dan kode kesalahan yang terkait dengan fungsi Anda.

```
# lambda_function.rb

require 'logger'

def handler(event:, context:)
  logger = Logger.new($stdout)
  logger.info('## ENVIRONMENT VARIABLES')
  logger.info(ENV.to_a)
  logger.info('## EVENT')
  logger.info(event)
  event.to_a
end
```

Output dari `logger` mencakup tingkat log, stempel waktu, dan ID permintaan.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO] 2020-01-31T22:12:58.534Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 ##
ENVIRONMENT VARIABLES

[INFO] 2020-01-31T22:12:58.534Z 1c8df7d3-xmpl-46da-9778-518e6eca8125
  environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d',
'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})

[INFO] 2020-01-31T22:12:58.535Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 ## EVENT

[INFO] 2020-01-31T22:12:58.535Z 1c8df7d3-xmpl-46da-9778-518e6eca8125 {'key':
'value'}

END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Duration: 2.75 ms Billed
Duration: 3 ms Memory Size: 128 MB Max Memory Used: 56 MB Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl17c2534a87870b4370 SegmentId: 073cxmpl3e442861
Sampled: true
```

Menginstrumentasi kode Ruby di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk memungkinkan Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, dari frontend API ke penyimpanan dan database di backend. Hanya dengan menambahkan SDK pustaka X-Ray ke konfigurasi build, Anda dapat merekam kesalahan dan latensi untuk panggilan apa pun yang dilakukan fungsi Anda ke AWS layanan.

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch



Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.

5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

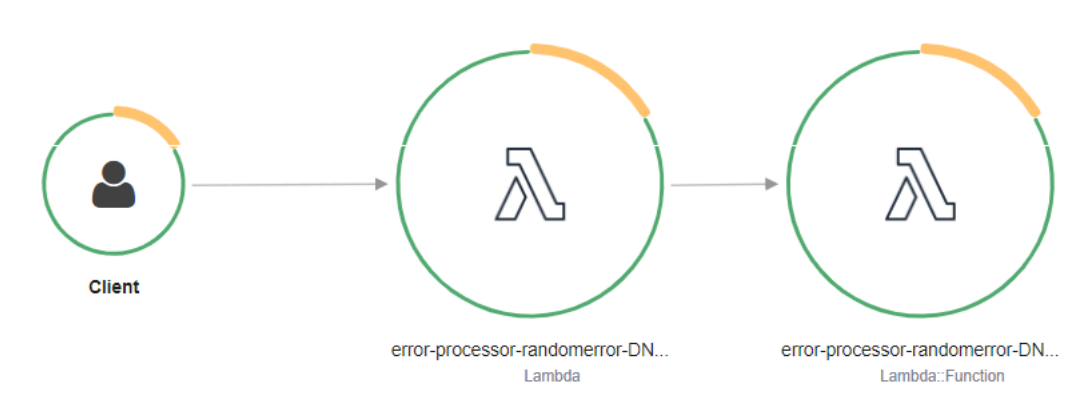
Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi selengkapnya, lihat [harga AWS X-Ray](#).

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda](#). Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

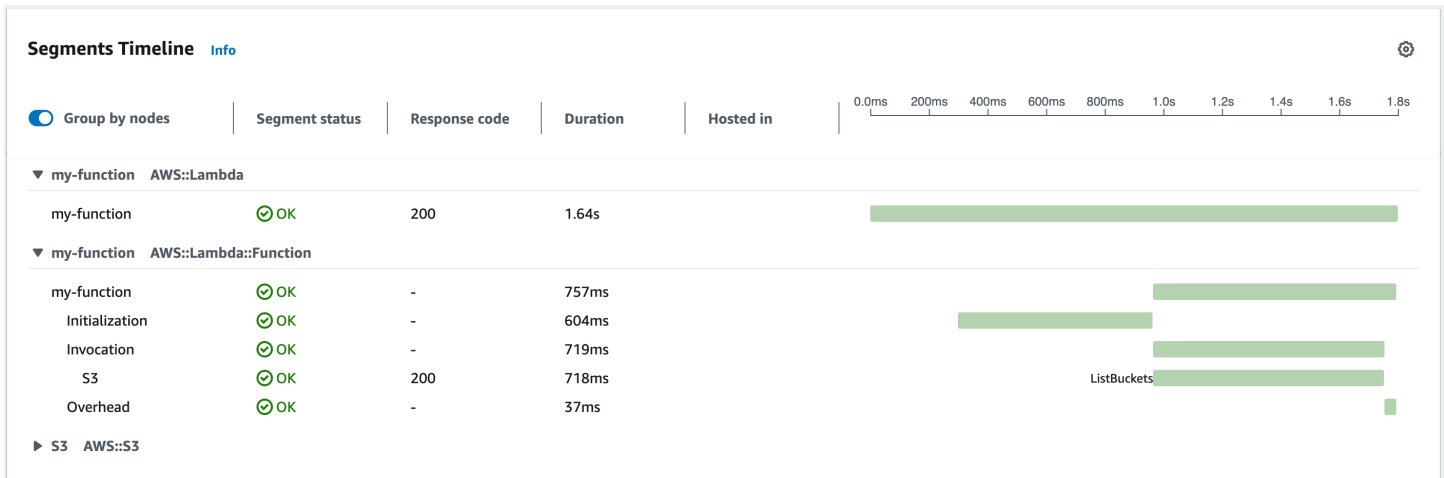
X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyortir dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal AWS : : Lambda

dan yang lainnya memiliki asal usul. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat. [the section called “Memahami jejak X-Ray”](#)

Anda dapat melakukan instrumentasi kode penanganan untuk merekam metadata dan melacak panggilan downstream. Untuk merekam detail tentang panggilan yang dilakukan handler Anda ke sumber daya dan layanan lain, gunakan X-Ray SDK untuk Ruby. Untuk mendapatkan SDK, tambahkan `aws-xray-sdk` paket ke dependensi aplikasi Anda.

Example [Kosong-Ruby/Fungsi/Gemfile](#)

```
# Gemfile
source 'https://rubygems.org'

gem 'aws-xray-sdk', '0.11.4'
gem 'aws-sdk-lambda', '1.39.0'
gem 'test-unit', '3.3.5'
```

Untuk instrumen AWS SDK klien, memerlukan `aws-xray-sdk/lambda` modul setelah membuat klien dalam kode inisialisasi.

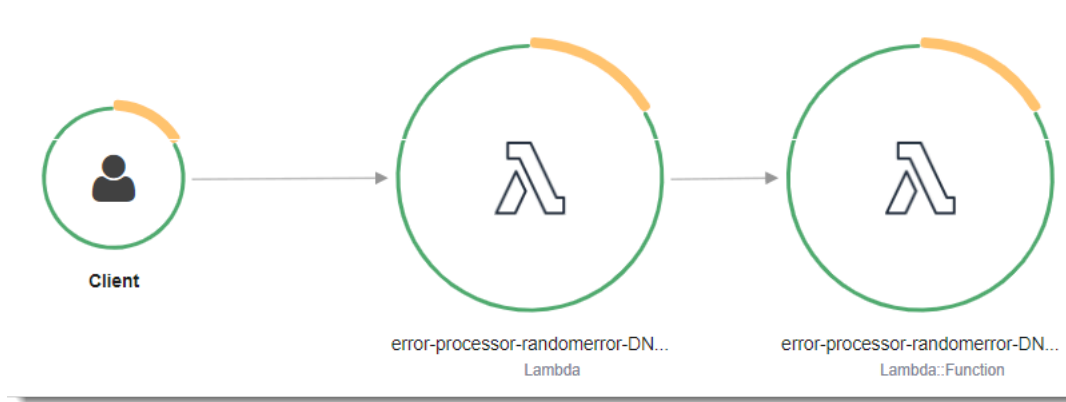
Example [blank-ruby/function/lambda_function.rb](#) - Menelusuri klien AWS SDK

```
# lambda_function.rb
require 'logger'
require 'json'
require 'aws-sdk-lambda'
$client = Aws::Lambda::Client.new()
$client.get_account_settings()

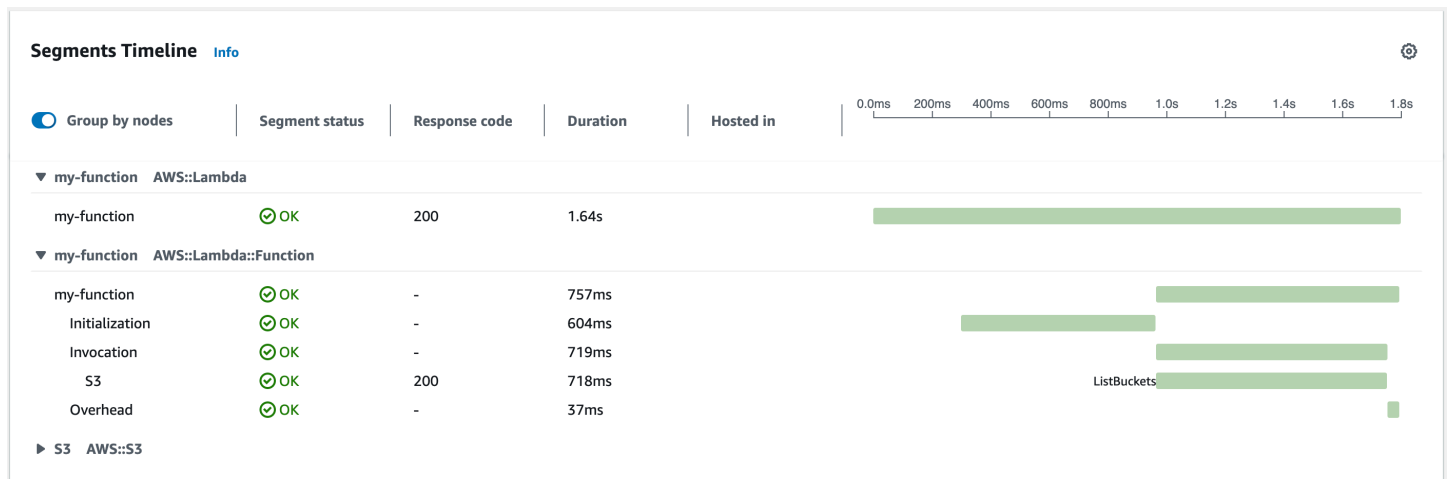
require 'aws-xray-sdk/lambda'

def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  ...
end
```

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal `usul`. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- **Inisialisasi** – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- **Doa** - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- **Overhead** - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat [the section called “Memahami jejak X-Ray”](#)

Anda juga dapat HTTP menginstrumentasikan klien, merekam SQL kueri, dan membuat subsegmen khusus dengan anotasi dan metadata. Untuk informasi selengkapnya, lihat [X-Ray SDK untuk Ruby](#) di Panduan AWS X-Ray Pengembang.

Bagian-bagian

- [Mengaktifkan penelusuran aktif dengan Lambda API](#)
- [Mengaktifkan penelusuran aktif dengan AWS CloudFormation](#)
- [Menyimpan dependensi runtime dalam satu lapisan](#)

Mengaktifkan penelusuran aktif dengan Lambda API

Untuk mengelola konfigurasi penelusuran dengan AWS CLI atau AWS SDK, gunakan API operasi berikut:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \  
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran aktif dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Lambda::Function  
    Properties:  
      TracingConfig:  
        Mode: Active  
      ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Serverless::Function  
    Properties:  
      Tracing: Active  
      ...
```

Menyimpan dependensi runtime dalam satu lapisan

Jika Anda menggunakan X-Ray SDK untuk instrumen AWS SDK klien kode fungsi Anda, paket penyebaran Anda bisa menjadi cukup besar. [Untuk menghindari mengunggah dependensi runtime setiap kali Anda memperbarui kode fungsi, paketkan X-Ray di SDK lapisan Lambda.](#)

Contoh berikut menunjukkan `AWS::Serverless::LayerVersion` sumber daya yang menyimpan X-Ray SDK untuk Ruby.

Example [template.yml](#) – Lapisan dependensi

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
        ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-ruby-lib
      Description: Dependencies for the blank-ruby sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - ruby2.5
```

Dengan konfigurasi ini, Anda memperbarui lapisan pustaka hanya jika Anda mengubah dependensi runtime Anda. Karena paket penerapan fungsi hanya berisi kode Anda, ini dapat membantu mengurangi waktu upload.

Membuat lapisan untuk dependensi memerlukan perubahan build untuk membuat arsip lapisan sebelum deployment. Untuk contoh pekerjaan, lihat aplikasi sampel [blank-ruby](#).

Membangun fungsi Lambda dengan Java

Anda dapat menjalankan kode Java di AWS Lambda. Lambda menyediakan [runtime](#) untuk Java yang menjalankan kode Anda untuk memproses peristiwa. Kode Anda berjalan di lingkungan Amazon Linux yang menyertakan AWS kredensial dari peran AWS Identity and Access Management (IAM) yang Anda kelola.

Lambda mendukung runtime Java berikut ini.

Java

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|---------|------------------|-------------------|---------------------|------------------|-----------------------|
| Jawa 21 | java21 | Amazon Linux 2023 | | | |
| Jawa 17 | java17 | Amazon Linux 2 | | | |
| Java 11 | java11 | Amazon Linux 2 | | | |
| Java 8 | java8.a12 | Amazon Linux 2 | | | |

Lambda menyediakan pustaka berikut untuk fungsi Java:

- [com.amazonaws:aws-lambda-java-core](#) (wajib) – Menentukan antarmuka metode handler dan objek konteks yang dilalui oleh runtime ke handler. Jika Anda menentukan jenis input Anda sendiri, ini adalah satu-satunya pustaka yang Anda butuhkan.
- [com.amazonaws:aws-lambda-java-events](#) – Jenis input untuk peristiwa dari layanan yang mengaktifkan fungsi Lambda.
- [com.amazonaws:aws-lambda-java-log4j2](#) – Pustaka appender untuk Apache Log4j 2 yang dapat Anda gunakan untuk menambahkan ID permintaan untuk invokasi saat ini ke [log fungsi](#).
- [AWS SDK for Java](#) 2.0 — SDK AWS resmi untuk bahasa pemrograman Java.

⚠ Important

Jangan gunakan komponen pribadi JDK API, seperti bidang pribadi, metode, atau kelas. Komponen API non-publik dapat berubah atau dihapus dalam pembaruan apa pun, menyebabkan aplikasi Anda rusak.

Untuk membuat fungsi Java

1. Buka [Konsol Lambda](#).
2. Pilih Buat fungsi.
3. Konfigurasi pengaturan berikut:
 - Nama fungsi: Masukkan nama untuk fungsi tersebut.
 - Runtime: Pilih Java 21.
4. Pilih Buat fungsi.
5. Untuk mengonfigurasi peristiwa uji, pilih Uji.
6. Untuk Nama peristiwa, masukkan **test**.
7. Pilih Simpan perubahan.
8. Untuk mengaktifkan fungsi, pilih Uji.

Konsol membuat fungsi Lambda dengan kelas handler bernama Hello. Karena Java adalah bahasa kompilasi, Anda tidak dapat melihat atau mengedit kode sumber di konsol Lambda, tetapi Anda dapat memodifikasi konfigurasinya, memanggilnya, dan mengonfigurasi pemicu.

📘 Note

Untuk memulai pengembangan aplikasi di lingkungan lokal Anda, gunakan salah satu [contoh aplikasi](#) yang tersedia di GitHub repositori panduan ini.

Kelas Hello memiliki fungsi bernama `handleRequest` yang mengambil objek peristiwa dan objek konteks. Ini adalah [fungsi handler](#) yang dipanggil Lambda saat fungsi tersebut dipanggil. Runtime fungsi Java mendapatkan peristiwa invokasi dari Lambda dan menyampaikannya ke handler. Dalam konfigurasi fungsi, nilai handler adalah `example.Hello::handleRequest`.

Untuk memperbarui kode fungsi, Anda membuat paket deployment, yang merupakan arsip file .zip yang berisi kode fungsi Anda. Seiring kemajuan pengembangan fungsi, Anda perlu menyimpan kode fungsi Anda dalam kontrol sumber, menambahkan pustaka, dan mengotomatiskan deployment. Mulai dengan [membuat paket deployment](#) dan memperbarui kode Anda di baris perintah.

Runtime fungsi melewati objek konteks ke handler, selain peristiwa invokasi. [Objek konteks](#) berisi informasi tambahan tentang lingkungan invokasi, fungsi, dan eksekusi. Informasi selengkapnya tersedia dari variabel lingkungan.

Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log. Fungsi runtime mengirimkan detail tentang setiap pemanggilan ke Log. CloudWatch Detail tersebut menyampaikan [log yang dihasilkan fungsi Anda](#) selama invokasi. Jika fungsi mengembalikan kesalahan, Lambda memformat kesalahan dan mengembalikannya ke pemanggil.

Topik

- [Tentukan penanganan fungsi Lambda di Java](#)
- [Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file](#)
- [Deploy fungsi Java Lambda dengan gambar kontainer](#)
- [Bekerja dengan lapisan untuk fungsi Java Lambda](#)
- [Meningkatkan kinerja startup dengan Lambda SnapStart](#)
- [Kustomisasi perilaku startup runtime Java untuk fungsi Lambda](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Java](#)
- [Log dan pantau fungsi Java Lambda](#)
- [Menginstrumentasi kode Java di AWS Lambda](#)
- [Contoh aplikasi Java untuk AWS Lambda](#)

Tentukan penanganan fungsi Lambda di Java

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

GitHub Repo untuk panduan ini menyediakan easy-to-deploy contoh aplikasi yang mendemonstrasikan berbagai jenis handler. Untuk detailnya, lihat [akhir topik ini](#).

Bagian-bagian

- [Contoh handler: Java 17 runtime](#)
- [Contoh handler: Java 11 runtime dan di bawahnya](#)
- [Kode inisialisasi](#)
- [Memilih tipe input dan output](#)
- [Antarmuka handler](#)
- [Praktik terbaik kode untuk fungsi Java Lambda](#)
- [Kode handler sampel](#)

Contoh handler: Java 17 runtime

Dalam contoh Java 17 berikut, kelas bernama `HandlerIntegerJava17` mendefinisikan metode handler bernama `handleRequest`. Metode handler mengambil input berikut:

- `AnIntegerRecord`, yang merupakan [catatan](#) Java kustom yang mewakili data peristiwa. Dalam contoh ini, kami mendefinisikan `IntegerRecord` sebagai berikut:

```
record IntegerRecord(int x, int y, String message) {  
}
```

- Sebuah [objek konteks](#), yang menyediakan metode dan properti yang memberikan informasi tentang pemanggilan, fungsi, dan lingkungan eksekusi.

Misalkan kita ingin menulis fungsi yang mencatat `message` dari `inputIntegerRecord`, dan mengembalikan jumlah `x` dan `y`. Berikut ini adalah kode fungsi:

Example [HandlerIntegerJava17.java](#)

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

// Handler value: example.HandlerInteger
public class HandlerIntegerJava17 implements RequestHandler<IntegerRecord, Integer>{

    @Override
    /*
     * Takes in an InputRecord, which contains two integers and a String.
     * Logs the String, then returns the sum of the two Integers.
     */
    public Integer handleRequest(IntegerRecord event, Context context)
    {
        LambdaLogger logger = context.getLogger();
        logger.log("String found: " + event.message());
        return event.x() + event.y();
    }
}

record IntegerRecord(int x, int y, String message) {
}
```

Anda menentukan metode mana yang ingin Lambda panggil dengan menyetel parameter handler pada konfigurasi fungsi Anda. Anda dapat mengekspresikan handler dalam format berikut:

- *package.Class::method* – Format penuh. Sebagai contoh: `example.Handler::handleRequest`.
- *package.Class*— Format singkatan untuk kelas yang mengimplementasikan antarmuka [handler](#). Sebagai contoh: `example.Handler`.

Saat Lambda memanggil handler Anda, [runtime Lambda](#) menerima peristiwa sebagai string yang JSON diformat -dan mengubahnya menjadi objek. Untuk contoh sebelumnya, contoh peristiwa mungkin terlihat seperti berikut:

Example [event.json](#)

```
{
  "x": 1,
  "y": 20,
  "message": "Hello World!"
}
```

Anda dapat menyimpan file ini dan menguji fungsi Anda secara lokal dengan perintah AWS Command Line Interface (CLI) berikut:

```
aws lambda invoke --function-name function_name --payload file:///event.json out.json
```

Contoh handler: Java 11 runtime dan di bawahnya

Lambda mendukung catatan di Java 17 dan runtime yang lebih baru. Di semua runtime Java, Anda dapat menggunakan kelas untuk mewakili data peristiwa. Contoh berikut mengambil daftar bilangan bulat dan objek konteks sebagai masukan, dan mengembalikan jumlah semua bilangan bulat dalam daftar.

Example [Handler.java](#)

Dalam contoh berikut, kelas bernama `Handler` menentukan metode handler bernama `handleRequest`. Metode handler mengambil peristiwa dan objek konteks sebagai input dan mengembalikan string.

Example [HandlerList.java](#)

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.List;

// Handler value: example.HandlerList
public class HandlerList implements RequestHandler<List<Integer>, Integer>{

    @Override
```

```
/*
 * Takes a list of Integers and returns its sum.
 */
public Integer handleRequest(List<Integer> event, Context context)
{
    LambdaLogger logger = context.getLogger();
    logger.log("EVENT TYPE: " + event.getClass().toString());
    return event.stream().mapToInt(Integer::intValue).sum();
}
}
```

Untuk contoh selengkapnya, lihat [Contoh kode handler](#).

Kode inisialisasi

Lambda menjalankan kode statis Anda dan konstruktor kelas selama [fase inisialisasi](#) sebelum menjalankan fungsi Anda untuk pertama kalinya. Sumber daya yang dibuat selama inisialisasi tetap berada di memori di antara pemanggilan dan dapat digunakan kembali oleh penanganan ribuan kali. Dengan demikian, Anda dapat menambahkan [kode inisialisasi](#) di luar metode handler utama Anda untuk menghemat waktu komputasi dan menggunakan kembali sumber daya di beberapa pemanggilan.

Dalam contoh berikut, kode inisialisasi klien berada di luar metode handler utama. Runtime menginisialisasi klien sebelum fungsi menyajikan acara pertamanya. Peristiwa selanjutnya jauh lebih cepat karena Lambda tidak perlu menginisialisasi klien lagi.

Example [Handler.java](#)

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.Map;

import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.GetAccountSettingsResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;

// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, String> {
```



```
private static final LambdaClient lambdaClient = LambdaClient.builder().build();

@Override
public String handleRequest(Map<String,String> event, Context context) {

    LambdaLogger logger = context.getLogger();
    logger.log("Handler invoked");

    GetAccountSettingsResponse response = null;
    try {
        response = lambdaClient.getAccountSettings();
    } catch(LambdaException e) {
        logger.log(e.getMessage());
    }
    return response != null ? "Total code size for your account is " +
response.accountLimit().totalCodeSize() + " bytes" : "Error";
}
}
```

Memilih tipe input dan output

Anda menentukan jenis objek yang peristiwa petakan ke tanda tangan metode handler. Dalam contoh sebelumnya, runtime Java mendeserialisasi peristiwa menjadi jenis yang mengimplementasikan antarmuka `Map<String,String>`. `tring-to-string` Peta S berfungsi untuk acara datar seperti berikut:

Example [Event.json](#) – Data cuaca

```
{
  "temperatureK": 281,
  "windKmh": -3,
  "humidityPct": 0.55,
  "pressureHPa": 1020
}
```

Namun, nilai setiap bidang harus berupa string atau angka. Jika kegiatan mencakup bidang yang memiliki objek sebagai nilai, runtime tidak dapat mendeserialisasi dan mengembalikan kesalahan.

Pilih jenis input yang berfungsi dengan data peristiwa yang diproses oleh fungsi Anda. Anda dapat menggunakan jenis dasar, jenis generik, atau jenis yang didefinisikan dengan baik.

Jenis input

- `Integer`, `Long`, `Double`, dll. — Peristiwa tersebut merupakan nomor tanpa format tambahan—misalnya, `3.5`. Runtime mengonversi nilai ke dalam objek dengan tipe yang ditentukan.
- `String`— Acara ini adalah JSON string, termasuk kutipan—misalnya, `"My string."` Runtime mengonversi nilai (tanpa tanda kutip) menjadi objek `String`.
- `Type`, `Map<String, Type>` dll. Event adalah sebuah JSON obyek. Runtime mendeserialisasikannya menjadi objek dengan jenis atau antarmuka yang ditentukan.
- `List<Integer>`, `List<String>`, `List<Object>`, dll. — Acara ini adalah JSON array. Runtime mendeserialisasikannya menjadi objek dengan jenis atau antarmuka yang ditentukan.
- `InputStream`- Acara ini adalah JSON jenis apa pun. Runtime menyampaikan aliran byte dokumen ke handler tanpa modifikasi. Anda mendeserialisasi input dan menuliskan output ke aliran output.
- Jenis pustaka — Untuk acara yang dikirim oleh AWS layanan, gunakan tipe di [aws-lambda-java-events](#) perpustakaan.

Jika Anda mendefinisikan tipe masukan Anda sendiri, itu harus berupa objek Java lama yang dapat diubah dan dapat diubah, dengan konstruktor dan properti default untuk setiap bidang dalam acara tersebut. POJO Kunci dalam peristiwa yang tidak memetakan ke properti serta properti yang tidak disertakan ke dalam peristiwa akan dijatuhkan tanpa kesalahan.

Tipe output dapat menjadi objek atau `void`. Runtime membuat serial nilai-nilai yang kembali ke dalam teks. Jika output adalah objek dengan bidang, runtime serialisasikannya ke dalam dokumen. JSON Jika ini adalah jenis yang membungkus nilai primitif, runtime mengembalikan representasi teks dari nilai tersebut.

Antarmuka handler

[aws-lambda-java-core](#) Pustaka mendefinisikan dua antarmuka untuk metode handler. Gunakan antarmuka yang disediakan untuk menyederhanakan konfigurasi handler dan memvalidasi tanda tangan metode handler pada waktu kompilasi.

- [com.amazonaws.services.lambda.runtime. RequestHandler](#)
- [com.amazonaws.services.lambda.runtime. RequestStreamHandler](#)

Antarmuka `RequestHandler` adalah jenis generik yang mengambil dua parameter: jenis input dan jenis output. Kedua jenis tersebut harus berupa objek. Saat Anda menggunakan antarmuka ini, runtime Java akan mendeserialisasi peristiwa menjadi objek dengan jenis input, dan menserialisasi output menjadi teks. Gunakan antarmuka ini saat serialisasi bawaan bekerja dengan tipe input dan output Anda.

Example [Handler.java](#) – Antarmuka handler

```
// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, String>{
    @Override
    public String handleRequest(Map<String,String> event, Context context)
```

Untuk menggunakan serialisasi Anda sendiri, terapkan antarmuka `RequestStreamHandler`. Dengan antarmuka ini, Lambda melewati aliran input dan aliran output ke handler Anda. Handler membaca byte dari aliran input, menuliskan aliran output, dan mengembalikan pembatalan.

Contoh Java 21 berikut menunjukkan bagaimana Anda dapat menggunakan fungsi Lambda untuk memproses pesanan. Contoh ini menggunakan jenis pembaca dan penulis buffer untuk bekerja dengan aliran input dan output, dan menunjukkan bagaimana Anda dapat menentukan catatan Java kustom untuk digunakan dalam fungsi Anda.

Example [HandlerStream.java](#)

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestStreamHandler;
import com.fasterxml.jackson.annotation.JsonProperty;
import com.fasterxml.jackson.databind.ObjectMapper;

import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.List;

public class HandlerStream implements RequestStreamHandler {

    private static final ObjectMapper objectMapper = new ObjectMapper();

    @Override
    public void handleRequest(InputStream input, OutputStream output, Context context)
    throws IOException {
        Order order = objectMapper.readValue(input, Order.class);
```

```
        processOrder(order);
        OrderAccepted orderAccepted = new OrderAccepted(order.orderId);

        objectMapper.writeValue(output, orderAccepted);
    }

    private void processOrder(Order order) {
        // business logic
    }

    public record Order(@JsonProperty("orderId") String orderId, @JsonProperty("items")
List<Item> items) { }

    public record Item(@JsonProperty("name") String name, @JsonProperty("quantity")
Integer quantity) { }

    public record OrderAccepted(@JsonProperty("orderId") String orderId) { }
}
```

Praktik terbaik kode untuk fungsi Java Lambda

Patuhi panduan dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji.
- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#). Misalnya, utamakan kerangka kerja injeksi dependensi Java (IoC) yang lebih sederhana seperti [Dagger](#) atau [Guice](#), daripada yang lebih kompleks seperti [Spring Framework](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi. Untuk fungsi yang ditulis di Java, hindari menggunggah seluruh AWS SDK pustaka sebagai bagian dari paket penerapan Anda. [Sebagai gantinya, secara selektif bergantung](#)

[pada modul yang mengambil komponen yang SDK Anda butuhkan \(misalnya DynamoDB, modul Amazon SDK S3, dan pustaka inti Lambda\).](#)

- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar

dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

- Hindari menggunakan DNS cache Java. Fungsi Lambda sudah cache DNS respons. Jika Anda menggunakan DNS cache lain, maka Anda mungkin mengalami batas waktu koneksi.

`java.util.logging.LoggerKelas` secara tidak langsung dapat mengaktifkan JVM DNS cache. Untuk mengganti pengaturan default, setel [networkaddress.cache.ttl](#) ke 0 sebelum menginisialisasi logger. Contoh:

```
public class MyHandler {
    // first set TTL property
    static{
        java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
    }
    // then instantiate logger
    var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
}
```

Untuk mencegah `UnknownHostException` kegagalan, kami sarankan pengaturan `networkaddress.cache.negative.ttl` ke 0. Anda dapat mengatur properti ini untuk fungsi Lambda dengan variabel `AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0` lingkungan.

Menonaktifkan JVM DNS cache tidak menonaktifkan cache terkelola Lambda. DNS

- Kurangi waktu yang dibutuhkan Lambda untuk membuka paket deployment yang ditulis di Java dengan meletakkan file `.jar` dependensi Anda dalam direktori/lib terpisah. Ini lebih cepat daripada memasukkan semua kode fungsi Anda dalam satu wadah yang berisi sejumlah besar file `.class`. Untuk instruksi, lihat [Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file](#).

Kode handler sampel

GitHub Repositori untuk panduan ini mencakup contoh aplikasi yang menunjukkan penggunaan berbagai jenis handler dan antarmuka. Setiap contoh aplikasi menyertakan skrip untuk penyebaran dan pembersihan yang mudah, AWS SAM templat, dan sumber daya pendukung.

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon GatewayAPI, Amazon, dan Amazon SQS Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan ketergantungan AWS SDK sebagai.
- [s3-java](#) — Fungsi Java yang memproses peristiwa notifikasi dari Amazon S3 dan menggunakan Java Class Library JCL () untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk memanggil fungsi.

s3-javaAplikasi java-events dan mengambil acara AWS layanan sebagai input dan mengembalikan string. Aplikasi java-basic meliputi beberapa jenis handler:

- [Handler.java](#) – Menggunakan `Map<String, String>` sebagai input.
- [HandlerInteger.java](#) — Mengambil `Integer` sebagai input.
- [HandlerList.java](#) — Mengambil `List<Integer>` sebagai input.
- [HandlerStream.java](#) — Mengambil `InputStream` dan `OutputStream` sebagai masukan.
- [HandlerString.java](#) — Mengambil `String` sebagai input.
- [HandlerWeatherData.java](#) — Mengambil tipe kustom sebagai input.

Untuk menguji jenis handler yang berbeda, cukup ubah nilai handler di template. AWS SAM Untuk instruksi terperinci, lihat file readme aplikasi sampel.

Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file

Kode AWS Lambda fungsi Anda terdiri dari skrip atau program yang dikompilasi dan dependensinya. Gunakan paket deployment untuk men-deploy fungsi kode Anda ke Lambda. Lambda mendukung dua tipe paket deployment: gambar kontainer dan arsip file .zip.

Halaman ini menjelaskan cara membuat paket deployment Anda sebagai file.zip atau file Jar, dan kemudian menggunakan paket deployment untuk menyebarkan kode fungsi Anda untuk AWS Lambda menggunakan (). AWS Command Line Interface AWS CLI

Bagian-bagian

- [Prasyarat](#)
- [Alat dan pustaka](#)
- [Membangun paket deployment dengan Gradle](#)
- [Membuat layer Java untuk dependensi Anda](#)
- [Membangun paket deployment dengan Maven](#)
- [Mengunggah paket penerapan dengan konsol Lambda](#)
- [Mengunggah paket penerapan dengan AWS CLI](#)
- [Mengunggah paket penerapan dengan AWS SAM](#)

Prasyarat

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Alat dan pustaka

Lambda menyediakan pustaka berikut untuk fungsi Java:

- [com.amazonaws: aws-lambda-java-core](#) (required) — Mendefinisikan antarmuka metode handler dan objek konteks yang diteruskan runtime ke handler. Jika Anda menentukan jenis input Anda sendiri, ini adalah satu-satunya pustaka yang Anda butuhkan.

- [com.amazonaws: aws-lambda-java-events](#) — Jenis masukan untuk acara dari layanan yang memanggil fungsi Lambda.
- [com.amazonaws: aws-lambda-java-log 4j2 - Pustaka appender untuk Apache Log4j 2 yang dapat Anda gunakan untuk menambahkan ID permintaan untuk pemanggilan saat ini ke log fungsi Anda.](#)
- [AWS SDK untuk Java 2.0](#) — Resmi AWS SDK untuk bahasa pemrograman Java.

Pustaka ini tersedia melalui [repositori pusat Maven](#). Tambahkan mereka ke definisi pembuatan Anda sebagai berikut:

Gradle

```
dependencies {  
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'  
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'  
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'  
}
```

Maven

```
<dependencies>  
  <dependency>  
    <groupId>com.amazonaws</groupId>  
    <artifactId>aws-lambda-java-core</artifactId>  
    <version>1.2.2</version>  
  </dependency>  
  <dependency>  
    <groupId>com.amazonaws</groupId>  
    <artifactId>aws-lambda-java-events</artifactId>  
    <version>3.11.1</version>  
  </dependency>  
  <dependency>  
    <groupId>com.amazonaws</groupId>  
    <artifactId>aws-lambda-java-log4j2</artifactId>  
    <version>1.5.1</version>  
  </dependency>  
</dependencies>
```

Untuk membuat paket deployment, kompilasi kode fungsi dan dependensi Anda ke dalam satu file.zip atau file Java Archive (.JAR). Untuk Gradle, [gunakan tipe build Zip](#). Untuk Apache Maven,

[gunakan plugin Maven Shade](#). Untuk mengunggah paket penerapan Anda, gunakan konsol Lambda, LambdaAPI, atau (). AWS Serverless Application Model AWS SAM

Note

Agar ukuran paket deployment Anda tetap kecil, kemas dependensi fungsi Anda dalam lapisan. Lapisan memungkinkan Anda mengelola dependensi secara mandiri, dapat digunakan oleh beberapa fungsi, dan dapat dibagikan ke akun lain. Untuk informasi selengkapnya, lihat [Lapisan Lambda](#).

Membangun paket deployment dengan Gradle

Untuk membuat paket penerapan dengan kode dan dependensi fungsi Anda di Gradle, gunakan tipe build. Zip Berikut adalah contoh dari contoh file [build.gradle lengkap](#):

Example build.gradle – Membangun tugas

```
task buildZip(type: Zip) {
    into('lib') {
        from(jar)
        from(configurations.runtimeClasspath)
    }
}
```

Konfigurasi bangunan ini menghasilkan paket deployment di direktori build/distributions. Dalam into('lib') pernyataan itu, jar tugas merakit arsip jar yang berisi kelas utama Anda ke dalam folder bernama lib. Selain itu, configurations.runtimeClassPath tugas menyalin pustaka dependensi dari classpath build ke folder yang sama. lib

Example build.gradle – Dependensi

```
dependencies {
    ...
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    implementation 'org.apache.logging.log4j:log4j-api:2.17.1'
    implementation 'org.apache.logging.log4j:log4j-core:2.17.1'
    runtimeOnly 'org.apache.logging.log4j:log4j-slf4j18-impl:2.17.1'
```

```
runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'  
...  
}
```

Lambda memuat JAR file dalam urutan abjad Unicode. Jika beberapa JAR file dalam `lib` direktori berisi kelas yang sama, yang pertama digunakan. Anda dapat menggunakan skrip shell berikut untuk mengidentifikasi kelas duplikat:

Example test-zip.sh

```
mkdir -p expanded  
unzip path/to/my/function.zip -d expanded  
find ./expanded/lib -name '*.jar' | xargs -n1 zipinfo -1 | grep '.*.class' | sort |  
uniq -c | sort
```

Membuat layer Java untuk dependensi Anda

Note

Menggunakan lapisan dengan fungsi dalam bahasa yang dikompilasi seperti Java mungkin tidak memberikan jumlah manfaat yang sama seperti dengan bahasa yang ditafsirkan seperti Python. Karena Java adalah bahasa yang dikompilasi, fungsi Anda masih harus memuat rakitan bersama secara manual ke dalam memori selama fase init, yang dapat meningkatkan waktu mulai dingin. Sebagai gantinya, kami sarankan untuk menyertakan kode bersama apa pun pada waktu kompilasi untuk memanfaatkan pengoptimalan kompiler bawaan apa pun.

Instruksi di bagian ini menunjukkan kepada Anda bagaimana memasukkan dependensi Anda dalam lapisan. Untuk petunjuk tentang cara menyertakan dependensi Anda dalam paket penerapan Anda, lihat atau [the section called “Membangun paket deployment dengan Gradle”](#) [the section called “Membangun paket deployment dengan Maven”](#)

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam `/opt` direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, `PATH` variabel sudah menyertakan jalur folder tertentu dalam direktori `/opt` Untuk memastikan bahwa `PATH` variabel mengambil konten lapisan Anda, file `layer.zip` Anda harus memiliki dependensi di jalur folder berikut:

- `java/lib (CLASSPATH)`

Misalnya, struktur file `layer.zip` Anda mungkin terlihat seperti berikut:

```
jackson.zip
# java/lib/jackson-core-2.2.3.jar
```

Selain itu, Lambda secara otomatis mendeteksi pustaka apa pun di `/opt/lib` direktori, dan binari apa pun di direktori `/opt/bin` Untuk memastikan bahwa Lambda menemukan konten layer Anda dengan benar, Anda juga dapat membuat layer dengan struktur berikut:

```
custom-layer.zip
# lib
  | lib_1
  | lib_2
# bin
  | bin_1
  | bin_2
```

Setelah Anda mengemas layer Anda, lihat [the section called “Membuat dan menghapus lapisan”](#) dan [the section called “Menambahkan lapisan”](#) untuk menyelesaikan setup layer Anda.

Membangun paket deployment dengan Maven

Untuk membangun paket deployment dengan Maven, gunakan [Plugin Maven Shade](#). Plugin membuat JAR file yang berisi kode fungsi yang dikompilasi dan semua dependensinya.

Example pom.xml – Konfigurasi plugin

```
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-shade-plugin</artifactId>
  <version>3.2.2</version>
  <configuration>
    <createDependencyReducedPom>>false</createDependencyReducedPom>
  </configuration>
  <executions>
    <execution>
      <phase>package</phase>
      <goals>
        <goal>shade</goal>
      </goals>
    </execution>
  </executions>
</plugin>
```

```

    </executions>
  </plugin>

```

Untuk membuat paket deployment, gunakan perintah `mvn package`.

```

[INFO] Scanning for projects...
[INFO] -----< com.example:java-maven >-----
[INFO] Building java-maven-function 1.0-SNAPSHOT
[INFO] -----[ jar ]-----
...
[INFO] --- maven-jar-plugin:2.4:jar (default-jar) @ java-maven ---
[INFO] Building jar: target/java-maven-1.0-SNAPSHOT.jar
[INFO]
[INFO] --- maven-shade-plugin:3.2.2:shade (default) @ java-maven ---
[INFO] Including com.amazonaws:aws-lambda-java-core:jar:1.2.2 in the shaded jar.
[INFO] Including com.amazonaws:aws-lambda-java-events:jar:3.11.1 in the shaded jar.
[INFO] Including joda-time:joda-time:jar:2.6 in the shaded jar.
[INFO] Including com.google.code.gson:gson:jar:2.8.6 in the shaded jar.
[INFO] Replacing original artifact with shaded artifact.
[INFO] Replacing target/java-maven-1.0-SNAPSHOT.jar with target/java-maven-1.0-
SNAPSHOT-shaded.jar
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 8.321 s
[INFO] Finished at: 2020-03-03T09:07:19Z
[INFO] -----

```

Perintah ini menghasilkan JAR file di target direktori.

Note

Jika Anda bekerja dengan [multi-release JAR \(MRJAR\)](#), Anda harus menyertakan MRJAR (yaitu shaded yang JAR dihasilkan oleh plugin Maven Shade) di `lib` direktori dan zip sebelum mengunggah paket penerapan Anda ke Lambda. Jika tidak, Lambda mungkin tidak membongkar JAR file Anda dengan benar, menyebabkan `MANIFEST.MF` file Anda diabaikan.

Jika Anda menggunakan pustaka appender (`aws-lambda-java-log4j2`), Anda juga harus mengonfigurasi trafo untuk plugin Maven Shade. Pustaka trafo menggabungkan versi file cache yang muncul di pustaka appender dan Log4j.

Example pom.xml – Konfigurasi plugin dengan appender Log4j 2

```

<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-shade-plugin</artifactId>
  <version>3.2.2</version>
  <configuration>
    <createDependencyReducedPom>>false</createDependencyReducedPom>
  </configuration>
  <executions>
    <execution>
      <phase>package</phase>
      <goals>
        <goal>shade</goal>
      </goals>
      <configuration>
        <transformers>
          <transformer
implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCacheFile
          </transformer>
        </transformers>
      </configuration>
    </execution>
  </executions>
  <dependencies>
    <dependency>
      <groupId>com.github.edwgiz</groupId>
      <artifactId>maven-shade-plugin.log4j2-cachefile-transformer</artifactId>
      <version>2.13.0</version>
    </dependency>
  </dependencies>
</plugin>


```

Mengunggah paket penerapan dengan konsol Lambda

Untuk membuat fungsi baru, Anda harus terlebih dahulu membuat fungsi di konsol, lalu mengunggah.zip atau JAR file Anda. Untuk memperbarui fungsi yang ada, buka halaman untuk fungsi Anda, lalu ikuti prosedur yang sama untuk menambahkan .zip atau JAR file Anda yang diperbarui.

Jika file paket penyebaran Anda kurang dari 50MB, Anda dapat membuat atau memperbarui fungsi dengan mengunggah file langsung dari mesin lokal Anda. Untuk.zip atau JAR file yang

lebih besar dari 50MB, Anda harus mengunggah paket Anda ke bucket Amazon S3 terlebih dahulu. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS Management Console, lihat [Memulai Amazon S3](#). Untuk mengunggah file menggunakan AWS CLI, lihat [Memindahkan objek](#) di Panduan AWS CLI Pengguna.

 Note

Anda tidak dapat mengubah [jenis paket penerapan](#) (.zip atau image kontainer) untuk fungsi yang ada. Misalnya, Anda tidak dapat mengonversi fungsi gambar kontainer untuk menggunakan arsip file.zip. Anda harus membuat fungsi baru.

Untuk membuat fungsi baru (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih Buat Fungsi.
2. Pilih Tulis dari awal.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda.
 - b. Untuk Runtime, pilih runtime yang ingin Anda gunakan.
 - c. (Opsional) Untuk Arsitektur, pilih arsitektur set instruksi untuk fungsi Anda. Arsitektur defaultnya adalah x86_64. Pastikan bahwa paket deployment .zip untuk fungsi Anda kompatibel dengan arsitektur set instruksi yang Anda pilih.
4. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan yang sudah ada.
5. Pilih Buat fungsi. Lambda menciptakan fungsi dasar 'Hello world' menggunakan runtime yang Anda pilih.

Untuk mengunggah .zip atau JAR arsip dari mesin lokal Anda (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah. Zip atau JAR file.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih file.zip atau .jar.
5. Untuk mengunggah .zip atau JAR file, lakukan hal berikut:

- a. Pilih Unggah, lalu pilih .zip atau JAR file Anda di pemilih file.
- b. Pilih Buka.
- c. Pilih Simpan.

Untuk mengunggah .zip atau JAR arsip dari bucket Amazon S3 (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah .zip atau JAR file baru.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih lokasi Amazon S3.
5. Rekatkan tautan Amazon S3 URL dari file.zip Anda dan pilih Simpan.

Mengunggah paket penerapan dengan AWS CLI

Anda dapat menggunakan [AWS CLI](#) untuk membuat fungsi baru atau memperbarui yang sudah ada menggunakan .zip atau JAR file. Gunakan [create-function](#) dan [update-function-code](#) perintah untuk menyebarkan .zip atau paket Anda. JAR Jika file Anda lebih kecil dari 50MB, Anda dapat mengunggah paket dari lokasi file di mesin build lokal Anda. Untuk file yang lebih besar, Anda harus mengunggah .zip atau JAR paket dari bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Note

Jika Anda mengunggah .zip atau JAR file dari bucket Amazon S3 menggunakan AWS CLI bucket, bucket harus berada di lokasi Wilayah AWS yang sama dengan fungsi Anda.

Untuk membuat fungsi baru menggunakan .zip atau JAR file dengan AWS CLI, Anda harus menentukan yang berikut:

- Nama fungsi Anda (`--function-name`)
- Runtime (`--runtime` fungsi Anda)
- Amazon Resource Name (ARN) dari [peran eksekusi](#) fungsi Anda (`--role`)
- Nama metode handler dalam kode fungsi Anda (`--handler`)

Anda juga harus menentukan lokasi .zip atau JAR file Anda. Jika .zip atau JAR file Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda create-function --function-name myFunction \  
--runtime java21 --handler example.handler \  
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi seperti `--code` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `S3ObjectVersion` parameter untuk objek berversi.

```
aws lambda create-function --function-name myFunction \  
--runtime java21 --handler example.handler \  
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \  
--code S3Bucket=amzn-s3-demo-  
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Untuk memperbarui fungsi yang ada menggunakan CLI, Anda menentukan nama fungsi Anda menggunakan `--function-name` parameter. Anda juga harus menentukan lokasi file.zip yang ingin Anda gunakan untuk memperbarui kode fungsi Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda update-function-code --function-name myFunction \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi `--s3-key` dan seperti `--s3-bucket` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `--s3-object-version` parameter untuk objek berversi.

```
aws lambda update-function-code --function-name myFunction \  
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject  
Version
```

Mengunggah paket penerapan dengan AWS SAM

Anda dapat menggunakan AWS SAM untuk mengotomatiskan penerapan kode fungsi, konfigurasi, dan dependensi Anda. AWS SAM adalah ekstensi yang menyediakan sintaks yang disederhanakan untuk mendefinisikan aplikasi tanpa server. AWS CloudFormation Templat contoh berikut mendefinisikan fungsi dengan paket deployment dalam direktori `build/distributions` yang digunakan Gradle:

Example template.yml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: An AWS Lambda application that calls the Lambda API.
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: build/distributions/java-basic.zip
      Handler: example.Handler
      Runtime: java21
      Description: Java function
      MemorySize: 512
      Timeout: 10
      # Function's execution role
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
        - AWSLambdaVPCLambdaAccessExecutionRole
      Tracing: Active
```

Untuk membuat fungsi, gunakan perintah `package` dan `deploy`. Perintah ini adalah kustomisasi ke AWS CLI. Mereka membungkus perintah lain untuk mengunggah paket penerapan ke Amazon S3, menulis ulang template dengan URI objek, dan memperbarui kode fungsi.

Skrip contoh berikut menjalankan pembuatan Gradle dan mengunggah paket deployment yang dibuatnya. Ini menciptakan AWS CloudFormation tumpukan saat pertama kali Anda menjalankannya. Jika tumpukan sudah ada, skrip akan memperbaruinya.

Example deploy.sh

```
#!/bin/bash
```

```
set -eo pipefail
aws cloudformation package --template-file template.yml --s3-bucket MY_BUCKET --output-
template-file out.yml
aws cloudformation deploy --template-file out.yml --stack-name java-basic --
capabilities CAPABILITY_NAMED_IAM
```

Untuk contoh kerja lengkap, lihat aplikasi sampel berikut:

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon GatewayAPI, Amazon, dan Amazon SQS Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan ketergantungan AWS SDK sebagai.
- [s3-java](#) — Fungsi Java yang memproses peristiwa notifikasi dari Amazon S3 dan menggunakan Java Class Library JCL () untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk memanggil fungsi.

Deploy fungsi Java Lambda dengan gambar kontainer

Ada tiga cara untuk membangun image container untuk fungsi Java Lambda:

- [Menggunakan gambar AWS dasar untuk Java](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [kustom](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Java](#) dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan [klien antarmuka runtime untuk Java](#) dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi penampung Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

Topik

- [AWS gambar dasar untuk Java](#)
- [Menggunakan gambar AWS dasar untuk Java](#)

- [Menggunakan gambar dasar alternatif dengan klien antarmuka runtime](#)

AWS gambar dasar untuk Java

AWS menyediakan gambar dasar berikut untuk Java:

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|-------|----------------|-------------------|--|-------------|
| 21 | Jawa 21 | Amazon Linux 2023 | Dockerfile untuk Java 21 di GitHub | |
| 17 | Jawa 17 | Amazon Linux 2 | Dockerfile untuk Java 17 di GitHub | |
| 11 | Java 11 | Amazon Linux 2 | Dockerfile untuk Java 11 di GitHub | |
| 8.al2 | Java 8 | Amazon Linux 2 | Dockerfile untuk Java 8 di GitHub | |

ECR [Repositori Amazon: gallery.ecr.aws/lambda/java](https://gallery.ecr.aws/lambda/java)

Gambar dasar Java 21 dan yang lebih baru didasarkan pada [gambar kontainer minimal Amazon Linux 2023](#). Gambar dasar sebelumnya menggunakan Amazon Linux 2. AL2023 memberikan beberapa keunggulan dibandingkan Amazon Linux 2, termasuk jejak penyebaran yang lebih kecil dan versi pustaka yang diperbarui seperti `glibc`

AL2 Gambar berbasis 023 menggunakan `microdnf` (symlinked `asdnf`) sebagai manajer paket, bukannya `dnf`, yang merupakan pengelola paket default di Amazon Linux 2. `microdnf` adalah implementasi mandiri dari `dnf`. Untuk daftar paket yang disertakan dalam gambar AL2 berbasis 023, lihat kolom Penampung Minimal di Membandingkan paket yang diinstal pada Gambar Kontainer [Amazon Linux 2023](#). Untuk informasi selengkapnya tentang perbedaan antara AL2 023 dan Amazon Linux 2, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di Blog Komputasi AWS .

Note

Untuk menjalankan gambar AL2 berbasis 023 secara lokal, termasuk with AWS Serverless Application Model (AWS SAM), Anda harus menggunakan Docker versi 20.10.10 atau yang lebih baru.

Menggunakan gambar AWS dasar untuk Java

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Java (misalnya, [Amazon Corretto](#))
- [Docker](#) (versi minimum 20.10.10 untuk Java 21 dan gambar dasar yang lebih baru)
- [Apache Maven](#) atau [Gradle](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Membuat gambar dari gambar dasar

Maven

1. Jalankan perintah berikut untuk membuat proyek Maven menggunakan [pola dasar](#) untuk Lambda. Parameter-parameter berikut diperlukan:
 - Layanan — AWS layanan Klien untuk digunakan dalam fungsi Lambda. Untuk daftar sumber yang tersedia, lihat [aws-sdk-java-v2/layanan](#) di GitHub.
 - wilayah — Wilayah AWS Tempat Anda ingin membuat fungsi Lambda.
 - groupId— Namespace paket lengkap aplikasi Anda.
 - artifactId— Nama proyek Anda. Ini menjadi nama direktori untuk proyek Anda.

Di Linux dan macOS, jalankan perintah ini:

```
mvn -B archetype:generate \  
  -DarchetypeGroupId=software.amazon.awssdk \  
  -DarchetypeArtifactId=archetype-lambda -Dservice=s3 -Dregion=US_WEST_2 \  
  -DgroupId=com.example.myapp \  
  -DpackageName=com.example.myapp
```

```
-DartifactId=myapp
```

Di PowerShell, jalankan perintah ini:

```
mvn -B archetype:generate `
  "-DarchetypeGroupId=software.amazon.awssdk" `
  "-DarchetypeArtifactId=archetype-lambda" "-Dservice=s3" "-Dregion=US_WEST_2"
  `
  "-DgroupId=com.example.myapp" `
  "-DartifactId=myapp"
```

Pola dasar Maven untuk Lambda telah dikonfigurasi sebelumnya untuk dikompilasi dengan Java SE 8 dan menyertakan ketergantungan pada file. AWS SDK for Java [Jika Anda membuat proyek Anda dengan pola dasar yang berbeda atau dengan menggunakan metode lain, Anda harus mengkonfigurasi compiler Java untuk Maven dan mendeklarasikan sebagai dependensi. SDK](#)

2. Buka `myapp/src/main/java/com/example/myapp` direktori, dan temukan `App.java` filenya. Ini adalah kode untuk fungsi Lambda. Anda dapat menggunakan kode sampel yang disediakan untuk pengujian, atau menggantinya dengan kode Anda sendiri.
3. Arahkan kembali ke direktori root proyek, lalu buat Dockerfile baru dengan konfigurasi berikut:
 - Atur FROM properti ke [URL gambar dasar](#).
 - Atur CMD argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada `USER` instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/java:21

# Copy function code and runtime dependencies from Maven layout
COPY target/classes ${LAMBDA_TASK_ROOT}
COPY target/dependency/* ${LAMBDA_TASK_ROOT}/lib/
```

```
# Set the CMD to your handler (could also be done as a parameter override
  outside of the Dockerfile)
CMD [ "com.example.myapp.App::handleRequest" ]
```

4. Kompilasi proyek dan kumpulkan dependensi runtime.

```
mvn compile dependency:copy-dependencies -DincludeScope=runtime
```

5. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar `docker-image` dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

Gradle

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir example
cd example
```

2. Jalankan perintah berikut agar Gradle membuat proyek aplikasi Java baru di direktori `example` di lingkungan Anda. Untuk Pilih skrip build DSL, pilih 2: Groovy.

```
gradle init --type java-application
```

3. Buka `/example/app/src/main/java/example` direktori, dan temukan `App.java` filenya. Ini adalah kode untuk fungsi Lambda. Anda dapat menggunakan kode contoh berikut untuk pengujian, atau menggantinya dengan kode Anda sendiri.

Example App.java

```
package com.example;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
public class App implements RequestHandler<Object, String> {
    public String handleRequest(Object input, Context context) {
        return "Hello world!";
    }
}
```

4. Buka file `build.gradle`. Jika Anda menggunakan kode fungsi sampel dari langkah sebelumnya, ganti isinya `build.gradle` dengan yang berikut ini. Jika Anda menggunakan kode fungsi Anda sendiri, ubah `build.gradle` file Anda sesuai kebutuhan.

Example build.gradle (Groovy) DSL

```
plugins {
    id 'java'
}
group 'com.example'
version '1.0-SNAPSHOT'
sourceCompatibility = 1.8
repositories {
    mavenCentral()
}
dependencies {
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.1'
}
jar {
    manifest {
        attributes 'Main-Class': 'com.example.App'
    }
}
```

5. `gradle init` Perintah dari langkah 2 juga menghasilkan kasus uji dummy di `app/test` direktori. Untuk keperluan tutorial ini, lewati tes yang sedang berjalan dengan menghapus `/test` direktori.
6. Bangun proyek.

```
gradle build
```

7. Di direktori root proyek (`/example`), buat Dockerfile dengan konfigurasi berikut:
 - Atur FROM properti ke [URIfgambar dasar](#).
 - Gunakan COPY perintah untuk menyalin kode fungsi dan dependensi runtime ke `{LAMBDA_TASK_ROOT}`, variabel lingkungan yang ditentukan [Lambda](#).
 - Atur CMD argumen ke penanganan fungsi Lambda.

Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/lambda/java:21

# Copy function code and runtime dependencies from Gradle layout
COPY app/build/classes/java/main ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override
# outside of the Dockerfile)
CMD [ "com.example.App::handleRequest" ]
```

8. Buat image Docker dengan perintah [docker](#) build. Contoh berikut menamai gambar `docker-image` dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda

menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

1. Mulai gambar Docker dengan perintah `docker run`. Dalam contoh ini, `docker-image` adalah nama gambar dan test tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

2. Dari jendela terminal baru, posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d  
'{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType "application/json"
```

3. Dapatkan ID kontainer.

```
docker ps
```

4. Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.

- Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
- Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECRRepository Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repository Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoriURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhirURI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{
  "ExecutedVersion": "$LATEST",
```

```
"statusCode": 200
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \
  --function-name hello-world \
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --publish
```

Menggunakan gambar dasar alternatif dengan klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda.

Instal klien antarmuka runtime untuk Java di Dockerfile Anda, atau sebagai ketergantungan dalam proyek Anda. Misalnya, untuk menginstal klien antarmuka runtime menggunakan manajer paket Maven, tambahkan yang berikut ini ke file Anda: `pom.xml`

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
  <version>2.3.2</version>
</dependency>
```

Untuk detail paket, lihat [AWS Lambda Java Runtime Interface Client](#) di Maven Central Repository. Anda juga dapat meninjau kode sumber klien antarmuka runtime di repositori [AWS Lambda Java Support Libraries](#) GitHub .

Contoh berikut menunjukkan cara membangun image container untuk Java menggunakan image [Amazon Corretto](#). Amazon Corretto adalah distribusi tanpa biaya, multiplatform, siap produksi dari Open Java Development Kit (Open). JDK Proyek Maven menyertakan klien antarmuka runtime sebagai dependensi.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Java (misalnya, [Amazon Corretto](#))
- [Docker](#)
- [Apache Maven](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Membuat gambar dari gambar dasar alternatif

1. Buat proyek Maven. Parameter-parameter berikut diperlukan:

- `groupId`— Namespace paket lengkap aplikasi Anda.
- `artifactId`— Nama proyek Anda. Ini menjadi nama direktori untuk proyek Anda.

Linux/macOS

```
mvn -B archetype:generate \  
  -DarchetypeArtifactId=maven-archetype-quickstart \  
  -DgroupId=example \  
  -DartifactId=myapp \  
  -DinteractiveMode=false
```

PowerShell

```
mvn -B archetype:generate \  
  -DarchetypeArtifactId=maven-archetype-quickstart \  
  -DgroupId=example \  
  -DartifactId=myapp
```



```
-DinteractiveMode=false
```

2. Buka direktori proyek.

```
cd myapp
```

3. Buka `pom.xml` file dan ganti isinya dengan yang berikut ini. File ini menyertakan [aws-lambda-java-runtime-interface-client](#) sebagai dependensi. Atau, Anda dapat menginstal klien antarmuka runtime di Dockerfile. Namun, pendekatan paling sederhana adalah memasukkan perpustakaan sebagai ketergantungan.

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>example</groupId>
  <artifactId>hello-lambda</artifactId>
  <packaging>jar</packaging>
  <version>1.0-SNAPSHOT</version>
  <name>hello-lambda</name>
  <url>http://maven.apache.org</url>
  <properties>
    <maven.compiler.source>1.8</maven.compiler.source>
    <maven.compiler.target>1.8</maven.compiler.target>
  </properties>
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
      <version>2.3.2</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-dependency-plugin</artifactId>
        <version>3.1.2</version>
        <executions>
          <execution>
            <id>copy-dependencies</id>
            <phase>package</phase>
```

```

        <goals>
          <goal>copy-dependencies</goal>
        </goals>
      </execution>
    </executions>
  </plugin>
</plugins>
</build>
</project>

```

4. Buka `myapp/src/main/java/com/example/myapp` direktori, dan temukan `App.java` filenya. Ini adalah kode untuk fungsi Lambda. Ganti kode dengan yang berikut ini.

Example fungsi handler

```

package example;

public class App {
    public static String sayHello() {
        return "Hello world!";
    }
}

```

5. `mvn -B archetype:generate` perintah dari langkah 1 juga menghasilkan kasus uji dummy di `src/test` direktori. Untuk keperluan tutorial ini, lewati tes yang sedang berjalan dengan menghapus seluruh `/test` direktori yang dihasilkan ini.
6. Arahkan kembali ke direktori root proyek, lalu buat `Dockerfile` baru. Contoh berikut `Dockerfile` menggunakan gambar Amazon [Corretto](#). Amazon Corretto adalah distribusi Open tanpa biaya, multiplatform, dan siap produksi. JDK
 - Atur `FROM` properti ke URI gambar dasar.
 - Atur `ENTRYPOINT` ke modul yang Anda inginkan untuk menjalankan wadah Docker saat dimulai. Dalam hal ini, modul adalah klien antarmuka runtime.
 - Atur `CMD` argumen ke penanganan fungsi Lambda.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada `USER` instruksi yang diberikan.

Example Dockerfile

```
FROM public.ecr.aws/amazoncorretto/amazoncorretto:21 as base

# Configure the build environment
FROM base as build
RUN yum install -y maven
WORKDIR /src

# Cache and copy dependencies
ADD pom.xml .
RUN mvn dependency:go-offline dependency:copy-dependencies

# Compile the function
ADD . .
RUN mvn package

# Copy the function artifact and dependencies onto a clean base
FROM base
WORKDIR /function

COPY --from=build /src/target/dependency/*.jar ./
COPY --from=build /src/target/*.jar ./

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/bin/java", "-cp", ".*",
"com.amazonaws.services.lambda.runtime.api.client.AWSLambda" ]
# Pass the name of the function handler as an argument to the runtime
CMD [ "example.App::sayHello" ]
```

7. Buat image Docker dengan perintah [docker build](#). Contoh berikut menamai gambar docker-image dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan

arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar secara lokal. Anda dapat [membangun emulator ke dalam gambar Anda](#) atau menggunakan prosedur berikut untuk menginstalnya di mesin lokal Anda.

Untuk menginstal dan menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Dari direktori proyek Anda, jalankan perintah berikut untuk mengunduh emulator antarmuka runtime (arsitektur x86-64) dari GitHub dan menginstalnya di mesin lokal Anda.

Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \  
  curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-  
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \  
  chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Untuk menginstal emulator arm64, ganti GitHub repositori URL di perintah sebelumnya dengan yang berikut:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/  
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"  
if (-not (Test-Path $dirPath)) {  
  New-Item -Path $dirPath -ItemType Directory  
}  
  
$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/  
releases/latest/download/aws-lambda-rie"  
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"  
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Untuk menginstal emulator arm64, ganti `$downloadLink` dengan yang berikut ini:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
```

2. Mulai gambar Docker dengan perintah `docker run`. Perhatikan hal berikut:

- `docker-image` adalah nama gambar dan test tag.
- `/usr/bin/java -cp './*' com.amazonaws.services.lambda.runtime.api.client.AWSLambda example.App::sayHello` adalah ENTRYPOINT diikuti oleh CMD dari Dockerfile Anda.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p 9000:8080 \
  --entrypoint /aws-lambda/aws-lambda-rie \
  docker-image:test \
  /usr/bin/java -cp './*' \
  com.amazonaws.services.lambda.runtime.api.client.AWSLambda \
  example.App::sayHello
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
  /usr/bin/java -cp './*' \
  com.amazonaws.services.lambda.runtime.api.client.AWSLambda \
  example.App::sayHello
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

3. Posting acara ke titik akhir lokal.**Linux/macOS**

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload": "hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{"payload": "hello world!"}' -ContentType "application/json"
```

4. Dapatkan ID kontainer.

```
docker ps
```

- Gunakan perintah [docker kill](#) untuk menghentikan wadah. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

- Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

- Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
```

```

    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}

```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositori URI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.


```
aws lambda create-function \  
  --function-name hello-world \  
  --package-type Image \  
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

9. Untuk melihat output fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --publish
```

```
--function-name hello-world \  
--image-uri 11112223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
--publish
```

Bekerja dengan lapisan untuk fungsi Java Lambda

[Lapisan Lambda](#) adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi. Membuat layer melibatkan tiga langkah umum:

1. Package konten layer Anda. Ini berarti membuat arsip file.zip yang berisi dependensi yang ingin Anda gunakan dalam fungsi Anda.
2. Buat layer di Lambda.
3. Tambahkan layer ke fungsi Anda.

Topik ini berisi langkah-langkah dan panduan tentang cara mengemas dan membuat lapisan Java Lambda dengan dependensi pustaka eksternal dengan benar.

Topik

- [Prasyarat](#)
- [Kompatibilitas lapisan Java dengan Amazon Linux](#)
- [Jalur lapisan untuk runtime Java](#)
- [Mengemas konten lapisan](#)
- [Membuat layer](#)
- [Menambahkan layer ke fungsi Anda](#)

Prasyarat

Untuk mengikuti langkah-langkah di bagian ini, Anda harus memiliki yang berikut:

- [Jawa 21](#)
- [Apache Maven 3.8.6 atau yang lebih baru](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Note

Pastikan bahwa versi Java yang dirujuk Maven sama dengan versi Java dari fungsi yang ingin Anda gunakan. Misalnya, untuk fungsi Java 21, `mvn -v` perintah harus mencantumkan Java versi 21 dalam output:

```
Apache Maven 3.8.6
...
Java version: 21.0.2, vendor: Oracle Corporation, runtime: /Library/Java/
JavaVirtualMachines/jdk-21.jdk/Contents/Home
...
```

Sepanjang topik ini, kami mereferensikan [layer-java](#) contoh aplikasi pada repositori [awsdocs](#) GitHub . Aplikasi ini berisi skrip yang mengunduh dependensi dan menghasilkan lapisan. Aplikasi ini juga berisi fungsi yang sesuai yang menggunakan dependensi dari lapisan. Setelah membuat layer, Anda dapat menerapkan dan memanggil fungsi yang sesuai untuk memverifikasi bahwa semuanya berfungsi dengan baik. Karena Anda menggunakan runtime Java 21 untuk fungsi, lapisan juga harus kompatibel dengan Java 21.

Aplikasi `layer-java` sampel berisi satu contoh dalam dua sub-direktori. `layerDirektori` berisi `pom.xml` file yang mendefinisikan dependensi lapisan, serta skrip untuk menghasilkan lapisan. `functionDirektori` berisi fungsi sampel untuk membantu menguji bahwa lapisan berfungsi. Tutorial ini berjalan melalui cara membuat dan mengemas layer ini.

Kompatibilitas lapisan Java dengan Amazon Linux

Langkah pertama untuk membuat layer adalah untuk menggabungkan semua konten layer Anda ke dalam arsip file.zip. Karena fungsi Lambda berjalan di [Amazon Linux](#), konten layer Anda harus dapat dikompilasi dan dibangun di lingkungan Linux.

Kode Java dirancang untuk menjadi platform-independen, sehingga Anda dapat mengemas lapisan Anda pada mesin lokal Anda bahkan jika itu tidak menggunakan lingkungan Linux. Setelah Anda mengunggah lapisan Java ke Lambda, itu akan tetap kompatibel dengan Amazon Linux.

Jalur lapisan untuk runtime Java

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam `/opt` direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, PATH variabel sudah menyertakan jalur folder tertentu dalam direktori `/opt` Untuk memastikan bahwa PATH variabel mengambil konten lapisan Anda, file `layer.zip` Anda harus memiliki dependensi di jalur folder berikut:

- `java/lib`

Misalnya, file layer .zip yang dihasilkan yang Anda buat dalam tutorial ini memiliki struktur direktori berikut:

```
layer_content.zip
# java
  # lib
    # layer-java-layer-1.0-SNAPSHOT.jar
```

layer-java-layer-1.0-SNAPSHOT.jar JARFile (sebuah uber-jar yang berisi semua dependensi yang diperlukan) terletak dengan benar di direktori. java/lib Ini memastikan bahwa Lambda dapat menemukan pustaka selama pemanggilan fungsi.

Mengemas konten lapisan

Dalam contoh ini, Anda mengemas dua pustaka Java berikut ke dalam satu JAR file:

- [aws-lambda-java-core](#)— Satu set minimal definisi antarmuka untuk bekerja dengan Java di AWS Lambda
- [Jackson](#) — Rangkaian alat pengolah data yang populer, terutama untuk bekerja dengan JSON

Selesaikan langkah-langkah berikut untuk menginstal dan mengemas konten lapisan.

Untuk menginstal dan mengemas konten lapisan Anda

1. Kloning [aws-lambda-developer-guide GitHub repo](#), yang berisi kode sampel yang Anda butuhkan di direktori. sample-apps/layer-java

```
git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
```

2. Arahkan ke layer direktori aplikasi layer-java sampel. Direktori ini berisi skrip yang Anda gunakan untuk membuat dan mengemas lapisan dengan benar.

```
cd aws-lambda-developer-guide/sample-apps/layer-java/layer
```

3. Periksa [pom.xml](#) file. Di <dependencies> bagian ini, Anda menentukan dependensi yang ingin Anda sertakan di lapisan, yaitu aws-lambda-java-core dan jackson-databind pustaka. Anda dapat memperbarui file ini untuk menyertakan dependensi apa pun yang ingin Anda sertakan dalam lapisan Anda sendiri.

Example pom.xml

```
<dependencies>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-lambda-java-core</artifactId>
    <version>1.2.3</version>
  </dependency>

  <dependency>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <version>2.17.0</version>
  </dependency>
</dependencies>
```

Note

<build>Bagian dari pom.xml file ini berisi dua plugin. [maven-compiler-plugin](#) Mengkompilasi kode sumber. [maven-shade-plugin](#) Paket artefak Anda ke dalam satu uber-jar.

4. Pastikan Anda memiliki izin untuk menjalankan kedua skrip.

```
chmod 744 1-install.sh && chmod 744 2-package.sh
```

5. Jalankan [1-install.sh](#) skrip menggunakan perintah berikut:

```
./1-install.sh
```

Skrip ini berjalan `mvn clean install` di direktori saat ini. Ini membuat uber-jar dengan semua dependensi yang diperlukan dalam direktori `target/`

Example 1-install.sh

```
mvn clean install
```

6. Jalankan [2-package.sh](#) skrip menggunakan perintah berikut:

```
./2-package.sh
```

Skrip ini menciptakan struktur `java/lib` direktori yang Anda butuhkan untuk mengemas konten lapisan Anda dengan benar. Kemudian menyalin `uber-jar` dari `/target` direktori ke direktori yang baru dibuat `java/lib`. Akhirnya, skrip zip isi `java` direktori ke dalam file bernama `layer_content.zip`. Ini adalah file.zip untuk layer Anda. Anda dapat membuka zip file dan memverifikasi bahwa itu berisi struktur file yang benar, seperti yang ditunjukkan pada [the section called “Jalur lapisan untuk runtime Java”](#) bagian.

Example 2-package.sh

```
mkdir java
mkdir java/lib
cp -r target/layer-java-layer-1.0-SNAPSHOT.jar java/lib/
zip -r layer_content.zip java
```

Membuat layer

Di bagian ini, Anda mengambil `layer_content.zip` file yang Anda buat di bagian sebelumnya dan mengunggahnya sebagai lapisan Lambda. Anda dapat mengunggah layer menggunakan AWS Management Console atau Lambda API melalui AWS Command Line Interface (AWS CLI). Saat Anda mengunggah file layer .zip Anda, dalam [PublishLayerVersion](#) AWS CLI perintah berikut, tentukan `java21` sebagai runtime yang kompatibel dan `arm64` sebagai arsitektur yang kompatibel.

```
aws lambda publish-layer-version --layer-name java-jackson-layer \
  --zip-file fileb://layer_content.zip \
  --compatible-runtimes java21 \
  --compatible-architectures "arm64"
```

Dari tanggapan, perhatikan `LayerVersionArn`, yang terlihat seperti `arn:aws:lambda:us-east-1:123456789012:layer:java-jackson-layer:1`. Anda akan memerlukan Amazon Resource Name (ARN) ini di langkah berikutnya dari tutorial ini, ketika Anda menambahkan layer ke fungsi Anda.

Menambahkan layer ke fungsi Anda

Di bagian ini, Anda menyebarkan contoh fungsi Lambda yang menggunakan pustaka Jackson dalam kode fungsinya, lalu Anda melampirkan layer. Untuk menyebarkan fungsi, Anda memerlukan file. [the section called “Peran eksekusi \(izin untuk fungsi untuk mengakses sumber daya lain\)”](#) Jika Anda tidak memiliki peran eksekusi yang ada, ikuti langkah-langkah di bagian yang dapat dilipat.

(Opsional) Buat peran eksekusi

Untuk membuat peran eksekusi

1. Buka [halaman peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.
 - Entitas tepercaya – Lambda.
 - Izin — AWSLambdaBasicExecutionRole.
 - Nama peran – **lambda-role**.

AWSLambdaBasicExecutionRoleKebijakan ini memiliki izin yang diperlukan fungsi untuk menulis log ke CloudWatch Log.

[Kode fungsi Lambda mengambil input Map<String, String> as, dan menggunakan Jackson untuk menulis input sebagai JSON String sebelum mengubahnya menjadi objek Java F1Car yang telah ditentukan sebelumnya.](#) Akhirnya, fungsi menggunakan bidang dari objek F1Car untuk membangun String yang fungsi kembali.

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.fasterxml.jackson.databind.ObjectMapper;

import java.io.IOException;
import java.util.Map;

public class Handler {

    public String handleRequest(Map<String, String> input, Context context) throws
        IOException {
```



```
// Parse the input JSON
ObjectMapper objectMapper = new ObjectMapper();
F1Car f1Car = objectMapper.readValue(objectMapper.writeValueAsString(input),
F1Car.class);

StringBuilder finalString = new StringBuilder();
finalString.append(f1Car.getDriver());
finalString.append(" is a driver for team ");
finalString.append(f1Car.getTeam());
return finalString.toString();
}
}
```

Untuk menyebarkan fungsi Lambda

1. Buka direktori `function/` tersebut. Jika saat ini Anda berada di `layer/` direktori, maka jalankan perintah berikut:

```
cd ../function
```

2. Bangun proyek menggunakan perintah Maven berikut:

```
mvn package
```

Perintah ini menghasilkan JAR file dalam `target/` direktori bernama `layer-java-function-1.0-SNAPSHOT.jar`.

3. Menyebarkan fungsi. Dalam AWS CLI perintah berikut, ganti `--role` parameter dengan peran eksekusi AndaARN:

```
aws lambda create-function --function-name java_function_with_layer \  
  --runtime java21 \  
  --architectures "arm64" \  
  --handler example.Handler::handleRequest \  
  --timeout 30 \  
  --role arn:aws:iam::123456789012:role/lambda-role \  
  --zip-file fileb://target/layer-java-function-1.0-SNAPSHOT.jar
```

4. Selanjutnya, pasang layer ke fungsi Anda. Dalam AWS CLI perintah berikut, ganti `--layers` parameter dengan versi layer ARN yang Anda catat sebelumnya:

```
aws lambda update-function-configuration --function-name java_function_with_layer \  
  --layers
```

```
--cli-binary-format raw-in-base64-out \  
--layers "arn:aws:lambda:us-east-1:123456789012:layer:java-jackson-layer:1"
```

5. Terakhir, coba panggil fungsi Anda menggunakan AWS CLI perintah berikut:

```
aws lambda invoke --function-name java_function_with_layer \  
--cli-binary-format raw-in-base64-out \  
--payload '{ "driver": "Max Verstappen", "team": "Red Bull" }' response.json
```

Anda akan melihat output seperti ini:

```
{  
  "StatusCode": 200,  
  "ExecutedVersion": "$LATEST"  
}
```

Ini menunjukkan bahwa fungsi tersebut dapat menggunakan ketergantungan Jackson untuk menjalankan fungsi dengan benar. Anda dapat memeriksa apakah `response.json` file output berisi String yang dikembalikan dengan benar:

```
"Max Verstappen is a driver for team Red Bull"
```

(Opsional) Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus layer Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih layer yang Anda buat.
3. Pilih Hapus, lalu pilih Hapus lagi.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.

3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Meningkatkan kinerja startup dengan Lambda SnapStart

Lambda SnapStart untuk Java dapat meningkatkan kinerja startup untuk aplikasi yang sensitif terhadap latensi hingga 10x tanpa biaya tambahan, biasanya tanpa perubahan pada kode fungsi Anda. Kontributor terbesar untuk latensi startup (sering disebut sebagai cold start time) adalah waktu yang dihabiskan Lambda untuk menginisialisasi fungsi, yang mencakup memuat kode fungsi, memulai runtime, dan menginisialisasi kode fungsi.

Dengan SnapStart, Lambda menginisialisasi fungsi Anda saat Anda mempublikasikan versi fungsi. Lambda mengambil snapshot [MicroVM Firecracker](#) dari memori dan status disk dari [lingkungan eksekusi](#) yang diinisialisasi, mengenkripsi snapshot, dan menyimpannya dalam cache untuk akses latensi rendah. Saat Anda memanggil versi fungsi untuk pertama kalinya, dan saat pemanggilan meningkat, Lambda melanjutkan lingkungan eksekusi baru dari snapshot yang di-cache alih-alih menginisiasinya dari awal, meningkatkan latensi startup.

Important

Jika aplikasi Anda bergantung pada keunikan status, Anda harus mengevaluasi kode fungsi Anda dan memverifikasi bahwa itu tahan terhadap operasi snapshot. Untuk informasi selengkapnya, lihat [Menangani keunikan dengan Lambda SnapStart](#).

Topik

- [Fitur yang didukung dan batasan](#)
- [Wilayah yang Didukung](#)
- [Pertimbangan kompatibilitas](#)
- [SnapStart harga](#)
- [Membandingkan Lambda SnapStart dan konkurensi yang disediakan](#)
- [Sumber daya tambahan](#)
- [Mengaktifkan dan mengelola Lambda SnapStart](#)
- [Menangani keunikan dengan Lambda SnapStart](#)
- [Menerapkan kode sebelum atau sesudah snapshot fungsi Lambda](#)
- [Pemantauan untuk Lambda SnapStart](#)
- [Model keamanan untuk Lambda SnapStart](#)

- [Maksimalkan kinerja Lambda SnapStart](#)

Fitur yang didukung dan batasan

SnapStart mendukung [runtime terkelola Java 11 dan Java](#) yang lebih baru. Runtime terkelola lainnya (seperti `nodejs20.x` dan `python3.12`), [Runtime khusus OS](#), dan [gambar kontainer](#) tidak didukung.

SnapStart tidak mendukung [konkurensi yang disediakan](#), [Amazon Elastic File System \(AmazonEFS\)](#), atau penyimpanan sementara yang lebih besar dari 512 MB.

Untuk bekerja dengan SnapStart, Anda dapat menggunakan konsol Lambda, AWS Command Line Interface (AWS CLI), Lambda API, AWS Serverless Application Model (AWS SAM) AWS SDK for Java AWS CloudFormation, dan AWS Cloud Development Kit (AWS CDK) Untuk informasi selengkapnya, lihat [Mengaktifkan dan mengelola Lambda SnapStart](#).

Note

Anda SnapStart hanya dapat menggunakan pada [versi fungsi yang diterbitkan](#) dan [alias](#) yang mengarah ke versi. Anda tidak dapat menggunakan SnapStart pada versi fungsi yang tidak dipublikasikan (\$LATEST).

Wilayah yang Didukung

SnapStart tersedia dalam hal berikut Wilayah AWS:

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Tokyo)

- Asia Pasifik (Seoul)
- Asia Pasifik (Osaka)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Kanada (Pusat)
- Eropa (Stockholm)
- Eropa (Frankfurt)
- Eropa (Zürich)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Paris)
- Eropa (Milan)
- Eropa (Spanyol)
- Timur Tengah (UAE)
- Timur Tengah (Bahrain)
- Amerika Selatan (Sao Paulo)

Pertimbangan kompatibilitas

Dengan SnapStart, Lambda menggunakan satu snapshot sebagai status awal untuk beberapa lingkungan eksekusi. Jika fungsi Anda menggunakan salah satu dari berikut ini selama [fase inisialisasi](#), maka Anda mungkin perlu membuat beberapa perubahan sebelum menggunakan SnapStart:

Keunikan

Jika kode inisialisasi Anda menghasilkan konten unik yang disertakan dalam snapshot, maka konten tersebut mungkin tidak unik saat digunakan kembali di seluruh lingkungan eksekusi. Untuk mempertahankan keunikan saat menggunakan SnapStart, Anda harus menghasilkan konten unik setelah inisialisasi. Ini termasuk rahasia unikIDs, unik, dan entropi yang digunakan untuk

menghasilkan pseudorandomness. Untuk mempelajari cara mengembalikan keunikan, lihat.

[Menangani keunikan dengan Lambda SnapStart](#)

Koneksi jaringan

Status koneksi yang ditetapkan fungsi Anda selama fase inisialisasi tidak dijamin saat Lambda melanjutkan fungsi Anda dari snapshot. Validasi status koneksi jaringan Anda dan buat kembali seperlunya. Dalam kebanyakan kasus, koneksi jaringan yang AWS SDK dibuat secara otomatis dilanjutkan. Untuk koneksi lain, tinjau [praktik terbaik](#).

Data sementara

Beberapa fungsi mengunduh atau menginisialisasi data sementara, seperti kredensial sementara atau stempel waktu yang di-cache, selama fase inisialisasi. Segarkan data singkat di penanganan fungsi sebelum menggunakannya, bahkan saat tidak menggunakan. SnapStart

SnapStart harga

Tidak ada biaya tambahan untuk SnapStart. Anda dikenakan biaya berdasarkan jumlah permintaan untuk fungsi Anda, waktu yang dibutuhkan kode Anda untuk menjalankan, dan memori yang dikonfigurasi untuk fungsi Anda. Durasi dihitung dari waktu kode Anda mulai berjalan hingga kembali atau berakhir, dibulatkan ke 1 ms terdekat.


[Biaya durasi berlaku untuk kode yang berjalan di penanganan fungsi, kode inisialisasi yang dideklarasikan di luar handler, waktu yang dibutuhkan untuk memuat runtime \(JVM\), dan kode apa pun yang berjalan di hook runtime.](#) Untuk informasi selengkapnya tentang cara Lambda menghitung durasi, lihat. [Pemantauan untuk Lambda SnapStart](#)

Untuk fungsi yang dikonfigurasi SnapStart, Lambda mendaur ulang lingkungan eksekusi secara berkala dan menjalankan kembali kode inisialisasi Anda. Untuk ketahanan, Lambda membuat snapshot di beberapa Wilayah. Biaya berlaku setiap kali Lambda menjalankan kembali kode inisialisasi Anda di Wilayah lain. [Untuk informasi selengkapnya tentang cara Lambda menghitung biaya, lihat Harga.AWS Lambda](#)

Membandingkan Lambda SnapStart dan konkurensi yang disediakan

Baik Lambda SnapStart dan [konkurensi yang disediakan dapat mengurangi start dingin dan latensi outlier](#) saat suatu fungsi meningkat. SnapStart membantu Anda meningkatkan kinerja startup hingga 10x tanpa biaya tambahan. Konkurensi yang disediakan membuat fungsi diinisialisasi dan siap merespons dalam milidetik dua digit. Mengkonfigurasi konkurensi yang disediakan menimbulkan

biaya ke Anda. Akun AWS Gunakan konkurensi yang disediakan jika aplikasi Anda memiliki persyaratan latensi start dingin yang ketat. Anda tidak dapat menggunakan keduanya SnapStart dan konkurensi yang disediakan pada versi fungsi yang sama.

 Note

SnapStart bekerja paling baik saat digunakan dengan pemanggilan fungsi dalam skala besar. Fungsi yang jarang dipanggil mungkin tidak mengalami peningkatan kinerja yang sama.

Sumber daya tambahan

Selain membaca topik lain di bagian ini, kami juga menyarankan Anda mencoba [Memulai lebih cepat dengan AWS Lambda SnapStart](#) lokakarya dan menonton [Fast cold start untuk sesi fungsi Java Anda](#) dari AWS re:invent 2022.

Mengaktifkan dan mengelola Lambda SnapStart

Untuk menggunakan SnapStart, aktifkan SnapStart pada fungsi Lambda baru atau yang sudah ada. Kemudian, publikasikan dan panggil versi fungsi.

Topik

- [Mengaktifkan SnapStart \(konsol\)](#)
- [Mengaktifkan SnapStart \(\)AWS CLI](#)
- [Mengaktifkan SnapStart \(\) API](#)
- [Lambda SnapStart dan status fungsi](#)
- [Memperbarui snapshot](#)
- [Menggunakan SnapStart dengan AWS SDK for Java](#)
- [Menggunakan SnapStart dengan AWS CloudFormation, AWS SAM, dan AWS CDK](#)
- [Menghapus snapshot](#)

Mengaktifkan SnapStart (konsol)

SnapStart Untuk mengaktifkan suatu fungsi

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih Konfigurasi, lalu pilih Konfigurasi umum.
4. Pada panel konfigurasi Umum, pilih Edit.
5. Pada halaman Edit pengaturan dasar, untuk SnapStart, pilih Versi yang diterbitkan.
6. Pilih Simpan.
7. [Publikasikan versi fungsi](#). Lambda menginisialisasi kode Anda, membuat snapshot dari lingkungan eksekusi yang diinisialisasi, dan kemudian menyimpan snapshot untuk akses latensi rendah.
8. [Memanggil versi fungsi](#).

Mengaktifkan SnapStart ()AWS CLI

SnapStart Untuk mengaktifkan fungsi yang ada

1. Perbarui konfigurasi fungsi dengan menjalankan [update-function-configuration](#) perintah dengan --snap-start opsi.

```
aws lambda update-function-configuration \  
  --function-name my-function \  
  --snap-start ApplyOn=PublishedVersions
```

2. Publikasikan versi fungsi dengan perintah [publish-version](#).

```
aws lambda publish-version \  
  --function-name my-function
```

3. Konfirmasikan yang SnapStart diaktifkan untuk versi fungsi dengan menjalankan [get-function-configuration](#) perintah dan menentukan nomor versi. Contoh berikut menentukan versi 1.

```
aws lambda get-function-configuration \  
  --function-name my-function:1
```

Jika respons menunjukkan bahwa [OptimizationStatus](#) adalah On dan [State](#) isActive, maka SnapStart diaktifkan dan snapshot tersedia untuk versi fungsi yang ditentukan.

```
"SnapStart": {  
  "ApplyOn": "PublishedVersions",  
  "OptimizationStatus": "On"  
},  
"State": "Active",
```

4. Panggil versi fungsi dengan menjalankan perintah [pemanggilan](#) dan menentukan versinya. Contoh berikut memanggil versi 1.

```
aws lambda invoke \  
  --cli-binary-format raw-in-base64-out \  
  --function-name my-function:1 \  
  --payload '{ "name": "Bob" }' \  
  response.json
```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Untuk mengaktifkan SnapStart saat Anda membuat fungsi baru

1. Buat fungsi dengan menjalankan perintah [create-function](#) dengan opsi `--snap-start`. Untuk `--role`, tentukan Nama Sumber Daya Amazon (ARN) [peran eksekusi](#) Anda.

```
aws lambda create-function \  
  --function-name my-function \  
  --runtime "java21" \  
  --zip-file fileb://my-function.zip \  
  --handler my-function.handler \  
  --role arn:aws:iam::111122223333:role/lambda-ex \  
  --snap-start ApplyOn=PublishedVersions
```

2. Buat versi dengan perintah [publish-version](#).

```
aws lambda publish-version \  
  --function-name my-function
```

3. Konfirmasikan yang SnapStart diaktifkan untuk versi fungsi dengan menjalankan [get-function-configuration](#) perintah dan menentukan nomor versi. Contoh berikut menentukan versi 1.

```
aws lambda get-function-configuration \  
  --function-name my-function:1
```

Jika respons menunjukkan bahwa [OptimizationStatus](#) adalah `On` dan [State](#) `isActive`, maka SnapStart diaktifkan dan snapshot tersedia untuk versi fungsi yang ditentukan.

```
"SnapStart": {  
  "ApplyOn": "PublishedVersions",  
  "OptimizationStatus": "On"  
},  
"State": "Active",
```

4. Panggil versi fungsi dengan menjalankan perintah [pemanggilan](#) dan menentukan versinya. Contoh berikut memanggil versi 1.

```
aws lambda invoke \  
  --cli-binary-format raw-in-base64-out \  
  --function-name my-function:1 \  
  --payload '{ "name": "Bob" }' \  
  response.json
```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Mengaktifkan SnapStart () API

Untuk mengaktifkan SnapStart

1. Lakukan salah satu hal berikut ini:
 - Buat fungsi baru dengan SnapStart diaktifkan dengan menggunakan [CreateFunction](#) API tindakan dengan [SnapStart](#) parameter.
 - Aktifkan SnapStart untuk fungsi yang ada dengan menggunakan [UpdateFunctionConfiguration](#) tindakan dengan [SnapStart](#) parameter.
2. Publikasikan versi fungsi dengan [PublishVersion](#) tindakan. Lambda menginisialisasi kode Anda, membuat snapshot dari lingkungan eksekusi yang diinisialisasi, dan kemudian menyimpan snapshot untuk akses latensi rendah.
3. Konfirmasikan bahwa SnapStart diaktifkan untuk versi fungsi dengan menggunakan [GetFunctionConfiguration](#) tindakan. Tentukan nomor versi untuk mengonfirmasi bahwa SnapStart diaktifkan untuk versi tersebut. Jika respons menunjukkan bahwa [OptimizationStatus](#) adalah `On` dan [State](#) `isActive`, maka SnapStart diaktifkan dan snapshot tersedia untuk versi fungsi yang ditentukan.

```
"SnapStart": {  
  "ApplyOn": "PublishedVersions",  
  "OptimizationStatus": "On"  
},  
"State": "Active",
```

4. Panggil versi fungsi dengan tindakan [Invoke](#).

Lambda SnapStart dan status fungsi

Status fungsi berikut dapat terjadi saat Anda menggunakan SnapStart. Mereka juga dapat terjadi ketika Lambda secara berkala mendaur ulang lingkungan eksekusi dan menjalankan kembali kode inisialisasi untuk fungsi yang dikonfigurasi. SnapStart

- **Pending**— Lambda menginisialisasi kode Anda dan mengambil snapshot dari lingkungan eksekusi yang diinisialisasi. Setiap pemanggilan atau API tindakan lain yang beroperasi pada versi fungsi akan gagal.
- **Active**— Pembuatan snapshot selesai dan Anda dapat menjalankan fungsinya. Untuk menggunakannya SnapStart, Anda harus memanggil versi fungsi yang diterbitkan, bukan versi yang tidak diterbitkan (\$LATEST).
- **Inactive**— Versi fungsi belum dipanggil selama 14 hari. Ketika versi fungsi menjadi **Inactive**, Lambda menghapus snapshot. Jika Anda memanggil versi fungsi setelah 14 hari, Lambda mengembalikan `SnapStartNotReadyException` respons dan mulai menginisialisasi snapshot baru. Tunggu hingga versi fungsi mencapai **Active** status, lalu panggil lagi. **InactiveStatus** juga dapat terjadi karena Lambda menjalankan daur ulang berkala dari lingkungan eksekusi. Dalam hal ini, jika fungsi Anda gagal untuk menginisialisasi, fungsi dapat memasukkan **Inactive** status.
- **Failed**— Lambda mengalami kesalahan saat menjalankan kode inisialisasi atau membuat snapshot.

Memperbarui snapshot

Lambda membuat snapshot untuk setiap versi fungsi yang diterbitkan. Untuk memperbarui snapshot, publikasikan versi fungsi baru. Lambda secara otomatis memperbarui snapshot Anda dengan runtime terbaru dan patch keamanan.

Menggunakan SnapStart dengan AWS SDK for Java

Untuk melakukan AWS SDK panggilan dari fungsi Anda, Lambda menghasilkan seperangkat kredensial singkat dengan mengasumsikan peran eksekusi fungsi Anda. Kredensial ini tersedia sebagai variabel lingkungan selama pemanggilan fungsi Anda. Anda tidak perlu memberikan kredensi untuk kode SDK langsung di. Secara default, rantai penyedia kredensi secara berurutan memeriksa setiap tempat di mana Anda dapat menyetel kredensialnya dan memilih yang pertama

tersedia—biasanya variabel lingkungan (`., dan`). `AWS_ACCESS_KEY_ID` `AWS_SECRET_ACCESS_KEY`
`AWS_SESSION_TOKEN`

Note

Ketika SnapStart diaktifkan, runtime Java secara otomatis menggunakan kredensial kontainer (`AWS_CONTAINER_CREDENTIALS_FULL_URI` dan `AWS_CONTAINER_AUTHORIZATION_TOKEN`) alih-alih variabel lingkungan kunci akses. Ini mencegah kredensi kedaluwarsa sebelum fungsi dipulihkan.

Menggunakan SnapStart dengan AWS CloudFormation, AWS SAM, dan AWS CDK

- AWS CloudFormation: Deklarasikan [SnapStart](#) entitas dalam template Anda.
- AWS Serverless Application Model (AWS SAM): Deklarasikan [SnapStart](#) properti di template Anda.
- AWS Cloud Development Kit (AWS CDK): Gunakan [SnapStartProperty](#) tipenya.

Menghapus snapshot

Lambda menghapus snapshot saat:

- Anda menghapus fungsi atau versi fungsi.
- Anda tidak memanggil versi fungsi selama 14 hari. [Setelah 14 hari tanpa pemanggilan, versi fungsi bertransisi ke status Tidak Aktif](#). Jika Anda memanggil versi fungsi setelah 14 hari, Lambda mengembalikan `SnapStartNotReadyException` respons dan mulai menginisialisasi snapshot baru. Tunggu hingga versi fungsi mencapai status [Aktif](#), lalu panggil lagi.

Lambda menghapus semua sumber daya yang terkait dengan snapshot yang dihapus sesuai dengan Peraturan Perlindungan Data Umum (). GDPR

Menangani keunikan dengan Lambda SnapStart

Saat pemanggilan ditingkatkan pada suatu SnapStart fungsi, Lambda menggunakan satu snapshot yang diinisialisasi untuk melanjutkan beberapa lingkungan eksekusi. Jika kode inisialisasi Anda menghasilkan konten unik yang disertakan dalam snapshot, maka konten tersebut mungkin tidak unik saat digunakan kembali di seluruh lingkungan eksekusi. Untuk mempertahankan keunikan saat menggunakan SnapStart, Anda harus menghasilkan konten unik setelah inisialisasi. Ini termasuk rahasia unikIDs, unik, dan entropi yang digunakan untuk menghasilkan pseudorandomness.

Kami merekomendasikan praktik terbaik berikut untuk membantu Anda mempertahankan keunikan dalam kode Anda. Lambda juga menyediakan [alat SnapStart pemindaian](#) sumber terbuka untuk membantu memeriksa kode yang mengasumsikan keunikan. Jika Anda menghasilkan data unik selama fase inisialisasi, maka Anda dapat menggunakan [kait runtime](#) untuk mengembalikan keunikan. Dengan runtime hooks, Anda dapat menjalankan kode tertentu segera sebelum Lambda mengambil snapshot atau segera setelah Lambda melanjutkan fungsi dari snapshot.

Hindari menyimpan status yang bergantung pada keunikan selama inisialisasi

Selama [fase inisialisasi](#) fungsi Anda, hindari caching data yang dimaksudkan untuk menjadi unik, seperti membuat ID unik untuk logging. Sebagai gantinya, kami menyarankan Anda menghasilkan data unik di dalam penanganan fungsi Anda atau menggunakan kait [runtime](#).

Example — Menghasilkan ID unik di function handler

Contoh berikut menunjukkan bagaimana untuk menghasilkan UUID dalam fungsi handler.

```
import java.util.UUID;
public class Handler implements RequestHandler<String, String> {
    private static UUID uniqueSandboxId = null;
    @Override
    public String handleRequest(String event, Context context) {
        if (uniqueSandboxId == null)
            uniqueSandboxId = UUID.randomUUID();
        System.out.println("Unique Sandbox Id: " + uniqueSandboxId);
        return "Hello, World!";
    }
}
```

Gunakan generator nomor pseudorandom yang aman secara kriptografis () CSPRNGs

Jika aplikasi Anda bergantung pada keacakan, kami sarankan Anda menggunakan generator nomor acak yang aman secara kriptografis (). CSPRNGs Runtime terkelola Lambda untuk Java mencakup dua built-in CSPRNGs (Open SSL 1.0.2 dan `java.security.SecureRandom`) yang secara otomatis mempertahankan keacakan dengan SnapStart Perangkat lunak yang selalu mendapatkan angka acak dari `/dev/random` atau `/dev/urandom` juga mempertahankan keacakan dengan SnapStart.

AWS pustaka kriptografi secara otomatis mempertahankan keacakan dengan SnapStart memulai dengan versi minimum yang ditentukan dalam tabel berikut. Jika Anda menggunakan pustaka ini dengan fungsi Lambda, pastikan Anda menggunakan versi minimum berikut atau versi yang lebih baru:

| Perpustakaan | Versi minimum yang didukung (x86) | Versi minimum yang didukung (ARM) |
|------------------------|-----------------------------------|-----------------------------------|
| AWS libcrypto (AWS-LC) | 1.16.0 | 1.30.0 |
| AWS libcrypto FIPS | 2.0.13 | 2.0.13 |

Jika Anda mengemas pustaka kriptografi sebelumnya dengan fungsi Lambda Anda sebagai dependensi transitif melalui pustaka berikut, pastikan Anda menggunakan versi minimum berikut atau versi yang lebih baru:

| Perpustakaan | Versi minimum yang didukung (x86) | Versi minimum yang didukung (ARM) |
|--------------------------------------|-----------------------------------|-----------------------------------|
| AWS SDK for Java 2.x | 2.23.20 | 2.26.12 |
| AWS Runtime Umum untuk Java | 0.29.8 | 0.29.25 |
| Penyedia Crypto Amazon Corretto | 2.4.1 | 2.4.1 |
| Penyedia Crypto Amazon Corretto FIPS | 2.4.1 | 2.4.1 |

Example — java.security. SecureRandom

Contoh berikut menggunakan `java.security.SecureRandom`, yang menghasilkan urutan nomor unik bahkan ketika fungsi dipulihkan dari snapshot.

```
import java.security.SecureRandom;
public class Handler implements RequestHandler<String, String> {
    private static SecureRandom rng = new SecureRandom();
    @Override
    public String handleRequest(String event, Context context) {
        for (int i = 0; i < 10; i++) {
            System.out.println(rng.next());
        }
        return "Hello, World!";
    }
}
```

SnapStart alat pemindaian

Lambda menyediakan alat pemindaian untuk membantu Anda memeriksa kode yang mengasumsikan keunikan. Alat SnapStart pemindaian adalah [SpotBugs](#) plugin sumber terbuka yang menjalankan analisis statis terhadap seperangkat aturan. Alat pemindaian membantu mengidentifikasi implementasi kode potensial yang mungkin mematahkan asumsi mengenai keunikan. Untuk petunjuk penginstalan dan daftar pemeriksaan yang dilakukan alat pemindaian, lihat repositori [aws-lambda-snapstart-java-rules](#) aktif. GitHub

Untuk mempelajari lebih lanjut tentang menangani keunikan dengan SnapStart, lihat [Memulai lebih cepat dengan AWS Lambda SnapStart](#) di AWS Compute Blog.

Menerapkan kode sebelum atau sesudah snapshot fungsi Lambda

Anda dapat menggunakan kait runtime untuk mengimplementasikan kode sebelum Lambda membuat snapshot atau setelah Lambda melanjutkan fungsi dari snapshot. Runtime hook tersedia sebagai bagian dari proyek Coordinated Restore at Checkpoint (cRAC) open-source. CRAC sedang dalam pengembangan untuk [Open Java Development Kit \(OpenJDK\)](#). Untuk contoh cara menggunakan cRAC dengan aplikasi referensi, lihat repositori [cRAC aktif](#). GitHub CraC menggunakan tiga elemen utama:

- `ResourceAntarmuka` dengan dua metode, `beforeCheckpoint()` dan `afterRestore()`. Gunakan metode ini untuk mengimplementasikan kode yang ingin Anda jalankan sebelum snapshot dan setelah pemulihan.
- `Context <R extends Resource>`— Untuk menerima pemberitahuan untuk pos pemeriksaan dan pemulihan, `a Resource` harus terdaftar dengan `a Context`
- `Core`— Layanan koordinasi, yang menyediakan global default `Context` melalui metode `statisCore.getGlobalContext()`.

Untuk informasi selengkapnya tentang `Context` dan `Resource`, lihat [Package org.crac](#) di dokumentasi cRAC.

Gunakan langkah-langkah berikut untuk mengimplementasikan kait runtime dengan paket [org.crac](#). Runtime Lambda berisi implementasi konteks cRAC khusus yang memanggil kait runtime Anda sebelum checkpointing dan setelah memulihkan.

Langkah 1: Perbarui konfigurasi build

Tambahkan `org.crac` dependensi ke konfigurasi build. Contoh berikut menggunakan Gradle. Untuk contoh untuk sistem build lainnya, lihat dokumentasi [Apache Maven](#).

```
dependencies {
    compile group: 'com.amazonaws', name: 'aws-lambda-java-core', version: '1.2.1'
    # All other project dependencies go here:
    # ...
    # Then, add the org.crac dependency:
    implementation group: 'org.crac', name: 'crac', version: '1.4.0'
}
```

Langkah 2: Perbarui penanganan Lambda

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Untuk informasi selengkapnya, lihat [Tentukan penanganan fungsi Lambda di Java](#).

Contoh handler berikut menunjukkan cara menjalankan kode sebelum checkpointing (`beforeCheckpoint()`) dan setelah restoring (`afterRestore()`). Handler ini juga mendaftarkan `Resource` ke global yang dikelola runtime. `Context`

Note

Saat Lambda membuat snapshot, kode inialisasi Anda dapat berjalan hingga 15 menit. Batas waktu adalah 130 detik atau batas [waktu fungsi yang dikonfigurasi](#) (maksimum 900 detik), mana yang lebih tinggi. Kait `beforeCheckpoint()` runtime Anda dihitung terhadap batas waktu kode inialisasi. Saat Lambda mengembalikan snapshot, runtime (JVM) harus dimuat dan kait `afterRestore()` runtime harus selesai dalam batas waktu tunggu (10 detik). Jika tidak, Anda akan mendapatkan `SnapStartTimeoutException`.

```
...
import org.crac.Resource;
import org.crac.Core;
...
public class CRaCDemo implements RequestStreamHandler, Resource {
    public CRaCDemo() {
        Core.getGlobalContext().register(this);
    }
    public String handleRequest(String name, Context context) throws IOException {
        System.out.println("Handler execution");
        return "Hello " + name;
    }
    @Override
    public void beforeCheckpoint(org.crac.Context<? extends Resource> context)
        throws Exception {
        System.out.println("Before checkpoint");
    }
    @Override
    public void afterRestore(org.crac.Context<? extends Resource> context)
```

```
throws Exception {
    System.out.println("After restore");
}
```

Contextnya mempertahankan a [WeakReference](#) ke objek terdaftar. Jika sampah [Resource](#) dikumpulkan, kait runtime tidak berjalan. Kode Anda harus mempertahankan referensi yang kuat Resource untuk menjamin bahwa hook runtime berjalan.

Berikut adalah dua contoh pola yang harus dihindari:

Example — Objek tanpa referensi yang kuat

```
Core.getGlobalContext().register( new MyResource() );
```

Example — Objek kelas anonim

```
Core.getGlobalContext().register( new Resource() {

    @Override
    public void afterRestore(Context<? extends Resource> context) throws Exception {
        // ...
    }

    @Override
    public void beforeCheckpoint(Context<? extends Resource> context) throws Exception {
        // ...
    }

} );
```

Sebaliknya, pertahankan referensi yang kuat. Dalam contoh berikut, sumber daya terdaftar bukan sampah yang dikumpulkan dan kait runtime berjalan secara konsisten.

Example — Objek dengan referensi yang kuat

```
Resource myResource = new MyResource(); // This reference must be maintained to prevent
the registered resource from being garbage collected
Core.getGlobalContext().register( myResource );
```

Pemantauan untuk Lambda SnapStart

Anda dapat memantau SnapStart fungsi Lambda Anda menggunakan Amazon CloudWatch, AWS X-Ray, dan. [Mengakses data telemetri real-time untuk ekstensi menggunakan Telemetri API](#)

Note

[Variabel `AWS_LAMBDA_LOG_GROUP_NAME` dan `AWS_LAMBDA_LOG_STREAM_NAME` lingkungan](#) tidak tersedia dalam fungsi Lambda SnapStart .

CloudWatch untuk SnapStart

Ada beberapa perbedaan dengan format [aliran CloudWatch log](#) untuk SnapStart fungsi:

- Log inisialisasi — Ketika lingkungan eksekusi baru dibuat, REPORT tidak menyertakan `Init Duration` bidang. Itu karena Lambda menginisialisasi SnapStart fungsi saat Anda membuat versi, bukan selama pemanggilan fungsi. Untuk SnapStart fungsi, `Init Duration` bidang ada dalam `INIT_REPORT` catatan. Catatan ini menunjukkan detail durasi untuk [Fase inisialisasi](#), termasuk durasi [kait beforeCheckpoint runtime](#) apa pun.
- Log pemanggilan — Ketika lingkungan eksekusi baru dibuat, REPORT termasuk `Restore Duration` dan `Billed Restore Duration` bidang:
 - `Restore Duration`: Waktu yang dibutuhkan Lambda untuk memulihkan snapshot, memuat runtime (JVM), dan menjalankan kait runtime apa pun. `afterRestore` Proses memulihkan snapshot dapat mencakup waktu yang dihabiskan untuk aktivitas di luar microVM. Kali ini dilaporkan di `Restore Duration`.
 - `Billed Restore Duration`: Waktu yang dibutuhkan Lambda untuk memuat runtime (JVM) dan menjalankan kait apa pun. `afterRestore` Anda tidak dikenakan biaya untuk waktu yang diperlukan untuk memulihkan snapshot.

Note

[Biaya durasi berlaku untuk kode yang berjalan di penanganan fungsi, kode inisialisasi yang dideklarasikan di luar handler, waktu yang diperlukan untuk memuat runtime \(JVM\), dan kode apa pun yang berjalan di hook runtime.](#) Untuk informasi selengkapnya, lihat [SnapStart harga](#).

Durasi awal dingin adalah jumlah dari `Restore Duration` + `Duration`.

Contoh berikut adalah kueri Lambda Insights yang mengembalikan persentil latensi untuk fungsi. SnapStart Untuk informasi selengkapnya tentang kueri Lambda Insights, lihat. [Contoh alur kerja menggunakan kueri untuk memecahkan masalah fungsi](#)

```
filter @type = "REPORT"
  | parse @log /\d+:\aws\lambda\(?<function>.*)/
  | parse @message /Restore Duration: (?<restoreDuration>.*?) ms/
  | stats
count(*) as invocations,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 50) as p50,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 90) as p90,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99) as p99,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99.9) as p99.9
group by function, (ispresent(@initDuration) or ispresent(restoreDuration)) as
coldstart
  | sort by coldstart desc
```

X-Ray penelusuran aktif untuk SnapStart

Anda dapat menggunakan [X-Ray](#) untuk melacak permintaan ke fungsi Lambda SnapStart . Ada beberapa perbedaan dengan subsegmen X-Ray untuk SnapStart fungsi:

- Tidak ada `Initialization` subsegmen untuk SnapStart fungsi.
- `Restore` [Subsegmen menunjukkan waktu yang dibutuhkan Lambda untuk memulihkan snapshot, memuat runtime \(JVM\), dan menjalankan kait runtime apa pun. `afterRestore`](#) Proses memulihkan snapshot dapat mencakup waktu yang dihabiskan untuk aktivitas di luar microVM. Kali ini dilaporkan di `Restore` subsegmen. Anda tidak dikenakan biaya untuk waktu yang dihabiskan di luar microVM untuk memulihkan snapshot.

Acara API telemetri untuk SnapStart

Lambda mengirimkan SnapStart peristiwa berikut ke: [Telemetri API](#)

- [platform.restoreStart](#)— Menunjukkan waktu ketika [Restore](#) fase dimulai.
- [platform.restoreRuntimeDone](#)— Menunjukkan apakah `Restore` fase itu berhasil. Lambda mengirimkan pesan ini saat runtime mengirimkan permintaan API `restore/next runtime`. Ada tiga kemungkinan status: sukses, gagal, dan batas waktu.

- [platform.restoreReport](#)— Menunjukkan berapa lama Restore fase berlangsung dan berapa milidetik Anda ditagih selama fase ini.

Amazon API Gateway dan metrik URL fungsi

Jika Anda membuat API web [menggunakan API Gateway](#), maka Anda dapat menggunakan [IntegrationLatency](#) metrik untuk mengukur end-to-end latensi (waktu antara saat API Gateway menyampaikan permintaan ke backend dan saat menerima respons dari backend).

Jika Anda menggunakan [URL fungsi Lambda](#), maka Anda dapat menggunakan [UrlRequestLatency](#) metrik untuk mengukur end-to-end latensi (waktu antara saat URL fungsi menerima permintaan dan saat URL fungsi mengembalikan respons).

Model keamanan untuk Lambda SnapStart

Lambda SnapStart mendukung enkripsi saat istirahat. Lambda mengenkripsi snapshot dengan file. AWS KMS key Secara default, Lambda menggunakan file. Kunci yang dikelola AWS Jika perilaku default ini sesuai dengan alur kerja Anda, maka Anda tidak perlu menyiapkan hal lain. Jika tidak, Anda dapat menggunakan `--kms-key-arn` opsi dalam [fungsi buat atau update-function-configuration](#) perintah untuk menyediakan kunci yang dikelola AWS KMS pelanggan. Anda dapat melakukan ini untuk mengontrol rotasi kunci KMS atau untuk memenuhi persyaratan organisasi Anda untuk mengelola kunci KMS. Kunci yang dikelola pelanggan dikenakan AWS KMS biaya standar. Untuk informasi selengkapnya, lihat [harga AWS Key Management Service](#).

Saat Anda menghapus versi SnapStart fungsi atau fungsi, semua Invoke permintaan ke fungsi atau versi fungsi tersebut gagal. Lambda secara otomatis menghapus snapshot yang tidak dipanggil selama 14 hari. Lambda menghapus semua sumber daya yang terkait dengan snapshot yang dihapus sesuai dengan Peraturan Perlindungan Data Umum (GDPR).

Maksimalkan kinerja Lambda SnapStart

Topik

- [Penyempurnaan performa](#)
- [Praktik terbaik jaringan](#)

Penyempurnaan performa

Note

SnapStart bekerja paling baik saat digunakan dengan pemanggilan fungsi dalam skala besar. Fungsi yang jarang dipanggil mungkin tidak mengalami peningkatan kinerja yang sama.

Untuk memaksimalkan manfaat SnapStart, kami menyarankan Anda memuat kelas pramuat yang berkontribusi pada latensi startup dalam kode inisialisasi Anda, bukan di penanganan fungsi. Ini memindahkan latensi yang terkait dengan pemuatan kelas berat keluar dari jalur pemanggilan, mengoptimalkan kinerja startup dengan SnapStart.

Jika Anda tidak dapat melakukan pramuat kelas selama inisialisasi, maka kami sarankan Anda memuat kelas dengan pemanggilan dummy. Untuk melakukan ini, perbarui kode fungsi handler, seperti yang ditunjukkan pada contoh berikut dari [fungsi pet store](#) pada GitHub repositori AWS Labs.

```
private static SpringLambdaContainerHandler<AwsProxyRequest, AwsProxyResponse> handler;
static {
    try {
        handler =
SpringLambdaContainerHandler.getAwsProxyHandler(PetStoreSpringAppConfig.class);

        // Use the onStartup method of the handler to register the custom filter
        handler.onStartup(servletContext -> {
            FilterRegistration.Dynamic registration =
servletContext.addFilter("CognitoIdentityFilter", CognitoIdentityFilter.class);
            registration.addMappingForUrlPatterns(EnumSet.of(DispatcherType.REQUEST),
false, "/*");
        });

        // Send a fake Amazon API Gateway request to the handler to load classes
        ahead of time
```

```
    ApiGatewayRequestIdentity identity = new ApiGatewayRequestIdentity();
    identity.setApiKey("foo");
    identity.setAccountId("foo");
    identity.setAccessKey("foo");

    AwsProxyRequestContext reqCtx = new AwsProxyRequestContext();
    reqCtx.setPath("/pets");
    reqCtx.setStage("default");
    reqCtx.setAuthorizer(null);
    reqCtx.setIdentity(identity);

    AwsProxyRequest req = new AwsProxyRequest();
    req.setHttpMethod("GET");
    req.setPath("/pets");
    req.setBody("");
    req.setRequestContext(reqCtx);

    Context ctx = new TestContext();
    handler.proxy(req, ctx);

} catch (ContainerInitializationException e) {
    // if we fail here. We re-throw the exception to force another cold start
    e.printStackTrace();
    throw new RuntimeException("Could not initialize Spring framework", e);
}
}
```

Praktik terbaik jaringan

Status koneksi yang ditetapkan fungsi Anda selama fase inisialisasi tidak dijamin saat Lambda melanjutkan fungsi Anda dari snapshot. Dalam kebanyakan kasus, koneksi jaringan yang AWS SDK dibuat secara otomatis dilanjutkan. Untuk koneksi lain, kami merekomendasikan praktik terbaik berikut.

Membangun kembali koneksi jaringan

Selalu buat kembali koneksi jaringan Anda saat fungsi Anda dilanjutkan dari snapshot. Kami menyarankan Anda membangun kembali koneksi jaringan di function handler. Atau, Anda dapat menggunakan [hook afterRestore runtime](#).

Jangan gunakan nama host sebagai pengenal lingkungan eksekusi yang unik

Kami merekomendasikan untuk tidak menggunakan `hostname` untuk mengidentifikasi lingkungan eksekusi Anda sebagai node atau wadah unik dalam aplikasi Anda. Dengan SnapStart, satu snapshot digunakan sebagai status awal untuk beberapa lingkungan eksekusi, dan semua lingkungan eksekusi mengembalikan `hostname` nilai yang sama untuk `InetAddress.getLocalHost()`. Untuk aplikasi yang memerlukan identitas atau `hostname` nilai lingkungan eksekusi yang unik, sebaiknya Anda membuat ID unik di pengendali fungsi. Atau, gunakan [hook afterRestore runtime](#) untuk menghasilkan ID unik, lalu gunakan ID unik sebagai pengenal untuk lingkungan eksekusi.

Hindari mengikat koneksi ke port sumber tetap

Kami menyarankan Anda menghindari pengikatan koneksi jaringan ke port sumber tetap. Koneksi dibuat kembali ketika fungsi dilanjutkan dari snapshot, dan koneksi jaringan yang terikat ke port sumber tetap mungkin gagal.

Hindari menggunakan DNS cache Java

Fungsi Lambda sudah cache DNS respons. Jika Anda menggunakan DNS cache lain dengan SnapStart, maka Anda mungkin mengalami batas waktu koneksi saat fungsi dilanjutkan dari snapshot.

`java.util.logging.LoggerKelas` secara tidak langsung dapat mengaktifkan JVM DNS cache. Untuk mengganti pengaturan default, setel [networkaddress.cache.ttl](#) ke 0 sebelum menginisialisasi logger. Contoh:

```
public class MyHandler {
    // first set TTL property
    static{
        java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
    }
    // then instantiate logger
    var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
}
```

Untuk mencegah `UnknownHostException` kegagalan, kami sarankan pengaturan `networkaddress.cache.negative.ttl` ke 0. Anda dapat mengatur properti ini untuk fungsi Lambda dengan variabel `AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0` lingkungan.

Menonaktifkan JVM DNS cache tidak menonaktifkan caching terkelola Lambda. DNS

Kustomisasi perilaku startup runtime Java untuk fungsi Lambda

Halaman ini menjelaskan pengaturan khusus untuk fungsi Java di AWS Lambda. Anda dapat menggunakan pengaturan ini untuk menyesuaikan perilaku startup runtime Java. Ini dapat mengurangi latensi fungsi secara keseluruhan dan meningkatkan kinerja fungsi secara keseluruhan, tanpa harus memodifikasi kode apa pun.

Bagian-bagian

- [Memahami variabel `JAVA_TOOL_OPTIONS` lingkungan](#)

Memahami variabel `JAVA_TOOL_OPTIONS` lingkungan

Di Java, Lambda mendukung variabel `JAVA_TOOL_OPTIONS` lingkungan untuk mengatur variabel baris perintah tambahan di Lambda. Anda dapat menggunakan variabel lingkungan ini dengan berbagai cara, seperti untuk menyesuaikan pengaturan kompilasi berjenjang. Contoh berikutnya menunjukkan bagaimana menggunakan variabel `JAVA_TOOL_OPTIONS` lingkungan untuk kasus penggunaan ini.

Contoh: Menyesuaikan pengaturan kompilasi berjenjang

Kompilasi berjenjang adalah fitur dari mesin virtual Java (JVM). Anda dapat menggunakan pengaturan kompilasi berjenjang tertentu untuk memanfaatkan kompiler JVM's just-in-time (JIT) sebaik-baiknya. Biasanya, kompiler C1 dioptimalkan untuk waktu start-up yang cepat. Kompiler C2 dioptimalkan untuk kinerja keseluruhan terbaik, tetapi juga menggunakan lebih banyak memori dan membutuhkan waktu lebih lama untuk mencapainya.

Ada 5 tingkat kompilasi berjenjang yang berbeda. Pada Level 0, JVM menginterpretasikan kode byte Java. Pada Level 4, JVM menggunakan kompiler C2 untuk menganalisis data profil yang dikumpulkan selama startup aplikasi. Seiring waktu, ia memantau penggunaan kode untuk mengidentifikasi pengoptimalan terbaik.

Menyesuaikan tingkat kompilasi berjenjang dapat membantu Anda mengurangi latensi start dingin fungsi Java. Misalnya, atur tingkat kompilasi berjenjang ke 1 agar JVM menggunakan kompiler C1. Kompiler ini dengan cepat menghasilkan kode asli yang dioptimalkan tetapi tidak menghasilkan data profil apa pun dan tidak pernah menggunakan kompiler C2.

Dalam runtime Java 17, JVM flag untuk kompilasi berjenjang diatur untuk berhenti di level 1 secara default. Untuk runtime Java 11 dan di bawahnya, Anda dapat mengatur tingkat kompilasi berjenjang ke 1 dengan melakukan langkah-langkah berikut:

Untuk menyesuaikan pengaturan kompilasi berjenjang (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi Java yang ingin Anda sesuaikan kompilasi berjenjang.
3. Pilih tab Konfigurasi, lalu pilih variabel Lingkungan di menu sebelah kiri.
4. Pilih Edit.
5. Pilih Tambahkan variabel lingkungan.
6. Untuk kuncinya, masukkan `JAVA_TOOL_OPTIONS`. Untuk nilainya, masukkan `-XX:+TieredCompilation -XX:TieredStopAtLevel=1`.

Edit environment variables

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#)

| Key | Value | |
|-------------------|--|--------|
| JAVA_TOOL_OPTIONS | -XX:+TieredCompilation -XX:TieredStopAtLevel=1 | Remove |

[Add environment variable](#)

► Encryption configuration

Cancel **Save**

7. Pilih Simpan.

Note

Anda juga dapat menggunakan Lambda SnapStart untuk mengurangi masalah start dingin. SnapStart menggunakan snapshot cache dari lingkungan eksekusi Anda untuk meningkatkan kinerja start-up secara signifikan. Untuk informasi selengkapnya tentang SnapStart fitur,

batasan, dan wilayah yang didukung, lihat [Meningkatkan kinerja startup dengan Lambda SnapStart](#).

Contoh: Menyesuaikan perilaku GC menggunakan `_ _ JAVA TOOL OPTIONS`

Java 11 runtime menggunakan [Serial](#) garbage collector (GC) untuk pengumpulan sampah. Secara default, runtime Java 17 juga menggunakan Serial GC. Namun, dengan Java 17 Anda juga dapat menggunakan variabel `JAVA_TOOL_OPTIONS` lingkungan untuk mengubah GC default. Anda dapat memilih antara Parallel GC dan [Shenandoah](#) GC.

Misalnya, jika beban kerja Anda menggunakan lebih banyak memori dan beberapa CPUs, pertimbangkan untuk menggunakan Parallel GC untuk kinerja yang lebih baik. Anda dapat melakukan ini dengan menambahkan berikut ini ke nilai variabel `JAVA_TOOL_OPTIONS` lingkungan Anda:

```
-XX:+UseParallelGC
```

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Java

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti yang memberikan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Metode konteks

- `getRemainingTimeInMillis()` – Mengembalikan jumlah milidetik yang tersisa sebelum waktu eksekusi habis.
- `getFunctionName()` – Mengembalikan nama fungsi Lambda.
- `getFunctionVersion()` – Mengembalikan [versi](#) fungsi.
- `getInvokedFunctionArn()`— Mengembalikan Amazon Resource Name (ARN) yang digunakan untuk memanggil fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `getMemoryLimitInMB()` – Mengembalikan jumlah memori yang dialokasikan untuk fungsi tersebut.
- `getAwsRequestId()` – Mengembalikan pengidentifikasi permintaan invokasi.
- `getLogGroupName()` – Mengembalikan grup log untuk fungsi.
- `getLogStreamName()` – Mengembalikan aliran log untuk instans fungsi.
- `getIdentity()` – (aplikasi seluler) Mengembalikan informasi tentang Amazon Cognito yang mengesahkan permintaan.
- `getClientContext()` – (aplikasi seluler) Mengembalikan konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
- `getLogger()` – Mengembalikan [objek logger](#) untuk fungsi.

Contoh berikut menunjukkan fungsi yang menggunakan objek konteks untuk mengakses logger Lambda.

Example [Handler.java](#)

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
```

```
import java.util.Map;

// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, Void>{

    @Override
    public Void handleRequest(Map<String,String> event, Context context)
    {
        LambdaLogger logger = context.getLogger();
        logger.log("EVENT TYPE: " + event.getClass());
        return null;
    }
}
```

Fungsi mencatat jenis kelas dari acara yang masuk sebelum kembalinya.

Example output log

```
EVENT TYPE: class java.util.LinkedHashMap
```

Antarmuka untuk objek konteks tersedia di [aws-lambda-java-core](#) perpustakaan. Anda dapat menerapkan antarmuka ini untuk membuat kelas konteks untuk pengujian. Contoh berikut menunjukkan kelas konteks yang mengembalikan nilai tiruan untuk sebagian besar properti dan logger uji kerja.

Example [TestContextsrc/test/java/contoh/ .java](#)

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.CognitoIdentity;
import com.amazonaws.services.lambda.runtime.ClientContext;
import com.amazonaws.services.lambda.runtime.LambdaLogger;

public class TestContext implements Context{

    public TestContext() {}
    public String getAwsRequestId(){
        return new String("495b12a8-xmpl-4eca-8168-160484189f99");
    }
    public String getLogGroupName(){
        return new String("/aws/lambda/my-function");
    }
}
```



```
}
public String getLogStreamName(){
    return new String("2020/02/26/[$LATEST]704f8dxmla04097b9134246b8438f1a");
}
public String getFunctionName(){
    return new String("my-function");
}
public String getFunctionVersion(){
    return new String("$LATEST");
}
public String getInvokedFunctionArn(){
    return new String("arn:aws:lambda:us-east-2:123456789012:function:my-function");
}
public CognitoIdentity getIdentity(){
    return null;
}
public ClientContext getClientContext(){
    return null;
}
public int getRemainingTimeInMillis(){
    return 300000;
}
public int getMemoryLimitInMB(){
    return 512;
}
public LambdaLogger getLogger(){
    return new TestLogger();
}
}
```

Untuk informasi lebih lanjut tentang log, lihat [Log dan pantau fungsi Java Lambda](#).

Konteks dalam aplikasi sampel

GitHub Repositori untuk panduan ini mencakup contoh aplikasi yang menunjukkan penggunaan objek konteks. Setiap contoh aplikasi menyertakan skrip untuk penyebaran dan pembersihan yang mudah, templat AWS Serverless Application Model (AWS SAM), dan sumber daya pendukung.

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.

- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon GatewayAPI, Amazon, dan Amazon SQS Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan ketergantungan AWS SDK sebagai.
- [s3-java](#) — Fungsi Java yang memproses peristiwa notifikasi dari Amazon S3 dan menggunakan Java Class Library JCL () untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk memanggil fungsi.

Log dan pantau fungsi Java Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda dan mengirim entri log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap pemanggilan dan output lainnya dari kode fungsi Anda ke aliran log. Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Untuk mengeluarkan log dari kode fungsi Anda, Anda dapat menggunakan metode di [java.lang.System](#), atau modul logging apa pun yang menulis ke stdout atau stderr.

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Menggunakan kontrol logging lanjutan Lambda dengan Java](#)
- [Menerapkan logging lanjutan dengan Log4j2 dan SLF4J](#)
- [Menggunakan alat logging dan pustaka lainnya](#)
- [Menggunakan Powertools untuk AWS Lambda \(Java\) dan AWS SAM untuk logging terstruktur](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)
- [Kode pencatatan sampel](#)

Membuat fungsi yang mengembalikan log

Untuk menghasilkan log dari kode fungsi, Anda dapat menggunakan metode di [java.lang.System](#), atau modul pencatatan apa pun yang menulis ke stdout atau stderr. [aws-lambda-java-core](#) Pustaka menyediakan kelas logger bernama `LambdaLogger` yang dapat Anda akses dari objek konteks. Kelas logger mendukung log beberapa baris.

Contoh berikut menggunakan logger `LambdaLogger` yang disediakan oleh objek konteks.

Example Handler.java

```
// Handler value: example.Handler
public class Handler implements RequestHandler<Object, String>{
```

```
Gson gson = new GsonBuilder().setPrettyPrinting().create();
@Override
public String handleRequest(Object event, Context context)
{
    LambdaLogger logger = context.getLogger();
    String response = new String("SUCCESS");
    // log execution details
    logger.log("ENVIRONMENT VARIABLES: " + gson.toJson(System.getenv()));
    logger.log("CONTEXT: " + gson.toJson(context));
    // process event
    logger.log("EVENT: " + gson.toJson(event));
    return response;
}
}
```

Example format log

```
START RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Version: $LATEST
ENVIRONMENT VARIABLES:
{
  "_HANDLER": "example.Handler",
  "AWS_EXECUTION_ENV": "AWS_Lambda_java8",
  "AWS_LAMBDA_FUNCTION_MEMORY_SIZE": "512",
  ...
}
CONTEXT:
{
  "memoryLimit": 512,
  "awsRequestId": "6bc28136-xmpl-4365-b021-0ce6b2e64ab0",
  "functionName": "java-console",
  ...
}
EVENT:
{
  "records": [
    {
      "messageId": "19dd0b57-xmpl-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
      ...
    }
  ]
}
```

```
END RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0
REPORT RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Duration: 198.50 ms Billed
Duration: 200 ms Memory Size: 512 MB Max Memory Used: 90 MB Init Duration: 524.75 ms
```

Runtime Java mencatat baris START, END, dan REPORT untuk setiap invokasi. Baris laporan memberikan detail berikut:

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Menggunakan kontrol logging lanjutan Lambda dengan Java

Untuk memberi Anda kontrol lebih besar atas bagaimana log fungsi Anda ditangkap, diproses, dan dikonsumsi, Anda dapat mengonfigurasi opsi logging berikut untuk runtime Java yang didukung:

- Format log - pilih antara teks biasa dan format JSON terstruktur untuk log fungsi Anda
- Tingkat log - untuk log dalam format JSON, pilih tingkat detail log yang dikirim CloudWatch Lambda, seperti ERROR, DEBUG, atau INFO
- Grup log - pilih grup CloudWatch log yang dikirimkan oleh fungsi Anda

Untuk informasi selengkapnya tentang opsi pencatatan ini, dan petunjuk tentang cara mengonfigurasi fungsi Anda untuk menggunakannya, lihat [the section called “Konfigurasi log fungsi”](#).

Untuk menggunakan format log dan opsi tingkat log dengan fungsi Java Lambda Anda, lihat panduan di bagian berikut.

Menggunakan format log JSON terstruktur dengan Java

Jika Anda memilih JSON untuk format log fungsi Anda, Lambda akan mengirim output log menggunakan kelas sebagai JSON `LambdaLogger` terstruktur. Setiap objek log JSON berisi setidaknya empat pasangan nilai kunci dengan kunci berikut:

- "timestamp"- waktu pesan log dihasilkan
- "level"- tingkat log yang ditetapkan untuk pesan
- "message"- isi pesan log
- "AWSrequestId"- ID permintaan unik untuk pemanggilan fungsi

Bergantung pada metode logging yang Anda gunakan, output log dari fungsi Anda yang ditangkap dalam format JSON juga dapat berisi pasangan nilai kunci tambahan.

Untuk menetapkan level ke log yang Anda buat menggunakan `LambdaLogger` logger, Anda perlu memberikan `LogLevel` argumen dalam perintah logging Anda seperti yang ditunjukkan pada contoh berikut.

Example Kode logging Java

```
LambdaLogger logger = context.getLogger();  
logger.log("This is a debug log", LogLevel.DEBUG);
```

Output log ini dengan kode contoh ini akan ditangkap di CloudWatch Log sebagai berikut:

Example Catatan log JSON

```
{  
  "timestamp": "2023-11-01T00:21:51.358Z",  
  "level": "DEBUG",  
  "message": "This is a debug log",  
  "AWSrequestId": "93f25699-2cbf-4976-8f94-336a0aa98c6f"  
}
```

Jika Anda tidak menetapkan level ke output log Anda, Lambda akan secara otomatis menentukannya INFO level.

Jika kode Anda sudah menggunakan pustaka logging lain untuk menghasilkan log terstruktur JSON, Anda tidak perlu membuat perubahan apa pun. Lambda tidak menyandikan dua kali log apa pun

yang sudah dikodekan JSON. Bahkan jika Anda mengonfigurasi fungsi Anda untuk menggunakan format log JSON, output logging Anda muncul CloudWatch dalam struktur JSON yang Anda tentukan.

Menggunakan penyaringan tingkat log dengan Java

AWS Lambda Untuk memfilter log aplikasi Anda sesuai dengan tingkat lognya, fungsi Anda harus menggunakan log berformat JSON. Anda dapat mencapai ini dengan dua cara:

- Buat output log menggunakan standar LambdaLogger dan konfigurasi fungsi Anda untuk menggunakan pemformatan log JSON. Lambda kemudian memfilter output log Anda menggunakan pasangan nilai kunci "level" di objek JSON yang dijelaskan di [the section called "Menggunakan format log JSON terstruktur dengan Java"](#) Untuk mempelajari cara mengonfigurasi format log fungsi Anda, lihat [the section called "Konfigurasi log fungsi"](#).
- Gunakan pustaka atau metode logging lain untuk membuat log terstruktur JSON dalam kode Anda yang menyertakan pasangan nilai kunci "level" yang menentukan tingkat keluaran log. Anda dapat menggunakan pustaka logging apa pun yang dapat menulis log JSON ke stdout atau stderr. Misalnya, Anda dapat menggunakan Powertools for AWS Lambda atau paket Log4j2 untuk menghasilkan output log terstruktur JSON dari kode Anda. Lihat [the section called "Menggunakan Powertools untuk AWS Lambda \(Java\) dan AWS SAM untuk logging terstruktur"](#) dan [the section called "Menerapkan logging lanjutan dengan Log4j2 dan SLF4J"](#) untuk mempelajari lebih lanjut.

Ketika Anda mengonfigurasi fungsi Anda untuk menggunakan pemfilteran tingkat log, Anda harus memilih dari opsi berikut untuk tingkat log yang ingin Lambda kirim ke Log: CloudWatch

| Tingkat log | Penggunaan standar |
|-----------------------|--|
| TRACE (paling detail) | Informasi paling halus yang digunakan untuk melacak jalur eksekusi kode Anda |
| AWAKUTU | Informasi terperinci untuk debugging sistem |
| INFO | Pesan yang merekam operasi normal fungsi Anda |
| PERINGATAN | Pesan tentang potensi kesalahan yang dapat menyebabkan perilaku tak terduga jika tidak ditangani |

| Tingkat log | Penggunaan standar |
|-----------------------|---|
| ERROR | Pesan tentang masalah yang mencegah kode berfungsi seperti yang diharapkan |
| FATAL (paling detail) | Pesan tentang kesalahan serius yang menyebabkan aplikasi berhenti berfungsi |

Agar Lambda dapat memfilter log fungsi Anda, Anda juga harus menyertakan pasangan nilai "timestamp" kunci dalam keluaran log JSON Anda. Waktu harus ditentukan dalam format stempel waktu [RFC 3339](#) yang valid. Jika Anda tidak menyediakan stempel waktu yang valid, Lambda akan menetapkan log INFO level dan menambahkan stempel waktu untuk Anda.

Lambda mengirimkan log dari level yang dipilih dan lebih rendah ke CloudWatch. Misalnya, jika Anda mengonfigurasi level log WARN, Lambda akan mengirim log yang sesuai dengan level WARN, ERROR, dan FATAL.

Menerapkan logging lanjutan dengan Log4j2 dan SLF4J

Note

AWS Lambda tidak menyertakan Log4j2 dalam runtime terkelola atau gambar wadah dasarnya. Oleh karena itu, ini tidak terpengaruh oleh masalah yang dijelaskan dalam CVE-2021-44228, CVE-2021-45046, dan CVE-2021-45105.

Untuk kasus di mana fungsi pelanggan menyertakan versi Log4j2 yang terpengaruh, kami telah menerapkan perubahan pada [runtime terkelola](#) Lambda Java dan [gambar wadah dasar](#) yang membantu mengurangi masalah di CVE-2021-44228, CVE-2021-45046, dan CVE-2021-45105. Sebagai hasil dari perubahan ini, pelanggan yang menggunakan Log4J2 mungkin melihat entri log tambahan, mirip dengan `Transforming org/apache/logging/log4j/core/lookup/JndiLookup (java.net.URLClassLoader@...)` String log apa pun yang mereferensikan jndi mapper di output Log4J2 akan diganti dengan `Patched JndiLookup::lookup()`

Terlepas dari perubahan ini, kami sangat mendorong semua pelanggan yang fungsinya termasuk Log4j2 untuk memperbarui ke versi terbaru. Secara khusus, pelanggan yang menggunakan pustaka `aws-lambda-java-log 4j2` dalam fungsinya harus memperbarui ke versi 1.5.0 (atau yang lebih baru), dan menerapkan ulang fungsi mereka. Versi ini memperbarui dependensi utilitas Log4j2 yang mendasarinya ke versi 2.17.0 (atau yang lebih baru). [Biner](#)

[aws-lambda-java-log 4j2 yang diperbarui tersedia di repositori Maven dan kode sumbernya tersedia di Github.](#)

Terakhir, perhatikan bahwa pustaka apa pun yang terkait dengan aws-lambda-java-log4j (v1.0.0 atau 1.0.1) tidak boleh digunakan dalam keadaan apa pun. Pustaka ini terkait dengan versi 1.x dari log4j yang berakhir pada tahun 2015. Pustaka tidak didukung, tidak dipelihara, tidak ditambah, dan memiliki kerentanan keamanan yang diketahui.

Untuk menyesuaikan output log, mendukung pencatatan selama pengujian unit, dan log panggilan AWS SDK, gunakan Apache Log4j2 dengan SLF4J. Log4j adalah pustaka log untuk program Java yang memungkinkan Anda mengonfigurasi tingkat log dan menggunakan pustaka appender. SLF4J adalah pustaka fasad yang memungkinkan Anda mengubah pustaka mana yang Anda gunakan tanpa mengubah kode fungsi Anda.

Untuk menambahkan ID permintaan ke log fungsi Anda, gunakan appender di pustaka [aws-lambda-java-log4j2](#).

Example [src/main/resources/log4j2.xml](#) – Konfigurasi appender

```
<Configuration>
  <Appenders>
    <Lambda name="Lambda" format="{env:AWS_LAMBDA_LOG_FORMAT:-TEXT}">
      <LambdaTextFormat>
        <PatternLayout>
          <pattern>%d{yyyy-MM-dd HH:mm:ss} %X{AWSRequestId} %-5p %c{1} - %m%n </
pattern>
        </PatternLayout>
      </LambdaTextFormat>
      <LambdaJSONFormat>
        <JsonTemplateLayout eventTemplateUri="classpath:LambdaLayout.json" />
      </LambdaJSONFormat>
    </Lambda>
  </Appenders>
  <Loggers>
    <Root level="{env:AWS_LAMBDA_LOG_LEVEL:-INFO}">
      <AppenderRef ref="Lambda"/>
    </Root>
    <Logger name="software.amazon.awssdk" level="WARN" />
    <Logger name="software.amazon.awssdk.request" level="DEBUG" />
  </Loggers>
</Configuration>
```

Anda dapat memutuskan bagaimana log Log4j2 Anda dikonfigurasi untuk teks biasa atau output JSON dengan menentukan tata letak di bawah tag dan. `<LambdaTextFormat>`
`<LambdaJSONFormat>`

Dalam contoh ini, dalam mode teks, setiap baris ditambahkan dengan tanggal, waktu, ID permintaan, tingkat log, dan nama kelas. Dalam mode JSON, `<JsonTemplateLayout>` digunakan dengan konfigurasi yang dikirimkan bersama dengan `aws-lambda-java-log4j2` perpustakaan.

SLF4J adalah pustaka fasad untuk login ke kode Java. Dalam kode fungsi Anda, Anda menggunakan pabrik logger SLF4J untuk mengambil logger dengan metode untuk tingkat log seperti `info()` dan `warn()`. Dalam konfigurasi build Anda, Anda menyertakan pustaka pencatatan dan adaptor SLF4J di classpath. Dengan mengubah pustaka dalam konfigurasi build, Anda dapat mengubah tipe logger tanpa mengubah kode fungsi Anda. SLF4J diperlukan untuk menangkap log dari SDK for Java.

Dalam contoh kode berikut, kelas handler menggunakan SLF4J untuk mengambil logger.

Example [src/main/java/example/HandlerS3.java](#) - Logging dengan SLF4J

```
package example;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;

import static org.apache.logging.log4j.CloseableThreadContext.put;

public class HandlerS3 implements RequestHandler<S3Event, String>{
    private static final Logger logger = LoggerFactory.getLogger(HandlerS3.class);

    @Override
    public String handleRequest(S3Event event, Context context) {
        for(var record : event.getRecords()) {
            try (var loggingCtx = put("awsRegion", record.getAwsRegion())) {
                loggingCtx.put("eventName", record.getEventName());
                loggingCtx.put("bucket", record.getS3().getBucket().getName());
                loggingCtx.put("key", record.getS3().getObject().getKey());

                logger.info("Handling s3 event");
            }
        }
    }
}
```

```
    }  
  }  
  
  return "Ok";  
}  
}
```

Kode ini menghasilkan output log seperti berikut:

Example format log

```
{  
  "timestamp": "2023-11-15T16:56:00.815Z",  
  "level": "INFO",  
  "message": "Handling s3 event",  
  "logger": "example.HandlerS3",  
  "AWSRequestId": "0bced576-3936-4e5a-9dcd-db9477b77f97",  
  "awsRegion": "eu-south-1",  
  "bucket": "java-logging-test-input-bucket",  
  "eventName": "ObjectCreated:Put",  
  "key": "test-folder/"  
}
```

Konfigurasi build mengambil dependensi runtime pada appender Lambda dan adaptor SLF4J, dan dependensi implementasi pada Log4j2.

Example build.gradle – dependensi pencatatan

```
dependencies {  
  ...  
  'com.amazonaws:aws-lambda-java-log4j2:[1.6.0,)',  
  'com.amazonaws:aws-lambda-java-events:[3.11.3,)',  
  'org.apache.logging.log4j:log4j-layout-template-json:[2.17.1,)',  
  'org.apache.logging.log4j:log4j-slf4j2-impl:[2.19.0,)',  
  ...  
}
```

Saat Anda menjalankan kode Anda secara lokal untuk pengujian, objek konteks dengan logger Lambda tidak tersedia, dan tidak ada ID permintaan untuk appender Lambda untuk digunakan. Misalnya konfigurasi uji, lihat aplikasi sampel di bagian berikutnya.

Menggunakan alat logging dan pustaka lainnya

[Powertools for AWS Lambda \(Java\)](#) adalah toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang. [Utilitas Logging](#) menyediakan logger yang dioptimalkan Lambda yang mencakup informasi tambahan tentang konteks fungsi di semua fungsi Anda dengan output terstruktur sebagai JSON. Gunakan utilitas ini untuk melakukan hal berikut:

- Tangkap bidang kunci dari konteks Lambda, cold start, dan struktur logging output sebagai JSON
- Log peristiwa pemanggilan Lambda saat diinstruksikan (dininaktifkan secara default)
- Cetak semua log hanya untuk persentase pemanggilan melalui pengambilan sampel log (dininaktifkan secara default)
- Tambahkan kunci tambahan ke log terstruktur kapan saja
- Gunakan pemformat log kustom (Bring Your Own Formatter) untuk mengeluarkan log dalam struktur yang kompatibel dengan RFC Logging organisasi Anda

Menggunakan Powertools untuk AWS Lambda (Java) dan AWS SAM untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Java dengan [Powertools terintegrasi untuk AWS Lambda \(Java\)](#) ~ modul menggunakan modul. AWS SAM Aplikasi ini mengimplementasikan backend API dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim permintaan GET ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan hello world pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Java 11
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75](#) atau yang lebih baru. Jika Anda memiliki versi CLI yang lebih lama, lihat [Memutakhirkan AWS SAM CLI. AWS SAM](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan template Hello World Java.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type Zip --runtime java11 --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan URL aplikasi yang digunakan:

```
aws cloudformation describe-stacks --stack-name sam-app --query 'Stacks[0].Outputs[?OutputKey=='HelloWorldApi`'].OutputValue' --output text
```

6. Memanggil titik akhir API:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name sam-app
```

Output log terlihat seperti ini:

```

2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.095000
  INIT_START Runtime Version: java:11.v15    Runtime Version ARN: arn:aws:lambda:eu-
central-1::runtime:0a25e3e7a1cc9ce404bc435eeb2ad358d8fa64338e618d0c224fe509403583ca
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.114000
  Picked up JAVA_TOOL_OPTIONS: -XX:+TieredCompilation -XX:TieredStopAtLevel=1
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.793000
  Transforming org/apache/logging/log4j/core/lookup/JndiLookup
(lambdainternal.CustomerClassLoader@1a6c5a9e)
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:35.252000
  START RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765 Version: $LATEST
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.531000 {
  "_aws": {
    "Timestamp": 1675416276051,
    "CloudWatchMetrics": [
      {
        "Namespace": "sam-app-powerools-java",
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ],
        "Dimensions": [
          [
            "Service",
            "FunctionName"
          ]
        ]
      }
    ]
  },
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
"Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "FunctionName": "sam-app>HelloWorldFunction-y9Iu1FLJJBGD",
  "functionVersion": "$LATEST",
  "ColdStart": 1.0,
  "Service": "service_undefined",
  "logStreamId": "2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81",
  "executionEnvironment": "AWS_Lambda_java11"
}

```

```

2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.974000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.AWSXRayRecorder <init>
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.config.DaemonConfiguration <init>
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000
 INFO: Environment variable AWS_XRAY_DAEMON_ADDRESS is set. Emitting to daemon on
 address XXXX.XXXX.XXXX.XXXX:2000.
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.331000
 09:24:37.294 [main] INFO helloworld.App - {"version":null,"resource":"/
hello","path":"/hello/","httpMethod":"GET","headers":{"Accept":["*/
*"],"CloudFront-Forwarded-Proto":"https","CloudFront-Is-Desktop-
Viewer":"true","CloudFront-Is-Mobile-Viewer":"false","CloudFront-Is-
SmartTV-Viewer":"false","CloudFront-Is-Tablet-Viewer":"false","CloudFront-
Viewer-ASN":"16509","CloudFront-Viewer-Country":"IE","Host":"XXXX.execute-
api.eu-central-1.amazonaws.com","User-Agent":"curl/7.86.0","Via":["2.0
f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)","X-Amz-
Cf-Id":["t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtivV1Q=="],"X-
Amzn-Trace-Id":["Root=1-63dcd2d1-25f90b9d1c753a783547f4dd"],"X-Forwarded-
For":["XX.XXX.XXX.XX, XX.XXX.XXX.XX"],"X-Forwarded-Port":["443"],"X-
Forwarded-Proto":["https"],"multiValueHeaders":{"Accept":["*/
*"],"CloudFront-Forwarded-Proto":["https"],"CloudFront-Is-Desktop-Viewer":
["true"],"CloudFront-Is-Mobile-Viewer":["false"],"CloudFront-Is-SmartTV-
Viewer":["false"],"CloudFront-Is-Tablet-Viewer":["false"],"CloudFront-Viewer-
ASN":["16509"],"CloudFront-Viewer-Country":["IE"],"Host":["XXXX.execute-
api.eu-central-1.amazonaws.com"],"User-Agent":["curl/7.86.0"],"Via":["2.0
f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)","X-Amz-
Cf-Id":["t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtivV1Q=="],"X-
Amzn-Trace-Id":["Root=1-63dcd2d1-25f90b9d1c753a783547f4dd"],"X-Forwarded-
For":["XXX, XXX"],"X-Forwarded-Port":["443"],"X-Forwarded-Proto":
["https"],"queryStringParameters":null,"multiValueQueryStringParameters":null,"pathParamet
{"accountId":"XXX","stage":"Prod","resourceId":"at73a1","requestId":"ba09ecd2-
acf3-40f6-89af-fad32df67597","operationName":null,"identity":
{"cognitoIdentityPoolId":null,"accountId":null,"cognitoIdentityId":null,"caller":null,"apiK
hello","httpMethod":"GET","apiId":"XXX","path":"/Prod/
hello/","authorizer":null},"body":null,"isBase64Encoded":false}
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.351000
 09:24:37.351 [main] INFO helloworld.App - Retrieving https://
checkip.amazonaws.com
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.313000 {
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
  "Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "xray_trace_id": "1-63dcd2d1-25f90b9d1c753a783547f4dd",
  "functionVersion": "$LATEST",

```

```

"Service": "service_undefined",
"logStreamId": "2023/02/03/[$LATEST]851411a899b545eea2cffebe4cfbec81",
"executionEnvironment": "AWS_Lambda_java11"
}
2023/02/03/[$LATEST]851411a899b545eea2cffebe4cfbec81 2023-02-03T09:24:39.371000 END
RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765
2023/02/03/[$LATEST]851411a899b545eea2cffebe4cfbec81 2023-02-03T09:24:39.371000
REPORT RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765    Duration: 4118.98 ms
Billed Duration: 4119 ms    Memory Size: 512 MB    Max Memory Used: 152 MB    Init
Duration: 1155.47 ms
XRAY TraceId: 1-63dcd2d1-25f90b9d1c753a783547f4dd    SegmentId: 3a028fee19b895cb
Sampled: true

```

8. Ini adalah titik akhir API publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Mengelola retensi log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log tanpa batas waktu, hapus grup log, atau konfigurasi periode retensi setelah itu secara CloudWatch otomatis menghapus log. Untuk mengatur penyimpanan log, tambahkan yang berikut ini ke AWS SAM templat Anda:

```

Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7

```

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, kami sarankan untuk menginstrumentasi fungsi Anda dengan AWS X-Ray. X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBUIQgUmVxdWVzdE1k0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzVlNGZiMjEgVmVyc2l1vb...",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0\"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15

detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
```

```

"events": [
  {
    "timestamp": 1559763003171,
    "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
    "ingestionTime": 1559763003309
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n$LATEST\n",
\r ...",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
    "ingestionTime": 1559763018353
  }
],
"nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}

```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Kode pencatatan sampel

GitHub Repositori untuk panduan ini mencakup contoh aplikasi yang menunjukkan penggunaan berbagai konfigurasi logging. Setiap contoh aplikasi menyertakan skrip untuk penyebaran dan pembersihan yang mudah, AWS SAM templat, dan sumber daya pendukung.

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon API Gateway, Amazon SQS, dan Amazon Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan AWS SDK sebagai dependensi.
- [s3-java](#) – Fungsi Java yang memproses kejadian pemberitahuan dari Amazon S3 dan menggunakan Java Class Library (JCL) untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk menjalankan fungsi.

Aplikasi sampel `java-basic` menunjukkan konfigurasi pencatatan minimal yang mendukung uji pencatatan. Kode handler menggunakan logger `LambdaLogger` yang disediakan oleh objek konteks. Untuk pengujian, aplikasi menggunakan `TestLogger` kelas khusus yang mengimplementasikan `LambdaLogger` antarmuka dengan logger `Log4j2`. Ini menggunakan `SLF4J` sebagai fasad untuk kompatibilitas dengan SDK. AWS Pustaka log masuk dikecualikan dari output pembuatan untuk menjaga paket deployment tetap kecil.

Menginstrumentasi kode Java di AWS Lambda

Lambda terintegrasi AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari dua SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK for Java](#)— An SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.
- [Powertools for AWS Lambda \(Java\)](#) - Toolkit pengembang untuk menerapkan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh. AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray](#). SDKs

Bagian-bagian

- [Menggunakan Powertools untuk AWS Lambda \(Java\) dan AWS SAM untuk melacak](#)
- [Menggunakan Powertools untuk AWS Lambda \(Java\) dan AWS CDK untuk melacak](#)
- [Menggunakan ADOT untuk instrumen fungsi Java Anda](#)
- [Menggunakan X-Ray SDK untuk instrumen fungsi Java Anda](#)
- [Mengaktifkan penelusuran dengan konsol Lambda](#)

- [Mengaktifkan penelusuran dengan Lambda API](#)
- [Mengaktifkan penelusuran dengan AWS CloudFormation](#)
- [Menafsirkan jejak X-Ray](#)
- [Menyimpan dependensi runtime dalam lapisan \(X-Ray\) SDK](#)
- [Penelusuran X-Ray dalam aplikasi sampel \(SDKX-Ray\)](#)

Menggunakan Powertools untuk AWS Lambda (Java) dan AWS SAM untuk melacak

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Java dengan [Powertools terintegrasi untuk modul AWS Lambda \(Java\)](#) menggunakan modul. AWS SAM Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan hello world pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Java 11
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan template Hello World Java.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type Zip --runtime java11 --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena `HelloWorldFunction` mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name sam-app --query  
'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Memanggil titik API akhir:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

```
New XRay Service Graph  
Start time: 2023-02-03 14:31:48+01:00  
End time: 2023-02-03 14:31:48+01:00  
Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-y9Iu1FLJJBGD -  
Edges: []  
Summary_statistics:  
  - total requests: 1  
  - ok count(2XX): 1  
  - error count(4XX): 0
```



```

- fault count(5XX): 0
- total response time: 5.587
Reference Id: 1 - client - sam-app>HelloWorldFunction-y9Iu1FLJJBGD - Edges: [0]
Summary_statistics:
- total requests: 0
- ok count(2XX): 0
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0

```

```

XRay Event [revision 3] at (2023-02-03T14:31:48.500000) with id
(1-63dd0cc4-3c869dec72a586875da39777) and duration (5.603s)
- 5.587s - sam-app>HelloWorldFunction-y9Iu1FLJJBGD [HTTP: 200]
- 4.053s - sam-app>HelloWorldFunction-y9Iu1FLJJBGD
- 1.181s - Initialization
- 4.037s - Invocation
- 1.981s - ## handleRequest
- 1.840s - ## getPageContents
- 0.000s - Overhead

```

- Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Menggunakan Powertools untuk AWS Lambda (Java) dan AWS CDK untuk melacak

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World Java dengan [Powertools terintegrasi untuk modul AWS Lambda \(Java\)](#) menggunakan modul. AWS CDK Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan pesan hello world.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [Java 11](#)
- [AWS CLI versi 2](#)
- [AWS CDK versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi baru Anda.

```
mkdir hello-world
cd hello-world
```

2. Inisialisasi aplikasi.

```
cdk init app --language java
```

3. Buat proyek maven dengan perintah berikut:

```
mkdir app
cd app
mvn archetype:generate -DgroupId=helloworld -DartifactId=Function -
DarchetypeArtifactId=maven-archetype-quickstart -DinteractiveMode=false
```

4. Buka pom.xml di hello-world\app\Function direktori dan ganti kode yang ada dengan kode berikut yang mencakup dependensi dan plugin maven untuk Powertools.

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>helloworld</groupId>
  <artifactId>Function</artifactId>
  <packaging>jar</packaging>
  <version>1.0-SNAPSHOT</version>
  <name>Function</name>
  <url>http://maven.apache.org</url>
  <properties>
    <maven.compiler.source>11</maven.compiler.source>
```

```
<maven.compiler.target>11</maven.compiler.target>
<log4j.version>2.17.2</log4j.version>
</properties>
<dependencies>
  <dependency>
    <groupId>junit</groupId>
    <artifactId>junit</artifactId>
    <version>3.8.1</version>
    <scope>test</scope>
  </dependency>
  <dependency>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-tracing</artifactId>
    <version>1.3.0</version>
  </dependency>
  <dependency>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-metrics</artifactId>
    <version>1.3.0</version>
  </dependency>
  <dependency>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-logging</artifactId>
    <version>1.3.0</version>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-lambda-java-core</artifactId>
    <version>1.2.2</version>
  </dependency>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-lambda-java-events</artifactId>
    <version>3.11.1</version>
  </dependency>
</dependencies>
<build>
  <plugins>
    <plugin>
      <groupId>org.codehaus.mojo</groupId>
      <artifactId>aspectj-maven-plugin</artifactId>
      <version>1.14.0</version>
      <configuration>
        <source>${maven.compiler.source}</source>
      </configuration>
    </plugin>
  </plugins>
</build>
```

```

<target>${maven.compiler.target}</target>
<complianceLevel>${maven.compiler.target}</complianceLevel>
<aspectLibraries>
  <aspectLibrary>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-tracing</artifactId>
  </aspectLibrary>
  <aspectLibrary>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-metrics</artifactId>
  </aspectLibrary>
  <aspectLibrary>
    <groupId>software.amazon.lambda</groupId>
    <artifactId>powertools-logging</artifactId>
  </aspectLibrary>
</aspectLibraries>
</configuration>
<executions>
  <execution>
    <goals>
      <goal>compile</goal>
    </goals>
  </execution>
</executions>
</plugin>
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-shade-plugin</artifactId>
  <version>3.4.1</version>
  <executions>
    <execution>
      <phase>package</phase>
      <goals>
        <goal>shade</goal>
      </goals>
      <configuration>
        <transformers>
          <transformer
implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCache
          </transformer>
        </transformers>
        <createDependencyReducedPom>>false</
createDependencyReducedPom>

```

```

        <finalName>function</finalName>

        </configuration>
    </execution>
</executions>
<dependencies>
    <dependency>
        <groupId>com.github.edwgiz</groupId>
        <artifactId>maven-shade-plugin.log4j2-cachefile-
transformer</artifactId>
        <version>2.15</version>
    </dependency>
</dependencies>
</plugin>
</plugins>
</build>
</project>

```

5. Buat `hello-world\app\src\main\resource` direktori dan buat `log4j.xml` untuk konfigurasi log.

```

mkdir -p src/main/resource
cd src/main/resource
touch log4j.xml

```

6. Buka `log4j.xml` dan tambahkan kode berikut.

```

<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
    <Appenders>
        <Console name="JsonAppender" target="SYSTEM_OUT">
            <JsonTemplateLayout
eventTemplateUri="classpath:LambdaJsonLayout.json" />
        </Console>
    </Appenders>
    <Loggers>
        <Logger name="JsonLogger" level="INFO" additivity="false">
            <AppenderRef ref="JsonAppender"/>
        </Logger>
        <Root level="info">
            <AppenderRef ref="JsonAppender"/>
        </Root>
    </Loggers>

```

```
</Configuration>
```

7. Buka `App.java` dari `hello-world\app\Function\src\main\java\helloworld` direktori dan ganti kode yang ada dengan kode berikut. Ini adalah kode untuk fungsi Lambda.

```
package helloworld;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.URL;
import java.util.HashMap;
import java.util.Map;
import java.util.stream.Collectors;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;
import software.amazon.lambda.powertools.logging.Logging;
import software.amazon.lambda.powertools.metrics.Metrics;
import software.amazon.lambda.powertools.tracing.CaptureMode;
import software.amazon.lambda.powertools.tracing.Tracing;

import static software.amazon.lambda.powertools.tracing.CaptureMode.*;

/**
 * Handler for requests to Lambda function.
 */
public class App implements RequestHandler<APIGatewayProxyRequestEvent,
    APIGatewayProxyResponseEvent> {
    Logger log = LogManager.getLogger(App.class);

    @Logging(logEvent = true)
    @Tracing(captureMode = DISABLED)
    @Metrics(captureColdStart = true)
    public APIGatewayProxyResponseEvent handleRequest(final
        APIGatewayProxyRequestEvent input, final Context context) {
        Map<String, String> headers = new HashMap<>();
        headers.put("Content-Type", "application/json");
    }
}
```

```

        headers.put("X-Custom-Header", "application/json");

        APIGatewayProxyResponseEvent response = new APIGatewayProxyResponseEvent()
            .withHeaders(headers);
        try {
            final String pageContents = this.getPageContents("https://
checkip.amazonaws.com");
            String output = String.format("{ \"message\": \"hello world\",
\"location\": \"%s\" }", pageContents);

            return response
                .withStatusCode(200)
                .withBody(output);
        } catch (IOException e) {
            return response
                .withBody("{}")
                .withStatusCode(500);
        }
    }
    @Tracing(namespace = "getPageContents")
    private String getPageContents(String address) throws IOException {
        log.info("Retrieving {}", address);
        URL url = new URL(address);
        try (BufferedReader br = new BufferedReader(new
InputStreamReader(url.openStream())))) {
            return br.lines().collect(Collectors.joining(System.lineSeparator()));
        }
    }
}

```

8. Buka `HelloWorldStack.java` dari `hello-world\src\main\java\com\myorg` direktori dan ganti kode yang ada dengan kode berikut. Kode ini menggunakan [Lambda Constructor](#) dan [ApiGatewayv2 Constructor](#) untuk membuat dan REST API fungsi Lambda.

```

package com.myorg;

import software.amazon.awscdk.*;
import software.amazon.awscdk.services.apigatewayv2.alpha.*;
import
    software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegration;
import
    software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegrationProps;
import software.amazon.awscdk.services.lambda.Code;

```

```
import software.amazon.awscdk.services.lambda.Function;
import software.amazon.awscdk.services.lambda.FunctionProps;
import software.amazon.awscdk.services.lambda.Runtime;
import software.amazon.awscdk.services.lambda.Tracing;
import software.amazon.awscdk.services.logs.RetentionDays;
import software.amazon.awscdk.services.s3.assets.AssetOptions;
import software.constructs.Construct;

import java.util.Arrays;
import java.util.List;

import static java.util.Collections.singletonList;
import static software.amazon.awscdk.BundlingOutput.ARCHIVED;

public class HelloWorldStack extends Stack {
    public HelloWorldStack(final Construct scope, final String id) {
        this(scope, id, null);
    }

    public HelloWorldStack(final Construct scope, final String id, final StackProps
props) {
        super(scope, id, props);

        List<String> functionPackagingInstructions = Arrays.asList(
            "/bin/sh",
            "-c",
            "cd Function " +
                "&& mvn clean install " +
                "&& cp /asset-input/Function/target/function.jar /asset-
output/"
        );
        BundlingOptions.Builder builderOptions = BundlingOptions.builder()
            .command(functionPackagingInstructions)
            .image(Runtime.JAVA_11.getBundlingImage())
            .volumes(singletonList(
                // Mount local .m2 repo to avoid download all the
dependencies again inside the container
                DockerVolume.builder()
                    .hostPath(System.getProperty("user.home") +
"/.m2/")
                    .containerPath("/root/.m2/")
                    .build()
            ))
            .user("root")
    }
}
```



```

        .outputType(ARCHIVED);

    Function function = new Function(this, "Function", FunctionProps.builder()
        .runtime(Runtime.JAVA_11)
        .code(Code.fromAsset("app", AssetOptions.builder()
            .bundling(builderOptions
                .command(functionPackagingInstructions)
                .build())
            .build()))
        .handler("helloworld.App::handleRequest")
        .memorySize(1024)
        .tracing(Tracing.ACTIVE)
        .timeout(Duration.seconds(10))
        .logRetention(RetentionDays.ONE_WEEK)
        .build());

    HttpApi httpApi = new HttpApi(this, "sample-api", HttpApiProps.builder()
        .apiName("sample-api")
        .build());

    httpApi.addRoutes(AddRoutesOptions.builder()
        .path("/")
        .methods(singletonList( HttpMethod.GET))
        .integration(new HttpLambdaIntegration("function", function,
HttpLambdaIntegrationProps.builder()
            .payloadFormatVersion(PayloadFormatVersion.VERSION_2_0)
            .build()))
        .build());

    new CfnOutput(this, "HttpApi", CfnOutputProps.builder()
        .description("Url for Http Api")
        .value(httpApi.getApiEndpoint())
        .build());
    }
}

```

9. Buka `pom.xml` dari `hello-world` direktori dan ganti kode yang ada dengan kode berikut.

```

<?xml version="1.0" encoding="UTF-8"?>
<project xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://
maven.apache.org/xsd/maven-4.0.0.xsd"
    xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <modelVersion>4.0.0</modelVersion>

```

```
<groupId>com.myorg</groupId>
<artifactId>hello-world</artifactId>
<version>0.1</version>

<properties>
  <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
  <cdk.version>2.70.0</cdk.version>
  <constructs.version>[10.0.0,11.0.0)</constructs.version>
  <junit.version>5.7.1</junit.version>
</properties>

<build>
  <plugins>
    <plugin>
      <groupId>org.apache.maven.plugins</groupId>
      <artifactId>maven-compiler-plugin</artifactId>
      <version>3.8.1</version>
      <configuration>
        <source>1.8</source>
        <target>1.8</target>
      </configuration>
    </plugin>

    <plugin>
      <groupId>org.codehaus.mojo</groupId>
      <artifactId>exec-maven-plugin</artifactId>
      <version>3.0.0</version>
      <configuration>
        <mainClass>com.myorg.HelloWorldApp</mainClass>
      </configuration>
    </plugin>
  </plugins>
</build>

<dependencies>
  <!-- AWS Cloud Development Kit -->
  <dependency>
    <groupId>software.amazon.awscdk</groupId>
    <artifactId>aws-cdk-lib</artifactId>
    <version>${cdk.version}</version>
  </dependency>
  <dependency>
    <groupId>software.constructs</groupId>
```

```

        <artifactId>constructs</artifactId>
        <version>${constructs.version}</version>
    </dependency>
    <dependency>
        <groupId>org.junit.jupiter</groupId>
        <artifactId>junit-jupiter</artifactId>
        <version>${junit.version}</version>
        <scope>test</scope>
    </dependency>
    <dependency>
        <groupId>software.amazon.awscdk</groupId>
        <artifactId>apigatewayv2-alpha</artifactId>
        <version>${cdk.version}-alpha.0</version>
    </dependency>
    <dependency>
        <groupId>software.amazon.awscdk</groupId>
        <artifactId>apigatewayv2-integrations-alpha</artifactId>
        <version>${cdk.version}-alpha.0</version>
    </dependency>
</dependencies>
</project>

```

10. Pastikan Anda berada di `hello-world` direktori dan menyebarkan aplikasi Anda.

```
cdk deploy
```

11. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
'Stacks[0].Outputs[?OutputKey==`HttpApi`].OutputValue' --output text
```

12. Memanggil titik API akhir:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

13. Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
sam traces
```

Output jejak terlihat seperti ini:

```

New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app>HelloWorldFunction-YBg8yfYt0c9j -
  Edges: [1]
    Summary_statistics:
      - total requests: 1
      - ok count(2XX): 1
      - error count(4XX): 0
      - fault count(5XX): 0
      - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app>HelloWorldFunction-YBg8yfYt0c9j
  - Edges: []
    Summary_statistics:
      - total requests: 1
      - ok count(2XX): 1
      - error count(4XX): 0
      - fault count(5XX): 0
      - total response time: 0.016
  Reference Id: 2 - client - sam-app>HelloWorldFunction-YBg8yfYt0c9j - Edges: [0]
    Summary_statistics:
      - total requests: 0
      - ok count(2XX): 0
      - error count(4XX): 0
      - fault count(5XX): 0
      - total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
(1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
- 0.924s - sam-app>HelloWorldFunction-YBg8yfYt0c9j [HTTP: 200]
- 0.016s - sam-app>HelloWorldFunction-YBg8yfYt0c9j
  - 0.739s - Initialization
  - 0.016s - Invocation
    - 0.013s - ## lambda_handler
      - 0.000s - ## app.hello
    - 0.000s - Overhead

```

14. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
cdk destroy
```

Menggunakan ADOT untuk instrumen fungsi Java Anda

ADOT menyediakan [lapisan](#) Lambda yang dikelola sepenuhnya yang mengemas semua yang Anda butuhkan untuk mengumpulkan data telemetri menggunakan file. OTEL SDK Dengan menggunakan lapisan ini, Anda dapat menginstruksikan fungsi Lambda Anda tanpa harus memodifikasi kode fungsi apa pun. Anda juga dapat mengonfigurasi lapisan Anda untuk melakukan inisialisasi kustom. OTEL Untuk informasi selengkapnya, lihat [Konfigurasi khusus untuk ADOT Kolektor di Lambda](#) dalam dokumentasi. ADOT

Untuk runtime Java, Anda dapat memilih antara dua lapisan untuk dikonsumsi:

- AWS lapisan Lambda terkelola untuk ADOT Java (Agen Instrumentasi Otomatis) - Lapisan ini secara otomatis mengubah kode fungsi Anda saat startup untuk mengumpulkan data penelusuran. Untuk petunjuk rinci tentang cara menggunakan layer ini bersama dengan agen ADOT Java, lihat [AWS Distro untuk OpenTelemetry Lambda Support for Java \(Auto-instrumentation Agent\)](#) dalam dokumentasi. ADOT
- AWS lapisan Lambda terkelola untuk ADOT Java - Lapisan ini juga menyediakan instrumentasi bawaan untuk fungsi Lambda, tetapi memerlukan beberapa perubahan kode manual untuk menginisialisasi. OTEL SDK Untuk petunjuk rinci tentang cara menggunakan lapisan ini, lihat [AWS Distro untuk OpenTelemetry Lambda Support](#) for Java ADOT di dokumentasi.

Menggunakan X-Ray SDK untuk instrumen fungsi Java Anda

Untuk merekam data tentang panggilan yang dilakukan fungsi Anda ke sumber daya dan layanan lain dalam aplikasi Anda, Anda dapat menambahkan X-Ray SDK untuk Java ke konfigurasi build Anda. Contoh berikut menunjukkan konfigurasi build Gradle yang menyertakan pustaka yang mengaktifkan instrumentasi otomatis klien. AWS SDK for Java 2.x

Example [build.gradle](#) – Melacak dependensi

```
dependencies {  
    implementation platform('software.amazon.awssdk:bom:2.16.1')  
    implementation platform('com.amazonaws:aws-xray-recorder-sdk-bom:2.11.0')  
    ...  
}
```

```
implementation 'com.amazonaws:aws-xray-recorder-sdk-core'  
implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk'  
implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk-v2-instrumentor'  
...  
}
```

Setelah Anda menambahkan dependensi yang benar dan membuat perubahan kode yang diperlukan, aktifkan penelusuran dalam konfigurasi fungsi Anda melalui konsol Lambda atau API

Mengaktifkan penelusuran dengan konsol Lambda

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

Mengaktifkan penelusuran dengan Lambda API

Konfigurasi penelusuran pada fungsi Lambda Anda dengan AWS CLI AWS SDK atau, gunakan operasi berikut API:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \
```

```
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda mempublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

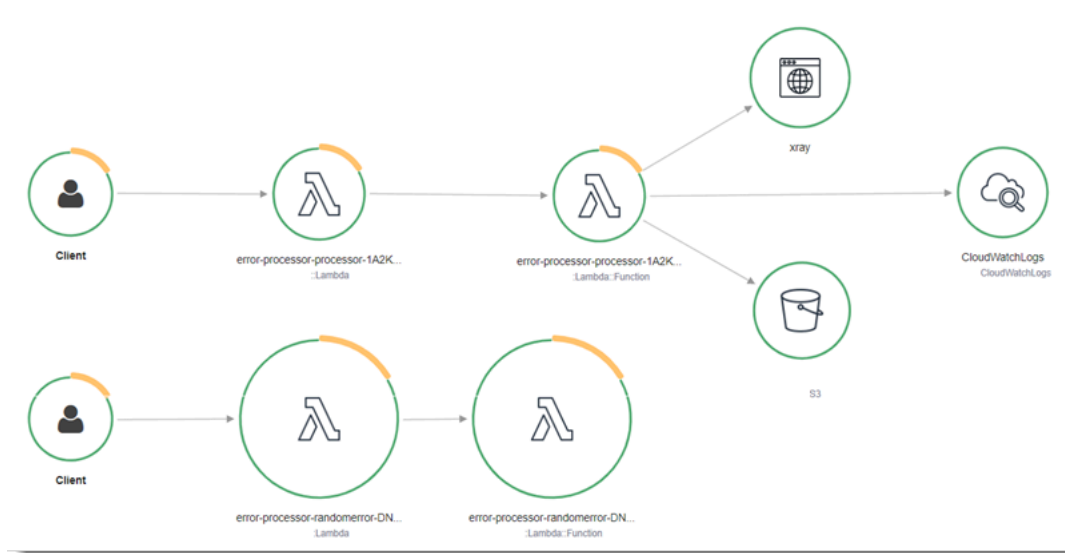
```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Menafsirkan jejak X-Ray

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses

kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch



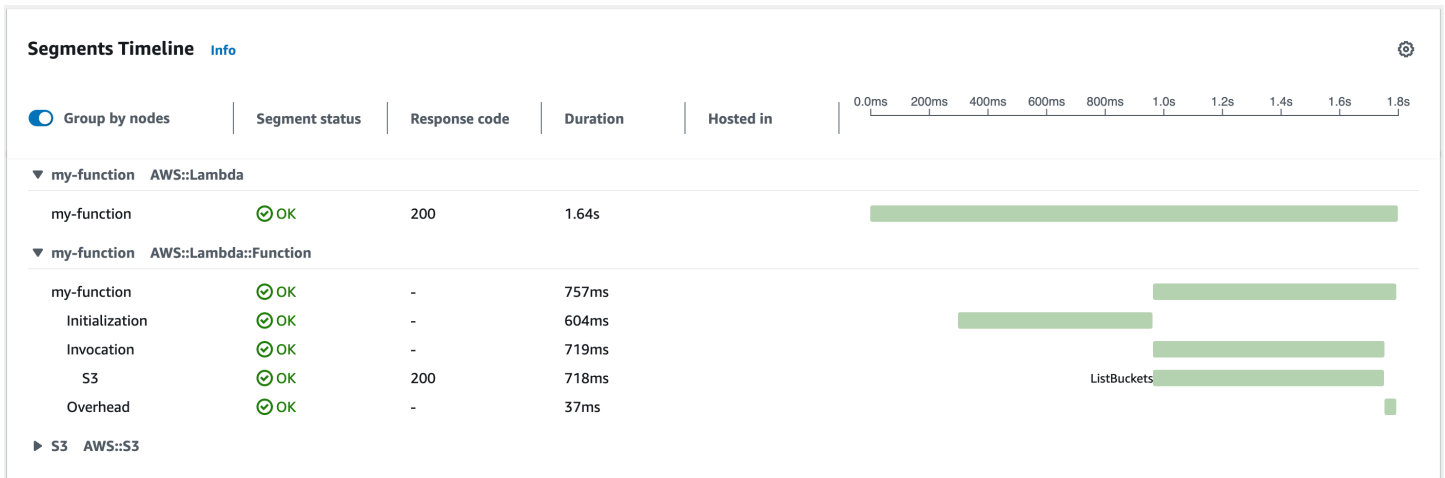
X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal AWS : : Lambda

dan yang lainnya memiliki asal usul. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen jejak yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut. Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat [the section called “Memahami jejak X-Ray”](#)

Note

[Lambda SnapStart](#) fungsi juga termasuk Restore subsegmen. Restore [Subsegmen menunjukkan waktu yang dibutuhkan Lambda untuk memulihkan snapshot, memuat runtime JVM \(\), dan menjalankan kait runtime apa pun. afterRestore](#) Proses memulihkan snapshot dapat mencakup waktu yang dihabiskan untuk aktivitas di luar microVM. Kali ini dilaporkan di Restore subsegmen. Anda tidak dikenakan biaya untuk waktu yang dihabiskan di luar microVM untuk memulihkan snapshot.

Anda juga dapat instrumen HTTP klien, merekam SQL kueri, dan membuat subsegmen kustom dengan anotasi dan metadata. Untuk informasi lebih lanjut, lihat [AWS X-Ray SDK for Java](#) dalam Panduan Pengembang AWS X-Ray .

Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi selengkapnya, lihat [harga AWS X-Ray](#).

Menyimpan dependensi runtime dalam lapisan (X-Ray) SDK

Jika Anda menggunakan X-Ray SDK untuk instrumen AWS SDK klien kode fungsi Anda, paket penyebaran Anda bisa menjadi cukup besar. [Untuk menghindari mengunggah dependensi runtime setiap kali Anda memperbarui kode fungsi, paketkan X-Ray di SDK lapisan Lambda.](#)

Contoh berikut menunjukkan `AWS::Serverless::LayerVersion` sumber daya yang menyimpan AWS SDK for Java dan X-Ray SDK untuk Java.

Example [template.yml](#) – Lapisan dependensi

Resources:

```
function:
  Type: AWS::Serverless::Function
  Properties:
    CodeUri: build/distributions/blank-java.zip
    Tracing: Active
    Layers:
      - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-java-lib
      Description: Dependencies for the blank-java sample app.
      ContentUri: build/blank-java-lib.zip
      CompatibleRuntimes:
        - java21
```

Dengan konfigurasi ini, Anda memperbarui lapisan pustaka hanya jika Anda mengubah dependensi runtime Anda. Karena paket penerapan fungsi hanya berisi kode Anda, ini dapat membantu mengurangi waktu upload.

Membuat lapisan untuk dependensi memerlukan perubahan konfigurasi pembangunan untuk membuat arsip lapisan sebelum deployment. Untuk contoh kerja, lihat aplikasi sampel [java-basic](#) di GitHub

Penelusuran X-Ray dalam aplikasi sampel (SDKX-Ray)

GitHub Repositori untuk panduan ini mencakup contoh aplikasi yang menunjukkan penggunaan penelusuran X-Ray. Setiap contoh aplikasi menyertakan skrip untuk penyebaran dan pembersihan yang mudah, AWS SAM templat, dan sumber daya pendukung.

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon GatewayAPI, Amazon, dan Amazon SQS Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan ketergantungan AWS SDK sebagai.

- [s3-java](#) — Fungsi Java yang memproses peristiwa notifikasi dari Amazon S3 dan menggunakan Java Class Library JCL () untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk memanggil fungsi.

Semua aplikasi sampel memiliki pelacakan aktif yang diaktifkan untuk fungsi Lambda. Misalnya, s3-java aplikasi menampilkan instrumentasi otomatis AWS SDK for Java 2.x klien, manajemen segmen untuk pengujian, subsegmen khusus, dan penggunaan lapisan Lambda untuk menyimpan dependensi runtime.

Contoh aplikasi Java untuk AWS Lambda

GitHub Repositori untuk panduan ini menyediakan contoh aplikasi yang menunjukkan penggunaan Java di AWS Lambda. Setiap contoh aplikasi menyertakan skrip untuk penyebaran dan pembersihan yang mudah, AWS CloudFormation templat, dan sumber daya pendukung.

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon API Gateway, Amazon SQS, dan Amazon Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari pustaka [aws-lambda-java-events](#) (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan AWS SDK sebagai dependensi.
- [s3-java](#) - Fungsi Java yang memproses kejadian pemberitahuan dari Amazon S3 dan menggunakan Java Class Library (JCL) untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk menjalankan fungsi.

Menjalankan kerangka kerja Java populer di Lambda

- [spring-cloud-function-samples](#) — Contoh dari Spring yang menunjukkan cara menggunakan framework Spring [Cloud Function untuk membuat fungsi](#) Lambda. AWS
- [Demo Aplikasi Boot Spring Tanpa Server](#) - Contoh yang menunjukkan cara mengatur aplikasi Spring Boot khas dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime khusus.
- [Demo Aplikasi Micronaut Tanpa Server](#) - Contoh yang menunjukkan cara menggunakan Micronaut dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime kustom. Pelajari lebih lanjut di panduan [Micronaut/Lambda](#).
- [Demo Aplikasi Quarkus Tanpa Server](#) - Contoh yang menunjukkan cara menggunakan Quarkus dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime kustom. [Pelajari lebih lanjut di panduan Quarkus/Lambda dan panduan Quarkus/SnapStart](#)

Jika Anda baru mengenal fungsi Lambda di Java, mulailah dengan contoh. `java-basic` Untuk memulai dengan sumber acara Lambda, lihat contohnya. `java-events` Kedua set contoh ini menunjukkan penggunaan pustaka Java Lambda, variabel lingkungan, AWS SDK, dan SDK. AWS X-Ray Contoh-contoh ini memerlukan pengaturan minimal dan Anda dapat menerapkannya dari baris perintah dalam waktu kurang dari satu menit.

Membangun fungsi Lambda dengan Go

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus. Gunakan [runtime khusus OS \(keluarga runtime\)](#) untuk menerapkan provided fungsi Go ke Lambda.

Topik

- [Dukungan runtime Go](#)
- [Alat dan pustaka](#)
- [Tentukan penanganan fungsi Lambda di Go](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Go](#)
- [Deploy fungsi Go Lambda dengan arsip file .zip](#)
- [Deploy fungsi Lambda Go dengan gambar kontainer](#)
- [Bekerja dengan lapisan untuk fungsi Go Lambda](#)
- [Log dan pantau fungsi Go Lambda](#)
- [Menginstrumentasi kode Go di AWS Lambda](#)

Dukungan runtime Go

[Runtime terkelola Go 1.x untuk Lambda tidak digunakan lagi](#). Jika Anda memiliki fungsi yang menggunakan runtime Go 1.x, Anda harus memigrasikan fungsi Anda ke atau. `provided.al2023` `provided.al2` `provided.al2Runtime` `provided.al2023` dan menawarkan beberapa keunggulan dibanding `go1.x`, termasuk dukungan untuk arsitektur arm64 (prosesor AWS Graviton2), binari yang lebih kecil, dan waktu pemanggilan yang sedikit lebih cepat.

Tidak diperlukan perubahan kode untuk migrasi ini. Satu-satunya perubahan yang diperlukan terkait dengan cara Anda membangun paket penerapan dan runtime mana yang Anda gunakan untuk membuat fungsi Anda. Untuk informasi selengkapnya, lihat [Memigrasi AWS Lambda fungsi dari runtime Go1.x ke runtime khusus di Amazon Linux 2 di Blog Komputasi.AWS](#)

Hanya OS

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------|------------------|-------------------|---------------------|------------------|-----------------------|
| Runtime Khusus OS | provided.a12023 | Amazon Linux 2023 | | | |
| Runtime Khusus OS | provided.a12 | Amazon Linux 2 | | | |

Alat dan pustaka

Lambda menyediakan alat dan pustaka berikut untuk runtime Go:

- [AWS SDK untuk Go](#): resmi AWS SDK untuk bahasa pemrograman Go.
- [github.com/aws/aws-lambda-go/lambda](https://github.com/aws/aws-lambda-go/tree/main/lambda): Implementasi model pemrograman Lambda untuk Go. Paket ini digunakan oleh AWS Lambda untuk memanggil [handler](#) Anda.
- [github.com/aws/aws-lambda-go/lambdacontext](https://github.com/aws/aws-lambda-go/tree/main/lambdacontext): Pembantu untuk mengakses informasi konteks dari objek konteks.
- [github.com/aws/aws-lambda-go/events](https://github.com/aws/aws-lambda-go/tree/main/events): Pustaka ini menyediakan definisi tipe untuk integrasi sumber peristiwa umum.
- [github.com/aws/aws-lambda-go/cmd/build-lambda-zip](https://github.com/aws/aws-lambda-go/tree/main/cmd/build-lambda-zip): Alat ini dapat digunakan untuk membuat arsip file.zip di Windows.

Untuk informasi lebih lanjut, lihat [aws-lambda-go](#) di GitHub.

Lambda menyediakan aplikasi contoh berikut untuk runtime Go:

Sampel aplikasi Lambda di Go

- [go-al2](#) - Fungsi hello world yang mengembalikan alamat IP publik. Aplikasi ini menggunakan runtime `provided.a12` khusus.
- [blank-go](#) — Fungsi Go yang menunjukkan penggunaan pustaka Go Lambda, logging, variabel lingkungan, dan file. AWS SDK Aplikasi ini menggunakan `go1.x` runtime.

Tentukan penanganan fungsi Lambda di Go

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Topik

- [Dasar-dasar Go handler](#)
- [Penamaan](#)
- [Handler fungsi Lambda menggunakan tipe terstruktur](#)
- [Menggunakan status global](#)
- [Praktik terbaik kode untuk fungsi Go Lambda](#)

Dasar-dasar Go handler

Fungsi Lambda yang ditulis di [Go](#) diprogram sebagai Go executable. Dalam kode fungsi Lambda Anda, Anda perlu menyertakan [aws-lambda-gopaket github.com/aws/ /lambda, yang mengimplementasikan model pemrograman Lambda](https://github.com/aws/aws-lambda-go) untuk Go. Selain itu, Anda perlu menerapkan kode fungsi handler dan fungsi `main()`.

Example Fungsi Go Lambda

```
package main

import (
    "context"
    "fmt"
    "github.com/aws/aws-lambda-go/lambda"
)

type MyEvent struct {
    Name string `json:"name"`
}

func HandleRequest(ctx context.Context, event *MyEvent) (*string, error) {
    if event == nil {
        return nil, fmt.Errorf("received nil event")
    }
    message := fmt.Sprintf("Hello %s!", event.Name)
```

```
    return &message, nil
}

func main() {
    lambda.Start(HandleRequest)
}
```

Berikut adalah contoh masukan untuk fungsi ini:

```
{
  "name": "Jane"
}
```

Perhatikan hal berikut:

- `package main`: Di Go, paket yang berisi `func main()` harus selalu diberi nama `main`.
- `import`: Gunakan ini untuk menyertakan pustaka yang diperlukan fungsi Lambda Anda. Dalam instans ini, hal ini termasuk:
 - konteks: [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Go](#).
 - `fmt`: Objek [Format](#) Go yang digunakan untuk memformat nilai fungsi Anda.
 - `github.com/aws/aws-lambda-go/lambda`: Seperti disebutkan sebelumnya, mengimplementasikan model pemrograman Lambda untuk Go.
- `func HandleRequest (ctx context.Context, event *MyEvent) (*string, error)`: Ini adalah tanda tangan handler Lambda Anda. Ini adalah titik masuk untuk fungsi Lambda Anda dan berisi logika yang dijalankan ketika fungsi Anda dipanggil. Selain itu, parameter yang disertakan menunjukkan hal berikut:
 - `ctx context.Context`: Menyediakan informasi runtime untuk invokasi fungsi Lambda Anda. `ctx` adalah variabel yang Anda laporkan untuk memanfaatkan informasi yang tersedia melalui [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Go](#).
 - `event * MyEvent`: Ini adalah parameter bernama `event` yang menunjuk ke `MyEvent`. Ini mewakili input ke fungsi Lambda.
 - `* string, error`: Handler mengembalikan dua nilai. Yang pertama adalah pointer ke string yang berisi hasil dari fungsi Lambda. Yang kedua adalah jenis kesalahan, yaitu `nil` jika tidak ada kesalahan dan berisi informasi [kesalahan](#) standar jika terjadi kesalahan.
 - `return & message, nil`: Mengembalikan dua nilai. Yang pertama adalah pointer ke pesan string, yang merupakan salam dibangun menggunakan `Name` bidang dari peristiwa input. Nilai kedua, `nil`, menunjukkan bahwa fungsi tersebut tidak mengalami kesalahan apa pun.

- `func main()`: Titik masuk yang menjalankan kode fungsi Lambda Anda. Ini wajib diisi.

Dengan menambahkan `lambda.Start(HandleRequest)` di antara `func main(){}` tanda kurung kode, fungsi Lambda Anda akan dijalankan. Standar bahasa Per Go, braket pembuka, `{` harus ditempatkan langsung di akhir tanda tangan `main` fungsi.

Penamaan

menyediakan.al2 dan menyediakan.al2023 runtime

Untuk fungsi Go yang menggunakan `provided.al2` atau `provided.al2023` runtime dalam [paket penyebaran .zip](#), file yang dapat dieksekusi yang berisi kode fungsi Anda harus diberi nama. `bootstrap` Jika Anda menerapkan fungsi dengan `file.zip`, `bootstrap` file harus berada di `root file.zip`. Untuk fungsi Go yang menggunakan `provided.al2` atau `provided.al2023` runtime dalam [gambar kontainer](#), Anda dapat menggunakan nama apa pun untuk file yang dapat dieksekusi.

Anda dapat menggunakan nama apa pun untuk handler. Untuk mereferensikan nilai handler dalam kode Anda, Anda dapat menggunakan variabel `_HANDLER` lingkungan.

runtime go1.x

Untuk fungsi Go yang menggunakan `go1.x` runtime, file yang dapat dieksekusi dan handler dapat berbagi nama apa pun. Misalnya, jika Anda menetapkan nilai handler ke `keHandler`, Lambda akan memanggil fungsi dalam `Handler` file `main()` yang dapat dieksekusi.

Untuk mengubah nama handler fungsi di konsol Lambda, di panel Pengaturan runtime, pilih `Edit`.

Handler fungsi Lambda menggunakan tipe terstruktur

Dalam contoh di atas, tipe input adalah string sederhana. Namun, Anda juga dapat menyampaikan peristiwa terstruktur ke handler fungsi Anda:

```
package main

import (
    "fmt"
    "github.com/aws/aws-lambda-go/lambda"
)
```

```
type MyEvent struct {
    Name string `json:"What is your name?"`
    Age  int    `json:"How old are you?"`
}

type MyResponse struct {
    Message string `json:"Answer"`
}

func HandleLambdaEvent(event *MyEvent) (*MyResponse, error) {
    if event == nil {
        return nil, fmt.Errorf("received nil event")
    }
    return &MyResponse{Message: fmt.Sprintf("%s is %d years old!", event.Name,
    event.Age)}, nil
}

func main() {
    lambda.Start(HandleLambdaEvent)
}
```

Berikut adalah contoh masukan untuk fungsi ini:

```
{
  "What is your name?": "Jim",
  "How old are you?": 33
}
```

Responsnya terlihat seperti ini:

```
{
  "Answer": "Jim is 33 years old!"
}
```

Untuk diekspor, nama bidang dalam struktur peristiwa harus dalam huruf kapital. Untuk informasi selengkapnya tentang penanganan AWS peristiwa dari sumber peristiwa, lihat [aws-lambda-go/events](https://aws.amazon.com/lambda/events/).

Tanda tangan handler yang valid

Anda memiliki beberapa pilihan ketika membangun handler fungsi Lambda di Go, tetapi Anda harus mematuhi aturan berikut:

- Handler harus berupa fungsi.
- Handler dapat mengambil antara 0 dan 2 argumen. Jika ada dua argumen, argumen pertama harus menerapkan `context.Context`.
- Handler dapat mengembalikan antara 0 dan 2 argumen. Jika ada nilai kembali tunggal, nilai harus menerapkan `error`. Jika ada dua nilai kembali, nilai kedua harus menerapkan `error`.

Daftar berikut ini mencantumkan tanda tangan handler yang valid. `TIn` dan `TOut` mewakili tipe yang kompatibel dengan pustaka standar `encoding/json`. Untuk informasi selengkapnya, lihat [func Unmarshal](#) untuk mempelajari cara tipe-tipe ini dideserialisasikan.

- `func ()`
- `func () error`
- `func (TIn) error`
- `func () (TOut, error)`
- `func (context.Context) error`
- `func (context.Context, TIn) error`
- `func (context.Context) (TOut, error)`
- `func (context.Context, TIn) (TOut, error)`

Menggunakan status global

Anda dapat menyatakan dan mengubah variabel global yang terpisah dari kode handler fungsi Lambda Anda. Selain itu, handler Anda dapat melaporkan fungsi `init` yang dilakukan saat handler Anda dimuat. Ini berperilaku sama AWS Lambda seperti yang terjadi pada program Go standar. Satu instans dari fungsi Lambda Anda tidak akan pernah menangani beberapa peristiwa sekaligus.

Example Fungsi Go dengan variabel global

Note

Kode ini menggunakan AWS SDK for Go V2. Untuk informasi selengkapnya, lihat [Memulai dengan AWS SDK for Go V2](#).

```
package main

import (
    "context"
    "github.com/aws/aws-lambda-go/lambda"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
    "log"
)

var invokeCount int
var myObjects []types.Object

func init() {
    // Load the SDK configuration
    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        log.Fatalf("Unable to load SDK config: %v", err)
    }

    // Initialize an S3 client
    svc := s3.NewFromConfig(cfg)

    // Define the bucket name as a variable so we can take its address
    bucketName := "amzn-s3-demo-bucket"
    input := &s3.ListObjectsV2Input{
        Bucket: &bucketName,
    }

    // List objects in the bucket
    result, err := svc.ListObjectsV2(context.TODO(), input)
    if err != nil {
        log.Fatalf("Failed to list objects: %v", err)
    }
}
```

```
    }
    myObjects = result.Contents
}

func LambdaHandler(ctx context.Context) (int, error) {
    invokeCount++
    for i, obj := range myObjects {
        log.Printf("object[%d] size: %d key: %s", i, obj.Size, *obj.Key)
    }
    return invokeCount, nil
}

func main() {
    lambda.Start(LambdaHandler)
}
```

Praktik terbaik kode untuk fungsi Go Lambda

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi.
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan

dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Go

Saat Lambda menjalankan fungsi Anda, ia meneruskan objek konteks ke [handler](#). Objek ini menyediakan metode dan properti dengan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Pustaka konteks Lambda menyediakan variabel, metode, dan sifat global berikut.

Variabel global

- `FunctionName` – Nama fungsi Lambda.
- `FunctionVersion` – [Versi](#) fungsi.
- `MemoryLimitInMB` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `LogGroupName` – Grup log untuk fungsi.
- `LogStreamName` – Aliran log untuk instans fungsi.

Metode konteks

- `Deadline` – Mengembalikan tanggal saat waktu pelaksanaan habis, dalam waktu Unix milidetik.

Properti konteks

- `InvokedFunctionArn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `AwsRequestId` – Pengidentifikasi permintaan invokasi.
- `Identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
- `ClientContext` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.

Mengakses informasi konteks aktif

Fungsi Lambda memiliki akses ke metadata tentang lingkungan mereka dan permintaan invokasi. Ini dapat diakses di [Konteks paket](#). Jika handler Anda mencakup `context.Context` sebagai

parameter, Lambda akan memasukkan informasi tentang fungsi Anda ke dalam Value properti konteks. Perhatikan bahwa Anda perlu mengimpor pustaka `lambdacontext` untuk mengakses konten dari `context.Context` objek.

```
package main

import (
    "context"
    "log"
    "github.com/aws/aws-lambda-go/lambda"
    "github.com/aws/aws-lambda-go/lambdacontext"
)

func CognitoHandler(ctx context.Context) {
    lc, _ := lambdacontext.FromContext(ctx)
    log.Print(lc.Identity.CognitoIdentityPoolID)
}

func main() {
    lambda.Start(CognitoHandler)
}
```

Dalam contoh di atas, `lc` adalah variabel yang digunakan untuk mengkonsumsi informasi bahwa objek konteks ditangkap dan `log.Print(lc.Identity.CognitoIdentityPoolID)` mencetak informasi itu, dalam hal ini, `CognitoIdentityPool ID`.

Contoh berikut memperkenalkan cara menggunakan objek konteks untuk memantau berapa lama waktu yang dibutuhkan fungsi Lambda untuk menyelesaikannya. Ini memungkinkan Anda untuk menganalisis ekspektasi kinerja dan menyesuaikan kode fungsi Anda, jika diperlukan.

```
package main

import (
    "context"
    "log"
    "time"
    "github.com/aws/aws-lambda-go/lambda"
)

func LongRunningHandler(ctx context.Context) (string, error) {

    deadline, _ := ctx.Deadline()
```

```
deadline = deadline.Add(-100 * time.Millisecond)
timeoutChannel := time.After(time.Until(deadline))

for {

    select {

        case <- timeoutChannel:
            return "Finished before timing out.", nil

        default:
            log.Print("hello!")
            time.Sleep(50 * time.Millisecond)
    }
}

}

func main() {
    lambda.Start(LongRunningHandler)
}
```

Deploy fungsi Go Lambda dengan arsip file .zip

Kode AWS Lambda fungsi Anda terdiri dari skrip atau program yang dikompilasi dan dependensinya. Gunakan paket deployment untuk men-deploy fungsi kode Anda ke Lambda. Lambda mendukung dua tipe paket deployment: gambar kontainer dan arsip file .zip.

Halaman ini menjelaskan cara membuat file.zip sebagai paket penerapan Anda untuk runtime Go, dan kemudian menggunakan file.zip untuk menyebarkan kode fungsi Anda AWS Lambda menggunakan, () AWS Management Console, dan AWS Command Line Interface (AWS CLI). AWS Serverless Application Model AWS SAM

Perhatikan bahwa Lambda menggunakan izin POSIX file, jadi Anda mungkin perlu [mengatur izin untuk folder paket penyebaran](#) sebelum membuat arsip file.zip.

Bagian-bagian

- [Membuat file .zip pada macOS dan Linux](#)
- [Membuat file .zip pada Windows](#)
- [Membuat dan memperbarui fungsi Go Lambda menggunakan file.zip](#)

Membuat file .zip pada macOS dan Linux

Langkah-langkah berikut menunjukkan cara mengkompilasi executable Anda menggunakan go build perintah dan membuat paket penyebaran file.zip untuk Lambda. Sebelum mengkompilasi kode Anda, pastikan Anda telah menginstal paket [lambda](#) dari GitHub Modul ini menyediakan implementasi antarmuka runtime, yang mengelola interaksi antara Lambda dan kode fungsi Anda. Untuk mengunduh pustaka ini, jalankan perintah berikut.

```
go get github.com/aws/aws-lambda-go/lambda
```

Jika fungsi Anda menggunakan AWS SDK for Go, unduh set SDK modul standar, bersama dengan API klien AWS layanan apa pun yang diperlukan oleh aplikasi Anda. Untuk mempelajari cara menginstal SDK for Go, lihat [Memulai dengan AWS SDK for Go V2](#).

Menggunakan keluarga runtime yang disediakan

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus. Gunakan [runtime khusus OS \(keluarga runtime\)](#) untuk menerapkan provided fungsi Go ke Lambda.

Untuk membuat paket penyebaran.zip (macOS/Linux)

1. Dalam direktori proyek yang berisi `main.go` file aplikasi Anda, kompilasi executable Anda. Perhatikan hal berikut:
 - Executable harus diberi nama. `bootstrap` Untuk informasi selengkapnya, lihat [Penamaan](#).
 - Tetapkan [arsitektur set instruksi](#) target Anda. Runtime khusus OS mendukung `arm64` dan `x86_64`.
 - Anda dapat menggunakan `lambda.norpc` tag opsional untuk mengecualikan komponen Remote Procedure Call (RPC) dari pustaka [lambda](#). RPCKomponen hanya diperlukan jika Anda menggunakan runtime Go 1.x yang tidak digunakan lagi. Tidak termasuk RPC mengurangi ukuran paket penyebaran.

Untuk arsitektur `arm64`:

```
GOOS=linux GOARCH=arm64 go build -tags lambda.norpc -o bootstrap main.go
```

Untuk arsitektur `x86_64`:

```
GOOS=linux GOARCH=amd64 go build -tags lambda.norpc -o bootstrap main.go
```

2. (Opsional) Anda mungkin perlu mengompilasi paket dengan `CGO_ENABLED=0` yang diatur di Linux:

```
GOOS=linux GOARCH=arm64 CGO_ENABLED=0 go build -o bootstrap -tags lambda.norpc main.go
```

Perintah ini membuat paket biner stabil untuk versi pustaka C standar (`libc`), yang mungkin berbeda di Lambda dan perangkat lainnya.

3. Buat paket deployment dengan mengemas executable dalam file `.zip`.

```
zip myFunction.zip bootstrap
```

Note

`bootstrapFile` harus berada di root file.zip.

4. Buat fungsi . Perhatikan hal berikut:

- Biner harus diberi nama `bootstrap`, tetapi nama handler bisa apa saja. Untuk informasi selengkapnya, lihat [Penamaan](#).
- `--architectures` Opsi ini hanya diperlukan jika Anda menggunakan `arm64`. Nilai defaultnya adalah `x86_64`.
- Untuk `--role`, tentukan Amazon Resource Name (ARN) dari [peran eksekusi](#).

```
aws lambda create-function --function-name myFunction \  
--runtime provided.al2023 --handler bootstrap \  
--architectures arm64 \  
--role arn:aws:iam::111122223333:role/lambda-ex \  
--zip-file fileb://myFunction.zip
```

Membuat file .zip pada Windows

Langkah-langkah berikut menunjukkan cara mengunduh [build-lambda-zip](#) alat untuk Windows dari GitHub, mengkompilasi executable Anda, dan membuat paket deployment .zip.

Note

Jika Anda belum melakukannya, Anda harus menginstal [git](#), lalu tambahkan executable `git` ke variabel lingkungan Windows `%PATH%` Anda.

Sebelum mengkompilasi kode Anda, pastikan Anda telah menginstal pustaka [lambda](#) dari GitHub. Untuk mengunduh pustaka ini, jalankan perintah berikut.

```
go get github.com/aws/aws-lambda-go/lambda
```

Jika fungsi Anda menggunakan AWS SDK for Go, unduh set SDK modul standar, bersama dengan API klien AWS layanan apa pun yang diperlukan oleh aplikasi Anda. Untuk mempelajari cara menginstal SDK for Go, lihat [Memulai dengan AWS SDK for Go V2](#).

Menggunakan keluarga runtime yang disediakan

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus. Gunakan [runtime khusus OS \(keluarga runtime\)](#) untuk menerapkan provided fungsi Go ke Lambda.

Untuk membuat paket penyebaran.zip (Windows)

1. Unduh build-lambda-zipalat dari GitHub.

```
go install github.com/aws/aws-lambda-go/cmd/build-lambda-zip@latest
```

2. Gunakan alat dari GOPATH Anda untuk membuat file .zip. Jika Anda memiliki penginstalan default Go, alat ini biasanya di %USERPROFILE%\Go\bin. Jika tidak, arahkan ke tempat Anda menginstal runtime Go dan lakukan salah satu hal berikut:

cmd.exe

Di cmd.exe, jalankan salah satu dari berikut ini, tergantung pada [arsitektur set instruksi](#) target Anda. Runtime khusus OS mendukung arm64 dan x86_64.

Anda dapat menggunakan `lambda.norpc` tag opsional untuk mengecualikan komponen Remote Procedure Call (RPC) dari pustaka [lambda](#). RPCKomponen hanya diperlukan jika Anda menggunakan runtime Go 1.x yang tidak digunakan lagi. Tidak termasuk RPC mengurangi ukuran paket penyebaran.

Example — Untuk arsitektur x86_64

```
set GOOS=linux
set GOARCH=amd64
set CGO_ENABLED=0
go build -tags lambda.norpc -o bootstrap main.go
%USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

Example — Untuk arsitektur arm64

```
set GOOS=linux
set GOARCH=arm64
set CGO_ENABLED=0
go build -tags lambda.norpc -o bootstrap main.go
```

```
%USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

PowerShell

Dalam PowerShell, jalankan salah satu dari berikut ini, tergantung pada [arsitektur set instruksi](#) target Anda. Runtime khusus OS mendukung arm64 dan x86_64.

Anda dapat menggunakan `lambda.norpc` tag opsional untuk mengecualikan komponen Remote Procedure Call (RPC) dari pustaka [lambda](#). RPCKomponen hanya diperlukan jika Anda menggunakan runtime Go 1.x yang tidak digunakan lagi. Tidak termasuk RPC mengurangi ukuran paket penyebaran.

Untuk arsitektur x86_64:

```
$env:GOOS = "linux"
$env:GOARCH = "amd64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

Untuk arsitektur arm64:

```
$env:GOOS = "linux"
$env:GOARCH = "arm64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

3. Buat fungsi . Perhatikan hal berikut:

- Biner harus diberi nama `bootstrap`, tetapi nama handler bisa apa saja. Untuk informasi selengkapnya, lihat [Penamaan](#).
- `--architectures`Opsi ini hanya diperlukan jika Anda menggunakan arm64. Nilai defaultnya adalah `x86_64`.
- Untuk `--role`, tentukan Amazon Resource Name (ARN) dari [peran eksekusi](#).

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--architectures arm64 \
```



```
--role arn:aws:iam::111122223333:role/Lambda-ex \  
--zip-file fileb://myFunction.zip
```

Membuat dan memperbarui fungsi Go Lambda menggunakan file.zip

Setelah Anda membuat paket.zip deployment, Anda dapat menggunakannya untuk membuat fungsi Lambda baru atau memperbarui yang sudah ada. Anda dapat menerapkan paket.zip Anda menggunakan konsol Lambda, the, AWS Command Line Interface dan Lambda. API Anda juga dapat membuat dan memperbarui fungsi Lambda menggunakan AWS Serverless Application Model (AWS SAM) dan. AWS CloudFormation

Ukuran maksimum untuk paket.zip deployment untuk Lambda adalah 250 MB (unzip). Perhatikan bahwa batas ini berlaku untuk ukuran gabungan semua file yang Anda unggah, termasuk lapisan Lambda apa pun.

Runtime Lambda membutuhkan izin untuk membaca file dalam paket deployment Anda. Dalam notasi oktal izin Linux, Lambda membutuhkan 644 izin untuk file yang tidak dapat dieksekusi (rw-r - r--) dan 755 izin () untuk direktori dan file yang dapat dieksekusi. rwxr-xr-x

Di Linux dan macOS, gunakan `chmod` perintah untuk mengubah izin file pada file dan direktori dalam paket penyebaran Anda. Misalnya, untuk memberikan file yang dapat dieksekusi izin yang benar, jalankan perintah berikut.

```
chmod 755 <filepath>
```

Untuk mengubah izin file di Windows, lihat [Mengatur, Melihat, Mengubah, atau Menghapus Izin pada Objek](#) dalam dokumentasi Microsoft Windows.

Membuat dan memperbarui fungsi dengan file.zip menggunakan konsol

Untuk membuat fungsi baru, Anda harus terlebih dahulu membuat fungsi di konsol, lalu mengunggah arsip.zip Anda. Untuk memperbarui fungsi yang ada, buka halaman untuk fungsi Anda, lalu ikuti prosedur yang sama untuk menambahkan file.zip Anda yang diperbarui.

Jika file.zip Anda kurang dari 50MB, Anda dapat membuat atau memperbarui fungsi dengan mengunggah file langsung dari mesin lokal Anda. Untuk file.zip yang lebih besar dari 50MB, Anda harus mengunggah paket Anda ke bucket Amazon S3 terlebih dahulu. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS Management Console, lihat [Memulai](#)

[Amazon S3](#). Untuk mengunggah file menggunakan AWS CLI, lihat [Memindahkan objek](#) di Panduan AWS CLI Pengguna.

 Note

Anda tidak dapat mengonversi fungsi gambar kontainer yang ada untuk menggunakan arsip.zip. Anda harus membuat fungsi baru.

Untuk membuat fungsi baru (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih Buat Fungsi.
2. Pilih Tulis dari awal.
3. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan nama untuk fungsi Anda.
 - b. Untuk Runtime, pilih `provided.al2023`.
4. (Opsional) Di bagian Izin, luaskan Ubah peran eksekusi default. Anda dapat membuat peran Eksekusi baru atau menggunakan yang sudah ada.
5. Pilih Buat fungsi. Lambda menciptakan fungsi dasar 'Hello world' menggunakan runtime yang Anda pilih.

Untuk mengunggah arsip.zip dari mesin lokal Anda (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih file.zip.
5. Untuk mengunggah file.zip, lakukan hal berikut:
 - a. Pilih Unggah, lalu pilih file.zip Anda di pemilih file.
 - b. Pilih Buka.
 - c. Pilih Simpan.

Untuk mengunggah arsip.zip dari bucket Amazon S3 (konsol)

1. Di [halaman Fungsi](#) konsol Lambda, pilih fungsi yang ingin Anda unggah file.zip baru.
2. Pilih tab Kode.
3. Di panel Sumber kode, pilih Unggah dari.
4. Pilih lokasi Amazon S3.
5. Rekatkan tautan Amazon S3 URL dari file.zip Anda dan pilih Simpan.

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CLI

Anda dapat menggunakan [AWS CLI](#) untuk membuat fungsi baru atau memperbarui yang sudah ada menggunakan file.zip. Gunakan [create-function](#) dan [update-function-code](#) perintah untuk menyebarkan paket.zip Anda. Jika file.zip Anda lebih kecil dari 50MB, Anda dapat mengunggah paket.zip dari lokasi file di mesin build lokal Anda. Untuk file yang lebih besar, Anda harus mengunggah paket.zip Anda dari bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Note

Jika Anda mengunggah file.zip dari bucket Amazon S3 menggunakan AWS CLI bucket, bucket harus berada di lokasi Wilayah AWS yang sama dengan fungsi Anda.

Untuk membuat fungsi baru menggunakan file.zip dengan AWS CLI, Anda harus menentukan yang berikut:

- Nama fungsi Anda (`--function-name`)
- Runtime (`--runtime` fungsi Anda)
- Amazon Resource Name (ARN) dari [peran eksekusi](#) fungsi Anda (`--role`)
- Nama metode handler dalam kode fungsi Anda (`--handler`)

Anda juga harus menentukan lokasi file.zip Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda create-function --function-name myFunction \
```

```
--runtime provided.al2023 --handler bootstrap \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi seperti `--code` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `S3ObjectVersion` parameter untuk objek berversi.

```
aws lambda create-function --function-name myFunction \  
--runtime provided.al2023 --handler bootstrap \  
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \  
--code S3Bucket=amzn-s3-demo-  
bucket,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Untuk memperbarui fungsi yang ada menggunakan CLI, Anda menentukan nama fungsi Anda menggunakan `--function-name` parameter. Anda juga harus menentukan lokasi file.zip yang ingin Anda gunakan untuk memperbarui kode fungsi Anda. Jika file.zip Anda terletak di folder di mesin build lokal Anda, gunakan `--zip-file` opsi untuk menentukan jalur file, seperti yang ditunjukkan pada perintah contoh berikut.

```
aws lambda update-function-code --function-name myFunction \  
--zip-file fileb://myFunction.zip
```

Untuk menentukan lokasi file.zip di bucket Amazon S3, gunakan opsi `--s3-key` dan seperti `--s3-bucket` yang ditunjukkan pada perintah contoh berikut. Anda hanya perlu menggunakan `--s3-object-version` parameter untuk objek berversi.

```
aws lambda update-function-code --function-name myFunction \  
--s3-bucket amzn-s3-demo-bucket --s3-key myFileName.zip --s3-object-version myObject  
Version
```

Membuat dan memperbarui fungsi dengan file.zip menggunakan Lambda API

Untuk membuat dan memperbarui fungsi menggunakan arsip file.zip, gunakan API operasi berikut:

- [CreateFunction](#)
- [UpdateFunctionCode](#)

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS SAM

The AWS Serverless Application Model (AWS SAM) adalah toolkit yang membantu merampingkan proses membangun dan menjalankan aplikasi tanpa server. AWS Anda menentukan sumber daya untuk aplikasi Anda dalam JSON template YAML atau dan menggunakan antarmuka baris AWS SAM perintah (AWS SAM CLI) untuk membangun, mengemas, dan menyebarkan aplikasi Anda. Saat Anda membuat fungsi Lambda dari AWS SAM template, AWS SAM secara otomatis membuat paket penerapan .zip atau gambar kontainer dengan kode fungsi Anda dan dependensi apa pun yang Anda tentukan. Untuk mempelajari lebih lanjut cara menggunakan AWS SAM untuk membangun dan menerapkan fungsi Lambda, [lihat Memulai](#) di Panduan AWS SAMAWS Serverless Application Model Pengembang.

Anda juga dapat menggunakan AWS SAM untuk membuat fungsi Lambda menggunakan arsip file.zip yang ada. Untuk membuat fungsi Lambda menggunakan AWS SAM, Anda dapat menyimpan file.zip di bucket Amazon S3 atau di folder lokal di mesin build Anda. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS SAM template Anda, `AWS::Serverless::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- diatur ke `Zip`
- `CodeUri`- diatur ke kode fungsi Amazon S3URI, jalur ke folder lokal, atau objek [FunctionCode](#)
- `Runtime`- Setel ke runtime yang Anda pilih

Dengan AWS SAM, jika file.zip Anda lebih besar dari 50MB, Anda tidak perlu mengunggahnya ke bucket Amazon S3 terlebih dahulu. AWS SAM dapat mengunggah paket.zip hingga ukuran maksimum yang diizinkan 250MB (unzip) dari lokasi di mesin build lokal Anda.

Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS SAM, lihat [AWS: :Serverless: :Function](#) dalam Panduan Pengembang.AWS SAM

Contoh: Menggunakan AWS SAM untuk membangun fungsi Go dengan `provided.al2023`

1. Buat AWS SAM template dengan properti berikut:

- `BuildMethod`: Menentukan compiler untuk aplikasi Anda. Gunakan `go1.x`.
- `Runtime`: Gunakan `provided.al2023`.

- `CodeUri`: Masukkan jalur ke kode Anda.
- `Arsitektur`: Gunakan `[arm64]` untuk arsitektur arm64. Untuk arsitektur set instruksi x86_64, gunakan `[amd64]` atau hapus properti. `Architectures`

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Metadata:
      BuildMethod: go1.x
    Properties:
      CodeUri: hello-world/ # folder where your main program resides
      Handler: bootstrap
      Runtime: provided.al2023
      Architectures: [arm64]
```

2. Gunakan perintah [sam build](#) untuk mengkompilasi executable.

```
sam build
```

3. Gunakan perintah [sam deploy](#) untuk menyebarkan fungsi ke Lambda.

```
sam deploy --guided
```

Membuat dan memperbarui fungsi dengan file.zip menggunakan AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk membuat fungsi Lambda menggunakan arsip file.zip. Untuk membuat fungsi Lambda dari file.zip, Anda harus terlebih dahulu mengunggah file Anda ke bucket Amazon S3. Untuk petunjuk tentang cara mengunggah file ke bucket Amazon S3 menggunakan AWS CLI, lihat [Memindahkan objek](#) di AWS CLI Panduan Pengguna.

Dalam AWS CloudFormation template Anda, `AWS::Lambda::Function` sumber daya menentukan fungsi Lambda Anda. Dalam sumber daya ini, atur properti berikut untuk membuat fungsi menggunakan arsip file.zip:

- `PackageType`- Setel ke `Zip`

- Code- Masukkan nama bucket Amazon S3 dan nama file.zip di dan bidang S3Bucket S3Key
- Runtime- Setel ke runtime yang Anda pilih

File.zip yang AWS CloudFormation menghasilkan tidak boleh melebihi 4MB. Untuk mempelajari selengkapnya tentang penerapan fungsi menggunakan file.zip di AWS CloudFormation, lihat [AWS: :Lambda: :Function](#) di Panduan Pengguna.AWS CloudFormation

Deploy fungsi Lambda Go dengan gambar kontainer

Ada dua cara untuk membangun image kontainer untuk fungsi Go Lambda:

- [Menggunakan gambar AWS dasar khusus OS](#)

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus.

Gunakan gambar [dasar khusus OS untuk membuat gambar](#) Go untuk Lambda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan `aws-lambda-go/lambda` paket dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda.

Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan `aws-lambda-go/lambda` paket dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi penampung Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

AWS gambar dasar untuk menerapkan fungsi Go

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus. Gunakan [gambar dasar khusus OS](#) untuk menerapkan fungsi Go ke Lambda.

Hanya OS

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|-------------------|------------------|-------------------|---------------------|------------------|-----------------------|
| Runtime Khusus OS | provided.a12023 | Amazon Linux 2023 | | | |
| Runtime Khusus OS | provided.a12 | Amazon Linux 2 | | | |

Galeri Publik Registri Kontainer Elastis Amazon: gallery.ecr.aws/lambda/provided

Klien antarmuka Go runtime

Paket `aws-lambda-go/lambda` termasuk implementasi dari antarmuka runtime. Untuk contoh cara menggunakan `aws-lambda-go/lambda` dalam gambar Anda, lihat [Menggunakan gambar AWS dasar khusus OS](#) atau [Menggunakan gambar AWS non-dasar](#).

Menggunakan gambar AWS dasar khusus OS

Go diimplementasikan secara berbeda dari runtime terkelola lainnya. Karena Go mengkompilasi secara native ke biner yang dapat dieksekusi, itu tidak memerlukan runtime bahasa khusus. Gunakan image [dasar khusus OS untuk membuat gambar](#) kontainer untuk fungsi Go.

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|--------|-------------------|-------------------|---|-------------|
| a12023 | Runtime Khusus OS | Amazon Linux 2023 | Dockerfile untuk Runtime khusus OS aktif GitHub | |
| a12 | Runtime Khusus OS | Amazon Linux 2 | Dockerfile untuk Runtime khusus OS aktif GitHub | |

Untuk informasi selengkapnya tentang gambar dasar ini, lihat [disediakan](#) di galeri ECR publik Amazon.

Anda harus menyertakan paket [aws-lambda-go/lambda](https://github.com/aws/aws-lambda-go) dengan handler Go Anda. Paket ini mengimplementasikan model pemrograman untuk Go, termasuk antarmuka runtime.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Go
- [Docker](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Membuat gambar dari gambar dasar.al2023 yang disediakan

Untuk membangun dan menerapkan fungsi Go dengan image **provided.al2023** dasar

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir hello
cd hello
```

2. Inisialisasi modul Go baru.

```
go mod init example.com/hello-world
```

3. Tambahkan pustaka lambda sebagai dependensi modul baru Anda.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Buat file bernama `main.go` dan kemudian buka di editor teks. Ini adalah kode untuk fungsi Lambda. Anda dapat menggunakan kode contoh berikut untuk pengujian, atau menggantinya dengan kode Anda sendiri.

```
package main

import (
    "context"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)
```

```
func handler(ctx context.Context, event events.APIGatewayProxyRequest)
(events.APIGatewayProxyResponse, error) {
    response := events.APIGatewayProxyResponse{
        StatusCode: 200,
        Body:        "\"Hello from Lambda!\"",
    }
    return response, nil
}

func main() {
    lambda.Start(handler)
}
```

5. Gunakan editor teks untuk membuat Dockerfile di direktori proyek Anda.

- Contoh berikut Dockerfile menggunakan build [multi-tahap](#). Ini memungkinkan Anda untuk menggunakan gambar dasar yang berbeda di setiap langkah. Anda dapat menggunakan satu gambar, seperti [image dasar Go](#), untuk mengkompilasi kode Anda dan membangun biner yang dapat dieksekusi. Anda kemudian dapat menggunakan gambar yang berbeda, seperti `provided.al2023`, dalam FROM pernyataan akhir untuk menentukan gambar yang Anda terapkan ke Lambda. Proses build dipisahkan dari image penerapan akhir, sehingga gambar akhir hanya berisi file yang diperlukan untuk menjalankan aplikasi.
- Anda dapat menggunakan `lambda.norpc` tag opsional untuk mengecualikan komponen Remote Procedure Call (RPC) dari pustaka [lambda](#). RPCKomponen hanya diperlukan jika Anda menggunakan runtime Go 1.x yang tidak digunakan lagi. Tidak termasuk RPC mengurangi ukuran paket penyebaran.
- [Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada USER instruksi yang diberikan.

Example — Multi-tahap membangun Dockerfile

Note

Pastikan bahwa versi Go yang Anda tentukan di Dockerfile Anda (misalnya, `golang:1.20`) adalah versi Go yang sama dengan yang Anda gunakan untuk membuat aplikasi Anda.

```
FROM golang:1.20 as build
WORKDIR /helloworld
# Copy dependencies list
COPY go.mod go.sum ./
# Build with optional lambda.norpc tag
COPY main.go .
RUN go build -tags lambda.norpc -o main main.go
# Copy artifacts to a clean image
FROM public.ecr.aws/lambda/provided:al2023
COPY --from=build /helloworld/main ./main
ENTRYPOINT [ "./main" ]
```

6. Buat image Docker dengan perintah `docker build`. Contoh berikut memberi nama gambar `docker-image` dan memberinya test `tag`.

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar Anda secara lokal. Emulator antarmuka runtime disertakan dalam gambar `provided.al2023` dasar.

Untuk menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Mulai gambar Docker dengan perintah `docker run`. Perhatikan hal berikut:
 - `docker-image` adalah nama gambar dan test tag.
 - `./main` adalah ENTRYPOINT dari Dockerfile Anda.

```
docker run -d -p 9000:8080 \  
--entrypoint /usr/local/bin/aws-lambda-rie \  
docker-image:test ./main
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

2. Dari jendela terminal baru, posting peristiwa ke titik akhir berikut menggunakan perintah `curl`:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Beberapa fungsi mungkin memerlukan JSON muatan. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d \  
'{"payload":"hello world!"}'
```

3. Dapatkan ID kontainer.

```
docker ps
```

4. Gunakan perintah [docker kill](#) untuk menghentikan kontainer. Dalam perintah ini, ganti `3766c4ab331c` dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti `111122223333` dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
```

```

        "encryptionType": "AES256"
    }
}
}

```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoryURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repository URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhir URI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Untuk melihat output dari fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```


Menggunakan gambar AWS non-dasar

Anda dapat membuat gambar kontainer untuk Go dari gambar AWS non-dasar. Contoh Dockerfile dalam langkah-langkah berikut menggunakan gambar dasar [Alpine](#).

Anda harus menyertakan paket [aws-lambda-go/lambda](#) dengan handler Go Anda. Paket ini mengimplementasikan model pemrograman untuk Go, termasuk antarmuka runtime.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- Go
- [Docker](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Membuat gambar dari gambar dasar alternatif

Untuk membangun dan menerapkan fungsi Go dengan image dasar Alpine

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir hello
cd hello
```

2. Inisialisasi modul Go baru.

```
go mod init example.com/hello-world
```

3. Tambahkan pustaka lambda sebagai dependensi modul baru Anda.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Buat file bernama `main.go` dan kemudian buka di editor teks. Ini adalah kode untuk fungsi Lambda. Anda dapat menggunakan kode contoh berikut untuk pengujian, atau menggantinya dengan kode Anda sendiri.

```
package main

import (
```

```

"context"
"github.com/aws/aws-lambda-go/events"
"github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, event events.APIGatewayProxyRequest)
(events.APIGatewayProxyResponse, error) {
    response := events.APIGatewayProxyResponse{
        StatusCode: 200,
        Body:        "\"Hello from Lambda!\"",
    }
    return response, nil
}

func main() {
    lambda.Start(handler)
}

```

- Gunakan editor teks untuk membuat Dockerfile di direktori proyek Anda. Contoh berikut Dockerfile menggunakan gambar dasar [Alpine](#). [Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada `USER` instruksi yang diberikan.

Example Dockerfile

Note

Pastikan bahwa versi Go yang Anda tentukan di Dockerfile Anda (misalnya, `golang:1.20`) adalah versi Go yang sama dengan yang Anda gunakan untuk membuat aplikasi Anda.

```

FROM golang:1.20.2-alpine3.16 as build
WORKDIR /helloworld
# Copy dependencies list
COPY go.mod go.sum ./
# Build
COPY main.go .
RUN go build -o main main.go

```

```
# Copy artifacts to a clean image
FROM alpine:3.16
COPY --from=build /helloworld/main /main
ENTRYPOINT [ "/main" ]
```

6. Buat image Docker dengan perintah [docker build](#). Contoh berikut memberi nama gambar `docker-image` dan memberinya test [tag](#).

```
docker build --platform linux/amd64 -t docker-image:test .
```

Note

Perintah menentukan `--platform linux/amd64` opsi untuk memastikan bahwa container Anda kompatibel dengan lingkungan eksekusi Lambda terlepas dari arsitektur mesin build Anda. Jika Anda berniat untuk membuat fungsi Lambda menggunakan arsitektur set ARM64 instruksi, pastikan untuk mengubah perintah untuk menggunakan `--platform linux/arm64` opsi sebagai gantinya.

(Opsional) Uji gambar secara lokal

Gunakan [emulator antarmuka runtime](#) untuk menguji gambar secara lokal. Anda dapat [membangun emulator ke dalam gambar Anda](#) atau menggunakan prosedur berikut untuk menginstalnya di mesin lokal Anda.

Untuk menginstal dan menjalankan emulator antarmuka runtime di mesin lokal Anda

1. Dari direktori proyek Anda, jalankan perintah berikut untuk mengunduh emulator antarmuka runtime (arsitektur x86-64) dari GitHub dan menginstalnya di mesin lokal Anda.

Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \
  curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-
runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
  chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

Untuk menginstal emulator arm64, ganti GitHub repositori URL di perintah sebelumnya dengan yang berikut:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Untuk menginstal emulator arm64, ganti `$downloadLink` dengan yang berikut ini:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
```

2. Mulai gambar Docker dengan perintah `docker run`. Perhatikan hal berikut:

- `docker-image` adalah nama gambar dan test tag.
- `/main` adalah ENTRYPOINT dari Dockerfile Anda.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
    /main
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
```

```
/main
```

Perintah ini menjalankan gambar sebagai wadah dan membuat titik akhir lokal di `localhost:9000/2015-03-31/functions/function/invocations`.

Note

Jika Anda membuat image Docker untuk arsitektur set ARM64 instruksi, pastikan untuk menggunakan `--platform linux/arm64` opsi alih-alih. `--platform linux/amd64`

3. Posting acara ke titik akhir lokal.

Linux/macOS

Di Linux dan macOS, jalankan perintah berikut: `curl`

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{"payload":"hello world!"}'
```

PowerShell

Dalam PowerShell, jalankan `Invoke-WebRequest` perintah berikut:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Perintah ini memanggil fungsi dengan peristiwa kosong dan mengembalikan respons. Jika Anda menggunakan kode fungsi Anda sendiri daripada kode fungsi sampel, Anda mungkin ingin memanggil fungsi dengan JSON payload. Contoh:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
"application/json"
```

4. Dapatkan ID kontainer.

```
docker ps
```

5. Gunakan perintah [docker kill](#) untuk menghentikan kontainer. Dalam perintah ini, ganti 3766c4ab331c dengan ID kontainer dari langkah sebelumnya.

```
docker kill 3766c4ab331c
```

Menyebarkan gambar

Untuk mengunggah gambar ke Amazon ECR dan membuat fungsi Lambda

1. Jalankan [get-login-password](#) perintah untuk mengautentikasi Docker CLI ke registri Amazon ECR Anda.
 - Tetapkan `--region` nilai ke Wilayah AWS tempat Anda ingin membuat ECR repositori Amazon.
 - Ganti 111122223333 dengan Akun AWS ID Anda.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Buat repositori di Amazon ECR menggunakan perintah [create-repository](#).

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

Note

ECR Repositori Amazon harus sama Wilayah AWS dengan fungsi Lambda.

Jika berhasil, Anda melihat respons seperti ini:

```
{
  "repository": {
    "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
    "registryId": "111122223333",
    "repositoryName": "hello-world",
    "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
    "createdAt": "2023-03-09T10:39:01+00:00",
    "imageTagMutability": "MUTABLE",
    "imageScanningConfiguration": {
      "scanOnPush": true
    },
    "encryptionConfiguration": {
      "encryptionType": "AES256"
    }
  }
}
```

3. Salin `repositoryUri` dari output pada langkah sebelumnya.
4. Jalankan perintah [tag docker](#) untuk menandai gambar lokal Anda ke ECR repositori Amazon Anda sebagai versi terbaru. Dalam perintah ini:
 - `docker-image:test` adalah nama dan [tag](#) gambar Docker Anda. Ini adalah nama gambar dan tag yang Anda tentukan dalam `docker build` perintah.
 - Ganti `<ECRrepositoryUri>` dengan `repositoryUri` yang Anda salin. Pastikan untuk menyertakan `:latest` di akhir URI.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Contoh:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world:latest
```

5. Jalankan perintah [docker push](#) untuk menyebarkan gambar lokal Anda ke repositori Amazon ECR. Pastikan untuk menyertakan `:latest` di akhir repositoriURI.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. [Buat peran eksekusi](#) untuk fungsi tersebut, jika Anda belum memilikinya. Anda memerlukan Amazon Resource Name (ARN) peran di langkah berikutnya.
7. Buat fungsi Lambda. Untuk `ImageUri`, tentukan repositori URI dari sebelumnya. Pastikan untuk menyertakan `:latest` di akhirURI.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

Note

Anda dapat membuat fungsi menggunakan gambar di AWS akun yang berbeda, selama gambar berada di Wilayah yang sama dengan fungsi Lambda. Untuk informasi selengkapnya, lihat [Izin ECR lintas akun Amazon](#).

8. Memanggil fungsi.

```
aws lambda invoke --function-name hello-world response.json
```

Anda akan melihat tanggapan seperti ini:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Untuk melihat output dari fungsi, periksa `response.json` file.

Untuk memperbarui kode fungsi, Anda harus membangun gambar lagi, mengunggah gambar baru ke ECR repositori Amazon, dan kemudian menggunakan [update-function-code](#) perintah untuk menyebarkan gambar ke fungsi Lambda.

Lambda menyelesaikan tag gambar ke intisari gambar tertentu. Ini berarti bahwa jika Anda mengarahkan tag gambar yang digunakan untuk menyebarkan fungsi ke gambar baru di Amazon ECR, Lambda tidak secara otomatis memperbarui fungsi untuk menggunakan gambar baru.

Untuk menyebarkan gambar baru ke fungsi Lambda yang sama, Anda harus menggunakan [update-function-code](#) perintah, meskipun tag gambar di ECR Amazon tetap sama. Dalam contoh berikut, `--publish` opsi membuat versi baru dari fungsi menggunakan gambar kontainer yang diperbarui.

```
aws lambda update-function-code \  
  --function-name hello-world \  
  --image-uri 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \  
  --publish
```

Bekerja dengan lapisan untuk fungsi Go Lambda

[Lapisan Lambda](#) adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi. Membuat layer melibatkan tiga langkah umum:

1. Package konten layer Anda. Ini berarti membuat arsip file.zip yang berisi dependensi yang ingin Anda gunakan dalam fungsi Anda.
2. Buat layer di Lambda.
3. Tambahkan layer ke fungsi Anda.

Kami tidak menyarankan menggunakan lapisan untuk mengelola dependensi untuk fungsi Lambda yang ditulis dalam Go. Ini karena fungsi Lambda di Go dikompilasi menjadi satu executable, yang Anda berikan ke Lambda saat Anda menerapkan fungsi Anda. Executable ini berisi kode fungsi dikompilasi Anda, bersama dengan semua dependensinya. Menggunakan lapisan tidak hanya mempersulit proses ini, tetapi juga menyebabkan peningkatan waktu mulai dingin karena fungsi Anda perlu memuat rakitan ekstra secara manual ke dalam memori selama fase init.

Untuk menggunakan dependensi eksternal dengan penangan Go Anda, sertakan dependensi tersebut secara langsung dalam paket penerapan Anda. Dengan demikian, Anda menyederhanakan proses penerapan dan juga memanfaatkan pengoptimalan kompiler Go bawaan. Untuk contoh cara mengimpor dan menggunakan dependensi seperti AWS SDK untuk Go di fungsi Anda, lihat [the section called “Handler”](#).

Log dan pantau fungsi Go Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda dan mengirim log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap invokasi ke pengaliran log, dan menyampaikan log serta output lain dari kode fungsi Anda. Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Halaman ini menjelaskan cara menghasilkan keluaran log dari kode fungsi Lambda Anda, dan mengakses log menggunakan AWS Command Line Interface, konsol Lambda, atau konsol CloudWatch

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)

Membuat fungsi yang mengembalikan log

Untuk menghasilkan log dari kode fungsi, Anda dapat menggunakan metode di [paket fmt](#), atau pustaka pencatatan apa pun yang menulis ke `stdout` atau `stderr`. Contoh berikut menggunakan [paket log](#).

Example [main.go](#) – Pencatatan

```
func handleRequest(ctx context.Context, event events.SQSEvent) (string, error) {
    // event
    eventJson, _ := json.MarshalIndent(event, "", " ")
    log.Printf("EVENT: %s", eventJson)
    // environment variables
    log.Printf("REGION: %s", os.Getenv("AWS_REGION"))
    log.Println("ALL ENV VARS:")
    for _, element := range os.Environ() {
        log.Println(element)
    }
}
```

Example format log

```
START RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Version: $LATEST
2020/03/27 03:40:05 EVENT: {
  "Records": [
    {
      "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
      "md5ofBody": "7b27xmplb47ff90a553787216d55d91d",
      "md5ofMessageAttributes": "",
      "attributes": {
        "ApproximateFirstReceiveTimestamp": "1523232000001",
        "ApproximateReceiveCount": "1",
        "SenderId": "123456789012",
        "SentTimestamp": "1523232000000"
      }
    },
    ...
  ]
}
2020/03/27 03:40:05 AWS_LAMBDA_LOG_STREAM_NAME=2020/03/27/
[$LATEST]569cxmplc3c34c7489e6a97ad08b4419
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_NAME=blank-go-function-9DV3XMPL6XBC
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_VERSION=$LATEST
2020/03/27 03:40:05 AWS_EXECUTION_ENV=AWS_Lambda_go1.x
END RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71
REPORT RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Duration: 38.66 ms Billed
Duration: 39 ms Memory Size: 128 MB Max Memory Used: 54 MB Init Duration: 203.69 ms
XRAY TraceId: 1-5e7d7595-212fxmpl9ee07c4884191322 SegmentId: 42ffxmpl0645f474 Sampled:
true
```

Runtime Go akan mencatat baris START, END, dan REPORT untuk setiap invokasi. Baris laporan memberikan detail berikut.

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.

- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, kami sarankan untuk menginstrumentasi fungsi Anda dengan `AWS X-Ray`. `X-Ray` mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBULQgUmVxdWVzdElk0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzVlNGZiMjEgVmVyc2lvc21vb... ",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0""",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15 detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "statusCode": 200,
  "executedVersion": "$LATEST"
}
{
  "events": [
    {
      "timestamp": 1559763003171,
      "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
      "ingestionTime": 1559763003309
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n$LATEST\n",
\r ...",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
      "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
      "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\n",

```



```
        "ingestionTime": 1559763018353
    }
  ],
  "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
  "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Menginstrumentasi kode Go di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari dua SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK for Go](#) — Sebuah SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray](#). SDKs

Bagian-bagian

- [Menggunakan ADOT untuk instrumen fungsi Go Anda](#)
- [Menggunakan X-Ray SDK untuk instrumen fungsi Go Anda](#)
- [Mengaktifkan penelusuran dengan konsol Lambda](#)
- [Mengaktifkan penelusuran dengan Lambda API](#)
- [Mengaktifkan penelusuran dengan AWS CloudFormation](#)

- [Menafsirkan jejak X-Ray](#)

Menggunakan ADOT untuk instrumen fungsi Go Anda

ADOT menyediakan [lapisan](#) Lambda yang dikelola sepenuhnya yang mengemas semua yang Anda butuhkan untuk mengumpulkan data telemetri menggunakan file. OTEL SDK Dengan menggunakan lapisan ini, Anda dapat menginstruksikan fungsi Lambda Anda tanpa harus memodifikasi kode fungsi apa pun. Anda juga dapat mengonfigurasi lapisan Anda untuk melakukan inisialisasi kustom. OTEL Untuk informasi selengkapnya, lihat [Konfigurasi khusus untuk ADOT Kolektor di Lambda](#) dalam dokumentasi. ADOT

Untuk runtime Go, Anda dapat menambahkan layer Lambda AWS terkelola ADOT untuk Go untuk menginstruksikan fungsi Anda secara otomatis. Untuk petunjuk rinci tentang cara menambahkan layer ini, lihat [AWS Distro untuk OpenTelemetry Lambda Support](#) for Go ADOT di dokumentasi.

Menggunakan X-Ray SDK untuk instrumen fungsi Go Anda

Untuk merekam detail tentang panggilan yang dilakukan oleh fungsi Lambda Anda ke sumber daya lain di aplikasi Anda, Anda juga dapat menggunakan AWS X-Ray SDK for Go. Untuk mendapatkan SDK, unduh SDK dari [GitHub repositorinya](#) dengan: `go get`

```
go get github.com/aws/aws-xray-sdk-go
```

Untuk instrumen AWS SDK klien, berikan klien ke `xray.AWS()` metode. Anda kemudian dapat melacak panggilan dengan menggunakan `WithContext` versi metode.

```
svc := s3.New(session.New())
xray.AWS(svc.Client)
...
svc.ListBucketsWithContext(ctx aws.Context, input *ListBucketsInput)
```

Setelah Anda menambahkan dependensi yang benar dan membuat perubahan kode yang diperlukan, aktifkan penelusuran dalam konfigurasi fungsi Anda melalui konsol Lambda atau API

Mengaktifkan penelusuran dengan konsol Lambda

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

Mengaktifkan penelusuran dengan Lambda API

Konfigurasikan penelusuran pada fungsi Lambda Anda dengan AWS CLI AWS SDK atau, gunakan operasi berikut API:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \  
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

Resources:

```
function:
  Type: AWS::Lambda::Function
  Properties:
    TracingConfig:
      Mode: Active
    ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
    ...
```

Menafsirkan jejak X-Ray

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch

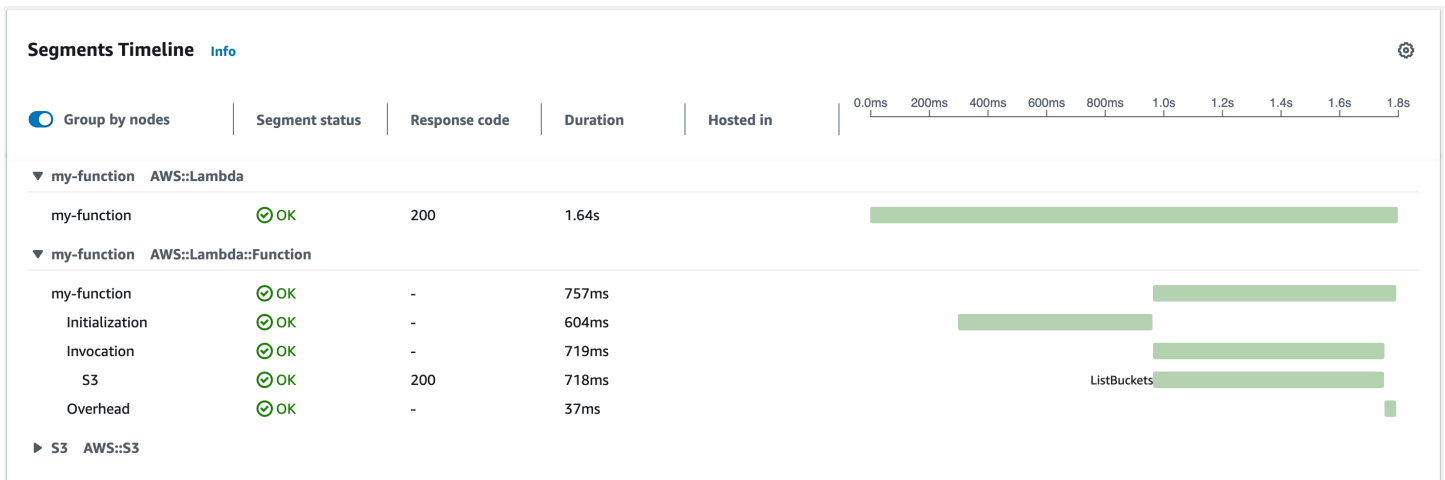


X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal usul. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat [the section called “Memahami jejak X-Ray”](#)

Anda juga dapat HTTP menginstrumentasikan klien, merekam SQL kueri, dan membuat subsegmen khusus dengan anotasi dan metadata. Untuk informasi selengkapnya, lihat [AWS X-Ray SDK untuk Go](#) di Panduan AWS X-Ray Pengembang.

Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi lebih lanjut, lihat [Harga AWS X-Ray](#).

Membangun fungsi Lambda dengan C#

Anda dapat menjalankan aplikasi.NET Anda di Lambda menggunakan runtime .NET 6 atau .NET 8 yang dikelola, runtime kustom, atau gambar kontainer. Setelah kode aplikasi dikompilasi, Anda dapat menerapkannya ke Lambda baik sebagai file.zip atau gambar kontainer. Lambda menyediakan runtime berikut untuk bahasa.NET:

.NET

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|--------|------------------|-------------------|---------------------|-------------------|-----------------------|
| .NET 8 | dotnet8 | Amazon Linux 2023 | | | |
| .NET 6 | dotnet6 | Amazon Linux 2 | 20 Des 2024 | Februari 28, 2025 | 31 Mar 2025 |

Menyiapkan lingkungan pengembangan .NET Anda

Untuk mengembangkan dan membangun fungsi Lambda Anda, Anda dapat menggunakan salah satu lingkungan pengembangan terintegrasi (IDE) .NET yang tersedia secara umum, termasuk Microsoft Visual Studio, Visual Studio Code, dan JetBrains Rider. Untuk menyederhanakan pengalaman pengembangan Anda, AWS sediakan satu set template proyek.NET, serta antarmuka baris perintah `Amazon.Lambda.Tools` perintah (CLI).

Jalankan perintah.NET CLI berikut untuk menginstal template proyek dan alat baris perintah ini.

Menginstal template proyek.NET

Untuk menginstal template proyek (.NET 8):

```
dotnet new install Amazon.Lambda.Templates
```

Untuk menginstal template proyek (.NET 6):

```
dotnet new --install Amazon.Lambda.Templates
```

Note

Jika Anda menggunakan runtime Lambda terkelola .NET 6, kami sarankan Anda meningkatkan untuk menggunakan .NET 8. Untuk mempelajari lebih lanjut, lihat [Mengelola upgrade AWS Lambda runtime](#) dan [Memperkenalkan runtime .NET 8 untuk AWS Lambda](#) di Compute Blog.AWS

Menginstal dan memperbarui alat CLI

Jalankan perintah berikut untuk menginstal, memperbarui, dan menghapus Amazon.Lambda.Tools CLI.

Untuk menginstal alat baris perintah:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Untuk memperbarui alat baris perintah:

```
dotnet tool update -g Amazon.Lambda.Tools
```

Untuk menghapus alat baris perintah:

```
dotnet tool uninstall -g Amazon.Lambda.Tools
```

Tentukan penanganan fungsi Lambda di C

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Ketika fungsi Anda dipanggil dan Lambda menjalankan metode handler fungsi Anda, ia meneruskan dua argumen ke fungsi Anda. Argumen pertama adalah event objek. Ketika yang lain AWS layanan memanggil fungsi Anda, event objek berisi data tentang peristiwa yang menyebabkan fungsi Anda dipanggil. Misalnya, event objek dari API Gateway berisi informasi tentang jalur, HTTP metode, dan HTTP header. Struktur acara yang tepat bervariasi sesuai dengan AWS layanan pemanggilan fungsi Anda. Lihat [Mengintegrasikan layanan lain](#) untuk informasi selengkapnya tentang format acara untuk layanan individual.

Lambda juga meneruskan context objek ke fungsi Anda. Objek ini berisi informasi tentang pemanggilan, fungsi, dan lingkungan eksekusi. Untuk informasi selengkapnya, lihat [the section called “Konteks”](#).

Format asli untuk semua peristiwa Lambda adalah aliran byte yang mewakili peristiwa yang diformat. JSON Kecuali parameter input dan output fungsi Anda bertipe `System.IO.Stream`, Anda harus membuat serialisasi. Tentukan serializer yang ingin Anda gunakan dengan mengatur atribut `LambdaSerializer` assembly. Untuk informasi selengkapnya, lihat [the section called “Serialisasi dalam fungsi Lambda”](#).

Topik

- [.NETmodel eksekusi untuk Lambda](#)
- [Penanganan perpustakaan kelas](#)
- [Penangan perakitan yang dapat dieksekusi](#)
- [Serialisasi dalam fungsi Lambda](#)
- [Sederhanakan kode fungsi dengan kerangka kerja Anotasi Lambda](#)
- [Pembatasan handler fungsi Lambda](#)
- [Praktik terbaik kode untuk fungsi C# Lambda](#)

.NETmodel eksekusi untuk Lambda

Ada dua model eksekusi yang berbeda untuk menjalankan fungsi Lambda di .NET: pendekatan perpustakaan kelas dan pendekatan perakitan yang dapat dieksekusi.

Dalam pendekatan pustaka kelas, Anda memberikan Lambda string yang menunjukkan `AssemblyName`, `ClassName`, dan `Method` fungsi yang akan dipanggil. Untuk informasi selengkapnya tentang format string ini, lihat [the section called “Penangan perpustakaan kelas”](#). Selama fase inisialisasi fungsi, kelas fungsi Anda diinisialisasi, dan kode apa pun dalam konstruktor dijalankan.

Dalam pendekatan perakitan yang dapat dieksekusi, Anda menggunakan fitur pernyataan [tingkat atas](#) C # 9. Pendekatan ini menghasilkan perakitan yang dapat dieksekusi yang dijalankan Lambda setiap kali menerima perintah pemanggilan untuk fungsi Anda. Anda hanya memberi Lambda nama rakitan yang dapat dieksekusi untuk dijalankan.

Bagian berikut memberikan contoh kode fungsi untuk dua pendekatan ini.

Penangan perpustakaan kelas

Kode fungsi Lambda berikut menunjukkan contoh metode handler (`FunctionHandler`) untuk fungsi Lambda yang menggunakan pendekatan pustaka kelas. Dalam contoh fungsi ini, Lambda menerima peristiwa API dari Gateway yang memanggil fungsi. Fungsi membaca catatan dari database dan mengembalikan catatan sebagai bagian dari respons API Gateway.

```
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);
```

```
return new APIGatewayProxyResponse
{
    StatusCode = (int)HttpStatusCode.OK,
    Body = JsonSerializer.Serialize(databaseRecord)
};
}
```

Saat Anda membuat fungsi Lambda, Anda perlu memberikan Lambda informasi tentang handler fungsi Anda dalam bentuk string handler. Ini memberi tahu Lambda metode mana dalam kode Anda untuk dijalankan ketika fungsi Anda dipanggil. Dalam C #, format string handler saat menggunakan pendekatan perpustakaan kelas adalah sebagai berikut:

ASSEMBLY::TYPE::METHOD, dimana:

- ASSEMBLY adalah nama dari .NET file perakitan untuk aplikasi Anda. Jika Anda menggunakan Amazon.Lambda.Tools CLI untuk membangun aplikasi Anda dan Anda tidak mengatur nama assembly menggunakan AssemblyName properti di file.csproj, maka ASSEMBLY hanya nama file.csproj Anda.
- TYPE adalah nama lengkap dari tipe handler, yang terdiri dari Namespace dan ClassName
- METHOD adalah nama metode fungsi handler dalam kode Anda.

Untuk kode contoh yang ditampilkan, jika perakitan diberi nama GetProductHandler, maka string handler akan

menjadi `GetProductHandler::GetProductHandler.Function::FunctionHandler`.

Penangan perakitan yang dapat dieksekusi

Dalam contoh berikut, fungsi Lambda didefinisikan sebagai perakitan yang dapat dieksekusi. Metode handler dalam kode ini Handler dinamai. Saat menggunakan rakitan yang dapat dieksekusi, runtime Lambda harus di-bootstrap. Untuk melakukan ini, Anda menggunakan `LambdaBootstrapBuilder.Create` metode ini. Metode ini mengambil sebagai input metode yang digunakan fungsi Anda sebagai handler dan serializer Lambda untuk digunakan.

Untuk informasi selengkapnya tentang menggunakan pernyataan tingkat atas, lihat [Memperkenalkan.NET6 runtime untuk AWS Lambda](#) di blog AWS komputasi.

```
namespace GetProductHandler;
```

```
IDatabaseRepository repo = new DatabaseRepository();

await LambdaBootstrapBuilder.Create<APIGatewayProxyRequest>(Handler, new
    DefaultLambdaJsonSerializer())
    .Build()
    .RunAsync();

async Task<APIGatewayProxyResponse> Handler(APIGatewayProxyRequest apigProxyEvent,
    ILambdaContext context)
{
    var id = input.PathParameters["id"];

    var databaseRecord = await this.repo.GetById(id);

    return new APIGatewayProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = JsonSerializer.Serialize(databaseRecord)
    };
};
```

Saat menggunakan rakitan yang dapat dieksekusi, string handler yang memberi tahu Lambda cara menjalankan kode Anda adalah nama perakitan. Dalam contoh ini, itu akan menjadi `GetProductHandler`.

Serialisasi dalam fungsi Lambda

Jika fungsi Lambda Anda menggunakan jenis input atau output selain `Stream` objek, Anda harus menambahkan pustaka serialisasi ke aplikasi Anda. Anda dapat menerapkan serialisasi baik menggunakan serialisasi berbasis refleksi standar yang disediakan oleh `System.Text.Json` dan `Newtonsoft.Json`, atau dengan menggunakan serialisasi yang [dihasilkan sumber](#).

Menggunakan serialisasi yang dihasilkan sumber

Serialisasi yang dihasilkan sumber adalah fitur dari .NET versi 6 dan yang lebih baru yang memungkinkan kode serialisasi dihasilkan pada waktu kompilasi. Ini menghilangkan kebutuhan untuk refleksi dan dapat meningkatkan kinerja fungsi Anda. Untuk menggunakan serialisasi yang dihasilkan sumber dalam fungsi Anda, lakukan hal berikut:

- Buat kelas parsial baru yang mewarisi dari `JsonSerializerContext`, menambahkan `JsonSerializable` atribut untuk semua jenis yang memerlukan serialisasi atau deserialisasi.

- Konfigurasi LambdaSerializer untuk menggunakan aSourceGeneratorLambdaJsonSerializer<T>.
- Perbarui serialisasi manual atau deserialisasi apa pun dalam kode aplikasi Anda untuk menggunakan kelas yang baru dibuat.

Sebuah fungsi contoh menggunakan sumber yang dihasilkan serialisasi ditampilkan dalam kode berikut.

```
[assembly:
  LambdaSerializer(typeof(SourceGeneratorLambdaJsonSerializer<CustomSerializer>))]

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord,
CustomSerializer.Default.Product)
        };
    }
}

[JsonSerializable(typeof(APIGatewayProxyRequest))]
[JsonSerializable(typeof(APIGatewayProxyResponse))]
[JsonSerializable(typeof(Product))]
public partial class CustomSerializer : JsonSerializerContext
{
```

```
}
```

Note

Jika Anda ingin menggunakan native sebelumnya compilation (AOT) dengan Lambda, Anda harus menggunakan serialisasi yang dihasilkan sumber.

Menggunakan serialisasi berbasis refleksi

AWS menyediakan pustaka bawaan untuk memungkinkan Anda menambahkan serialisasi ke aplikasi dengan cepat. Anda mengonfigurasi ini menggunakan `Amazon.Lambda.Serialization.Json` NuGet paket `Amazon.Lambda.Serialization.SystemTextJson` atau. Di belakang layar, `Amazon.Lambda.Serialization.SystemTextJson` gunakan `System.Text.Json` untuk melakukan tugas serialisasi, dan `Amazon.Lambda.Serialization.Json` menggunakan `Newtonsoft.Json` paket.

Anda juga dapat membuat pustaka serialisasi Anda sendiri dengan mengimplementasikan `ILambdaSerializer` antarmuka, yang tersedia sebagai bagian dari `Amazon.Lambda.Core` perpustakaan. Antarmuka ini mendefinisikan dua metode:

- `T Deserialize<T>(Stream requestStream);`

Anda menerapkan metode ini untuk deserialisasi payload permintaan dari objek ke objek yang diteruskan `Invoke API` ke penanganan fungsi Lambda Anda.

- `T Serialize<T>(T response, Stream responseStream);`

Anda menerapkan metode ini untuk membuat serial hasil yang dikembalikan dari penanganan fungsi Lambda Anda ke dalam payload respons yang dikembalikan operasi. `Invoke API`

Sederhanakan kode fungsi dengan kerangka kerja Anotasi Lambda

Anotasi Lambda adalah kerangka kerja untuk .NET6 dan .NET8 yang menyederhanakan penulisan fungsi Lambda menggunakan C#. Dengan kerangka kerja Anotasi, Anda dapat mengganti banyak kode dalam fungsi Lambda yang ditulis menggunakan model pemrograman biasa. Kode yang ditulis menggunakan kerangka kerja menggunakan ekspresi sederhana yang memungkinkan Anda untuk fokus pada logika bisnis Anda.

Contoh kode berikut menunjukkan bagaimana menggunakan kerangka anotasi dapat menyederhanakan penulisan fungsi Lambda. Contoh pertama menunjukkan kode yang ditulis menggunakan model program Lambda biasa, dan yang kedua menunjukkan yang setara menggunakan kerangka kerja Anotasi.

```
public APIGatewayHttpApiV2ProxyResponse LambdaMathAdd(APIGatewayHttpApiV2ProxyRequest
    request, ILambdaContext context)
{
    if (!request.PathParameters.TryGetValue("x", out var xs))
    {
        return new APIGatewayHttpApiV2ProxyResponse
        {
            StatusCode = (int)HttpStatusCode.BadRequest
        };
    }
    if (!request.PathParameters.TryGetValue("y", out var ys))
    {
        return new APIGatewayHttpApiV2ProxyResponse
        {
            StatusCode = (int)HttpStatusCode.BadRequest
        };
    }
    var x = int.Parse(xs);
    var y = int.Parse(ys);
    return new APIGatewayHttpApiV2ProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = (x + y).ToString(),
        Headers = new Dictionary<string, string> { { "Content-Type", "text/plain" } }
    };
}
```

```
[LambdaFunction]
[HttpApi(LambdaHttpMethod.Get, "/add/{x}/{y}")]
public int Add(int x, int y)
{
    return x + y;
}
```

Untuk contoh lain bagaimana menggunakan Anotasi Lambda dapat menyederhanakan kode Anda, lihat [contoh aplikasi lintas layanan](#) ini di repositori. `awsdocs/aws-doc-sdk-examples` GitHub Folder `PamApiAnnotations` menggunakan Anotasi Lambda di file utama. `function.cs` Sebagai

perbandingan, PamApi folder memiliki file setara yang ditulis menggunakan model pemrograman Lambda biasa.

Kerangka kerja Anotasi menggunakan [generator sumber](#) untuk menghasilkan kode yang diterjemahkan dari model pemrograman Lambda ke kode yang terlihat pada contoh kedua.

Untuk informasi selengkapnya tentang cara menggunakan Anotasi Lambda untuk .NET, lihat sumber daya berikut:

- [aws/aws-lambda-dotnet](#) GitHub Repositori.
- [Memperkenalkan .NET Anotasi Lambda Framework \(Pratinjau\)](#) di Blog Alat AWS Pengembang.
- [Amazon.Lambda.Annotations](#) NuGet Paketnya.

Injeksi ketergantungan dengan kerangka kerja Anotasi Lambda

Anda juga dapat menggunakan kerangka kerja Anotasi Lambda untuk menambahkan injeksi ketergantungan ke fungsi Lambda Anda menggunakan sintaks yang Anda kenal. Saat Anda menambahkan `[LambdaStartup]` atribut ke `Startup.cs` file, kerangka kerja Anotasi Lambda akan menghasilkan kode yang diperlukan pada waktu kompilasi.

```
[LambdaStartup]
public class Startup
{
    public void ConfigureServices(IServiceCollection services)
    {
        services.AddSingleton<IDatabaseRepository, DatabaseRepository>();
    }
}
```

Fungsi Lambda Anda dapat menyuntikkan layanan menggunakan injeksi konstruktor atau dengan menyuntikkan ke dalam metode individual menggunakan atribut. `[FromServices]`

```
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))

namespace GetProductHandler;

public class Function
{
```

```
private readonly IDatabaseRepository _repo;

public Function(IDatabaseRepository repo)
{
    this._repo = repo;
}

[LambdaFunction]
[HttpApi(LambdaHttpMethod.Get, "/product/{id}")]
public async Task<Product> FunctionHandler([FromServices] IDatabaseRepository repository, string id)
{
    return await this._repo.GetById(id);
}
}
```

Pembatasan handler fungsi Lambda

Perhatikan bahwa ada beberapa pembatasan pada tanda tangan handler.

- Mungkin tidak `unsafe` dan menggunakan tipe pointer dalam tanda tangan handler, meskipun Anda dapat menggunakan `unsafe` konteks di dalam metode handler dan dependensinya. Untuk informasi selengkapnya, lihat [unsafe \(Referensi C#\) di situs](#) web Microsoft Docs.
- Ini mungkin tidak melewati sejumlah variabel parameter menggunakan `params` kata kunci, atau digunakan `ArgIterator` sebagai input atau parameter pengembalian, yang digunakan untuk mendukung sejumlah variabel parameter.
- Handler mungkin bukan metode generik, misalnya, `IList<T>Sort<T>(IList<T>input)`.
- Handler asinkron dengan tanda tangan `async void` tidak didukung.

Praktik terbaik kode untuk fungsi C# Lambda

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji.
- Kontrol dependensi dalam paket penerapan fungsi Anda. Lingkungan AWS Lambda eksekusi berisi sejumlah pustaka. Untuk mengaktifkan serangkaian fitur dan pembaruan keamanan terbaru, Lambda akan memperbarui pustaka ini secara berkala. Pembaruan ini dapat memberikan

perubahan kecil pada perilaku fungsi Lambda Anda. Untuk memiliki kendali penuh atas dependensi yang digunakan fungsi Anda, kemas semua dependensi Anda dengan paket deployment Anda.

- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).
- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi. Untuk fungsi yang ditulis dalam .NET, hindari mengunggah seluruh AWS SDK perpustakaan sebagai bagian dari paket penerapan Anda. Sebagai gantinya, secara selektif bergantung pada modul yang mengambil komponen yang SDK Anda butuhkan (misalnya DynamoDB, modul Amazon SDK S3, dan pustaka inti Lambda).
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.

- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs APIPembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [APIreferensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Bangun dan terapkan fungsi C# Lambda dengan arsip file.zip

Paket penerapan .NET (arsip file.zip) berisi rakitan yang dikompilasi fungsi Anda bersama dengan semua dependensi perakitannya. Paket ini juga berisi file `proj.deps.json`. Ini memberi sinyal ke runtime .NET semua dependensi fungsi Anda dan `proj.runtimeconfig.json` file, yang digunakan untuk mengonfigurasi runtime.

Untuk menerapkan fungsi Lambda individual, Anda dapat menggunakan CLI Global `Amazon.Lambda.Tools .NET Lambda`. Menggunakan `dotnet lambda deploy-function` perintah secara otomatis membuat paket penyebaran.zip dan menyebarkannya ke Lambda. Namun, kami menyarankan Anda menggunakan kerangka kerja seperti AWS Serverless Application Model (AWS SAM) atau AWS Cloud Development Kit (AWS CDK) untuk menyebarkan aplikasi.NET Anda. **AWS**

Aplikasi tanpa server biasanya terdiri dari kombinasi fungsi Lambda dan AWS layanan kerja sama lain yang dikelola untuk melakukan tugas bisnis tertentu. AWS SAM dan AWS CDK menyederhanakan membangun dan menerapkan fungsi Lambda dengan yang lain dalam skala besar. AWS layanan [Spesifikasi AWS SAM template](#) menyediakan sintaks sederhana dan bersih untuk menggambarkan fungsi Lambda, API, izin, konfigurasi, dan sumber daya AWS lain yang membentuk aplikasi tanpa server Anda. Dengan [AWS CDK](#) Anda mendefinisikan infrastruktur cloud sebagai kode untuk membantu Anda membangun aplikasi yang andal, terukur, dan hemat biaya di cloud menggunakan bahasa pemrograman modern dan kerangka kerja seperti .NET. Baik AWS CDK dan AWS SAM menggunakan CLI Global `.NET Lambda` untuk mengemas fungsi Anda.

Meskipun dimungkinkan untuk menggunakan [lapisan Lambda](#) dengan fungsi di C # dengan [menggunakan CLI CLI.NET Core, kami sarankan](#) untuk tidak melakukannya. Fungsi dalam C# yang menggunakan lapisan secara manual memuat rakitan bersama ke dalam memori selama [Fase inisialisasi](#), yang dapat meningkatkan waktu mulai dingin. Sebagai gantinya, sertakan semua kode bersama pada waktu kompilasi untuk memanfaatkan pengoptimalan bawaan compiler.NET.

Anda dapat menemukan petunjuk untuk membangun dan menerapkan fungsi.NET Lambda menggunakan AWS SAM, CLI Global Lambda, dan `.NET Lambda Global` di AWS CDK bagian berikut.

Topik

- [Menggunakan CLI Global .NET Lambda](#)
- [Menyebarkan fungsi C# Lambda menggunakan AWS SAM](#)
- [Menyebarkan fungsi C# Lambda menggunakan AWS CDK](#)

- [Menyebarkan aplikasi ASP.NET](#)

Menggunakan CLI Global .NET Lambda

.NET CLI dan ekstensi .NET Lambda Global Tools (`Amazon.Lambda.Tools`) menawarkan cara lintas platform untuk membuat aplikasi Lambda berbasis .NET, mengemasnya, dan menyebarkannya ke Lambda. Di bagian ini, Anda mempelajari cara membuat proyek Lambda.NET baru menggunakan templat .NET CLI dan Amazon Lambda, dan mengemas dan menerapkannya menggunakan `Amazon.Lambda.Tools`

Topik

- [Prasyarat](#)
- [Membuat proyek .NET menggunakan .NET CLI](#)
- [Menerapkan proyek .NET menggunakan .NET CLI](#)
- [Menggunakan layer Lambda dengan .NET CLI](#)

Prasyarat

.NET 8 SDK

Jika Anda belum melakukannya, instal SDK [.NET 8](#) dan Runtime.

AWS Templat proyek `Amazon.Lambda.Templates` .NET

Untuk menghasilkan kode fungsi Lambda Anda, gunakan paket [Amazon.Lambda.Templates](#) NuGet Untuk menginstal paket template ini, jalankan perintah berikut:

```
dotnet new install Amazon.Lambda.Templates
```

AWS `Amazon.Lambda.Tools` .NET Alat CLI Global

Untuk membuat fungsi Lambda Anda, Anda menggunakan [Amazon.Lambda.Tools](#) ekstensi .NET [Global Tools](#). Untuk menginstal `Amazon.Lambda.Tools`, jalankan perintah berikut:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Untuk informasi selengkapnya tentang `Amazon.Lambda.Tools` ekstensi .NET CLI, lihat [AWS Ekstensi untuk repositori .NET CLI](#) di GitHub

Membuat proyek .NET menggunakan .NET CLI

Di .NET CLI, Anda menggunakan `dotnet new` perintah untuk membuat proyek .NET dari baris perintah. Lambda menawarkan template tambahan menggunakan paket.

[Amazon.Lambda.Templates](#) NuGet

Setelah menginstal paket ini, jalankan perintah berikut untuk melihat daftar template yang tersedia.

```
dotnet new list
```

Untuk memeriksa rincian tentang templat , gunakan opsi `help`. Misalnya, untuk melihat detail tentang `lambda.EmptyFunction` template, jalankan perintah berikut.

```
dotnet new lambda.EmptyFunction --help
```

Untuk membuat template dasar untuk fungsi.NET Lambda, gunakan template.

`lambda.EmptyFunction` Ini menciptakan fungsi sederhana yang mengambil string sebagai input dan mengubahnya menjadi huruf besar menggunakan `ToUpper` metode. Template ini mendukung opsi berikut:

- `--name` – Nama fungsi.
- `--region`— AWS Wilayah untuk membuat fungsi di.
- `--profile`— Nama profil di file AWS SDK for .NET kredensial Anda. Untuk mempelajari selengkapnya tentang profil kredensial.NET, lihat [Mengonfigurasi AWS kredensial](#) di SDK for AWS .NET Developer Guide.

Dalam contoh ini, kita membuat fungsi kosong baru bernama `myDotnetFunction` menggunakan profil default dan Wilayah AWS pengaturan:

```
dotnet new lambda.EmptyFunction --name myDotnetFunction
```

Perintah ini membuat file dan direktori berikut di direktori proyek Anda.

```
### myDotnetFunction
### src
#   ### myDotnetFunction
#       ### Function.cs
#       ### Readme.md
```



```
#      ### aws-lambda-tools-defaults.json
#      ### myDotnetFunction.csproj
### test
    ### myDotnetFunction.Tests
        ### FunctionTest.cs
        ### myDotnetFunction.Tests.csproj
```

Di bawah direktori `src/myDotnetFunction`, periksa file-file berikut:

- `aws-lambda-tools-defaults.json`: Ini adalah tempat Anda menentukan opsi baris perintah saat men-deploy fungsi Lambda Anda. Sebagai contoh:

```
"profile" : "default",
"region" : "us-east-2",
"configuration" : "Release",
"function-architecture": "x86_64",
"function-runtime": "dotnet8",
"function-memory-size" : 256,
"function-timeout" : 30,
"function-handler" : "myDotnetFunction::myDotnetFunction.Function::FunctionHandler"
```

- `Function.cs`: Kode fungsi handler Lambda Anda. Ini adalah templat C# yang menyertakan pustaka `Amazon.Lambda.Core` default dan atribut `LambdaSerializer` default. Untuk informasi selengkapnya tentang persyaratan dan opsi serialisasi, lihat [Serialisasi dalam fungsi Lambda](#). Ini juga mencakup fungsi sampel yang dapat Anda edit untuk menerapkan kode fungsi Lambda Anda.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted into
// a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace myDotnetFunction;

public class Function
{
    /// <summary>
    /// A simple function that takes a string and does a ToUpper
    /// </summary>
    /// <param name="input"></param>
```

```

    /// <param name="context"></param>
    /// <returns></returns>
    public string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}

```

- DotnetFunction.csproj saya: File [MSBuild](#) yang mencantumkan file dan rakitan yang terdiri dari aplikasi Anda.

```

<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
    <!-- This property makes the build directory similar to a publish directory and
helps the AWS .NET Lambda Mock Test Tool find project dependencies. -->
    <CopyLocalLockFileAssemblies>true</CopyLocalLockFileAssemblies>
    <!-- Generate ready to run images during publishing to improve cold start time.
-->
    <PublishReadyToRun>true</PublishReadyToRun>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.2.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.SystemTextJson"
Version="2.4.0" />
  </ItemGroup>
</Project>

```

- Readme: Gunakan file ini untuk mendokumentasikan fungsi Lambda Anda.

Di bawah direktori `myfunction/test`, periksa file-file berikut:

- DotnetFunction.tests.csproj saya: Seperti disebutkan sebelumnya, ini adalah file [MSBuild](#) yang mencantumkan file dan rakitan yang terdiri dari proyek pengujian Anda. Perhatikan juga bahwa ini menyertakan `Amazon.Lambda.Core` pustaka, sehingga Anda dapat dengan mulus mengintegrasikan template Lambda apa pun yang diperlukan untuk menguji fungsi Anda.

```

<Project Sdk="Microsoft.NET.Sdk">

```

```
...  
  
<PackageReference Include="Amazon.Lambda.Core" Version="2.2.0 " />  
  
...
```

- **FunctionTest.cs**: File template kode C # yang sama yang disertakan dalam direktori. `src` Edit file ini untuk mencerminkan kode produksi fungsi Anda dan mengujinya sebelum mengunggah fungsi Lambda Anda ke lingkungan produksi.

```
using Xunit;  
using Amazon.Lambda.Core;  
using Amazon.Lambda.TestUtilities;  
  
using MyFunction;  
  
namespace MyFunction.Tests  
{  
    public class FunctionTest  
    {  
        [Fact]  
        public void TestToUpperFunction()  
        {  
  
            // Invoke the lambda function and confirm the string was upper cased.  
            var function = new Function();  
            var context = new TestLambdaContext();  
            var upperCase = function.FunctionHandler("hello world", context);  
  
            Assert.Equal("HELLO WORLD", upperCase);  
        }  
    }  
}
```

Menerapkan proyek .NET menggunakan .NET CLI

Untuk membangun paket penyebaran Anda dan menyebarkannya ke Lambda, Anda menggunakan alat CLI. `Amazon.Lambda.Tools` Untuk menerapkan fungsi Anda dari file yang Anda buat di langkah sebelumnya, pertama-tama navigasikan ke folder yang berisi `.csproj` file fungsi Anda.

```
cd myDotnetFunction/src/myDotnetFunction
```

Untuk menyebarkan kode Anda ke Lambda sebagai paket penyebaran .zip, jalankan perintah berikut. Pilih nama fungsi Anda sendiri.

```
dotnet lambda deploy-function myDotnetFunction
```

Selama penyebaran, wizard meminta Anda untuk memilih file. [the section called “Peran eksekusi \(izin untuk fungsi untuk mengakses sumber daya lain\)”](#) Untuk contoh ini, pilih `lambda_basic_role`.

Setelah Anda menerapkan fungsi Anda, Anda dapat mengujinya di cloud menggunakan `dotnet lambda invoke-function` perintah. Untuk contoh kode dalam `lambda.EmptyFunction` template, Anda dapat menguji fungsi Anda dengan meneruskan string menggunakan `--payload` opsi.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything is OK"
```

Jika fungsi Anda telah berhasil di-deploy, Anda akan melihat output yang mirip dengan berikut ini.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything is OK"
Amazon Lambda Tools for .NET Core applications (5.8.0)
Project Home: https://github.com/aws/aws-extensions-for-dotnet-cli, https://github.com/aws/aws-lambda-dotnet

Payload:
"JUST CHECKING IF EVERYTHING IS OK"

Log Tail:
START RequestId: id Version: $LATEST
END RequestId: id
REPORT RequestId: id Duration: 0.99 ms          Billed Duration: 1 ms          Memory
Size: 256 MB      Max Memory Used: 12 MB
```

Menggunakan layer Lambda dengan .NET CLI

Note

Menggunakan lapisan dengan fungsi dalam bahasa yang dikompilasi seperti C # mungkin tidak memberikan jumlah manfaat yang sama seperti dengan bahasa yang ditafsirkan seperti

Python. Karena C# adalah bahasa yang dikompilasi, fungsi Anda masih harus memuat rakitan bersama secara manual ke dalam memori selama fase init, yang dapat meningkatkan waktu mulai dingin. Sebagai gantinya, kami sarankan untuk menyertakan kode bersama apa pun pada waktu kompilasi untuk memanfaatkan pengoptimalan kompiler bawaan apa pun.

.NET CLI mendukung perintah untuk membantu Anda mempublikasikan lapisan dan menerapkan fungsi C# yang menggunakan lapisan. Untuk memublikasikan layer ke bucket Amazon S3 tertentu, jalankan perintah berikut di direktori yang sama dengan file Anda .csproj:

```
dotnet lambda publish-layer <layer_name> --layer-type runtime-package-store --s3-bucket <s3_bucket_name>
```

Kemudian, ketika Anda menerapkan fungsi Anda menggunakan .NET CLI, tentukan layer ARN konsumsi dalam perintah berikut:

```
dotnet lambda deploy-function <function_name> --function-layers arn:aws:lambda:us-east-1:123456789012:layer:layer-name:1
```

Untuk contoh lengkap fungsi Hello World, lihat [blank-csharp-with-layers](#) sampelnya.

Menyebarkan fungsi C# Lambda menggunakan AWS SAM

The AWS Serverless Application Model (AWS SAM) adalah toolkit yang membantu merampingkan proses membangun dan menjalankan aplikasi tanpa server. AWS Anda menentukan sumber daya untuk aplikasi Anda dalam template YAMM atau JSON dan menggunakan antarmuka baris AWS SAM perintah (AWS SAM CLI) untuk membangun, mengemas, dan menyebarkan aplikasi Anda. Saat Anda membuat fungsi Lambda dari AWS SAM template, AWS SAM secara otomatis membuat paket penerapan .zip atau gambar kontainer dengan kode fungsi Anda dan dependensi apa pun yang Anda tentukan. AWS SAM kemudian menyebarkan fungsi Anda menggunakan [AWS CloudFormation tumpukan](#). Untuk mempelajari lebih lanjut cara menggunakan AWS SAM untuk membangun dan menerapkan fungsi Lambda, [lihat Memulai](#) di Panduan AWS SAMAWS Serverless Application Model Pengembang.

Langkah-langkah berikut menunjukkan kepada Anda cara mengunduh, membangun, dan menyebarkan contoh aplikasi.NET Hello World menggunakan AWS SAM. Contoh aplikasi ini menggunakan fungsi Lambda dan endpoint Amazon API Gateway untuk mengimplementasikan backend API dasar. Saat Anda mengirim permintaan HTTP GET ke titik akhir API Gateway, API

Gateway akan memanggil fungsi Lambda Anda. Fungsi mengembalikan pesan “hello world”, bersama dengan alamat IP dari instance fungsi Lambda yang memproses permintaan Anda.

Saat Anda membangun dan menerapkan aplikasi Anda menggunakan AWS SAM, di belakang layar AWS SAM CLI menggunakan perintah untuk mengemas dotnet lambda package bundel kode fungsi Lambda individual.

Prasyarat

.NET 8 SDK

Instal [.NET 8](#) SDK dan Runtime.

AWS SAM CLI versi 1.39 atau yang lebih baru

Untuk mempelajari cara menginstal AWS SAM CLI versi terbaru, lihat [Menginstal CLI AWS SAM](#).

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan template Hello world .NET menggunakan perintah berikut.

```
sam init --app-template hello-world --name sam-app \  
--package-type Zip --runtime dotnet8
```

Perintah ini membuat file dan direktori berikut di direktori proyek Anda.

```
### sam-app  
### README.md  
### events  
#   ### event.json  
### omnisharp.json  
### samconfig.toml  
### src  
#   ### HelloWorld  
#       ### Function.cs  
#       ### HelloWorld.csproj  
#       ### aws-lambda-tools-defaults.json  
### template.yaml  
### test  
### HelloWorld.Test  
### FunctionTest.cs  
### HelloWorld.Tests.csproj
```

2. Arahkan ke direktori yang berisi `filetemplate.yaml` file. File ini adalah tempate yang mendefinisikan AWS resource untuk aplikasi Anda, termasuk fungsi Lambda dan API Gateway API.

```
cd sam-app
```

3. Untuk membangun sumber aplikasi Anda, jalankan perintah berikut.

```
sam build
```

4. Untuk menyebarkan aplikasi Anda AWS, jalankan perintah berikut.

```
sam deploy --guided
```

Perintah ini mengemas dan menyebarkan aplikasi Anda dengan serangkaian prompt berikut. Untuk menerima opsi default, tekan Enter.

Note

Karena HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, apakah ini baik-baik saja? , pastikan untuk masuky.

- Nama Stack: Nama tumpukan yang akan digunakan. AWS CloudFormation Nama ini harus unik untuk Anda Akun AWS dan Wilayah AWS.
- Wilayah AWS: Wilayah AWS Anda ingin menerapkan aplikasi Anda ke.
- Konfirmasikan perubahan sebelum penerapan: Pilih ya untuk meninjau set perubahan apa pun secara manual sebelum AWS SAM menerapkan perubahan aplikasi. Jika Anda memilih tidak, AWS SAM CLI secara otomatis menyebarkan perubahan aplikasi.
- Izinkan pembuatan peran SAM CLI IAM: Banyak AWS SAM templat, termasuk Hello world dalam contoh ini, buat peran AWS Identity and Access Management (IAM) untuk memberikan izin fungsi Lambda Anda untuk mengakses yang lain. AWS layanan Pilih Ya untuk memberikan izin untuk menyebarkan AWS CloudFormation tumpukan yang membuat atau memodifikasi peran IAM.
- Nonaktifkan rollback: Secara default, jika AWS SAM menemukan kesalahan selama pembuatan atau penyebaran tumpukan Anda, itu akan memutar tumpukan kembali ke versi sebelumnya. Pilih Tidak untuk menerima default ini.

- HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, apakah ini baik-baik saja: Entery.
 - Simpan argumen ke `samconfig.toml`: Pilih `ya` untuk menyimpan pilihan konfigurasi Anda. Di masa mendatang, Anda dapat menjalankan ulang `sam deploy` tanpa parameter untuk menerapkan perubahan pada aplikasi Anda.
5. Ketika penerapan aplikasi Anda selesai, CLI mengembalikan Amazon Resource Name (ARN) dari fungsi Hello World Lambda dan peran IAM yang dibuat untuknya. Ini juga menampilkan titik akhir API Gateway API Anda. Untuk menguji aplikasi Anda, buka titik akhir di browser. Anda akan melihat respons yang mirip dengan yang berikut ini.

```
{"message":"hello world","location":"34.244.135.203"}
```

6. Untuk menghapus sumber daya Anda, jalankan perintah berikut. Perhatikan bahwa titik akhir API yang Anda buat adalah titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir ini setelah pengujian.

```
sam delete
```

Langkah selanjutnya

Untuk mempelajari selengkapnya tentang penggunaan AWS SAM untuk membangun dan menerapkan fungsi Lambda menggunakan .NET, lihat sumber daya berikut:

- [Panduan Pengembang AWS Serverless Application Model \(AWS SAM\)](#)
- [Membangun Aplikasi .NET Tanpa Server dengan AWS Lambda dan SAM CLI](#)

Menyebarkan fungsi C# Lambda menggunakan AWS CDK

AWS Cloud Development Kit (AWS CDK) Ini adalah kerangka pengembangan perangkat lunak open-source untuk mendefinisikan infrastruktur cloud sebagai kode dengan bahasa pemrograman modern dan kerangka kerja seperti .NET. AWS CDK proyek dijalankan untuk menghasilkan AWS CloudFormation template yang kemudian digunakan untuk menyebarkan kode Anda.

Untuk membangun dan menyebarkan contoh aplikasi Hello world .NET menggunakan AWS CDK, ikuti petunjuk di bagian berikut. Aplikasi sampel mengimplementasikan backend API dasar yang terdiri dari titik akhir API Gateway dan fungsi Lambda. API Gateway memanggil fungsi Lambda saat

Anda mengirim permintaan HTTP GET ke titik akhir. Fungsi mengembalikan pesan Hello world, bersama dengan alamat IP dari instance Lambda yang memproses permintaan Anda.

Prasyarat

.NET 8 SDK

Instal [.NET 8](#) SDK dan Runtime.

AWS CDK versi 2

Untuk mempelajari cara menginstal versi terbaru, AWS CDK lihat [Memulai dengan AWS CDK di Panduan Pengembang AWS Cloud Development Kit \(AWS CDK\) v2](#).

Menyebarkan aplikasi sampel AWS CDK

1. Buat direktori proyek untuk aplikasi sampel dan navigasikan ke dalamnya.

```
mkdir hello-world
cd hello-world
```

2. Menginisialisasi AWS CDK aplikasi baru dengan menjalankan perintah berikut.

```
cdk init app --language csharp
```

Perintah membuat file dan direktori berikut di direktori proyek Anda

```
### README.md
### cdk.json
### src
  ### HelloWorld
  #   ### GlobalSuppressions.cs
  #   ### HelloWorld.csproj
  #   ### HelloWorldStack.cs
  #   ### Program.cs
  ### HelloWorld.sln
```

3. Buka `src` direktori dan buat fungsi Lambda baru menggunakan .NET CLI. Ini adalah fungsi yang akan Anda terapkan menggunakan AWS CDK. Dalam contoh ini, Anda membuat fungsi Hello world bernama `HelloWorldLambda` menggunakan `lambda.EmptyFunction` template.

```
cd src
dotnet new lambda.EmptyFunction -n HelloWorldLambda
```

Setelah langkah ini, struktur direktori Anda di dalam direktori proyek Anda akan terlihat seperti berikut.

```
### README.md
### cdk.json
### src
  ### HelloWorld
  #   ### GlobalSuppressions.cs
  #   ### HelloWorld.csproj
  #   ### HelloWorldStack.cs
  #   ### Program.cs
  ### HelloWorld.sln
  ### HelloWorldLambda
    ### src
    #   ### HelloWorldLambda
    #   ### Function.cs
    #   ### HelloWorldLambda.csproj
    #   ### Readme.md
    #   ### aws-lambda-tools-defaults.json
    ### test
    #   ### HelloWorldLambda.Tests
    #   ### FunctionTest.cs
    #   ### HelloWorldLambda.Tests.csproj
```

4. Buka `HelloWorldStack.cs` file dari `src/HelloWorld` direktori. Ganti isi file dengan kode berikut.

```
using Amazon.CDK;
using Amazon.CDK.AWS.Lambda;
using Amazon.CDK.AWS.Logs;
using Constructs;

namespace CdkTest
{
    public class HelloWorldStack : Stack
    {
        internal HelloWorldStack(Construct scope, string id, IStackProps props =
            null) : base(scope, id, props)
```

```

    {
        var buildOption = new BundlingOptions()
        {
            Image = Runtime.DOTNET_8.BundlingImage,
            User = "root",
            OutputType = BundlingOutput.ARCHIVED,
            Command = new string[]{
                "/bin/sh",
                "-c",
                " dotnet tool install -g Amazon.Lambda.Tools"+
                " && dotnet build"+
                " && dotnet lambda package --output-package /asset-output/
function.zip"
            }
        };

        var helloWorldLambdaFunction = new Function(this,
            "HelloWorldFunction", new FunctionProps
            {
                Runtime = Runtime.DOTNET_8,
                MemorySize = 1024,
                LogRetention = RetentionDays.ONE_DAY,
                Handler =
                "HelloWorldLambda::HelloWorldLambda.Function::FunctionHandler",
                Code = Code.FromAsset("./src/HelloWorldLambda/src/
HelloWorldLambda", new Amazon.CDK.AWS.S3.Assets.AssetOptions
                {
                    Bundling = buildOption
                }
            )),
        });
    }
}
}

```

Ini adalah kode untuk mengkompilasi dan menggabungkan kode aplikasi, serta definisi fungsi Lambda itu sendiri. `BundlingOptions` objek memungkinkan file zip dibuat, bersama dengan serangkaian perintah yang digunakan untuk menghasilkan konten file zip. Dalam hal ini, `dotnet lambda package` perintah digunakan untuk mengkompilasi dan menghasilkan file zip.

5. Untuk menyebarkan aplikasi Anda, jalankan perintah berikut.

```
cdk deploy
```

6. Memanggil fungsi Lambda yang Anda gunakan menggunakan .NET Lambda CLI.

```
dotnet lambda invoke-function HelloWorldFunction -p "hello world"
```

7. Setelah selesai menguji, Anda dapat menghapus sumber daya yang Anda buat, kecuali jika Anda ingin mempertahankannya. Jalankan perintah berikut untuk menghapus sumber daya Anda.

```
cdk destroy
```

Langkah selanjutnya

Untuk mempelajari selengkapnya tentang penggunaan AWS CDK untuk membangun dan menerapkan fungsi Lambda menggunakan .NET, lihat sumber daya berikut:

- [Bekerja dengan AWS CDK di C #](#)
- [Membangun, mengemas, dan mempublikasikan fungsi .NET C # Lambda dengan CDK AWS](#)

Menyebarkan aplikasi ASP.NET

Selain menghosting fungsi berbasis acara, Anda juga dapat menggunakan .NET dengan Lambda untuk meng-host aplikasi ASP.NET ringan. Anda dapat membangun dan menyebarkan aplikasi ASP.NET menggunakan paket. `Amazon.Lambda.AspNetCoreServer` NuGet Di bagian ini, Anda mempelajari cara menerapkan API web ASP.NET ke Lambda menggunakan tooling .NET Lambda CLI.

Topik

- [Prasyarat](#)
- [Menyebarkan API Web ASP.NET ke Lambda](#)
- [Menerapkan API minimal ASP.NET ke Lambda](#)

Prasyarat

.NET 8 SDK

Instal [.NET 8](#) SDK dan ASP.NET Core Runtime.

Amazon.Lambda.Tools

Untuk membuat fungsi Lambda Anda, Anda menggunakan [Amazon.Lambda.Tools](#) ekstensi.NET [Global Tools](#). Untuk menginstal Amazon.Lambda.Tools, jalankan perintah berikut:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Untuk informasi selengkapnya tentang Amazon.Lambda.Tools ekstensi.NET CLI, lihat [AWS Ekstensi untuk repositori.NET CLI](#) di GitHub

Amazon.Lambda.Templates

Untuk menghasilkan kode fungsi Lambda Anda, gunakan paket. [Amazon.Lambda.Templates](#) NuGet Untuk menginstal paket template ini, jalankan perintah berikut:

```
dotnet new --install Amazon.Lambda.Templates
```

Menyebarkan API Web ASP.NET ke Lambda

Untuk menerapkan API web menggunakan ASP.NET, Anda dapat menggunakan template .NET Lambda untuk membuat proyek API web baru. Gunakan perintah berikut untuk menginisialisasi proyek API web ASP.NET baru. Dalam perintah contoh, kami memberi nama proyek AspNetOnLambda.

```
dotnet new serverless.AspNetCoreWebAPI -n AspNetOnLambda
```

Perintah ini membuat file dan direktori berikut di direktori proyek Anda.

```
.
### AspNetOnLambda
  ### src
  #   ### AspNetOnLambda
  #     ### AspNetOnLambda.csproj
  #     ### Controllers
  #     #   ### ValuesController.cs
  #     ### LambdaEntryPoint.cs
  #     ### LocalEntryPoint.cs
  #     ### Readme.md
  #     ### Startup.cs
  #     ### appsettings.Development.json
```

```
#      ### appsettings.json
#      ### aws-lambda-tools-defaults.json
#      ### serverless.template
### test
    ### AspNetOnLambda.Tests
        ### AspNetOnLambda.Tests.csproj
        ### SampleRequests
        #      ### ValuesController-Get.json
        ### ValuesControllerTests.cs
        ### appsettings.json
```

Ketika Lambda memanggil fungsi Anda, titik masuk yang digunakannya adalah file. `LambdaEntryPoint.cs` File yang dibuat oleh `template.NET Lambda` berisi kode berikut.

```
namespace AspNetOnLambda;

public class LambdaEntryPoint : Amazon.Lambda.AspNetCoreServer.APIGatewayProxyFunction
{
    protected override void Init(IWebHostBuilder builder)
    {
        builder
            .UseStartup#Startup#();
    }

    protected override void Init(IHostBuilder builder)
    {
    }
}
```

Titik masuk yang digunakan oleh Lambda harus mewarisi dari salah satu dari tiga kelas dasar dalam paket. `Amazon.Lambda.AspNetCoreServer` Ketiga kelas dasar ini adalah:

- `APIGatewayProxyFunction`
- `APIGatewayHttpApiV2ProxyFunction`
- `ApplicationLoadBalancerFunction`

Kelas default yang digunakan saat Anda membuat `LambdaEntryPoint.cs` file menggunakan `template.NET Lambda` yang disediakan adalah. `APIGatewayProxyFunction` Kelas dasar yang Anda gunakan dalam fungsi Anda bergantung pada lapisan API mana yang berada di depan fungsi Lambda Anda.

Masing-masing dari tiga kelas dasar berisi metode publik bernama `FunctionHandlerAsync`. Nama metode ini akan membentuk bagian dari [string handler](#) yang digunakan Lambda untuk memanggil fungsi Anda. `FunctionHandlerAsync` metode ini mengubah payload acara masuk menjadi format ASP.NET yang benar dan respons ASP.NET kembali ke muatan respons Lambda. Untuk `AspNetOnLambda` proyek contoh yang ditampilkan, string handler adalah sebagai berikut.

```
AspNetOnLambda::AspNetOnLambda.LambdaEntryPoint::FunctionHandlerAsync
```

Untuk menerapkan API ke Lambda, jalankan perintah berikut untuk menavigasi ke direktori yang berisi file kode sumber Anda dan menerapkan fungsi Anda menggunakan AWS CloudFormation

```
cd AspNetOnLambda/src/AspNetOnLambda
dotnet lambda deploy-serverless
```

Tip

Saat Anda menerapkan API menggunakan **`dotnet lambda deploy-serverless`** perintah, AWS CloudFormation beri nama pada fungsi Lambda Anda berdasarkan nama tumpukan yang Anda tentukan selama penerapan. Untuk memberikan nama khusus pada fungsi Lambda Anda, edit `serverless.template` file untuk menambahkan `FunctionName` properti ke sumber daya `AWS::Serverless::Function` Lihat [Jenis nama](#) di Panduan AWS CloudFormation Pengguna untuk mempelajari lebih lanjut.

Menerapkan API minimal ASP.NET ke Lambda

Untuk menerapkan API minimal ASP.NET ke Lambda, Anda dapat menggunakan template .NET Lambda untuk membuat proyek API minimal yang baru. Gunakan perintah berikut untuk menginisialisasi proyek API minimal yang baru. Dalam contoh ini, kami memberi nama `proyekMinimalApiOnLambda`.

```
dotnet new serverless.AspNetCoreMinimalAPI -n MinimalApiOnLambda
```

Perintah membuat file dan direktori berikut di direktori proyek Anda.

```
### MinimalApiOnLambda
  ### src
    ### MinimalApiOnLambda
```

```
### Controllers
#   ### CalculatorController.cs
### MinimalApiOnLambda.csproj
### Program.cs
### Readme.md
### appsettings.Development.json
### appsettings.json
### aws-lambda-tools-defaults.json
### serverless.template
```

Program.cs File berisi kode berikut.

```
var builder = WebApplication.CreateBuilder(args);

// Add services to the container.
builder.Services.AddControllers();

// Add AWS Lambda support. When application is run in Lambda Kestrel is swapped out as
// the web server with Amazon.Lambda.AspNetCoreServer. This
// package will act as the webserver translating request and responses between the
// Lambda event source and ASP.NET Core.
builder.Services.AddAWSLambdaHosting(LambdaEventSource.RestApi);

var app = builder.Build();

app.UseHttpsRedirection();
app.UseAuthorization();
app.MapControllers();

app.MapGet("/", () => "Welcome to running ASP.NET Core Minimal API on AWS Lambda");

app.Run();
```

Untuk mengonfigurasi API minimal agar berjalan di Lambda, Anda mungkin perlu mengedit kode ini agar permintaan dan tanggapan antara Lambda dan ASP.NET Core diterjemahkan dengan benar. Secara default, fungsi dikonfigurasi untuk sumber peristiwa REST API. Untuk HTTP API atau penyeimbang beban aplikasi, ganti (*LambdaEventSource.RestApi*) dengan salah satu opsi berikut:

- (*LambdaEventSource.HttpApi*)
- (*LambdaEventSource.ApplicationLoadBalancer*)

Untuk menerapkan API minimal Anda ke Lambda, jalankan perintah berikut untuk menavigasi ke direktori yang berisi file kode sumber Anda dan menerapkan fungsi Anda menggunakan AWS CloudFormation

```
cd MinimalApiOnLambda/src/MinimalApiOnLambda  
dotnet lambda deploy-serverless
```

Menyebarkan. NET Fungsi Lambda dengan gambar kontainer

Ada tiga cara untuk membangun gambar kontainer untuk file. NET Fungsi Lambda:

- [Menggunakan gambar AWS dasar untuk. NET](#)

[Gambar AWS dasar](#) dimuat sebelumnya dengan runtime bahasa, klien antarmuka runtime untuk mengelola interaksi antara Lambda dan kode fungsi Anda, dan emulator antarmuka runtime untuk pengujian lokal.

- [Menggunakan gambar AWS dasar khusus OS](#)

[AWS Gambar dasar khusus OS](#) berisi distribusi Amazon Linux dan emulator antarmuka [runtime](#). Gambar-gambar ini biasanya digunakan untuk membuat gambar kontainer untuk bahasa yang dikompilasi, seperti [Go](#) dan [Rust](#), dan untuk versi bahasa atau bahasa yang Lambda tidak menyediakan gambar dasar, seperti Node.js 19. Anda juga dapat menggunakan gambar dasar khusus OS untuk mengimplementasikan runtime [khusus](#). Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan klien [antarmuka runtime untuk. NET](#) dalam gambar.

- [Menggunakan gambar AWS non-dasar](#)

Anda dapat menggunakan gambar dasar alternatif dari registri kontainer lain, seperti Alpine Linux atau Debian. Anda juga dapat menggunakan gambar kustom yang dibuat oleh organisasi Anda. Untuk membuat gambar kompatibel dengan Lambda, Anda harus menyertakan klien [antarmuka runtime untuk. NET](#) dalam gambar.

Tip

Untuk mengurangi waktu yang dibutuhkan agar fungsi kontainer Lambda menjadi aktif, lihat [Menggunakan build multi-tahap](#) dalam dokumentasi Docker. Untuk membuat gambar kontainer yang efisien, ikuti [Praktik terbaik untuk menulis Dockerfiles](#).

Halaman ini menjelaskan cara membuat, menguji, dan menyebarkan gambar kontainer untuk Lambda.

Topik

- [AWS gambar dasar untuk. NET](#)
- [Menggunakan gambar AWS dasar untuk. NET](#)

- [Menggunakan gambar dasar alternatif dengan klien antarmuka runtime](#)

AWS gambar dasar untuk .NET

AWS menyediakan gambar dasar berikut untuk .NET:

| Tanda | Waktu berjalan | Sistem operasi | Dockerfile | penghentian |
|-------|----------------|-------------------|--|-------------|
| 8 | .NET8 | Amazon Linux 2023 | Dockerfile untuk .NET8 pada GitHub | |
| 6 | .NET6 | Amazon Linux 2 | Dockerfile untuk .NET6 pada GitHub | 20 Des 2024 |

ECRRepositori Amazon: gallery.ecr.aws/lambda/dotnet

Menggunakan gambar AWS dasar untuk .NET

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [.NETSDK](#)Langkah-langkah berikut menggunakan .NET8 gambar dasar. Pastikan bahwa Anda .NETversi cocok dengan versi [gambar dasar](#) yang Anda tentukan di Dockerfile Anda.
- [Docker](#)

Membuat dan menyebarkan gambar menggunakan gambar dasar

[Dalam langkah-langkah berikut, Anda menggunakan Amazon.Lambda.Templates dan Amazon.Lambda.Tools untuk membuat file .NETproyek.](#) Kemudian, Anda membuat gambar Docker, mengunggah gambar ke AmazonECR, dan menerapkannya ke fungsi Lambda.

1. Instal paket [Amazon.Lambda.Templates](#). NuGet

```
dotnet new install Amazon.Lambda.Templates
```

2. Buat a .NETproyek menggunakan `lambda.image.EmptyFunction` template.

```
dotnet new lambda.image.EmptyFunction --name MyFunction --region us-east-1
```

3. Buka direktori *MyFunction/src/MyFunction* tersebut. Di sinilah file proyek disimpan. Periksa file-file berikut:

- `aws-lambda-tools-defaults.json` — File ini adalah tempat Anda menentukan opsi baris perintah saat menerapkan fungsi Lambda Anda.
- `Function.cs` - Kode fungsi handler Lambda Anda. Ini adalah template C # yang mencakup `Amazon.Lambda.Core` pustaka default dan `LambdaSerializer` atribut default. Untuk informasi selengkapnya tentang persyaratan dan opsi serialisasi, lihat [Serialisasi dalam fungsi Lambda](#). Anda dapat menggunakan kode yang disediakan untuk pengujian, atau menggantinya dengan kode Anda sendiri.
- `MyFunction.csproj` — A. NET [file proyek](#), yang mencantumkan file dan rakitan yang terdiri dari aplikasi Anda.
- `README.md` - File ini berisi informasi lebih lanjut tentang fungsi Lambda sampel.

4. Periksa Dockerfile di direktori `src/MyFunction` Anda dapat menggunakan Dockerfile yang disediakan untuk pengujian, atau menggantinya dengan milik Anda sendiri. Jika Anda menggunakan sendiri, pastikan untuk:

- Atur FROM properti ke [URlgambar dasar](#). Anda. NETversi harus cocok dengan versi gambar dasar.
- Atur CMD argumen ke penanganan fungsi Lambda. Ini harus cocok dengan `image-command` in `aws-lambda-tools-defaults.json`.

[Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER](#) Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke `root` pengguna ketika tidak ada `USER` instruksi yang diberikan.

Example Dockerfile

```
# You can also pull these images from DockerHub amazon/aws-lambda-dotnet:8
FROM public.ecr.aws/lambda/dotnet:8

# Copy function code to Lambda-defined environment variable
COPY publish/* ${LAMBDA_TASK_ROOT}
```

```
# Set the CMD to your handler (could also be done as a parameter override outside
of the Dockerfile)
CMD [ "MyFunction::MyFunction.Function::FunctionHandler" ]
```

5. [Instal Amazon.Lambda.Tools. NETAlat Global.](#)

```
dotnet tool install -g Amazon.Lambda.Tools
```

Jika Amazon.Lambda.Tools sudah diinstal, pastikan Anda memiliki versi terbaru.

```
dotnet tool update -g Amazon.Lambda.Tools
```

6. Ubah direktori ke `MyFunction/src/MyFunction`, jika Anda belum ada di sana.

```
cd src/MyFunction
```

7. Gunakan Amazon.Lambda.Tools untuk membuat image Docker, mendorongnya ke repositori ECR Amazon baru, dan menerapkan fungsi Lambda.

Untuk `--function-role`, tentukan nama peran—bukan Amazon Resource Name (ARN)—dari [peran eksekusi](#) untuk fungsi tersebut. Misalnya, `lambda-role`.

```
dotnet lambda deploy-function MyFunction --function-role lambda-role
```

Untuk informasi lebih lanjut tentang Amazon.Lambda.Tools. NETGlobal Tool, lihat [AWS Ekstensi untuk .NET CLI](#) repositori aktif. GitHub

8. Memanggil fungsi.

```
dotnet lambda invoke-function MyFunction --payload "Testing the function"
```

Jika semuanya berhasil, Anda akan melihat hal berikut:

```
Payload:
"TESTING THE FUNCTION"

Log Tail:
START RequestId: id Version: $LATEST
END RequestId: id
```

```
REPORT RequestId: id Duration: 0.99 ms Billed Duration: 1 ms Memory  
Size: 256 MB Max Memory Used: 12 MB
```

9. Hapus fungsi Lambda.

```
dotnet lambda delete-function MyFunction
```

Menggunakan gambar dasar alternatif dengan klien antarmuka runtime

Jika Anda menggunakan gambar [dasar khusus OS atau gambar dasar](#) alternatif, Anda harus menyertakan klien antarmuka runtime dalam gambar Anda. Klien antarmuka runtime memperluas [Menggunakan runtime Lambda untuk runtime khusus API](#), yang mengelola interaksi antara Lambda dan kode fungsi Anda.

Contoh berikut menunjukkan bagaimana membangun image container untuk .NET menggunakan gambar AWS non-dasar, dan cara menambahkan [Amazon.Lambda.RuntimeSupport](#) paket, yang merupakan klien antarmuka runtime Lambda untuk .NET. Contoh Dockerfile menggunakan Microsoft .NET8 gambar dasar.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [.NETSDK](#)— Langkah-langkah berikut menggunakan a. NET8 gambar dasar. Pastikan bahwa Anda .NET versi cocok dengan versi [gambar dasar](#) yang Anda tentukan di Dockerfile Anda.
- [Docker](#)

Membuat dan menyebarkan gambar menggunakan gambar dasar alternatif

1. Instal paket [Amazon.Lambda.Templates](#). NuGet

```
dotnet new install Amazon.Lambda.Templates
```

2. Buat a. NET proyek menggunakan `lambda.CustomRuntimeFunction` template. Template ini termasuk [Amazon.Lambda.RuntimeSupport](#) paket.

```
dotnet new lambda.CustomRuntimeFunction --name MyFunction --region us-east-1
```

3. Buka direktori `MyFunction/src/MyFunction` tersebut. Di sinilah file proyek disimpan. Periksa file-file berikut:
 - `aws-lambda-tools-defaults.json` — File ini adalah tempat Anda menentukan opsi baris perintah saat menerapkan fungsi Lambda Anda.
 - `Function.cs` - Kode berisi kelas dengan `Main` metode yang menginisialisasi `Amazon.Lambda.RuntimeSupport` perpustakaan sebagai bootstrap. `MainMetode` ini adalah titik masuk untuk proses fungsi. `MainMetode` ini membungkus fungsi handler dalam pembungkus yang dapat digunakan bootstrap. Untuk informasi selengkapnya, lihat [Menggunakan Amazon.Lambda.RuntimeSupport sebagai perpustakaan kelas](#) di GitHub repositori.
 - `MyFunction.csproj` — A. NET [file proyek](#), yang mencantumkan file dan rakitan yang terdiri dari aplikasi Anda.
 - `README.md` - File ini berisi informasi lebih lanjut tentang fungsi Lambda sampel.
4. Buka `aws-lambda-tools-defaults.json` file dan Tambahkan baris berikut:

```
"package-type": "image",  
"docker-host-build-output-dir": "./bin/Release/Lambda-publish"
```

- `package-type`: Mendefinisikan paket deployment sebagai image container.
- `docker-host-build-output-dir`: Menetapkan direktori output untuk proses build.

Example `aws-lambda-tools-defaults.json`

```
{  
  "Information": [  
    "This file provides default values for the deployment wizard inside Visual  
    Studio and the AWS Lambda commands added to the .NET Core CLI.",  
    "To learn more about the Lambda commands with the .NET Core CLI execute the  
    following command at the command line in the project root directory.",  
    "dotnet lambda help",  
    "All the command line options for the Lambda command can be specified in this  
    file."  
  ],  
  "profile": "",  
  "region": "us-east-1",  
  "configuration": "Release",  
  "function-runtime": "provided.al2023",  
}
```

```

"function-memory-size": 256,
"function-timeout": 30,
"function-handler": "bootstrap",
"msbuild-parameters": "--self-contained true",
"package-type": "image",
"docker-host-build-output-dir": "./bin/Release/lambda-publish"
}

```

5. Buat Dockerfile di direktori. *MyFunction*/src/*MyFunction* Contoh berikut Dockerfile menggunakan Microsoft. NETgambar dasar bukan [gambar AWS dasar](#).

- Atur FROM properti ke pengidentifikasi gambar dasar. Anda. NETversi harus cocok dengan versi gambar dasar.
- Gunakan COPY perintah untuk menyalin fungsi ke /var/task direktori.
- Atur ENTRYPOINT ke modul yang Anda inginkan untuk menjalankan wadah Docker saat dimulai. Dalam hal ini, modul adalah bootstrap, yang menginisialisasi Amazon.Lambda.RuntimeSupport perpustakaan.

Perhatikan bahwa contoh Dockerfile tidak menyertakan instruksi. USER Saat Anda menyebarkan gambar kontainer ke Lambda, Lambda secara otomatis mendefinisikan pengguna Linux default dengan izin yang paling tidak memiliki hak istimewa. Ini berbeda dari perilaku Docker standar yang default ke root pengguna ketika tidak ada USER instruksi yang diberikan.

Example Dockerfile

```

# You can also pull these images from DockerHub amazon/aws-lambda-dotnet:8
FROM mcr.microsoft.com/dotnet/runtime:8.0

# Set the image's internal work directory
WORKDIR /var/task

# Copy function code to Lambda-defined environment variable
COPY "bin/Release/net8.0/linux-x64" .

# Set the entrypoint to the bootstrap
ENTRYPOINT ["/usr/bin/dotnet", "exec", "/var/task/bootstrap.dll"]

```

6. [Instal Amazon.Lambda.Tools. NETEkstensi Alat Global](#).

```
dotnet tool install -g Amazon.Lambda.Tools
```


Jika Amazon.Lambda.Tools sudah diinstal, pastikan Anda memiliki versi terbaru.

```
dotnet tool update -g Amazon.Lambda.Tools
```

- Gunakan Amazon.Lambda.Tools untuk membuat image Docker, mendorongnya ke repositori ECR Amazon baru, dan menerapkan fungsi Lambda.

Untuk `--function-role`, tentukan nama peran—bukan Amazon Resource Name (ARN)—dari [peran eksekusi](#) untuk fungsi tersebut. Misalnya, `lambda-role`.

```
dotnet lambda deploy-function MyFunction --function-role lambda-role
```

Untuk informasi lebih lanjut tentang Amazon.Lambda.Tools. NETCLIEkstensi, lihat [AWS Ekstensi untuk .NETCL](#)irepositori aktif. GitHub

- Memanggil fungsi.

```
dotnet lambda invoke-function MyFunction --payload "Testing the function"
```

Jika semuanya berhasil, Anda akan melihat hal berikut:

Payload:

```
"TESTING THE FUNCTION"
```

Log Tail:

```
START RequestId: id Version: $LATEST
```

```
END RequestId: id
```

```
REPORT RequestId: id Duration: 0.99 ms          Billed Duration: 1 ms          Memory  
Size: 256 MB      Max Memory Used: 12 MB
```

- Hapus fungsi Lambda.

```
dotnet lambda delete-function MyFunction
```

Kompilasi kode fungsi.NET Lambda ke format runtime asli

.NET 8 mendukung kompilasi asli ahead-of-time (AOT). Dengan AOT asli, Anda dapat mengkompilasi kode fungsi Lambda Anda ke format runtime asli, yang menghilangkan kebutuhan untuk mengkompilasi kode.NET saat runtime. Kompilasi AOT asli dapat mengurangi waktu mulai dingin untuk fungsi Lambda yang Anda tulis di.NET. Untuk informasi selengkapnya, lihat [Memperkenalkan runtime .NET 8 untuk AWS Lambda](#) di AWS Compute Blog.

Bagian-bagian

- [waktu aktif Lambda](#)
- [Prasyarat](#)
- [Memulai](#)
- [Serialisasi](#)
- [Pemangkasan](#)
- [Pemecahan Masalah](#)

waktu aktif Lambda

Untuk menerapkan build fungsi Lambda dengan kompilasi AOT asli, gunakan runtime .NET 8 Lambda yang dikelola. Runtime ini mendukung penggunaan arsitektur x86_64 dan arm64.

Saat Anda menerapkan fungsi.NET Lambda tanpa menggunakan AOT, aplikasi Anda pertama kali dikompilasi ke dalam kode Bahasa Menengah (IL). Saat runtime, compiler just-in-time (JIT) di runtime Lambda mengambil kode IL dan mengkompilasinya ke dalam kode mesin sesuai kebutuhan. Dengan fungsi Lambda yang dikompilasi sebelumnya dengan AOT asli, Anda mengkompilasi kode Anda ke dalam kode mesin saat Anda menerapkan fungsi Anda, jadi Anda tidak bergantung pada runtime .NET atau SDK di runtime Lambda untuk mengkompilasi kode Anda sebelum dijalankan.

Salah satu batasan AOT adalah bahwa kode aplikasi Anda harus dikompilasi dalam lingkungan dengan sistem operasi Amazon Linux 2023 (AL2023) yang sama dengan yang digunakan runtime .NET 8. .NET Lambda CLI menyediakan fungsionalitas untuk mengkompilasi aplikasi Anda dalam wadah Docker menggunakan gambar AL2023.

Untuk menghindari potensi masalah dengan kompatibilitas lintas arsitektur, kami sangat menyarankan agar Anda mengkompilasi kode Anda di lingkungan dengan arsitektur prosesor yang sama dengan yang Anda konfigurasi untuk fungsi Anda. Untuk mempelajari lebih lanjut tentang batasan kompilasi lintas arsitektur, lihat [Kompilasi silang](#) dalam dokumentasi Microsoft .NET.

Prasyarat

Docker

Untuk menggunakan AOT asli, kode fungsi Anda harus dikompilasi dalam lingkungan dengan sistem operasi AL2023 yang sama dengan runtime .NET 8. Perintah .NET CLI di bagian berikut menggunakan Docker untuk mengembangkan dan membangun fungsi Lambda di lingkungan AL2023.

.NET 8 SDK

Kompilasi AOT asli adalah fitur dari .NET 8. Anda harus menginstal [.NET 8 SDK](#) pada mesin build Anda, tidak hanya runtime.

Amazon.Lambda.Tools

Untuk membuat fungsi Lambda Anda, Anda menggunakan [Amazon.Lambda.Tools](#) ekstensi .NET Global Tools. Untuk menginstal Amazon.Lambda.Tools, jalankan perintah berikut:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Untuk informasi selengkapnya tentang Amazon.Lambda.Tools ekstensi .NET CLI, lihat [AWS Extensions for .NET CLI](#) repository on GitHub

Amazon.Lambda.Templates

Untuk menghasilkan kode fungsi Lambda Anda, gunakan paket [Amazon.Lambda.Templates](#) NuGet. Untuk menginstal paket template ini, jalankan perintah berikut:

```
dotnet new install Amazon.Lambda.Templates
```

Memulai

Baik .NET Global CLI dan AWS Serverless Application Model (AWS SAM) menyediakan template memulai untuk membangun aplikasi menggunakan AOT asli. Untuk membangun fungsi AOT Lambda asli pertama Anda, lakukan langkah-langkah dalam instruksi berikut.

Untuk menginisialisasi dan menerapkan fungsi Lambda yang dikompilasi AOT asli

1. Inisialisasi proyek baru menggunakan template AOT asli dan kemudian navigasikan ke direktori yang berisi file yang dibuat `.cs` dan `.csproj`. Dalam contoh ini, kita menamai fungsi `kitaNativeAotSample`.

```
dotnet new lambda.NativeAOT -n NativeAotSample
cd ./NativeAotSample/src/NativeAotSample
```

`Function.csFile` yang dibuat oleh template AOT asli berisi kode fungsi berikut.

```
using Amazon.Lambda.Core;
using Amazon.Lambda.RuntimeSupport;
using Amazon.Lambda.Serialization.SystemTextJson;
using System.Text.Json.Serialization;

namespace NativeAotSample;

public class Function
{
    /// <summary>
    /// The main entry point for the Lambda function. The main function is called
    /// once during the Lambda init phase. It
    /// initializes the .NET Lambda runtime client passing in the function handler
    /// to invoke for each Lambda event and
    /// the JSON serializer to use for converting Lambda JSON format to the .NET
    /// types.
    /// </summary>
    private static async Task Main()
    {
        Func<string, ILambdaContext, string> handler = FunctionHandler;
        await LambdaBootstrapBuilder.Create(handler, new
        SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>())
            .Build()
            .RunAsync();
    }

    /// <summary>
    /// A simple function that takes a string and does a ToUpper.
    ///
    /// To use this handler to respond to an AWS event, reference the appropriate
    package from
```

```

    /// https://github.com/aws/aws-lambda-dotnet#events
    /// and change the string input parameter to the desired event type. When the
    event type
    /// is changed, the handler type registered in the main method needs to be
    updated and the LambdaFunctionJsonSerializerContext
    /// defined below will need the JsonSerializable updated. If the return type
    and event type are different then the
    /// LambdaFunctionJsonSerializerContext must have two JsonSerializable
    attributes, one for each type.
    ///
    // When using Native AOT extra testing with the deployed Lambda functions is
    required to ensure
    // the libraries used in the Lambda function work correctly with Native AOT. If
    a runtime
    // error occurs about missing types or methods the most likely solution will be
    to remove references to trim-unsafe
    // code or configure trimming options. This sample defaults to partial TrimMode
    because currently the AWS
    // SDK for .NET does not support trimming. This will result in a larger
    executable size, and still does not
    // guarantee runtime trimming errors won't be hit.
    /// </summary>
    /// <param name="input"></param>
    /// <param name="context"></param>
    /// <returns></returns>
    public static string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}

/// <summary>
/// This class is used to register the input event and return type for the
    FunctionHandler method with the System.Text.Json source generator.
/// There must be a JsonSerializable attribute for each type used as the input and
    return type or a runtime error will occur
/// from the JSON serializer unable to find the serialization information for
    unknown types.
/// </summary>
[JsonSerializable(typeof(string))]
public partial class LambdaFunctionJsonSerializerContext : JsonSerializerContext
{
    // By using this partial class derived from JsonSerializerContext, we can
    generate reflection free JSON Serializer code at compile time

```

```
// which can deserialize our class and properties. However, we must attribute
this class to tell it what types to generate serialization code for.
// See https://docs.microsoft.com/en-us/dotnet/standard/serialization/system-
text-json-source-generation
```

Native AOT mengkompilasi aplikasi Anda menjadi satu biner asli. Titik masuk biner itu adalah metodenya. `static Main` Di dalam `static Main`, runtime Lambda di-bootstrap dan metode disiapkan. `FunctionHandler` Sebagai bagian dari bootstrap runtime, serializer yang dihasilkan sumber dikonfigurasi menggunakan `new SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>()`

2. Untuk menyebarkan aplikasi Anda ke Lambda, pastikan Docker berjalan di lingkungan lokal Anda dan jalankan perintah berikut.

```
dotnet lambda deploy-function
```

Di belakang layar, CLI `global.NET` mengunduh image `AL2023 Docker` dan mengkompilasi kode aplikasi Anda di dalam wadah yang sedang berjalan. Biner yang dikompilasi adalah output kembali ke sistem file lokal Anda sebelum diterapkan ke Lambda.

3. Uji fungsi Anda dengan menjalankan perintah berikut. Ganti `<FUNCTION_NAME>` dengan nama yang Anda pilih untuk fungsi Anda di wizard penerapan.

```
dotnet lambda invoke-function <FUNCTION_NAME> --payload "hello world"
```

Respons dari CLI mencakup detail kinerja untuk start dingin (durasi inisialisasi) dan total waktu berjalan untuk pemanggilan fungsi Anda.

4. Untuk menghapus AWS sumber daya yang Anda buat dengan mengikuti langkah-langkah sebelumnya, jalankan perintah berikut. Ganti `<FUNCTION_NAME>` dengan nama yang Anda pilih untuk fungsi Anda di wizard penerapan. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan tagihan yang tidak perlu ditagih ke Anda. Akun AWS

```
dotnet lambda delete-function <FUNCTION_NAME>
```

Serialisasi

Untuk menyebarkan fungsi ke Lambda menggunakan AOT asli, kode fungsi Anda harus [menggunakan](#) serialisasi yang dihasilkan sumber. Alih-alih menggunakan refleksi run-time untuk

mengumpulkan metadata yang diperlukan untuk mengakses properti objek untuk serialisasi, generator sumber menghasilkan file sumber C# yang dikompilasi saat Anda membangun aplikasi Anda. Untuk mengonfigurasi serializer yang dihasilkan sumber Anda dengan benar, pastikan Anda menyertakan objek input dan output apa pun yang digunakan fungsi Anda, serta jenis kustom apa pun. Misalnya, fungsi Lambda yang menerima peristiwa dari API Gateway REST API dan mengembalikan Product tipe kustom akan menyertakan serializer yang didefinisikan sebagai berikut.

```
[JsonSerializable(typeof(APIGatewayProxyRequest))]  
[JsonSerializable(typeof(APIGatewayProxyResponse))]  
[JsonSerializable(typeof(Product))]  
public partial class CustomSerializer : JsonSerializerContext  
{  
}
```

Pemangkasan

Native AOT memangkas kode aplikasi Anda sebagai bagian dari kompilasi untuk memastikan bahwa biner sekecil mungkin. .NET 8 untuk Lambda memberikan dukungan pemangkasan yang lebih baik dibandingkan dengan versi sebelumnya .NET. Support telah ditambahkan ke [pustaka runtime Lambda](#), [.NET SDK,AWS .NET Lambda Annotations](#), dan [.NET 8](#) itu sendiri.

Peningkatan ini menawarkan potensi untuk menghilangkan peringatan pemangkasan waktu pembuatan, tetapi .NET tidak akan pernah sepenuhnya aman. Ini berarti bahwa bagian pustaka yang diandalkan fungsi Anda dapat dipangkas sebagai bagian dari langkah kompilasi. Anda dapat mengelola ini dengan mendefinisikan `TrimmerRootAssemblies` sebagai bagian dari `.csproj` file Anda seperti yang ditunjukkan pada contoh berikut.

```
<ItemGroup>  
  <TrimmerRootAssembly Include="AWSSDK.Core" />  
  <TrimmerRootAssembly Include="AWSXRayRecorder.Core" />  
  <TrimmerRootAssembly Include="AWSXRayRecorder.Handlers.AwsSdk" />  
  <TrimmerRootAssembly Include="Amazon.Lambda.APIGatewayEvents" />  
  <TrimmerRootAssembly Include="bootstrap" />  
  <TrimmerRootAssembly Include="Shared" />  
</ItemGroup>
```

Perhatikan bahwa saat Anda menerima peringatan trim, menambahkan kelas yang menghasilkan peringatan `TrimmerRootAssembly` mungkin tidak menyelesaikan masalah. Peringatan

trim menunjukkan bahwa kelas mencoba mengakses beberapa kelas lain yang tidak dapat ditentukan hingga runtime. Untuk menghindari kesalahan runtime, tambahkan kelas kedua ini ke `TrimmedRootAssembly`.

Untuk mempelajari selengkapnya tentang mengelola peringatan trim, lihat [Pengantar untuk memangkas peringatan](#) di dokumentasi Microsoft .NET.

Pemecahan Masalah

Kesalahan: Kompilasi asli lintas-OS tidak didukung.

Versi alat Amazon.Lambda.Tools global.NET Core Anda sudah ketinggalan zaman. Perbarui ke versi terbaru dan coba lagi.

Docker: sistem operasi gambar “linux” tidak dapat digunakan pada platform ini.

Docker pada sistem Anda dikonfigurasi untuk menggunakan wadah Windows. Tukar ke wadah Linux untuk menjalankan lingkungan build AOT asli.

Untuk informasi selengkapnya tentang kesalahan umum, lihat repositori [AWS NativeAOT for .NET](#) di GitHub

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi C

Saat Lambda menjalankan fungsi Anda, Lambda meneruskan objek konteks ke [handler](#). Objek ini menyediakan properti dengan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Properti konteks

- `FunctionName` – Nama fungsi Lambda.
- `FunctionVersion` – [Versi](#) fungsi.
- `InvokedFunctionArn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `MemoryLimitInMB` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `AwsRequestId` – Pengidentifikasi permintaan invokasi.
- `LogGroupName` – Grup log untuk fungsi.
- `LogStreamName` – Aliran log untuk instans fungsi.
- `RemainingTime (TimeSpan)` – Jumlah milidetik yang tersisa sebelum waktu eksekusi habis.
- `Identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
- `ClientContext` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
- `Logger` [Objek logger](#) untuk fungsi.

Anda dapat menggunakan informasi dalam `ILambdaContext` objek untuk menampilkan informasi tentang pemanggilan fungsi Anda untuk tujuan pemantauan. Kode berikut memberikan contoh bagaimana menambahkan informasi konteks ke kerangka logging terstruktur. Dalam contoh ini, fungsi `AwsRequestId` menambah output log. Fungsi ini juga menggunakan `RemainingTime` properti untuk membatalkan tugas dalam penerbangan jika batas waktu fungsi Lambda akan tercapai.

```
[assembly:  
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer)  
  
namespace GetProductHandler;
```

```
public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
request, ILambdaContext context)
    {
        Logger.AppendKey("AwsRequestId", context.AwsRequestId);

        var id = request.PathParameters["id"];

        using var cts = new CancellationTokenSource();

        try
        {
            cts.CancelAfter(context.RemainingTime.Add(TimeSpan.FromSeconds(-1)));

            var databaseRecord = await this._repo.GetById(id, cts.Token);

            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.OK,
                Body = JsonSerializer.Serialize(databaseRecord)
            };
        }
        finally
        {
            cts.Cancel();

            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.InternalServerError,
                Body = JsonSerializer.Serialize(databaseRecord)
            };
        }
    }
}
```

Log dan pantau fungsi C# Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda dan mengirim entri log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap pemanggilan dan output lainnya dari kode fungsi Anda ke aliran log. Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Menggunakan alat logging dan pustaka](#)
- [Menggunakan Powertools untuk AWS Lambda \(.NET\) dan AWS SAM untuk logging terstruktur](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)

Membuat fungsi yang mengembalikan log

Untuk menghasilkan log dari kode fungsi, Anda dapat menggunakan metode di [kelas Konsol](#), atau pustaka pencatatan yang menulis ke `stdout` atau `stderr`.

The .NET runtime mencatat REPORT baris START, END, dan untuk setiap pemanggilan. Baris laporan memberikan perincian berikut.

REPORT bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.
- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.

- XRAY TraceId— Untuk permintaan yang dilacak, [ID AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Menggunakan alat logging dan pustaka

[Powertools untuk AWS Lambda \(. NET\)](#) adalah toolkit pengembang untuk mengimplementasikan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang. [Utilitas Logging](#) menyediakan logger yang dioptimalkan Lambda yang mencakup informasi tambahan tentang konteks fungsi di semua fungsi Anda dengan output terstruktur sebagai JSON. Gunakan utilitas ini untuk melakukan hal berikut:

- Tangkap bidang kunci dari konteks Lambda, cold start, dan struktur logging output sebagai JSON
- Log peristiwa pemanggilan Lambda saat diinstruksikan (dinonaktifkan secara default)
- Cetak semua log hanya untuk persentase pemanggilan melalui pengambilan sampel log (dinonaktifkan secara default)
- Tambahkan kunci tambahan ke log terstruktur kapan saja
- Gunakan pemformat log kustom (Bring Your Own Formatter) untuk mengeluarkan log dalam struktur yang kompatibel dengan Logging organisasi Anda RFC

Menggunakan Powertools untuk AWS Lambda (. NET) dan AWS SAM untuk logging terstruktur

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menyebarkan contoh aplikasi Hello World C# dengan [Powertools terintegrasi untuk \(. AWS Lambda NET\)](#) modul menggunakan AWS SAM. Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan hello world pesan.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- . NET6 atau . NET8

- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan TypeScript template Hello World.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type Zip --runtime dotnet6 --no-tracing
```

2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

4. Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

Note

Karena HelloWorldFunction mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

5. Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name sam-app --query 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Memanggil titik API akhir:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

7. Untuk mendapatkan log untuk fungsi tersebut, jalankan [log sam](#). Untuk informasi selengkapnya, lihat [Bekerja dengan log](#) di Panduan AWS Serverless Application Model Pengembang.

```
sam logs --stack-name sam-app
```

Output log terlihat seperti ini:

```
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8
2023-02-20T14:15:27.988000 INIT_START Runtime Version:
dotnet:6.v13 Runtime Version ARN: arn:aws:lambda:ap-
southeast-2::runtime:699f346a05dae24c58c45790bc4089f252bf17dae3997e79b17d939a288aa1ec
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:28.229000
START RequestId: bed25b38-d012-42e7-ba28-f272535fb80e Version: $LATEST
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:29.259000
2023-02-20T14:15:29.201Z bed25b38-d012-42e7-ba28-f272535fb80e info
{"_aws":{"Timestamp":1676902528962,"CloudWatchMetrics":[{"Namespace":"sam-
app-logging","Metrics":[{"Name":"ColdStart","Unit":"Count"}],"Dimensions":
[["FunctionName"],["Service"]]}]},"FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","Service":"PowertoolsHelloWorld","ColdStart":1}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.479000
2023-02-20T14:15:30.479Z bed25b38-d012-42e7-ba28-f272535fb80e info
{"ColdStart":true,"XrayTraceId":"1-63f3807f-5dbcb9910c96f50742707542","CorrelationId":"d3d
a549-4d67b2fdc015","FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionVersion":"$LATEST","FunctionMemorySize":256,"FunctionArn":"arn:aws:lambda:ap-
southeast-2:123456789012:function:sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionRequestId":"bed25b38-d012-42e7-ba28-
f272535fb80e","Timestamp":"2023-02-20T14:15:30.4602970Z","Level":"Information","Service":"Pow
ertoolsHelloWorld","Message":"world API - HTTP 200"}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.599000
2023-02-20T14:15:30.599Z bed25b38-d012-42e7-ba28-f272535fb80e info
{"_aws":{"Timestamp":1676902528922,"CloudWatchMetrics":[{"Namespace":"sam-
app-logging","Metrics":[{"Name":"ApiRequestCount","Unit":"Count"}],"Dimensions":
[["Service"]]}]},"Service":"PowertoolsHelloWorld","ApiRequestCount":1}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.680000 END
RequestId: bed25b38-d012-42e7-ba28-f272535fb80e
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.680000
REPORT RequestId: bed25b38-d012-42e7-ba28-f272535fb80e Duration: 2450.99 ms
Billed Duration: 2451 ms Memory Size: 256 MB Max Memory Used: 74 MB Init
Duration: 240.05 ms
XRAY TraceId: 1-63f3807f-5dbcb9910c96f50742707542 SegmentId: 16b362cd5f52cba0
```

- Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

Mengelola retensi log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log tanpa batas waktu, hapus grup log, atau konfigurasi periode retensi setelah itu secara CloudWatch otomatis menghapus log. Untuk mengatur penyimpanan log, tambahkan yang berikut ini ke AWS SAM templat Anda:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih kelompok log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, sebaiknya instrumentasi fungsi Anda dengan AWS X-Ray X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBULQgUmVxdWVzdElk0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzVlNGZiMjEgVmVyc2lvc21vb... ",
  "ExecutedVersion": "$LATEST"
```



```
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \  
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --  
decode
```

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST  
"AWS_SESSION_TOKEN": "AgoJb3JpZ22luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-  
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0\"", ask/lib:/opt/lib",  
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed  
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15 detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`.

Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
}
{
  "events": [
    {
      "timestamp": 1559763003171,
      "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
      "ingestionTime": 1559763003309
    },
    {
      "timestamp": 1559763003173,
```

```

      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\$LATEST\",
\r ...",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003173,
    "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
    "ingestionTime": 1559763018353
  },
  {
    "timestamp": 1559763003218,
    "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
    "ingestionTime": 1559763018353
  }
],
"nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}

```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Menginstrumentasi kode C # di AWS Lambda

Lambda terintegrasi dengan AWS X-Ray untuk membantu Anda melacak, men-debug, dan mengoptimalkan aplikasi Lambda. Anda dapat menggunakan X-Ray untuk melacak permintaan saat melintasi sumber daya dalam aplikasi Anda, yang mungkin termasuk fungsi Lambda dan layanan lainnya. AWS

Untuk mengirim data penelusuran ke X-Ray, Anda dapat menggunakan salah satu dari tiga SDK pustaka:

- [AWS Distro for OpenTelemetry \(ADOT\)](#) — Distribusi () yang aman, siap produksi, dan AWS didukung (). OpenTelemetry OTel SDK
- [AWS X-Ray SDK for .NET](#)— An SDK untuk menghasilkan dan mengirim data jejak ke X-Ray.
- [Powertools untuk AWS Lambda \(. NET\)](#) - Toolkit pengembang untuk menerapkan praktik terbaik Tanpa Server dan meningkatkan kecepatan pengembang.

Masing-masing SDKs menawarkan cara untuk mengirim data telemetri Anda ke layanan X-Ray. Anda kemudian dapat menggunakan X-Ray untuk melihat, memfilter, dan mendapatkan wawasan tentang metrik kinerja aplikasi Anda untuk mengidentifikasi masalah dan peluang pengoptimalan.

Important

X-Ray dan Powertools untuk AWS Lambda SDKs adalah bagian dari solusi instrumentasi terintegrasi yang ditawarkan oleh. AWS Lapisan ADOT Lambda adalah bagian dari standar industri untuk melacak instrumentasi yang mengumpulkan lebih banyak data secara umum, tetapi mungkin tidak cocok untuk semua kasus penggunaan. Anda dapat menerapkan end-to-end penelusuran di X-Ray menggunakan salah satu solusi. Untuk mempelajari lebih lanjut tentang memilih di antara mereka, lihat [Memilih antara AWS Distro untuk Telemetri Terbuka dan X-Ray. SDKs](#)

Bagian-bagian

- [Menggunakan Powertools untuk AWS Lambda \(. NET\) dan AWS SAM untuk melacak](#)
- [Menggunakan X-Ray SDK untuk instrumen Anda. NETfungsi](#)
- [Mengaktifkan penelusuran dengan konsol Lambda](#)
- [Mengaktifkan penelusuran dengan Lambda API](#)

- [Mengaktifkan penelusuran dengan AWS CloudFormation](#)
- [Menafsirkan jejak X-Ray](#)

Menggunakan Powertools untuk AWS Lambda (.NET) dan AWS SAM untuk melacak

Ikuti langkah-langkah di bawah ini untuk mengunduh, membangun, dan menerapkan contoh aplikasi Hello World C# dengan [Powertools terintegrasi untuk \(. AWS Lambda NET\)](#) modul menggunakan AWS SAM. Aplikasi ini mengimplementasikan API backend dasar dan menggunakan Powertools untuk memancarkan log, metrik, dan jejak. Ini terdiri dari titik akhir Amazon API Gateway dan fungsi Lambda. Saat Anda mengirim GET permintaan ke titik akhir API Gateway, fungsi Lambda memanggil, mengirim log dan metrik menggunakan Format Metrik Tertanam CloudWatch ke, dan mengirimkan jejak ke. AWS X-Ray Fungsi mengembalikan pesan hello world.

Prasyarat

Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- .NET6 atau .NET8
- [AWS CLI versi 2](#)
- [AWS SAM CLI versi 1.75 atau yang lebih baru](#). Jika Anda memiliki versi yang lebih lama AWS SAM CLI, lihat [Memutakhirkan file. AWS SAM CLI](#)

Menyebarkan aplikasi sampel AWS SAM

1. Inisialisasi aplikasi menggunakan TypeScript template Hello World.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type Zip --runtime dotnet6 --no-tracing
```


2. Bangun aplikasi.

```
cd sam-app && sam build
```

3. Terapkan aplikasi.

```
sam deploy --guided
```

- Ikuti petunjuk di layar. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

 Note

Karena `HelloWorldFunction` mungkin tidak memiliki otorisasi yang ditentukan, Apakah ini baik-baik saja? , pastikan untuk masuk.

- Dapatkan aplikasi yang digunakan: URL

```
aws cloudformation describe-stacks --stack-name sam-app --query  
'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

- Memanggil titik API akhir:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Jika berhasil, Anda akan melihat tanggapan ini:

```
{"message":"hello world"}
```

- Untuk mendapatkan jejak untuk fungsi tersebut, jalankan [jejak sam](#).

```
aws sam traces
```

Output jejak terlihat seperti ini:

```
New XRay Service Graph  
Start time: 2023-02-20 23:05:16+08:00  
End time: 2023-02-20 23:05:16+08:00  
Reference Id: 0 - AWS::Lambda - sam-app-HelloWorldFunction-pNjub7mEoew - Edges:  
[1]  
  Summary_statistics:  
    - total requests: 1  
    - ok count(2XX): 1  
    - error count(4XX): 0  
    - fault count(5XX): 0  
    - total response time: 2.814  
Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-pNjub7mEoew  
- Edges: []
```

```
Summary_statistics:
```

- total requests: 1
- ok count(2XX): 1
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 2.429

```
Reference Id: 2 - (Root) AWS::ApiGateway::Stage - sam-app/Prod - Edges: [0]
```

```
Summary_statistics:
```

- total requests: 1
- ok count(2XX): 1
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 2.839

```
Reference Id: 3 - client - sam-app/Prod - Edges: [2]
```

```
Summary_statistics:
```

- total requests: 0
- ok count(2XX): 0
- error count(4XX): 0
- fault count(5XX): 0
- total response time: 0

```
XRay Event [revision 3] at (2023-02-20T23:05:16.521000) with id
(1-63f38c2c-270200b1d292a442c8e8a00) and duration (2.877s)
```

- 2.839s - sam-app/Prod [HTTP: 200]
- 2.836s - Lambda [HTTP: 200]
- 2.814s - sam-app-HelloWorldFunction-pNjujb7mEoew [HTTP: 200]
- 2.429s - sam-app-HelloWorldFunction-pNjujb7mEoew
- 0.230s - Initialization
- 2.389s - Invocation
- 0.600s - ## FunctionHandler
 - 0.517s - Get Calling IP
- 0.039s - Overhead

8. Ini adalah API titik akhir publik yang dapat diakses melalui internet. Kami menyarankan Anda menghapus titik akhir setelah pengujian.

```
sam delete
```

X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan

5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Menggunakan X-Ray SDK untuk instrumen Anda. NETfungsi

Anda dapat menggunakan instrumen kode fungsi Anda untuk merekam metadata dan melacak panggilan downstream. Untuk merekam detail tentang panggilan yang dilakukan fungsi Anda ke sumber daya dan layanan lain, gunakan file AWS X-Ray SDK for .NET. Untuk mendapatkan SDK, tambahkan `AWSXRayRecorder` paket ke file proyek Anda.

```
<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.SQSEvents" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.Json" Version="2.1.0" />
    <PackageReference Include="AWSSDK.Core" Version="3.7.103.24" />
    <PackageReference Include="AWSSDK.Lambda" Version="3.7.104.3" />
    <PackageReference Include="AWSXRayRecorder.Core" Version="2.13.0" />
    <PackageReference Include="AWSXRayRecorder.Handlers.AwsSdk" Version="2.11.0" />
  </ItemGroup>
</Project>
```

Ada berbagai paket Nuget yang menyediakan instrumentasi otomatis untuk AWS SDKs, Entity Framework dan permintaan. HTTP Untuk melihat set lengkap opsi konfigurasi, lihat [AWS X-Ray SDK untuk .NET](#) di Panduan AWS X-Ray Pengembang.

Setelah Anda menambahkan paket Nuget yang diinginkan, konfigurasi instrumentasi otomatis. Praktik terbaik adalah melakukan konfigurasi ini di luar fungsi handler fungsi Anda. Hal ini memungkinkan Anda untuk mengambil keuntungan dari penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Dalam contoh kode berikut, `RegisterXRayForAllServices` metode ini dipanggil dalam konstruktor fungsi untuk menambahkan instrumentasi untuk semua AWS SDK panggilan.

```
[assembly:
  LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer
```



```
namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        // Add auto instrumentation for all AWS SDK calls
        // It is important to call this method before initializing any SDK clients
        AWSSDKHandler.RegisterXRayForAllServices();
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Mengaktifkan penelusuran dengan konsol Lambda

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.

6. Pilih Simpan.

Mengaktifkan penelusuran dengan Lambda API

Konfigurasi penelusuran pada fungsi Lambda Anda dengan AWS CLI AWS SDK atau, gunakan operasi berikut API:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \  
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Lambda::Function  
    Properties:  
      TracingConfig:  
        Mode: Active  
      ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Menafsirkan jejak X-Ray

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

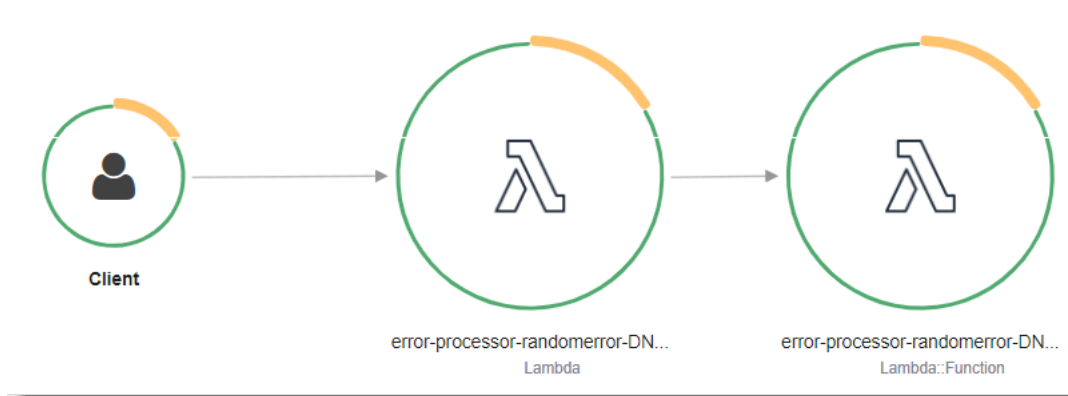
Setelah mengonfigurasi penelusuran aktif, Anda dapat mengamati permintaan tertentu melalui aplikasi Anda. [Grafik layanan X-Ray](#) menunjukkan informasi tentang aplikasi Anda dan semua komponennya. Contoh berikut menunjukkan aplikasi dengan dua fungsi. Fungsi utama memproses kejadian dan terkadang mengembalikan kesalahan. Fungsi kedua di bagian atas memproses kesalahan yang muncul di grup log pertama dan menggunakan AWS SDK untuk memanggil X-Ray, Amazon Simple Storage Service (Amazon S3), dan Amazon Logs. CloudWatch



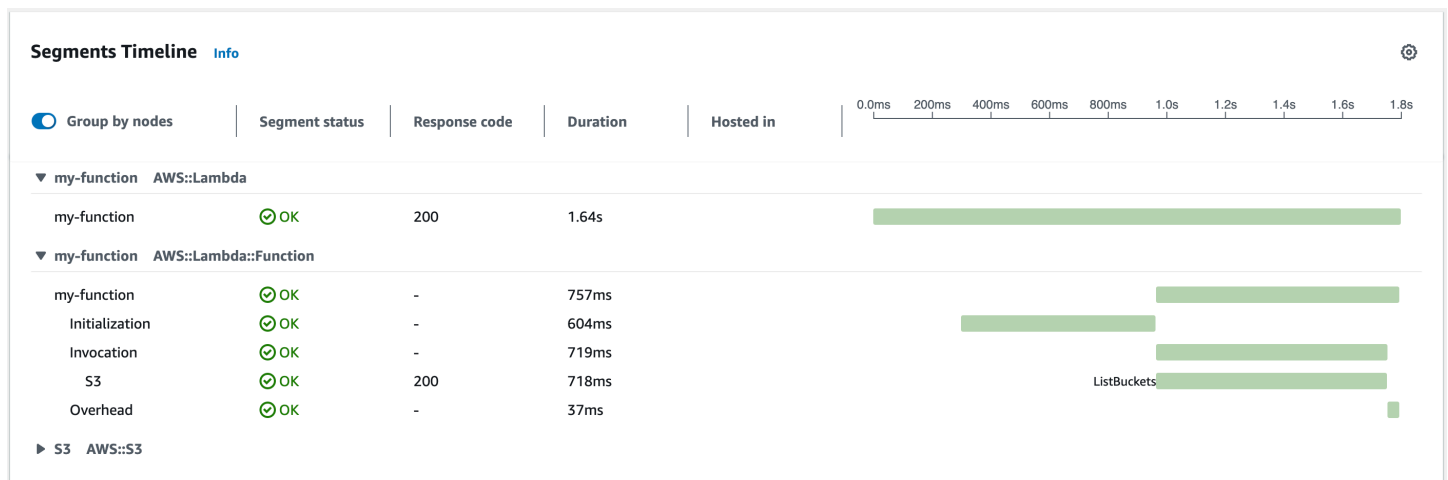
X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan

5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda. Contoh berikut menunjukkan jejak dengan dua segmen ini. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal `usul`. `AWS::Lambda::Function` Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.



Contoh ini memperluas `AWS::Lambda::Function` segmen untuk menunjukkan tiga subsegmennya.

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen jejak yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Contoh jejak yang ditunjukkan di sini menggambarkan segmen fungsi gaya lama. Perbedaan antara segmen gaya lama dan baru dijelaskan dalam paragraf berikut. Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Segmen fungsi gaya lama berisi subsegmen berikut:

- Inisialisasi – Mewakili waktu yang dihabiskan untuk memuat fungsi dan menjalankan [kode inisialisasi](#). Subsegmen ini hanya muncul untuk peristiwa pertama yang diproses oleh setiap instance fungsi Anda.
- Doa - Merupakan waktu yang dihabiskan untuk menjalankan kode handler Anda.
- Overhead - Merupakan waktu yang dihabiskan runtime Lambda untuk mempersiapkan diri untuk menangani acara berikutnya.

Segmen fungsi gaya baru tidak berisi subsegmen. Invocation Sebagai gantinya, subsegmen pelanggan dilampirkan langsung ke segmen fungsi. Untuk informasi lebih lanjut tentang struktur segmen fungsi gaya lama dan baru, lihat. [the section called “Memahami jejak X-Ray”](#)

Anda juga dapat instrumen HTTP klien, merekam SQL kueri, dan membuat subsegmen kustom dengan anotasi dan metadata. Untuk informasi selengkapnya, lihat [AWS X-Ray SDK for .NET](#) di Panduan AWS X-Ray Pengembang.

Harga

Anda dapat menggunakan penelusuran X-Ray secara gratis setiap bulan hingga batas tertentu sebagai bagian dari Tingkat AWS Gratis. Di luar ambang batas itu, X-Ray mengenakan biaya untuk penyimpanan dan pengambilan jejak. Untuk informasi lebih lanjut, lihat [Harga AWS X-Ray](#).

AWS Lambdapengujian fungsi di C

Note

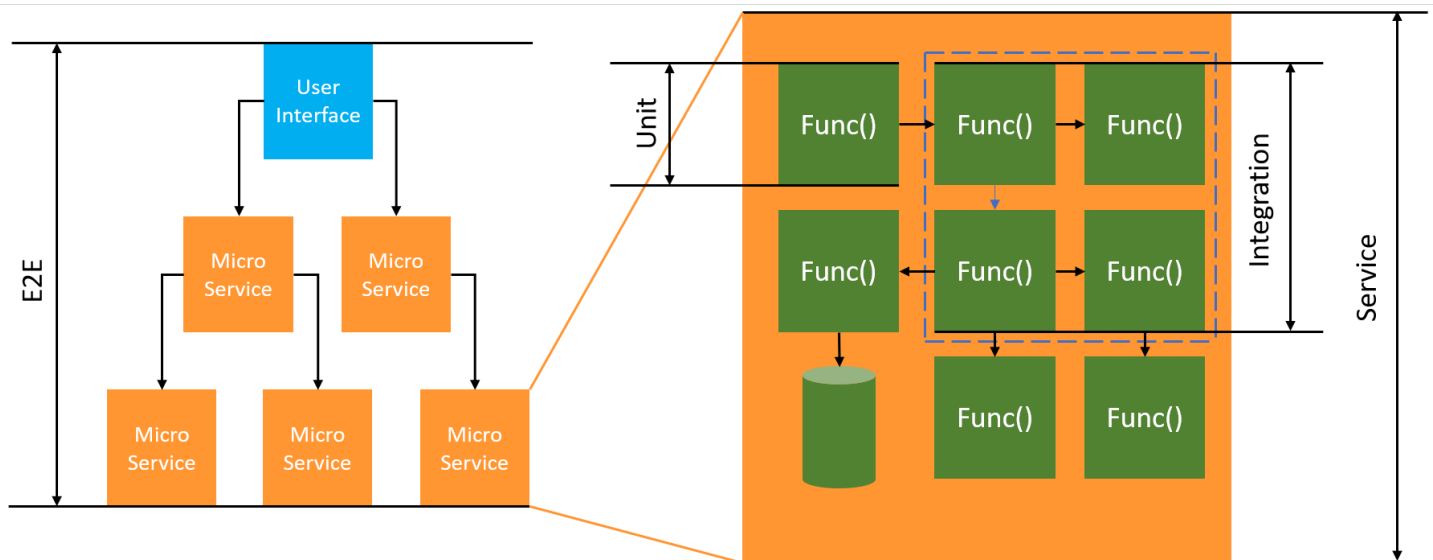
Lihat bagian [Fungsi pengujian](#) untuk pengenalan lengkap tentang teknik dan praktik terbaik untuk menguji solusi tanpa server.

Menguji fungsi tanpa server menggunakan jenis dan teknik pengujian tradisional, tetapi Anda juga harus mempertimbangkan pengujian aplikasi tanpa server secara keseluruhan. Pengujian berbasis cloud akan memberikan ukuran kualitas yang paling akurat dari fungsi dan aplikasi tanpa server Anda.

Arsitektur aplikasi tanpa server mencakup layanan terkelola yang menyediakan fungsionalitas aplikasi penting melalui panggilan API. Untuk alasan ini, siklus pengembangan Anda harus menyertakan pengujian otomatis yang memverifikasi fungsionalitas saat fungsi dan layanan Anda berinteraksi.

Jika Anda tidak membuat pengujian berbasis cloud, Anda dapat mengalami masalah karena perbedaan antara lingkungan lokal dan lingkungan yang diterapkan. Proses integrasi berkelanjutan Anda harus menjalankan pengujian terhadap serangkaian sumber daya yang disediakan di cloud sebelum mempromosikan kode Anda ke lingkungan penerapan berikutnya, seperti QA, Staging, atau Production.

Lanjutkan membaca panduan singkat ini untuk mempelajari strategi pengujian untuk aplikasi tanpa server, atau kunjungi [repositori Sampel Uji Tanpa Server](#) untuk menyelami contoh-contoh praktis, khusus untuk bahasa dan runtime pilihan Anda.



Untuk pengujian tanpa server, Anda masih akan menulis unit, integrasi, dan end-to-end pengujian.

- Tes unit - Tes yang dijalankan terhadap blok kode yang terisolasi. Misalnya, memverifikasi logika bisnis untuk menghitung biaya pengiriman yang diberikan item dan tujuan tertentu.
- Tes integrasi - Tes yang melibatkan dua atau lebih komponen atau layanan yang berinteraksi, biasanya di lingkungan cloud. Misalnya, memverifikasi fungsi memproses peristiwa dari antrian.
- End-to-end tes - Tes yang memverifikasi perilaku di seluruh aplikasi. Misalnya, memastikan infrastruktur diatur dengan benar dan bahwa peristiwa mengalir antar layanan seperti yang diharapkan untuk merekam pesanan pelanggan.

Menguji aplikasi tanpa server

Anda biasanya akan menggunakan campuran pendekatan untuk menguji kode aplikasi tanpa server Anda, termasuk pengujian di cloud, pengujian dengan tiruan, dan kadang-kadang menguji dengan emulator.

Pengujian di cloud

Pengujian di cloud sangat berharga untuk semua fase pengujian, termasuk pengujian unit, pengujian integrasi, dan end-to-end pengujian. Anda menjalankan pengujian terhadap kode yang diterapkan di cloud dan berinteraksi dengan layanan berbasis cloud. Pendekatan ini memberikan ukuran kualitas kode Anda yang paling akurat.

Cara mudah untuk men-debug fungsi Lambda Anda di cloud adalah melalui konsol dengan acara pengujian. Peristiwa pengujian adalah input JSON ke fungsi Anda. Jika fungsi Anda tidak

memerlukan input, acara dapat berupa dokumen ({}) JSON kosong. Konsol menyediakan contoh peristiwa untuk berbagai integrasi layanan. Setelah membuat acara di konsol, Anda dapat membagikannya dengan tim Anda untuk membuat pengujian lebih mudah dan konsisten.

Note

[Menguji fungsi di konsol](#) adalah cara cepat untuk memulai, tetapi mengotomatiskan siklus pengujian Anda memastikan kualitas aplikasi dan kecepatan pengembangan.

Alat pengujian

Untuk mempercepat siklus pengembangan Anda, ada sejumlah alat dan teknik yang dapat Anda gunakan saat menguji fungsi Anda. Misalnya, [mode AWS SAM Akselerasi](#) dan [AWS CDK tonton](#) mengurangi waktu yang diperlukan untuk memperbarui lingkungan cloud.

Cara Anda mendefinisikan kode fungsi Lambda Anda membuatnya mudah untuk menambahkan pengujian unit. Lambda membutuhkan konstruktor publik tanpa parameter untuk menginisialisasi kelas Anda. Memperkenalkan konstruktor internal kedua memberi Anda kendali atas dependensi yang digunakan aplikasi Anda.

```
[assembly:
  LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function(): this(null)
    {
    }

    internal Function(IDatabaseRepository repo)
    {
        this._repo = repo ?? new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
request)
```



```
{
    var id = request.PathParameters["id"];

    var databaseRecord = await this._repo.GetById(id);

    return new APIGatewayProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = JsonSerializer.Serialize(databaseRecord)
    };
}
```

Untuk menulis tes untuk fungsi ini, Anda dapat menginisialisasi instance baru Function kelas Anda dan meneruskan implementasi tiruan dari `IDatabaseRepository` Contoh di bawah ini menggunakan `XUnitMoq`, dan `FluentAssertions` untuk menulis tes sederhana memastikan `FunctionHandler` pengembalian kode status 200.

```
using Xunit;
using Moq;
using FluentAssertions;

public class FunctionTests
{
    [Fact]
    public async Task TestLambdaHandler_WhenInputIsValid_ShouldReturn200StatusCode()
    {
        // Arrange
        var mockDatabaseRepository = new Mock<IDatabaseRepository>();

        var functionUnderTest = new Function(mockDatabaseRepository.Object);

        // Act
        var response = await functionUnderTest.FunctionHandler(new
        APIGatewayProxyRequest());

        // Assert
        response.StatusCode.Should().Be(200);
    }
}
```

Untuk contoh yang lebih rinci, termasuk contoh pengujian asinkron, lihat repositori [sampel pengujian .NET](#) pada GitHub

Membangun fungsi Lambda dengan PowerShell

Bagian berikut menjelaskan bagaimana pola pemrograman umum dan konsep inti berlaku ketika Anda membuat kode fungsi Lambda. PowerShell

Lambda menyediakan contoh aplikasi berikut untuk: PowerShell

- [blank-powershell](#) — PowerShell Fungsi yang menunjukkan penggunaan logging, variabel lingkungan, dan SDK. AWS

Sebelum memulai, Anda harus terlebih dahulu mengatur lingkungan PowerShell pengembangan. Untuk petunjuk tentang cara melakukannya, lihat [Menyiapkan Lingkungan PowerShell Pembangunan](#).

Untuk mempelajari cara menggunakan AWSLambdaPSCore modul untuk mengunduh PowerShell proyek sampel dari templat, membuat paket PowerShell penerapan, dan menerapkan PowerShell fungsi ke AWS Cloud, lihat. [Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip](#)

Lambda menyediakan runtime berikut untuk bahasa.NET:

.NET

| Nama | Pengidentifikasi | Sistem operasi | Tanggal pengusangan | Buat fungsi blok | Pembaruan fungsi blok |
|--------|------------------|-------------------|---------------------|-------------------|-----------------------|
| .NET 8 | dotnet8 | Amazon Linux 2023 | | | |
| .NET 6 | dotnet6 | Amazon Linux 2 | 20 Des 2024 | Februari 28, 2025 | 31 Mar 2025 |

Topik

- [Menyiapkan Lingkungan PowerShell Pembangunan](#)
- [Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip](#)
- [Tentukan penanganan fungsi Lambda di PowerShell](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi PowerShell](#)
- [Log dan pantau fungsi Powershell Lambda](#)

Menyiapkan Lingkungan PowerShell Pembangunan

Lambda menyediakan seperangkat alat dan pustaka untuk runtime. PowerShell Untuk petunjuk penginstalan, lihat [Alat Lambda untuk PowerShell aktif](#). GitHub

AWSLambdaPSCore Modul ini mencakup cmdlet berikut untuk membantu penulis dan mempublikasikan fungsi Lambda PowerShell :

- Dapatkan- `AWSPowerShellLambdaTemplate` — Mengembalikan daftar template memulai.
- New- `AWSPowerShellLambda` — Membuat PowerShell skrip awal berdasarkan template.
- Publikasikan- `AWSPowerShellLambda` — Menerbitkan PowerShell skrip yang diberikan ke Lambda.
- Baru- `AWSPowerShellLambdaPackage` — Membuat paket penyebaran Lambda yang dapat Anda gunakan dalam sistem CI/CD untuk penyebaran.

Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip

Paket penerapan untuk PowerShell runtime berisi PowerShell skrip Anda, PowerShell modul yang diperlukan untuk PowerShell skrip Anda, dan rakitan yang diperlukan untuk meng-host Core.

PowerShell

Buat fungsi Lambda

Untuk mulai menulis dan menjalankan PowerShell skrip dengan Lambda, Anda dapat menggunakan `New-AWSPowerShell11Lambda` cmdlet untuk membuat skrip pemula berdasarkan templat. Anda dapat menggunakan cmdlet `Publish-AWSPowerShell11Lambda` untuk men-deploy skrip Anda ke Lambda. Kemudian, Anda dapat menguji skrip Anda melalui baris perintah atau konsol Lambda.

Untuk membuat PowerShell skrip baru, unggah, dan uji, lakukan hal berikut:

1. Untuk menampilkan daftar templat yang tersedia, jalankan perintah berikut:

```
PS C:\> Get-AWSPowerShell11LambdaTemplate

Template          Description
-----          -
Basic             Bare bones script
CodeCommitTrigger Script to process AWS CodeCommit Triggers
...
```

2. Untuk membuat skrip sampel berdasarkan templat `Basic`, jalankan perintah berikut:

```
New-AWSPowerShell11Lambda -ScriptName MyFirstPSScript -Template Basic
```

File baru bernama `MyFirstPSScript.ps1` dibuat di subdirektori baru dari direktori saat ini. Nama direktori didasarkan pada parameter `-ScriptName`. Anda dapat menggunakan parameter `-Directory` untuk memilih direktori alternatif.

Anda dapat melihat file baru tersebut memiliki konten berikut:

```
# PowerShell script file to run as a Lambda function
#
# When executing in Lambda the following variables are predefined.
# $LambdaInput - A PSObject that contains the Lambda function input data.
# $LambdaContext - An Amazon.Lambda.Core.ILambdaContext object that contains
information about the currently running Lambda environment.
```

```
#
# The last item in the PowerShell pipeline is returned as the result of the Lambda
function.
#
# To include PowerShell modules with your Lambda function, like the
AWSPowerShell.NetCore module, add a "#Requires" statement
# indicating the module and version.

#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}

# Uncomment to send the input to CloudWatch Logs
# Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
```

3. Untuk melihat bagaimana pesan log dari PowerShell skrip Anda dikirim ke Amazon CloudWatch Logs, batalkan komentar pada `Write-Host` baris skrip sampel.

Untuk mendemonstrasikan bagaimana Anda dapat mengembalikan data dari fungsi Lambda Anda, tambahkan garis baru di akhir skrip dengan `$PSVersionTable`. Ini menambah `$PSVersionTable` ke PowerShell pipa. Setelah PowerShell skrip selesai, objek terakhir dalam PowerShell pipeline adalah data pengembalian untuk fungsi Lambda. `$PSVersionTable` adalah variabel PowerShell global yang juga memberikan informasi tentang lingkungan berjalan.

Setelah membuat perubahan ini, dua baris terakhir dari skrip sampel akan terlihat seperti ini:

```
Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
$PSVersionTable
```

4. Setelah mengedit file `MyFirstPSScript.ps1`, ubah direktori ke lokasi skrip. Kemudian jalankan perintah berikut untuk menerbitkan skrip ke Lambda:

```
Publish-AWSPowerShellLambda -ScriptPath .\MyFirstPSScript.ps1 -Name
MyFirstPSScript -Region us-east-2
```

Perhatikan bahwa parameter `-Name` menentukan nama fungsi Lambda, yang muncul di konsol Lambda. Anda dapat menggunakan fungsi ini untuk mengaktifkan skrip Anda secara manual.

5. Panggil fungsi Anda menggunakan perintah AWS Command Line Interface (AWS CLI) `invoke`.

```
> aws lambda invoke --function-name MyFirstPSScript out
```

Tentukan penanganan fungsi Lambda di PowerShell

Ketika fungsi Lambda dipanggil, penanganan Lambda memanggil skrip. PowerShell

Ketika PowerShell skrip dipanggil, variabel-variabel berikut telah ditentukan sebelumnya:

- **\$ LambdaInput** — Sebuah PObject yang berisi input ke handler. Input ini dapat berupa data peristiwa (diterbitkan oleh sumber peristiwa) atau input kustom yang Anda berikan, seperti string atau objek data kustom apa pun.
- **\$ LambdaContext** — LambdaContext Objek Amazon.Lambda.Core.I yang dapat Anda gunakan untuk mengakses informasi tentang pemanggilan saat ini—seperti nama fungsi saat ini, batas memori, waktu eksekusi yang tersisa, dan pencatatan.

Misalnya, perhatikan PowerShell contoh kode berikut.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}  
Write-Host 'Function Name:' $LambdaContext.FunctionName
```

Script ini mengembalikan FunctionName properti yang diperoleh dari LambdaContext variabel \$.

Note

Anda diminta untuk menggunakan `#Requires` pernyataan dalam PowerShell skrip Anda untuk menunjukkan modul yang menjadi sandaran skrip Anda. Pernyataan ini melakukan dua tugas penting. 1) Ini berkomunikasi dengan pengembang lain modul mana yang digunakan skrip, dan 2) mengidentifikasi modul dependen yang perlu dikemas AWS PowerShell alat dengan skrip, sebagai bagian dari penerapan. Untuk informasi selengkapnya tentang `#Requires` pernyataan di PowerShell, lihat [Tentang membutuhkan](#). Untuk informasi selengkapnya tentang paket PowerShell penerapan, lihat [Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip](#).

Saat fungsi PowerShell Lambda Anda menggunakan AWS PowerShell cmdlet, pastikan untuk menetapkan `#Requires` pernyataan yang mereferensikan `AWSPowerShell.NetCore` modul, yang mendukung PowerShell Core—dan bukan modul, yang hanya mendukung Windows. `AWSPowerShell PowerShell` Selain itu, pastikan untuk menggunakan versi 3.3.270.0 atau yang lebih baru dari `AWSPowerShell.NetCore` yang mengoptimalkan proses impor cmdlet. Jika Anda menggunakan versi lama, Anda

akan mengalami proses mulai dari awal dalam waktu yang lebih lama. Untuk informasi selengkapnya, lihat [AWS Alat untuk PowerShell](#).

Mengembalikan data

Beberapa invokasi Lambda dimaksudkan untuk mengembalikan data ke pemanggilnya. Misalnya, jika invokasi adalah sebagai respons terhadap permintaan web yang berasal dari API Gateway, fungsi Lambda kita harus mengembalikan respons tersebut. Untuk PowerShell Lambda, objek terakhir yang ditambahkan ke PowerShell pipeline adalah data pengembalian dari pemanggilan Lambda. Jika objek berupa string, data akan dikembalikan apa adanya. Jika tidak, objek dikonversi ke JSON dengan menggunakan cmdlet `ConvertTo-Json`.

Misalnya, perhatikan PowerShell pernyataan berikut, yang `$PSVersionTable` menambah PowerShell pipa:

```
$PSVersionTable
```

Setelah PowerShell skrip selesai, objek terakhir dalam PowerShell pipeline adalah data pengembalian untuk fungsi Lambda. `$PSVersionTable` adalah variabel PowerShell global yang juga memberikan informasi tentang lingkungan berjalan.

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi PowerShell

Ketika Lambda menjalankan fungsi Anda, hal ini melewati informasi konteks dengan membuat variabel `$LambdaContext` tersedia untuk [handler](#). Variabel ini menyediakan metode dan properti dengan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Properti konteks

- `FunctionName` – Nama fungsi Lambda.
- `FunctionVersion` – [Versi](#) fungsi.
- `InvokedFunctionArn`— Amazon Resource Name (ARN) yang digunakan untuk menjalankan fungsi. Menunjukkan jika pemicu menyebutkan nomor versi atau alias.
- `MemoryLimitInMB` – Jumlah memori yang dialokasikan untuk fungsi tersebut.
- `AwsRequestId` – Pengidentifikasi permintaan invokasi.
- `LogGroupName` – Grup log untuk fungsi.
- `LogStreamName` – Aliran log untuk instans fungsi.
- `RemainingTime` – Jumlah milidetik yang tersisa sebelum waktu eksekusi habis.
- `Identity` – (aplikasi seluler) Informasi tentang identitas Amazon Cognito yang mengesahkan permintaan.
- `ClientContext` – (aplikasi seluler) Konteks klien yang disediakan untuk Lambda oleh aplikasi klien.
- `Logger` – [Objek logger](#) untuk fungsi.

Cuplikan PowerShell kode berikut menunjukkan fungsi handler sederhana yang mencetak beberapa informasi konteks.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host 'Function name:' $LambdaContext.FunctionName
Write-Host 'Remaining milliseconds:' $LambdaContext.RemainingTime.TotalMilliseconds
Write-Host 'Log group name:' $LambdaContext.LogGroupName
Write-Host 'Log stream name:' $LambdaContext.LogStreamName
```

Log dan pantau fungsi Powershell Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda dan mengirim log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap invokasi ke pengaliran log, dan menyampaikan log serta output lain dari kode fungsi Anda. Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch log Log dengan Lambda](#).

Halaman ini menjelaskan cara menghasilkan keluaran log dari kode fungsi Lambda Anda, dan mengakses log menggunakan AWS Command Line Interface, konsol Lambda, atau konsol. CloudWatch

Bagian-bagian

- [Membuat fungsi yang mengembalikan log](#)
- [Melihat log di konsol Lambda](#)
- [Melihat log di CloudWatch konsol](#)
- [Melihat log menggunakan AWS Command Line Interface \(AWS CLI\)](#)
- [Menghapus log](#)

Membuat fungsi yang mengembalikan log

[Untuk mengeluarkan log dari kode fungsi, Anda dapat menggunakan cmdlet di Microsoft PowerShell.Utility](#), atau modul logging apa pun yang menulis ke stdout atau stderr. Contoh berikut menggunakan Write-Host.

Example [function/Handler.ps1](#) – Pencatatan

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host `## Environment variables
Write-Host AWS_LAMBDA_FUNCTION_VERSION=$Env:AWS_LAMBDA_FUNCTION_VERSION
Write-Host AWS_LAMBDA_LOG_GROUP_NAME=$Env:AWS_LAMBDA_LOG_GROUP_NAME
Write-Host AWS_LAMBDA_LOG_STREAM_NAME=$Env:AWS_LAMBDA_LOG_STREAM_NAME
Write-Host AWS_EXECUTION_ENV=$Env:AWS_EXECUTION_ENV
Write-Host AWS_LAMBDA_FUNCTION_NAME=$Env:AWS_LAMBDA_FUNCTION_NAME
Write-Host PATH=$Env:PATH
Write-Host `## Event
Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 3)
```

Example format log

```

START RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Version: $LATEST
Importing module ./Modules/AWSPowerShell.NetCore/3.3.618.0/AWSPowerShell.NetCore.psd1
[Information] - ## Environment variables
[Information] - AWS_LAMBDA_FUNCTION_VERSION=$LATEST
[Information] - AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/blank-powershell-
function-18CIXMPLHFAJJ
[Information] - AWS_LAMBDA_LOG_STREAM_NAME=2020/04/01/
[$LATEST]53c5xmpl52d64ed3a744724d9c201089
[Information] - AWS_EXECUTION_ENV=AWS_Lambda_dotnet6_powershell_1.0.0
[Information] - AWS_LAMBDA_FUNCTION_NAME=blank-powershell-function-18CIXMPLHFAJJ
[Information] - PATH=/var/lang/bin:/usr/local/bin:/usr/bin:/bin:/opt/bin
[Information] - ## Event
[Information] -
{
  "Records": [
    {
      "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1523232000000",
        "SenderId": "123456789012",
        "ApproximateFirstReceiveTimestamp": "1523232000001"
      },
      ...
    }
  ]
}
END RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed
REPORT RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Duration: 3906.38 ms Billed
Duration: 4000 ms Memory Size: 512 MB Max Memory Used: 367 MB Init Duration: 5960.19
ms
XRAY TraceId: 1-5e843da6-733cxmple7d0c3c020510040 SegmentId: 3913xmpl20999446 Sampled:
true

```

Runtime .NET mencatat baris START, END, dan REPORT untuk setiap invokasi. Baris laporan memberikan perincian berikut.

Laporkan bidang data baris

- RequestId— ID permintaan unik untuk pemanggilan.

- Durasi – Jumlah waktu yang digunakan oleh metode handler fungsi Anda gunakan untuk memproses peristiwa.
- Durasi yang Ditagih – Jumlah waktu yang ditagihkan untuk invokasi.
- Ukuran Memori – Jumlah memori yang dialokasikan untuk fungsi.
- Memori Maks yang Digunakan – Jumlah memori yang digunakan oleh fungsi.
- Durasi Init – Untuk permintaan pertama yang dilayani, lama waktu yang diperlukan runtime untuk memuat fungsi dan menjalankan kode di luar metode handler.
- XRAY TraceId — Untuk permintaan yang dilacak, ID [AWS X-Ray jejak](#).
- SegmentId— Untuk permintaan yang dilacak, ID segmen X-Ray.
- Diambil Sampel – Untuk permintaan yang dilacak, hasil pengambilan sampel.

Melihat log di konsol Lambda

Anda dapat menggunakan konsol Lambda untuk melihat output log setelah Anda memanggil fungsi Lambda.

Jika kode Anda dapat diuji dari editor Kode tertanam, Anda akan menemukan log dalam hasil eksekusi. Saat Anda menggunakan fitur pengujian konsol untuk menjalankan fungsi, Anda akan menemukan Keluaran Log di bagian Detail.

Melihat log di CloudWatch konsol

Anda dapat menggunakan CloudWatch konsol Amazon untuk melihat log untuk semua pemanggilan fungsi Lambda.

Untuk melihat log di CloudWatch konsol

1. Buka [halaman Grup log](#) di CloudWatch konsol.
2. Pilih grup log untuk fungsi Anda (`/aws/lambda/your-function-name`).
3. Pilih pengaliran log.

Setiap aliran log sesuai dengan [instans fungsi Anda](#). Pengaliran log muncul saat Anda memperbarui fungsi Lambda dan saat instans tambahan dibuat untuk menangani beberapa invokasi bersamaan. Untuk menemukan log untuk pemanggilan tertentu, kami sarankan untuk menginstrumentasi fungsi Anda dengan [AWS X-Ray](#). AWS X-Ray mencatat detail tentang permintaan dan pengaliran log di jejak.

Melihat log menggunakan AWS Command Line Interface (AWS CLI)

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBU1QgUmVxdWVzdE1k0iA4N2QwNDRi0C1mMTU0LTExZTgt0GNkYS0y0Tc0YzV1NGZiMjEgVmVyc2lvb...",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas base64 untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`.

Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0""",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan skrip berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15 detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "statusCode": 200,
  "executedVersion": "$LATEST"
}
{
  "events": [
    {
      "timestamp": 1559763003171,
      "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
      "ingestionTime": 1559763003309
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n",
\r ...",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
      "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
```



```
      "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
  MB\t\n",
      "ingestionTime": 1559763018353
    }
  ],
  "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
  "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Menghapus log

Grup log tidak terhapus secara otomatis ketika Anda menghapus suatu fungsi. Untuk menghindari penyimpanan log secara tidak terbatas, hapus kelompok log, atau [lakukan konfigurasi periode penyimpanan](#), yang setelahnya log akan dihapus secara otomatis.

Membangun fungsi Lambda dengan Rust

Karena Rust mengkompilasi ke kode asli, Anda tidak memerlukan runtime khusus untuk menjalankan kode Rust di Lambda. Sebagai gantinya, gunakan [klien runtime Rust](#) untuk membangun proyek Anda secara lokal, lalu terapkan ke Lambda menggunakan runtime atau `provided.al2023` atau `provided.al2`. Saat Anda menggunakan `provided.al2023` atau `provided.al2`, Lambda secara otomatis menjaga sistem operasi tetap up to date dengan patch terbaru.

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

Alat dan pustaka untuk Rust

- [AWS SDK for Rust](#): AWS SDK for Rust menyediakan Rust API untuk berinteraksi dengan layanan infrastruktur Amazon Web Services.
- [Klien runtime Rust untuk Lambda](#): Klien runtime Rust adalah paket eksperimental. Hal ini dapat melanggar perubahan dan tidak direkomendasikan untuk produksi.
- [Cargo Lambda](#): Perpustakaan ini menyediakan aplikasi baris perintah untuk bekerja dengan fungsi Lambda yang dibangun dengan Rust.
- [Lambda HTTP](#): Pustaka ini menyediakan pembungkus untuk bekerja dengan peristiwa HTTP.
- [Ekstensi Lambda](#): Pustaka ini menyediakan dukungan untuk menulis Ekstensi Lambda dengan Rust.
- [AWS Lambda Peristiwa](#): Pustaka ini menyediakan definisi tipe untuk integrasi sumber peristiwa umum.

Contoh aplikasi Lambda untuk Rust

- Fungsi [Lambda Dasar: Fungsi](#) Rust yang menunjukkan cara memproses peristiwa dasar.
- [Fungsi Lambda dengan penanganan kesalahan](#): Fungsi Rust yang menunjukkan cara menangani kesalahan Rust khusus di Lambda.
- [Fungsi Lambda dengan sumber daya bersama](#): Proyek Rust yang menginisialisasi sumber daya bersama sebelum membuat fungsi Lambda.

- [Peristiwa HTTP Lambda](#): Fungsi Rust yang menangani peristiwa HTTP.
- [Peristiwa Lambda HTTP dengan header CORS](#): Fungsi Rust yang menggunakan Tower untuk menyuntikkan header CORS.
- [Lambda REST API](#): REST API yang menggunakan Axum dan Diesel untuk terhubung ke database PostgreSQL.
- [Demo Rust Tanpa Server](#): Proyek Rust yang menunjukkan penggunaan pustaka Lambda Rust, logging, variabel lingkungan, dan SDK. AWS
- Ekstensi [Lambda Dasar: Ekstensi](#) Rust yang menunjukkan cara memproses peristiwa ekstensi dasar.
- [Lambda Logs Amazon Data Firehose Extension: Ekstensi](#) Rust yang menunjukkan cara mengirim log Lambda ke Firehose.

Topik

- [Tentukan penangan fungsi Lambda di Rust](#)
- [Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Rust](#)
- [Memproses peristiwa HTTP dengan Rust](#)
- [Menyebarkan fungsi Rust Lambda dengan arsip file.zip](#)
- [Log dan pantau fungsi Rust Lambda](#)

Tentukan penanganan fungsi Lambda di Rust

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

Handler fungsi Lambda Anda adalah metode dalam kode fungsi Anda yang memproses peristiwa. Saat fungsi Anda diaktifkan, Lambda menjalankan metode handler. Fungsi Anda berjalan sampai handler mengembalikan respons, keluar, atau waktu habis.

Topik

- [Dasar-dasar penanganan karat](#)
- [Menggunakan status bersama](#)
- [Praktik terbaik kode untuk fungsi Rust Lambda](#)

Dasar-dasar penanganan karat

Tulis kode fungsi Lambda Anda sebagai Rust yang dapat dieksekusi. Menerapkan kode fungsi handler dan fungsi utama dan termasuk yang berikut:

- Peti [lambda_runtime](#) dari crates.io, yang mengimplementasikan model pemrograman Lambda untuk Rust.
- Sertakan [Tokio dalam dependensi](#) Anda. [Klien runtime Rust untuk Lambda](#) menggunakan Tokio untuk menangani panggilan asinkron.

Example - Rust handler yang memproses peristiwa JSON

Contoh berikut menggunakan peti [serde_json](#) untuk memproses peristiwa dasar: JSON

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};

async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}
```

```
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Perhatikan hal berikut:

- `use`: Mengimpor pustaka yang dibutuhkan fungsi Lambda Anda.
- `async fn main`: Titik masuk yang menjalankan kode fungsi Lambda. Klien runtime Rust menggunakan [Tokio](#) sebagai runtime async, jadi Anda harus membubuhi keterangan fungsi utama dengan `#[tokio::main]`
- `async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error>`: Ini adalah tanda tangan penanganan Lambda. Ini termasuk kode yang berjalan ketika fungsi dipanggil.
 - `LambdaEvent<Value>`: Ini adalah tipe generik yang menjelaskan peristiwa yang diterima oleh runtime Lambda serta konteks fungsi [Lambda](#).
 - `Result<Value, Error>`: Fungsi mengembalikan `Result` tipe. Jika fungsinya berhasil, hasilnya adalah JSON nilai. Jika fungsinya tidak berhasil, hasilnya adalah kesalahan.

Menggunakan status bersama

Anda dapat mendeklarasikan variabel bersama yang independen dari kode handler fungsi Lambda Anda. Variabel ini dapat membantu Anda memuat informasi status selama [Fase inisialisasi](#), sebelum fungsi Anda menerima peristiwa apa pun.

Example — Bagikan klien Amazon S3 di seluruh instance fungsi

Perhatikan hal berikut:

- `use aws_sdk_s3::Client`: Contoh ini mengharuskan Anda untuk menambahkan `aws-sdk-s3 = "0.26.0"` ke daftar dependensi dalam file `AndaCargo.toml`.
- `aws_config::from_env`: Contoh ini mengharuskan Anda untuk menambahkan `aws-config = "0.55.1"` ke daftar dependensi dalam file `AndaCargo.toml`.

```
use aws_sdk_s3::Client;
use lambda_runtime::{service_fn, Error, LambdaEvent};
use serde::{Deserialize, Serialize};
```

```

#[derive(Deserialize)]
struct Request {
    bucket: String,
}

#[derive(Serialize)]
struct Response {
    keys: Vec<String>,
}

async fn handler(client: &Client, event: LambdaEvent<Request>) -> Result<Response,
Error> {
    let bucket = event.payload.bucket;
    let objects = client.list_objects_v2().bucket(bucket).send().await?;
    let keys = objects
        .contents()
        .map(|s| s.iter().flat_map(|o| o.key().map(String::from)).collect())
        .unwrap_or_default();
    Ok(Response { keys })
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    let shared_config = aws_config::from_env().load().await;
    let client = Client::new(&shared_config);
    let shared_client = &client;
    lambda_runtime::run(service_fn(move |event: LambdaEvent<Request>| async move {
        handler(&shared_client, event).await
    })))
    .await
}

```

Praktik terbaik kode untuk fungsi Rust Lambda

Patuhi pedoman dalam daftar berikut untuk menggunakan praktik pengkodean terbaik saat membangun fungsi Lambda Anda:

- Pisahkan handler Lambda dari logika inti Anda. Ini memungkinkan Anda untuk membuat fungsi yang lebih dapat teruji.
- Minimalkan kompleksitas dependensi Anda. Utamakan memilih kerangka kerja lebih sederhana yang cepat dimuat dalam memulai [lingkungan eksekusi](#).

- Minimalkan ukuran paket penerapan Anda sesuai kebutuhan runtime-nya. Ini akan mengurangi jumlah waktu yang dibutuhkan untuk mengunduh dan membongkar paket deployment Anda sebelum invokasi.
- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.
- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs APIPembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [APIreferensi](#) untuk daftar yang tersedia APIs untuk umum.

- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Menggunakan objek konteks Lambda untuk mengambil informasi fungsi Rust

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

Ketika Lambda menjalankan fungsi Anda, ia menambahkan objek konteks ke LambdaEvent yang diterima [handler](#). Objek ini menyediakan properti dengan informasi tentang lingkungan invokasi, fungsi, dan eksekusi.

Properti konteks

- `request_id`: ID AWS permintaan yang dihasilkan oleh layanan Lambda.
- `deadline`: Batas waktu eksekusi untuk pemanggilan saat ini dalam milidetik.
- `invoked_function_arn`: Nama Sumber Daya Amazon (ARN) dari fungsi Lambda yang dipanggil.
- `xray_trace_id`: ID AWS X-Ray jejak untuk pemanggilan saat ini.
- `client_content`: Objek konteks klien dikirim oleh AWS ponselSDK. Bidang ini kosong kecuali fungsi dipanggil menggunakan AWS ponselSDK.
- `identity`: Identitas Amazon Cognito yang memanggil fungsi. Bidang ini kosong kecuali permintaan pemanggilan ke Lambda APIs dibuat menggunakan AWS kredensial yang dikeluarkan oleh kumpulan identitas Amazon Cognito.
- `env_config`: Konfigurasi fungsi Lambda dari variabel lingkungan lokal. Properti ini mencakup informasi seperti nama fungsi, alokasi memori, versi, dan aliran log.

Mengakses informasi konteks aktif

Fungsi Lambda memiliki akses ke metadata tentang lingkungan mereka dan permintaan invokasi. LambdaEventObjek yang diterima oleh penanganan fungsi Anda mencakup context metadata:

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};
```

```
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    let invoked_function_arn = event.context.invoked_function_arn;
    Ok(json!({ "message": format!("Hello, this is function
{invoked_function_arn}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Memproses peristiwa HTTP dengan Rust

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

API Amazon API Gateway, Application Load Balancers, dan [URL fungsi Lambda](#) dapat mengirim peristiwa HTTP ke Lambda. Anda dapat menggunakan peti [aws_lambda_events](#) dari [crates.io](#) untuk [memproses peristiwa](#) dari sumber-sumber ini.

Example — Menangani permintaan proxy API Gateway

Perhatikan hal berikut:

- use `aws_lambda_events::apigw::`{ApiGatewayProxyRequest, ApiGatewayProxyResponse}: Peti [aws_lambda_events mencakup banyak acara](#) Lambda. Untuk mengurangi waktu kompilasi, gunakan flag fitur untuk mengaktifkan acara yang Anda butuhkan. Contoh:`aws_lambda_events = { version = "0.8.3", default-features = false, features = ["apigw"] }`.
- use `http::HeaderMap`: Impor ini mengharuskan Anda untuk menambahkan peti [http](#) ke dependensi Anda.

```
use aws_lambda_events::apigw::{ApiGatewayProxyRequest, ApiGatewayProxyResponse};
use http::HeaderMap;
use lambda_runtime::{service_fn, Error, LambdaEvent};

async fn handler(
    _event: LambdaEvent<ApiGatewayProxyRequest>,
) -> Result<ApiGatewayProxyResponse, Error> {
    let mut headers = HeaderMap::new();
    headers.insert("content-type", "text/html".parse().unwrap());
    let resp = ApiGatewayProxyResponse {
        status_code: 200,
        multi_value_headers: headers.clone(),
        is_base64_encoded: false,
        body: Some("Hello AWS Lambda HTTP request".into()),
        headers,
```

```

    };
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}

```

[Klien runtime Rust untuk Lambda](#) juga menyediakan abstraksi atas jenis acara ini yang memungkinkan Anda bekerja dengan tipe HTTP asli, terlepas dari layanan mana yang mengirimkan peristiwa. Kode berikut ini setara dengan contoh sebelumnya, dan berfungsi di luar kotak dengan URL fungsi Lambda, Application Load Balancers, dan API Gateway.

Note

[Peti lambda_http menggunakan peti lambda_runtime di bawahnya.](#) Anda tidak perlu mengimpor `lambda_runtime` secara terpisah.

Example — Menangani permintaan HTTP

```

use lambda_http::{service_fn, Error, IntoResponse, Request, RequestExt, Response};

async fn handler(event: Request) -> Result<impl IntoResponse, Error> {
    let resp = Response::builder()
        .status(200)
        .header("content-type", "text/html")
        .body("Hello AWS Lambda HTTP request")
        .map_err(Box::new)?;
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_http::run(service_fn(handler)).await
}

```

Untuk contoh lain tentang cara menggunakan `lambda_http`, lihat [contoh kode http-axum](#) pada repositori Labs. AWS GitHub

Contoh acara HTTP Lambda untuk Rust

- [Peristiwa HTTP Lambda](#): Fungsi Rust yang menangani peristiwa HTTP.
- [Peristiwa Lambda HTTP dengan header CORS](#): Fungsi Rust yang menggunakan Tower untuk menyuntikkan header CORS.
- [Peristiwa HTTP Lambda dengan sumber daya bersama](#): Fungsi Rust yang menggunakan sumber daya bersama yang diinisialisasi sebelum penanganan fungsi dibuat.

Menyebarkan fungsi Rust Lambda dengan arsip file.zip

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

Halaman ini menjelaskan cara mengkompilasi fungsi Rust Anda, dan kemudian menerapkan biner yang dikompilasi untuk AWS Lambda menggunakan Cargo [Lambda](#). Ini juga menunjukkan bagaimana menerapkan biner yang dikompilasi dengan AWS Command Line Interface dan AWS Serverless Application Model CLI

Bagian-bagian

- [Prasyarat](#)
- [Membangun fungsi Rust di macOS, Windows, atau Linux](#)
- [Menerapkan biner fungsi Rust dengan Cargo Lambda](#)
- [Memanggil fungsi Rust Anda dengan Cargo Lambda](#)

Prasyarat

- [Karat](#)
- [AWS Command Line Interface \(AWS CLI\) versi 2](#)

Membangun fungsi Rust di macOS, Windows, atau Linux

[Langkah-langkah berikut menunjukkan cara membuat proyek untuk fungsi Lambda pertama Anda dengan Rust dan mengompilasinya dengan Cargo Lambda.](#)

1. Instal Cargo Lambda, subperintah Cargo, yang mengkompilasi fungsi Rust untuk Lambda di macOS, Windows, dan Linux.

Untuk menginstal Cargo Lambda pada sistem apa pun yang telah menginstal Python 3, gunakan pip:

```
pip3 install cargo-lambda
```

Untuk menginstal Cargo Lambda di macOS atau Linux, gunakan Homebrew:

```
brew tap cargo-lambda/cargo-lambda
brew install cargo-lambda
```

[Untuk menginstal Cargo Lambda di Windows, gunakan Scoop:](#)

```
scoop bucket add cargo-lambda
scoop install cargo-lambda/cargo-lambda
```

Untuk opsi lain, lihat [Instalasi](#) di dokumentasi Cargo Lambda.

2. Buat struktur paket. Perintah ini membuat beberapa kode fungsi dasar `src/main.rs`. Anda dapat menggunakan kode ini untuk menguji atau menggantinya dengan kode Anda sendiri.

```
cargo lambda new my-function
```

3. Di dalam direktori root paket, jalankan subperintah [build](#) untuk mengkompilasi kode dalam fungsi Anda.

```
cargo lambda build --release
```

(Opsional) Jika Anda ingin menggunakan AWS Graviton2 di Lambda, tambahkan `--arm64` bendera untuk mengkompilasi kode Anda. ARM CPUs

```
cargo lambda build --release --arm64
```

4. Sebelum menerapkan fungsi Rust Anda, konfigurasi AWS kredensial pada mesin Anda.

```
aws configure
```

Menerapkan biner fungsi Rust dengan Cargo Lambda

Gunakan subperintah [deploy](#) untuk menyebarkan biner yang dikompilasi ke Lambda. Perintah ini menciptakan [peran eksekusi](#) dan kemudian membuat fungsi Lambda. Untuk menentukan peran eksekusi yang ada, gunakan [flag `--iam-role`](#).

```
cargo lambda deploy my-function
```

Menerapkan biner fungsi Rust Anda dengan AWS CLI

Anda juga dapat menerapkan biner Anda dengan file. AWS CLI

1. Gunakan subperintah [build](#) untuk membangun paket deployment .zip.

```
cargo lambda build --release --output-format zip
```

2. [Untuk menyebarkan paket.zip ke Lambda, jalankan perintah create-function.](#)

- Untuk `--runtime`, tentukan `provided.al2023`. Ini adalah runtime [khusus OS](#). Runtime khusus OS digunakan untuk menyebarkan binari yang dikompilasi dan runtime khusus ke Lambda.
- Untuk `--role`, tentukan ARN [peran eksekusi](#).

```
aws lambda create-function \  
  --function-name my-function \  
  --runtime provided.al2023 \  
  --role arn:aws:iam::111122223333:role/lambda-role \  
  --handler rust.handler \  
  --zip-file fileb://target/lambda/my-function/bootstrap.zip
```

Menerapkan biner fungsi Rust Anda dengan AWS SAM CLI

Anda juga dapat menerapkan biner Anda dengan file. AWS SAM CLI

1. Buat AWS SAM template dengan definisi sumber daya dan properti. Untuk Runtime, tentukan `provided.al2023`. Ini adalah runtime [khusus OS](#). Runtime khusus OS digunakan untuk menyebarkan binari yang dikompilasi dan runtime khusus ke Lambda.

Untuk informasi selengkapnya tentang penerapan fungsi Lambda AWS SAM menggunakan, [AWSlihat: :Serverless: :Function](#) dalam Panduan Pengembang.AWS Serverless Application Model

Example SAMdefinisi sumber daya dan properti untuk biner Rust

```
AWSTemplateFormatVersion: '2010-09-09'  
Transform: AWS::Serverless-2016-10-31  
Description: SAM template for Rust binaries  
Resources:  
  RustFunction:  
    Type: AWS::Serverless::Function  
    Properties:  
      CodeUri: target/lambda/my-function/  
      Handler: rust.handler  
      Runtime: provided.al2023  
Outputs:  
  RustFunction:  
    Description: "Lambda Function ARN"  
    Value: !GetAtt RustFunction.Arn
```

- Gunakan subperintah [build](#) untuk mengkompilasi fungsi.

```
cargo lambda build --release
```

- Gunakan perintah [sam deploy](#) untuk menyebarkan fungsi ke Lambda.

```
sam deploy --guided
```

Untuk informasi selengkapnya tentang membangun fungsi Rust dengan AWS SAM CLI, lihat [Membangun fungsi Lambda Karat dengan Cargo Lambda](#) di Panduan Pengembang.AWS Serverless Application Model

Memanggil fungsi Rust Anda dengan Cargo Lambda

Gunakan subperintah [pemanggilan](#) untuk menguji fungsi Anda dengan payload.

```
cargo lambda invoke --remote --data-ascii '{"command": "Hello world"}' my-function
```

Memanggil fungsi Rust Anda dengan AWS CLI

Anda juga dapat menggunakan AWS CLI untuk menjalankan fungsi.

```
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --  
payload '{"command": "Hello world"}' /tmp/out.txt
```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Log dan pantau fungsi Rust Lambda

Note

[Klien runtime Rust](#) adalah paket eksperimental. Hal ini dapat berubah dan dimaksudkan hanya untuk tujuan evaluasi.

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda dan mengirim log ke Amazon. CloudWatch Fungsi Lambda Anda dilengkapi dengan grup CloudWatch log Log dan aliran log untuk setiap instance fungsi Anda. Lingkungan runtime Lambda mengirimkan detail tentang setiap invokasi ke pengaliran log, dan menyampaikan log serta output lain dari kode fungsi Anda. Untuk informasi selengkapnya, lihat [Menggunakan CloudWatch log Log dengan Lambda](#). Halaman ini menjelaskan cara menghasilkan output log dari kode fungsi Lambda Anda.

Membuat fungsi yang menulis log

Untuk mengeluarkan log dari kode fungsi Anda, Anda dapat menggunakan fungsi logging apa pun yang menulis ke `stdout` atau `stderr`, seperti `println!` makro. Contoh berikut digunakan `println!` untuk mencetak pesan ketika fungsi handler dimulai dan sebelum selesai.

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    println!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    println!("Rust function responds to {}", &first_name);
    Ok(json!({ "message": format!("Hello, {}!", first_name) }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Menerapkan logging lanjutan dengan peti Tracing

[Tracing](#) adalah kerangka kerja untuk menginstrumentasi program Rust untuk mengumpulkan informasi diagnostik berbasis peristiwa yang terstruktur. Kerangka kerja ini menyediakan utilitas

untuk menyesuaikan tingkat dan format keluaran logging, seperti membuat pesan log JSON terstruktur. Untuk menggunakan framework ini, Anda harus menginisialisasi subscriber sebelum mengimplementasikan fungsi handler. Kemudian, Anda dapat menggunakan melacak makro seperti `debug`, `info`, dan `error`, untuk menentukan tingkat logging yang Anda inginkan untuk setiap skenario.

Example — Menggunakan peti Tracing

Perhatikan hal berikut:

- `tracing_subscriber::fmt().json()`: Ketika opsi ini disertakan, log diformat dalam JSON. Untuk menggunakan opsi ini, Anda harus menyertakan `json` fitur dalam `tracing-subscriber` ketergantungan (misalnya, `tracing-subscriber = { version = "0.3.11", features = ["json"] }`).
- `#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]`: Anotasi ini menghasilkan rentang setiap kali handler dipanggil. Rentang menambahkan ID permintaan ke setiap baris log.
- `{ %first_name }`: Konstruksi ini menambahkan `first_name` bidang ke baris log tempat ia digunakan. Nilai untuk bidang ini sesuai dengan variabel dengan nama yang sama.

```
use lambda_runtime::{service_fn, Error, LambdaEvent};
use serde_json::{json, Value};
#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    tracing::info!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    tracing::info!({ %first_name }, "Rust function responds to event");
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt().json()
        .with_max_level(tracing::Level::INFO)
        // this needs to be set to remove duplicated information in the log.
        .with_current_span(false)
        // this needs to be set to false, otherwise ANSI color codes will
        // show up in a confusing manner in CloudWatch logs.
        .with_ansi(false)
}
```

```
// disabling time is handy because CloudWatch will add the ingestion time.
.without_time()
// remove the name of the function from every log entry
.with_target(false)
.init();
lambda_runtime::run(service_fn(handler)).await
}
```

Ketika fungsi Rust ini dipanggil, ia mencetak dua baris log yang mirip dengan yang berikut ini:

```
{"level":"INFO","fields":{"message":"Rust function invoked"},"spans":
[{"req_id":"45daaaa7-1a72-470c-9a62-e79860044bb5","name":"handler"}]}
{"level":"INFO","fields":{"message":"Rust function responds to
event","first_name":"David"},"spans":[{"req_id":"45daaaa7-1a72-470c-9a62-
e79860044bb5","name":"handler"}]}
```

Praktik terbaik untuk bekerja dengan AWS Lambda fungsi

Berikut adalah praktik terbaik yang direkomendasikan untuk menggunakan AWS Lambda:

Topik

- [Kode fungsi](#)
- [Konfigurasi fungsi](#)
- [Skalabilitas fungsi](#)
- [Metrik dan alarm](#)
- [Bekerja dengan stream](#)
- [Praktik terbaik keamanan](#)

Kode fungsi

- Manfaatkan penggunaan kembali lingkungan eksekusi untuk meningkatkan kinerja fungsi Anda. Inisialisasi SDK klien dan koneksi database di luar fungsi handler, dan cache aset statis secara lokal di direktori. /tmp Invokasi selanjutnya yang diproses oleh instans yang sama dari fungsi Anda dapat menggunakan kembali sumber daya ini. Ini menghemat biaya dengan mengurangi waktu pengoperasian fungsi.

Untuk menghindari potensi kebocoran data di seluruh invokasi, jangan menggunakan lingkungan eksekusi untuk menyimpan data pengguna, peristiwa, atau informasi lainnya implikasi keamanan. Jika fungsi Anda bergantung pada status yang dapat disenyapkan yang tidak dapat disimpan dalam memori di dalam handler, pertimbangkan untuk membuat fungsi terpisah atau versi terpisah dari fungsi untuk setiap pengguna.

- Gunakan arahan keep-alive untuk mempertahankan koneksi yang persisten. Lambda membersihkan koneksi idle dari waktu ke waktu. Mencoba menggunakan ulang koneksi idle saat mengidentifikasi suatu fungsi akan menyebabkan kesalahan koneksi. Untuk mempertahankan koneksi yang persisten, gunakan arahan tetap aktif yang berkaitan dengan runtime Anda. Sebagai contoh, lihat [Menggunakan Kembali Koneksi dengan Keep-Alive di Node.js](#).
- Gunakan [variabel lingkungan](#) untuk meneruskan parameter operasional ke fungsi Anda. Misalnya, jika Anda ingin menulis ke bucket Amazon S3 alih-alih melakukan hard-coding nama bucket yang Anda tulis, konfigurasi nama bucket sebagai variabel lingkungan.

- Hindari menggunakan pemanggilan rekursif dalam fungsi Lambda Anda, di mana fungsi memanggil dirinya sendiri atau memulai proses yang dapat memanggil fungsi lagi. Hal ini dapat menyebabkan volume invokasi fungsi yang tidak diinginkan dan peningkatan biaya. Jika Anda melihat volume pemanggilan yang tidak diinginkan, setelah konkurensi fungsi cadangan untuk 0 segera membatasi semua pemanggilan ke fungsi, saat Anda memperbarui kode.
- Jangan gunakan non-dokumen, non-publik APIs dalam kode fungsi Lambda Anda. Untuk runtime AWS Lambda terkelola, Lambda secara berkala menerapkan pembaruan keamanan dan fungsional ke internal Lambda. APIs API Pembaruan internal ini mungkin tidak kompatibel ke belakang, yang menyebabkan konsekuensi yang tidak diinginkan seperti kegagalan pemanggilan jika fungsi Anda memiliki ketergantungan pada non-publik ini. APIs Lihat [API referensi](#) untuk daftar yang tersedia APIs untuk umum.
- Tulis kode idempoten. Menulis kode idempoten untuk fungsi Anda memastikan bahwa peristiwa duplikat ditangani dengan cara yang sama. Kode Anda harus memvalidasi peristiwa dengan benar dan menangani peristiwa duplikat dengan anggun. Untuk informasi selengkapnya, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten?](#) .

Untuk praktik terbaik kode khusus bahasa, lihat bagian berikut:

- [the section called “Praktik terbaik kode untuk fungsi Lambda Node.js”](#)
- [the section called “Praktik terbaik kode untuk fungsi Lambda TypeScript”](#)
- [the section called “Praktik terbaik kode untuk fungsi Lambda Python”](#)
- [the section called “Praktik terbaik kode untuk fungsi Ruby Lambda”](#)
- [the section called “Praktik terbaik kode untuk fungsi Java Lambda”](#)
- [the section called “Praktik terbaik kode untuk fungsi Go Lambda”](#)
- [the section called “Praktik terbaik kode untuk fungsi C# Lambda”](#)
- [the section called “Praktik terbaik kode untuk fungsi Rust Lambda”](#)

Konfigurasi fungsi

- Pengujian kinerja fungsi Lambda Anda merupakan bagian penting dalam memastikan Anda memilih konfigurasi ukuran memori yang optimal. Setiap peningkatan ukuran memori memicu peningkatan yang setara dalam CPU tersedia untuk fungsi Anda. [Penggunaan memori untuk fungsi Anda ditentukan per pemanggilan dan dapat dilihat di Amazon. CloudWatch](#) Dari setiap invokasi, entri REPORT : akan dibuat, sebagaimana ditunjukkan di bawah ini:

```
REPORT RequestId: 3604209a-e9a3-11e6-939a-754dd98c7be3 Duration: 12.34 ms Billed
Duration: 100 ms Memory Size: 128 MB Max Memory Used: 18 MB
```

Dengan menganalisis bidang `Max Memory Used`:, Anda dapat menentukan apakah fungsi Anda perlu memori lebih besar atau jika ukuran memori fungsi Anda disediakan secara berlebihan.

Untuk menemukan konfigurasi memori yang tepat untuk fungsi Anda, sebaiknya gunakan proyek [AWS Lambda Power Tuning](#) open source. Untuk informasi selengkapnya, lihat [AWS Lambda Power Tuning aktif](#). GitHub

Untuk mengoptimalkan kinerja fungsi, kami juga merekomendasikan penerapan pustaka yang dapat memanfaatkan `Advanced Vector Extensions 2 (AVX2)`. Ini memungkinkan Anda untuk memproses beban kerja yang menuntut, termasuk inferensi pembelajaran mesin, pemrosesan media, komputasi kinerja tinggi (HPC), simulasi ilmiah, dan pemodelan keuangan. Untuk informasi selengkapnya, lihat [Membuat AWS Lambda fungsi yang lebih cepat dengan AVX2](#).

- Uji muatan fungsi Lambda Anda untuk menentukan nilai waktu habis yang optimal. Penting untuk menganalisis berapa lama fungsi Anda berjalan sehingga Anda dapat menentukan dengan lebih baik setiap masalah dengan layanan dependensi yang dapat meningkatkan konkurensi fungsi di luar yang Anda harapkan. Hal ini penting terutama ketika fungsi Lambda Anda melakukan panggilan jaringan ke sumber daya yang mungkin tidak menangani penskalaan Lambda.
- Gunakan izin yang paling membatasi saat menyetel kebijakan. IAM Pahami sumber daya dan operasional kebutuhan fungsi Lambda Anda, dan batasi peran eksekusi ke izin ini. Untuk informasi selengkapnya, lihat [Mengelola izin di AWS Lambda](#).
- Jadilah akrab dengan [Kuota Lambda](#). Ukuran muatan, deskriptor file, dan ruang `/tmp` sering diabaikan saat menentukan batas sumber daya runtime.
- Hapus fungsi Lambda yang tidak lagi Anda gunakan. Dengan melakukannya, fungsi yang tidak digunakan tidak dihitung sia-sia terhadap batas ukuran paket deployment Anda.
- Jika Anda menggunakan Amazon Simple Queue Service sebagai sumber peristiwa, pastikan nilai dari waktu invokasi fungsi yang diharapkan tidak melebihi nilai [Visibility Timeout](#) di antrean. Ini berlaku baik untuk [CreateFunction](#) dan [UpdateFunctionConfiguration](#).
 - Dalam kasus `CreateFunction`, AWS Lambda akan gagal proses pembuatan fungsi.
 - Dalam kasus `UpdateFunctionConfiguration`, itu dapat menghasilkan duplikat pemanggilan fungsi.

Skalabilitas fungsi

- Biasakan diri dengan kendala throughput hulu dan hilir Anda. Sementara fungsi Lambda berskala mulus dengan beban, dependensi hulu dan hilir mungkin tidak memiliki kemampuan throughput yang sama. Jika Anda perlu membatasi seberapa tinggi skala fungsi Anda, Anda dapat [mengonfigurasi konkurensi cadangan](#) pada fungsi Anda.
- Bangun toleransi throttle. Jika fungsi sinkron Anda mengalami pelambatan karena lalu lintas melebihi laju penskalaan Lambda, Anda dapat menggunakan strategi berikut untuk meningkatkan toleransi throttle:
 - Gunakan [batas waktu, percobaan ulang, dan backoff](#) dengan jitter. Menerapkan strategi ini memperlancar pemanggilan yang dicoba ulang, dan membantu memastikan Lambda dapat meningkatkan skala dalam hitungan detik untuk meminimalkan pelambatan pengguna akhir.
 - Gunakan [konkurensi yang disediakan](#). Konkurensi yang disediakan adalah jumlah lingkungan eksekusi pra-inisialisasi yang dialokasikan Lambda ke fungsi Anda. Lambda menangani permintaan masuk menggunakan konkurensi yang disediakan bila tersedia. Lambda juga dapat menskalakan fungsi Anda di atas dan di luar pengaturan konkurensi yang disediakan jika diperlukan. Mengkonfigurasi konkurensi yang disediakan menimbulkan biaya tambahan ke akun Anda. AWS

Metrik dan alarm

- Gunakan [Lihat metrik untuk fungsi Lambda](#) dan [CloudWatch Alarm](#) alih-alih membuat atau memperbarui metrik dari dalam kode fungsi Lambda Anda. Ini adalah cara yang jauh lebih efisien untuk melacak kondisi fungsi Lambda Anda, memungkinkan Anda mengetahui masalah di awal proses pengembangan. Misalnya, Anda dapat mengonfigurasi alarm berdasarkan perkiraan durasi invokasi fungsi Lambda Anda untuk mengatasi hambatan atau keterlambatan yang terkait dengan kode fungsi Anda.
- Manfaatkan library logging dan [AWS Lambda Metrics and Dimensions](#) untuk menangkap error aplikasi (mis. ERR, ERROR, WARNING, dll.)
- Gunakan Deteksi [Anomali AWS Biaya untuk mendeteksi](#) aktivitas yang tidak biasa di akun Anda. Deteksi Anomali Biaya menggunakan pembelajaran mesin untuk terus memantau biaya dan penggunaan Anda sambil meminimalkan peringatan positif palsu. Deteksi Anomali Biaya menggunakan data dari AWS Cost Explorer, yang memiliki penundaan hingga 24 jam. Akibatnya, diperlukan waktu hingga 24 jam untuk mendeteksi anomali setelah penggunaan terjadi. Untuk

memulai dengan Deteksi Anomali Biaya, Anda harus terlebih dahulu [mendaftar ke Cost Explorer](#). Kemudian, [akses Deteksi Anomali Biaya](#).

Bekerja dengan stream

- Uji dengan batch dan ukuran catatan berbeda sehingga frekuensi polling dari tiap sumber peristiwa disesuaikan dengan seberapa cepat fungsi Anda mampu menyelesaikan tugasnya. [CreateEventSourceMapping](#) BatchSize Parameter mengontrol jumlah maksimum catatan yang dapat dikirim ke fungsi Anda dengan setiap pemanggilan. Ukuran batch yang lebih besar sering kali dapat menyerap overhead secara lebih efisien di serangkaian catatan yang lebih besar, sehingga meningkatkan throughput Anda.

Secara default, Lambda memanggil fungsi Anda segera setelah catatan tersedia. Jika batch yang dibaca Lambda dari sumber peristiwa hanya memiliki satu catatan di dalamnya, Lambda hanya mengirimkan satu catatan ke fungsi tersebut. Untuk menghindari menjalankan fungsi dengan sejumlah kecil catatan, Anda dapat memberi tahu sumber acara untuk menyangga catatan hingga 5 menit dengan mengonfigurasi jendela batching. Sebelum menjalankan fungsi, Lambda terus membaca catatan dari sumber acara hingga mengumpulkan batch penuh, jendela batching kedaluwarsa, atau batch mencapai batas muatan 6 MB. Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

- Tingkatkan throughput pemrosesan aliran Kinesis dengan menambahkan pecahan. Stream Kinesis terdiri dari satu atau lebih shard. Tingkat di mana Lambda dapat membaca data dari skala Kinesis secara linier dengan jumlah pecahan. Peningkatan jumlah shard akan secara langsung meningkatkan jumlah maksimal invokasi fungsi Lambda konkuren dan dapat meningkatkan throughput pemrosesan aliran Kinesis Anda. Untuk informasi selengkapnya tentang hubungan antara pecahan dan pemanggilan fungsi, lihat [the section called “Polling dan batching stream”](#). Jika Anda meningkatkan jumlah serpihan dalam pengaliran Kinesis, pastikan Anda sudah memilih

kunci partisi yang baik (lihat [Kunci Partisi](#)) untuk data Anda, sehingga catatan terkait berakhir pada serpihan yang sama dan data Anda terdistribusi dengan baik.

- Gunakan [CloudWatchAmazon](#) IteratorAge untuk menentukan apakah aliran Kinesis Anda sedang diproses. Misalnya, konfigurasi CloudWatch alarm dengan pengaturan maksimum hingga 30000 (30 detik).

Praktik terbaik keamanan

- Pantau penggunaan Anda AWS Lambda karena berkaitan dengan praktik terbaik keamanan dengan menggunakan AWS Security Hub. Hub Keamanan menggunakan kontrol keamanan untuk mengevaluasi konfigurasi sumber daya dan standar keamanan guna membantu Anda mematuhi berbagai kerangka kerja kepatuhan. Untuk informasi selengkapnya tentang penggunaan Security Hub guna mengevaluasi sumber daya Lambda, lihat [AWS Lambda kontrol](#) di AWS Security Hub Panduan Pengguna.
- Pantau log aktivitas jaringan Lambda menggunakan Amazon Lambda GuardDuty Protection. GuardDuty Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan saat fungsi Lambda dipanggil di perangkat Anda. Akun AWS Misalnya, jika salah satu fungsi Anda menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency. GuardDuty memantau log aktivitas jaringan yang dihasilkan saat fungsi Lambda dipanggil. Untuk mempelajari selengkapnya, lihat [Perlindungan Lambda](#) di GuardDuty Panduan Pengguna Amazon.

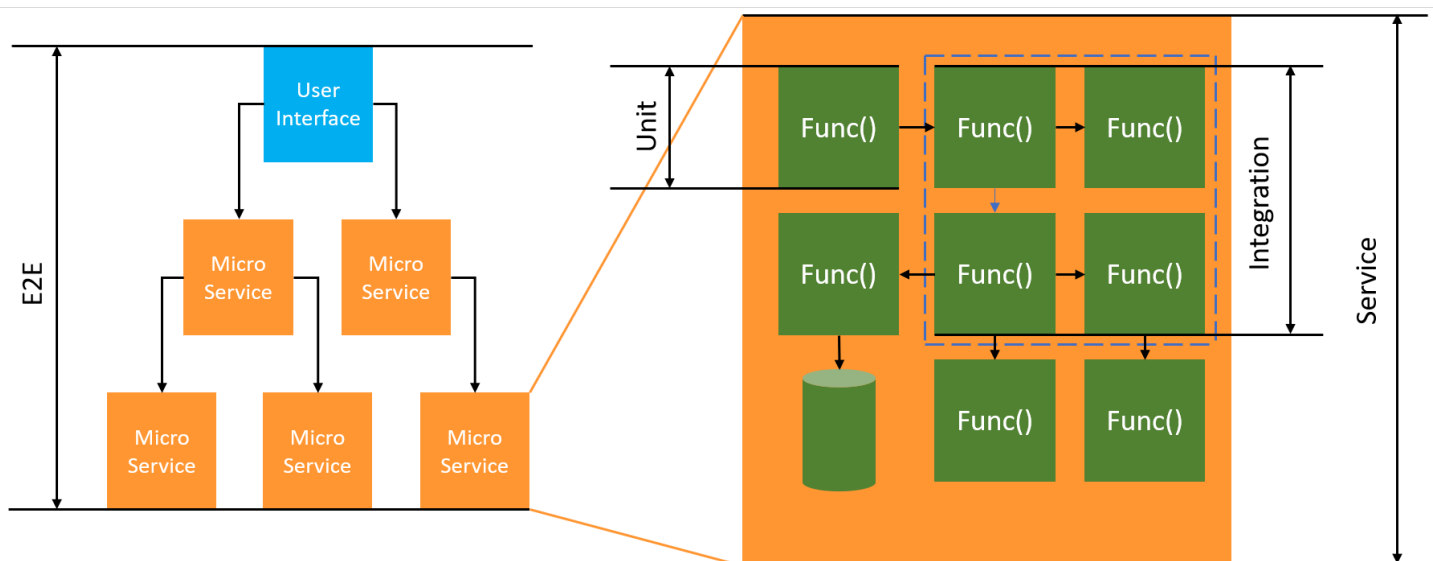
Cara menguji fungsi dan aplikasi tanpa server

Menguji fungsi tanpa server menggunakan jenis dan teknik pengujian tradisional, tetapi Anda juga harus mempertimbangkan pengujian aplikasi tanpa server secara keseluruhan. Pengujian berbasis cloud akan memberikan ukuran kualitas yang paling akurat dari fungsi dan aplikasi tanpa server Anda.

Arsitektur aplikasi tanpa server mencakup layanan terkelola yang menyediakan fungsionalitas aplikasi penting melalui API panggilan. Untuk alasan ini, siklus pengembangan Anda harus menyertakan pengujian otomatis yang memverifikasi fungsionalitas saat fungsi dan layanan Anda berinteraksi.

Jika Anda tidak membuat pengujian berbasis cloud, Anda dapat mengalami masalah karena perbedaan antara lingkungan lokal dan lingkungan yang diterapkan. Proses integrasi berkelanjutan Anda harus menjalankan pengujian terhadap serangkaian sumber daya yang disediakan di cloud sebelum mempromosikan kode Anda ke lingkungan penerapan berikutnya, seperti QA, Staging, atau Production.

Lanjutkan membaca panduan singkat ini untuk mempelajari strategi pengujian untuk aplikasi tanpa server, atau kunjungi [repositori Sampel Uji Tanpa Server](#) untuk menyelami contoh-contoh praktis, khusus untuk bahasa dan runtime pilihan Anda.



Untuk pengujian tanpa server, Anda masih akan menulis unit, integrasi, dan end-to-end pengujian.

- Tes unit - Tes yang dijalankan terhadap blok kode yang terisolasi. Misalnya, memverifikasi logika bisnis untuk menghitung biaya pengiriman yang diberikan item dan tujuan tertentu.
- Tes integrasi - Tes yang melibatkan dua atau lebih komponen atau layanan yang berinteraksi, biasanya di lingkungan cloud. Misalnya, memverifikasi fungsi memproses peristiwa dari antrian.
- End-to-end tes - Tes yang memverifikasi perilaku di seluruh aplikasi. Misalnya, memastikan infrastruktur diatur dengan benar dan bahwa peristiwa mengalir antar layanan seperti yang diharapkan untuk merekam pesanan pelanggan.

Hasil bisnis yang ditargetkan

Menguji solusi tanpa server mungkin memerlukan sedikit lebih banyak waktu untuk menyiapkan pengujian yang memverifikasi interaksi berbasis peristiwa antar layanan. Ingatlah alasan bisnis praktis berikut saat Anda membaca panduan ini:

- Tingkatkan kualitas aplikasi Anda
- Kurangi waktu untuk membangun fitur dan memperbaiki bug

Kualitas aplikasi tergantung pada pengujian berbagai skenario untuk memverifikasi fungsionalitas. Mempertimbangkan skenario bisnis dengan cermat dan mengotomatiskan pengujian tersebut untuk dijalankan terhadap layanan cloud akan meningkatkan kualitas aplikasi Anda.

Bug perangkat lunak dan masalah konfigurasi memiliki dampak paling kecil pada biaya dan jadwal ketika tertangkap selama siklus pengembangan berulang. Jika masalah tetap tidak terdeteksi selama pengembangan, menemukan dan memperbaiki produksi membutuhkan lebih banyak usaha oleh lebih banyak orang.

Strategi pengujian tanpa server yang terencana dengan baik akan meningkatkan kualitas perangkat lunak dan meningkatkan waktu iterasi dengan memverifikasi fungsi dan aplikasi Lambda Anda berfungsi seperti yang diharapkan di lingkungan cloud.

Apa yang harus diuji

Sebaiknya gunakan strategi pengujian yang menguji perilaku layanan terkelola, konfigurasi cloud, kebijakan keamanan, dan integrasi dengan kode Anda untuk meningkatkan kualitas perangkat lunak. Pengujian perilaku, juga dikenal sebagai pengujian kotak hitam, memverifikasi sistem berfungsi seperti yang diharapkan tanpa mengetahui semua internal.

- Jalankan pengujian unit untuk memeriksa logika bisnis di dalam fungsi Lambda.
- Verifikasi layanan terintegrasi benar-benar dipanggil, dan parameter input sudah benar.
- Periksa apakah suatu peristiwa melewati semua layanan yang diharapkan end-to-end dalam alur kerja.

Dalam arsitektur berbasis server tradisional, tim sering mendefinisikan ruang lingkup pengujian untuk hanya menyertakan kode yang berjalan pada server aplikasi. Komponen, layanan, atau dependensi lainnya sering dianggap eksternal dan di luar ruang lingkup untuk pengujian.

Aplikasi tanpa server sering terdiri dari unit kerja kecil, seperti fungsi Lambda yang mengambil produk dari database, atau memproses item dari antrian, atau mengubah ukuran gambar dalam penyimpanan. Setiap komponen berjalan di lingkungan mereka sendiri. Tim kemungkinan akan bertanggung jawab atas banyak unit kecil ini dalam satu aplikasi.

Beberapa fungsi aplikasi dapat didelegasikan sepenuhnya ke layanan terkelola seperti Amazon S3, atau dibuat tanpa menggunakan kode yang dikembangkan secara internal. Tidak perlu menguji layanan terkelola ini, tetapi Anda perlu menguji integrasi dengan layanan ini.

Cara menguji tanpa server

Anda mungkin akrab dengan cara menguji aplikasi yang digunakan secara lokal: Anda menulis tes yang berjalan terhadap kode yang berjalan sepenuhnya di sistem operasi desktop Anda, atau di dalam wadah. Misalnya, Anda dapat memanggil komponen layanan web lokal dengan permintaan dan kemudian membuat pernyataan tentang respons.

Solusi tanpa server dibuat dari kode fungsi dan layanan terkelola berbasis cloud, seperti antrian, database, bus acara, dan sistem pesan. Semua komponen ini terhubung melalui arsitektur berbasis peristiwa, di mana pesan, yang disebut peristiwa, mengalir dari satu sumber daya ke sumber daya lainnya. Interaksi ini dapat sinkron, seperti ketika layanan web segera mengembalikan hasil, atau tindakan asinkron yang selesai di lain waktu, seperti menempatkan item dalam antrian atau memulai langkah alur kerja. Strategi pengujian Anda harus mencakup kedua skenario dan menguji interaksi antar layanan. Untuk interaksi asinkron, Anda mungkin perlu mendeteksi efek samping pada komponen hilir yang mungkin tidak segera diamati.

Mereplikasi seluruh lingkungan cloud, termasuk antrian, tabel database, bus acara, kebijakan keamanan, dan banyak lagi, tidak praktis. Anda pasti akan mengalami masalah karena perbedaan antara lingkungan lokal Anda dan lingkungan yang Anda gunakan di cloud. Variasi antara lingkungan Anda akan meningkatkan waktu untuk mereproduksi dan memperbaiki bug.

Dalam aplikasi tanpa server, komponen arsitektur umumnya ada seluruhnya di cloud, jadi pengujian terhadap kode dan layanan di cloud diperlukan untuk mengembangkan fitur dan memperbaiki bug.

Teknik pengujian

Pada kenyataannya, strategi pengujian Anda kemungkinan akan mencakup campuran teknik untuk meningkatkan kualitas solusi Anda. Anda akan menggunakan tes interaktif cepat untuk men-debug fungsi di konsol, pengujian unit otomatis untuk memeriksa logika bisnis yang terisolasi, verifikasi panggilan ke layanan eksternal dengan tiruan, dan pengujian sesekali terhadap emulator yang meniru layanan.

- Pengujian di cloud - Anda menyebarkan infrastruktur dan kode untuk menguji dengan layanan aktual, kebijakan keamanan, konfigurasi, dan parameter spesifik infrastruktur. Pengujian berbasis cloud memberikan ukuran kualitas kode yang paling akurat.

Mendebug fungsi di konsol adalah cara cepat untuk menguji di cloud. Anda dapat memilih dari pustaka peristiwa pengujian sampel atau membuat acara khusus untuk menguji fungsi secara terpisah. Anda juga dapat berbagi acara pengujian melalui konsol dengan tim Anda.

Untuk mengotomatiskan pengujian dalam siklus hidup pengembangan dan pembuatan, Anda perlu menguji di luar konsol. Lihat bagian pengujian khusus bahasa dalam panduan ini untuk strategi dan sumber daya otomatisasi.

- Pengujian dengan tiruan (juga disebut palsu) - Mocks adalah objek dalam kode Anda yang mensimulasikan dan berdiri untuk layanan eksternal. Mocks memberikan perilaku yang telah ditentukan sebelumnya untuk memverifikasi panggilan dan parameter layanan. Palsu adalah implementasi tiruan yang mengambil jalan pintas untuk menyederhanakan atau meningkatkan kinerja. Misalnya, objek akses data palsu mungkin mengembalikan data dari datastore dalam memori. Mocks dapat meniru dan menyederhanakan dependensi yang kompleks, tetapi juga dapat menyebabkan lebih banyak tiruan untuk menggantikan dependensi bersarang.
- Pengujian dengan emulator - Anda dapat mengatur aplikasi (terkadang dari pihak ketiga) untuk meniru layanan cloud di lingkungan lokal Anda. Kecepatan adalah kekuatan mereka, tetapi pengaturan dan paritas dengan layanan produksi adalah kelemahan mereka. Gunakan emulator dengan hemat.

Pengujian di cloud

Pengujian di cloud sangat berharga untuk semua fase pengujian, termasuk pengujian unit, pengujian integrasi, dan end-to-end pengujian. Saat menjalankan pengujian terhadap kode berbasis cloud yang juga berinteraksi dengan layanan berbasis cloud, Anda mendapatkan ukuran kualitas kode yang paling akurat.

Cara mudah untuk menjalankan fungsi Lambda di cloud adalah dengan acara pengujian di AWS Management Console. Peristiwa pengujian adalah JSON masukan ke fungsi Anda. Jika fungsi Anda tidak memerlukan input, acara dapat berupa JSON dokumen kosong ({}). Konsol menyediakan contoh peristiwa untuk berbagai integrasi layanan. Setelah membuat acara di konsol, Anda juga dapat membagikannya dengan tim Anda untuk membuat pengujian lebih mudah dan konsisten.

Pelajari cara [men-debug fungsi sampel di konsol](#).

Note

Meskipun menjalankan fungsi di konsol adalah cara cepat untuk men-debug, mengotomatiskan siklus pengujian Anda sangat penting untuk meningkatkan kualitas aplikasi dan kecepatan pengembangan.

Sampel otomatisasi pengujian tersedia di [repositori Sampel Uji Tanpa Server](#). Baris perintah berikut menjalankan contoh [uji integrasi Python](#) otomatis:

```
python -m pytest -s tests/integration -v
```

Meskipun pengujian berjalan secara lokal, ia berinteraksi dengan sumber daya berbasis cloud. Sumber daya ini telah digunakan menggunakan alat baris AWS SAM perintah AWS Serverless Application Model dan. Kode pengujian pertama-tama mengambil output tumpukan yang diterapkan, yang mencakup API titik akhir, fungsi ARN, dan peran keamanan. Selanjutnya, pengujian mengirimkan permintaan ke API titik akhir, yang merespons dengan daftar bucket Amazon S3. Pengujian ini berjalan sepenuhnya terhadap sumber daya berbasis cloud untuk memverifikasi sumber daya tersebut digunakan, diamankan, dan berfungsi seperti yang diharapkan.

```
===== test session starts =====
platform darwin -- Python 3.10.10, pytest-7.3.1, pluggy-1.0.0
-- /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-lambda/
venv/bin/python
cachedir: .pytest_cache
```



```

rootdir: /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-
lambda
plugins: mock-3.10.0
collected 1 item

tests/integration/test_api_gateway.py::TestApiGateway::test_api_gateway

--> Stack outputs:

HelloWorldApi
= https://p7teqs3162.execute-api.us-east-2.amazonaws.com/Prod/hello/
> API Gateway endpoint URL for Prod stage for Hello World function

PythonTestDemo
= arn:aws:lambda:us-east-2:123456789012:function:testing-apigw-lambda-
PythonTestDemo-iSij8evaTdx1
> Hello World Lambda Function ARN

PythonTestDemoIamRole
= arn:aws:iam::123456789012:role/testing-apigw-lambda-PythonTestDemoRole-
IZELQQ9MG4HQ
> Implicit IAM Role created for Hello World function

--> Found API endpoint for "testing-apigw-lambda" stack...
--> https://p7teqs3162.execute-api.us-east-2.amazonaws.com/Prod/hello/
API Gateway response:
amplify-dev-123456789-deployment|myapp-prod-p-loggingbucket-123456|s3-java-
bucket-123456789
PASSED

===== 1 passed in 1.53s =====

```

Untuk pengembangan aplikasi cloud-native, pengujian di cloud memberikan manfaat berikut:

- Anda dapat menguji setiap layanan yang tersedia.
- Anda selalu menggunakan layanan terbaru APIs dan mengembalikan nilai.
- Lingkungan pengujian cloud sangat mirip dengan lingkungan produksi Anda.
- Pengujian dapat mencakup kebijakan keamanan, kuota layanan, konfigurasi, dan parameter spesifik infrastruktur.
- Setiap pengembang dapat dengan cepat membuat satu atau lebih lingkungan pengujian di cloud.

- Tes cloud meningkatkan kepercayaan bahwa kode Anda akan berjalan dengan benar dalam produksi.

Pengujian di cloud memang memiliki beberapa kelemahan. Hal negatif yang paling jelas dari pengujian di cloud adalah bahwa penyebaran ke lingkungan cloud biasanya membutuhkan waktu lebih lama daripada penerapan ke lingkungan desktop lokal.

Untungnya, alat seperti [AWS Serverless Application Model \(AWS SAM\) Accelerate](#), [mode tontonan AWS Cloud Development Kit \(AWS CDK\)](#), dan [SST](#)(pihak ke-3) mengurangi latensi yang terlibat dengan iterasi penyebaran cloud. Alat-alat ini dapat memantau infrastruktur dan kode Anda dan secara otomatis menyebarkan pembaruan tambahan ke lingkungan cloud Anda.

Note

Lihat cara [membuat infrastruktur sebagai kode](#) di Panduan Pengembang Tanpa Server untuk mempelajari selengkapnya AWS Serverless Application Model, AWS CloudFormation, dan AWS Cloud Development Kit (AWS CDK)

Tidak seperti pengujian lokal, pengujian di cloud membutuhkan sumber daya tambahan yang dapat menimbulkan biaya layanan. Membuat lingkungan pengujian yang terisolasi dapat meningkatkan beban DevOps tim Anda, terutama di organisasi dengan kontrol ketat seputar akun dan infrastruktur. Meski begitu, ketika bekerja dengan skenario infrastruktur yang kompleks, biaya dalam waktu pengembang untuk mengatur dan memelihara lingkungan lokal yang rumit bisa serupa (atau lebih mahal) daripada menggunakan lingkungan pengujian sekali pakai yang dibuat dengan Infrastruktur sebagai alat otomatisasi Kode.

Pengujian di cloud, bahkan dengan pertimbangan ini, masih merupakan cara terbaik untuk menjamin kualitas solusi tanpa server Anda.

Menguji dengan tiruan

Pengujian dengan tiruan adalah teknik di mana Anda membuat objek pengganti dalam kode Anda untuk mensimulasikan perilaku layanan cloud.

Misalnya, Anda dapat menulis pengujian yang menggunakan tiruan layanan Amazon S3 yang mengembalikan respons tertentu setiap kali metode `CreateObject` dipanggil. Saat pengujian berjalan, tiruan mengembalikan respons terprogram tersebut tanpa memanggil Amazon S3, atau titik akhir layanan lainnya.

Objek tiruan sering dihasilkan oleh kerangka kerja tiruan untuk mengurangi upaya pengembangan. Beberapa kerangka kerja tiruan bersifat generik dan yang lainnya dirancang khusus untuk AWS SDKs, seperti [Moto](#), perpustakaan Python untuk layanan dan sumber daya ejaan. AWS

Perhatikan bahwa objek tiruan berbeda dari emulator karena tiruan biasanya dibuat atau dikonfigurasi oleh pengembang sebagai bagian dari kode pengujian, sedangkan emulator adalah aplikasi mandiri yang mengekspos fungsionalitas dengan cara yang sama seperti sistem yang mereka tiru.

Keuntungan menggunakan tiruan meliputi:

- Mocks dapat mensimulasikan layanan pihak ketiga yang berada di luar kendali aplikasi Anda, seperti APIs dan penyedia perangkat lunak sebagai layanan (SaaS), tanpa memerlukan akses langsung ke layanan tersebut.
- Mocks berguna untuk menguji kondisi kegagalan, terutama ketika kondisi seperti itu sulit untuk disimulasikan, seperti pemadaman layanan.
- Mock dapat memberikan pengujian lokal yang cepat setelah dikonfigurasi.
- Mocks dapat memberikan perilaku pengganti untuk hampir semua jenis objek, sehingga strategi mengejek dapat menciptakan cakupan untuk berbagai layanan yang lebih luas daripada emulator.
- Ketika fitur atau perilaku baru tersedia, pengujian tiruan dapat bereaksi lebih cepat. Dengan menggunakan kerangka kerja tiruan generik, Anda dapat mensimulasikan fitur baru segera setelah pembaruan AWS SDK tersedia.

Pengujian tiruan memiliki kelemahan ini:

- Mocks umumnya memerlukan upaya pengaturan dan konfigurasi yang tidak sepele, khususnya ketika mencoba menentukan nilai pengembalian dari layanan yang berbeda untuk mengejek respons dengan benar.
- Mocks ditulis, dikonfigurasi, dan harus dikelola oleh pengembang, meningkatkan tanggung jawab mereka.
- Anda mungkin perlu memiliki akses ke cloud untuk memahami APIs dan mengembalikan nilai layanan.
- Mocks bisa sulit dipertahankan. Saat API tanda tangan cloud yang diejek berubah, atau skema nilai pengembalian berkembang, Anda perlu memperbarui tiruan Anda. Mocks juga memerlukan pembaruan jika Anda memperluas logika aplikasi Anda untuk melakukan panggilan ke yang baru APIs.
- Pengujian yang menggunakan tiruan mungkin lolos di lingkungan desktop tetapi gagal di cloud. Hasil mungkin tidak cocok dengan saat ini API. Konfigurasi layanan dan kuota tidak dapat diuji.

- Kerangka kerja tiruan terbatas dalam menguji atau mendeteksi pembatasan kebijakan atau kuota AWS Identity and Access Management (IAM). Meskipun tiruan lebih baik dalam mensimulasikan ketika otorisasi gagal atau kuota terlampaui, pengujian tidak dapat menentukan hasil mana yang benar-benar akan terjadi di lingkungan produksi.

Pengujian dengan emulasi

Emulator biasanya merupakan aplikasi yang berjalan secara lokal yang meniru layanan produksi. AWS

Emulator memiliki APIs yang mirip dengan rekan cloud mereka dan memberikan nilai pengembalian yang serupa. Mereka juga dapat mensimulasikan perubahan status yang diprakarsai oleh API panggilan. Misalnya, Anda dapat menggunakan AWS SAM untuk menjalankan fungsi dengan AWS SAM lokal untuk meniru layanan Lambda sehingga Anda dapat dengan cepat memanggil fungsi. Lihat [AWS SAM lokal](#) di Panduan AWS Serverless Application Model Pengembang untuk detailnya.

Keuntungan dari tes dengan emulator meliputi:

- Emulator dapat memfasilitasi iterasi dan pengujian pengembangan lokal yang cepat.
- Emulator menyediakan lingkungan yang akrab bagi pengembang yang terbiasa mengembangkan kode di lingkungan lokal. Misalnya, jika Anda terbiasa dengan pengembangan aplikasi n-tier, Anda mungkin memiliki mesin database dan server web, mirip dengan yang berjalan dalam produksi, berjalan di mesin lokal Anda untuk menyediakan kemampuan pengujian cepat, lokal, dan terisolasi.
- Emulator tidak memerlukan perubahan apa pun pada infrastruktur cloud (seperti akun cloud pengembang), sehingga mudah diterapkan dengan pola pengujian yang ada.

Pengujian dengan emulator memiliki kelemahan ini:

- Emulator bisa sulit diatur dan direplikasi, terutama bila digunakan dalam pipa CI/CD. Hal ini dapat meningkatkan beban kerja staf TI atau pengembang yang mengelola perangkat lunak mereka sendiri.
- Fitur yang ditiru dan APIs biasanya tertinggal dari pembaruan layanan. Hal ini dapat menyebabkan kesalahan karena kode yang diuji tidak cocok dengan yang sebenarnya API, dan menghambat adopsi fitur baru.
- Emulator memerlukan dukungan, pembaruan, perbaikan bug, dan peningkatan paritas fitur. Ini adalah tanggung jawab penulis emulator, yang bisa menjadi perusahaan pihak ketiga.

- Pengujian yang mengandalkan emulator dapat memberikan hasil yang sukses secara lokal, tetapi gagal di cloud karena kebijakan keamanan produksi, konfigurasi antar-layanan, atau melebihi kuota Lambda.
- Banyak AWS layanan tidak memiliki emulator yang tersedia. Jika Anda mengandalkan emulasi, Anda mungkin tidak memiliki opsi pengujian yang memuaskan untuk bagian dari aplikasi Anda.

Praktik terbaik

Bagian berikut memberikan rekomendasi untuk pengujian aplikasi tanpa server yang sukses.

Anda dapat menemukan contoh praktis pengujian dan otomatisasi pengujian di repositori [Sampel Uji Tanpa Server](#).

Prioritaskan pengujian di cloud

Pengujian di cloud memberikan cakupan pengujian yang paling andal, akurat, dan lengkap. Melakukan pengujian dalam konteks cloud akan menguji secara komprehensif tidak hanya logika bisnis tetapi juga kebijakan keamanan, konfigurasi layanan, kuota, dan API tanda tangan terbaru dan nilai pengembalian.

Struktur kode Anda untuk pengujian

Sederhanakan pengujian dan fungsi Lambda Anda dengan memisahkan kode khusus Lambda dari logika bisnis inti Anda.

Penangan fungsi Lambda Anda harus berupa adaptor ramping yang mengambil data peristiwa dan hanya meneruskan detail yang penting bagi metode logika bisnis Anda. Dengan strategi ini, Anda dapat membungkus tes komprehensif seputar logika bisnis Anda tanpa mengkhawatirkan detail khusus Lambda. Fungsi AWS Lambda Anda seharusnya tidak memerlukan pengaturan lingkungan yang kompleks atau sejumlah besar dependensi untuk membuat dan menginisialisasi komponen yang sedang diuji.

Secara umum, Anda harus menulis handler yang mengekstrak dan memvalidasi data dari objek peristiwa dan konteks yang masuk, kemudian mengirimkan masukan itu ke metode yang melakukan logika bisnis Anda.

Mempercepat loop umpan balik pengembangan

Ada alat dan teknik untuk mempercepat loop umpan balik pengembangan. Misalnya, [mode AWS SAM Akselerasi dan AWS CDK tonton](#) mengurangi waktu yang diperlukan untuk memperbarui lingkungan cloud.

Sampel dalam [repositori Sampel Uji GitHub Tanpa Server](#) mengeksplorasi beberapa teknik ini.

Kami juga menyarankan Anda membuat dan menguji sumber daya cloud sedini mungkin selama pengembangan—tidak hanya setelah check-in ke kontrol sumber. Praktik ini memungkinkan eksplorasi dan eksperimen yang lebih cepat saat mengembangkan solusi. Selain itu, mengotomatiskan penerapan dari mesin pengembangan membantu Anda menemukan masalah konfigurasi cloud lebih cepat dan mengurangi upaya yang sia-sia untuk pembaruan dan proses peninjauan kode.

Fokus pada tes integrasi

Saat membangun aplikasi dengan Lambda, menguji komponen bersama-sama adalah praktik terbaik.

Tes yang dijalankan terhadap dua atau lebih komponen arsitektur disebut tes integrasi. Tujuan dari tes integrasi adalah untuk memahami tidak hanya bagaimana kode Anda akan dijalankan di seluruh komponen, tetapi bagaimana lingkungan hosting kode Anda akan berperilaku. `end-to-end` Tes E adalah jenis tes integrasi khusus yang memverifikasi perilaku di seluruh aplikasi.

Untuk membangun pengujian integrasi, terapkan aplikasi Anda ke lingkungan cloud. Ini dapat dilakukan dari lingkungan lokal atau melalui pipa CI/CD. Kemudian, tulis tes untuk menjalankan sistem di bawah test (SUT) dan memvalidasi perilaku yang diharapkan.

Misalnya, sistem yang diuji bisa menjadi aplikasi yang menggunakan API Gateway, Lambda dan DynamoDB. Pengujian dapat membuat HTTP panggilan sintetis ke titik akhir API Gateway dan memvalidasi bahwa respons tersebut menyertakan muatan yang diharapkan. Tes ini memvalidasi bahwa kode AWS Lambda sudah benar, dan setiap layanan dikonfigurasi dengan benar untuk menangani permintaan, termasuk izin IAM di antara mereka. Selanjutnya, Anda dapat merancang tes untuk menulis catatan dari berbagai ukuran untuk memverifikasi kuota layanan Anda, seperti ukuran catatan maksimal di DynamoDB, diatur dengan benar.



Buat lingkungan pengujian yang terisolasi

Pengujian di cloud biasanya membutuhkan lingkungan pengembang yang terisolasi, sehingga pengujian, data, dan peristiwa tidak tumpang tindih.

Salah satu pendekatannya adalah menyediakan setiap pengembang AWS akun khusus. Ini akan menghindari konflik dengan penamaan sumber daya yang dapat terjadi ketika beberapa pengembang bekerja di basis kode bersama, mencoba menyebarkan sumber daya, atau memanggil file. API

Proses pengujian otomatis harus membuat sumber daya bernama unik untuk setiap tumpukan. Misalnya, Anda dapat mengatur skrip atau file TOML konfigurasi sehingga perintah AWS SAM CLI [sam deploy](#) atau [sam sync](#) akan secara otomatis menentukan tumpukan dengan awalan unik.

Dalam beberapa kasus, pengembang berbagi AWS akun. Ini mungkin karena memiliki sumber daya di tumpukan Anda yang mahal untuk dioperasikan, atau untuk menyediakan dan mengkonfigurasi. Misalnya, database dapat dibagikan untuk membuatnya lebih mudah untuk mengatur dan menyemai data dengan benar

Jika pengembang berbagi akun, Anda harus menetapkan batasan untuk mengidentifikasi kepemilikan dan menghilangkan tumpang tindih. Salah satu cara untuk melakukannya adalah dengan mengawali nama tumpukan dengan pengguna IDs pengembang. Pendekatan populer lainnya adalah mengatur tumpukan berdasarkan cabang kode. Dengan batas cabang, lingkungan terisolasi, tetapi pengembang masih dapat berbagi sumber daya, seperti database relasional. Pendekatan ini adalah praktik terbaik ketika pengembang bekerja di lebih dari satu cabang sekaligus.

Pengujian di cloud sangat berharga untuk semua fase pengujian, termasuk pengujian unit, pengujian integrasi, dan end-to-end pengujian. Mempertahankan isolasi yang tepat sangat penting; tetapi Anda masih ingin lingkungan QA Anda menyerupai lingkungan produksi Anda sedekat mungkin. Untuk alasan ini, tim menambahkan proses kontrol perubahan untuk lingkungan QA.

Untuk lingkungan pra-produksi dan produksi, batasan biasanya ditarik pada tingkat akun untuk melindungi beban kerja dari masalah tetangga yang bising dan menerapkan kontrol keamanan hak istimewa paling sedikit untuk melindungi data sensitif. Beban kerja memiliki kuota. Anda tidak ingin pengujian Anda mengkonsumsi kuota yang dialokasikan untuk produksi (tetangga yang bising) atau memiliki akses ke data pelanggan. Pengujian beban adalah aktivitas lain yang harus Anda isolasi dari tumpukan produksi Anda.

Dalam semua kasus, lingkungan harus dikonfigurasi dengan peringatan dan kontrol untuk menghindari pengeluaran yang tidak perlu. Misalnya, Anda dapat membatasi jenis, tingkat, atau ukuran sumber daya yang dapat dibuat, dan mengatur peringatan email ketika perkiraan biaya melebihi ambang batas yang diberikan.

Gunakan tiruan untuk logika bisnis yang terisolasi

Kerangka kerja tiruan adalah alat yang berharga untuk menulis tes unit cepat. Mereka sangat bermanfaat ketika tes mencakup logika bisnis internal yang kompleks, seperti perhitungan atau simulasi matematika atau keuangan. Cari pengujian unit yang memiliki sejumlah besar kasus uji atau variasi input, di mana input tersebut tidak mengubah pola atau konten panggilan ke layanan cloud lainnya.

Kode yang dicakup oleh pengujian unit dengan tiruan juga harus dicakup oleh pengujian di cloud. Ini direkomendasikan karena laptop pengembang atau lingkungan mesin build dapat dikonfigurasi secara berbeda dari lingkungan produksi di cloud. Misalnya, fungsi Lambda Anda dapat menggunakan lebih banyak memori atau waktu daripada yang dialokasikan saat dijalankan dengan parameter input tertentu. Atau kode Anda mungkin menyertakan variabel lingkungan yang tidak dikonfigurasi dengan cara yang sama (atau sama sekali), dan perbedaannya dapat menyebabkan kode berperilaku berbeda atau gagal.

Manfaat tiruan kurang untuk tes integrasi, karena tingkat upaya untuk mengimplementasikan tiruan yang diperlukan meningkat dengan jumlah titik koneksi. end-to-end Pengujian E tidak boleh menggunakan tiruan, karena tes ini umumnya berurusan dengan status dan logika kompleks yang tidak dapat dengan mudah disimulasikan dengan kerangka kerja tiruan.

Terakhir, hindari menggunakan layanan cloud tiruan untuk memvalidasi implementasi panggilan layanan yang tepat. Sebagai gantinya, lakukan panggilan layanan cloud di cloud untuk memvalidasi perilaku, konfigurasi, dan implementasi fungsional.

Gunakan emulator dengan hemat

Emulator dapat nyaman untuk beberapa kasus penggunaan, misalnya, untuk tim pengembangan dengan akses internet terbatas, tidak dapat diandalkan, atau lambat. Tetapi, dalam kebanyakan keadaan, pilih untuk menggunakan emulator dengan hemat.

Dengan menghindari emulator, Anda akan dapat membangun dan berinovasi dengan fitur layanan terbaru dan terkini. APIs Anda tidak akan terjebak menunggu rilis vendor untuk mencapai paritas fitur. Anda akan mengurangi biaya di muka dan berkelanjutan untuk pembelian dan konfigurasi pada beberapa sistem pengembangan dan membangun mesin. Selain itu, Anda akan menghindari masalah bahwa banyak layanan cloud tidak memiliki emulator yang tersedia. Strategi pengujian yang bergantung pada emulasi akan membuat tidak mungkin untuk menggunakan layanan tersebut (yang mengarah ke solusi yang berpotensi lebih mahal) atau menghasilkan kode dan konfigurasi yang tidak diuji dengan baik.

Ketika Anda menggunakan emulasi untuk pengujian, Anda masih harus menguji di cloud untuk memverifikasi konfigurasi dan untuk menguji interaksi dengan layanan cloud yang hanya dapat disimulasikan atau diejek di lingkungan yang ditiru.

Tantangan pengujian secara lokal

Saat Anda menggunakan emulator dan panggilan tiruan untuk menguji di desktop lokal Anda, Anda mungkin mengalami inkonsistensi pengujian saat kode Anda berkembang dari lingkungan ke lingkungan di pipeline CI/CD Anda. Pengujian unit untuk memvalidasi logika bisnis aplikasi Anda di desktop Anda mungkin tidak secara akurat menguji aspek penting dari layanan cloud.

Contoh berikut memberikan kasus yang harus diperhatikan saat menguji secara lokal dengan tiruan dan emulator:

Contoh: Fungsi Lambda membuat bucket S3

Jika logika fungsi Lambda bergantung pada pembuatan bucket S3, pengujian lengkap harus mengonfirmasi bahwa Amazon S3 dipanggil dan bucket berhasil dibuat.

- Dalam pengaturan pengujian tiruan, Anda mungkin mengejek respons sukses dan berpotensi menambahkan kasus uji untuk menangani respons kegagalan.
- Dalam skenario pengujian emulasi, `CreateBucketAPI` mungkin dipanggil, tetapi Anda perlu menyadari bahwa identitas yang membuat panggilan lokal tidak akan berasal dari layanan

Lambda. Identitas panggilan tidak akan mengambil peran keamanan seperti di cloud, sehingga otentikasi placeholder akan digunakan sebagai gantinya, mungkin dengan peran yang lebih permisif atau identitas pengguna yang akan berbeda saat dijalankan di cloud.

Pengaturan tiruan dan emulasi akan menguji apa yang akan dilakukan fungsi Lambda jika memanggil Amazon S3; namun, tes tersebut tidak akan memverifikasi bahwa fungsi Lambda, seperti yang dikonfigurasi, mampu berhasil membuat bucket Amazon S3. Anda harus memastikan peran yang ditetapkan ke fungsi memiliki kebijakan keamanan terlampir yang memungkinkan fungsi untuk melakukan `s3:CreateBucket` tindakan. Jika tidak, fungsi tersebut kemungkinan akan gagal saat diterapkan ke lingkungan cloud.

Contoh: Fungsi Lambda memproses pesan dari antrian Amazon SQS

Jika SQS antrian Amazon adalah sumber fungsi Lambda, pengujian lengkap harus memverifikasi bahwa fungsi Lambda berhasil dipanggil saat pesan dimasukkan ke dalam antrian.

Pengujian emulasi dan pengujian tiruan umumnya diatur untuk menjalankan kode fungsi Lambda secara langsung, dan untuk mensimulasikan SQS integrasi Amazon dengan meneruskan muatan JSON peristiwa (atau objek deserialisasi) sebagai input penanganan fungsi.

Pengujian lokal yang mensimulasikan SQS integrasi Amazon akan menguji apa yang akan dilakukan fungsi Lambda ketika dipanggil oleh SQS Amazon dengan muatan tertentu, tetapi pengujian tidak akan memverifikasi bahwa SQS Amazon akan berhasil menjalankan fungsi Lambda ketika digunakan ke lingkungan cloud.

Beberapa contoh masalah konfigurasi yang mungkin Anda temui dengan Amazon SQS dan Lambda termasuk yang berikut:

- Batas waktu SQS visibilitas Amazon terlalu rendah, menghasilkan beberapa pemanggilan ketika hanya satu yang dimaksudkan.
- Peran eksekusi fungsi Lambda tidak mengizinkan membaca pesan dari antrian (melalui `sqs:ReceiveMessage`, `sqs:DeleteMessage`, atau). `sqs:GetQueueAttributes`
- Contoh peristiwa yang diteruskan ke fungsi Lambda melebihi kuota ukuran SQS pesan Amazon. Oleh karena itu, tes ini tidak valid karena Amazon tidak SQS akan pernah dapat mengirim pesan sebesar itu.

Seperti yang ditunjukkan oleh contoh-contoh ini, tes yang mencakup logika bisnis tetapi bukan konfigurasi antara layanan cloud cenderung memberikan hasil yang tidak dapat diandalkan.

FAQ

Saya memiliki fungsi Lambda yang melakukan perhitungan dan mengembalikan hasil tanpa memanggil layanan lain. Apakah saya benar-benar perlu mengujinya di cloud?

Ya. Fungsi Lambda memiliki parameter konfigurasi yang dapat mengubah hasil pengujian. Semua kode fungsi Lambda memiliki ketergantungan pada pengaturan [batas waktu](#) dan [memori](#), yang dapat menyebabkan fungsi gagal jika pengaturan tersebut tidak diatur dengan benar. [Kebijakan Lambda juga memungkinkan pencatatan keluaran standar ke Amazon. CloudWatch](#) Bahkan jika kode Anda tidak menelepon CloudWatch secara langsung, izin diperlukan untuk mengaktifkan logging. Izin yang diperlukan ini tidak dapat diejek atau ditiru secara akurat.

Bagaimana pengujian di cloud dapat membantu pengujian unit? Jika ada di cloud dan terhubung ke sumber daya lain, bukankah itu tes integrasi?

Kami mendefinisikan pengujian unit sebagai pengujian yang beroperasi pada komponen arsitektur secara terpisah, tetapi ini tidak mencegah pengujian dari memasukkan komponen yang dapat memanggil layanan lain atau menggunakan beberapa komunikasi jaringan.

Banyak aplikasi tanpa server memiliki komponen arsitektur yang dapat diuji secara terpisah, bahkan di cloud. Salah satu contohnya adalah fungsi Lambda yang mengambil input, memproses data, dan mengirim pesan ke antrian AmazonSQS. Tes unit dari fungsi ini kemungkinan akan menguji apakah nilai input menghasilkan nilai tertentu yang ada dalam pesan antrian.

Pertimbangkan tes yang ditulis dengan menggunakan pola Arrange, Act, Assert:

- Atur: Alokasikan sumber daya (antrian untuk menerima pesan, dan fungsi yang sedang diuji).
- Tindakan: Panggil fungsi yang sedang diuji.
- Tegaskan: Ambil pesan yang dikirim oleh fungsi, dan validasi output.

Pendekatan pengujian tiruan akan melibatkan mengejek antrian dengan objek tiruan dalam proses, dan membuat instance dalam proses dari kelas atau modul yang berisi kode fungsi Lambda. Selama fase Assert, pesan antrian akan diambil dari objek yang diejek.

Dalam pendekatan berbasis cloud, pengujian akan membuat SQS antrian Amazon untuk keperluan pengujian, dan akan menerapkan fungsi Lambda dengan variabel lingkungan yang dikonfigurasi untuk menggunakan antrian SQS Amazon yang terisolasi sebagai tujuan keluaran. Setelah menjalankan fungsi Lambda, pengujian akan mengambil pesan dari antrian Amazon. SQS

Pengujian berbasis cloud akan menjalankan kode yang sama, menegaskan perilaku yang sama, dan memvalidasi kebenaran fungsional aplikasi. Namun, itu akan memiliki keuntungan tambahan karena dapat memvalidasi pengaturan fungsi Lambda: IAM peranIAM, kebijakan, dan batas waktu fungsi dan pengaturan memori.

Langkah dan sumber daya selanjutnya

Gunakan sumber daya berikut untuk mempelajari lebih lanjut dan mengeksplorasi contoh-contoh praktis pengujian.

Contoh implementasi

[Repositori Sampel Uji Tanpa Server](#) pada GitHub berisi contoh nyata pengujian yang mengikuti pola dan praktik terbaik yang dijelaskan dalam panduan ini. Repositori berisi kode sampel dan panduan panduan dari proses pengujian tiruan, emulasi, dan cloud yang dijelaskan di bagian sebelumnya. Gunakan repositori ini untuk mempercepat panduan pengujian tanpa server terbaru dari AWS

Bacaan lebih lanjut

Kunjungi [Serverless Land](#) untuk mengakses blog, video, dan pelatihan terbaru untuk teknologi tanpa AWS server.

Posting AWS blog berikut juga disarankan untuk dibaca:

- [Mempercepat pengembangan tanpa server dengan AWS SAM Accelerate \(posting blog\)](#) AWS
- [Meningkatkan kecepatan pengembangan dengan CDK Watch](#) (posting AWS blog)
- [Integrasi layanan mengejek dengan AWS Step Functions Lokal](#) (AWS posting blog)
- [Memulai dengan menguji aplikasi tanpa server](#) (AWS posting blog)

Alat

- AWS SAM — [Menguji dan men-debug aplikasi tanpa server](#)
- AWS SAM — [Mengintegrasikan dengan tes otomatis](#)
- Lambda - Menguji fungsi [Lambda di konsol Lambda](#)

Memanggil Lambda dengan acara dari layanan lain AWS

Beberapa AWS layanan dapat langsung memanggil fungsi Lambda menggunakan pemicu. Layanan ini mendorong peristiwa ke Lambda, dan fungsi segera dipanggil saat peristiwa yang ditentukan terjadi. Pemicu cocok untuk peristiwa diskrit dan pemrosesan waktu nyata. Saat Anda [membuat pemicu menggunakan konsol Lambda, konsol](#) berinteraksi dengan AWS layanan terkait untuk mengonfigurasi pemberitahuan peristiwa pada layanan tersebut. Pemicunya sebenarnya disimpan dan dikelola oleh layanan yang menghasilkan peristiwa, bukan oleh Lambda.

Peristiwa adalah data yang terstruktur dalam JSON format. JSONStrukturnya bervariasi tergantung pada layanan yang menghasilkannya dan jenis acara, tetapi semuanya berisi data yang dibutuhkan fungsi untuk memproses acara.

Suatu fungsi dapat memiliki banyak pemicu. Setiap pemicu bertindak sebagai klien yang menjalankan fungsi Anda secara independen, dan setiap peristiwa yang diteruskan Lambda ke fungsi Anda hanya memiliki data dari satu pemicu. Lambda mengubah dokumen acara menjadi objek dan meneruskannya ke penanganan fungsi Anda.

[Bergantung pada layanannya, pemanggilan yang digerakkan oleh peristiwa dapat sinkron atau asinkron.](#)

- Untuk pemanggilan sinkron, layanan yang menghasilkan acara menunggu respons dari fungsi Anda. Layanan itu mendefinisikan data yang diperlukan fungsi untuk dikembalikan dalam respons. Layanan mengontrol strategi kesalahan, seperti apakah akan mencoba lagi kesalahan.
- Untuk invokasi asinkron, Lambda mengantrekan peristiwa sebelum memberikannya ke fungsi Anda. Ketika Lambda mengantri acara, ia segera mengirimkan respons sukses ke layanan yang menghasilkan acara tersebut. Setelah fungsi memproses peristiwa, Lambda tidak mengembalikan respons ke layanan penghasil peristiwa.

Membuat pemicu

Cara termudah untuk membuat pemicu adalah dengan menggunakan konsol Lambda. [Saat Anda membuat pemicu menggunakan konsol, Lambda secara otomatis menambahkan izin yang diperlukan ke kebijakan berbasis sumber daya fungsi.](#)

Untuk membuat pemicu menggunakan konsol Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih fungsi yang ingin Anda buat pemacu.
3. Di panel Ikhtisar fungsi, pilih Tambah pemacu.
4. Pilih AWS layanan yang ingin Anda gunakan untuk menjalankan fungsi Anda.
5. Isi opsi di panel konfigurasi Pemacu dan pilih Tambah. Bergantung pada pilihan AWS layanan Anda untuk menjalankan fungsi Anda, opsi konfigurasi pemacu akan berbeda.

Layanan yang dapat memanggil fungsi Lambda

Tabel berikut mencantumkan layanan yang dapat memanggil fungsi Lambda.

| Layanan | Metode pemanggilan |
|---|---|
| Amazon Managed Streaming for Apache Kafka | Pemetaan sumber acara |
| Apache Kafka yang dikelola sendiri | Pemetaan sumber acara |
| API Gerbang Amazon | Digerakkan oleh peristiwa; doa sinkron |
| AWS CloudFormation | Digerakkan oleh peristiwa; pemanggilan asinkron |
| CloudWatch Log Amazon | Digerakkan oleh peristiwa; pemanggilan asinkron |
| AWS CodeCommit | Digerakkan oleh peristiwa; pemanggilan asinkron |
| AWS CodePipeline | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Amazon Cognito | Digerakkan oleh peristiwa; doa sinkron |
| AWS Config | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Amazon Connect | Digerakkan oleh peristiwa; doa sinkron |
| Amazon DynamoDB | Pemetaan sumber acara |
| Amazon Elastic File System | Integrasi khusus |

| Layanan | Metode pemanggilan |
|--|--|
| Elastic Load Balancing (Application Load Balancer) | Digerakkan oleh peristiwa; doa sinkron |
| Amazon EventBridge (CloudWatch Acara) | Digerakkan oleh peristiwa; pemanggilan asinkron (bus acara), pemanggilan sinkron atau asinkron (pipa dan jadwal) |
| AWS IoT | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Amazon Kinesis | Pemetaan sumber acara |
| Amazon Data Firehose | Digerakkan oleh peristiwa; doa sinkron |
| Amazon Lex | Digerakkan oleh peristiwa; doa sinkron |
| Amazon MQ | Pemetaan sumber acara |
| Layanan Email Amazon Sederhana | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Layanan Pemberitahuan Sederhana Amazon | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Layanan Antrian Sederhana Amazon | Pemetaan sumber acara |
| Amazon Simple Storage Service (Amazon S3) | Digerakkan oleh peristiwa; pemanggilan asinkron |
| Batch Layanan Penyimpanan Sederhana Amazon | Digerakkan oleh peristiwa; doa sinkron |
| Secrets Manager | Integrasi khusus |
| AWS Step Functions | Digerakkan oleh peristiwa; pemanggilan sinkron atau asinkron |
| VPCKisi Amazon | Digerakkan oleh peristiwa; doa sinkron |
| AWS X-Ray | Integrasi khusus |

Menggunakan Lambda dengan Apache Kafka yang dikelola sendiri

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Lambda mendukung [Apache Kafka](#) sebagai [sumber peristiwa](#). Apache Kafka adalah platform streaming peristiwa sumber terbuka yang mendukung beban kerja seperti alur data dan analisis streaming.

Anda dapat menggunakan layanan Kafka AWS terkelola Amazon Managed Streaming for Apache Kafka (MSKAmazon), atau cluster Kafka yang dikelola sendiri. Untuk detail tentang menggunakan Lambda dengan AmazonMSK, lihat. [Menggunakan Lambda dengan Amazon MSK](#)

Topik ini menjelaskan cara menggunakan Lambda dengan klaster Kafka yang dikelola sendiri. Dalam AWS terminologi, cluster yang dikelola sendiri mencakup cluster Kafka yang tidak AWS dihosting. Misalnya, Anda dapat meng-host cluster Kafka Anda dengan penyedia cloud seperti [Confluent](#) Cloud.

Apache Kafka sebagai sumber acara beroperasi mirip dengan menggunakan Amazon Simple Queue Service (AmazonSQS) atau Amazon Kinesis. Lambda melakukan polling secara internal untuk pesan baru dari sumber peristiwa, lalu memanggil fungsi Lambda target secara sinkron. Lambda membaca pesan dalam batch dan menyediakan ini untuk fungsi Anda sebagai muatan acara. Ukuran batch maksimum dapat dikonfigurasi. (Default adalah 100 pesan.)

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Untuk sumber peristiwa berbasis Kafka, Lambda mendukung parameter kontrol pemrosesan, seperti jendela batching dan ukuran batch. Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Untuk contoh cara menggunakan Kafka yang dikelola sendiri sebagai sumber acara, lihat [Menggunakan Apache Kafka yang dihosting sendiri sebagai sumber acara](#) di Blog Komputasi. AWS Lambda AWS

Topik

- [Contoh peristiwa](#)
- [Mengkonfigurasi sumber acara Apache Kafka yang dikelola sendiri untuk Lambda](#)
- [Memproses pesan Apache Kafka yang dikelola sendiri dengan Lambda](#)
- [Menggunakan pemfilteran acara dengan sumber acara Apache Kafka yang dikelola sendiri](#)
- [Menangkap batch yang dibuang untuk sumber acara Apache Kafka yang dikelola sendiri](#)
- [Memecahkan masalah kesalahan pemetaan sumber acara Apache Kafka yang dikelola sendiri](#)

Contoh peristiwa

Lambda mengirimkan batch pesan dalam parameter peristiwa ketika memanggil fungsi Lambda Anda. Muatan peristiwa berisi array pesan. Setiap item array berisi detail dari topik Kafka dan pengidentifikasi Kafka partisi, bersama-sama dengan stempel waktu dan pesan berkode base64.

```
{
  "eventSource": "SelfManagedKafka",
  "bootstrapServers": "b-2.demo-cluster-1.a1bcde.c1.kafka.us-east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-east-1.amazonaws.com:9092",
  "records": {
    "mytopic-0": [
      {
        "topic": "mytopic",
        "partition": 0,
        "offset": 15,
        "timestamp": 1545084650987,
        "timestampType": "CREATE_TIME",
        "key": "abcDEFghiJKLmnoPQRstuVWXYZ1234==",
        "value": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
        "headers": [
          {
            "headerKey": [
              104,
              101,
              97,
```

```
        100,  
        101,  
        114,  
        86,  
        97,  
        108,  
        117,  
        101  
    ]  
  }  
] }  
] }  
] }  
}
```

Mengonfigurasi sumber acara Apache Kafka yang dikelola sendiri untuk Lambda

Sebelum Anda membuat pemetaan sumber peristiwa untuk cluster Apache Kafka yang dikelola sendiri, Anda perlu memastikan bahwa klaster Anda dan tempat VPC tinggalnya dikonfigurasi dengan benar. Anda juga perlu memastikan bahwa [peran eksekusi fungsi Lambda Anda memiliki izin](#) yang diperlukan IAM.

Ikuti petunjuk di bagian berikut untuk mengonfigurasi cluster Apache Kafka dan fungsi Lambda yang dikelola sendiri. Untuk mempelajari cara membuat pemetaan sumber peristiwa, lihat [the section called “Menambahkan klaster Kafka sebagai sumber peristiwa”](#).

Topik

- [Otentikasi cluster Kafka](#)
- [Konfigurasi jaringan](#)
- [API akses dan izin fungsi Lambda](#)

Otentikasi cluster Kafka

Lambda mendukung beberapa metode untuk mengautentikasi dengan klaster Apache Kafka yang dikelola sendiri. Pastikan Anda mengonfigurasi cluster Kafka untuk menggunakan salah satu metode otentikasi yang didukung ini. Untuk informasi lebih lanjut tentang keamanan Kafka, lihat bagian [Keamanan](#) dari dokumentasi Kafka.

VPC akses

Jika hanya pengguna Kafka yang VPC mengakses broker Kafka Anda, Anda harus mengonfigurasi sumber acara Kafka untuk akses Amazon Virtual Private Cloud (AmazonVPC).

SASL/SCRAM otentikasi

Lambda mendukung otentikasi Simple Authentication and Security Layer/Salted Challenge Response Authentication Mechanism (SASL/SCRAM) otentikasi dengan enkripsi Transport Layer Security (TLS). SASL_SSL Lambda mengirimkan kredensial terenkripsi untuk mengautentikasi dengan kluster. Lambda tidak mendukung SASL/SCRAM dengan plaintext (PLAIN). SASL_PLAINTEXT Untuk informasi selengkapnya tentang SASL/SCRAM otentikasi, lihat [RFC5802](#).

Lambda juga mendukung SASL/PLAIN otentikasi. Karena mekanisme ini menggunakan kredensial teks yang jelas, koneksi ke server harus menggunakan TLS enkripsi untuk memastikan bahwa kredensialnya dilindungi.

Untuk SASL autentikasi, Anda menyimpan kredensial masuk sebagai rahasia. AWS Secrets Manager Untuk informasi selengkapnya tentang menggunakan Secrets Manager, lihat [Tutorial: Membuat dan mengambil rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Important

Untuk menggunakan Secrets Manager untuk otentikasi, rahasia harus disimpan di AWS wilayah yang sama dengan fungsi Lambda Anda.

TLS otentikasi timbal balik

Mutual TLS (mTLS) menyediakan otentikasi dua arah antara klien dan server. Klien mengirimkan sertifikat ke server untuk server untuk memverifikasi klien, dan server mengirimkan sertifikat ke klien untuk klien untuk memverifikasi server.

Dalam Apache Kafka yang dikelola sendiri, Lambda bertindak sebagai klien. Anda mengonfigurasi sertifikat klien (sebagai rahasia di Secrets Manager) untuk mengautentikasi Lambda dengan broker Kafka Anda. Sertifikat klien harus ditandatangani oleh CA di toko kepercayaan server.


Cluster Kafka mengirimkan sertifikat server ke Lambda untuk mengautentikasi broker Kafka dengan Lambda. Sertifikat server dapat berupa sertifikat CA publik atau sertifikat CA/Self-signed private.

Sertifikat CA publik harus ditandatangani oleh otoritas sertifikat (CA) yang ada di toko kepercayaan Lambda. Untuk sertifikat CA/Self-signed privat, Anda mengonfigurasi sertifikat CA root server (sebagai rahasia di Secrets Manager). Lambda menggunakan sertifikat root untuk memverifikasi broker Kafka.

Untuk informasi selengkapnya tentang mTLS, lihat [Memperkenalkan TLS autentikasi timbal balik untuk Amazon MSK sebagai sumber peristiwa](#).

Mengonfigurasi rahasia sertifikat klien

AUTHRahasia CLIENT CERTIFICATE TLS __ memerlukan bidang sertifikat dan bidang kunci pribadi. Untuk kunci pribadi terenkripsi, rahasianya memerlukan kata sandi kunci pribadi. Baik sertifikat dan kunci pribadi harus dalam PEM format.

 Note

Lambda mendukung [PBES1](#) (tetapi tidak [PBES2](#)) algoritma enkripsi kunci pribadi.

Bidang sertifikat harus berisi daftar sertifikat, dimulai dengan sertifikat klien, diikuti oleh sertifikat perantara, dan diakhiri dengan sertifikat root. Setiap sertifikat harus dimulai pada baris baru dengan struktur berikut:

```
-----BEGIN CERTIFICATE-----
    <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager mendukung rahasia hingga 65.536 byte, yang merupakan ruang yang cukup untuk rantai sertifikat yang panjang.

Kunci pribadi harus dalam format [PKCS#8](#), dengan struktur berikut:

```
-----BEGIN PRIVATE KEY-----
    <private key contents>
-----END PRIVATE KEY-----
```

Untuk kunci pribadi terenkripsi, gunakan struktur berikut:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
<private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

Contoh berikut menunjukkan isi rahasia untuk m TLS otentikasi menggunakan kunci pribadi terenkripsi. Untuk kunci pribadi terenkripsi, sertakan kata sandi kunci pribadi dalam rahasia.

```
{"privateKeyPassword":"testpassword",
"certificate":"-----BEGIN CERTIFICATE-----
MIIe5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPim040s1cRqtFHxoa10QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFGjCCA2qgAwIBAgIQdJNZd6uFf9hbNC5RdfmHrzANBqkqhkiG9w0BAQsFADBB
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
-----END CERTIFICATE-----",
"privateKey":"-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDANBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzg09IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}
```

Mengkonfigurasi rahasia sertifikat CA root server

Anda membuat rahasia ini jika broker Kafka Anda menggunakan TLS enkripsi dengan sertifikat yang ditandatangani oleh CA pribadi. Anda dapat menggunakan TLS enkripsi untuk VPC, SASL/SCRAM, SASL/PLAIN, atau m TLS otentikasi.

Rahasia sertifikat CA root server memerlukan bidang yang berisi sertifikat root CA broker Kafka dalam PEM format. Contoh berikut menunjukkan struktur rahasia.

```
{"certificate":"-----BEGIN CERTIFICATE-----
MIID7zCCAtagAwIBAgIBADANBgkqhkiG9w0BAQsFADCBMDELMAkGA1UEBhMCVVMx
EDA0BgNVBAGTB0FyaXpvbmExEzARBgNVBAcTC1Njb3R0c2RhbGUxJTAjBgNVBAoT
HFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4x0zA5BgNVBAMTM1N0YXJmaWVs
ZCBTZjJ2aWNLcyBSb290IENlcnRpZmljYXR1IEF1dG...
-----END CERTIFICATE-----"
```

```
}
```

Konfigurasi jaringan

Agar Lambda dapat menggunakan cluster Kafka Anda sebagai sumber peristiwa, Lambda memerlukan akses ke Amazon tempat klaster VPC Anda berada. Kami menyarankan Anda menerapkan AWS PrivateLink [VPCtitik akhir](#) untuk Lambda untuk mengakses Anda. VPC Terapkan titik akhir untuk Lambda dan (). AWS Security Token Service AWS STS Jika broker menggunakan otentikasi, gunakan juga VPC endpoint untuk Secrets Manager. Jika Anda mengonfigurasi [tujuan saat kegagalan](#), gunakan juga VPC titik akhir untuk layanan tujuan.

Atau, pastikan bahwa yang VPC terkait dengan cluster Kafka Anda mencakup satu NAT gateway per subnet publik. Untuk informasi selengkapnya, lihat [the section called “Akses internet untuk VPC fungsi”](#).

Jika Anda menggunakan VPC titik akhir, Anda juga harus mengonfigurasinya untuk [mengaktifkan DNS nama pribadi](#).

Saat Anda membuat pemetaan sumber peristiwa untuk cluster Apache Kafka yang dikelola sendiri, Lambda memeriksa apakah Elastic Network Interfaces (ENIs) sudah ada untuk subnet dan grup keamanan klaster Anda. VPC Jika Lambda menemukan yang ada ENIs, ia mencoba untuk menggunakannya kembali. Jika tidak, Lambda membuat yang baru ENIs untuk terhubung ke sumber acara dan memanggil fungsi Anda.

Note

Fungsi Lambda selalu berjalan di dalam yang VPCs dimiliki oleh layanan Lambda. Ini VPCs dikelola secara otomatis oleh layanan dan tidak terlihat oleh pelanggan. Anda juga dapat menghubungkan fungsi Anda ke AmazonVPC. Dalam kedua kasus tersebut, VPC konfigurasi fungsi Anda tidak memengaruhi pemetaan sumber peristiwa. Hanya konfigurasi sumber acara yang VPC menentukan bagaimana Lambda terhubung ke sumber acara Anda.

Untuk informasi selengkapnya tentang mengonfigurasi jaringan, lihat [Menyiapkan AWS Lambda dengan cluster Apache Kafka VPC di dalam Blog Komputasi AWS](#) .

VPCaturan kelompok keamanan

Konfigurasi grup keamanan untuk Amazon VPC yang berisi klaster Anda dengan aturan berikut (minimal):

- Aturan masuk - Izinkan semua lalu lintas di port broker Kafka untuk grup keamanan yang ditentukan untuk sumber acara Anda. Kafka menggunakan port 9092 secara default.
- Aturan keluar - Izinkan semua lalu lintas di port 443 untuk semua tujuan. Izinkan semua lalu lintas di port broker Kafka untuk grup keamanan yang ditentukan untuk sumber acara Anda. Kafka menggunakan port 9092 secara default.
- Jika Anda menggunakan VPC titik akhir alih-alih NAT gateway, grup keamanan yang terkait dengan VPC titik akhir harus mengizinkan semua lalu lintas masuk pada port 443 dari grup keamanan sumber acara.

Bekerja dengan titik VPC akhir

Saat Anda menggunakan VPC titik akhir, API panggilan untuk memanggil fungsi Anda dirutekan melalui titik akhir ini menggunakan. ENIs Kepala layanan Lambda perlu memanggil `sts:AssumeRole` dan `lambda:InvokeFunction` pada peran dan fungsi apa pun yang menggunakannya. ENIs

Secara default, VPC titik akhir memiliki IAM kebijakan yang terbuka. Praktik terbaik adalah membatasi kebijakan ini untuk memungkinkan hanya prinsipal tertentu untuk melakukan tindakan yang diperlukan menggunakan titik akhir itu. Untuk memastikan bahwa pemetaan sumber peristiwa Anda dapat menjalankan fungsi Lambda Anda, kebijakan VPC titik akhir harus mengizinkan prinsip layanan Lambda untuk memanggil dan. `sts:AssumeRole` `lambda:InvokeFunction` Membatasi kebijakan VPC titik akhir Anda untuk mengizinkan hanya API panggilan yang berasal dari organisasi Anda mencegah pemetaan sumber peristiwa berfungsi dengan baik.

Contoh kebijakan VPC endpoint berikut menunjukkan cara memberikan akses yang diperlukan ke prinsipal layanan Lambda untuk titik akhir AWS STS dan Lambda.

Example VPCkebijakan titik akhir - AWS STS titik akhir

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "*"
    }
  ]
}
```



```

    }
  ]
}

```

Example VPCkebijakan titik akhir - Titik akhir Lambda

```

{
  "Statement": [
    {
      "Action": "lambda:InvokeFunction",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "*"
    }
  ]
}

```

Jika broker Kafka Anda menggunakan otentikasi, Anda juga dapat membatasi kebijakan VPC titik akhir untuk titik akhir Secrets Manager. Untuk memanggil Secrets ManagerAPI, Lambda menggunakan peran fungsi Anda, bukan kepala layanan Lambda. Contoh berikut menunjukkan kebijakan titik akhir Secrets Manager.

Example VPCkebijakan endpoint - titik akhir Secrets Manager

```

{
  "Statement": [
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "customer_function_execution_role_arn"
        ]
      },
      "Resource": "customer_secret_arn"
    }
  ]
}

```

Jika Anda memiliki tujuan pada kegagalan yang dikonfigurasi, Lambda juga menggunakan peran fungsi Anda untuk memanggil `s3:PutObject` salah satunya `publish`, `sqs:sendMessage` atau menggunakan `Lambda-managed`. ENIs

API akses dan izin fungsi Lambda

Selain mengakses cluster Kafka yang dikelola sendiri, fungsi Lambda Anda memerlukan izin untuk melakukan berbagai tindakan. API Anda menambahkan izin ini ke [peran eksekusi](#) fungsi. Jika pengguna Anda memerlukan akses ke API tindakan apa pun, tambahkan izin yang diperlukan ke kebijakan identitas untuk AWS Identity and Access Management (IAM) pengguna atau peran.

Izin fungsi Lambda diperlukan

Untuk membuat dan menyimpan log dalam grup log di Amazon CloudWatch Logs, fungsi Lambda Anda harus memiliki izin berikut dalam peran pelaksanaannya:

- [log: CreateLogGroup](#)
- [log: CreateLogStream](#)
- [log: PutLogEvents](#)

Izin fungsi Lambda opsional

Fungsi Lambda Anda mungkin juga memerlukan izin untuk:

- Jelaskan rahasia Secrets Manager Anda.
- Akses AWS Key Management Service (AWS KMS) kunci terkelola pelanggan Anda.
- Akses Amazon VPC.
- Kirim catatan pemanggilan yang gagal ke tujuan.

Secrets Manager dan AWS KMS izin

Bergantung pada jenis kontrol akses yang Anda konfigurasi untuk broker Kafka Anda, fungsi Lambda Anda mungkin memerlukan izin untuk mengakses rahasia Secrets Manager Anda atau untuk mendekripsi kunci yang dikelola pelanggan Anda. AWS KMS Untuk mengakses sumber daya ini, peran eksekusi fungsi Anda harus memiliki izin berikut:

- [manajer rahasia: GetSecretValue](#)
- [kms:Decrypt](#)

VPCizin

Jika hanya pengguna dalam a yang VPC dapat mengakses cluster Apache Kafka yang dikelola sendiri, fungsi Lambda Anda harus memiliki izin untuk mengakses sumber daya Amazon Anda. VPC Sumber daya ini termasuk AndaVPC, subnet, grup keamanan, dan antarmuka jaringan. Untuk mengakses sumber daya ini, peran eksekusi fungsi Anda harus memiliki izin berikut:

- [EC2: CreateNetworkInterface](#)
- [EC2: DescribeNetworkInterfaces](#)
- [EC2: DescribeVpcs](#)
- [EC2: DeleteNetworkInterface](#)
- [EC2: DescribeSubnets](#)
- [EC2: DescribeSecurityGroups](#)

Menambahkan izin ke peran eksekusi

[Untuk mengakses AWS layanan lain yang digunakan cluster Apache Kafka yang dikelola sendiri, Lambda menggunakan kebijakan izin yang Anda tentukan dalam peran eksekusi fungsi Lambda Anda.](#)

Secara default, Lambda tidak diizinkan untuk melakukan tindakan yang diperlukan atau opsional untuk klaster Apache Kafka yang dikelola sendiri. Anda harus membuat dan mendefinisikan tindakan ini dalam [kebijakan IAM kepercayaan](#) untuk peran eksekusi Anda. Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan Lambda mengakses sumber daya Amazon VPC Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ],
```

```
    "Resource": "*"
  }
]
}
```

Memberikan akses kepada pengguna dengan kebijakan IAM

Secara default, pengguna dan peran tidak memiliki izin untuk melakukan [API operasi sumber peristiwa](#). Untuk memberikan akses ke pengguna di organisasi atau akun Anda, Anda membuat atau memperbarui kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat [Mengontrol akses ke AWS sumber daya menggunakan kebijakan](#) di Panduan IAM Pengguna.

Memproses pesan Apache Kafka yang dikelola sendiri dengan Lambda

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Topik

- [Menambahkan klaster Kafka sebagai sumber peristiwa](#)
- [Parameter konfigurasi Apache Kafka yang dikelola sendiri](#)
- [Menggunakan klaster Kafka sebagai sumber peristiwa](#)
- [Posisi awal polling dan streaming](#)
- [Penskalaan otomatis sumber peristiwa Kafka](#)
- [CloudWatch Metrik Amazon](#)

Menambahkan klaster Kafka sebagai sumber peristiwa

[Untuk membuat pemetaan sumber peristiwa, tambahkan cluster Kafka Anda sebagai pemicu fungsi Lambda menggunakan konsol Lambda, sebuah, atau AWS SDK\(\).AWS Command Line InterfaceAWS CLI](#)

Bagian ini menjelaskan cara membuat pemetaan sumber peristiwa menggunakan konsol Lambda dan AWS CLI.

Prasyarat

- Klaster Apache Kafka yang dikelola sendiri. Lambda mendukung Apache Kafka versi 0.10.1.0 dan yang lebih baru.
- [Peran eksekusi](#) dengan izin untuk mengakses AWS sumber daya yang digunakan cluster Kafka yang dikelola sendiri.

ID grup konsumen yang dapat disesuaikan

Saat mengatur Kafka sebagai sumber acara, Anda dapat menentukan ID grup konsumen. ID grup konsumen ini adalah pengenal yang ada untuk grup konsumen Kafka yang Anda inginkan agar fungsi Lambda Anda bergabung. Anda dapat menggunakan fitur ini untuk memigrasikan pengaturan pemrosesan catatan Kafka yang sedang berlangsung dengan mulus dari konsumen lain ke Lambda.

Jika Anda menentukan ID grup konsumen dan ada poller aktif lainnya dalam grup konsumen tersebut, Kafka mendistribusikan pesan ke semua konsumen. Dengan kata lain, Lambda tidak menerima semua pesan untuk topik Kafka. Jika Anda ingin Lambda menangani semua pesan dalam topik, matikan poller lain di grup konsumen tersebut.

Selain itu, jika Anda menentukan ID grup konsumen, dan Kafka menemukan grup konsumen yang sudah ada dengan ID yang sama, Lambda mengabaikan parameter untuk `StartingPosition` pemetaan sumber peristiwa Anda. Sebaliknya, Lambda mulai memproses catatan sesuai dengan offset yang dilakukan dari kelompok konsumen. Jika Anda menentukan ID grup konsumen, dan Kafka tidak dapat menemukan grup konsumen yang ada, maka Lambda mengonfigurasi sumber acara Anda dengan yang ditentukan. `StartingPosition`

ID grup konsumen yang Anda tentukan harus unik di antara semua sumber acara Kafka Anda. Setelah membuat pemetaan sumber acara Kafka dengan ID grup konsumen yang ditentukan, Anda tidak dapat memperbarui nilai ini.

Menambahkan klaster Kafka yang dikelola sendiri (konsol)

Ikuti langkah-langkah untuk menambahkan klaster Apache Kafka yang dikelola sendiri dan topik Kafka sebagai pemicu untuk fungsi Lambda Anda.

Untuk menambahkan pemicu Apache Kafka untuk fungsi Lambda Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Lambda Anda.

3. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.
4. Pada Konfigurasi pemicu, lakukan hal berikut:
 - a. Pilih jenis pemicu Apache Kafka.
 - b. Untuk Server bootstrap, masukkan alamat pasangan host dan port broker Kafka di klaster Anda, lalu pilih Tambahkan. Ulangi untuk setiap broker Kafka di klaster.
 - c. Untuk Nama topik, masukkan nama topik Kafka yang digunakan untuk menyimpan catatan dalam klaster.
 - d. (Opsional) Untuk Ukuran batch, masukkan jumlah maksimum catatan yang akan diterima dalam satu batch.
 - e. Untuk jendela Batch, masukkan jumlah maksimum detik yang dihabiskan Lambda untuk mengumpulkan catatan sebelum menjalankan fungsi.
 - f. (Opsional) Untuk ID grup Konsumen, masukkan ID grup konsumen Kafka untuk bergabung.
 - g. (Opsional) Untuk posisi Mulai, pilih Terbaru untuk mulai membaca aliran dari catatan terbaru, Potong cakrawala untuk memulai pada catatan paling awal yang tersedia, atau Pada stempel waktu untuk menentukan stempel waktu untuk mulai membaca.
 - h. (Opsional) Untuk VPC, pilih Amazon VPC untuk cluster Kafka Anda. Kemudian, pilih VPCsubnet dan grup VPC keamanan.

Pengaturan ini diperlukan jika hanya pengguna dalam VPC akses broker Anda.

- i. (Opsional) Untuk Otentikasi, pilih Tambah, lalu lakukan hal berikut:
 - i. Pilih protokol akses atau otentikasi broker Kafka di cluster Anda.
 - Jika broker Kafka Anda menggunakan SASL/PLAIN otentikasi, pilih BASIC _ . AUTH
 - Jika broker Anda menggunakan SASL/SCRAM otentikasi, pilih salah satu SCRAM protokol SASL_ .
 - Jika Anda mengonfigurasi TLS otentikasi m, pilih protokol CLIENT_ _ CERTIFICATE TLS _ AUTH.
 - ii. Untuk TLS otentikasi SASL/SCRAM atau m, pilih kunci rahasia Secrets Manager yang berisi kredensi untuk cluster Kafka Anda.
- j. (Opsional) Untuk Enkripsi, pilih rahasia Secrets Manager yang berisi sertifikat CA root yang digunakan broker Kafka Anda untuk TLS enkripsi, jika broker Kafka Anda menggunakan sertifikat yang ditandatangani oleh CA pribadi.

Pengaturan ini berlaku untuk TLS enkripsi untuk SASL/SCRAM atau SASL/PLAIN, dan untuk TLS otentikasi m.

- k. Untuk membuat pemicu dalam status nonaktif untuk pengujian (disarankan), hapus Aktifkan pemicu. Atau, untuk segera mengaktifkan pemicu, pilih Aktifkan pemicu.

5. Untuk membuat pemicu, pilih Tambahkan.

Menambahkan kluster Kafka yang dikelola sendiri (AWS CLI)

Gunakan contoh AWS CLI perintah berikut untuk membuat dan melihat pemicu Apache Kafka yang dikelola sendiri untuk fungsi Lambda Anda.

Menggunakan SASL/SCRAM

Jika pengguna Kafka mengakses broker Kafka Anda melalui internet, tentukan rahasia Secrets Manager yang Anda buat untuk SASL/SCRAM otentikasi. Contoh berikut menggunakan [create-event-source-mapping](#) AWS CLI perintah untuk memetakan fungsi Lambda bernama `my-kafka-function` ke topik Kafka bernama `AWSKafkaTopic`

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration Type=SASL_SCRAM_512_AUTH,URI=arn:aws:secretsmanager:us-east-1:111122223333:secret:MyBrokerSecretName \
  --function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":  
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Menggunakan a VPC

Jika hanya pengguna Kafka yang VPC mengakses broker Kafka Anda, Anda harus menentukan, subnet VPC, dan VPC grup keamanan Anda. Contoh berikut menggunakan [create-event-source-mapping](#) AWS CLI perintah untuk memetakan fungsi Lambda bernama `my-kafka-function` ke topik Kafka bernama `AWSKafkaTopic`

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration '[{"Type": "VPC_SUBNET", "URI":  
"subnet:subnet-0011001100"}, {"Type": "VPC_SUBNET", "URI":  
"subnet:subnet-0022002200"}, {"Type": "VPC_SECURITY_GROUP", "URI":  
"security_group:sg-0123456789"}]' \
```

```
--function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
--self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Melihat status menggunakan AWS CLI

Contoh berikut menggunakan [get-event-source-mapping](#) AWS CLI perintah untuk menggambarkan status pemetaan sumber peristiwa yang Anda buat.

```
aws lambda get-event-source-mapping
--uuid dh38738e-992b-343a-1077-3478934hjkfd7
```

Parameter konfigurasi Apache Kafka yang dikelola sendiri

Semua jenis sumber acara Lambda berbagi hal yang sama [CreateEventSourceMapping](#) dan [UpdateEventSourceMapping](#) API operasi. Namun, hanya beberapa parameter yang berlaku untuk Apache Kafka.

| Parameter | Diperlukan | Default | Catatan |
|--------------------------------|------------|------------|---|
| BatchSize | T | 100 | Maksimum: 10.000. |
| Diaktifkan | N | Diaktifkan | none |
| FunctionName | T | N/A | none |
| FilterCriteria | T | N/A | Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda |
| MaximumBatchingWindowInSeconds | T | 500 ms | Perilaku batching |
| SelfManagedEventSource | T | N/A | Daftar Broker Kafka. Hanya dapat mengatur di Create |

| Parameter | Diperlukan | Default | Catatan |
|-----------------------------------|------------|---|---|
| SelfManagedKafkaEventSourceConfig | T | Berisi ConsumerGroupId bidang yang default ke nilai unik. | Hanya dapat mengatur di Create |
| SourceAccessConfigurations | T | Tidak ada kredensial | VPCinformasi atau kredensi otentikasi untuk cluster Untuk SASL_PLAIN, atur ke BASIC_AUTH |
| StartingPosition | T | N/A | AT_TIMESTAMP, TRIM_HORIZON, atau LATEST Hanya dapat mengatur di Create |
| StartingPositionTimestamp | T | N/A | Diperlukan jika StartingPosition disetel ke AT_TIMESTAMP |
| Topik | T | N/A | Nama topik Hanya dapat mengatur di Create |

Menggunakan klaster Kafka sebagai sumber peristiwa

[Saat Anda menambahkan Apache Kafka atau MSK cluster Amazon sebagai pemicu fungsi Lambda Anda, cluster digunakan sebagai sumber peristiwa.](#)

Lambda membaca data peristiwa dari topik Kafka yang Anda tentukan seperti Topics dalam [CreateEventSourceMapping](#) permintaan, berdasarkan StartingPosition yang Anda tentukan. Setelah pemrosesan berhasil, topik Kafka Anda dijalankan untuk klaster Kafka Anda.

Jika Anda menentukan `StartingPosition` sebagai `LATEST`, Lambda mulai membaca dari pesan terbaru di setiap partisi milik topik. Karena mungkin ada beberapa penundaan setelah konfigurasi pemicu sebelum Lambda mulai membaca pesan, Lambda tidak membaca pesan apa pun yang dihasilkan selama jendela ini.

Lambda memproses catatan dari satu atau beberapa partisi topik Kafka yang Anda tentukan dan kirimkan JSON muatan ke fungsi Anda. Bila lebih banyak rekaman tersedia, Lambda terus memproses catatan dalam batch, berdasarkan `BatchSize` nilai yang Anda tentukan dalam [CreateEventSourceMapping](#) permintaan, hingga fungsi Anda mengikuti topik.

Jika fungsi Anda mengembalikan kesalahan untuk salah satu pesan dalam batch, Lambda mencoba ulang seluruh batch pesan sampai berhasil diproses atau pesan berakhir. Anda dapat mengirim catatan yang gagal dalam semua upaya percobaan ulang ke [tujuan yang gagal untuk diproses](#) nanti.

Note

Sementara fungsi Lambda biasanya memiliki batas waktu tunggu maksimum 15 menit, pemetaan sumber acara untuk Amazon, Apache Kafka yang dikelola sendiri, MSK Amazon DocumentDB, dan Amazon MQ untuk ActiveMQ dan RabbitMQ hanya mendukung fungsi dengan batas waktu tunggu maksimum 14 menit. Kendala ini memastikan bahwa pemetaan sumber peristiwa dapat menangani kesalahan fungsi dan percobaan ulang dengan benar.

Posisi awal polling dan streaming

Ketahui bahwa polling streaming selama pembuatan dan pembaruan pemetaan sumber acara pada akhirnya konsisten.

- Selama pembuatan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk memulai acara polling dari aliran.
- Selama pembaruan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk menghentikan dan memulai kembali acara pemungutan suara dari aliran.

Perilaku ini berarti bahwa jika Anda menentukan `LATEST` sebagai posisi awal untuk aliran, pemetaan sumber peristiwa dapat melewatkan peristiwa selama pembuatan atau pembaruan. Untuk memastikan bahwa tidak ada peristiwa yang terlewatkan, tentukan posisi awal aliran sebagai `TRIM_HORIZON` atau `AT_TIMESTAMP`.

Penskalaan otomatis sumber peristiwa Kafka

Saat Anda awalnya membuat [sumber acara](#) Apache Kafka, Lambda mengalokasikan satu konsumen untuk memproses semua partisi dalam topik Kafka. Setiap konsumen memiliki beberapa prosesor yang berjalan secara paralel untuk menangani peningkatan beban kerja. Selain itu, Lambda secara otomatis meningkatkan atau menurunkan jumlah konsumen, berdasarkan beban kerja. Untuk mempertahankan pemesanan pesan di setiap partisi, jumlah maksimum konsumen adalah satu konsumen per partisi dalam topik.

Dalam interval satu menit, Lambda mengevaluasi lag offset konsumen dari semua partisi dalam topik. Jika lag terlalu tinggi, partisi menerima pesan lebih cepat daripada yang dapat diproses Lambda. Jika perlu, Lambda menambahkan atau menghapus konsumen dari topik tersebut. Proses penskalaan penambahan atau penghapusan konsumen terjadi dalam waktu tiga menit setelah evaluasi.

Jika fungsi target Lambda Anda kelebihan beban, Lambda mengurangi jumlah konsumen. Tindakan ini mengurangi beban kerja pada fungsi dengan mengurangi jumlah pesan yang dapat konsumen ambil dan kirim ke fungsi.

Untuk memantau throughput dari topik Kafka Anda, Anda dapat melihat metrik konsumen Apache Kafka, seperti `consumer_lag` dan `consumer_offset`. Untuk memeriksa berapa banyak fungsi invokasi yang terjadi secara paralel, Anda juga dapat memantau [metrik konkurensi](#) untuk fungsi Anda.

CloudWatch Metrik Amazon

Lambda memancarkan `OffsetLag` metrik saat fungsi Anda memproses catatan. Nilai metrik ini adalah perbedaan offset antara catatan terakhir yang ditulis ke topik sumber peristiwa Kafka dan catatan terakhir yang diproses oleh grup konsumen fungsi Anda. Anda dapat menggunakan `OffsetLag` untuk memperkirakan latensi antara saat catatan ditambahkan dan kapan grup konsumen Anda memprosesnya.

Tren yang meningkat `OffsetLag` dapat menunjukkan masalah dengan poller dalam kelompok konsumen fungsi Anda. Untuk informasi selengkapnya, lihat [Lihat metrik untuk fungsi Lambda](#).

Menggunakan pemfilteran acara dengan sumber acara Apache Kafka yang dikelola sendiri

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called “Penyaringan acara”](#).

Bagian ini berfokus pada penyaringan acara untuk sumber acara Apache Kafka yang dikelola sendiri.

Topik

- [Dasar-dasar penyaringan acara Apache Kafka yang dikelola sendiri](#)

Dasar-dasar penyaringan acara Apache Kafka yang dikelola sendiri

Misalkan produser menulis pesan ke topik di cluster Apache Kafka yang dikelola sendiri, baik dalam JSON format yang valid atau sebagai string biasa. Contoh catatan akan terlihat seperti berikut, dengan pesan dikonversi ke string yang dikodekan Base64 di bidang. `value`

```
{
  "mytopic-0": [
    {
      "topic": "mytopic",
      "partition": 0,
      "offset": 15,
      "timestamp": 1545084650987,
      "timestampType": "CREATE_TIME",
      "value": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
      "headers": []
    }
  ]
}
```

Misalkan produser Apache Kafka Anda menulis pesan ke topik Anda dalam format berikut JSON.

```
{
  "device_ID": "AB1234",
  "session": {
    "start_time": "yyyy-mm-ddThh:mm:ss",
    "duration": 162
  }
}
```

Anda dapat menggunakan `value` kunci untuk memfilter catatan. Misalkan Anda ingin memfilter hanya catatan-catatan di mana `device_ID` dimulai dengan huruf AB. `FilterCriteriaObjeknya` adalah sebagai berikut.

```
{
```

```

    "Filters": [
      {
        "Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"
      }
    ]
  }

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```

{
  "value": {
    "device_ID": [ { "prefix": "AB" } ]
  }
}

```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "value" : { "device_ID" : [ { "prefix": "AB" } ] } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```

aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/  
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :  
[ { \"prefix\": \"AB\" } ] } }"]}'

```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```

aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \

```

```
--filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"]}]'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : { "device_ID" : [ { "prefix": "AB" } ] } }'
```

Dengan Apache Kafka yang dikelola sendiri, Anda juga dapat memfilter catatan di mana pesannya adalah string biasa. Misalkan Anda ingin mengabaikan pesan-pesan di mana string adalah “kesalahan”. `FilterCriteriaObjek` akan terlihat sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"value\" : [ { \"anything-but\": [ \"error\" ] } ] }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```
{
  "value": [
    {
      "anything-but": [ "error" ]
    }
  ]
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "value" : [ { "anything-but": [ "error" ] } ] }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/  
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":  
[ \"error\" ] } ] }"]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":  
[ \"error\" ] } ] }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : [ { "anything-but": [ "error" ] } ] }'
```

Pesan Apache Kafka yang dikelola sendiri harus berupa UTF -8 string yang dikodekan, baik string biasa atau dalam format. JSON itu karena Lambda menerjemahkan array byte Kafka menjadi UTF -8 sebelum menerapkan kriteria filter. Jika pesan Anda menggunakan pengkodean lain, seperti UTF -16 atau ASCII, atau jika format pesan tidak cocok dengan format, Lambda `FilterCriteria` hanya memproses filter metadata. Tabel berikut merangkum perilaku spesifik:

| Format pesan masuk | Format pola filter untuk properti pesan | Tindakan yang dihasilkan |
|------------------------------------|---|--|
| Tali polos | Tali polos | Filter Lambda berdasarkan kriteria filter Anda. |
| Tali polos | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Tali polos | Valid JSON | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tali polos | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |
| String yang tidak dikodekan UTF -8 | JSON, string polos, atau tidak ada pola | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |

Menangkap batch yang dibuang untuk sumber acara Apache Kafka yang dikelola sendiri

Untuk menyimpan catatan pemanggilan pemetaan sumber peristiwa yang gagal, tambahkan tujuan ke pemetaan sumber peristiwa fungsi Anda. Setiap catatan yang dikirim ke tujuan adalah JSON dokumen dengan metadata tentang pemanggilan yang gagal. Anda dapat mengonfigurasi SNS topik Amazon, SQS antrian Amazon, atau bucket S3 sebagai tujuan. Peran eksekusi Anda harus memiliki izin untuk tujuan:

- Untuk SQS tujuan: [sqs: SendMessage](#)
- Untuk SNS tujuan: [SNS: Publikasikan](#)
- Untuk tujuan bucket S3: [s3: PutObject](#) dan [s3: ListBuckets](#)

Anda harus menerapkan VPC endpoint untuk layanan tujuan on-failure Anda di dalam cluster Apache Kafka Anda. VPC

Selain itu, jika Anda mengonfigurasi KMS kunci tujuan, Lambda memerlukan izin berikut tergantung pada jenis tujuan:

- Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk tujuan S3, [kms: GenerateDataKey diperlukan](#). Jika tujuan bucket KMS kunci dan S3 berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi agar memungkinkan `kms: GenerateDataKey`
- [Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk SQS tujuan, KMS: Decrypt dan kms: diperlukan. GenerateDataKey](#) Jika tujuan KMS kunci dan SQS antrean berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi untuk mengizinkan `KMS:Decrypt`, `kms:`, `kms:`, dan `kms:GenerateDataKey`. `DescribeKey` `ReEncrypt`
- [Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk SNS tujuan, KMS: Decrypt dan kms: diperlukan. GenerateDataKey](#) Jika tujuan KMS kunci dan SNS topik berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi untuk mengizinkan `KMS:Decrypt`, `kms:`, `kms:`, dan `kms:GenerateDataKey`. `DescribeKey` `ReEncrypt`

Mengonfigurasi tujuan yang gagal untuk pemetaan sumber acara Apache Kafka yang dikelola sendiri

Untuk mengonfigurasi tujuan saat gagal menggunakan konsol, ikuti langkah-langkah berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambahkan tujuan.
4. Untuk Sumber, pilih Pemanggilan pemetaan sumber acara.
5. Untuk pemetaan sumber peristiwa, pilih sumber peristiwa yang dikonfigurasi untuk fungsi ini.
6. Untuk Kondisi, pilih On failure. Untuk pemanggilan pemetaan sumber peristiwa, ini adalah satu-satunya kondisi yang diterima.
7. Untuk tipe Tujuan, pilih tipe tujuan yang Lambda kirimkan catatan pemanggilan.
8. Untuk Tujuan, pilih sumber daya.
9. Pilih Simpan.

Anda juga dapat mengonfigurasi tujuan pada kegagalan menggunakan file. AWS CLI Misalnya, [create-event-source-mapping](#) perintah berikut menambahkan pemetaan sumber peristiwa dengan tujuan SQS kegagalan ke: MyFunction

```
aws lambda create-event-source-mapping \  
--function-name "MyFunction" \  
--event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/  
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2 \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-  
east-1:123456789012:dest-queue"}}'
```

[update-event-source-mapping](#) Perintah berikut menambahkan tujuan kegagalan S3 ke sumber acara yang terkait dengan input: uuid

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:s3:::dest-bucket"}}'
```

Untuk menghapus tujuan, berikan string kosong sebagai argumen ke `destination-config` parameter:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

SNS dan SQS contoh catatan pemanggilan

Contoh berikut menunjukkan apa yang Lambda kirim ke SNS topik atau tujuan SQS antrian untuk pemanggilan sumber acara Kafka yang gagal. Setiap kunci di bawah `recordsInfo` berisi topik dan partisi Kafka, dipisahkan oleh tanda hubung. Misalnya, untuk kuncinya `"Topic-0"`, `Topic` adalah topik Kafka, dan `0` merupakan partisi. Untuk setiap topik dan partisi, Anda dapat menggunakan data offset dan stempel waktu untuk menemukan catatan pemanggilan asli.

```
{
  "requestContext": {
    "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
    "condition": "RetryAttemptsExhausted | MaximumPayloadSizeExceeded",
    "approximateInvokeCount": 1
  },
  "responseContext": { // null if record is MaximumPayloadSizeExceeded
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T00:38:06.021Z",
  "KafkaBatchInfo": {
    "batchSize": 500,
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
    "bootstrapServers": "...",
    "payloadSize": 2039086, // In bytes
    "recordsInfo": {
      "Topic-0": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
      },
      "Topic-1": {
```

```

        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
    }
}
}
}
}

```

Catatan pemanggilan contoh tujuan S3

Untuk tujuan S3, Lambda mengirimkan seluruh catatan pemanggilan bersama dengan metadata ke tujuan. Contoh berikut menunjukkan bahwa Lambda mengirim ke tujuan bucket S3 untuk pemanggilan sumber peristiwa Kafka yang gagal. Selain semua bidang dari contoh sebelumnya untuk SQS dan SNS tujuan, payload bidang berisi catatan pemanggilan asli sebagai string yang JSON diloloskan.

```

{
  "requestContext": {
    "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
    "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
    "approximateInvokeCount": 1
  },
  "responseContext": { // null if record is MaximumPayloadSizeExceeded
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T00:38:06.021Z",
  "KafkaBatchInfo": {
    "batchSize": 500,
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
    "bootstrapServers": "...",
    "payloadSize": 2039086, // In bytes
    "recordsInfo": {
      "Topic-0": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",

```

```

        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
    },
    "Topic-1": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
    }
}
},
"payload": "<Whole Event>" // Only available in S3
}

```

Tip

Sebaiknya aktifkan versi S3 di bucket tujuan Anda.

Memecahkan masalah kesalahan pemetaan sumber acara Apache Kafka yang dikelola sendiri

Topik berikut memberikan saran pemecahan masalah untuk kesalahan dan masalah yang mungkin Anda temui saat menggunakan Apache Kafka yang dikelola sendiri dengan Lambda. Jika Anda menemukan masalah yang tidak tercantum di sini, Anda dapat menggunakan tombol Umpan Balik di halaman ini untuk melaporkannya.

Untuk bantuan lebih lanjut tentang pemecahan masalah, kunjungi Pusat [AWS Pengetahuan](#).

Kesalahan otentikasi dan otorisasi

Jika salah satu izin yang diperlukan untuk mengkonsumsi data dari cluster Kafka tidak ada, Lambda menampilkan salah satu pesan kesalahan berikut dalam pemetaan sumber peristiwa di bawah.

LastProcessingResult

Pesan kesalahan

- [Cluster gagal mengotorisasi Lambda](#)

- [Otentikasi SASL gagal](#)
- [Server gagal mengautentikasi Lambda](#)
- [Lambda gagal mengautentikasi server](#)
- [Sertifikat atau kunci pribadi yang diberikan tidak valid](#)

Cluster gagal mengotorisasi Lambda

Untuk SASL/SCRAM atau mTLS, kesalahan ini menunjukkan bahwa pengguna yang disediakan tidak memiliki semua izin daftar kontrol akses (ACL) Kafka yang diperlukan berikut:

- DescribeConfigs Cluster
- Jelaskan Grup
- Baca Grup
- Jelaskan Topik
- Baca Topik

Saat Anda membuat Kafka ACL dengan `kafka-cluster` izin yang diperlukan, tentukan topik dan kelompokkan sebagai sumber daya. Nama topik harus cocok dengan topik dalam pemetaan sumber acara. Nama grup harus cocok dengan UUID pemetaan sumber peristiwa.

Setelah Anda menambahkan izin yang diperlukan ke peran eksekusi, mungkin perlu beberapa menit agar perubahan diterapkan.

Otentikasi SASL gagal

Untuk SASL/SCRAM atau SASL/PLAIN, kesalahan ini menunjukkan bahwa kredensyal masuk yang diberikan tidak valid.

Server gagal mengautentikasi Lambda

Kesalahan ini menunjukkan bahwa broker Kafka gagal mengautentikasi Lambda. Ini dapat terjadi karena salah satu alasan berikut:

- Anda tidak memberikan sertifikat klien untuk otentikasi mTLS.
- Anda memberikan sertifikat klien, tetapi broker Kafka tidak dikonfigurasi untuk menggunakan otentikasi mTLS.
- Sertifikat klien tidak dipercaya oleh broker Kafka.

Lambda gagal mengautentikasi server

Kesalahan ini menunjukkan bahwa Lambda gagal mengautentikasi broker Kafka. Ini dapat terjadi karena salah satu alasan berikut:

- Broker Kafka menggunakan sertifikat yang ditandatangani sendiri atau CA pribadi, tetapi tidak memberikan sertifikat CA root server.
- Sertifikat CA root server tidak cocok dengan root CA yang menandatangani sertifikat broker.
- Validasi nama host gagal karena sertifikat broker tidak berisi nama DNS broker atau alamat IP sebagai nama alternatif subjek.

Sertifikat atau kunci pribadi yang diberikan tidak valid

Kesalahan ini menunjukkan bahwa konsumen Kafka tidak dapat menggunakan sertifikat atau kunci pribadi yang disediakan. Pastikan sertifikat dan kunci menggunakan format PEM, dan bahwa enkripsi kunci pribadi menggunakan algoritma PBES1.

Kesalahan pemetaan sumber peristiwa

Katika Anda menambahkan kluster Apache Kafka Anda sebagai [sumber peristiwa](#) untuk fungsi Lambda Anda, jika fungsi Anda mengalami kesalahan, konsumen Kafka Anda berhenti memproses rekaman. Konsumen partisi topik adalah mereka yang berlangganan, membaca, dan memproses catatan Anda. Konsumen Kafka Anda lainnya dapat melanjutkan pemrosesan catatan, asalkan tidak mengalami kesalahan yang sama.

Untuk menentukan penyebab penghentian konsumen, periksa bidang `StateTransitionReason` dalam respons dari `EventSourceMapping`. Daftar berikut menjelaskan kesalahan sumber peristiwa yang dapat Anda terima:

ESM_CONFIG_NOT_VALID

Konfigurasi pemetaan sumber peristiwa tidak valid.

EVENT_SOURCE_AUTHN_ERROR

Lambda tidak dapat mengautentikasi sumber acara.

EVENT_SOURCE_AUTHZ_ERROR

Lambda tidak memiliki izin yang diperlukan untuk mengakses sumber acara.

FUNCTION_CONFIG_NOT_VALID

Konfigurasi fungsi tidak valid.

Note

Jika catatan peristiwa Lambda Anda melebihi batas ukuran yang diizinkan sebesar 6 MB, catatan dapat tidak diproses.

Memanggil fungsi Lambda menggunakan titik akhir Amazon Gateway API

Anda dapat membuat web API dengan HTTP titik akhir untuk fungsi Lambda Anda dengan menggunakan Amazon API Gateway. API Gateway menyediakan alat untuk membuat dan mendokumentasikan web APIs yang merutekan HTTP permintaan ke fungsi Lambda. Anda dapat mengamankan akses ke Anda API dengan kontrol otentikasi dan otorisasi. Anda APIs dapat melayani lalu lintas melalui internet atau hanya dapat diakses di dalam Anda VPC.

Sumber daya dalam Anda API menentukan satu atau lebih metode, seperti GET atau POST. Metode memiliki integrasi yang merutekan permintaan ke fungsi Lambda atau jenis integrasi lainnya. Anda dapat menentukan setiap sumber daya dan metode secara individual, atau menggunakan jenis sumber daya dan metode khusus untuk mencocokkan semua permintaan yang sesuai dengan suatu pola. [Sumber daya proksi](#) menangkap semua jalur di bawah sumber daya. ANY Metode ini menangkap semua HTTP metode.

Bagian-bagian

- [Memilih API tipe](#)
- [Menambahkan titik akhir ke fungsi Lambda Anda](#)
- [Integrasi proxy](#)
- [Format acara](#)
- [Format respons](#)
- [Izin](#)
- [Aplikasi sampel](#)
- [Tutorial: Menggunakan Lambda dengan Gateway API](#)
- [Menangani kesalahan Lambda dengan API Gateway API](#)

Memilih API tipe

API Gateway mendukung tiga jenis fungsi Lambda APIs yang memanggil:

- [HTTP API](#): Ringan, latensi rendah RESTful API.
- [REST API](#): Dapat disesuaikan, kaya fitur. RESTful API
- [WebSocket API](#): Sebuah web API yang memelihara koneksi persisten dengan klien untuk komunikasi full-duplex.

HTTP APIs dan REST APIs keduanya RESTful APIs memproses HTTP permintaan dan mengembalikan respons. HTTP APIs lebih baru dan dibangun dengan API Gateway versi 2 API. Fitur-fitur berikut ini baru untuk HTTP APIs:

HTTP API fitur

- Deployment otomatis – Saat Anda memodifikasi rute atau integrasi, mengubah deployment secara otomatis ke tahap yang deployment otomatisnya diaktifkan.
- Tahap default - Anda dapat membuat tahap default (`$default`) untuk melayani permintaan di jalur root API milik Anda URL. Untuk tahap yang diberi nama, Anda harus menyertakan nama tahap di awal jalur.
- CORS konfigurasi - Anda dapat mengonfigurasi API untuk menambahkan CORS header ke respons keluar, alih-alih menambahkannya secara manual dalam kode fungsi Anda.

REST APIs adalah klasik RESTful APIs yang didukung API Gateway sejak diluncurkan. REST APIs saat ini memiliki lebih banyak fitur penyesuaian, integrasi, dan manajemen.

REST API fitur

- Jenis integrasi - REST APIs mendukung integrasi Lambda kustom. Dengan integrasi kustom, Anda dapat mengirim hanya badan permintaan ke fungsi, atau menerapkan templat transformasi ke badan permintaan sebelum mengirimkannya ke fungsi.
- Kontrol akses — REST APIs mendukung lebih banyak opsi untuk otentikasi dan otorisasi.
- Pemantauan dan penelusuran — REST APIs mendukung opsi AWS X-Ray penelusuran dan pencatatan tambahan.

Untuk perbandingan mendetail, lihat [Memilih antara HTTP APIs dan REST APIs](#) di Panduan Pengembang API Gateway.

WebSocket APIs juga menggunakan API Gateway versi 2 API dan mendukung set fitur serupa. Gunakan a WebSocket API untuk aplikasi yang mendapat manfaat dari koneksi persisten antara klien dan API. WebSocket APIs menyediakan komunikasi duplex penuh, yang berarti bahwa klien dan API dapat mengirim pesan terus menerus tanpa menunggu tanggapan.

HTTP APIs mendukung format acara yang disederhanakan (versi 2.0). Contoh berikut menunjukkan peristiwa dari sebuah HTTP API.

Example APIAcara proxy gateway (HTTPAPI)

```
{
  "version": "2.0",
  "routeKey": "ANY /nodejs-apig-function-1G3XMPLZXVXYI",
  "rawPath": "/default/nodejs-apig-function-1G3XMPLZXVXYI",
  "rawQueryString": "",
  "cookies": [
    "s_fid=7AABXMPL1AFD9BBF-0643XMPL09956DE2",
    "regStatus=pre-register"
  ],
  "headers": {
    "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
    "accept-encoding": "gzip, deflate, br",
    ...
  },
  "requestContext": {
    "accountId": "123456789012",
    "apiId": "r3pmxmplak",
    "domainName": "r3pmxmplak.execute-api.us-east-2.amazonaws.com",
    "domainPrefix": "r3pmxmplak",
    "http": {
      "method": "GET",
      "path": "/default/nodejs-apig-function-1G3XMPLZXVXYI",
      "protocol": "HTTP/1.1",
      "sourceIp": "205.255.255.176",
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
    },
    "requestId": "JKJaXmPLvHcESHA=",
    "routeKey": "ANY /nodejs-apig-function-1G3XMPLZXVXYI",
    "stage": "default",
    "time": "10/Mar/2020:05:16:23 +0000",
    "timeEpoch": 1583817383220
  },
  "isBase64Encoded": true
}
```

Untuk informasi selengkapnya, lihat [Membuat integrasi AWS Lambda proxy untuk HTTP APIs di API Gateway](#).

Menambahkan titik akhir ke fungsi Lambda Anda

Untuk menambahkan titik akhir publik ke fungsi Lambda Anda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.
4. Pilih APIGateway.
5. Pilih Buat API atau Gunakan yang sudah ada API.
 - a. BaruAPI: Untuk APItipe, pilih HTTPAPI. Untuk informasi selengkapnya, lihat [Memilih API tipe](#).
 - b. AdaAPI: Pilih API dari daftar dropdown atau masukkan API ID (misalnya, r3pmxmplak).
6. Untuk Keamanan, pilih Terbuka.
7. Pilih Tambahkan.

Integrasi proxy

APIGateway APIs terdiri dari tahapan, sumber daya, metode, dan integrasi. Tahap dan sumber daya menentukan jalur titik akhir:

APIformat jalur

- /prod/ – Tahap prod dan sumber daya root.
- /prod/user – Tahap prod dan sumber daya user.
- /dev/{proxy+} – Rute mana pun di tahap dev.
- /— (HTTPAPIs) Tahap default dan sumber daya root.

Integrasi Lambda memetakan kombinasi jalur dan HTTP metode ke fungsi Lambda. Anda dapat mengonfigurasi API Gateway untuk meneruskan isi HTTP permintaan apa adanya (integrasi kustom), atau untuk merangkum badan permintaan dalam dokumen yang mencakup semua informasi permintaan termasuk header, sumber daya, jalur, dan metode.

Untuk informasi selengkapnya, lihat [Integrasi proxy Lambda](#) di Gateway. API

Format acara

Amazon API Gateway memanggil fungsi Anda [secara sinkron](#) dengan peristiwa yang berisi JSON representasi permintaan. HTTP Untuk integrasi kustom, kejadian adalah badan dari permintaan. Untuk integrasi proksi, kejadian memiliki struktur yang telah ditentukan. Contoh berikut menunjukkan peristiwa proxy dari API Gateway RESTAPI.

Example APIAcara proxy gateway (RESTAPI)

```
{
  "resource": "/",
  "path": "/",
  "httpMethod": "GET",
  "requestContext": {
    "resourcePath": "/",
    "httpMethod": "GET",
    "path": "/Prod/",
    ...
  },
  "headers": {
    "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
    "accept-encoding": "gzip, deflate, br",
    "Host": "70ixmpl4f1.execute-api.us-east-2.amazonaws.com",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36",
    "X-Amzn-Trace-Id": "Root=1-5e66d96f-7491f09xmpl179d18acf3d050",
    ...
  },
  "multiValueHeaders": {
    "accept": [
      "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
    ],
    "accept-encoding": [
      "gzip, deflate, br"
    ],
    ...
  },
  "queryStringParameters": null,
  "multiValueQueryStringParameters": null,
  "pathParameters": null,
  "stageVariables": null,
```

```
"body": null,  
"isBase64Encoded": false  
}
```

Format respons

APIGateway menunggu respons dari fungsi Anda dan menyampaikan hasilnya ke pemanggil. Untuk integrasi kustom, Anda menentukan respons integrasi dan respons metode untuk mengonversi output dari fungsi menjadi HTTP respons. Untuk integrasi proksi, fungsi harus merespons dengan representasi respons dalam format tertentu.

Contoh berikut menunjukkan objek respons dari fungsi Node.js. Objek respons mewakili HTTP respons sukses yang berisi JSON dokumen.

Example index.mjs - Objek respons integrasi proxy (Node.js)

```
var response = {  
  "statusCode": 200,  
  "headers": {  
    "Content-Type": "application/json"  
  },  
  "isBase64Encoded": false,  
  "multiValueHeaders": {  
    "X-Custom-Header": ["My value", "My other value"],  
  },  
  "body": "{\n  \"TotalCodeSize\": 104330022,\n  \"FunctionCount\": 26\n}"  
}
```

Runtime Lambda membuat serial objek respon ke dalam JSON dan mengirimkannya ke file. API APISparsing respon dan menggunakannya untuk membuat HTTP respon, yang kemudian dikirim ke klien yang membuat permintaan asli.

Example HTTPrespon

```
< HTTP/1.1 200 OK  
< Content-Type: application/json  
< Content-Length: 55  
< Connection: keep-alive  
< x-amzn-RequestId: 32998fea-xmpl-4268-8c72-16138d629356  
< X-Custom-Header: My value  
< X-Custom-Header: My other value  
< X-Amzn-Trace-Id: Root=1-5e6aa925-ccecxmplbae116148e52f036
```

```
<
{
  "TotalCodeSize": 104330022,
  "FunctionCount": 26
}
```

Izin

Amazon API Gateway mendapatkan izin untuk menjalankan fungsi Anda dari kebijakan berbasis [sumber daya](#) fungsi. Anda dapat memberikan izin pemanggilan ke seluruh API, atau memberikan akses terbatas ke tahap, sumber daya, atau metode.

Saat menambahkan API ke fungsi menggunakan konsol Lambda, menggunakan konsol API Gateway, atau dalam AWS SAM templat, kebijakan berbasis sumber daya fungsi akan diperbarui secara otomatis. Berikut ini adalah contoh kebijakan fungsi.

Example kebijakan fungsi

```
{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "nodejs-apig-functiongetEndpointPermissionProd-BWDBXMPLXE2F",
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-2:111122223333:function:nodejs-apig-
function-1G3MXMPLXVXYI",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:execute-api:us-east-2:111122223333:ktyvxmplsl1/*/"
        }
      }
    }
  ]
}
```

```
}

```

Anda dapat mengelola izin kebijakan fungsi secara manual dengan API operasi berikut:

- [AddPermission](#)
- [RemovePermission](#)
- [GetPolicy](#)

Untuk memberikan izin pemanggilan ke yang sudah ada API, gunakan perintah. `add-permission`
Contoh:

```
aws lambda add-permission \
  --function-name my-function \
  --statement-id apigateway-get --action lambda:InvokeFunction \
  --principal apigateway.amazonaws.com \
  --source-arn "arn:aws:execute-api:us-east-2:123456789012:mnh1xmpli7/default/GET/"

```

Anda akan melihat output berikut:

```
{
  "Statement": [{"Sid": "apigateway-test-2", "Effect": "Allow", "Principal": {"Service": "apigateway.amazonaws.com"}, "Action": "lambda:InvokeFunction", "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function", "Condition": {"ArnLike": {"AWS:SourceArn": "arn:aws:execute-api:us-east-2:123456789012:mnh1xmpli7/default/GET"}}}]
}
```

Note

Jika fungsi API Anda dan berbeda Wilayah AWS, pengenal Wilayah di sumber ARN harus cocok dengan Wilayah fungsi, bukan Wilayah fungsi. API Ketika API Gateway memanggil fungsi, ia menggunakan sumber daya ARN yang didasarkan pada ARN fungsi API, tetapi dimodifikasi agar sesuai dengan Wilayah fungsi.

Sumber ARN dalam contoh ini memberikan izin untuk integrasi pada GET metode sumber daya root di tahap default API, dengan ID `mnh1xmpli7`. Anda dapat menggunakan tanda bintang di sumber ARN untuk memberikan izin ke beberapa tahapan, metode, atau sumber daya.

Pola sumber daya

- `mnh1xmpli7/*/GET/*`— GET metode pada semua sumber daya di semua tahap.
- `mnh1xmpli7/prod/ANY/user`— ANY metode pada user sumber daya di prod panggung.
- `mnh1xmpli7/**/*` – Metode apa pun pada semua sumber daya di semua tahap.

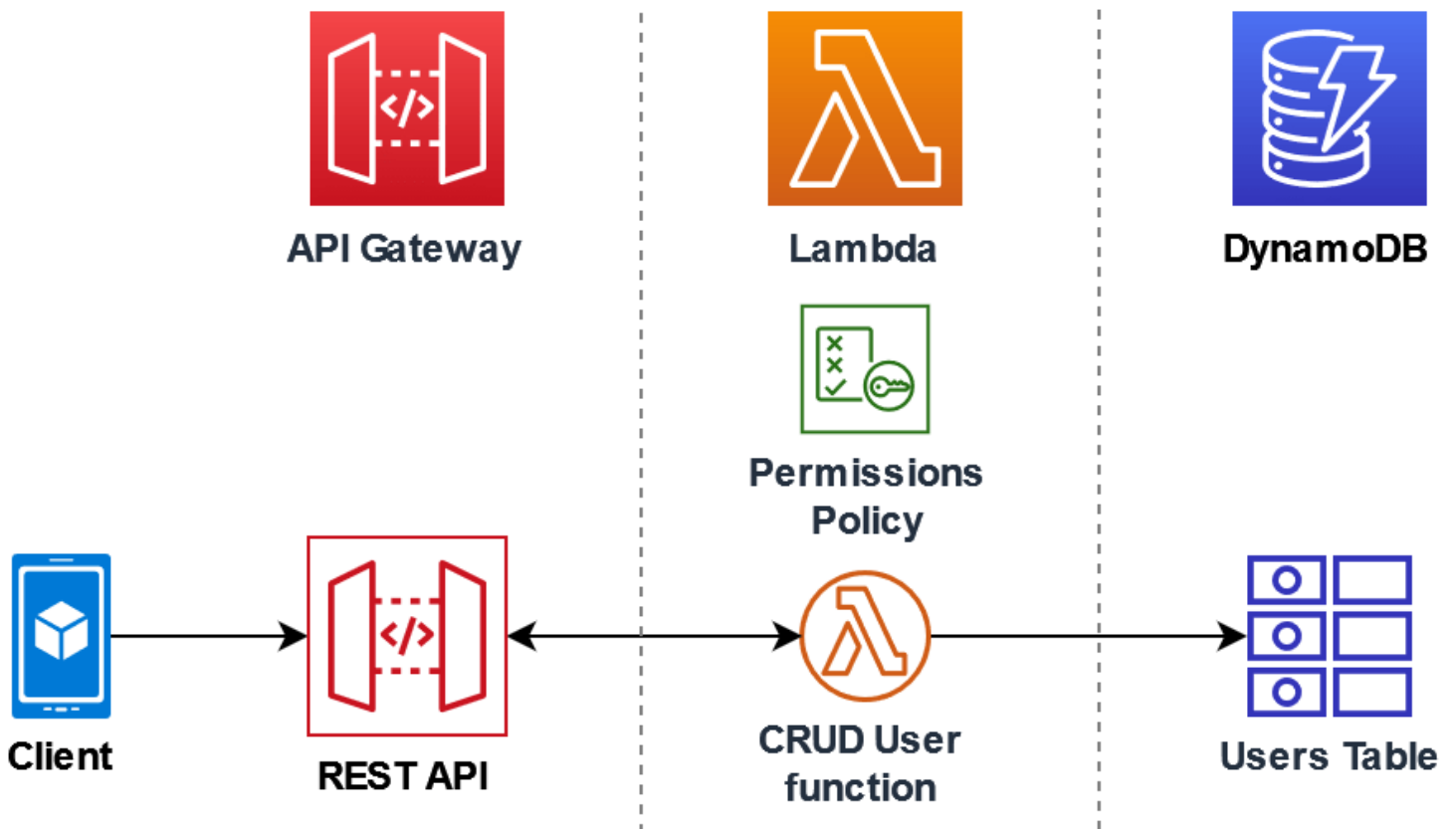
Untuk perincian tentang melihat kebijakan dan menghapus pernyataan, lihat [Bekerja dengan kebijakan berbasis sumber daya di Lambda IAM](#).

Aplikasi sampel

Aplikasi sampel [APIGateway dengan Node.js](#) menyertakan fungsi dengan AWS SAM templat yang membuat REST API yang mengaktifkan AWS X-Ray penelusuran. Ini juga mencakup skrip untuk menyebarkan, menjalankan fungsi, menguji, dan membersihkan API.

Tutorial: Menggunakan Lambda dengan Gateway API

Dalam tutorial ini, Anda membuat REST API melalui mana Anda memanggil fungsi Lambda menggunakan HTTP permintaan. Fungsi Lambda Anda akan melakukan operasi create, read, update, dan delete (CRUD) pada tabel DynamoDB. Fungsi ini disediakan di sini untuk demonstrasi, tetapi Anda akan belajar mengkonfigurasi API Gateway REST API yang dapat memanggil fungsi Lambda apa pun.



Menggunakan API Gateway memberi pengguna HTTP titik akhir yang aman untuk menjalankan fungsi Lambda Anda dan dapat membantu mengelola panggilan dalam jumlah besar ke fungsi Anda dengan membatasi lalu lintas dan secara otomatis memvalidasi dan mengotorisasi panggilan. API APIGateway juga menyediakan kontrol keamanan yang fleksibel menggunakan AWS Identity and Access Management (IAM) dan Amazon Cognito. Ini berguna untuk kasus penggunaan di mana otorisasi terlebih dahulu diperlukan untuk panggilan ke aplikasi Anda.

Untuk menyelesaikan tutorial ini, Anda akan melalui tahapan berikut:

1. Membuat dan mengkonfigurasi fungsi Lambda di Python atau Node.js untuk melakukan operasi pada tabel DynamoDB.
2. Buat API Gateway REST API in untuk terhubung ke fungsi Lambda Anda.
3. Buat tabel DynamoDB dan mengujinya dengan fungsi Lambda Anda di konsol.
4. Terapkan API dan uji pengaturan lengkap menggunakan curl di terminal.

Dengan menyelesaikan tahapan ini, Anda akan belajar cara menggunakan API Gateway untuk membuat HTTP titik akhir yang dapat menjalankan fungsi Lambda dengan aman pada skala apa

pun. Anda juga akan belajar cara menyebarkan AndaAPI, dan cara mengujinya di konsol dan dengan mengirim HTTP permintaan menggunakan terminal.

Bagian-bagian

- [Prasyarat](#)
- [Membuat kebijakan izin](#)
- [Membuat peran eksekusi](#)
- [Buat fungsi](#)
- [Memanggil fungsi menggunakan AWS CLI](#)
- [Buat API Gateway REST API menggunakan](#)
- [Buat sumber daya di Anda REST API](#)
- [Buat HTTP POST metode](#)
- [Membuat tabel DynamoDB](#)
- [Uji integrasi API Gateway, Lambda, dan DynamoDB](#)
- [Menyebarkan API](#)
- [Gunakan curl untuk memanggil fungsi Anda menggunakan permintaan HTTP](#)
- [Bersihkan sumber daya Anda \(opsional\)](#)

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Instal AWS Command Line Interface

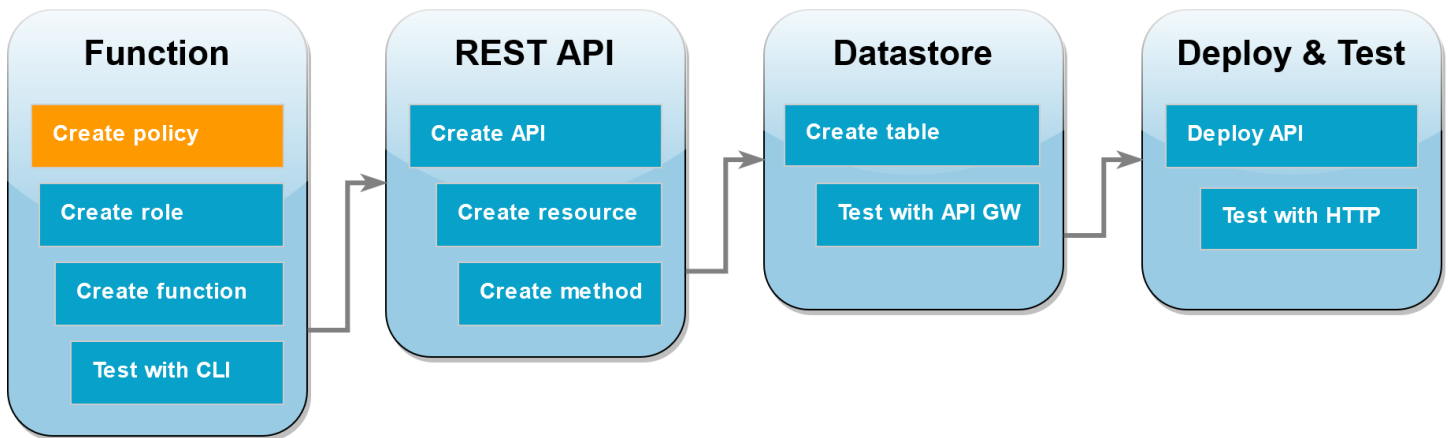
Jika Anda belum menginstal AWS Command Line Interface, ikuti langkah-langkah di [Menginstal atau memperbarui versi terbaru AWS CLI untuk menginstalnya](#).

Tutorial ini membutuhkan terminal baris perintah atau shell untuk menjalankan perintah. Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa CLI perintah Bash yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#).

Membuat kebijakan izin



Sebelum Anda dapat membuat [peran eksekusi](#) untuk fungsi Lambda Anda, Anda harus terlebih dahulu membuat kebijakan izin untuk memberikan izin fungsi Anda untuk mengakses sumber daya yang diperlukan. AWS Untuk tutorial ini, kebijakan memungkinkan Lambda untuk melakukan CRUD operasi pada tabel DynamoDB dan menulis ke Amazon Logs. CloudWatch

Untuk membuat kebijakan

1. Buka [halaman Kebijakan](#) IAM konsol.
2. Pilih Buat Kebijakan.
3. Pilih JSONtab, lalu tempelkan kebijakan khusus berikut ke JSON editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1428341300017",
      "Action": [
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ],
}
```

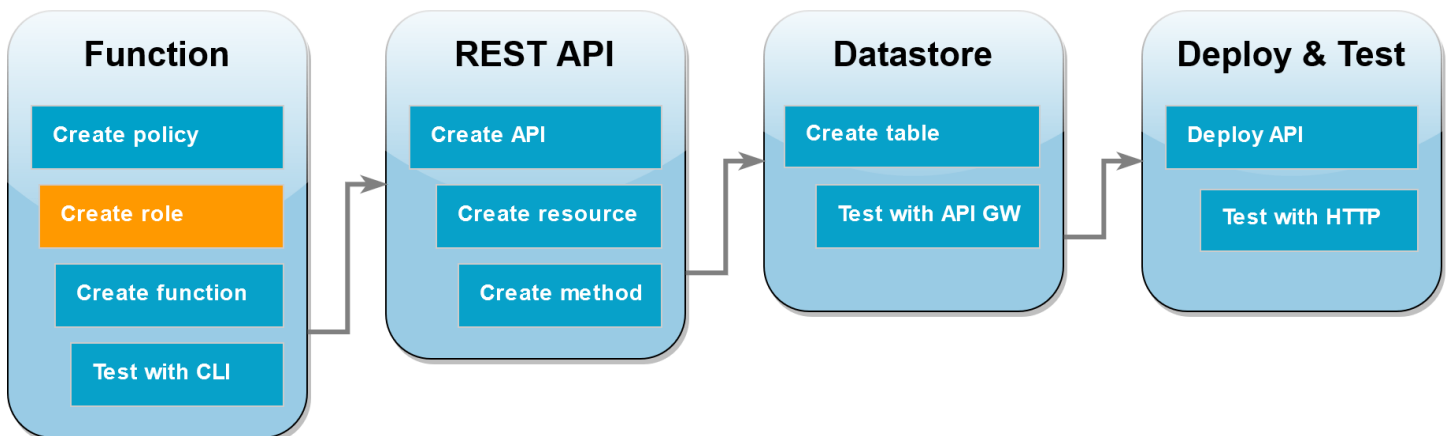
```

    "Sid": "",
    "Resource": "*",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Effect": "Allow"
  }
]
}

```

4. Pilih Selanjutnya: Tag.
5. Pilih Berikutnya: Tinjau.
6. Di bawah Kebijakan peninjauan, untuk Nama kebijakan, masukkan **lambda-apigateway-policy**.
7. Pilih Buat kebijakan.

Membuat peran eksekusi



Peran [eksekusi adalah peran](#) AWS Identity and Access Management (IAM) yang memberikan izin fungsi Lambda untuk AWS mengakses layanan dan sumber daya. Untuk mengaktifkan fungsi Anda menjalankan operasi pada tabel DynamoDB, Anda melampirkan kebijakan izin yang Anda buat di langkah sebelumnya.

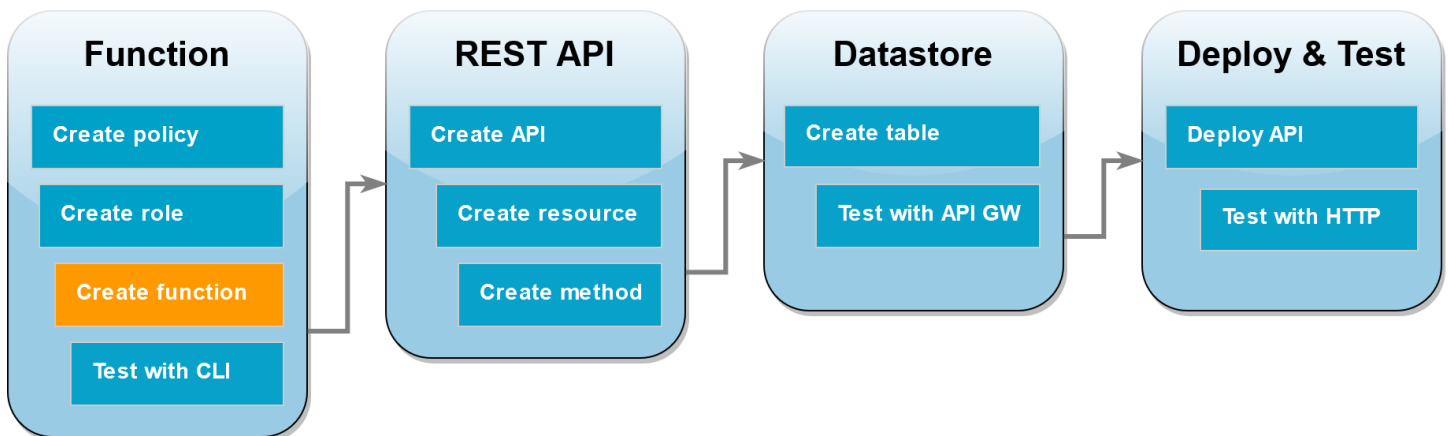
Untuk membuat peran eksekusi dan melampirkan kebijakan izin kustom

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih Buat peran.

3. Untuk jenis entitas tepercaya, pilih AWS layanan, lalu untuk kasus penggunaan, pilih Lambda.
4. Pilih Berikutnya.
5. Dalam kotak pencarian kebijakan, masukkan **lambda-apigateway-policy**.
6. Di hasil penelusuran, pilih kebijakan yang Anda buat (**lambda-apigateway-policy**), lalu pilih Berikutnya.
7. Di bawah Rincian peran, untuk nama Peran, masukkan **lambda-apigateway-role**, lalu pilih Buat peran.

Kemudian dalam tutorial, Anda memerlukan Amazon Resource Name (ARN) dari peran yang baru saja Anda buat. Pada halaman Peran IAM konsol, pilih nama peran Anda (**lambda-apigateway-role**) dan salin Peran yang ARN ditampilkan di halaman Ringkasan.

Buat fungsi



Contoh kode berikut menerima input peristiwa dari API Gateway menentukan operasi untuk melakukan pada tabel DynamoDB Anda akan membuat dan beberapa data payload. Jika parameter yang diterima fungsi valid, ia melakukan operasi yang diminta di atas meja.

Node.js

Example index.mjs

```

import { DynamoDBDocumentClient, PutCommand, GetCommand,
  UpdateCommand, DeleteCommand } from "@aws-sdk/lib-dynamodb";
import { DynamoDBClient } from "@aws-sdk/client-dynamodb";

const ddbClient = new DynamoDBClient({ region: "us-east-2" });
const ddbDocClient = DynamoDBDocumentClient.from(ddbClient);
  
```



```
// Define the name of the DDB table to perform the CRUD operations on
const tablename = "lambda-apigateway";

/**
 * Provide an event that contains the following keys:
 *
 * - operation: one of 'create,' 'read,' 'update,' 'delete,' or 'echo'
 * - payload: a JSON object containing the parameters for the table item
 *   to perform the operation on
 */
export const handler = async (event, context) => {

    const operation = event.operation;

    if (operation == 'echo'){
        return(event.payload);
    }

    else {
        event.payload.TableName = tablename;
        let response;

        switch (operation) {
            case 'create':
                response = await ddbDocClient.send(new PutCommand(event.payload));
                break;
            case 'read':
                response = await ddbDocClient.send(new GetCommand(event.payload));
                break;
            case 'update':
                response = ddbDocClient.send(new UpdateCommand(event.payload));
                break;
            case 'delete':
                response = ddbDocClient.send(new DeleteCommand(event.payload));
                break;
            default:
                response = 'Unknown operation: ${operation}';
        }
        console.log(response);
        return response;
    }
};
```

Note

Dalam contoh ini, nama tabel DynamoDB didefinisikan sebagai variabel dalam kode fungsi Anda. Dalam aplikasi nyata, praktik terbaik adalah meneruskan parameter ini sebagai variabel lingkungan dan untuk menghindari hardcoding nama tabel. Untuk informasi selengkapnya lihat [Menggunakan variabel AWS Lambda lingkungan](#).

Untuk membuat fungsi

1. Simpan contoh kode sebagai file bernama `index.mjs` dan, jika perlu, edit AWS wilayah yang ditentukan dalam kode. Wilayah yang ditentukan dalam kode harus sama dengan wilayah tempat Anda membuat tabel DynamoDB nanti dalam tutorial.
2. Buat paket penyebaran menggunakan zip perintah berikut.

```
zip function.zip index.mjs
```

3. Buat fungsi Lambda menggunakan perintah `create-function` AWS CLI Untuk `role` parameter, masukkan peran eksekusi Amazon Resource Name (ARN) yang Anda salin sebelumnya.

```
aws lambda create-function \  
--function-name LambdaFunctionOverHttps \  
--zip-file fileb://function.zip \  
--handler index.handler \  
--runtime nodejs20.x \  
--role arn:aws:iam::123456789012:role/service-role/lambda-apigateway-role
```

Python 3

Example LambdaFunctionOverHttps.py

```
import boto3  
  
# Define the DynamoDB table that Lambda will connect to  
table_name = "lambda-apigateway"  
  
# Create the DynamoDB resource  
dynamo = boto3.resource('dynamodb').Table(table_name)
```

```
# Define some functions to perform the CRUD operations
def create(payload):
    return dynamo.put_item(Item=payload['Item'])

def read(payload):
    return dynamo.get_item(Key=payload['Key'])

def update(payload):
    return dynamo.update_item(**{k: payload[k] for k in ['Key', 'UpdateExpression',
    'ExpressionAttributeNames', 'ExpressionAttributeValues'] if k in payload})

def delete(payload):
    return dynamo.delete_item(Key=payload['Key'])

def echo(payload):
    return payload

operations = {
    'create': create,
    'read': read,
    'update': update,
    'delete': delete,
    'echo': echo,
}

def lambda_handler(event, context):
    '''Provide an event that contains the following keys:
    - operation: one of the operations in the operations dict below
    - payload: a JSON object containing parameters to pass to the
    operation being performed
    ...'''

    operation = event['operation']
    payload = event['payload']

    if operation in operations:
        return operations[operation](payload)

    else:
        raise ValueError(f'Unrecognized operation "{operation}"')
```

Note

Dalam contoh ini, nama tabel DynamoDB didefinisikan sebagai variabel dalam kode fungsi Anda. Dalam aplikasi nyata, praktik terbaik adalah meneruskan parameter ini sebagai variabel lingkungan dan untuk menghindari hardcoding nama tabel. Untuk informasi selengkapnya lihat [Menggunakan variabel AWS Lambda lingkungan](#).

Untuk membuat fungsi

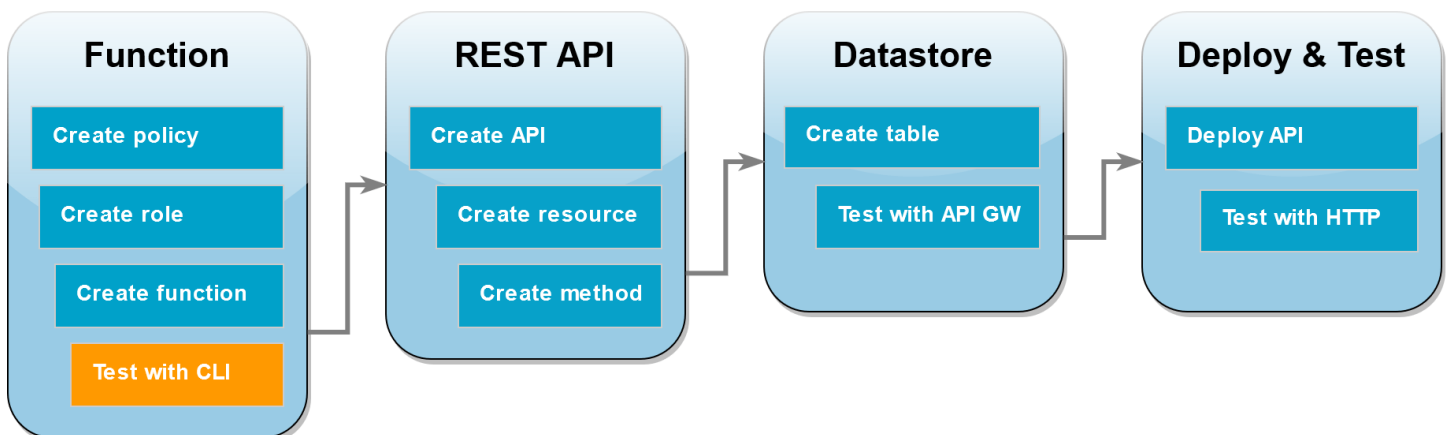
1. Simpan contoh kode sebagai file bernama `LambdaFunctionOverHttps.py`.
2. Buat paket penyebaran menggunakan zip perintah berikut.

```
zip function.zip LambdaFunctionOverHttps.py
```

3. Buat fungsi Lambda menggunakan perintah `create-function` AWS CLI Untuk `role` parameter, masukkan peran eksekusi Amazon Resource Name (ARN) yang Anda salin sebelumnya.

```
aws lambda create-function \  
--function-name LambdaFunctionOverHttps \  
--zip-file fileb://function.zip \  
--handler LambdaFunctionOverHttps.lambda_handler \  
--runtime python3.12 \  
--role arn:aws:iam::123456789012:role/service-role/lambda-apigateway-role
```

Memanggil fungsi menggunakan AWS CLI



Sebelum mengintegrasikan fungsi Anda dengan API Gateway, konfirmasikan bahwa Anda telah berhasil menerapkan fungsi tersebut. Buat acara pengujian yang berisi parameter yang API akan dikirim API Gateway Anda ke Lambda dan gunakan AWS CLI `invoke` perintah untuk menjalankan fungsi Anda.

Untuk menjalankan fungsi Lambda dengan AWS CLI

1. Simpan berikut ini JSON sebagai file bernama `input.txt`.

```
{
  "operation": "echo",
  "payload": {
    "somekey1": "somevalue1",
    "somekey2": "somevalue2"
  }
}
```

2. Jalankan perintah `invoke` AWS CLI berikut.

```
aws lambda invoke \
--function-name LambdaFunctionOverHttps \
--payload file://input.txt outputfile.txt \
--cli-binary-format raw-in-base64-out
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

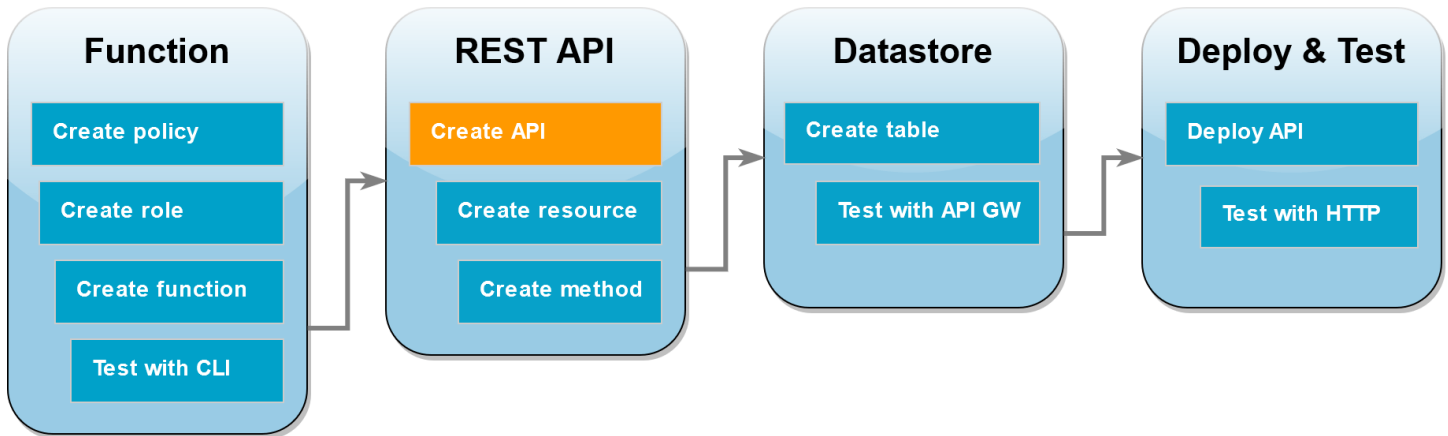
Anda akan melihat tanggapan berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "LATEST"
}
```

3. Konfirmasikan bahwa fungsi Anda melakukan echo operasi yang Anda tentukan dalam acara JSON pengujian. Periksa `outputfile.txt` file dan verifikasi berisi yang berikut:

```
{"somekey1": "somevalue1", "somekey2": "somevalue2"}
```

Buat API Gateway REST API menggunakan

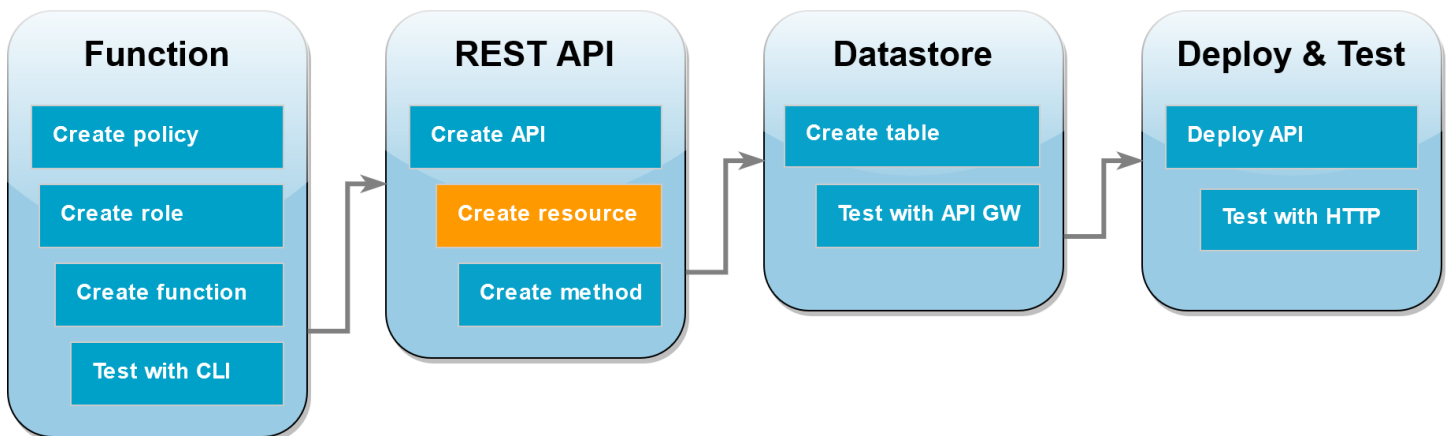


Pada langkah ini, Anda membuat API Gateway yang akan REST API Anda gunakan untuk menjalankan fungsi Lambda Anda.

Untuk membuat API

1. Buka [konsol API Gateway](#).
2. Pilih Buat API.
3. Di dalam RESTAPIkotak, pilih Build.
4. Di bawah APIdetail, biarkan Baru API dipilih, dan untuk APINama, masukkan **DynamoDBOperations**.
5. Pilih Buat API.

Buat sumber daya di Anda REST API

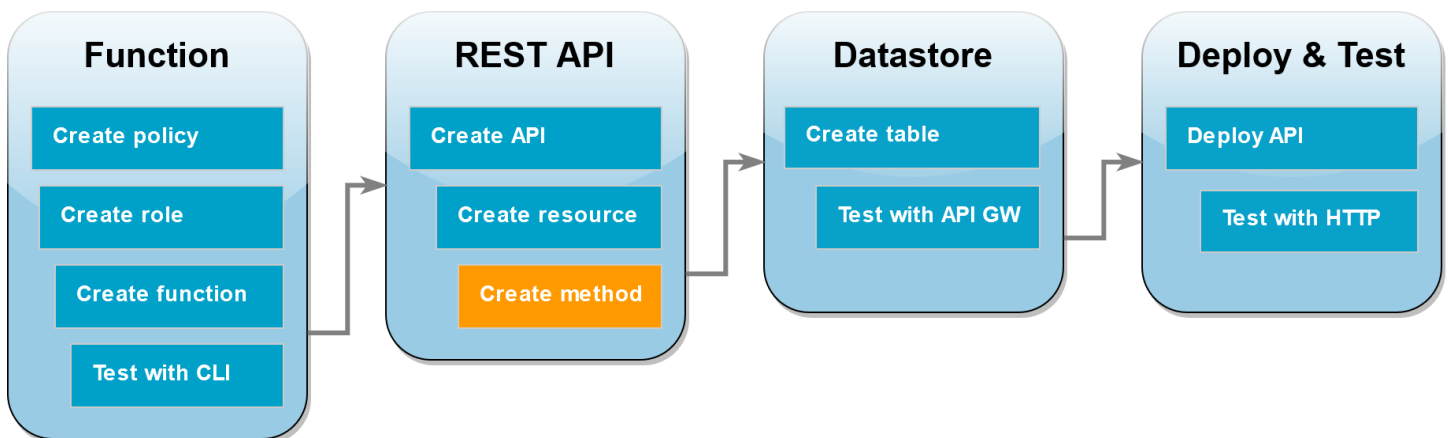


Untuk menambahkan HTTP metode ke AndaAPI, Anda harus terlebih dahulu membuat sumber daya agar metode tersebut dapat beroperasi. Di sini Anda membuat sumber daya untuk mengelola tabel DynamoDB Anda.

Untuk membuat sumber daya

1. Di [konsol API Gateway](#), pada halaman Sumber Daya untuk AndaAPI, pilih Buat Sumber Daya.
2. Dalam Rincian sumber daya, untuk nama Sumber daya masukkan **DynamoDBManager**.
3. Pilih Buat Sumber Daya.

Buat HTTP POST metode



Pada langkah ini, Anda membuat metode (POST) untuk DynamoDBManager sumber daya Anda. Anda menautkan POST metode ini ke fungsi Lambda Anda sehingga ketika metode menerima HTTP permintaan, API Gateway memanggil fungsi Lambda Anda.

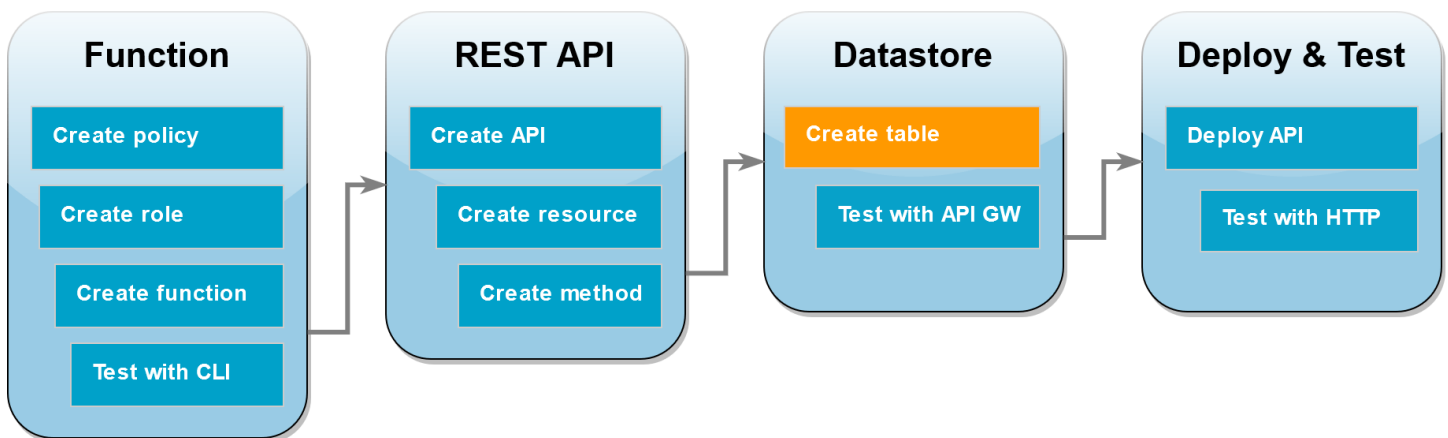
Note

Untuk tujuan tutorial ini, satu HTTP metode (POST) digunakan untuk memanggil fungsi Lambda tunggal yang melakukan semua operasi pada tabel DynamoDB Anda. Dalam aplikasi nyata, praktik terbaik adalah menggunakan fungsi dan HTTP metode Lambda yang berbeda untuk setiap operasi. Untuk informasi lebih lanjut, lihat [Monolit Lambda](#) di Tanah Tanpa Server.

Untuk membuat POST metode

1. Pada halaman Sumber Daya untuk AndaAPI, pastikan bahwa /DynamoDBManager sumber daya disorot. Kemudian, di panel Methods, pilih Create Method.
2. Untuk jenis Metode, pilih POST.
3. Untuk jenis Integrasi, biarkan fungsi Lambda dipilih.
4. Untuk fungsi Lambda, pilih Amazon Resource Name (ARN) untuk fungsi Anda (LambdaFunctionOverHttps).
5. Pilih metode Buat.

Membuat tabel DynamoDB

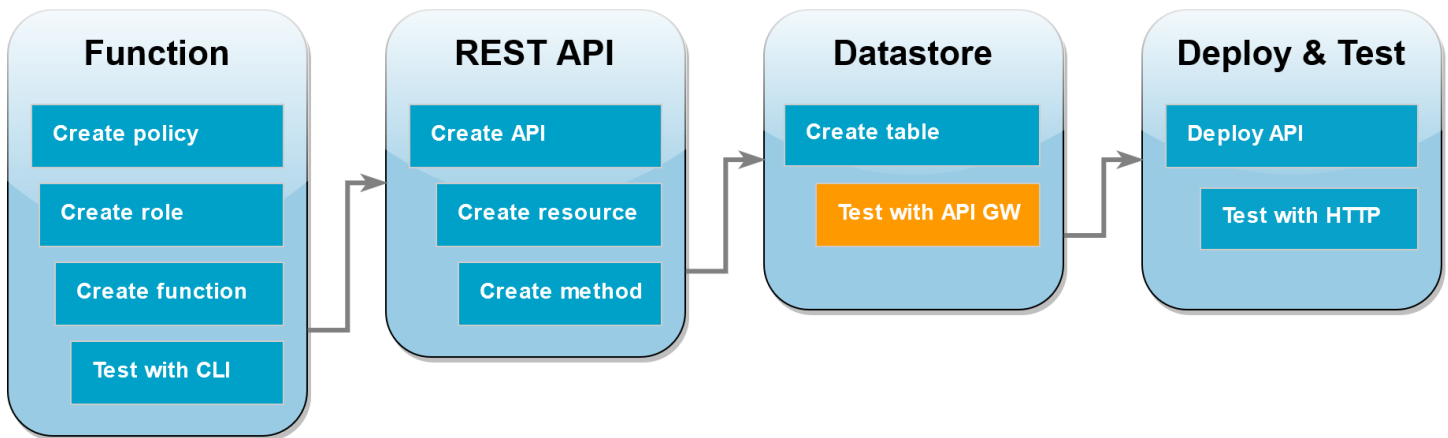


Buat tabel DynamoDB kosong tempat fungsi Lambda Anda akan melakukan operasi. CRUD

Untuk membuat tabel DynamoDB

1. Buka [halaman Tabel](#) di konsol DynamoDB.
2. Pilih Buat tabel.
3. Di bawah Rincian tabel, lakukan hal berikut:
 1. Untuk Nama tabel, masukkan **lambda-apigateway**.
 2. Untuk kunci Partition, masukkan **id**, dan simpan tipe data yang ditetapkan sebagai String.
4. Di bawah Pengaturan tabel, pertahankan pengaturan Default.
5. Pilih Buat tabel.

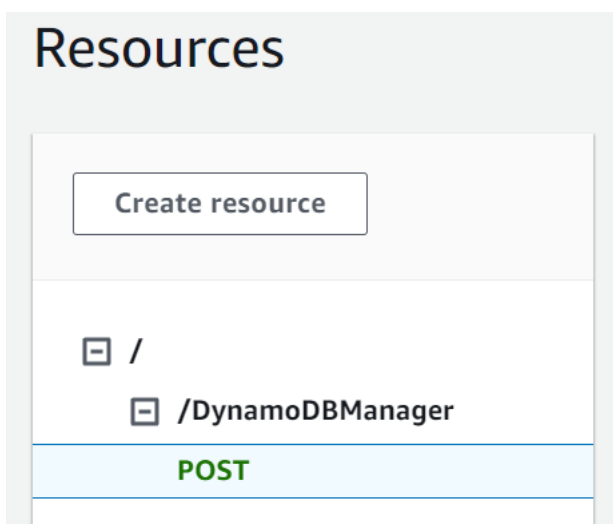
Uji integrasi API Gateway, Lambda, dan DynamoDB



Anda sekarang siap untuk menguji integrasi API metode API Gateway Anda dengan fungsi Lambda dan tabel DynamoDB Anda. Menggunakan konsol API Gateway, Anda mengirim permintaan langsung ke POST metode Anda menggunakan fungsi pengujian konsol. Pada langkah ini, Anda pertama kali menggunakan create operasi untuk menambahkan item baru ke tabel DynamoDB Anda, kemudian Anda menggunakan operasi untuk update memodifikasi item.

Tes 1: Untuk membuat item baru di tabel DynamoDB Anda

1. Di [konsol API Gateway](#), pilih API (DynamoDBOperations).
2. Pilih POST metode di bawah DynamoDBManager sumber daya.



3. Pilih tab Uji. Anda mungkin perlu memilih tombol panah kanan untuk menampilkan tab.
4. Di bawah metode Test, biarkan string Query dan Header kosong. Untuk badan Permintaan, tempel yang berikut iniJSON:

```
{
  "operation": "create",
  "payload": {
    "Item": {
      "id": "1234ABCD",
      "number": 5
    }
  }
}
```

5. Pilih Uji.

Hasil yang ditampilkan saat tes selesai harus menunjukkan status `200`. Kode status ini menunjukkan bahwa `create` operasi berhasil.

Untuk mengonfirmasi, periksa apakah tabel DynamoDB Anda sekarang berisi item baru.

6. Buka [halaman Tabel](#) konsol DynamoDB dan pilih tabel. `lambda-apigateway`
7. Pilih Jelajahi item tabel. Di panel Item yang dikembalikan, Anda akan melihat satu item dengan id `1234ABCD` dan nomornya `5`.

Tes 2: Untuk memperbarui item dalam tabel DynamoDB Anda

1. Di [konsol API Gateway](#), kembali ke tab Test POST metode Anda.
2. Di bawah metode Test, biarkan string Query dan Header kosong. Untuk badan Permintaan, tempel yang berikut iniJSON:

```
{
  "operation": "update",
  "payload": {
    "Key": {
      "id": "1234ABCD"
    },
    "AttributeUpdates": {
      "number": {
        "Value": 10
      }
    }
  }
}
```

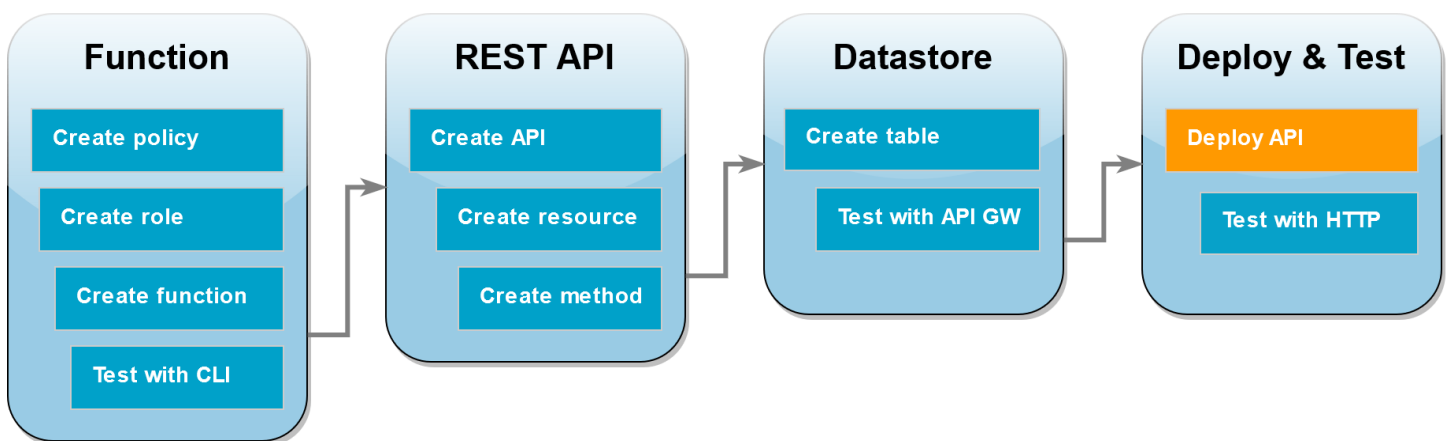
3. Pilih Uji.

Hasil yang ditampilkan saat tes selesai harus menunjukkan status 200. Kode status ini menunjukkan bahwa update operasi berhasil.

Untuk mengonfirmasi, periksa apakah item di tabel DynamoDB Anda telah dimodifikasi.

4. Buka [halaman Tabel](#) konsol DynamoDB dan pilih tabel. `lambda-apigateway`
5. Pilih Jelajahi item tabel. Di panel Item yang dikembalikan, Anda akan melihat satu item dengan id `1234ABCD` dan nomornya `10`.

Menyebarkan API

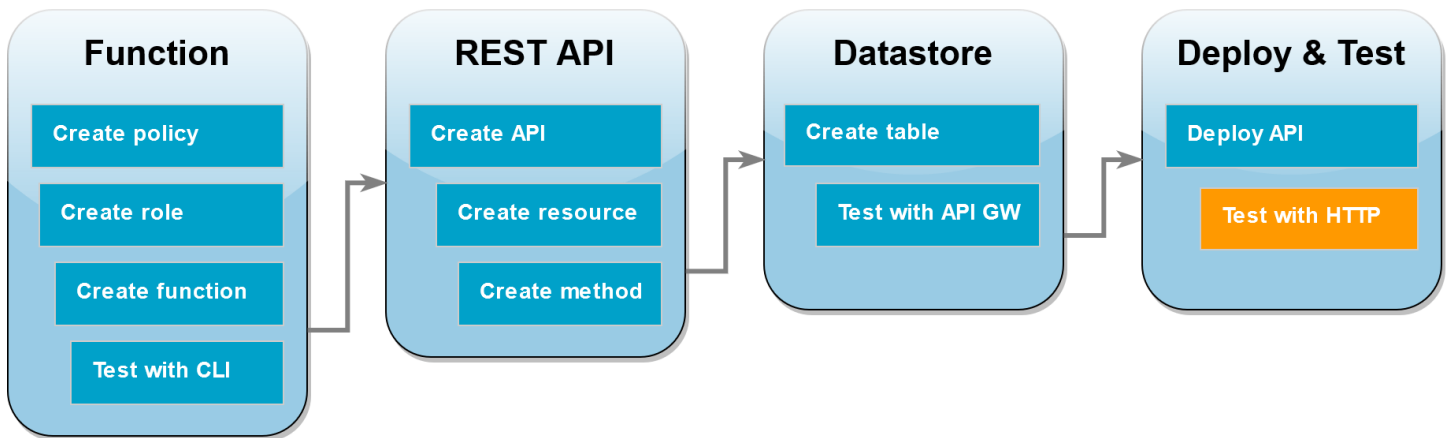


Agar klien dapat memanggil API, Anda harus membuat penyebaran dan tahap terkait. Sebuah panggung mewakili snapshot Anda API termasuk metode dan integrasinya.

Untuk menyebarkan API

1. Buka API halaman [konsol API Gateway](#) dan pilih `DynamoDBOperationsAPI`.
2. Pada halaman Resources untuk Anda API pilih `Deploy API`.
3. Untuk Stage, pilih `*Tahap baru*`, lalu untuk nama Stage, masukkan `test`
4. Pilih `Deploy`.
5. Di panel Detail tahap, salin `URLInvoke`. Anda akan menggunakan ini di langkah berikutnya untuk menjalankan fungsi Anda menggunakan HTTP permintaan.

Gunakan curl untuk memanggil fungsi Anda menggunakan permintaan HTTP



Anda sekarang dapat menjalankan fungsi Lambda Anda dengan mengeluarkan HTTP permintaan ke Anda. API Pada langkah ini, Anda akan membuat item baru di tabel DynamoDB Anda dan kemudian melakukan operasi baca, perbarui, dan hapus pada item tersebut.

Untuk membuat item di tabel DynamoDB Anda menggunakan curl

1. Jalankan `curl` perintah berikut menggunakan pemanggilan yang URL Anda salin pada langkah sebelumnya. Saat Anda menggunakan curl dengan opsi `-d` (data), secara otomatis menggunakan HTTP POST metode ini.

```
curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager \
-d '{"operation": "create", "payload": {"Item": {"id": "5678EFGH", "number": 15}}}'
```

Jika operasi berhasil, Anda akan melihat respons yang dikembalikan dengan kode HTTP status 200.

2. Anda juga dapat menggunakan konsol DynamoDB untuk memverifikasi bahwa item baru ada di tabel Anda dengan melakukan hal berikut:
 1. Buka [halaman Tabel](#) konsol DynamoDB dan pilih tabel. `lambda-apigateway`
 2. Pilih Jelajahi item tabel. Di panel Item yang dikembalikan, Anda akan melihat item dengan id `5678EFGH` dan nomornya `15`.

Untuk membaca item di tabel DynamoDB Anda menggunakan curl

- Jalankan `curl` perintah berikut untuk membaca nilai item yang baru saja Anda buat. Gunakan panggilan Anda sendiri. URL

```
curl https://avos4dr2rk.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager -d \
'{"operation": "read", "payload": {"Key": {"id": "5678EFGH"}}}'
```

Anda akan melihat output seperti salah satu dari berikut ini tergantung pada apakah Anda memilih kode fungsi Node.js atau Python:

Node.js

```
{"$metadata":
{"statusCode":200,"requestId":"7BP3G5Q0C001E50FBQI9NS099JVV4KQNS05AEMVJF66Q9ASUAAJG",
"attempts":1,"totalRetryDelay":0},"Item":{"id":"5678EFGH","number":15}}
```

Python

```
{"Item":{"id":"5678EFGH","number":15},"ResponseMetadata":
{"RequestId":"QNDJICE52E86B82VETR6RKBE5BVV4KQNS05AEMVJF66Q9ASUAAJG",
"HTTPStatusCode":200,"HTTPHeaders":{"server":"Server","date":"Wed, 31 Jul 2024
00:37:01 GMT","content-type":"application/x-amz-json-1.0",
"content-length":"52","connection":"keep-alive","x-amzn-
requestid":"QNDJICE52E86B82VETR6RKBE5BVV4KQNS05AEMVJF66Q9ASUAAJG","x-amz-
crc32":"2589610852"},
"RetryAttempts":0}}
```

Untuk memperbarui item dalam tabel DynamoDB Anda menggunakan curl

1. Jalankan curl perintah berikut untuk memperbarui item yang baru saja Anda buat dengan mengubah number nilainya. Gunakan panggilan Anda sendiri. URL

```
curl https://avos4dr2rk.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager \
-d '{"operation": "update", "payload": {"Key": {"id": "5678EFGH"},
"UpdateExpression": "SET #num = :new_value", "ExpressionAttributeNames": {"#num":
"number"}, "ExpressionAttributeValues": {":new_value": 42}}}'
```

2. Untuk mengonfirmasi bahwa nilai number item telah diperbarui, jalankan perintah baca lainnya:

```
curl https://avos4dr2rk.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager \
-d '{"operation": "read", "payload": {"Key": {"id": "5678EFGH"}}}'
```

Untuk menghapus item dalam tabel DynamoDB Anda menggunakan curl

1. Jalankan `curl` perintah berikut untuk menghapus item yang baru saja Anda buat. Gunakan panggilan Anda sendiri. URL

```
curl https://l8togsqxd8.execute-api.us-east-2.amazonaws.com/test/DynamoDBManager \
-d '{"operation": "delete", "payload": {"Key": {"id": "5678EFGH"}}}'
```

2. Konfirmasikan bahwa operasi penghapusan berhasil. Di panel Item yang dikembalikan dari halaman item Jelajahi konsol DynamoDB, verifikasi bahwa item dengan 5678EFGH id tidak lagi ada di tabel.

Bersihkan sumber daya Anda (opsional)

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus API

1. Buka [APIshalaman](#) konsol API Gateway.
2. Pilih yang API Anda buat.

3. Pilih Tindakan, Hapus.
4. Pilih Hapus.

Untuk menghapus tabel DynamoDB

1. Buka [halaman Tabel](#) di konsol DynamoDB.
2. Pilih tabel yang Anda buat.
3. Pilih Hapus.
4. Masukkan **delete** di kotak teks.
5. Pilih Hapus tabel.

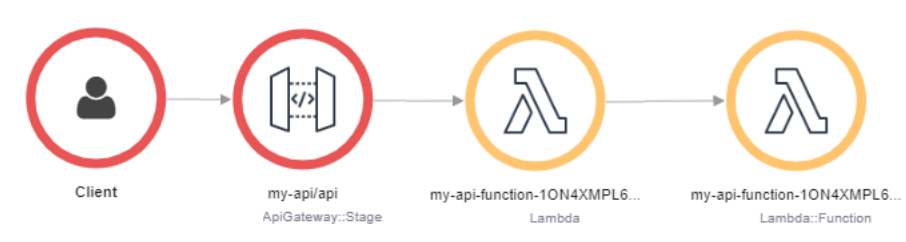
Menangani kesalahan Lambda dengan API Gateway API

API Gateway memperlakukan semua kesalahan invokasi dan fungsi sebagai kesalahan internal. Jika API Lambda menolak permintaan invokasi, API Gateway mengembalikan kode kesalahan 500. Jika fungsi berjalan, tetapi mengembalikan kesalahan atau mengembalikan respons dalam format yang salah, API Gateway mengembalikan kode 502. Dalam kedua kasus tersebut, badan respons dari API Gateway adalah `{"message": "Internal server error"}`.

Note

API Gateway tidak mencoba lagi invokasi Lambda apa pun. Jika Lambda mengembalikan kesalahan, API Gateway mengembalikan respons kesalahan ke klien.

Contoh berikut menunjukkan peta jejak X-Ray untuk permintaan yang mengakibatkan kesalahan fungsi dan 502 dari API Gateway. Klien menerima pesan kesalahan umum.

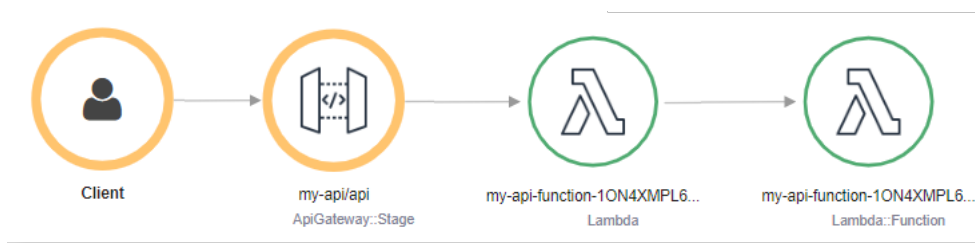


Untuk menyesuaikan respons kesalahan, Anda harus menangkap kesalahan dalam kode dan memformat tanggapan dalam format yang diperlukan.

Example [index.mjs](#) - Kesalahan pemformatan

```
var formatError = function(error){
  var response = {
    "statusCode": error.statusCode,
    "headers": {
      "Content-Type": "text/plain",
      "x-amzn-ErrorType": error.code
    },
    "isBase64Encoded": false,
    "body": error.code + ": " + error.message
  }
  return response
}
```

API Gateway mengonversi respons ini menjadi kesalahan HTTP dengan kode dan badan status kustom. Di peta jejak, node fungsi berwarna hijau karena menangani kesalahan tersebut.



Menggunakan AWS Lambda dengan Komposer Aplikasi AWS

Komposer Aplikasi AWS adalah pembangun visual untuk merancang aplikasi modern pada AWS. Anda mendesain arsitektur aplikasi Anda dengan menyeret, mengelompokkan, dan menghubungkan AWS layanan dalam kanvas visual. Application Composer membuat template infrastruktur sebagai kode (IaC) dari desain Anda yang dapat Anda gunakan menggunakan atau. [AWS SAM](#) [AWS CloudFormation](#)

Mengekspor fungsi Lambda ke Komposer Aplikasi

Anda dapat mulai menggunakan Application Composer dengan membuat proyek baru berdasarkan konfigurasi fungsi Lambda yang ada menggunakan konsol Lambda. Untuk mengekspor konfigurasi dan kode fungsi Anda ke Application Composer untuk membuat proyek baru, lakukan hal berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang ingin Anda gunakan sebagai dasar untuk proyek Application Composer Anda.

3. Di panel Ikhtisar fungsi, pilih Ekspor ke Komposer Aplikasi.

Untuk mengekspor konfigurasi dan kode fungsi Anda ke Application Composer, Lambda membuat bucket Amazon S3 di akun Anda untuk menyimpan sementara data ini.

4. Di kotak dialog, pilih Konfirmasi dan buat proyek untuk menerima nama default untuk bucket ini dan ekspor konfigurasi dan kode fungsi Anda ke Application Composer.
5. (Opsional) Untuk memilih nama lain untuk bucket Amazon S3 yang dibuat Lambda, masukkan nama baru dan pilih Konfirmasi dan buat proyek. Nama bucket Amazon S3 harus unik secara global dan mengikuti aturan [penamaan bucket](#).
6. Untuk menyimpan file proyek dan fungsi Anda di Application Composer, aktifkan [mode sinkronisasi lokal](#).

Note

Jika Anda pernah menggunakan fitur Ekspor ke Komposer Aplikasi sebelumnya dan membuat bucket Amazon S3 menggunakan nama default, Lambda dapat menggunakan kembali bucket ini jika masih ada. Terima nama bucket default di kotak dialog untuk menggunakan kembali bucket yang ada.

Konfigurasi bucket transfer Amazon S3

Bucket Amazon S3 yang dibuat Lambda untuk mentransfer konfigurasi fungsi Anda secara otomatis mengenkripsi objek menggunakan standar enkripsi 256. AES Lambda juga mengonfigurasi bucket untuk menggunakan [kondisi pemilik bucket](#) untuk memastikan bahwa hanya Anda Akun AWS yang dapat menambahkan objek ke bucket.

Lambda mengonfigurasi bucket untuk menghapus objek secara otomatis 10 hari setelah diunggah. Namun, Lambda tidak secara otomatis menghapus bucket itu sendiri. Untuk menghapus ember dari Anda Akun AWS, ikuti petunjuk di [Menghapus ember](#). Nama bucket default menggunakan awalan `lambdasam-`, string alfanumerik 10 digit, dan fungsi yang Wilayah AWS Anda buat di:

```
lambdasam-06f22da95b-us-east-1
```

Untuk menghindari biaya tambahan yang ditambahkan ke Anda Akun AWS, kami sarankan Anda menghapus bucket Amazon S3 segera setelah Anda selesai mengekspor fungsi Anda ke Application Composer.

[Harga Amazon S3](#) standar berlaku.

Izin yang diperlukan

Untuk menggunakan integrasi Lambda dengan fitur Application Composer, Anda memerlukan izin tertentu untuk mengunduh AWS SAM template dan menulis konfigurasi fungsi Anda ke Amazon S3.

Untuk mengunduh AWS SAM templat, Anda harus memiliki izin untuk menggunakan API tindakan berikut:

- [GetPolicy](#)
- [saya: GetPolicyVersion](#)
- [saya: GetRole](#)
- [saya: GetRolePolicy](#)
- [saya: ListAttachedRolePolicies](#)
- [saya: ListRolePolicies](#)
- [saya: ListRoles](#)

Anda dapat memberikan izin untuk menggunakan semua tindakan ini dengan menambahkan kebijakan [AWSLambda_ReadOnlyAccess](#) AWS terkelola ke peran IAM pengguna Anda.

Agar Lambda dapat menulis konfigurasi fungsi Anda ke Amazon S3, Anda harus memiliki izin untuk menggunakan tindakan berikut: API

- [S3: PutObject](#)
- [S3: CreateBucket](#)
- [S3: PutBucketEncryption](#)
- [S3: PutBucketLifecycleConfiguration](#)

Jika Anda tidak dapat mengekspor konfigurasi fungsi Anda ke Application Composer, periksa apakah akun Anda memiliki izin yang diperlukan untuk operasi ini. Jika Anda memiliki izin yang diperlukan, tetapi masih tidak dapat mengekspor konfigurasi fungsi Anda, periksa [kebijakan berbasis sumber daya yang mungkin membatasi](#) akses ke Amazon S3.

Sumber daya lainnya

Untuk tutorial yang lebih rinci tentang cara merancang aplikasi tanpa server di Application Composer berdasarkan fungsi Lambda yang ada, lihat. [Infrastruktur sebagai kode \(IaC\)](#)

[Untuk menggunakan Application Composer dan AWS SAM untuk merancang dan menyebarkan aplikasi tanpa server lengkap menggunakan Lambda, Anda juga dapat mengikuti Komposer Aplikasi AWS tutorial di Workshop Pola Tanpa Server.AWS](#)

Menggunakan AWS Lambda dengan AWS CloudFormation

Dalam AWS CloudFormation template, Anda dapat menentukan fungsi Lambda sebagai target sumber daya khusus. Gunakan sumber daya khusus untuk memproses parameter, mengambil nilai konfigurasi, atau memanggil AWS layanan lain selama peristiwa siklus hidup tumpukan.

Contoh berikut memanggil fungsi yang ditentukan di bagian lain dalam templat.

Example – Penentuan sumber daya kustom

```
Resources:
  primerinvoke:
    Type: AWS::CloudFormation::CustomResource
    Version: "1.0"
    Properties:
      ServiceToken: !GetAtt primer.Arn
      FunctionName: !Ref randomerror
```

Token layanan adalah Amazon Resource Name (ARN) dari fungsi yang AWS CloudFormation dipanggil saat Anda membuat, memperbarui, atau menghapus tumpukan. Anda juga dapat menyertakan properti tambahan seperti `FunctionName`, yang AWS CloudFormation lolos ke fungsi Anda apa adanya.

AWS CloudFormation memanggil [fungsi](#) Lambda Anda secara asinkron dengan peristiwa yang menyertakan panggilan balik. URL

Example — acara AWS CloudFormation pesan

```
{
  "RequestType": "Create",
  "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-processor-primer-14R0R2T3JKU66",
  "ResponseURL": "https://cloudformation-custom-resource-response-useast1.s3-us-east-1.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-east-1%3A123456789012%3Astack/lambda-error-processor/1134083a-2608-1e91-9897-022501a2c456%7Cprimerinvoke%7C5d478078-13e9-baf0-464a-7ef285ecc786?AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Expires=1555451971&Signature=28UijZePE5I4dvukKQqM%2F9Rf1o4%3D",
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-processor/1134083a-2608-1e91-9897-022501a2c456",
  "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
```

```

    "LogicalResourceId": "primerinvoke",
    "ResourceType": "AWS::CloudFormation::CustomResource",
    "ResourceProperties": {
      "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-processor-primer-14R0R2T3JKU66",
      "FunctionName": "lambda-error-processor-randomerror-ZWUC391MQAJK"
    }
  }
}

```

Fungsi ini bertanggung jawab untuk mengembalikan respons ke panggilan balik URL yang menunjukkan keberhasilan atau kegagalan. Untuk sintaksis respons lengkap, lihat [Objek respons sumber daya kustom](#).

Example — respons sumber daya AWS CloudFormation khusus

```

{
  "Status": "SUCCESS",
  "PhysicalResourceId": "2019/04/18/[$LATEST]b3d1bfc65f19ec610654e4d9b9de47a0",
  "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-processor/1134083a-2608-1e91-9897-022501a2c456",
  "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
  "LogicalResourceId": "primerinvoke"
}

```

AWS CloudFormation menyediakan perpustakaan bernama `cfn-response` yang menangani pengiriman respons. Jika Anda menentukan fungsi Anda dalam template, Anda dapat meminta perpustakaan berdasarkan nama. AWS CloudFormation kemudian menambahkan perpustakaan ke paket penerapan yang dibuatnya untuk fungsi tersebut.

Jika fungsi yang digunakan Sumber Daya Kustom memiliki [Antarmuka Jaringan Elastis](#) yang melekat padanya, tambahkan sumber daya berikut ke VPC kebijakan di mana **region** Wilayah fungsi berada tanpa tanda hubung. Misalnya, `us-east-1` adalah `useast1`. Ini akan memungkinkan Custom Resource untuk merespons callback URL yang mengirimkan sinyal kembali ke AWS CloudFormation tumpukan.

```

arn:aws:s3:::cloudformation-custom-resource-response-region",
"arn:aws:s3:::cloudformation-custom-resource-response-region/*",

```

Contoh fungsi berikut memanggil suatu fungsi kedua. Jika panggilan berhasil, fungsi mengirimkan respons sukses AWS CloudFormation, dan pembaruan tumpukan berlanjut. Template menggunakan

tipe sumber daya [AWS::Serverless::Function](#) yang disediakan oleh AWS Serverless Application Model

Example — Fungsi sumber daya khusus

```
Transform: 'AWS::Serverless-2016-10-31'
Resources:
  primer:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs16.x
      InlineCode: |
        var aws = require('aws-sdk');
        var response = require('cfn-response');
        exports.handler = function(event, context) {
          // For Delete requests, immediately send a SUCCESS response.
          if (event.RequestType == "Delete") {
            response.send(event, context, "SUCCESS");
            return;
          }
          var responseStatus = "FAILED";
          var responseData = {};
          var functionName = event.ResourceProperties.FunctionName
          var lambda = new aws.Lambda();
          lambda.invoke({ FunctionName: functionName }, function(err, invokeResult) {
            if (err) {
              responseData = {Error: "Invoke call failed"};
              console.log(responseData.Error + ":\n", err);
            }
            else responseStatus = "SUCCESS";
            response.send(event, context, responseStatus, responseData);
          });
        };
      Description: Invoke a function to create a log stream.
      MemorySize: 128
      Timeout: 8
      Role: !GetAtt role.Arn
      Tracing: Active
```

Jika fungsi yang dipanggil sumber daya kustom tidak ditentukan dalam template, Anda bisa mendapatkan kode sumber `cfn-response` dari [modul `cfn-response` di Panduan Pengguna](#) AWS CloudFormation

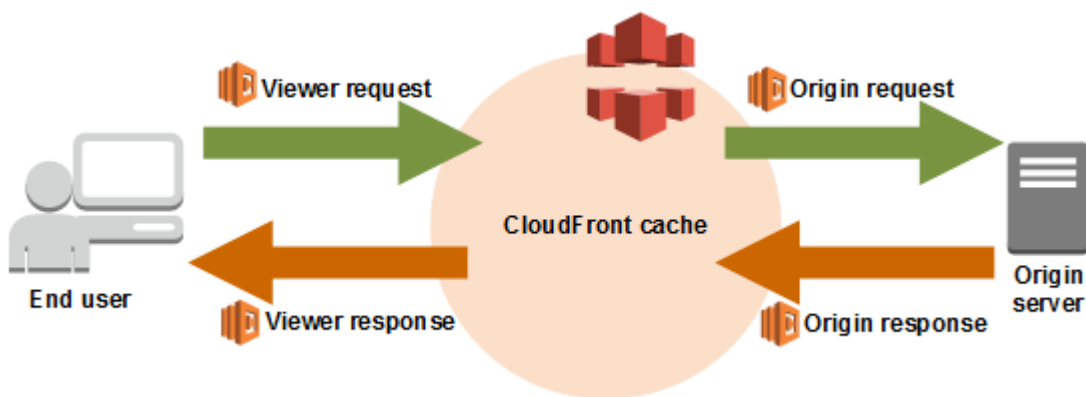
Untuk informasi selengkapnya tentang sumber daya kustom, lihat [Sumber daya kustom](#) dalam Panduan Pengguna AWS CloudFormation .

Menggunakan AWS Lambda dengan CloudFront Lambda @Edge

[Lambda @Edge](#) adalah ekstensi AWS Lambda yang memungkinkan Anda menerapkan fungsi Python dan Node.js di lokasi tepi Amazon. CloudFront Kasus penggunaan umum Lambda @Edge adalah menggunakan fungsi untuk menyesuaikan konten yang diberikan CloudFront distribusi Anda kepada pengguna akhir Anda. Memanggil fungsi-fungsi ini lebih dekat ke penampil alih-alih di server asal secara signifikan mengurangi latensi dan meningkatkan pengalaman pengguna.

Saat Anda mengaitkan CloudFront distribusi dengan fungsi Lambda @Edge, CloudFront mencegat permintaan dan respons di lokasi tepi. CloudFront kemudian memanggil fungsi Lambda Anda dengan mengirimkan acara. Anda dapat CloudFront menjalankan fungsi Lambda Anda ketika peristiwa berikut terjadi:

- Saat CloudFront menerima permintaan dari penampil (permintaan penampil)
- Sebelum CloudFront meneruskan permintaan ke asal (permintaan asal)
- Ketika CloudFront menerima respons dari asal (respons asal)
- Sebelum CloudFront mengembalikan respons ke penampil (respons penampil)



Note

Lambda@Edge mendukung set runtime dan fitur yang terbatas. Untuk detailnya, lihat [Persyaratan dan pembatasan fungsi Lambda](#) di panduan CloudFront pengembang Amazon.

Berikut ini adalah contoh dari suatu CloudFront peristiwa.

Example CloudFront pesan acara

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionId": "EDFDVBD6EXAMPLE"
        },
        "request": {
          "clientIp": "2001:0db8:85a3:0:0:8a2e:0370:7334",
          "method": "GET",
          "uri": "/picture.jpg",
          "headers": {
            "host": [
              {
                "key": "Host",
                "value": "d111111abcdef8.cloudfront.net"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "curl/7.51.0"
              }
            ]
          }
        }
      }
    }
  ]
}
```

Untuk informasi lebih lanjut tentang menggunakan Lambda@Edge, lihat [Menggunakan CloudFront dengan Lambda@Edge](#).

Memproses acara Amazon DocumentDB dengan Lambda

Anda dapat menggunakan fungsi Lambda untuk memproses peristiwa di [aliran perubahan Amazon DocumentDB \(dengan kompatibilitas MongoDB\) dengan mengonfigurasi cluster Amazon DocumentDB](#) sebagai sumber peristiwa. Kemudian, Anda dapat mengotomatiskan beban kerja berbasis peristiwa dengan menjalankan fungsi Lambda Anda setiap kali data berubah dengan cluster Amazon DocumentDB Anda.

Note

Lambda hanya mendukung Amazon DocumentDB versi 4.0 dan 5.0. Lambda tidak mendukung versi 3.6.

Selain itu, untuk pemetaan sumber acara, Lambda mendukung cluster berbasis instance dan cluster regional saja. [Lambda tidak mendukung cluster elastis atau cluster global](#). Batasan ini tidak berlaku saat menggunakan Lambda sebagai klien untuk terhubung ke Amazon DocumentDB. Lambda dapat terhubung ke semua jenis cluster untuk melakukan CRUD operasi.

Lambda memproses peristiwa dari Amazon DocumentDB mengubah aliran secara berurutan sesuai urutan kedatangannya. Karena itu, fungsi Anda hanya dapat menangani satu pemanggilan bersamaan dari Amazon DocumentDB sekaligus. Untuk memantau fungsi Anda, Anda dapat melacak [metrik konkurensinya](#).

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Topik

- [Contoh acara Amazon DocumentDB](#)
- [Prasyarat dan izin](#)
- [Konfigurasi jaringan](#)

- [Membuat pemetaan sumber peristiwa Amazon DocumentDB \(konsol\)](#)
- [Membuat pemetaan sumber peristiwa Amazon DocumentDB \(atau\) SDK CLI](#)
- [Posisi awal polling dan streaming](#)
- [Memantau sumber acara Amazon DocumentDB Anda](#)
- [Tutorial: Menggunakan AWS Lambda dengan Amazon DocumentDB Streams](#)

Contoh acara Amazon DocumentDB

```
{
  "eventSourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:canaryclusterb2a659a2-qo5tcmqkc103",
  "events": [
    {
      "event": {
        "_id": {
          "_data": "0163eeb6e7000000090100000009000041e1"
        },
        "clusterTime": {
          "$timestamp": {
            "t": 1676588775,
            "i": 9
          }
        },
        "documentKey": {
          "_id": {
            "$oid": "63eeb6e7d418cd98afb1c1d7"
          }
        },
        "fullDocument": {
          "_id": {
            "$oid": "63eeb6e7d418cd98afb1c1d7"
          },
          "anyField": "sampleValue"
        },
        "ns": {
          "db": "test_database",
          "coll": "test_collection"
        },
        "operationType": "insert"
      }
    }
  ]
}
```

```
  ],  
  "eventSource": "aws:docdb"  
}
```

Untuk informasi selengkapnya tentang peristiwa dalam contoh ini dan bentuknya, lihat [Mengubah Acara](#) di situs web Dokumentasi MongoDB.

Prasyarat dan izin

Sebelum Anda dapat menggunakan Amazon DocumentDB sebagai sumber acara untuk fungsi Lambda Anda, perhatikan prasyarat berikut. Anda harus:

- Memiliki cluster Amazon DocumentDB yang ada di tempat yang Akun AWS sama Wilayah AWS dan sebagai fungsi Anda. Jika Anda tidak memiliki cluster yang ada, Anda dapat membuatnya dengan mengikuti langkah-langkah di [Memulai dengan Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB](#). Atau, serangkaian langkah pertama dalam [Tutorial: Menggunakan AWS Lambda dengan Amazon DocumentDB Streams](#) memandu Anda membuat cluster Amazon DocumentDB dengan semua prasyarat yang diperlukan.
- Izinkan Lambda mengakses sumber daya Amazon Virtual Private Cloud VPC (Amazon) yang terkait dengan cluster Amazon DocumentDB Anda. Untuk informasi selengkapnya, lihat [Konfigurasi jaringan](#).
- Aktifkan TLS di cluster Amazon DocumentDB Anda. Ini adalah pengaturan default. Jika Anda menonaktifkan TLS, maka Lambda tidak dapat berkomunikasi dengan cluster Anda.
- Aktifkan aliran perubahan di cluster Amazon DocumentDB Anda. Untuk informasi selengkapnya, lihat [Menggunakan Ubah Aliran dengan Amazon DocumentDB](#) di Panduan Pengembang Amazon DocumentDB.
- Berikan Lambda kredensial untuk mengakses klaster Amazon DocumentDB Anda. Saat menyiapkan sumber acara, berikan [AWS Secrets Manager](#) kunci yang berisi detail otentikasi (nama pengguna dan kata sandi) yang diperlukan untuk mengakses klaster Anda. Untuk menyediakan kunci ini selama persiapan, lakukan salah satu hal berikut:
 - Jika Anda menggunakan konsol Lambda untuk persiapan, berikan kunci di bidang kunci manajer Rahasia.
 - Jika Anda menggunakan AWS Command Line Interface (AWS CLI) untuk persiapan, berikan kunci ini di `source-access-configurations` opsi. Anda dapat menyertakan opsi ini dengan [create-event-source-mapping](#) perintah atau [update-event-source-mapping](#) perintah. Sebagai contoh:

```
aws lambda create-event-source-mapping \  
  ...  
  --source-access-configurations  
  '[{"Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-  
west-2:123456789012:secret:DocDBSecret-AbC4E6"}]' \  
  ...
```

- Berikan izin Lambda untuk mengelola sumber daya yang terkait dengan aliran Amazon DocumentDB Anda. Tambahkan izin berikut secara manual ke [peran eksekusi](#) fungsi Anda:
 - [RDS: DescribeDBClusters](#)
 - [RDSDescribeDBCluster: DescribeDBClusterParameterGroups](#)
 - [RDSDescribeDBSubnet: DescribeDBSubnets](#)
 - [EC2: CreateNetworkInterface](#)
 - [EC2: DescribeNetworkInterfaces](#)
 - [EC2: DescribeVpcs](#)
 - [EC2: DeleteNetworkInterface](#)
 - [EC2: DescribeSubnets](#)
 - [EC2: DescribeSecurityGroups](#)
 - [kms:Decrypt](#)
 - [manajer rahasia: GetSecretValue](#)
- Pertahankan ukuran peristiwa aliran perubahan Amazon DocumentDB yang Anda kirim ke Lambda di bawah 6 MB. Lambda mendukung ukuran payload hingga 6 MB. Jika aliran perubahan Anda mencoba mengirim Lambda peristiwa yang lebih besar dari 6 MB, maka Lambda akan menghapus pesan dan memancarkan metrik. `OversizedRecordCount` Lambda memancarkan semua metrik dengan upaya terbaik.

Note

Sementara fungsi Lambda biasanya memiliki batas waktu tunggu maksimum 15 menit, pemetaan sumber acara untuk Amazon, Apache Kafka yang dikelola sendiri, MSK Amazon DocumentDB, dan Amazon MQ untuk ActiveMQ dan RabbitMQ hanya mendukung fungsi dengan batas waktu tunggu maksimum 14 menit. Kendala ini memastikan bahwa pemetaan sumber peristiwa dapat menangani kesalahan fungsi dan percobaan ulang dengan benar.

Konfigurasi jaringan

Agar Lambda dapat menggunakan klaster Amazon DocumentDB Anda sebagai sumber peristiwa, Lambda memerlukan akses ke Amazon VPC tempat klaster Anda berada. Kami menyarankan Anda menerapkan AWS PrivateLink [VPCtitik akhir](#) untuk Lambda untuk mengakses Anda. VPC Menerapkan VPC endpoint untuk Lambda dan, jika cluster menggunakan otentikasi, gunakan juga endpoint untuk Secrets Manager. VPC

Atau, pastikan bahwa yang VPC terkait dengan klaster Amazon DocumentDB Anda menyertakan NAT satu gateway per subnet publik. Untuk informasi selengkapnya, lihat [the section called “Akses internet untuk VPC fungsi”](#).

Jika Anda menggunakan VPC titik akhir, Anda juga harus mengonfigurasinya untuk [mengaktifkan DNS nama pribadi](#).

Saat Anda membuat pemetaan sumber peristiwa untuk klaster Amazon DocumentDB, Lambda memeriksa apakah Elastic ENIs Network Interfaces () sudah ada untuk subnet dan grup keamanan klaster Anda. VPC Jika Lambda menemukan yang ada ENIs, ia mencoba untuk menggunakannya kembali. Jika tidak, Lambda membuat yang baru ENIs untuk terhubung ke sumber acara dan memanggil fungsi Anda.

Note

Fungsi Lambda selalu berjalan di dalam yang VPCs dimiliki oleh layanan Lambda. Ini VPCs dikelola secara otomatis oleh layanan dan tidak terlihat oleh pelanggan. Anda juga dapat menghubungkan fungsi Anda ke AmazonVPC. Dalam kedua kasus tersebut, VPC konfigurasi fungsi Anda tidak memengaruhi pemetaan sumber peristiwa. Hanya konfigurasi sumber acara yang VPC menentukan bagaimana Lambda terhubung ke sumber acara Anda.

VPCaturan kelompok keamanan

Konfigurasi grup keamanan untuk Amazon VPC yang berisi klaster Anda dengan aturan berikut (minimal):

- Aturan masuk - Izinkan semua lalu lintas di port klaster Amazon DocumentDB untuk grup keamanan yang ditentukan untuk sumber peristiwa Anda. Amazon DocumentDB menggunakan port 27017 secara default.

- Aturan keluar - Izinkan semua lalu lintas di port 443 untuk semua tujuan. Izinkan semua lalu lintas di port cluster Amazon DocumentDB. Amazon DocumentDB menggunakan port 27017 secara default.
- Jika Anda menggunakan VPC titik akhir alih-alih NAT gateway, grup keamanan yang terkait dengan VPC titik akhir harus mengizinkan semua lalu lintas masuk pada port 443 dari grup keamanan sumber acara.

Bekerja dengan titik VPC akhir

Saat Anda menggunakan VPC titik akhir, API panggilan untuk memanggil fungsi Anda dirutekan melalui titik akhir ini menggunakan. ENIs Kepala layanan Lambda perlu memanggil `lambda:InvokeFunction` fungsi apa pun yang menggunakannya. ENIs

Secara default, VPC titik akhir memiliki IAM kebijakan yang terbuka. Praktik terbaik adalah membatasi kebijakan ini untuk hanya mengizinkan prinsipal tertentu untuk melakukan tindakan yang diperlukan menggunakan titik akhir tersebut. Untuk memastikan bahwa pemetaan sumber peristiwa Anda dapat menjalankan fungsi Lambda Anda, kebijakan VPC titik akhir harus mengizinkan prinsip layanan Lambda untuk memanggil. `lambda:InvokeFunction` Membatasi kebijakan VPC titik akhir Anda untuk hanya mengizinkan API panggilan yang berasal dari organisasi Anda mencegah pemetaan sumber peristiwa berfungsi dengan baik.

Contoh kebijakan VPC endpoint berikut menunjukkan cara memberikan akses yang diperlukan untuk titik akhir Lambda.

Example VPCkebijakan titik akhir - Titik akhir Lambda

```
{
  "Statement": [
    {
      "Action": "lambda:InvokeFunction",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "*"
    }
  ]
}
```

Jika klaster Amazon DocumentDB menggunakan autentikasi, Anda juga dapat membatasi kebijakan titik akhir untuk titik akhir VPC Secrets Manager. Untuk memanggil Secrets Manager API, Lambda menggunakan peran fungsi Anda, bukan kepala layanan Lambda. Contoh berikut menunjukkan kebijakan titik akhir Secrets Manager.

Example VPCkebijakan endpoint - titik akhir Secrets Manager

```
{
  "Statement": [
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "customer_function_execution_role_arn"
        ]
      },
      "Resource": "customer_secret_arn"
    }
  ]
}
```

Membuat pemetaan sumber peristiwa Amazon DocumentDB (konsol)

[Agar fungsi Lambda dapat dibaca dari aliran perubahan klaster Amazon DocumentDB, buat pemetaan sumber peristiwa.](#) Bagian ini menjelaskan cara melakukan ini dari konsol Lambda. Untuk AWS SDK dan AWS CLI instruksi, lihat [the section called “Membuat pemetaan sumber peristiwa Amazon DocumentDB \(atau\) SDK CLI”](#).

Untuk membuat pemetaan sumber peristiwa Amazon DocumentDB (konsol)

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.
4. Di bawah konfigurasi Trigger, dalam daftar dropdown, pilih DocumentDB.
5. Konfigurasi opsi yang diperlukan, lalu pilih Tambah.

Lambda mendukung opsi berikut untuk sumber acara Amazon DocumentDB:

- Cluster DocumentDB - Pilih cluster Amazon DocumentDB.
- Aktifkan pemicu - Pilih apakah Anda ingin segera mengaktifkan pemicu. Jika Anda memilih kotak centang ini, maka fungsi Anda segera mulai menerima lalu lintas dari aliran perubahan Amazon DocumentDB yang ditentukan setelah pembuatan pemetaan sumber peristiwa. Kami menyarankan Anda mengosongkan kotak centang untuk membuat pemetaan sumber peristiwa dalam status dinonaktifkan untuk pengujian. Setelah pembuatan, Anda dapat mengaktifkan pemetaan sumber acara kapan saja.
- Nama database — Masukkan nama database dalam cluster untuk dikonsumsi.
- (Opsional) Nama koleksi — Masukkan nama koleksi dalam database untuk dikonsumsi. Jika Anda tidak menentukan koleksi, maka Lambda akan mendengarkan semua peristiwa dari setiap koleksi dalam database.
- Ukuran Batch - Atur jumlah maksimum pesan yang akan diambil dalam satu batch, hingga 10.000. Ukuran batch default adalah 100.
- Posisi awal — Pilih posisi dalam aliran untuk mulai membaca catatan dari.
 - Terbaru - Memproses hanya catatan baru yang ditambahkan ke aliran. Fungsi Anda mulai memproses catatan hanya setelah Lambda selesai membuat sumber acara Anda. Ini berarti bahwa beberapa catatan mungkin dijatuhkan sampai sumber acara Anda berhasil dibuat.
 - Trim horizon – Memproses semua rekaman dalam aliran. Lambda menggunakan durasi retensi log klaster Anda untuk menentukan dari mana harus mulai membaca peristiwa. Secara khusus, Lambda mulai membaca dari `current_time - log_retention_duration` Aliran perubahan Anda harus sudah aktif sebelum stempel waktu ini agar Lambda dapat membaca semua peristiwa dengan benar.
 - Pada stempel waktu – Proses rekaman dimulai dari waktu tertentu. Aliran perubahan Anda harus sudah aktif sebelum stempel waktu yang ditentukan agar Lambda dapat membaca semua peristiwa dengan benar.
- Otentikasi — Pilih metode otentikasi untuk mengakses broker di cluster Anda.
 - BASIC_AUTH — Dengan otentikasi dasar, Anda harus memberikan kunci Secrets Manager yang berisi kredensi untuk mengakses klaster Anda.
- Kunci Secrets Manager - Pilih kunci Secrets Manager yang berisi detail otentikasi (nama pengguna dan kata sandi) yang diperlukan untuk mengakses klaster Amazon DocumentDB Anda.
- (Opsional) Jendela Batch - Atur jumlah waktu maksimum dalam hitungan detik untuk mengumpulkan catatan sebelum menjalankan fungsi Anda, hingga 300.
- (Opsional) Konfigurasi dokumen lengkap — Untuk operasi pembaruan dokumen, pilih apa yang ingin Anda kirim ke aliran. Nilai defaultnya adalah `Default`, yang berarti bahwa untuk setiap

peristiwa aliran perubahan, Amazon DocumentDB hanya mengirimkan delta yang menjelaskan perubahan yang dibuat. Untuk informasi selengkapnya tentang bidang ini, lihat [FullDocument](#) di dokumentasi MongoDB JavadocAPI.

- **Default** — Lambda hanya mengirimkan sebagian dokumen yang menjelaskan perubahan yang dibuat.
- **UpdateLookup**— Lambda mengirimkan delta yang menjelaskan perubahan, bersama dengan salinan seluruh dokumen.

Membuat pemetaan sumber peristiwa Amazon DocumentDB (atau) SDK CLI

Untuk membuat atau mengelola pemetaan sumber peristiwa Amazon DocumentDB dengan, Anda dapat [AWS SDK](#) menggunakan operasi berikut: API

- [CreateEventSourceMapping](#)
- [ListEventSourceMappings](#)
- [GetEventSourceMapping](#)
- [UpdateEventSourceMapping](#)
- [DeleteEventSourceMapping](#)

Untuk membuat pemetaan sumber acara dengan AWS CLI, gunakan [create-event-source-mapping](#) perintah. Contoh berikut menggunakan perintah ini untuk memetakan fungsi bernama `my-function` ke aliran perubahan Amazon DocumentDB. Sumber peristiwa ditentukan oleh Amazon Resource Name (ARN), dengan ukuran batch 500, dimulai dari stempel waktu dalam waktu Unix. Perintah ini juga menentukan kunci Secrets Manager yang digunakan Lambda untuk terhubung ke Amazon DocumentDB. Selain itu, ini termasuk `document-db-event-source-config` parameter yang menentukan database dan koleksi untuk dibaca.

```
aws lambda create-event-source-mapping --function-name my-function \  
    --event-source-arn arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-  
epzcyvu4pjjoy \  
    --batch-size 500 \  
    --starting-position AT_TIMESTAMP \  
    --starting-position-timestamp 1541139109 \  

```

```
--source-access-configurations
'["Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocDBSecret-BATjxi"]]' \
--document-db-event-source-config '{"DatabaseName":"test_database",
"CollectionName": "test_collection"}' \
```

Anda akan melihat output seperti ini:

```
{
  "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
  "BatchSize": 500,
  "DocumentDBEventSourceConfig": {
    "CollectionName": "test_collection",
    "DatabaseName": "test_database",
    "FullDocument": "Default"
  },
  "MaximumBatchingWindowInSeconds": 0,
  "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
  "LastModified": 1541348195.412,
  "LastProcessingResult": "No records processed",
  "State": "Creating",
  "StateTransitionReason": "User action"
}
```

Setelah pembuatan, Anda dapat menggunakan [update-event-source-mapping](#) perintah untuk memperbarui pengaturan untuk sumber acara Amazon DocumentDB Anda. Contoh berikut memperbarui ukuran batch menjadi 1.000 dan jendela batch menjadi 10 detik. Untuk perintah ini, Anda memerlukan UUID pemetaan sumber acara Anda, yang dapat Anda ambil menggunakan `list-event-source-mapping` perintah atau konsol Lambda.

```
aws lambda update-event-source-mapping --function-name my-function \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--batch-size 1000 \
--batch-window 10
```

Anda akan melihat output ini yang terlihat seperti ini:

```
{
  "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
```

```
"BatchSize": 500,
"DocumentDBEventSourceConfig": {
  "CollectionName": "test_collection",
  "DatabaseName": "test_database",
  "FullDocument": "Default"
},
"MaximumBatchingWindowInSeconds": 0,
"EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-epzcyvu4pjoy",
"FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
"LastModified": 1541359182.919,
"LastProcessingResult": "OK",
"State": "Updating",
"StateTransitionReason": "User action"
}
```

Lambda memperbarui pengaturan secara asinkron, sehingga Anda mungkin tidak melihat perubahan ini dalam output sampai proses selesai. Untuk melihat pengaturan saat ini dari pemetaan sumber acara Anda, gunakan [get-event-source-mapping](#) perintah.

```
aws lambda get-event-source-mapping --uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b
```

Anda akan melihat output ini yang terlihat seperti ini:

```
{
  "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
  "DocumentDBEventSourceConfig": {
    "CollectionName": "test_collection",
    "DatabaseName": "test_database",
    "FullDocument": "Default"
  },
  "BatchSize": 1000,
  "MaximumBatchingWindowInSeconds": 10,
  "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-epzcyvu4pjoy",
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
  "LastModified": 1541359182.919,
  "LastProcessingResult": "OK",
  "State": "Enabled",
  "StateTransitionReason": "User action"
}
```

Untuk menghapus pemetaan sumber peristiwa Amazon DocumentDB Anda, gunakan perintah [delete-event-source-mapping](#)

```
aws lambda delete-event-source-mapping \  
  --uuid 2b733gdc-8ac3-cdf5-af3a-1827b3b11284
```

Posisi awal polling dan streaming

Ketahui bahwa polling streaming selama pembuatan dan pembaruan pemetaan sumber acara pada akhirnya konsisten.

- Selama pembuatan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk memulai acara polling dari aliran.
- Selama pembaruan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk menghentikan dan memulai kembali acara pemungutan suara dari aliran.

Perilaku ini berarti bahwa jika Anda menentukan LATEST sebagai posisi awal untuk aliran, pemetaan sumber peristiwa dapat melewati peristiwa selama pembuatan atau pembaruan. Untuk memastikan bahwa tidak ada peristiwa yang terlewatkan, tentukan posisi awal aliran sebagai TRIM_HORIZON atau AT_TIMESTAMP.

Memantau sumber acara Amazon DocumentDB Anda

Untuk membantu Anda memantau sumber peristiwa Amazon DocumentDB, Lambda memancarkan metrik saat fungsi Anda `IteratorAge` selesai memproses sekumpulan rekaman. Usia iterator adalah perbedaan antara stempel waktu acara terbaru dan stempel waktu saat ini. Pada dasarnya, `IteratorAge` metrik menunjukkan berapa umur catatan terakhir yang diproses dalam batch. Jika fungsi Anda saat ini memproses peristiwa baru, maka Anda dapat menggunakan usia iterator untuk memperkirakan latensi antara saat catatan ditambahkan dan saat fungsi Anda memprosesnya. Tren yang meningkat `IteratorAge` dapat menunjukkan masalah dengan fungsi Anda. Untuk informasi selengkapnya, lihat [Lihat metrik untuk fungsi Lambda](#).

Aliran perubahan Amazon DocumentDB tidak dioptimalkan untuk menangani kesenjangan waktu yang besar antar peristiwa. Jika sumber peristiwa Amazon DocumentDB Anda tidak menerima peristiwa apa pun untuk jangka waktu yang lama, Lambda dapat menonaktifkan pemetaan sumber peristiwa. Panjang periode waktu ini dapat bervariasi dari beberapa minggu hingga beberapa bulan tergantung pada ukuran cluster dan beban kerja lainnya.

Lambda mendukung muatan hingga 6 MB. Namun, peristiwa aliran perubahan Amazon DocumentDB dapat berukuran hingga 16 MB. Jika aliran perubahan Anda mencoba mengirim Lambda peristiwa aliran perubahan yang lebih besar dari 6 MB, maka Lambda akan menghapus pesan dan memancarkan metrik. `OversizedRecordCount` Lambda memancarkan semua metrik dengan upaya terbaik.

Tutorial: Menggunakan AWS Lambda dengan Amazon DocumentDB Streams

Dalam tutorial ini, Anda membuat fungsi Lambda dasar yang menggunakan peristiwa dari aliran perubahan Amazon DocumentDB (dengan kompatibilitas MongoDB). Untuk menyelesaikan tutorial ini, Anda akan melalui tahapan berikut:

- Siapkan cluster Amazon DocumentDB Anda, sambungkan ke sana, dan aktifkan aliran perubahan di dalamnya.
- Buat fungsi Lambda Anda, dan konfigurasi cluster Amazon DocumentDB Anda sebagai sumber peristiwa untuk fungsi Anda.
- Uji end-to-end penyiapan dengan memasukkan item ke dalam database Amazon DocumentDB Anda.

Topik

- [Prasyarat](#)
- [Ciptakan AWS Cloud9 lingkungan](#)
- [Buat grup EC2 keamanan Amazon](#)
- [Buat cluster Amazon DocumentDB](#)
- [Buat rahasia di Secrets Manager](#)
- [Instal cangkang mongo](#)
- [Connect ke cluster Amazon DocumentDB](#)
- [Aktifkan aliran perubahan](#)
- [Buat titik VPC akhir antarmuka](#)
- [Buat peran eksekusi](#)
- [Buat fungsi Lambda](#)
- [Buat pemetaan sumber acara Lambda](#)
- [Uji fungsi Anda - pemanggilan manual](#)

- [Uji fungsi Anda - masukkan catatan](#)
- [Uji fungsi Anda - perbarui catatan](#)
- [Uji fungsi Anda - hapus catatan](#)
- [Bersihkan sumber daya Anda](#)

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan masukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Instal AWS Command Line Interface

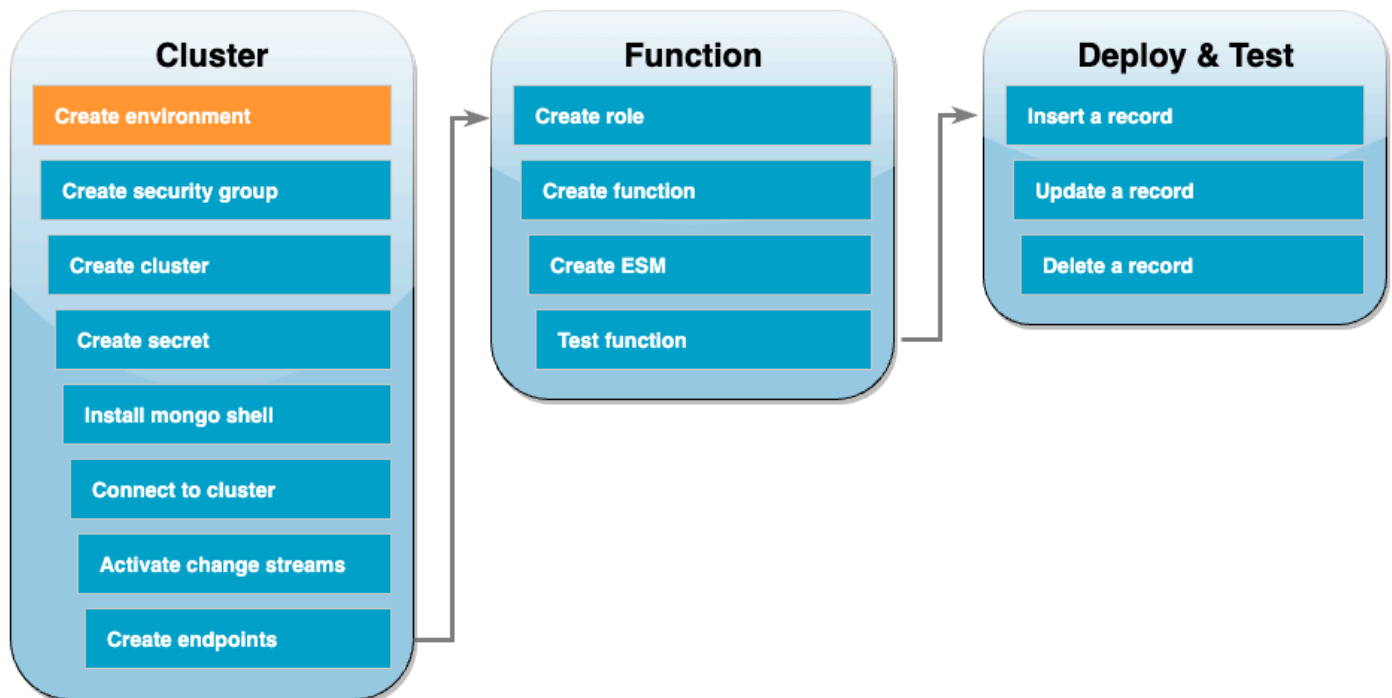
Jika Anda belum menginstal AWS Command Line Interface, ikuti langkah-langkah di [Menginstal atau memperbarui versi terbaru AWS CLI untuk menginstalnya](#).

Tutorial ini membutuhkan terminal baris perintah atau shell untuk menjalankan perintah. Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa CLI perintah Bash yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#).

Ciptakan AWS Cloud9 lingkungan



Sebelum membuat fungsi Lambda, Anda perlu membuat dan mengonfigurasi cluster Amazon DocumentDB Anda. Langkah-langkah untuk mengatur cluster Anda dalam tutorial ini didasarkan pada prosedur di [Memulai dengan Amazon DocumentDB](#).

Note

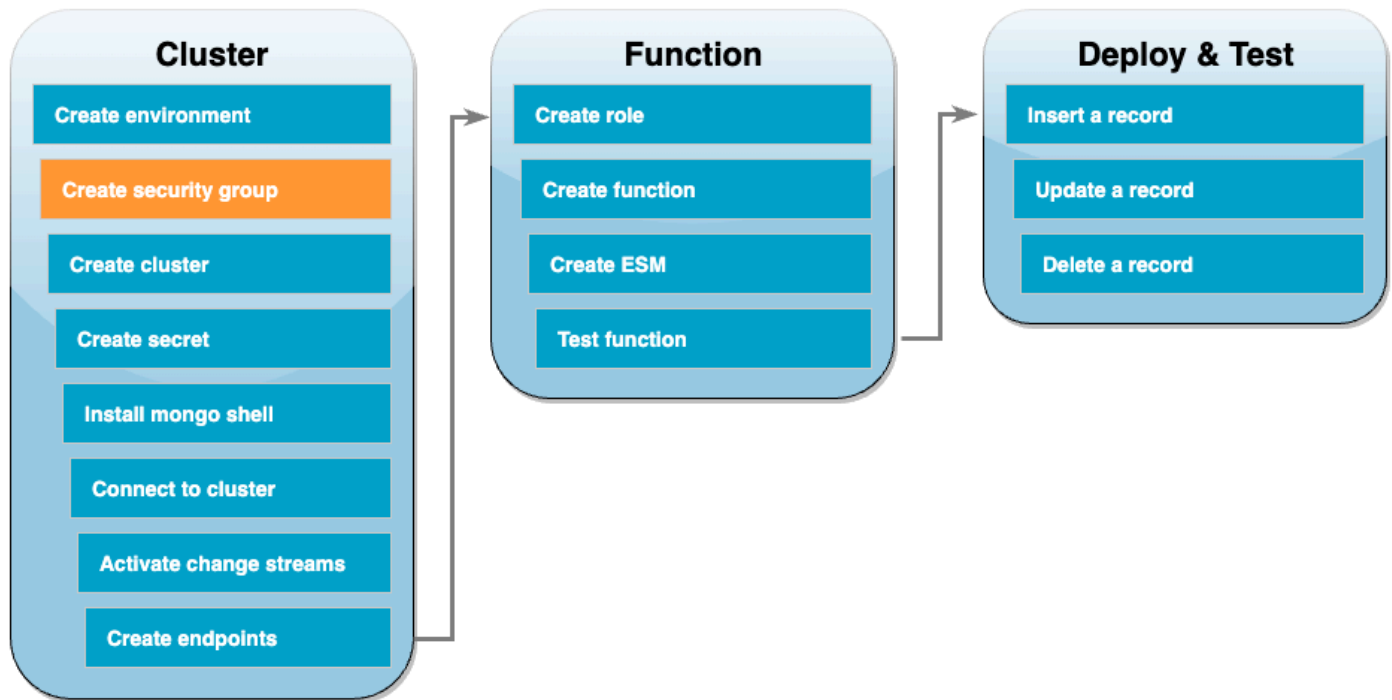
Jika Anda sudah menyiapkan kluster Amazon DocumentDB, pastikan Anda mengaktifkan aliran perubahan dan membuat titik akhir antarmuka yang diperlukan. VPC Kemudian, Anda dapat langsung melompat ke langkah-langkah pembuatan fungsi.

Pertama, ciptakan AWS Cloud9 lingkungan. Anda akan menggunakan lingkungan ini di seluruh tutorial ini untuk terhubung ke dan menanyakan cluster Amazon DocumentDB Anda.

Untuk menciptakan AWS Cloud9 lingkungan

1. Buka [AWS Cloud9 konsol](#) dan pilih Buat lingkungan.
2. Buat lingkungan dengan konfigurasi berikut:
 - Di bawah Detail:
 - Nama: DocumentDBCloud9Environment
 - Jenis lingkungan: EC2 Contoh baru
 - Di bawah EC2contoh Baru:
 - Jenis contoh: t2.micro (1 GiB RAM + 1 v) CPU
 - Platform: Amazon Linux 2
 - Batas waktu: 30 menit
 - Di bawah Pengaturan jaringan:
 - Koneksi: AWS Systems Manager (SSM)
 - Perluas dropdown VPCpengaturan.
 - Amazon Virtual Private Cloud (VPC: Pilih default [Anda. VPC](#))
 - Subnet: Tidak ada preferensi
 - Simpan semua pengaturan default lainnya.
3. Pilih Buat. Penyediaan AWS Cloud9 lingkungan baru Anda dapat memakan waktu beberapa menit.

Buat grup EC2 keamanan Amazon



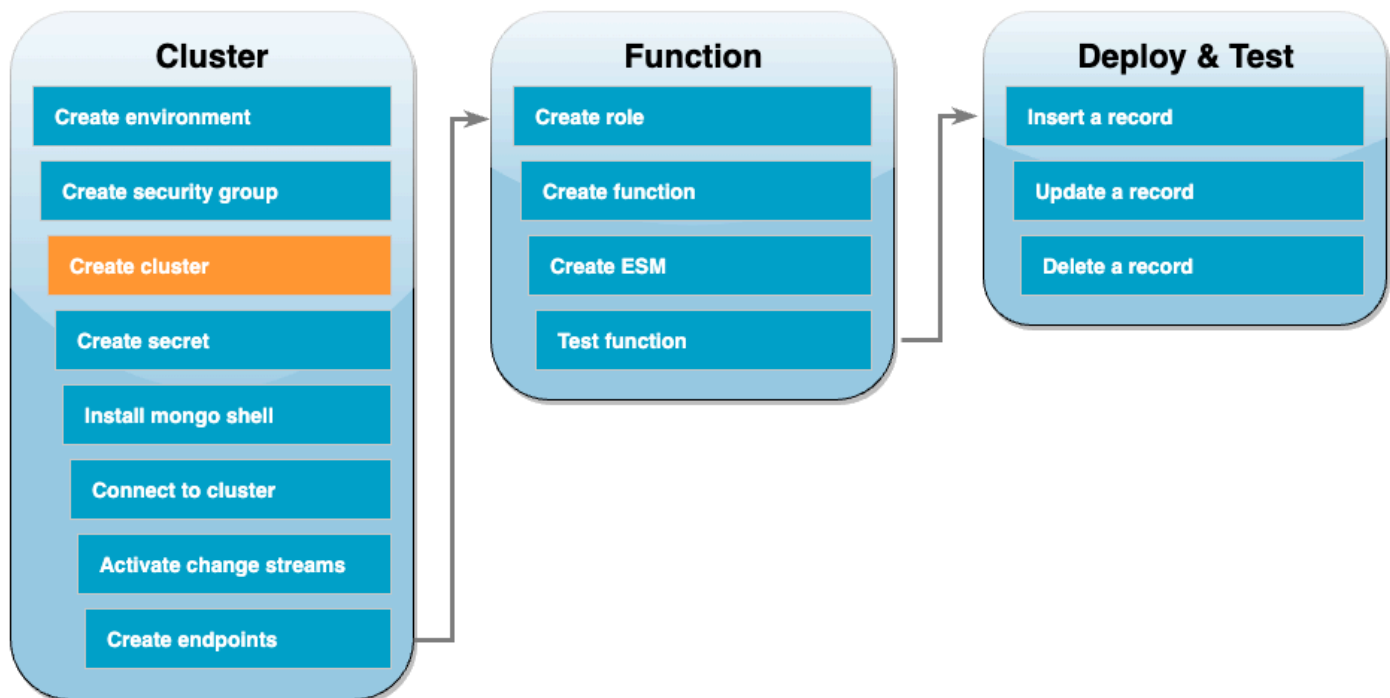
Selanjutnya, buat [grup EC2 keamanan Amazon](#) dengan aturan yang memungkinkan lalu lintas antara cluster Amazon DocumentDB Anda dan lingkungan Anda. AWS Cloud9

Untuk membuat grup EC2 keamanan

1. Buka [EC2konsol](#). Di bawah Jaringan dan Keamanan, pilih Grup keamanan.
2. Pilih Buat grup keamanan.
3. Buat grup keamanan dengan konfigurasi berikut:
 - Di bawah Detail dasar:
 - Nama grup keamanan: `DocDBTutorial`
 - Deskripsi: Grup keamanan untuk lalu lintas antara AWS Cloud9 dan Amazon DocumentDB.
 - VPC: Pilih [default](#) AndaVPC.
 - Di Aturan masuk, pilih Tambahkan aturan. Buat aturan dengan konfigurasi berikut:
 - Jenis: Kustom TCP
 - Rentang pelabuhan: 27017
 - Sumber: Kustom

- Di kotak pencarian di sebelah Sumber, pilih grup keamanan untuk AWS Cloud9 lingkungan yang Anda buat di langkah sebelumnya. Untuk melihat daftar grup keamanan yang tersedia, masukkan `c1oud9` di kotak pencarian. Pilih grup keamanan dengan nama `aws-c1oud9-<environment_name>`.
 - Simpan semua pengaturan default lainnya.
4. Pilih Buat grup keamanan.

Buat cluster Amazon DocumentDB



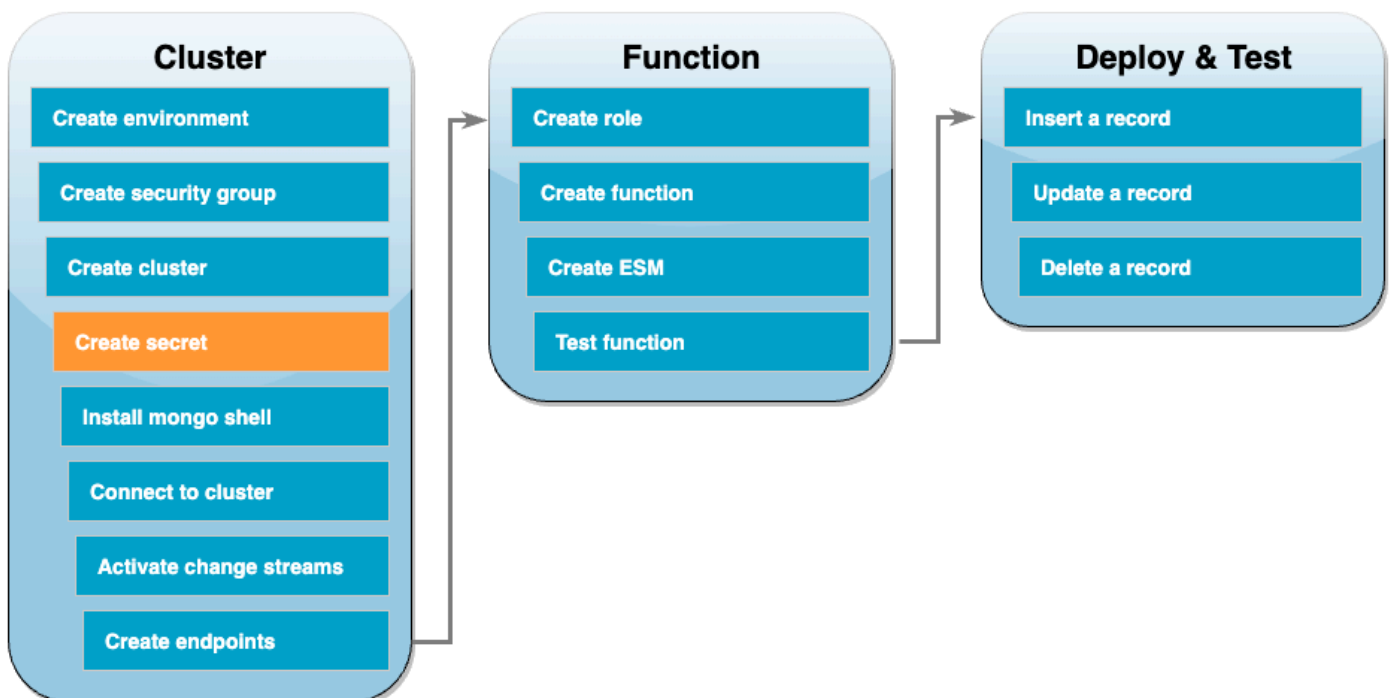
Pada langkah ini, Anda akan membuat cluster Amazon DocumentDB menggunakan grup keamanan dari langkah sebelumnya.

Untuk membuat cluster Amazon DocumentDB

1. Buka konsol [Amazon DocumentDB](#). Di bawah Cluster, pilih Buat.
2. Buat cluster dengan konfigurasi berikut:
 - Untuk tipe Cluster, pilih Instance Based Cluster.
 - Di bawah Konfigurasi:
 - Versi mesin: 5.0.0

- Kelas instance: db.t3.medium (uji coba gratis memenuhi syarat)
 - Jumlah contoh: 1
 - Di bawah Otentikasi:
 - Masukkan Nama Pengguna dan Kata Sandi yang diperlukan untuk terhubung ke klaster Anda (kredensi yang sama seperti yang Anda gunakan untuk membuat rahasia di langkah sebelumnya). Di Konfirmasi kata sandi, konfirmasi kata sandi Anda.
 - Aktifkan Tampilkan pengaturan lanjutan.
 - Di bawah Pengaturan jaringan:
 - Virtual Private Cloud (VPC): Pilih [default](#) AndaVPC.
 - Grup subnet: default
 - VPCgrup keamanan: Selain itudefault (VPC), pilih grup DocDBTutorial (VPC) keamanan yang Anda buat di langkah sebelumnya.
 - Simpan semua pengaturan default lainnya.
3. Pilih Buat klaster. Penyediaan cluster Amazon DocumentDB Anda dapat memakan waktu beberapa menit.

Buat rahasia di Secrets Manager



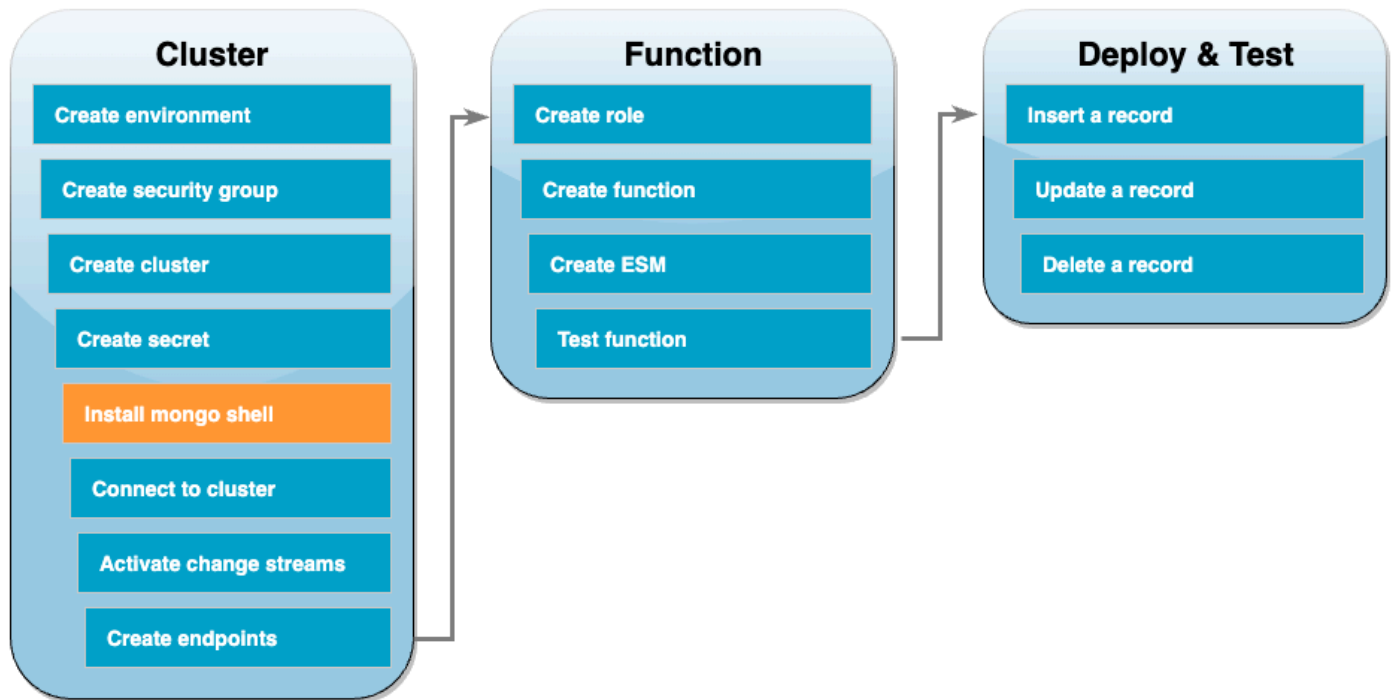
Untuk mengakses klaster Amazon DocumentDB Anda secara manual, Anda harus memberikan kredensi nama pengguna dan kata sandi. Agar Lambda dapat mengakses klaster Anda, Anda harus memberikan rahasia Secrets Manager yang berisi kredensial akses yang sama ini saat menyiapkan pemetaan sumber acara Anda. Pada langkah ini, Anda akan membuat rahasia ini.

Untuk membuat rahasia di Secrets Manager

1. Buka konsol [Secrets Manager](#) dan pilih Simpan rahasia baru.
2. Untuk Pilih jenis rahasia, pilih opsi berikut:
 - Di bawah Detail dasar:
 - Jenis rahasia: Kredensi untuk database Amazon DocumentDB Anda
 - Di bawah Kredensial, masukkan nama pengguna dan kata sandi yang akan Anda gunakan untuk mengakses klaster Amazon DocumentDB Anda.
 - Database: Pilih cluster Amazon DocumentDB Anda.
 - Pilih Berikutnya.
3. Untuk Konfigurasi rahasia, pilih opsi berikut:
 - Nama rahasia — DocumentDBSecret
 - Pilih Berikutnya.
4. Pilih Berikutnya.
5. Pilih Toko.
6. Segarkan konsol untuk memverifikasi bahwa Anda berhasil menyimpan DocumentDBSecret rahasia.

Catat Rahasia ARN Rahasia Anda Anda akan membutuhkannya di langkah selanjutnya.

Instal cangkang mongo



Pada langkah ini, Anda akan menginstal shell mongo di AWS Cloud9 lingkungan Anda. Mongo shell adalah utilitas baris perintah yang Anda gunakan untuk menghubungkan dan menanyakan cluster Amazon DocumentDB Anda.

Untuk menginstal shell mongo di lingkungan Anda AWS Cloud9

1. Buka [konsol AWS Cloud9](#). Di sebelah DocumentDBCloud9Environment lingkungan yang Anda buat sebelumnya, klik tautan Buka di bawah AWS Cloud9 IDE kolom.
2. Di jendela terminal, buat file repositori MongoDB dengan perintah berikut:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
\ngpgkey=https://www.mongodb.org/static/pgp/server-5.0.asc" | sudo tee /etc/
yum.repos.d/mongodb-org-5.0.repo
```

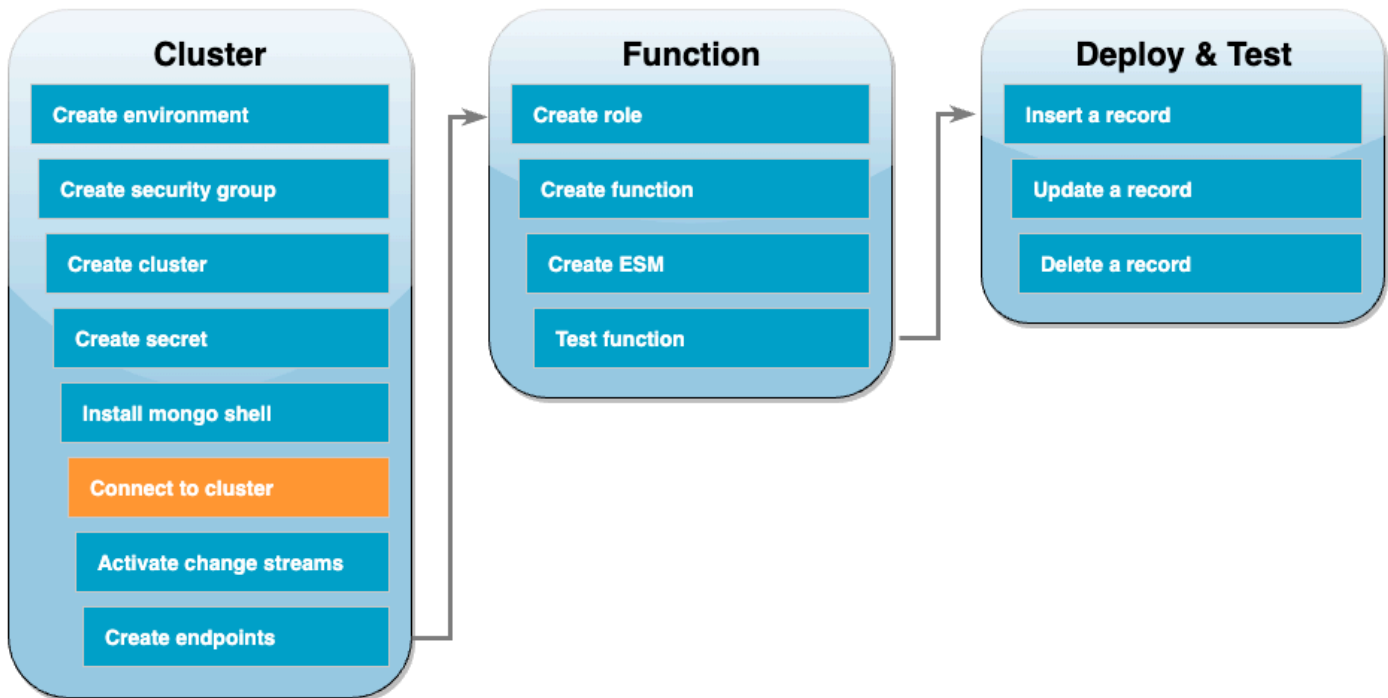
3. Kemudian, instal shell mongo dengan perintah berikut:

```
sudo yum install -y mongodb-org-shell
```

- Untuk mengenkripsi data dalam perjalanan, unduh [kunci publik untuk Amazon DocumentDB](#). Perintah berikut mengunduh file bernama `global-bundle.pem`:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Connect ke cluster Amazon DocumentDB



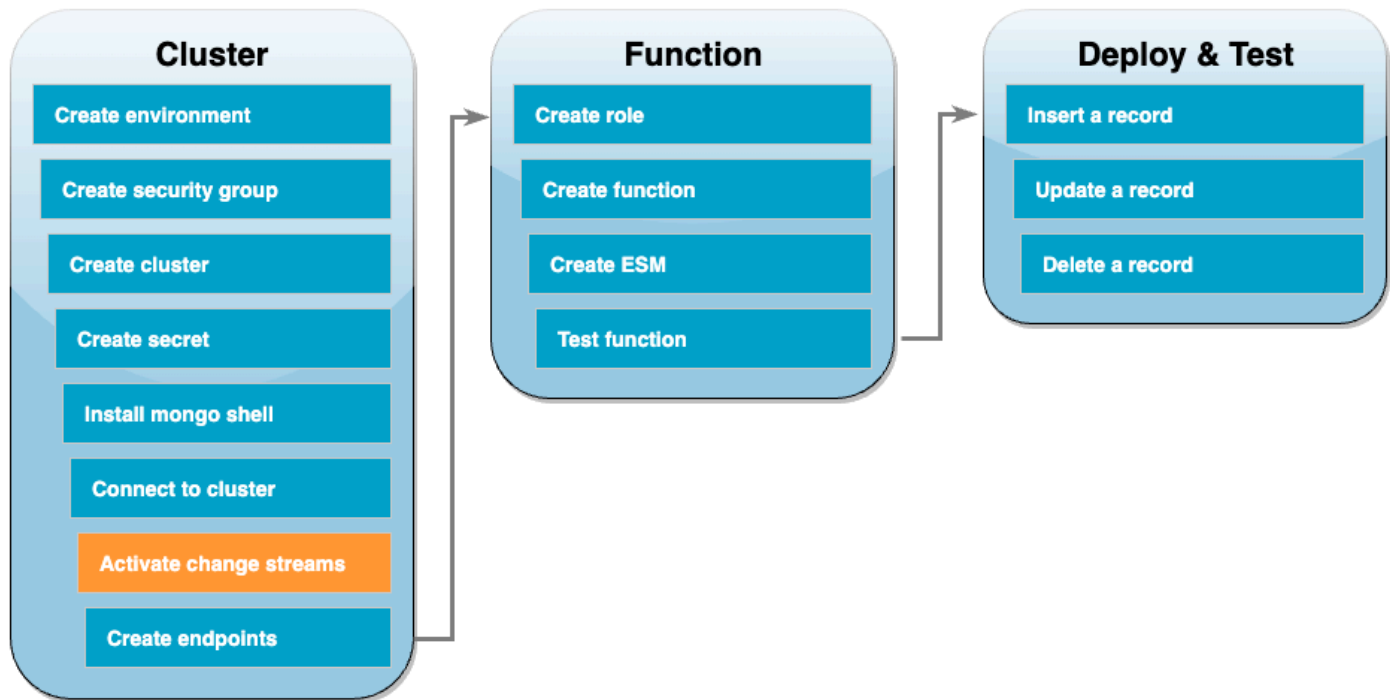
Anda sekarang siap untuk terhubung ke cluster Amazon DocumentDB Anda menggunakan shell mongo.

Untuk terhubung ke cluster Amazon DocumentDB Anda

- Buka konsol [Amazon DocumentDB](#). Di bawah Cluster, pilih klaster Anda dengan memilih pengenal klaster.
- Di tab Connectivity & security, di bawah Connect to this cluster with the mongo shell, pilih Copy.
- Di AWS Cloud9 lingkungan Anda, tempelkan perintah ini ke terminal. Ganti `<insertYourPassword>` dengan kata sandi yang benar.

Setelah memasukkan perintah ini, jika command prompt menjadi `s0:PRIMARY>`, maka Anda terhubung ke cluster Amazon DocumentDB Anda.

Aktifkan aliran perubahan



Untuk tutorial ini, Anda akan melacak perubahan pada `products` koleksi `docdbdemo` database di cluster Amazon DocumentDB Anda. Anda melakukan ini dengan mengaktifkan [aliran perubahan](#). Pertama, buat `docdbdemo` database dan uji dengan memasukkan catatan.

Untuk membuat database baru di dalam klaster Anda

1. Di AWS Cloud9 lingkungan Anda, pastikan Anda masih [terhubung ke klaster Amazon DocumentDB Anda](#).
2. Di jendela terminal, gunakan perintah berikut untuk membuat database baru yang disebut `docdbdemo`:

```
use docdbdemo
```

3. Kemudian, gunakan perintah berikut untuk menyisipkan catatan ke `docdbdemo`:

```
db.products.insert({"hello":"world"})
```

Anda akan melihat output seperti ini:

```
WriteResult({ "nInserted" : 1 })
```

- Gunakan perintah berikut untuk daftar semua database:

```
show dbs
```

Pastikan output Anda berisi docdbdemo database:

```
docdbdemo 0.000GB
```

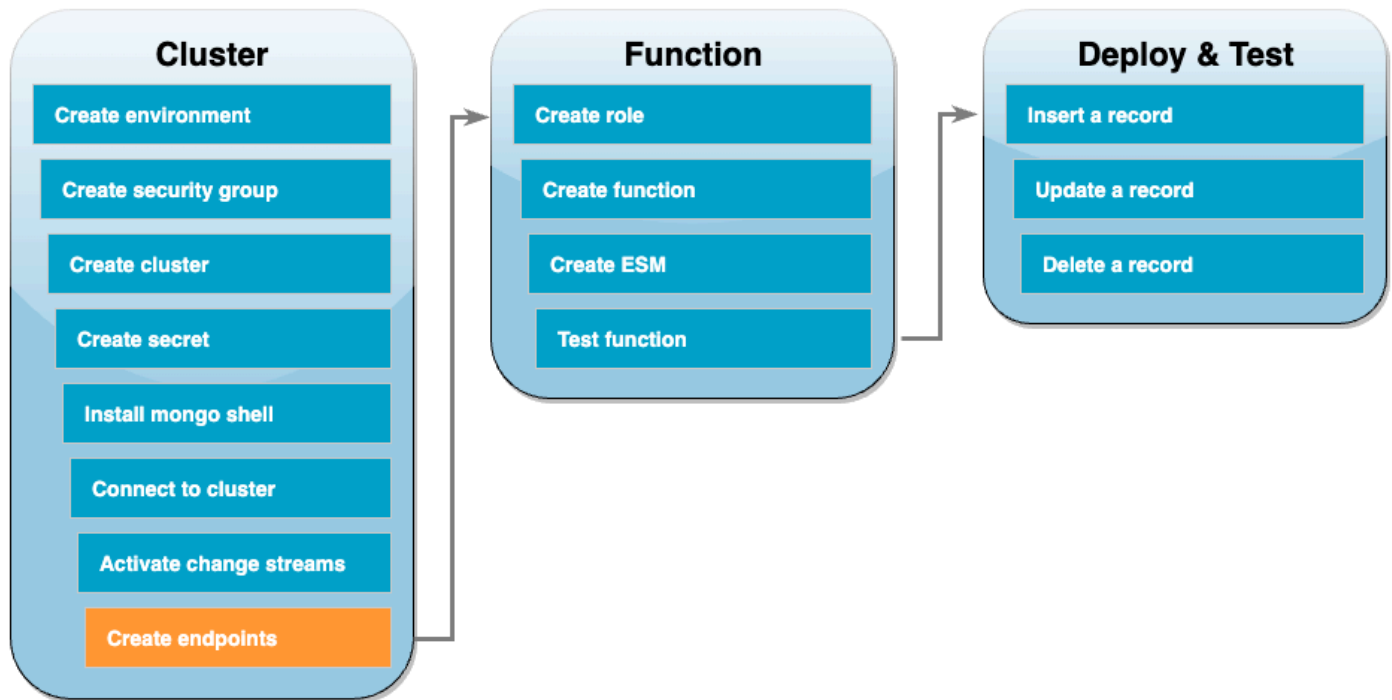
Selanjutnya, aktifkan aliran perubahan pada products koleksi docdbdemo database menggunakan perintah berikut:

```
db.adminCommand({modifyChangeStreams: 1,  
  database: "docdbdemo",  
  collection: "products",  
  enable: true});
```

Anda akan melihat output seperti ini:

```
{ "ok" : 1, "operationTime" : Timestamp(1680126165, 1) }
```

Buat titik VPC akhir antarmuka



Selanjutnya, buat [VPCtitik akhir antarmuka](#) untuk memastikan bahwa Lambda dan Secrets Manager (digunakan nanti untuk menyimpan kredensial akses cluster kami) dapat terhubung ke default Anda. VPC

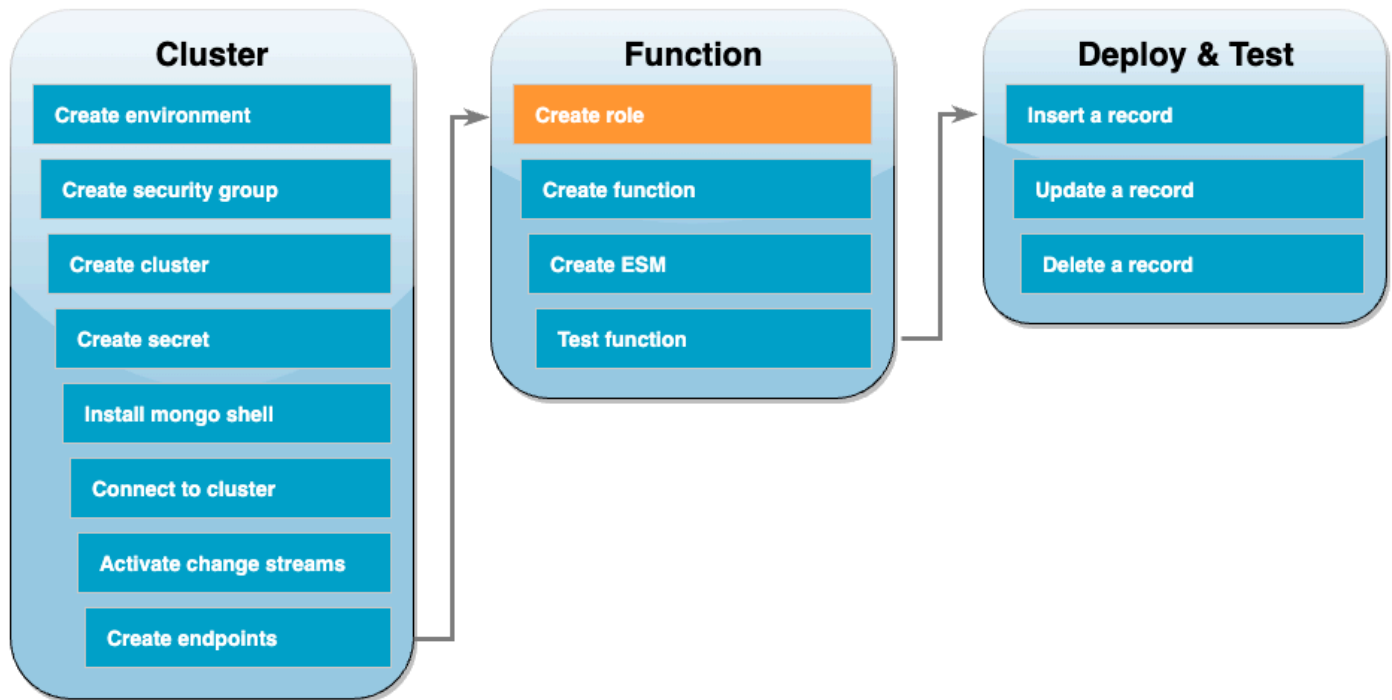
Untuk membuat titik VPC akhir antarmuka

1. Buka [VPCkonsol](#). Di menu sebelah kiri, di bawah Virtual Private Cloud, pilih Endpoints.
2. Pilih Buat Titik Akhir. Buat titik akhir dengan konfigurasi berikut:
 - Untuk tag Nama, masukkan `lambda-default-vpc`.
 - Untuk kategori Layanan, pilih AWS layanan.
 - Untuk Layanan, masukkan `lambda` di kotak pencarian. Pilih layanan dengan format `com.amazonaws.<region>.lambda`.
 - Untuk VPC, pilih [default](#) Anda VPC.
 - Untuk Subnet, centang kotak di sebelah setiap zona ketersediaan. Pilih subnet ID yang benar untuk setiap zona ketersediaan.
 - Untuk jenis alamat IP, pilih IPv4.

- Untuk grup Keamanan, pilih grup VPC keamanan default (Nama grupdefault), dan grup keamanan yang Anda buat sebelumnya (Nama grupDocDBTutorial).
 - Simpan semua pengaturan default lainnya.
 - Pilih Buat Titik Akhir.
3. Sekali lagi, pilih Buat titik akhir. Buat titik akhir dengan konfigurasi berikut:
- Untuk tag Nama, masukkansecretsmanager-default-vpc.
 - Untuk kategori Layanan, pilih AWS layanan.
 - Untuk Layanan, masukkan secretsmanager di kotak pencarian. Pilih layanan dengan formatcom.amazonaws.<region>.secretsmanager.
 - Untuk VPC, pilih [default](#) AndaVPC.
 - Untuk Subnet, centang kotak di sebelah setiap zona ketersediaan. Pilih subnet ID yang benar untuk setiap zona ketersediaan.
 - Untuk jenis alamat IP, pilihIPv4.
 - Untuk grup Keamanan, pilih grup VPC keamanan default (Nama grupdefault), dan grup keamanan yang Anda buat sebelumnya (Nama grupDocDBTutorial).
 - Simpan semua pengaturan default lainnya.
 - Pilih Buat Titik Akhir.

Ini melengkapi bagian pengaturan cluster dari tutorial ini.

Buat peran eksekusi



Pada rangkaian langkah berikutnya, Anda akan membuat fungsi Lambda Anda. Pertama, Anda perlu membuat peran eksekusi yang memberikan izin fungsi Anda untuk mengakses klaster Anda. Anda melakukannya dengan membuat IAM kebijakan terlebih dahulu, lalu melampirkan kebijakan ini ke IAM peran.

Untuk membuat IAM kebijakan

1. Buka [halaman Kebijakan](#) di IAM konsol dan pilih Buat kebijakan.
2. Pilih JSONtab. Dalam kebijakan berikut, ganti sumber daya Secrets Manager ARN di baris terakhir pernyataan dengan rahasia Anda ARN dari sebelumnya, dan salin kebijakan tersebut ke editor.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LambdaESMNetworkingAccess",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",

```

```

        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kms:Decrypt"
    ],
    "Resource": "*"
},
{
    "Sid": "LambdaDocDBESMAccess",
    "Effect": "Allow",
    "Action": [
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBSubnetGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "LambdaDocDBESMGetSecretValueAccess",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocumentDBSecret"
}
]
}

```

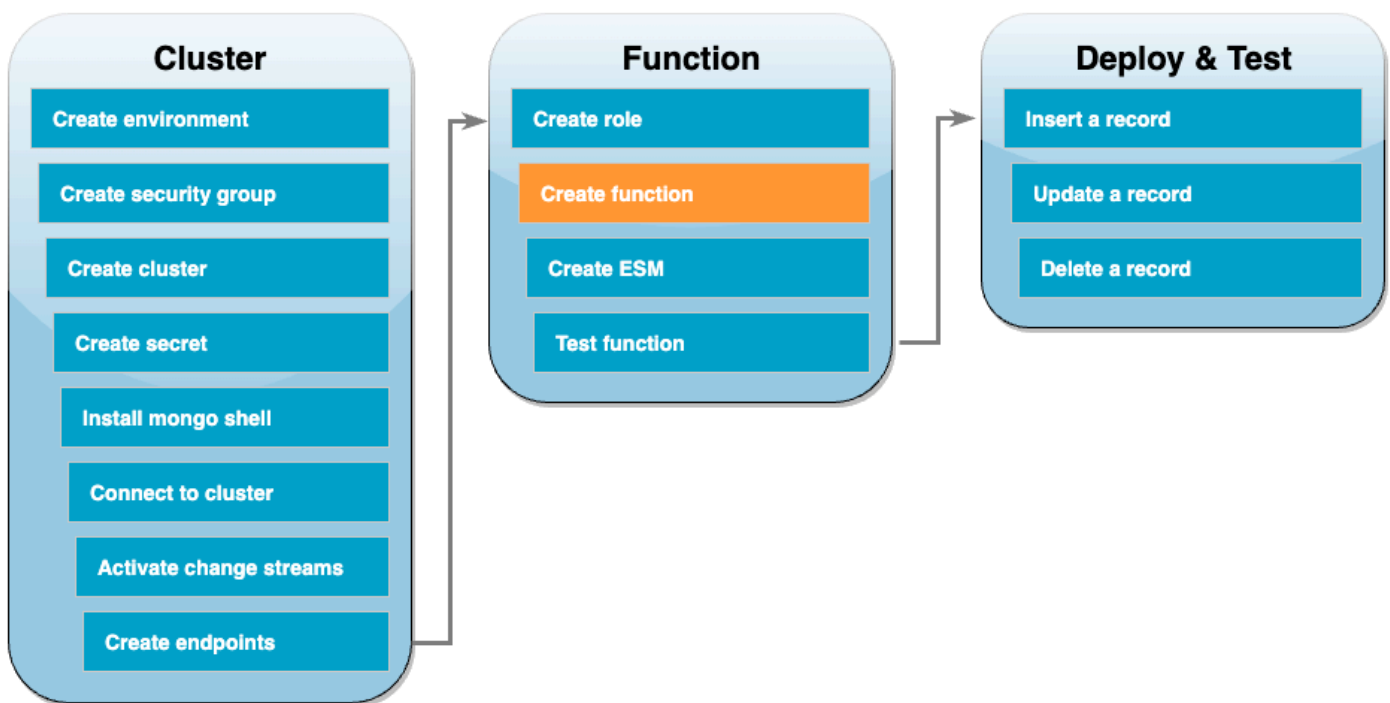
3. Pilih Berikutnya: Tag, lalu pilih Berikutnya: Tinjau.
4. Untuk Nama, masukkan AWSDocumentDBLambdaPolicy.
5. Pilih Buat kebijakan.

Untuk membuat IAM peran

1. Buka [halaman Peran](#) di IAM konsol dan pilih Buat peran.
2. Untuk Pilih entitas tepercaya, pilih opsi berikut:
 - Jenis entitas tepercaya - AWS layanan
 - Kasus penggunaan - Lambda

- Pilih Berikutnya.
3. Untuk Menambahkan izin, pilih `AWSDocumentDBLambdaPolicy` kebijakan yang baru saja Anda buat, serta `AWSLambdaBasicExecutionRole` untuk memberikan izin fungsi Anda untuk menulis ke Amazon CloudWatch Logs.
 4. Pilih Berikutnya.
 5. Untuk Nama peran, masukkan `AWSDocumentDBLambdaExecutionRole`.
 6. Pilih Buat peran.

Buat fungsi Lambda



Kode contoh berikut menerima input peristiwa Amazon DocumentDB dan memproses pesan yang dikandungnya.

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Go.

```
package main

import (
    "context"
    "encoding/json"
    "fmt"

    "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
    Events []Record `json:"events"`
}

type Record struct {
    Event struct {
        OperationType string `json:"operationType"`
        NS             struct {
            DB string `json:"db"`
            Coll string `json:"coll"`
        } `json:"ns"`
        FullDocument interface{} `json:"fullDocument"`
    } `json:"event"`
}

func main() {
    lambda.Start(handler)
}

func handler(ctx context.Context, event Event) (string, error) {
```



```

fmt.Println("Loading function")
for _, record := range event.Events {
    logDocumentDBEvent(record)
}

return "OK", nil
}

func logDocumentDBEvent(record Record) {
    fmt.Printf("Operation type: %s\n", record.Event.OperationType)
    fmt.Printf("db: %s\n", record.Event.NS.DB)
    fmt.Printf("collection: %s\n", record.Event.NS.Coll)
    docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", " ")
    fmt.Printf("Full document: %s\n", string(docBytes))
}

```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan menggunakan Lambda. JavaScript

```

console.log('Loading function');
exports.handler = async (event, context) => {
    event.events.forEach(record => {
        logDocumentDBEvent(record);
    });
    return 'OK';
};

const logDocumentDBEvent = (record) => {
    console.log('Operation type: ' + record.event.operationType);
    console.log('db: ' + record.event.ns.db);
    console.log('collection: ' + record.event.ns.coll);
}

```

```
    console.log('Full document:', JSON.stringify(record.event.fullDocument, null, 2));
  });
};
```

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan TypeScript

```
import { DocumentDBEventRecord, DocumentDBEventSubscriptionContext } from 'aws-lambda';

console.log('Loading function');

export const handler = async (
  event: DocumentDBEventSubscriptionContext,
  context: any
): Promise<string> => {
  event.events.forEach((record: DocumentDBEventRecord) => {
    logDocumentDBEvent(record);
  });
  return 'OK';
};

const logDocumentDBEvent = (record: DocumentDBEventRecord): void => {
  console.log('Operation type: ' + record.event.operationType);
  console.log('db: ' + record.event.ns.db);
  console.log('collection: ' + record.event.ns.coll);
  console.log('Full document:', JSON.stringify(record.event.fullDocument, null, 2));
};
```

PHP

SDKuntuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Amazon DocumentDB dengan menggunakan Lambda. PHP

```
<?php

require __DIR__.'/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Handler;

class DocumentDBEventHandler implements Handler
{
    public function handle($event, Context $context): string
    {
        $events = $event['events'] ?? [];
        foreach ($events as $record) {
            $this->logDocumentDBEvent($record['event']);
        }
        return 'OK';
    }

    private function logDocumentDBEvent($event): void
    {
        // Extract information from the event record

        $operationType = $event['operationType'] ?? 'Unknown';
        $db = $event['ns']['db'] ?? 'Unknown';
        $collection = $event['ns']['coll'] ?? 'Unknown';
        $fullDocument = $event['fullDocument'] ?? [];

        // Log the event details

        echo "Operation type: $operationType\n";
        echo "Database: $db\n";
        echo "Collection: $collection\n";
        echo "Full document: " . json_encode($fullDocument, JSON_PRETTY_PRINT) .
        "\n";
    }
}

return new DocumentDBEventHandler();
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Python.

```
import json

def lambda_handler(event, context):
    for record in event.get('events', []):
        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})

    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
    print("Full document:", json.dumps(full_document, indent=2))
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Ruby.

```
require 'json'

def lambda_handler(event:, context:)
  event['events'].each do |record|
    log_document_db_event(record)
  end
  'OK'
end

def log_document_db_event(record)
  event_data = record['event'] || {}
  operation_type = event_data['operationType'] || 'Unknown'
  db = event_data.dig('ns', 'db') || 'Unknown'
  collection = event_data.dig('ns', 'coll') || 'Unknown'
  full_document = event_data['fullDocument'] || {}

  puts "Operation type: #{operation_type}"
  puts "db: #{db}"
  puts "collection: #{collection}"
  puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::documentdb::{DocumentDbEvent, DocumentDbInnerEvent},
};
```

```
// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
  ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<DocumentDbEvent>) ->Result<(),
  Error> {

    tracing::info!("Event Source ARN: {:?}", event.payload.event_source_arn);
    tracing::info!("Event Source: {:?}", event.payload.event_source);

    let records = &event.payload.events;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_document_db_event(record);
    }

    tracing::info!("Document db records processed");

    // Prepare the response
    Ok(())

}

fn log_document_db_event(record: &DocumentDbInnerEvent)-> Result<(), Error>{
    tracing::info!("Change Event: {:?}", record.event);

    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
```

```
tracing_subscriber::fmt()
.with_max_level(tracing::Level::INFO)
.with_target(false)
.without_time()
.init();

let func = service_fn(function_handler);
lambda_runtime::run(func).await?;
Ok(())
}
```

Untuk membuat fungsi Lambda

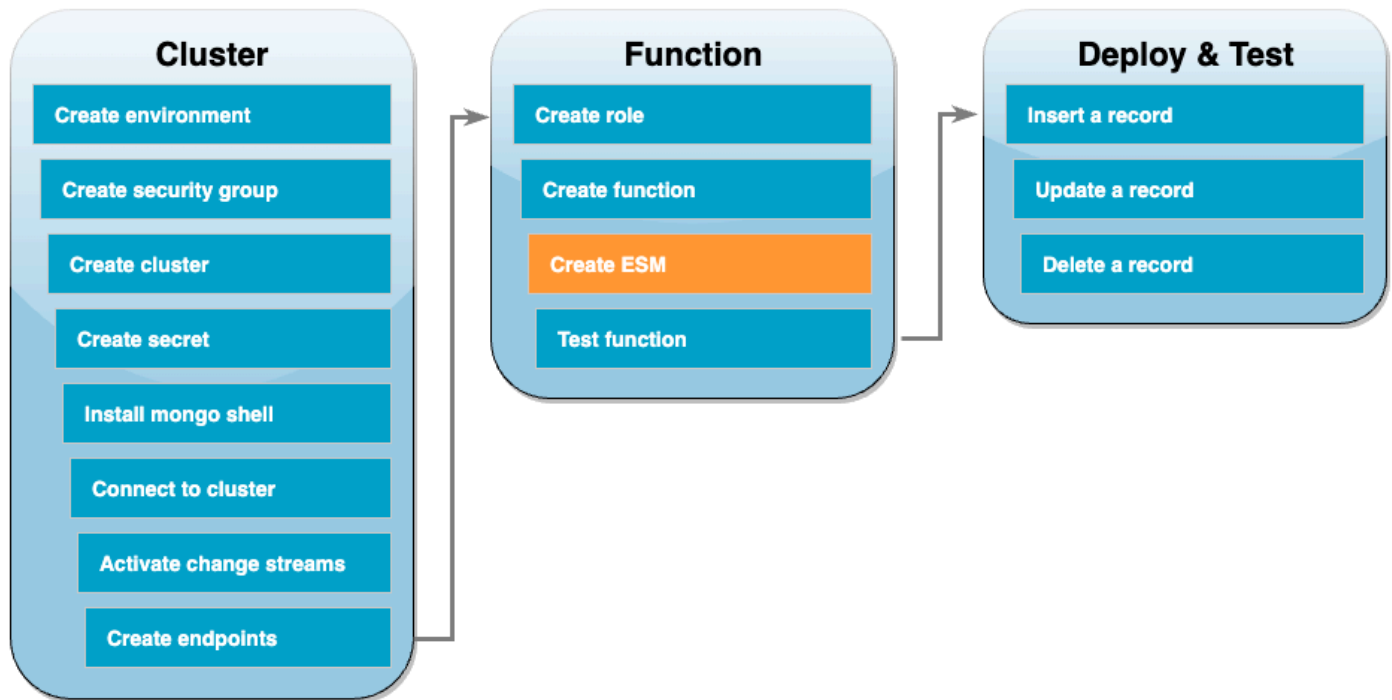
1. Salin kode sampel ke file dengan nama `index.js`.
2. Buat paket penyebaran dengan perintah berikut.

```
zip function.zip index.js
```

3. Gunakan CLI perintah berikut untuk membuat fungsi. Ganti `us-east-1` dengan Wilayah AWS, dan `123456789012` dengan ID akun Anda.

```
aws lambda create-function \
  --function-name ProcessDocumentDBRecords \
  --zip-file fileb://function.zip --handler index.handler --runtime nodejs20.x \
  --region us-east-1 \
  --role arn:aws:iam::123456789012:role/AWSDocumentDBLambdaExecutionRole
```

Buat pemetaan sumber acara Lambda



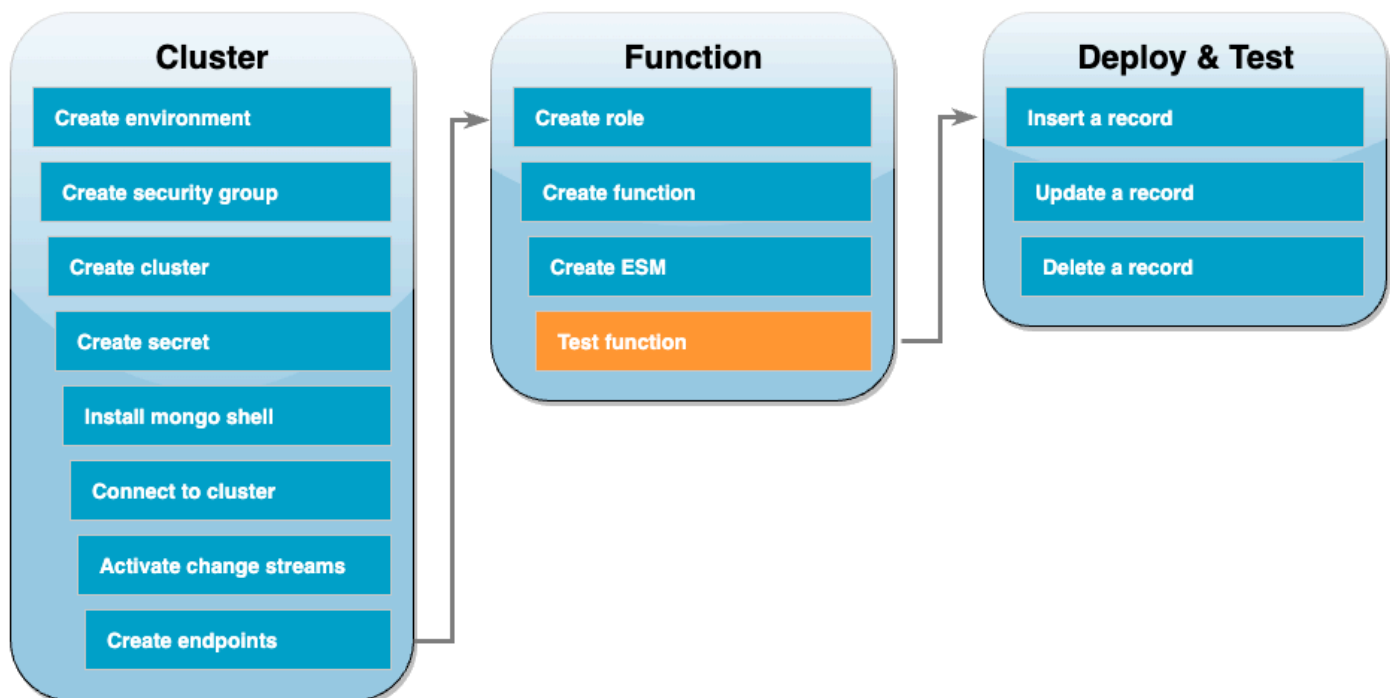
Buat pemetaan sumber peristiwa yang mengaitkan aliran perubahan Amazon DocumentDB Anda dengan fungsi Lambda Anda. Setelah Anda membuat pemetaan sumber acara ini, AWS Lambda segera mulai polling aliran.

Untuk membuat pemetaan sumber acara

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih `ProcessDocumentDBRecords` fungsi yang Anda buat sebelumnya.
3. Pilih tab Konfigurasi, lalu pilih Pemicu di menu sebelah kiri.
4. Pilih Tambahkan pemicu.
5. Di bawah konfigurasi Trigger, untuk sumbernya, pilih Amazon DocumentDB.
6. Buat pemetaan sumber acara dengan konfigurasi berikut:
 - Cluster Amazon DocumentDB — Pilih cluster yang Anda buat sebelumnya.
 - Nama basis data - docdbdemo
 - Nama koleksi - produk
 - Ukuran Batch - 1
 - Posisi awal - Terbaru

- Otentikasi — _ BASIC AUTH
 - Kunci Secrets Manager - Pilih yang baru saja DocumentDBSecret Anda buat.
 - Jendela Batch - 1
 - Konfigurasi dokumen lengkap - UpdateLookup
7. Pilih Tambahkan. Membuat pemetaan sumber acara Anda dapat memakan waktu beberapa menit.

Uji fungsi Anda - pemanggilan manual



Untuk menguji apakah Anda membuat pemetaan fungsi dan sumber peristiwa dengan benar, panggil fungsi Anda menggunakan perintah `invoke` Untuk melakukan ini, pertama-tama salin peristiwa berikut JSON ke dalam file bernama `input.txt`:

```
{
  "eventSourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:canaryclusterb2a659a2-
qo5tcmqkc103",
  "events": [
    {
      "event": {
        "_id": {
          "_data": "0163eeb6e7000000090100000009000041e1"
        }
      }
    }
  ]
}
```

```
    },
    "clusterTime": {
      "$timestamp": {
        "t": 1676588775,
        "i": 9
      }
    },
    "documentKey": {
      "_id": {
        "$oid": "63eeb6e7d418cd98afb1c1d7"
      }
    },
    "fullDocument": {
      "_id": {
        "$oid": "63eeb6e7d418cd98afb1c1d7"
      },
      "anyField": "sampleValue"
    },
    "ns": {
      "db": "docdbdemo",
      "coll": "products"
    },
    "operationType": "insert"
  }
}
],
"eventSource": "aws:docdb"
}
```

Kemudian, gunakan perintah berikut untuk memanggil fungsi Anda dengan acara ini:

```
aws lambda invoke \
  --function-name ProcessDocumentDBRecords \
  --cli-binary-format raw-in-base64-out \
  --region us-east-1 \
  --payload file://input.txt out.txt
```

Anda akan melihat respons yang terlihat seperti berikut:

```
{
  "StatusCode": 200,
  "ExecutedVersion": "$LATEST"
```

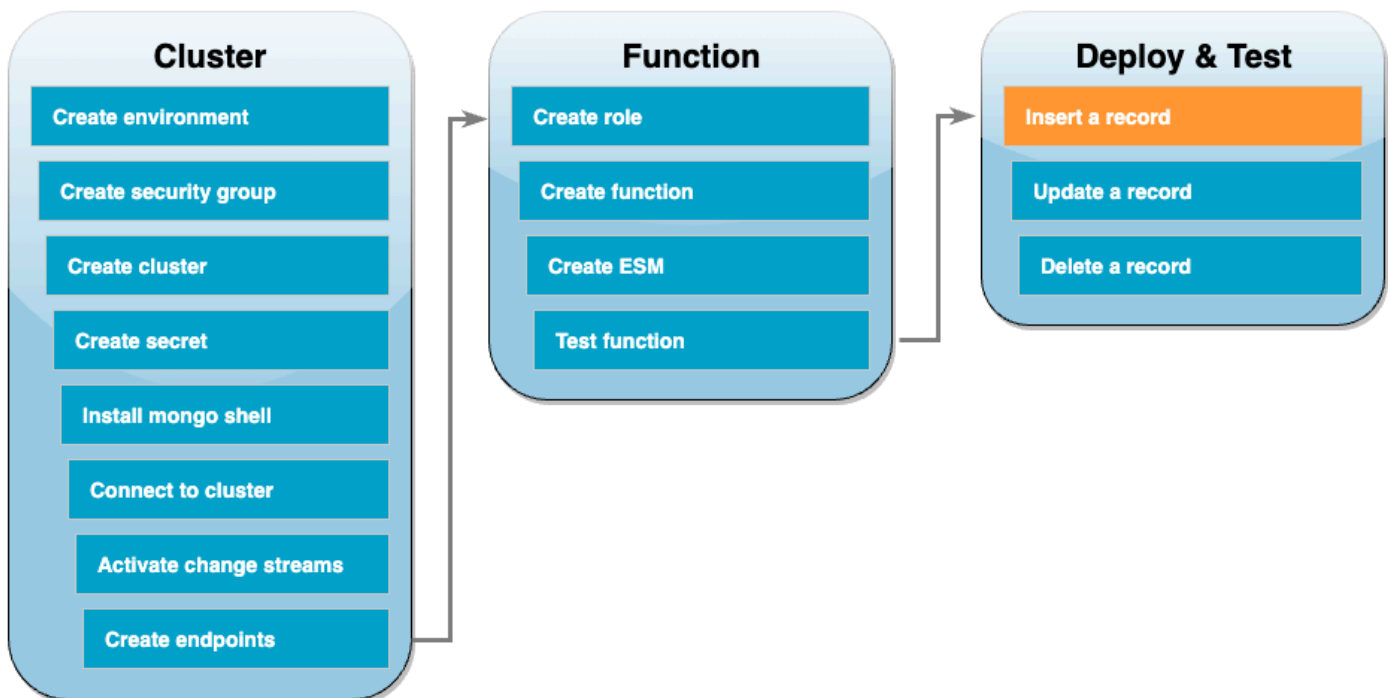
```
}
```

Anda dapat memverifikasi bahwa fungsi Anda berhasil memproses peristiwa dengan memeriksa CloudWatch Log.

Untuk memverifikasi pemanggilan manual melalui Log CloudWatch

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih tab Monitor, lalu pilih Lihat CloudWatch log. Ini akan membawa Anda ke grup log tertentu yang terkait dengan fungsi Anda di CloudWatch konsol.
3. Pilih aliran log terbaru. Dalam pesan log, Anda akan melihat acara tersebutJSON.

Uji fungsi Anda - masukkan catatan



Uji end-to-end penyiapan Anda dengan berinteraksi langsung dengan database Amazon DocumentDB Anda. Pada rangkaian langkah berikutnya, Anda akan memasukkan catatan, memperbaruinya, lalu menghapusnya.

Untuk menyisipkan catatan

1. [Sambungkan kembali ke cluster Amazon DocumentDB di lingkungan Anda.](#) AWS Cloud9

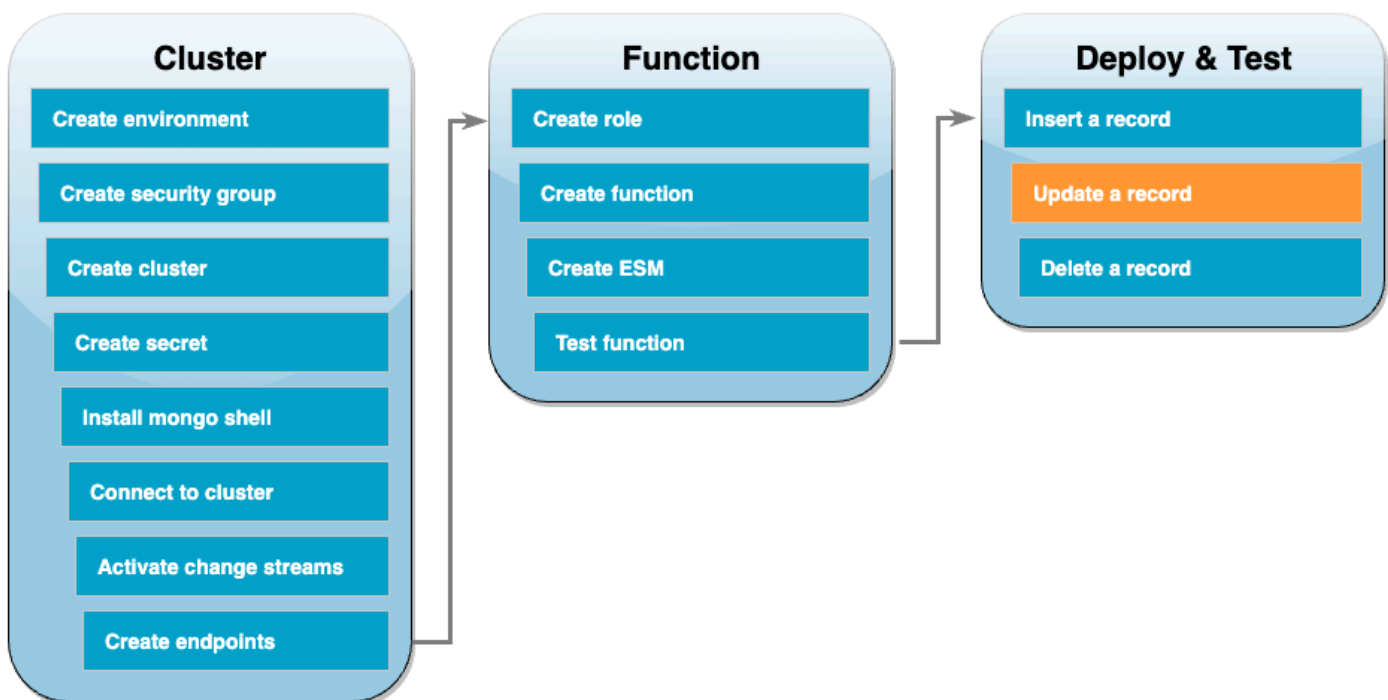
- Gunakan perintah ini untuk memastikan bahwa Anda saat ini menggunakan docdbdemo database:

```
use docdbdemo
```

- Masukkan catatan ke dalam products koleksi docdbdemo database:

```
db.products.insert({"name":"Pencil", "price": 1.00})
```

Uji fungsi Anda - perbarui catatan

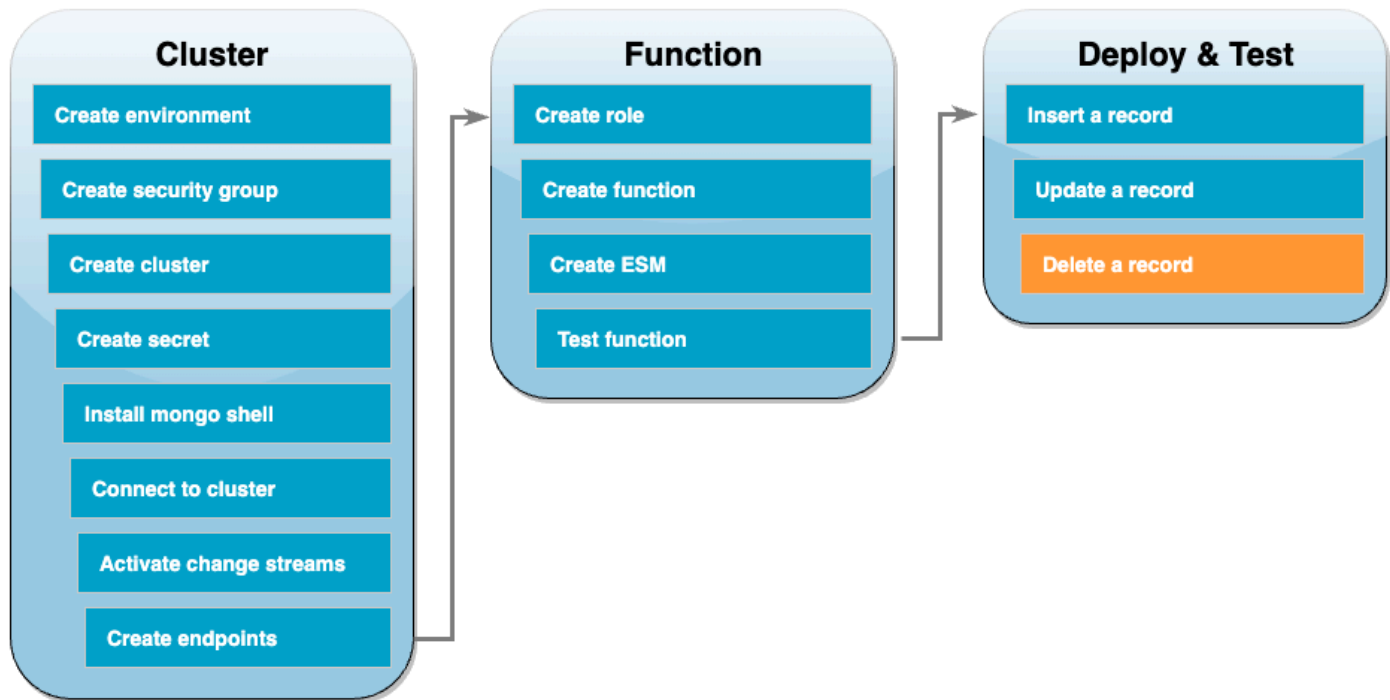


Selanjutnya, perbarui catatan yang baru saja Anda masukkan dengan perintah berikut:

```
db.products.update(  
  { "name": "Pencil" },  
  { $set: { "price": 0.50 } }  
)
```

Verifikasi bahwa fungsi Anda berhasil memproses peristiwa ini dengan memeriksa CloudWatch Log.

Uji fungsi Anda - hapus catatan



Terakhir, hapus catatan yang baru saja Anda perbarui dengan perintah berikut:

```
db.products.remove( { "name": "Pencil" } )
```

Verifikasi bahwa fungsi Anda berhasil memproses peristiwa ini dengan memeriksa CloudWatch Log.

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus sumber daya AWS yang tidak lagi Anda gunakan, Anda mencegah biaya yang tidak perlu untuk Akun AWS Anda.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus titik VPC akhir

1. Buka [VPCkonsol](#). Di menu sebelah kiri, di bawah Virtual Private Cloud, pilih Endpoints.
2. Pilih titik akhir yang Anda buat.
3. Pilih Tindakan, Hapus VPC titik akhir.
4. Masukkan **delete** di bidang input teks.
5. Pilih Hapus.

Untuk menghapus cluster Amazon DocumentDB

1. Buka konsol [Amazon DocumentDB](#).
2. Pilih cluster Amazon DocumentDB yang Anda buat untuk tutorial ini, dan nonaktifkan perlindungan penghapusan.
3. Di halaman utama Clusters, pilih kembali cluster Amazon DocumentDB Anda.
4. Pilih Tindakan, Hapus.
5. Untuk Buat snapshot klaster akhir, pilih No.
6. Masukkan **delete** di bidang input teks.
7. Pilih Hapus.

Untuk menghapus rahasia di Secrets Manager

1. Buka konsol [Secrets Manager](#).
2. Pilih rahasia yang Anda buat untuk tutorial ini.
3. Pilih Tindakan, Hapus rahasia.
4. Pilih Jadwalkan penghapusan.

Untuk menghapus grup EC2 keamanan Amazon

1. Buka [EC2konsol](#). Di bawah Jaringan dan Keamanan, pilih Grup keamanan.
2. Pilih grup keamanan yang Anda buat untuk tutorial ini.
3. Pilih Tindakan, Hapus grup keamanan.
4. Pilih Hapus.

Untuk menghapus AWS Cloud9 lingkungan

1. Buka [konsol AWS Cloud9](#).
2. Pilih lingkungan yang Anda buat untuk tutorial ini.
3. Pilih Hapus.
4. Masukkan **delete** di bidang input teks.
5. Pilih Hapus.

Menggunakan AWS Lambda dengan Amazon DynamoDB

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Anda dapat menggunakan AWS Lambda fungsi untuk memproses catatan dalam aliran [Amazon DynamoDB](#). Dengan DynamoDB Streams, Anda dapat memicu fungsi Lambda untuk melakukan pekerjaan tambahan setiap kali tabel DynamoDB diperbarui.

Topik

- [Polling dan batching stream](#)
- [Posisi awal polling dan streaming](#)
- [Pembaca serpihan secara bersamaan di DynamoDB Streams](#)
- [Contoh peristiwa](#)
- [Memproses catatan DynamoDB dengan Lambda](#)
- [Mengkonfigurasi respons batch sebagian dengan DynamoDB dan Lambda](#)
- [Menyimpan catatan yang dibuang untuk sumber peristiwa DynamoDB di Lambda](#)
- [Pemantauan dengan CloudWatch Log](#)
- [Menerapkan pemrosesan aliran DynamoDB stateful di Lambda](#)
- [Parameter Lambda untuk pemetaan sumber peristiwa Amazon DynamoDB](#)
- [Menggunakan pemfilteran acara dengan sumber acara DynamoDB](#)
- [Tutorial: Menggunakan AWS Lambda dengan aliran Amazon DynamoDB](#)

Polling dan batching stream

Lambda melakukan polling shard dalam aliran DynamoDB untuk catatan dengan tingkat dasar sebanyak 4 kali per detik. Saat rekaman tersedia, Lambda memanggil fungsi Anda dan menunggu hasilnya. Jika pemrosesan berhasil, Lambda melanjutkan polling sampai menerima lebih banyak catatan.

Secara default, Lambda memanggil fungsi Anda segera setelah catatan tersedia. Jika batch yang dibaca Lambda dari sumber peristiwa hanya memiliki satu catatan di dalamnya, Lambda hanya

mengirimkan satu catatan ke fungsi tersebut. Untuk menghindari menjalankan fungsi dengan sejumlah kecil catatan, Anda dapat memberi tahu sumber acara untuk menyangga catatan hingga 5 menit dengan mengonfigurasi jendela batching. Sebelum menjalankan fungsi, Lambda terus membaca catatan dari sumber acara hingga mengumpulkan batch penuh, jendela batching kedaluwarsa, atau batch mencapai batas muatan 6 MB. Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Lambda tidak menunggu [ekstensi](#) yang dikonfigurasi selesai sebelum mengirim batch berikutnya untuk diproses. Dengan kata lain, ekstensi Anda dapat terus berjalan saat Lambda memproses kumpulan catatan berikutnya. Hal ini dapat menyebabkan masalah pembatasan jika Anda melanggar pengaturan atau [batasan konkurensi](#) akun Anda. Untuk mendeteksi apakah ini merupakan masalah potensial, pantau fungsi Anda dan periksa apakah Anda melihat [metrik konkurensi](#) yang lebih tinggi dari yang diharapkan untuk pemetaan sumber peristiwa Anda. Karena waktu yang singkat di antara pemanggilan, Lambda mungkin secara singkat melaporkan penggunaan konkurensi yang lebih tinggi daripada jumlah pecahan. Ini bisa benar bahkan untuk fungsi Lambda tanpa ekstensi.

Konfigurasi [ParallelizationFactor](#) pengaturan untuk memproses satu pecahan aliran DynamoDB dengan lebih dari satu pemanggilan Lambda secara bersamaan. Anda dapat menentukan jumlah batch bersamaan yang polling-nya dibuat Lambda dari shard melalui faktor paralelisasi mulai dari 1 (default) hingga 10. Misalnya, saat Anda menyetel `ParallelizationFactor` ke 2, Anda dapat memiliki maksimum 200 pemanggilan Lambda bersamaan untuk memproses 100 pecahan aliran DynamoDB (meskipun dalam praktiknya, Anda mungkin melihat nilai yang berbeda untuk metrik). `ConcurrentExecutions` Hal ini membantu meningkatkan skala throughput pemrosesan ketika volume data tidak stabil dan `IteratorAge` tinggi. Saat Anda meningkatkan jumlah batch bersamaan per pecahan, Lambda masih memastikan pemrosesan dalam urutan pada level item (partisi dan kunci sortir).

Posisi awal polling dan streaming

Ketahui bahwa polling streaming selama pembuatan dan pembaruan pemetaan sumber acara pada akhirnya konsisten.

- Selama pembuatan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk memulai acara polling dari aliran.
- Selama pembaruan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk menghentikan dan memulai kembali acara pemungutan suara dari aliran.

Perilaku ini berarti bahwa jika Anda menentukan LATEST sebagai posisi awal untuk aliran, pemetaan sumber peristiwa dapat melewati peristiwa selama pembuatan atau pembaruan. Untuk memastikan bahwa tidak ada peristiwa yang terlewatkan, tentukan posisi awal aliran sebagai TRIM_HORIZON.

Pembaca serpihan secara bersamaan di DynamoDB Streams

Untuk tabel Single-region yang bukan tabel global, Anda dapat mendesain hingga dua fungsi Lambda untuk dibaca dari pecahan DynamoDB Streams yang sama secara bersamaan. Melebihi batas ini dapat mengakibatkan throttling permintaan. Untuk tabel global, kami sarankan Anda membatasi jumlah fungsi simultan menjadi satu untuk menghindari pembatasan permintaan.

Contoh peristiwa

Example

```
{
  "Records": [
    {
      "eventID": "1",
      "eventVersion": "1.0",
      "dynamodb": {
        "Keys": {
          "Id": {
            "N": "101"
          }
        }
      },
      "NewImage": {
        "Message": {
          "S": "New item!"
        }
      }
    }
  ]
}
```

```
    },
    "Id": {
      "N": "101"
    }
  },
  "StreamViewType": "NEW_AND_OLD_IMAGES",
  "SequenceNumber": "111",
  "SizeBytes": 26
},
"awsRegion": "us-west-2",
"eventName": "INSERT",
"eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
"eventSource": "aws:dynamodb"
},
{
  "eventID": "2",
  "eventVersion": "1.0",
  "dynamodb": {
    "OldImage": {
      "Message": {
        "S": "New item!"
      },
      "Id": {
        "N": "101"
      }
    },
    "SequenceNumber": "222",
    "Keys": {
      "Id": {
        "N": "101"
      }
    },
    "SizeBytes": 59,
    "NewImage": {
      "Message": {
        "S": "This item has changed"
      },
      "Id": {
        "N": "101"
      }
    },
    "StreamViewType": "NEW_AND_OLD_IMAGES"
  },
}
```

```
    "awsRegion": "us-west-2",
    "eventName": "MODIFY",
    "eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
    "eventSource": "aws:dynamodb"
  }
]}
```

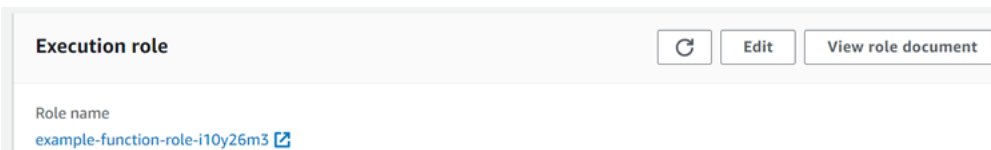
Memproses catatan DynamoDB dengan Lambda

Buat pemetaan sumber kejadian untuk memberi tahu Lambda agar mengirim rekaman dari aliran Anda ke fungsi Lambda. Anda dapat membuat beberapa pemetaan sumber kejadian untuk memproses data yang sama dengan beberapa fungsi Lambda, atau untuk memproses item dari beberapa aliran dengan satu fungsi.

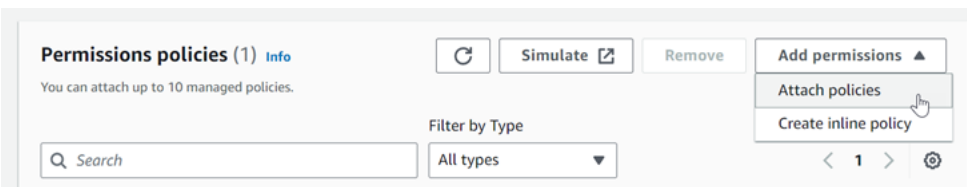
Untuk mengonfigurasi fungsi agar dibaca dari DynamoDB Streams, lampirkan kebijakan terkelola ke peran eksekusi, lalu buat [AWSLambdaDynamoDBExecutionRole](#) AWS pemicu DynamoDB.

Untuk menambahkan izin dan membuat pemicu

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih tab Konfigurasi, lalu pilih Izin.
4. Di bawah Nama peran, pilih tautan ke peran eksekusi Anda. Tautan ini membuka peran di IAM konsol.

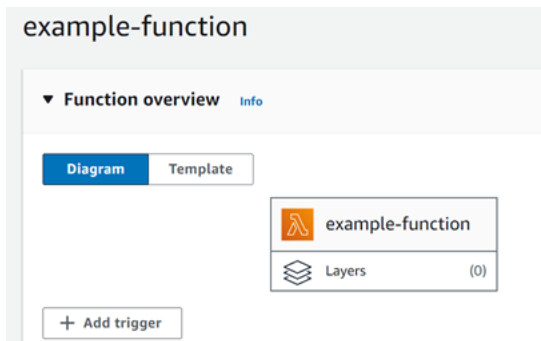


5. Pilih Tambahkan izin, lalu pilih Lampirkan kebijakan.



6. Di bidang pencarian, masukkan `AWSLambdaDynamoDBExecutionRole`. Tambahkan kebijakan ini ke peran eksekusi Anda. Ini adalah kebijakan AWS terkelola yang berisi izin yang perlu dibaca fungsi Anda dari aliran DynamoDB. Untuk informasi selengkapnya tentang kebijakan ini, lihat [AWSLambdaDynamoDBExecutionRole](#) di Referensi Kebijakan AWS Terkelola.

7. Kembali ke fungsi Anda di konsol Lambda. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.



8. Pilih jenis pemicu.
9. Konfigurasi opsi yang diperlukan, lalu pilih Tambah.

Lambda mendukung opsi berikut untuk sumber acara DynamoDB:

Opsi sumber kejadian

- Tabel DynamoDB – Tabel DynamoDB tempat untuk membaca catatan.
- Ukuran batch – Jumlah rekaman yang akan dikirimkan ke fungsi dalam setiap batch, paling banyak 10.000. Lambda meneruskan semua rekaman dalam batch ke fungsi dalam satu panggilan, selama ukuran total kejadian tidak melebihi [batas payload](#) untuk invokasi sinkron (6 MB).
- Jendela batch – Tentukan jumlah waktu maksimum untuk mengumpulkan rekaman sebelum memanggil fungsi, dalam hitungan detik.
- Posisi mulai – Hanya memproses rekaman baru, atau semua rekaman yang ada.
 - Terbaru – Memproses rekaman baru yang ditambahkan ke stream.
 - Trim horizon – Memproses semua rekaman dalam aliran.

Setelah memproses rekaman yang sudah ada, fungsi berhenti dan melanjutkan memproses rekaman baru.

- Tujuan gagal — SQS Antrian standar atau SNS topik standar untuk catatan yang tidak dapat diproses. Ketika Lambda membuang sekumpulan catatan yang terlalu tua atau telah kehabisan semua percobaan ulang, Lambda mengirimkan detail tentang batch ke antrian atau topik.
- Percobaan ulang – Jumlah maksimum percobaan ulang Lambda saat fungsi memunculkan kesalahan. Hal ini tidak berlaku untuk kesalahan layanan atau pembatasan di mana batch tidak mencapai fungsi.
- Maximum age of record – Usia maksimum rekaman yang dikirimkan Lambda ke fungsi Anda.

- Split batch on error – Ketika fungsi mengembalikan kesalahan, bagi batch menjadi dua bagian sebelum mencoba kembali. Pengaturan ukuran batch asli Anda tetap tidak berubah.
- Batch bersamaan per pecahan — Secara bersamaan memproses beberapa batch dari pecahan yang sama.
- Diaktifkan – Atur ke true untuk mengaktifkan pemetaan sumber kejadian. Atur ke false untuk menghentikan pemrosesan rekaman. Lambda mencatat rekaman terakhir yang diproses dan melanjutkan pemrosesan dari titik tersebut saat pemetaan diaktifkan kembali.

Note

Anda tidak dikenakan biaya untuk GetRecords API panggilan yang dipanggil oleh Lambda sebagai bagian dari pemacu DynamoDB.

Untuk mengelola konfigurasi sumber kejadian nanti, pilih pemacu di desainer.

Mengkonfigurasi respons batch sebagian dengan DynamoDB dan Lambda

Ketika menggunakan dan memproses data streaming dari sumber peristiwa, secara default Lambda memeriksa urutan nomor tertinggi batch hanya ketika batch berhasil diselesaikan. Lambda memperlakukan semua hasil lain sebagai sepenuhnya gagal dan mencoba lagi pemrosesan batch hingga batas coba lagi. Untuk memungkinkan keberhasilan parsial saat memproses batch dari aliran, aktifkan `ReportBatchItemFailures`. Mengizinkan keberhasilan parsial dapat membantu mengurangi jumlah percobaan ulang pada catatan, meskipun tidak sepenuhnya mencegah kemungkinan percobaan ulang dalam catatan yang sukses.

Untuk mengaktifkan `ReportBatchItemFailures`, sertakan nilai enum

`ReportBatchItemFailures` dalam [FunctionResponseTypes](#) daftar. Daftar ini menunjukkan tipe respon yang diaktifkan untuk fungsi Anda. Anda dapat mengonfigurasi daftar ini saat [membuat](#) atau [memperbarui](#) pemetaan sumber peristiwa.

Sintaks laporan

Saat mengonfigurasi pelaporan pada kegagalan item batch, kelas `StreamsEventResponse` dikembalikan dengan daftar kegagalan item batch. Anda dapat menggunakan objek `StreamsEventResponse` untuk mengembalikan nomor urutan catatan gagal pertama dalam batch. Anda juga dapat membuat kelas kustom Anda sendiri menggunakan sintaks respons yang benar. JSONStruktur berikut menunjukkan sintaks respons yang diperlukan:

```
{
  "batchItemFailures": [
    {
      "itemIdentifier": "<SequenceNumber>"
    }
  ]
}
```

Note

Jika `batchItemFailures` array berisi beberapa item, Lambda menggunakan catatan dengan nomor urut terendah sebagai pos pemeriksaan. Lambda kemudian mencoba kembali semua catatan mulai dari pos pemeriksaan itu.

Status berhasil dan gagal

Lambda memperlakukan batch sebagai sepenuhnya berhasil jika Anda mengembalikan salah satu dari berikut:

- Daftar `batchItemFailure` kosong
- Daftar `batchItemFailure` nol
- `EventResponse` kosong
- `EventResponse` nol

Lambda memperlakukan batch sebagai sepenuhnya gagal jika Anda mengembalikan salah satu dari berikut:

- String `itemIdentifier` kosong
- `itemIdentifier` nol
- `itemIdentifier` dengan nama kunci yang buruk

Lambda mencoba kembali kegagalan berdasarkan strategi coba lagi Anda.

Membagi batch

Jika invokasi Anda gagal dan `BisectBatchOnFunctionError` diaktifkan, batch dibagi terlepas dari pengaturan `ReportBatchItemFailures` Anda.

Ketika respons berhasil batch parsial diterima dan kedua `BisectBatchOnFunctionError` dan `ReportBatchItemFailures` diaktifkan, batch dibagi dua di nomor urutan yang dikembalikan dan Lambda mencoba hanya catatan yang tersisa.

Berikut adalah beberapa contoh kode fungsi yang mengembalikan daftar pesan gagal IDs dalam batch:

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
        ILambdaContext context)
```



```
{
    context.Logger.LogInformation($"Beginning to process
{dynamoEvent.Records.Count} records...");
    List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
List<StreamsEventResponse.BatchItemFailure>();
    StreamsEventResponse streamsEventResponse = new StreamsEventResponse();


    foreach (var record in dynamoEvent.Records)
    {
        try
        {
            var sequenceNumber = record.Dynamodb.SequenceNumber;
            context.Logger.LogInformation(sequenceNumber);
        }
        catch (Exception ex)
        {
            context.Logger.LogError(ex.Message);
            batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
{ ItemIdentifier = record.Dynamodb.SequenceNumber });
        }
    }

    if (batchItemFailures.Count > 0)
    {
        streamsEventResponse.BatchItemFailures = batchItemFailures;
    }

    context.Logger.LogInformation("Stream processing complete.");
    return streamsEventResponse;
}
}
```

Go

SDKuntuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

type BatchItemFailure struct {
    ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
    BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
(*BatchResult, error) {
    var batchItemFailures []BatchItemFailure
    curRecordSequenceNumber := ""

    for _, record := range event.Records {
        // Process your record
        curRecordSequenceNumber = record.Change.SequenceNumber
    }

    if curRecordSequenceNumber != "" {
        batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
curRecordSequenceNumber})
    }

    batchResult := BatchResult{
        BatchItemFailures: batchItemFailures,
    }

    return &batchResult, nil
}

func main() {
    lambda.Start(HandleRequest)
```

```
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengaturnya dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
    Serializable> {

    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
    context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
    ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
    input.getRecords()) {
            try {
                //Process your record
```

```
        StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
        curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

    } catch (Exception e) {
        /* Since we are working with streams, we can return the failed
        item immediately.
           Lambda will immediately begin to retry processing from this
        failed item onwards. */
        batchItemFailures.add(new
StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
        return new StreamsEventResponse(batchItemFailures);
    }
}

return new StreamsEventResponse();
}
}
```

JavaScript

SDKuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. JavaScript

```
export const handler = async (event) => {
    const records = event.Records;
    let curRecordSequenceNumber = "";

    for (const record of records) {
        try {
            // Process your record
            curRecordSequenceNumber = record.dynamodb.SequenceNumber;
        } catch (e) {
            // Return failed record's sequence number
        }
    }
}
```

```
        return { batchItemFailures: [{ itemIdentifier:
curRecordSequenceNumber }] };
    }
}

return { batchItemFailures: [] };
};
```

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. TypeScript

```
import {
    DynamoDBBatchResponse,
    DynamoDBBatchItemFailure,
    DynamoDBStreamEvent,
} from "aws-lambda";

export const handler = async (
    event: DynamoDBStreamEvent
): Promise<DynamoDBBatchResponse> => {
    const batchItemFailures: DynamoDBBatchItemFailure[] = [];
    let curRecordSequenceNumber;


    for (const record of event.Records) {
        curRecordSequenceNumber = record.dynamodb?.SequenceNumber;

        if (curRecordSequenceNumber) {
            batchItemFailures.push({
                itemIdentifier: curRecordSequenceNumber,
            });
        }
    }

    return { batchItemFailures: batchItemFailures };
};
```

PHP

SDKuntuk PHP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. PHP

```
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $dynamoDbEvent = new DynamoDbEvent($event);
        $this->logger->info("Processing records");

        $records = $dynamoDbEvent->getRecords();
        $failedRecords = [];
        foreach ($records as $record) {
```

```

        try {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data
        } catch (Exception $e) {
            $this->logger->error($e->getMessage());
            // failed processing the record
            $failedRecords[] = $record->getSequenceNumber();
        }
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords records");

    // change format for the response
    $failures = array_map(
        fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
        $failedRecords
    );

    return [
        'batchItemFailures' => $failures
    ];
}

$logger = new StderrLogger();
return new Handler($logger);

```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Ruby.

```
def lambda_handler(event:, context:)
    records = event["Records"]
    cur_record_sequence_number = ""

    records.each do |record|
        begin
            # Process your record
            cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
        rescue StandardError => e
            # Return failed record's sequence number
            return {"batchItemFailures" => [{"itemIdentifier" =>
cur_record_sequence_number}]}
        end
    end
end
```



```

end

{"batchItemFailures" => []}
end

```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Rust.

```

use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;

    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

```

```
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("").to_string(),
            });
            return Ok(response);
        }

        // Process your record here...
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
            immediately.
            Lambda will immediately begin to retry processing from this failed
            item onwards. */
            return Ok(response);
        }
    }

    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
        time.
        .without_time()
        .init();
}
```

```
run(service_fn(function_handler)).await
}
```

Menyimpan catatan yang dibuang untuk sumber peristiwa DynamoDB di Lambda

Penanganan kesalahan untuk pemetaan sumber peristiwa DynamoDB tergantung pada apakah kesalahan terjadi sebelum fungsi dipanggil atau selama pemanggilan fungsi:

- Sebelum pemanggilan: Jika pemetaan sumber peristiwa Lambda tidak dapat menjalankan fungsi karena pembatasan atau masalah lain, fungsi tersebut akan mencoba lagi hingga catatan kedaluwarsa atau melebihi usia maksimum yang dikonfigurasi pada pemetaan sumber peristiwa (). [MaximumRecordAgeInSeconds](#)
- Selama pemanggilan: Jika fungsi dipanggil tetapi menampilkan kesalahan, Lambda mencoba ulang hingga catatan kedaluwarsa, melebihi usia maksimum ([MaximumRecordAgeInSeconds](#)), atau mencapai kuota coba ulang yang dikonfigurasi (). [MaximumRetryAttempts](#) Untuk kesalahan fungsi, Anda juga dapat mengonfigurasi [BisectBatchOnFunctionError](#), yang membagi batch yang gagal menjadi dua batch yang lebih kecil, mengisolasi catatan buruk dan menghindari batas waktu. Memisahkan batch tidak menghabiskan kuota coba lagi.

Jika tindakan penanganan kesalahan gagal, Lambda membuang rekaman dan melanjutkan pemrosesan batch dari aliran. Dengan pengaturan default, ini berarti rekaman yang buruk dapat memblokir pemrosesan pada shard yang terpengaruh hingga selama satu hari. Untuk menghindari hal ini, konfigurasi pemetaan sumber kejadian fungsi Anda dengan jumlah percobaan ulang yang wajar dan usia maksimum rekaman yang sesuai dengan kasus penggunaan Anda.

Mengonfigurasi tujuan untuk pemanggilan yang gagal

Untuk menyimpan catatan pemanggilan pemetaan sumber peristiwa yang gagal, tambahkan tujuan ke pemetaan sumber peristiwa fungsi Anda. Setiap catatan yang dikirim ke tujuan adalah JSON dokumen dengan metadata tentang pemanggilan yang gagal. Anda dapat mengonfigurasi SNS topik Amazon atau SQS antrian Amazon apa pun sebagai tujuan. Peran eksekusi Anda harus memiliki izin untuk tujuan:

- Untuk SQS tujuan: [sqs: SendMessage](#)

- Untuk SNS tujuan: [SNS: Publikasikan](#)

Untuk mengonfigurasi tujuan saat gagal menggunakan konsol, ikuti langkah-langkah berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambahkan tujuan.
4. Untuk Sumber, pilih Pemanggilan pemetaan sumber acara.
5. Untuk pemetaan sumber peristiwa, pilih sumber peristiwa yang dikonfigurasi untuk fungsi ini.
6. Untuk Kondisi, pilih On failure. Untuk pemanggilan pemetaan sumber peristiwa, ini adalah satu-satunya kondisi yang diterima.
7. Untuk tipe Tujuan, pilih tipe tujuan yang Lambda kirimkan catatan pemanggilan.
8. Untuk Tujuan, pilih sumber daya.
9. Pilih Simpan.

Anda juga dapat mengonfigurasi tujuan pada kegagalan menggunakan AWS Command Line Interface (AWS CLI). Misalnya, [create-event-source-mapping](#) perintah berikut menambahkan pemetaan sumber peristiwa dengan tujuan SQS kegagalan ke: MyFunction

```
aws lambda create-event-source-mapping \  
--function-name "MyFunction" \  
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/  
stream/2024-06-10T19:26:16.525 \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-  
east-1:123456789012:dest-queue"}}'
```

[update-event-source-mapping](#) Perintah berikut memperbarui pemetaan sumber peristiwa untuk mengirim catatan pemanggilan yang gagal ke SNS tujuan setelah dua percobaan ulang, atau jika catatan berusia lebih dari satu jam.

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--maximum-retry-attempts 2 \  
--maximum-record-age-in-seconds 3600 \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-  
east-1:123456789012:dest-topic"}}'
```

Pengaturan yang diperbarui diterapkan secara asinkron dan tidak muncul dalam output hingga proses selesai. Gunakan [get-event-source-mapping](#) perintah untuk melihat status saat ini.

Untuk menghapus tujuan, berikan string kosong sebagai argumen ke `destination-config` parameter:

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Contoh berikut menunjukkan catatan invokasi untuk aliran DynamoDB.

Example Rekaman Invokasi

```
{  
  "requestContext": {  
    "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",  
    "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",  
    "condition": "RetryAttemptsExhausted",  
    "approximateInvokeCount": 1  
  },  
  "responseContext": {  
    "statusCode": 200,  
    "executedVersion": "$LATEST",  
    "functionError": "Unhandled"  
  },  
  "version": "1.0",  
  "timestamp": "2019-11-14T00:13:49.717Z",  
  "DDBStreamBatchInfo": {  
    "shardId": "shardId-00000001573689847184-864758bb",  
    "startSequenceNumber": "800000000003126276362",  
    "endSequenceNumber": "800000000003126276362",  
    "approximateArrivalOfFirstRecord": "2019-11-14T00:13:19Z",  
    "approximateArrivalOfLastRecord": "2019-11-14T00:13:19Z",  
    "batchSize": 1,  
    "streamArn": "arn:aws:dynamodb:us-east-2:123456789012:table/mytable/  
stream/2019-11-14T00:04:06.388"  
  }  
}
```

Anda dapat menggunakan informasi ini guna mengambil rekaman yang terpengaruh dari aliran untuk pemecahan masalah. Rekaman aktual tidak disertakan, jadi Anda harus memproses rekaman ini dan mengambilnya dari aliran sebelum kedaluwarsa dan hilang.

Pemantauan dengan CloudWatch Log

Lambda memancarkan metrik `IteratorAge` saat fungsi Anda menyelesaikan pemrosesan suatu batch rekaman. Metrik menunjukkan berapa usia rekaman terakhir dalam batch saat pemrosesan selesai. Jika fungsi Anda memproses kejadian baru, Anda dapat menggunakan usia iterator untuk memperkirakan latensi antara waktu saat rekaman ditambahkan dan saat fungsi memprosesnya.

Tren yang meningkat dalam usia iterator dapat menandakan masalah dengan fungsi Anda. Untuk informasi selengkapnya, lihat [Lihat metrik untuk fungsi Lambda](#).

Menerapkan pemrosesan aliran DynamoDB stateful di Lambda

Fungsi Lambda dapat menjalankan aplikasi pemrosesan aliran berkelanjutan. Aliran merupakan data tidak terbatas yang mengalir terus-menerus melalui aplikasi Anda. Untuk menganalisis informasi dari input yang terus diperbarui ini, Anda dapat mengikat catatan yang disertakan menggunakan jendela yang didefinisikan dalam hal waktu.

Jatuh jendela adalah jendela waktu yang berbeda yang membuka dan menutup secara berkala. Secara default, pemanggilan Lambda tanpa status — Anda tidak dapat menggunakannya untuk memproses data di beberapa pemanggilan berkelanjutan tanpa database eksternal. Namun, dengan jendela yang jatuh, Anda dapat mempertahankan status Anda di seluruh pemanggilan. Status ini berisi hasil agregat pesan yang sebelumnya diproses untuk jendela saat ini. Status Anda maksimal bisa sebesar 1 MB per shard. Jika melebihi ukuran tersebut, Lambda mengakhiri jendela lebih awal.

Setiap rekaman dalam aliran milik jendela tertentu. Lambda akan memproses setiap rekaman setidaknya sekali, tetapi tidak menjamin bahwa setiap rekaman akan diproses hanya sekali. Dalam kasus yang jarang terjadi, seperti penanganan kesalahan, beberapa catatan mungkin diproses lebih dari sekali. Catatan selalu diproses secara berurutan pertama kali. Jika catatan diproses lebih dari satu kali, mereka mungkin diproses rusak.

Agregasi dan pemrosesan

Fungsi yang dikelola pengguna Anda dipanggil baik untuk agregasi maupun untuk memproses hasil akhir agregasi tersebut. Lambda mengumpulkan semua catatan yang diterima di jendela. Anda dapat menerima catatan ini dalam beberapa batch, masing-masing sebagai invokasi terpisah. Setiap invokasi menerima status. Jadi, saat menggunakan jendela tumbling, respons fungsi Lambda Anda

harus berisi state properti. Jika respons tidak berisi state properti, Lambda menganggap ini sebagai pemanggilan yang gagal. Untuk memenuhi kondisi ini, fungsi Anda dapat mengembalikan `TimeWindowEventResponse` objek, yang memiliki JSON bentuk sebagai berikut:

Example Nilai `TimeWindowEventResponse`

```
{
  "state": {
    "1": 282,
    "2": 715
  },
  "batchItemFailures": []
}
```

Note

Untuk fungsi Java, sebaiknya gunakan `Map<String, String>` untuk mewakili status.

Di akhir jendela, tanda `isFinalInvokeForWindow` diatur ke `true` untuk menunjukkan bahwa ini adalah status akhir dan bahwa itu siap untuk diproses. Setelah pemrosesan, jendela selesai, dan invokasi akhir Anda selesai, lalu status dihapus.

Di akhir jendela Anda, Lambda menggunakan pemrosesan akhir untuk tindakan pada hasil agregasi. Pemrosesan akhir Anda dipanggil secara sinkron. Setelah pemanggilan berhasil, fungsi Anda memeriksa nomor urut dan pemrosesan aliran berlanjut. Jika invokasi tidak berhasil, fungsi Lambda Anda menunda pemrosesan lebih lanjut sampai invokasi sukses.

Example `DynamodbTimeWindowEvent`

```
{
  "Records": [
    {
      "eventID": "1",
      "eventName": "INSERT",
      "eventVersion": "1.0",
      "eventSource": "aws:dynamodb",
      "awsRegion": "us-east-1",
      "dynamodb": {
        "Keys": {
```

```
        "Id":{
            "N":"101"
        }
    },
    "NewImage":{
        "Message":{
            "S":"New item!"
        },
        "Id":{
            "N":"101"
        }
    },
    "SequenceNumber":"111",
    "SizeBytes":26,
    "StreamViewType":"NEW_AND_OLD_IMAGES"
},
"eventSourceARN":"stream-ARN"
},
{
    "eventID":"2",
    "eventName":"MODIFY",
    "eventVersion":"1.0",
    "eventSource":"aws:dynamodb",
    "awsRegion":"us-east-1",
    "dynamodb":{
        "Keys":{
            "Id":{
                "N":"101"
            }
        },
        "NewImage":{
            "Message":{
                "S":"This item has changed"
            },
            "Id":{
                "N":"101"
            }
        },
        "OldImage":{
            "Message":{
                "S":"New item!"
            },
            "Id":{
                "N":"101"
            }
        }
    }
}
```



```
    }
  },
  "SequenceNumber": "222",
  "SizeBytes": 59,
  "StreamViewType": "NEW_AND_OLD_IMAGES"
},
"eventSourceARN": "stream-ARN"
},
{
  "eventID": "3",
  "eventName": "REMOVE",
  "eventVersion": "1.0",
  "eventSource": "aws:dynamodb",
  "awsRegion": "us-east-1",
  "dynamodb": {
    "Keys": {
      "Id": {
        "N": "101"
      }
    },
    "OldImage": {
      "Message": {
        "S": "This item has changed"
      },
      "Id": {
        "N": "101"
      }
    },
    "SequenceNumber": "333",
    "SizeBytes": 38,
    "StreamViewType": "NEW_AND_OLD_IMAGES"
  },
  "eventSourceARN": "stream-ARN"
}
],
"window": {
  "start": "2020-07-30T17:00:00Z",
  "end": "2020-07-30T17:05:00Z"
},
"state": {
  "1": "state1"
},
"shardId": "shard123456789",
"eventSourceARN": "stream-ARN",
```

```
"isFinalInvokeForWindow": false,
"isWindowTerminatedEarly": false
}
```

Konfigurasi

Anda dapat mengonfigurasi jendela berguling saat membuat atau memperbarui pemetaan sumber peristiwa. Untuk mengkonfigurasi jendela tumbling, tentukan jendela dalam hitungan detik ([TumblingWindowInSeconds](#)). Contoh berikut AWS Command Line Interface (AWS CLI) perintah membuat pemetaan sumber acara streaming yang memiliki jendela jatuh 120 detik. Fungsi Lambda yang didefinisikan untuk agregasi dan pemrosesan diberi nama `tumbling-window-example-function`.

```
aws lambda create-event-source-mapping \
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525 \
--function-name tumbling-window-example-function \
--starting-position TRIM_HORIZON \
--tumbling-window-in-seconds 120
```

Lambda menentukan jatuh batas jendela berguling berdasarkan waktu ketika catatan dimasukkan ke dalam aliran. Semua catatan memiliki stempel waktu perkiraan yang tersedia yang digunakan Lambda dalam penentuan batas.

Agregasi jendela berguling tidak mendukung shard ulang. Ketika shard berakhir, Lambda menganggap jendela ditutup, dan shard anak memulai jendela mereka sendiri dalam status baru.

Jendela berguling sepenuhnya mendukung kebijakan coba lagi yang ada `maxRetryAttempts` dan `maxRecordAge`.

Example Handler.py - Agregasi dan pemrosesan

Fungsi Python berikut menunjukkan cara untuk menggabungkan, lalu memproses status akhir Anda:

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

    #Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
```

```

    print('Destination invoke')
else:
    print('Aggregate invoke')

#Check for early terminations
if event['isWindowTerminatedEarly']:
    print('Window terminated early')

#Aggregation logic
state = event['state']
for record in event['Records']:
    state[record['dynamodb']['NewImage']['Id']] = state.get(record['dynamodb']
['NewImage']['Id'], 0) + 1

print('Returning state: ', state)
return {'state': state}

```

Parameter Lambda untuk pemetaan sumber peristiwa Amazon DynamoDB

Semua jenis sumber acara Lambda berbagi hal yang sama [CreateEventSourceMapping](#) dan [UpdateEventSourceMapping](#) API operasi. Namun, hanya beberapa parameter yang berlaku untuk DynamoDB Streams.

| Parameter | Diperlukan | Default | Catatan |
|----------------------------|------------|---------|--|
| BatchSize | T | 100 | Maksimum: 10.000. |
| BisectBatchOnFunctionError | T | false | none |
| DestinationConfig | T | N/A | SQS Antrian Amazon standar atau tujuan SNS topik Amazon standar untuk catatan yang dibuang |
| Diaktifkan | T | true | none |
| EventSourceArn | T | N/A | ARN dari aliran data atau konsumen aliran |

| Parameter | Diperlukan | Default | Catatan |
|--------------------------------|------------|---------|---|
| FilterCriteria | T | N/A | Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda |
| FunctionName | T | N/A | none |
| FunctionResponseType | T | N/A | Agar fungsi Anda melaporkan kegagalan tertentu dalam satu batch, sertakan nilainya <code>ReportBatchItemFailures</code> <code>FunctionResponseType</code> . Untuk informasi selengkapnya, lihat Mengkonfigurasi respons batch sebagian dengan DynamoDB dan Lambda . |
| MaximumBatchingWindowInSeconds | T | 0 | none |

| Parameter | Diperlukan | Default | Catatan |
|---------------------------|------------|---------|---|
| MaximumRecordAgeInSeconds | T | -1 | -1 berarti tak terbatas: catatan gagal dicoba lagi sampai catatan berakhir. Batas retensi data untuk DynamoDB Streams adalah 24 jam . Minimal: -1 Maksimal: 604.800 |
| MaximumRetryAttempts | T | -1 | -1 berarti tak terbatas: catatan gagal dicoba ulang sampai catatan kedaluwarsa Minimal: 0 Maksimum: 10.000. |
| ParallelizationFactor | T | 1 | Maksimal: 10 |
| StartingPosition | T | N/A | TRIM_HORIZON atau LATEST |
| TumblingWindowInSeconds | T | N/A | Minimal: 0 Maksimal: 900 |

Menggunakan pemfilteran acara dengan sumber acara DynamoDB

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called “Penyaringan acara”](#).

Bagian ini berfokus pada penyaringan acara untuk sumber acara DynamoDB.

Topik

- [Acara DynamoDB](#)
- [Pemfilteran dengan atribut tabel](#)
- [Memfilter dengan ekspresi Boolean](#)
- [Menggunakan operator Exists](#)
- [JSONformat untuk pemfilteran DynamoDB](#)

Acara DynamoDB

Misalkan Anda memiliki tabel DynamoDB dengan CustomerName kunci utama dan atribut dan. AccountManager PaymentTerms Berikut ini menunjukkan contoh catatan dari aliran tabel DynamoDB Anda.

```
{
  "eventID": "1",
  "eventVersion": "1.0",
  "dynamodb": {
    "ApproximateCreationDateTime": "1678831218.0",
    "Keys": {
      "CustomerName": {
        "S": "AnyCompany Industries"
      },
      "NewImage": {
        "AccountManager": {
          "S": "Pat Candella"
        },
        "PaymentTerms": {
          "S": "60 days"
        },
        "CustomerName": {
          "S": "AnyCompany Industries"
        }
      },
      "SequenceNumber": "111",
      "SizeBytes": 26,
      "StreamViewType": "NEW_IMAGE"
    }
  }
}
```

Untuk memfilter berdasarkan nilai kunci dan atribut dalam tabel DynamoDB Anda, gunakan kunci dynamodb dalam catatan. Bagian berikut memberikan contoh untuk berbagai jenis filter.

Pemfilteran dengan tombol tabel

Misalkan Anda ingin fungsi Anda memproses hanya catatan-catatan di mana kunci utamanya CustomerName adalah "AnyCompany Industri." FilterCriteriaObjeknya adalah sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"dynamodb\" : { \"Keys\" : { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```
{
  "dynamodb": {
    "Keys": {
      "CustomerName": {
        "S": [ "AnyCompany Industries" ]
      }
    }
  }
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany Industries" ] } } } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" : { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"]}]'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" : { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"]}]'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany Industries" ] } } } }'
```

Pemfilteran dengan atribut tabel

Dengan DynamoDB, Anda juga dapat menggunakan `NewImage` tombol `OldImage` and untuk memfilter nilai atribut. Misalkan Anda ingin memfilter catatan di mana `AccountManager` atribut dalam gambar tabel terbaru adalah “Pat Candella” atau “Shirley Rodriguez.” `FilterCriteria`Objeknya adalah sebagai berikut.

```
{
  "Filters": [
    {
```



```

    "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S
\" : [ \"Pat Candella\", \"Shirley Rodriguez\" ] } } } }"
  }
]
}

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```

{
  "dynamodb": {
    "NewImage": {
      "AccountManager": {
        "S": [ "Pat Candella", "Shirley Rodriguez" ]
      }
    }
  }
}

```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```

{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella",
"Shirley Rodriguez" ] } } } }

```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```

aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez
\" ] } } } }"]}]}'

```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez\" ] } } } }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella", "Shirley Rodriguez" ] } } } }'
```

Memfilter dengan ekspresi Boolean

Anda juga dapat membuat filter menggunakan AND ekspresi Boolean. Ekspresi ini dapat mencakup parameter kunci dan atribut tabel Anda. Misalkan Anda ingin memfilter catatan di mana NewImage nilainya AccountManager adalah “Pat Candella” dan OldImage nilainya adalah “Terry Whitlock”. FilterCriteriaObjeknya adalah sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" : { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```
{
  "dynamodb" : {
    "NewImage" : {
      "AccountManager" : {
        "S" : [
```

```

        "Pat Candella"
      ]
    }
  },
  "dynamodb": {
    "OldImage": {
      "AccountManager": {
        "S": [
          "Terry Whitlock"
        ]
      }
    }
  }
}

```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" : [ "Terry Whitlock" ] } } } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" : { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }"}']
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" : { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } } ]}]'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" : [ "Terry Whitlock" ] } } } }'
```

Note

DynamoDB event filtering tidak mendukung penggunaan operator numerik (sama numerik dan rentang numerik). Bahkan jika item dalam tabel Anda disimpan sebagai angka, parameter ini dikonversi ke string dalam objek JSON rekaman.

Menggunakan operator Exists

Karena cara objek JSON peristiwa dari DynamoDB terstruktur, menggunakan operator Exists memerlukan perhatian khusus. Operator Exists hanya bekerja pada node daun dalam acara tersebut JSON, jadi jika pola filter Anda menggunakan Exists untuk menguji node perantara, itu tidak akan berfungsi. Pertimbangkan item tabel DynamoDB berikut:

```
{
  "UserID": {"S": "12345"},
  "Name": {"S": "John Doe"},
  "Organizations": {"L": [
    {"S": "Sales"},
    {"S": "Marketing"},
    {"S": "Support"}
  ]}
}
```

```

    ]
  }
}

```

Anda mungkin ingin membuat pola filter seperti berikut ini yang akan menguji peristiwa yang berisi "Organizations":

```
{ "dynamodb" : { "NewImage" : { "Organizations" : [ { "exists": true } ] } } }
```

Namun, pola filter ini tidak akan pernah mengembalikan kecocokan karena "Organizations" bukan simpul daun. Contoh berikut menunjukkan bagaimana benar menggunakan operator Exists untuk membangun pola filter yang diinginkan:

```
{ "dynamodb" : { "NewImage" : { "Organizations": { "L": { "S": [ { "exists": true } ] } } } } }
```

JSONformat untuk pemfilteran DynamoDB

Untuk memfilter peristiwa dengan benar dari sumber DynamoDB, bidang data dan kriteria filter Anda untuk bidang data dynamodb () harus dalam format yang valid. JSON Jika salah satu bidang tidak dalam JSON format yang valid, Lambda akan menghapus pesan atau melempar pengecualian. Tabel berikut merangkum perilaku spesifik:

| Format data masuk | Format pola filter untuk properti data | Tindakan yang dihasilkan |
|-------------------|---|--|
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Bukan JSON | Lambda melempar pengecualian pada saat pembuatan atau pembaruan pemetaan sumber acara. Pola filter untuk |

| Format data masuk | Format pola filter untuk properti data | Tindakan yang dihasilkan |
|-------------------|---|--|
| | | properti data harus dalam JSON format yang valid. |
| Bukan JSON | Valid JSON | Lambda menjatuhkan rekor. |
| Bukan JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Bukan JSON | Bukan JSON | Lambda melempar pengecualian pada saat pembuatan atau pembaruan pemetaan sumber acara. Pola filter untuk properti data harus dalam JSON format yang valid. |

Tutorial: Menggunakan AWS Lambda dengan aliran Amazon DynamoDB

Dalam tutorial ini, Anda membuat fungsi Lambda untuk menggunakan kejadian dari aliran Amazon DynamoDB.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```

Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (\) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa CLI perintah Bash yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh CLI perintah dalam panduan ini menggunakan pemformatan Linux. Perintah yang menyertakan JSON dokumen inline harus diformat ulang jika Anda menggunakan Windows CLI

Buat peran eksekusi

Buat [peran eksekusi](#) yang memberikan izin fungsi Anda untuk mengakses AWS sumber daya.

Untuk membuat peran eksekusi

1. Buka [halaman peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.
 - Entitas tepercaya – Lambda.
 - Izin — AWSLambdaDynamoDBExecutionRole.
 - Nama peran – **lambda-dynamodb-role**.

Ini AWSLambdaDynamoDBExecutionRolememiliki izin bahwa fungsi perlu membaca item dari DynamoDB dan menulis log ke Log. CloudWatch

Buat fungsi

Buat fungsi Lambda yang memproses peristiwa DynamoDB Anda. Kode fungsi menulis beberapa data peristiwa yang masuk ke CloudWatch Log.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly: LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext context)
    {
        context.Logger.LogInformation($"Beginning to process {dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }


        context.Logger.LogInformation("Stream processing complete.");
    }
}
```



```
}  
}
```

Go

SDKuntuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
package main  
  
import (  
    "context"  
    "github.com/aws/aws-lambda-go/lambda"  
    "github.com/aws/aws-lambda-go/events"  
    "fmt"  
)  
  
func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,  
error) {  
    if len(event.Records) == 0 {  
        return nil, fmt.Errorf("received empty event")  
    }  
  
    for _, record := range event.Records {  
        LogDynamoDBRecord(record)  
    }  
  
    message := fmt.Sprintf("Records processed: %d", len(event.Records))  
    return &message, nil  
}  
  
func main() {
```

```
lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
    fmt.Println(record.EventID)
    fmt.Println(record.EventName)
    fmt.Printf("%+v\n", record.Change)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
    com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
        GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
```

```

        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
    GSON.toJson(record.getDynamodb()));
    }
}

```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan JavaScript

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};

```

Mengonsumsi acara DynamoDB dengan Lambda menggunakan TypeScript

```

export const handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

```

```
});  
}  
const logDynamoDBRecord = (record) => {  
  console.log(record.eventID);  
  console.log(record.eventName);  
  console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);  
};
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan PHP

```
<?php  
  
# using bref/bref and bref/logger for simplicity  
  
use Bref\Context\Context;  
use Bref\Event\DynamoDb\DynamoDbEvent;  
use Bref\Event\DynamoDb\DynamoDbHandler;  
use Bref\Logger\StderrLogger;  
  
require __DIR__ . '/vendor/autoload.php';  
  
class Handler extends DynamoDbHandler  
{  
  private StderrLogger $logger;  
  
  public function __construct(StderrLogger $logger)  
  {  
    $this->logger = $logger;  
  }  
  
  /**  
   * @throws JsonException
```

```
* @throws \Bref\Event\InvalidLambdaEvent
*/
public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
{
    $this->logger->info("Processing DynamoDb table items");
    $records = $event->getRecords();

    foreach ($records as $record) {
        $eventName = $record->getEventName();
        $keys = $record->getKeys();
        $old = $record->getOldImage();
        $new = $record->getNewImage();

        $this->logger->info("Event Name:". $eventName. "\n");
        $this->logger->info("Keys:". json_encode($keys). "\n");
        $this->logger->info("Old Image:". json_encode($old). "\n");
        $this->logger->info("New Image:". json_encode($new));

        // TODO: Do interesting work based on the new data

        // Any exception thrown will be logged and the invocation will be
        marked as failed
    }

    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords items");
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Python.

```
import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Ruby.

```
def lambda_handler(event:, context:)
  return 'received empty event' if event['Records'].empty?

  event['Records'].each do |record|
    log_dynamodb_record(record)
  end

  "Records processed: #{event['Records'].length}"
end

def log_dynamodb_record(record)
```

```
puts record['eventID']
puts record['eventName']
puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
};

// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features = ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }
}
```

```
    for record in records{
        log_dynamo_dbrecord(record);
    }

    tracing::info!("Dynamo db records processed");

    // Prepare the response
    Ok(())
}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())
}
```

Untuk membuat fungsi

1. Salin kode sampel ke file dengan nama `example.js`.
2. Buat paket deployment.

```
zip function.zip example.js
```


3. Buat fungsi Lambda dengan perintah create-function.

```
aws lambda create-function --function-name ProcessDynamoDBRecords \  
  --zip-file fileb://function.zip --handler example.handler --runtime nodejs18.x \  
 \  
  --role arn:aws:iam::111122223333:role/lambda-dynamodb-role
```

Tes fungsi Lambda

Pada langkah ini, Anda menjalankan fungsi Lambda Anda secara manual menggunakan invoke AWS Lambda CLI perintah dan contoh peristiwa DynamoDB berikut. Salin berikut ini ke dalam file bernama `input.txt`.

Example input.txt

```
{  
  "Records": [  
    {  
      "eventID": "1",  
      "eventName": "INSERT",  
      "eventVersion": "1.0",  
      "eventSource": "aws:dynamodb",  
      "awsRegion": "us-east-1",  
      "dynamodb": {  
        "Keys": {  
          "Id": {  
            "N": "101"  
          }  
        },  
        "NewImage": {  
          "Message": {  
            "S": "New item!"  
          },  
          "Id": {  
            "N": "101"  
          }  
        },  
        "SequenceNumber": "111",  
        "SizeBytes": 26,  
        "StreamViewType": "NEW_AND_OLD_IMAGES"  
      },  
      "eventSourceARN": "stream-ARN"  
    }  
  ]  
}
```

```
},
{
  "eventID":"2",
  "eventName":"MODIFY",
  "eventVersion":"1.0",
  "eventSource":"aws:dynamodb",
  "awsRegion":"us-east-1",
  "dynamodb":{
    "Keys":{
      "Id":{
        "N":"101"
      }
    },
    "NewImage":{
      "Message":{
        "S":"This item has changed"
      },
      "Id":{
        "N":"101"
      }
    },
    "OldImage":{
      "Message":{
        "S":"New item!"
      },
      "Id":{
        "N":"101"
      }
    },
    "SequenceNumber":"222",
    "SizeBytes":59,
    "StreamViewType":"NEW_AND_OLD_IMAGES"
  },
  "eventSourceARN":"stream-ARN"
},
{
  "eventID":"3",
  "eventName":"REMOVE",
  "eventVersion":"1.0",
  "eventSource":"aws:dynamodb",
  "awsRegion":"us-east-1",
  "dynamodb":{
    "Keys":{
      "Id":{
```

```

        "N":"101"
      }
    },
    "OldImage":{
      "Message":{
        "S":"This item has changed"
      },
      "Id":{
        "N":"101"
      }
    },
    "SequenceNumber":"333",
    "SizeBytes":38,
    "StreamViewType":"NEW_AND_OLD_IMAGES"
  },
  "eventSourceARN":"stream-ARN"
}
]
}

```

Jalankan perintah `invoke` berikut.

```

aws lambda invoke --function-name ProcessDynamoDBRecords \
  --cli-binary-format raw-in-base64-out \
  --payload file://input.txt outputfile.txt

```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Fungsi mengembalikan message string dalam badan respons.

Verifikasikan output dalam `outputfile.txt` file.

Buat tabel DynamoDB dengan aliran yang diaktifkan

Buat tabel Amazon DynamoDB dengan aliran yang diaktifkan.

Untuk membuat tabel DynamoDB

1. Buka [Konsol DynamoDB](#).

2. Pilih Buat tabel.
3. Buat tabel dengan pengaturan berikut.
 - Nama tabel – **lambda-dynamodb-stream**
 - Kunci utama – **id** (string)
4. Pilih Buat.

Untuk mengaktifkan stream

1. Buka [Konsol DynamoDB](#).
2. Pilih Tables.
3. Pilih tabel lambda-dynamodb-stream.
4. Di bawah Ekspor dan aliran, pilih detail aliran DynamoDB.
5. Pilih Nyalakan.
6. Untuk tipe Tampilan, pilih Atribut kunci saja.
7. Pilih Aktifkan aliran.

Tuliskan alirannyaARN. Anda memerlukan ini di langkah berikutnya ketika Anda mengaitkan aliran dengan fungsi Lambda Anda. Untuk informasi selengkapnya tentang mengaktifkan aliran, lihat [Menangkap aktivitas tabel dengan DynamoDB Streams](#).

Tambahkan sumber acara di AWS Lambda

Buat pemetaan sumber peristiwa di AWS Lambda. Pemetaan sumber peristiwa ini mengaitkan aliran DynamoDB dengan fungsi Lambda Anda. Setelah Anda membuat pemetaan sumber acara ini, AWS Lambda mulailah polling aliran.

Jalankan perintah AWS CLI `create-event-source-mapping` berikut. Setelah perintah berjalan, catatUUID. Anda akan memerlukan ini UUID untuk merujuk ke pemetaan sumber peristiwa dalam perintah apa pun, misalnya, saat menghapus pemetaan sumber peristiwa.

```
aws lambda create-event-source-mapping --function-name ProcessDynamoDBRecords \  
--batch-size 100 --starting-position LATEST --event-source DynamoDB-stream-arn
```

Ini membuat pemetaan di antara aliran DynamoDB yang ditentukan dan fungsi Lambda. Anda dapat mengaitkan aliran DynamoDB dengan beberapa fungsi Lambda, dan mengaitkan fungsi

Lambda yang sama dengan beberapa aliran. Namun, fungsi Lambda akan membagikan throughput pembacaan untuk aliran yang mereka bagikan.

Anda bisa mendapatkan daftar pemetaan sumber kejadian dengan menjalankan perintah berikut.

```
aws lambda list-event-source-mappings
```

Daftar tersebut mengembalikan semua pemetaan sumber kejadian yang Anda buat, dan antara lain menampilkan `LastProcessingResult` untuk setiap pemetaan. Bidang ini digunakan untuk memberikan pesan informatif jika terjadi masalah. Nilai seperti `No records processed` (menunjukkan bahwa AWS Lambda belum memulai polling atau bahwa tidak ada catatan dalam aliran) dan `OK` (menunjukkan AWS Lambda berhasil membaca catatan dari aliran dan memanggil fungsi Lambda Anda) menunjukkan bahwa tidak ada masalah. Jika ada masalah, Anda akan menerima pesan kesalahan.

Jika Anda memiliki banyak pemetaan sumber kejadian, gunakan parameter nama fungsi untuk mempersempit hasil.

```
aws lambda list-event-source-mappings --function-name ProcessDynamoDBRecords
```

Uji penyiapan

Uji end-to-end pengalamannya. Saat Anda melakukan pembaruan tabel, DynamoDB menuliskan catatan peristiwa ke aliran. Saat AWS Lambda melakukan polling terhadap aliran, ini mendeteksi catatan baru dalam aliran dan memanggil fungsi Lambda Anda atas nama Anda dengan mengirimkan peristiwa ke fungsi tersebut.

1. Di konsol DynamoDB, tambahkan, perbarui, dan hapus item di tabel. DynamoDB menuliskan catatan tindakan ini ke aliran.
2. AWS Lambda polling aliran dan ketika mendeteksi pembaruan ke aliran, ia memanggil fungsi Lambda Anda dengan meneruskan data peristiwa yang ditemukannya di aliran.
3. Fungsi Anda berjalan dan membuat log di Amazon CloudWatch. Anda dapat memverifikasi log yang dilaporkan di CloudWatch konsol Amazon.

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus tabel DynamoDB

1. Buka [halaman Tabel](#) di konsol DynamoDB.
2. Pilih tabel yang Anda buat.
3. Pilih Hapus.
4. Masukkan **delete** di kotak teks.
5. Pilih Hapus tabel.

Memproses peristiwa EC2 siklus hidup Amazon dengan fungsi Lambda

Anda dapat menggunakannya AWS Lambda untuk memproses peristiwa siklus hidup dari Amazon Elastic Compute Cloud dan mengelola sumber daya Amazon. EC2 Amazon EC2 mengirimkan peristiwa ke [Amazon EventBridge \(CloudWatch Acara\)](#) untuk [peristiwa siklus hidup](#) seperti saat instance mengubah status, saat snapshot volume Amazon Elastic Block Store selesai, atau saat instance spot dijadwalkan untuk dihentikan. Anda mengonfigurasi EventBridge (CloudWatch Peristiwa) untuk meneruskan peristiwa tersebut ke fungsi Lambda untuk diproses.

EventBridge (CloudWatch Peristiwa) memanggil fungsi Lambda Anda secara asinkron dengan dokumen peristiwa dari Amazon. EC2

Example kejadian siklus hidup instans

```
{
  "version": "0",
  "id": "b6ba298a-7732-2226-xmpl-976312c1a050",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "111122223333",
  "time": "2019-10-02T17:59:30Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:111122223333:instance/i-0c314xmplcd5b8173"
  ],
  "detail": {
    "instance-id": "i-0c314xmplcd5b8173",
    "state": "running"
  }
}
```

Untuk detail tentang mengonfigurasi acara, lihat [Memanggil fungsi Lambda sesuai jadwal](#). Untuk fungsi contoh yang memproses notifikasi EBS snapshot Amazon, lihat [EventBridge Penjadwal untuk Amazon](#). EBS

Anda juga dapat menggunakan AWS SDK untuk mengelola instance dan sumber daya lainnya dengan Amazon EC2API.

Memberikan izin untuk EventBridge (Acara) CloudWatch

Untuk memproses peristiwa siklus hidup dari AmazonEC2, EventBridge (CloudWatch Acara) memerlukan izin untuk menjalankan fungsi Anda. Izin ini berasal dari [kebijakan berbasis sumber daya](#) milik fungsi. Jika Anda menggunakan konsol EventBridge (CloudWatch Peristiwa) untuk mengonfigurasi pemicu peristiwa, konsol akan memperbarui kebijakan berbasis sumber daya atas nama Anda. Jika tidak, tambahkan pernyataan seperti berikut:

Example pernyataan kebijakan berbasis sumber daya untuk pemberitahuan siklus hidup Amazon EC2

```
{
  "Sid": "ec2-events",
  "Effect": "Allow",
  "Principal": {
    "Service": "events.amazonaws.com"
  },
  "Action": "lambda:InvokeFunction",
  "Resource": "arn:aws:lambda:us-east-1:12456789012:function:my-function",
  "Condition": {
    "ArnLike": {
      "AWS:SourceArn": "arn:aws:events:us-east-1:12456789012:rule/*"
    }
  }
}
```

Untuk menambahkan pernyataan, gunakan `add-permission` AWS CLI perintah.

```
aws lambda add-permission --action lambda:InvokeFunction --statement-id ec2-events \
--principal events.amazonaws.com --function-name my-function --source-arn
'arn:aws:events:us-east-1:12456789012:rule/*'
```

Jika fungsi Anda menggunakan AWS SDK untuk mengelola EC2 sumber daya Amazon, tambahkan EC2 izin Amazon ke [peran eksekusi](#) fungsi.

Memproses permintaan Application Load Balancer dengan Lambda

Anda dapat menggunakan fungsi Lambda untuk memproses permintaan dari Application Load Balancer. Elastic Load Balancing mendukung fungsi Lambda sebagai target untuk Application Load Balancer. Gunakan aturan penyeimbang beban untuk merutekan HTTP permintaan ke fungsi, berdasarkan nilai jalur atau header. Memproses permintaan dan mengembalikan HTTP respon dari fungsi Lambda Anda.

Elastic Load Balancing akan memanggil fungsi Lambda Anda secara sinkron dengan kejadian yang berisi badan dan metadata permintaan.

Example Kejadian permintaan Application Load Balancer

```
{
  "requestContext": {
    "elb": {
      "targetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/lambda-279XGJDqGZ5rsrHC2Fjr/49e9d65c45c6791a"
    }
  },
  "httpMethod": "GET",
  "path": "/lambda",
  "queryStringParameters": {
    "query": "1234ABCD"
  },
  "headers": {
    "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8",
    "accept-encoding": "gzip",
    "accept-language": "en-US,en;q=0.9",
    "connection": "keep-alive",
    "host": "lambda-alb-123578498.us-east-1.elb.amazonaws.com",
    "upgrade-insecure-requests": "1",
    "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36",
    "x-amzn-trace-id": "Root=1-5c536348-3d683b8b04734faae651f476",
    "x-forwarded-for": "72.12.164.125",
    "x-forwarded-port": "80",
    "x-forwarded-proto": "http",
    "x-imforwards": "20"
  },
  "body": ""
}
```

```
"isBase64Encoded": False
}
```

Fungsi Anda memproses peristiwa dan mengembalikan dokumen respons ke penyeimbang beban diJSON. Elastic Load Balancing mengubah dokumen menjadi respons HTTP sukses atau kesalahan dan mengembalikannya ke pengguna.

Example format dokumen respons

```
{
  "statusCode": 200,
  "statusDescription": "200 OK",
  "isBase64Encoded": False,
  "headers": {
    "Content-Type": "text/html"
  },
  "body": "<h1>Hello from Lambda!</h1>"
}
```

Untuk mengonfigurasi Application Load Balancer sebagai pemicu fungsi, berikan izin kepada Elastic Load Balancing untuk menjalankan fungsi, buat grup target yang merutekan permintaan ke fungsi, dan tambahkan aturan ke load balancer yang mengirim permintaan ke grup target.

Gunakan perintah `add-permission` untuk menambahkan pernyataan izin ke kebijakan berbasis sumber daya milik fungsi Anda.

```
aws lambda add-permission --function-name alb-function \
--statement-id load-balancer --action "lambda:InvokeFunction" \
--principal elasticloadbalancing.amazonaws.com
```

Anda akan melihat output berikut:

```
{
  "Statement": "{\"Sid\":\"load-balancer\",\"Effect\":\"Allow\",\"Principal\":\n{\"Service\":\"elasticloadbalancing.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\n\",\"Resource\":\"arn:aws:lambda:us-west-2:123456789012:function:alb-function\"}"
}
```

Untuk petunjuk konfigurasi Application Load Balancer dan grup target, lihat [Fungsi Lambda sebagai target](#) dalam Panduan Pengguna untuk Application Load Balancer.

Memanggil fungsi Lambda sesuai jadwal

[Amazon EventBridge Scheduler adalah penjadwal](#) tanpa server yang memungkinkan Anda membuat, menjalankan, dan mengelola tugas dari satu layanan terpusat dan terkelola. Dengan EventBridge Scheduler, Anda dapat membuat jadwal menggunakan ekspresi cron dan rate untuk pola berulang, atau mengonfigurasi pemanggilan satu kali. Anda dapat mengatur jendela waktu fleksibel untuk pengiriman, menentukan batas coba lagi, dan mengatur waktu retensi maksimum untuk peristiwa yang belum diproses.

Saat Anda mengatur EventBridge Scheduler dengan Lambda EventBridge, Scheduler memanggil fungsi Lambda Anda secara asinkron. Halaman ini menjelaskan cara menggunakan EventBridge Scheduler untuk menjalankan fungsi Lambda pada jadwal.

Mengatur peran eksekusi

Saat Anda membuat jadwal baru, EventBridge Scheduler harus memiliki izin untuk menjalankan API operasi targetnya atas nama Anda. Anda memberikan izin ini ke EventBridge Scheduler menggunakan peran eksekusi. Kebijakan izin yang Anda lampirkan ke peran eksekusi jadwal menentukan izin yang diperlukan. Izin ini bergantung pada target yang ingin API Anda panggil EventBridge Scheduler.

Bila Anda menggunakan konsol EventBridge Scheduler untuk membuat jadwal, seperti dalam prosedur berikut, EventBridge Scheduler secara otomatis mengatur peran eksekusi berdasarkan target yang Anda pilih. Jika Anda ingin membuat jadwal menggunakan salah satu EventBridge Scheduler SDKs, atau AWS CLI atau AWS CloudFormation, Anda harus memiliki peran eksekusi yang ada yang memberikan izin EventBridge Scheduler yang diperlukan untuk memanggil target. Untuk informasi selengkapnya tentang mengatur peran eksekusi secara manual untuk jadwal Anda, lihat [Menyiapkan peran eksekusi](#) di Panduan Pengguna EventBridge Penjadwal.

Buat jadwal

Untuk membuat jadwal dengan menggunakan konsol

1. Buka konsol Amazon EventBridge Scheduler di <https://console.aws.amazon.com/scheduler/rumah>.
2. Pada halaman Jadwal, pilih Buat jadwal.
3. Pada halaman Tentukan detail jadwal, di bagian Nama jadwal dan deskripsi, lakukan hal berikut:

- a. Untuk nama Jadwal, masukkan nama untuk jadwal Anda. Misalnya, **MyTestSchedule**.
- b. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk jadwal Anda. Misalnya, **My first schedule**.
- c. Untuk grup Jadwal, pilih grup jadwal dari daftar dropdown. Jika Anda tidak memiliki grup, pilih default. Untuk membuat grup jadwal, pilih buat jadwal Anda sendiri.

Anda menggunakan grup jadwal untuk menambahkan tag ke grup jadwal.

4. • Pilih opsi jadwal Anda.

| Kejadian | Lakukan ini... | |
|---|--|--|
| <p>Jadwal satu kali</p> <p>Jadwal satu kali memanggil target hanya sekali pada tanggal dan waktu yang Anda tentukan.</p> | <p>Untuk tanggal dan waktu, lakukan hal berikut:</p> <ul style="list-style-type: none"> • Masukkan tanggal yang valid dalam YYYY/MM/DD format. • Masukkan stempel waktu dalam format 24 jamhh : mm. • Untuk Timezone, pilih zona waktu. | |
| <p>Jadwal berulang</p> <p>Jadwal berulang memanggil target pada tingkat yang Anda tentukan menggunakan cron ekspresi atau ekspresi tingkat.</p> | <p>a. Untuk jenis Jadwal, lakukan salah satu hal berikut:</p> <ul style="list-style-type: none"> • Untuk menggunakan ekspresi cron untuk menentukan jadwal, pilih Jadwal berbasis Cron dan masukkan ekspresi cron. • Untuk menggunakan ekspresi tingkat untuk menentukan jadwal, | |

| Kejadian | Lakukan ini... | |
|----------|---|--|
| | <p>pilih Jadwal berbasis tingkat dan masukkan ekspresi laju.</p> <p>Untuk informasi selengkapnya tentang ekspresi cron dan rate, lihat Menjadwalkan jenis pada EventBridge Scheduler di Panduan Pengguna EventBridge Penjadwal Amazon.</p> <p>b. Untuk jendela waktu Fleksibel, pilih Nonaktif untuk mematikan opsi, atau pilih salah satu jendela waktu yang telah ditentukan sebelumnya</p> <p>a. Misalnya, jika Anda memilih 15 menit dan Anda menetapkan jadwal berulang untuk memanggil targetnya setiap jam sekali, jadwal berjalan dalam 15 menit setelah dimulainya setiap jam.</p> | |

5. (Opsional) Jika Anda memilih Jadwal berulang pada langkah sebelumnya, di bagian Jangka Waktu, lakukan hal berikut:
 - a. Untuk Timezone, pilih zona waktu.

- b. Untuk Tanggal dan waktu mulai, masukkan tanggal yang valid dalam YYYY/MM/DD format, lalu tentukan stempel waktu dalam format 24 jamhh : mm.
 - c. Untuk Tanggal dan waktu berakhir, masukkan tanggal yang valid dalam YYYY/MM/DD format, lalu tentukan stempel waktu dalam format 24 jamhh : mm.
6. Pilih Berikutnya.
 7. Pada halaman Pilih target, pilih AWS API operasi yang dipanggil EventBridge Scheduler:
 - a. Pilih AWS Lambda Panggil.
 - b. Di bagian Memanggil, pilih fungsi atau pilih Buat fungsi Lambda baru.
 - c. (Opsional) Masukkan JSON muatan. Jika Anda tidak memasukkan payload, EventBridge Scheduler menggunakan peristiwa kosong untuk menjalankan fungsi.
 8. Pilih Berikutnya.
 9. Pada halaman Pengaturan, lakukan hal berikut:
 - a. Untuk mengaktifkan jadwal, di bawah Status jadwal, alihkan Aktifkan jadwal.
 - b. Untuk mengonfigurasi kebijakan coba ulang untuk jadwal Anda, di bawah Kebijakan Coba ulang dan antrean huruf mati (DLQ), lakukan hal berikut:
 - Beralih Coba Lagi.
 - Untuk usia maksimum acara, masukkan jam maksimum dan min yang harus disimpan oleh EventBridge Scheduler untuk menyimpan acara yang belum diproses.
 - Waktu maksimum adalah 24 jam.
 - Untuk percobaan ulang Maksimum, masukkan jumlah maksimum kali EventBridge Scheduler mencoba ulang jadwal jika target mengembalikan kesalahan.

Nilai maksimumnya adalah 185 percobaan ulang.

Dengan kebijakan coba lagi, jika jadwal gagal memanggil targetnya, EventBridge Scheduler menjalankan kembali jadwal. Jika dikonfigurasi, Anda harus mengatur waktu retensi maksimum dan mencoba ulang untuk jadwal.

- c. Pilih tempat EventBridge Scheduler menyimpan acara yang tidak terkirim.

| Opsi antrian huruf mati () DLQ | Lakukan ini... |
|--|---|
| Jangan simpan | Pilih Tidak Ada. |
| Simpan acara di tempat yang sama Akun AWS di mana Anda membuat jadwal | <ul style="list-style-type: none"> a. Pilih Pilih SQS antrian Amazon di my Akun AWS as a DLQ. b. Pilih Nama Sumber Daya Amazon (ARN) dari SQS antrian Amazon. |
| Simpan acara di tempat yang berbeda Akun AWS dari tempat Anda membuat jadwal | <ul style="list-style-type: none"> a. Pilih Tentukan SQS antrian Amazon di yang lain Akun AWS sebagai DLQ. b. Masukkan Nama Sumber Daya Amazon (ARN) dari SQS antrian Amazon. |

- d. Untuk menggunakan kunci yang dikelola pelanggan untuk mengenkripsi input target Anda, di bawah Enkripsi, pilih Sesuaikan pengaturan enkripsi (lanjutan).

Jika Anda memilih opsi ini, masukkan KMS kunci yang ada ARN atau pilih Buat AWS KMS key untuk menavigasi ke AWS KMS konsol. Untuk informasi selengkapnya tentang cara EventBridge Scheduler mengenkripsi data Anda saat istirahat, lihat [Enkripsi saat istirahat di Panduan Pengguna EventBridge Penjadwal Amazon](#).

- e. Agar EventBridge Scheduler membuat peran eksekusi baru untuk Anda, pilih Buat peran baru untuk jadwal ini. Kemudian, masukkan nama untuk nama Peran. Jika Anda memilih opsi ini, EventBridge Scheduler melampirkan izin yang diperlukan untuk target template Anda ke peran.

10. Pilih Berikutnya.

11. Di halaman Tinjau dan buat jadwal, tinjau detail jadwal Anda. Di setiap bagian, pilih Edit untuk kembali ke langkah itu dan mengedit detailnya.

12. Pilih Buat jadwal.

Anda dapat melihat daftar jadwal baru dan yang sudah ada di halaman Jadwal. Di bawah kolom Status, verifikasi bahwa jadwal baru Anda Diaktifkan.

Untuk mengonfirmasi bahwa EventBridge Scheduler memanggil fungsi, [periksa log Amazon CloudWatch fungsi](#).

Sumber daya terkait

Untuk informasi selengkapnya tentang EventBridge Scheduler, lihat berikut ini:

- [EventBridge Panduan Pengguna Scheduler](#)
- [EventBridge Referensi Scheduler API](#)
- [EventBridge Penetapan Harga Scheduler](#)

Menggunakan AWS Lambda dengan AWS IoT

AWS IoT menyediakan komunikasi yang aman antara perangkat yang terhubung ke internet (seperti sensor) dan Cloud. AWS Ini memungkinkan Anda untuk mengumpulkan, menyimpan, dan menganalisis data telemetri dari beberapa perangkat.

Anda dapat membuat AWS IoT aturan untuk perangkat Anda untuk berinteraksi dengan AWS layanan. AWS IoT [Rules Engine](#) menyediakan bahasa SQL berbasis untuk memilih data dari muatan pesan dan mengirim data ke layanan lain, seperti Amazon S3, Amazon DynamoDB, dan. AWS Lambda Anda menetapkan aturan untuk menjalankan fungsi Lambda ketika Anda ingin memanggil layanan AWS lain atau layanan pihak ketiga.

Saat pesan IoT yang masuk memicu aturan, AWS IoT memanggil fungsi Lambda Anda secara asinkron dan meneruskan data dari pesan IoT ke [fungsi](#) tersebut.

Contoh berikut menunjukkan pembacaan kelembapan dari sensor rumah kaca. Nilai baris dan pos mengidentifikasi lokasi sensor. Contoh kejadian ini didasarkan pada jenis rumah kaca dalam [tutorial Aturan AWS IoT](#).

Example AWS IoT pesan acara

```
{
  "row" : "10",
  "pos" : "23",
  "moisture" : "75"
}
```

Untuk invokasi asinkron, Lambda mengantrekan pesan dan [mencoba lagi](#) jika fungsi Anda mengembalikan kesalahan. Konfigurasi fungsi Anda dengan [tujuan](#) untuk menyimpan kejadian yang tidak dapat diproses oleh fungsi Anda.

Anda perlu memberikan izin untuk AWS IoT layanan untuk menjalankan fungsi Lambda Anda. Gunakan perintah `add-permission` untuk menambahkan pernyataan izin ke kebijakan berbasis sumber daya milik fungsi Anda.

```
aws lambda add-permission --function-name my-function \
--statement-id iot-events --action "lambda:InvokeFunction" --principal
iot.amazonaws.com
```

Anda akan melihat output berikut:

```
{
  "Statement": "{\\"Sid\\":\\"iot-events\\",\\"Effect\\":\\"Allow\\",\\"Principal\\":
  {\\"Service\\":\\"iot.amazonaws.com\\"},\\"Action\\":\\"lambda:InvokeFunction\\",\\"Resource\\":
  \\"arn:aws:lambda:us-east-1:123456789012:function:my-function\\"}"
}
```

Untuk informasi selengkapnya tentang cara menggunakan Lambda AWS IoT, lihat [Membuat AWS Lambda aturan](#).

Bagaimana Lambda memproses catatan dari Amazon Kinesis Data Streams

Anda dapat menggunakan fungsi Lambda untuk memproses rekaman dalam aliran data [Amazon Kinesis](#). [Anda dapat memetakan fungsi Lambda ke konsumen throughput bersama Kinesis Data Streams \(iterator standar\), atau ke konsumen throughput khusus dengan fan-out yang disempurnakan.](#) Untuk iterator standar, Lambda polling setiap pecahan dalam aliran Kinesis Anda untuk catatan menggunakan protokol. HTTP Pemetaan sumber kejadian berbagi throughput baca dengan konsumen lain dari shard tersebut.

Untuk perincian tentang aliran data Kinesis, lihat [Data Pembacaan dari Amazon Kinesis Data Streams](#).

Note

Kinesis mengenakan biaya untuk setiap shard dan, untuk keluaran yang ditingkatkan, pembacaan data dari aliran. Untuk perincian harga, lihat [harga Amazon Kinesis](#).

Topik

- [Polling dan batching stream](#)
- [Contoh peristiwa](#)
- [Memproses rekaman Amazon Kinesis Data Streams dengan Lambda](#)
- [Mengonfigurasi respons batch sebagian dengan Kinesis Data Streams dan Lambda](#)
- [Menyimpan catatan batch yang dibuang untuk sumber peristiwa Kinesis Data Streams di Lambda](#)
- [Menerapkan pemrosesan Kinesis Data Streams stateful di Lambda](#)
- [Parameter Lambda untuk pemetaan sumber peristiwa Amazon Kinesis Data Streams](#)
- [Menggunakan pemfilteran acara dengan sumber acara Kinesis](#)
- [Tutorial: Menggunakan Lambda dengan Kinesis Data Streams](#)

Polling dan batching stream

Lambda membaca rekaman dari aliran data dan memanggil fungsi Anda [secara sinkron](#) dengan kejadian yang berisi rekaman aliran. Lambda membaca rekaman dalam batch dan memanggil fungsi Anda untuk memproses rekaman dari batch. Setiap batch berisi catatan dari satu shard/aliran data.

Untuk aliran data Kinesis standar, Lambda melakukan polling pecahan di aliran Anda untuk catatan dengan kecepatan sekali per detik untuk setiap pecahan. Untuk [Kinesis yang ditingkatkan fan-out](#), Lambda menggunakan koneksi /2 untuk HTTP mendengarkan rekaman yang didorong dari Kinesis. Setelah catatan tersedia, Lambda menginvokasi fungsi Anda dan menunggu hasilnya.

Secara default, Lambda memanggil fungsi Anda segera setelah catatan tersedia. Jika batch yang dibaca Lambda dari sumber peristiwa hanya memiliki satu catatan di dalamnya, Lambda hanya mengirimkan satu catatan ke fungsi tersebut. Untuk menghindari menjalankan fungsi dengan sejumlah kecil catatan, Anda dapat memberi tahu sumber acara untuk menyangga catatan hingga 5 menit dengan mengonfigurasi jendela batching. Sebelum menjalankan fungsi, Lambda terus membaca catatan dari sumber acara hingga mengumpulkan batch penuh, jendela batching kedaluwarsa, atau batch mencapai batas muatan 6 MB. Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Lambda tidak menunggu [ekstensi](#) yang dikonfigurasi selesai sebelum mengirim batch berikutnya untuk diproses. Dengan kata lain, ekstensi Anda dapat terus berjalan saat Lambda memproses kumpulan catatan berikutnya. Hal ini dapat menyebabkan masalah pembatasan jika Anda melanggar pengaturan atau [batas konkurensi](#) akun Anda. Untuk mendeteksi apakah ini merupakan masalah potensial, pantau fungsi Anda dan periksa apakah Anda melihat [metrik konkurensi](#) yang lebih tinggi dari yang diharapkan untuk pemetaan sumber peristiwa Anda. Karena waktu yang singkat di antara pemanggilan, Lambda mungkin secara singkat melaporkan penggunaan konkurensi yang lebih tinggi daripada jumlah pecahan. Ini bisa benar bahkan untuk fungsi Lambda tanpa ekstensi.

Konfigurasi [ParallelizationFactor](#) pengaturan untuk memproses satu pecahan aliran data Kinesis dengan lebih dari satu pemanggilan Lambda secara bersamaan. Anda dapat menentukan jumlah batch bersamaan yang polling-nya dibuat Lambda dari shard melalui faktor paralelisasi mulai dari 1 (default) hingga 10. Misalnya, saat Anda menyetel `ParallelizationFactor` ke 2, Anda dapat memiliki maksimum 200 pemanggilan Lambda bersamaan untuk memproses 100 pecahan data Kinesis (meskipun dalam praktiknya, Anda mungkin melihat nilai yang berbeda untuk metrik).

`ConcurrentExecutions` Hal ini membantu meningkatkan skala throughput pemrosesan ketika volume data tidak stabil dan `IteratorAge` tinggi. Saat Anda meningkatkan jumlah batch bersamaan per pecahan, Lambda masih memastikan pemrosesan in-order pada tingkat kunci partisi.

Anda juga dapat menggunakan `ParallelizationFactor` dengan agregasi Kinesis. Perilaku pemetaan sumber acara bergantung pada apakah Anda menggunakan [fan-out yang disempurnakan](#):

- Tanpa fan-out yang disempurnakan: Semua peristiwa di dalam acara agregat harus memiliki kunci partisi yang sama. Kunci partisi juga harus cocok dengan peristiwa agregat. Jika peristiwa di dalam peristiwa agregat memiliki kunci partisi yang berbeda, Lambda tidak dapat menjamin pemrosesan peristiwa secara berurutan dengan kunci partisi.
- Dengan fan-out yang disempurnakan: Pertama, Lambda menerjemahkan peristiwa agregat ke dalam acara individualnya. Acara agregat dapat memiliki kunci partisi yang berbeda dari peristiwa yang dikandungnya. Namun, peristiwa yang tidak sesuai dengan kunci partisi [dijatuhkan dan hilang](#). Lambda tidak memproses peristiwa ini, dan tidak mengirimnya ke tujuan kegagalan yang dikonfigurasi.

Contoh peristiwa

Example

```
{
  "Records": [
    {
      "kinesis": {
        "kinesisSchemaVersion": "1.0",
        "partitionKey": "1",
        "sequenceNumber":
"49590338271490256608559692538361571095921575989136588898",
        "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
        "approximateArrivalTimestamp": 1545084650.987
      },
      "eventSource": "aws:kinesis",
      "eventVersion": "1.0",
      "eventID":
"shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
      "eventName": "aws:kinesis:record",
      "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
      "awsRegion": "us-east-2",
    }
  ]
}
```

```

        "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
    },
    {
        "kinesis": {
            "kinesisSchemaVersion": "1.0",
            "partitionKey": "1",
            "sequenceNumber":
"49590338271490256608559692540925702759324208523137515618",
            "data": "VGhpcyBpcyBvbmx5IGEgdGVzdC4=",
            "approximateArrivalTimestamp": 1545084711.166
        },
        "eventSource": "aws:kinesis",
        "eventVersion": "1.0",
        "eventID":
"shardId-000000000006:49590338271490256608559692540925702759324208523137515618",
        "eventName": "aws:kinesis:record",
        "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
        "awsRegion": "us-east-2",
        "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
    }
]
}

```

Memproses rekaman Amazon Kinesis Data Streams dengan Lambda

Untuk memproses rekaman Amazon Kinesis Data Streams dengan Lambda, buat konsumen untuk streaming Anda, lalu buat pemetaan sumber peristiwa Lambda.

Mengonfigurasi aliran data dan fungsi Anda

Fungsi Lambda Anda adalah aplikasi konsumen untuk aliran data Anda. Itu memproses satu batch rekaman pada satu waktu dari setiap shard. Anda dapat memetakan fungsi Lambda ke konsumen dengan throughput bersama (iterator standar), atau ke konsumen dengan throughput khusus dengan [keluaran yang ditingkatkan](#).

- **Iterator standar:** Lambda polling setiap pecahan dalam aliran Kinesis Anda untuk catatan dengan kecepatan dasar sekali per detik. Saat tersedia lebih banyak rekaman, Lambda melanjutkan pemrosesan batch sampai fungsi dapat menyusul aliran. Pemetaan sumber kejadian berbagi throughput baca dengan konsumen lain dari shard tersebut.

- Peningkatan fan-out: [Untuk meminimalkan latensi dan memaksimalkan throughput baca, buat konsumen aliran data dengan fan-out yang disempurnakan](#). Konsumen dengan keluaran yang ditingkatkan mendapatkan koneksi khusus ke setiap shard yang tidak memengaruhi pembacaan aplikasi lain dari aliran tersebut. Konsumen aliran menggunakan HTTP/2 untuk mengurangi latensi dengan mendorong rekaman ke Lambda melalui koneksi yang sudah berlangsung lama dan dengan mengompresi header permintaan. Anda dapat membuat konsumen streaming dengan Kinesis [RegisterStreamConsumer](#) API.

```
aws kinesis register-stream-consumer \  
--consumer-name con1 \  
--stream-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream
```

Anda akan melihat output berikut:

```
{  
  "Consumer": {  
    "ConsumerName": "con1",  
    "ConsumerARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream/  
consumer/con1:1540591608",  
    "ConsumerStatus": "CREATING",  
    "ConsumerCreationTimestamp": 1540591608.0  
  }  
}
```

Untuk meningkatkan kecepatan proses fungsi Anda merekam, [tambahkan pecahan ke aliran data Anda](#). Lambda memproses rekaman dalam setiap shard secara berurutan. Lambda menghentikan pemrosesan rekaman tambahan dalam shard jika fungsi Anda mengembalikan kesalahan. Makin banyak shard, makin banyak batch yang diproses sekaligus sehingga mengurangi dampak kesalahan terhadap konkurensi.

Apabila fungsi Anda tidak dapat menskalakan naik untuk menangani jumlah total batch yang bersamaan, [mintalah kenaikan kuota](#) atau [cadangkan konkurensi](#) untuk fungsi Anda.

Buat pemetaan sumber acara untuk menjalankan fungsi Lambda

Untuk menjalankan fungsi Lambda Anda dengan catatan dari aliran data Anda, buat pemetaan sumber [peristiwa](#). Anda dapat membuat beberapa pemetaan sumber kejadian untuk memproses data yang sama dengan beberapa fungsi Lambda, atau untuk memproses item dari beberapa aliran data

dengan satu fungsi. Saat memproses item dari beberapa aliran, setiap batch berisi catatan hanya dari satu pecahan atau aliran.

Anda dapat mengonfigurasi pemetaan sumber peristiwa untuk memproses catatan dari aliran yang berbeda. Akun AWS Untuk mempelajari selengkapnya, lihat [the section called “Pemetaan lintas akun”](#).

Sebelum Anda membuat pemetaan sumber peristiwa, Anda perlu memberikan izin fungsi Lambda Anda untuk membaca dari aliran data Kinesis. Lambda memerlukan izin berikut untuk mengelola sumber daya yang terkait dengan aliran data Kinesis Anda:

- [kinesis: DescribeStream](#)
- [kinesis: Ringkasan DescribeStream](#)
- [kinesis: GetRecords](#)
- [kinesis: GetShard Iterator](#)
- [kinesis: ListShards](#)
- [kinesis: ListStreams](#)
- [kinesis: SubscribeTo Pecahan](#)

Kebijakan AWS terkelola [AWSLambdaKinesisExecutionRole](#) mencakup izin ini. Tambahkan kebijakan terkelola ini ke fungsi Anda seperti yang dijelaskan dalam prosedur berikut.

AWS Management Console

Untuk menambahkan izin Kinesis ke fungsi Anda

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.
2. Di tab Konfigurasi, pilih Izin.
3. Di panel Peran eksekusi, di bawah Nama peran, pilih tautan ke peran eksekusi fungsi Anda. Tautan ini membuka halaman untuk peran itu di konsol IAM.
4. Di panel Kebijakan izin, pilih Tambahkan izin, lalu pilih Lampirkan kebijakan.
5. Di bidang pencarian, masukkan **AWSLambdaKinesisExecutionRole**.
6. Pilih kotak centang di samping kebijakan dan pilih Tambah izin.

AWS CLI

Untuk menambahkan izin Kinesis ke fungsi Anda

- Jalankan perintah CLI berikut untuk menambahkan `AWSLambdaKinesisExecutionRole` kebijakan ke peran eksekusi fungsi Anda:

```
aws iam attach-role-policy \  
--role-name MyFunctionRole \  
--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole
```

AWS SAM

Untuk menambahkan izin Kinesis ke fungsi Anda

- Dalam definisi fungsi Anda, tambahkan `Policies` properti seperti yang ditunjukkan pada contoh berikut:

```
Resources:  
  MyFunction:  
    Type: AWS::Serverless::Function  
    Properties:  
      CodeUri: ./my-function/  
      Handler: index.handler  
      Runtime: nodejs20.x  
      Policies:  
        - AWSLambdaKinesisExecutionRole
```

Setelah mengonfigurasi izin yang diperlukan, buat pemetaan sumber acara.

AWS Management Console

Untuk membuat pemetaan sumber peristiwa Kinesis

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda.
2. Di panel Ikhtisar fungsi, pilih Tambah pemicu.
3. Di bawah Konfigurasi pemicu, untuk sumbernya, pilih Kinesis.
4. Pilih aliran Kinesis yang ingin Anda buat pemetaan sumber acara dan, secara opsional, konsumen aliran Anda.

5. (Opsional) edit ukuran Batch, Posisi awal, dan jendela Batch untuk pemetaan sumber acara Anda.
6. Pilih Tambahkan.

Saat membuat pemetaan sumber peristiwa dari konsol, peran IAM Anda harus memiliki izin [kinesis: ListStreams](#) dan [kinesis: Konsumen](#). ListStream

AWS CLI

Untuk membuat pemetaan sumber peristiwa Kinesis

- Jalankan perintah CLI berikut untuk membuat pemetaan sumber peristiwa Kinesis. Pilih ukuran batch Anda sendiri dan posisi awal sesuai dengan kasus penggunaan Anda.

```
aws lambda create-event-source-mapping \  
--function-name MyFunction \  
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \  
--starting-position LATEST \  
--batch-size 100
```

Untuk menentukan jendela batching, tambahkan `--maximum-batching-window-in-seconds` opsi. Untuk informasi selengkapnya tentang penggunaan parameter ini dan parameter lainnya, lihat [create-event-source-mapping](#) di Referensi Perintah.AWS CLI

AWS SAM

Untuk membuat pemetaan sumber peristiwa Kinesis

- Dalam definisi fungsi Anda, tambahkan `KinesisEvent` properti seperti yang ditunjukkan pada contoh berikut:

```
Resources:  
  MyFunction:  
    Type: AWS::Serverless::Function  
    Properties:  
      CodeUri: ./my-function/  
      Handler: index.handler  
      Runtime: nodejs20.x  
      Policies:  
        - AWSLambdaKinesisExecutionRole  
    Events:
```

```
KinesisEvent:
  Type: Kinesis
  Properties:
    Stream: !GetAtt MyKinesisStream.Arn
    StartingPosition: LATEST
    BatchSize: 100

MyKinesisStream:
  Type: AWS::Kinesis::Stream
  Properties:
    ShardCount: 1
```

Untuk mempelajari selengkapnya tentang membuat pemetaan sumber peristiwa untuk Kinesis Data Streams di AWS SAM, lihat [Kinesis](#) dalam Panduan Pengembang AWS Serverless Application Model

Posisi awal polling dan streaming

Ketahui bahwa polling streaming selama pembuatan dan pembaruan pemetaan sumber acara pada akhirnya konsisten.

- Selama pembuatan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk memulai acara polling dari aliran.
- Selama pembaruan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk menghentikan dan memulai kembali acara pemungutan suara dari aliran.

Perilaku ini berarti bahwa jika Anda menentukan LATEST sebagai posisi awal untuk aliran, pemetaan sumber peristiwa dapat melewatkan peristiwa selama pembuatan atau pembaruan. Untuk memastikan bahwa tidak ada peristiwa yang terlewatkan, tentukan posisi awal aliran sebagai TRIM_HORIZON atau AT_TIMESTAMP.

Membuat pemetaan sumber peristiwa lintas akun

Amazon Kinesis Data [Streams](#) mendukung kebijakan berbasis sumber daya. Karena itu, Anda dapat memproses data yang dicerna ke dalam aliran dalam satu Akun AWS dengan fungsi Lambda di akun lain.

Untuk membuat pemetaan sumber peristiwa untuk fungsi Lambda Anda menggunakan aliran Kinesis yang Akun AWS berbeda, Anda harus mengonfigurasi aliran menggunakan kebijakan berbasis sumber daya untuk memberikan izin fungsi Lambda Anda untuk membaca item. Untuk mempelajari cara mengonfigurasi streaming agar memungkinkan akses lintas akun, lihat [Berbagi akses dengan AWS Lambda fungsi lintas akun](#) di panduan Pengembang Amazon Kinesis Streams.

Setelah mengonfigurasi aliran Anda dengan kebijakan berbasis sumber daya yang memberi fungsi Lambda Anda izin yang diperlukan, buat pemetaan sumber peristiwa menggunakan salah satu metode yang dijelaskan di bagian sebelumnya.

Jika Anda memilih untuk membuat pemetaan sumber acara menggunakan konsol Lambda, tempelkan ARN aliran Anda langsung ke bidang input. Jika Anda ingin menentukan konsumen untuk streaming Anda, menempelkan ARN konsumen secara otomatis mengisi bidang aliran.

Mengonfigurasi respons batch sebagian dengan Kinesis Data Streams dan Lambda

Ketika menggunakan dan memproses data streaming dari sumber peristiwa, secara default Lambda memeriksa urutan nomor tertinggi batch hanya ketika batch berhasil diselesaikan. Lambda memperlakukan semua hasil lain sebagai sepenuhnya gagal dan mencoba lagi pemrosesan batch hingga batas coba lagi. Untuk memungkinkan keberhasilan parsial saat memproses batch dari aliran, aktifkan `ReportBatchItemFailures`. Mengizinkan keberhasilan parsial dapat membantu mengurangi jumlah percobaan ulang pada catatan, meskipun tidak sepenuhnya mencegah kemungkinan percobaan ulang dalam catatan yang sukses.

Untuk mengaktifkan `ReportBatchItemFailures`, sertakan nilai enum **`ReportBatchItemFailures`** dalam daftar [FunctionResponseJenis](#). Daftar ini menunjukkan tipe respon yang diaktifkan untuk fungsi Anda. Anda dapat mengonfigurasi daftar ini saat [membuat](#) atau [memperbarui](#) pemetaan sumber peristiwa.

Sintaks laporan

Saat mengonfigurasi pelaporan pada kegagalan item batch, kelas `StreamsEventResponse` dikembalikan dengan daftar kegagalan item batch. Anda dapat menggunakan objek `StreamsEventResponse` untuk mengembalikan nomor urutan catatan gagal pertama dalam batch. Anda juga dapat membuat kelas kustom Anda sendiri menggunakan sintaks respons yang benar. Struktur JSON berikut menunjukkan sintaks respons yang diperlukan:

```
{
```

```
"batchItemFailures": [  
  {  
    "itemIdentifier": "<SequenceNumber>"  
  }  
]
```

Note

Jika `batchItemFailures` array berisi beberapa item, Lambda menggunakan catatan dengan nomor urut terendah sebagai pos pemeriksaan. Lambda kemudian mencoba kembali semua catatan mulai dari pos pemeriksaan itu.

Status berhasil dan gagal

Lambda memperlakukan batch sebagai sepenuhnya berhasil jika Anda mengembalikan salah satu dari berikut:

- Daftar `batchItemFailure` kosong
- Daftar `batchItemFailure` nol
- `EventResponse` kosong
- `EventResponse` nol

Lambda memperlakukan batch sebagai sepenuhnya gagal jika Anda mengembalikan salah satu dari berikut:

- String `itemIdentifier` kosong
- `itemIdentifier` nol
- `itemIdentifier` dengan nama kunci yang buruk

Lambda mencoba kembali kegagalan berdasarkan strategi coba lagi Anda.

Membagi batch

Jika invokasi Anda gagal dan `BisectBatchOnFunctionError` diaktifkan, batch dibagi terlepas dari pengaturan `ReportBatchItemFailures` Anda.

Ketika respons berhasil batch parsial diterima dan kedua `BisectBatchOnError` dan `ReportBatchItemFailures` diaktifkan, batch dibagi dua di nomor urutan yang dikembalikan dan Lambda mencoba hanya catatan yang tersisa.

Berikut adalah beberapa contoh kode fungsi yang mengembalikan daftar ID pesan gagal dalam batch:

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
        ILambdaContext context)
    {
```

```

    if (evnt.Records.Count == 0)
    {
        Logger.LogInformation("Empty Kinesis Event received");
        return new StreamsEventResponse();
    }

    foreach (var record in evnt.Records)
    {
        try
        {
            Logger.LogInformation($"Processed Event with EventId:
{record.EventId}");
            string data = await GetRecordDataAsync(record.Kinesis, context);
            Logger.LogInformation($"Data: {data}");
            // TODO: Do interesting work based on the new data
        }
        catch (Exception ex)
        {
            Logger.LogError($"An error occurred {ex.Message}");
            /* Since we are working with streams, we can return the failed
item immediately.
            Lambda will immediately begin to retry processing from this
failed item onwards. */
            return new StreamsEventResponse
            {
                BatchItemFailures = new
List<StreamsEventResponse.BatchItemFailure>
                {
                    new StreamsEventResponse.BatchItemFailure
{ ItemIdentifier = record.Kinesis.SequenceNumber }
                }
            };
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
records.");
        return new StreamsEventResponse();
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
    }

```

```

        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}

public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}

```

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Go.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
(map[string]interface{}, error) {
    batchItemFailures := []map[string]interface{}{}

```



```
for _, record := range kinesisEvent.Records {
    curRecordSequenceNumber := ""

    // Process your record
    if /* Your record processing condition here */ {
        curRecordSequenceNumber = record.Kinesis.SequenceNumber
    }

    // Add a condition to check if the record processing failed
    if curRecordSequenceNumber != "" {
        batchItemFailures = append(batchItemFailures, map[string]interface{}{
            "itemIdentifier": curRecordSequenceNumber})
    }
}

kinesisBatchResponse := map[string]interface{}{
    "batchItemFailures": batchItemFailures,
}
return kinesisBatchResponse, nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
```

```
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
ArrayList<>();
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
item immediately.
                Lambda will immediately begin to retry processing from this
failed item onwards. */
                batchItemFailures.add(new
StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

        return new StreamsEventResponse(batchItemFailures);
    }
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Javascript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
      immediately.
      Lambda will immediately begin to retry processing from this failed
      item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Melaporkan kegagalan item batch Kinesis dengan penggunaan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
      immediately.
      Lambda will immediately begin to retry processing from this failed
      item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  logger.info(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};
```

```
async function getRecordDataAsync(  
    payload: KinesisStreamRecordPayload  
) : Promise<string> {  
    var data = Buffer.from(payload.data, "base64").toString("utf-8");  
    await Promise.resolve(1); //Placeholder for actual async work  
    return data;  
}
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
<?php  
  
# using bref/bref and bref/logger for simplicity  
  
use Bref\Context\Context;  
use Bref\Event\Kinesis\KinesisEvent;  
use Bref\Event\Handler as StdHandler;  
use Bref\Logger\StderrLogger;  
  
require __DIR__ . '/vendor/autoload.php';  
  
class Handler implements StdHandler  
{  
    private StderrLogger $logger;  
    public function __construct(StderrLogger $logger)  
    {  
        $this->logger = $logger;  
    }  
}
```

```
/**
 * @throws JsonException
 * @throws \Bref\Event\InvalidLambdaEvent
 */
public function handle(mixed $event, Context $context): array
{
    $kinesisEvent = new KinesisEvent($event);
    $this->logger->info("Processing records");
    $records = $kinesisEvent->getRecords();

    $failedRecords = [];
    foreach ($records as $record) {
        try {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data
        } catch (Exception $e) {
            $this->logger->error($e->getMessage());
            // failed processing the record
            $failedRecords[] = $record->getSequenceNumber();
        }
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords records");

    // change format for the response
    $failures = array_map(
        fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
        $failedRecords
    );

    return [
        'batchItemFailures' => $failures
    ];
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
      # immediately.
      # Lambda will immediately begin to retry processing from this failed item
      # onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
  sleep(1)
  data
end
```


Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",
            record.event_id.as_deref().unwrap_or_default()
        );

        let record_processing_result = process_record(record);

        if record_processing_result.is_err() {
            response.batch_item_failures.push(KinesisBatchItemFailure {
                item_identifier: record.kinesis.sequence_number.clone(),
```

```

        });
        /* Since we are working with streams, we can return the failed item
immediately.
        Lambda will immediately begin to retry processing from this failed
item onwards. */
        return Ok(response);
    }
}

tracing::info!(
    "Successfully processed {} records",
    event.payload.records.len()
);

Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());

    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
time.
        .without_time()
        .init();
}

```

```
run(service_fn(function_handler)).await
}
```

Menyimpan catatan batch yang dibuang untuk sumber peristiwa Kinesis Data Streams di Lambda

Penanganan kesalahan untuk pemetaan sumber peristiwa Kinesis tergantung pada apakah kesalahan terjadi sebelum fungsi dipanggil atau selama pemanggilan fungsi:

- Sebelum pemanggilan: [Jika pemetaan sumber peristiwa Lambda tidak dapat menjalankan fungsi karena pembatasan atau masalah lain, fungsi tersebut akan mencoba lagi hingga catatan kedaluwarsa atau melebihi usia maksimum yang dikonfigurasi pada pemetaan sumber peristiwa \(Detik\). `MaximumRecord AgeIn`](#)
- Selama pemanggilan: [Jika fungsi dipanggil tetapi mengembalikan kesalahan, Lambda mencoba ulang hingga catatan kedaluwarsa, melebihi usia maksimum \(`MaximumRecordAgeInDetik`\), atau mencapai kuota coba lagi yang dikonfigurasi \(`Upaya`\). `MaximumRetry`](#) Untuk kesalahan fungsi, Anda juga dapat mengonfigurasi [BisectBatchOnFunctionKesalahan](#), yang membagi batch yang gagal menjadi dua batch yang lebih kecil, mengisolasi catatan buruk dan menghindari batas waktu. Memisahkan batch tidak menghabiskan kuota coba lagi.

Jika tindakan penanganan kesalahan gagal, Lambda membuang rekaman dan melanjutkan pemrosesan batch dari aliran. Dengan pengaturan default, ini berarti rekaman yang buruk dapat memblokir pemrosesan pada shard yang terpengaruh selama hingga satu minggu. Untuk menghindari hal ini, konfigurasi pemetaan sumber kejadian fungsi Anda dengan jumlah percobaan ulang yang wajar dan usia maksimum rekaman yang sesuai dengan kasus penggunaan Anda.

Mengonfigurasi tujuan untuk pemanggilan yang gagal

Untuk menyimpan catatan pemanggilan pemetaan sumber peristiwa yang gagal, tambahkan tujuan ke pemetaan sumber peristiwa fungsi Anda. Setiap catatan yang dikirim ke tujuan adalah dokumen JSON dengan metadata tentang pemanggilan yang gagal. Anda dapat mengonfigurasi topik Amazon SNS atau antrian Amazon SQS sebagai tujuan. Peran eksekusi Anda harus memiliki izin untuk tujuan:

- Untuk tujuan SQS: [sqs: SendMessage](#)
- [Untuk tujuan SNS: SNS: Publikasikan](#)

Untuk mengonfigurasi tujuan saat gagal menggunakan konsol, ikuti langkah-langkah berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambahkan tujuan.
4. Untuk Sumber, pilih Pemanggilan pemetaan sumber acara.
5. Untuk pemetaan sumber peristiwa, pilih sumber peristiwa yang dikonfigurasi untuk fungsi ini.
6. Untuk Kondisi, pilih On failure. Untuk pemanggilan pemetaan sumber peristiwa, ini adalah satu-satunya kondisi yang diterima.
7. Untuk tipe Tujuan, pilih tipe tujuan yang Lambda kirimkan catatan pemanggilan.
8. Untuk Tujuan, pilih sumber daya.
9. Pilih Simpan.

Anda juga dapat mengonfigurasi tujuan pada kegagalan menggunakan AWS Command Line Interface (AWS CLI). Misalnya, perintah [create-event-source-mapping](#) berikut [menambahkan pemetaan](#) sumber peristiwa dengan tujuan kegagalan SQS ke: MyFunction

```
aws lambda create-event-source-mapping \  
--function-name "MyFunction" \  
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-  
east-1:123456789012:dest-queue"}}'
```

Perintah [update-event-source-mapping](#) berikut memperbarui pemetaan sumber peristiwa untuk mengirim catatan pemanggilan yang gagal ke tujuan SNS setelah dua percobaan ulang, atau jika catatan berusia lebih dari satu jam.

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--maximum-retry-attempts 2 \  
--maximum-record-age-in-seconds 3600 \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-  
east-1:123456789012:dest-topic"}}'
```

Pengaturan yang diperbarui diterapkan secara asinkron dan tidak muncul dalam output hingga proses selesai. Gunakan perintah [get-event-source-mapping](#) untuk melihat status saat ini.

Untuk menghapus tujuan, berikan string kosong sebagai argumen ke `destination-config` parameter:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Contoh berikut menunjukkan apa yang Lambda kirim ke antrian SQS atau topik SNS untuk pemanggilan sumber peristiwa Kinesis yang gagal. Karena Lambda hanya mengirimkan metadata untuk jenis tujuan ini, gunakan `streamArn`, `shardId`, `startSequenceNumber`, dan `endSequenceNumber` bidang untuk mendapatkan catatan asli lengkap.

```
{
  "requestContext": {
    "requestId": "c9b8fa9f-5a7f-xmpl-af9c-0c604cde93a5",
    "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
    "condition": "RetryAttemptsExhausted",
    "approximateInvokeCount": 1
  },
  "responseContext": {
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T00:38:06.021Z",
  "KinesisBatchInfo": {
    "shardId": "shardId-000000000001",
    "startSequenceNumber":
"49601189658422359378836298521827638475320189012309704722",
    "endSequenceNumber":
"49601189658422359378836298522902373528957594348623495186",
    "approximateArrivalOfFirstRecord": "2019-11-14T00:38:04.835Z",
    "approximateArrivalOfLastRecord": "2019-11-14T00:38:05.580Z",
    "batchSize": 500,
    "streamArn": "arn:aws:kinesis:us-east-2:123456789012:stream/mystream"
  }
}
```

Anda dapat menggunakan informasi ini guna mengambil rekaman yang terpengaruh dari aliran untuk pemecahan masalah. Rekaman aktual tidak disertakan, jadi Anda harus memproses rekaman ini dan mengambilnya dari aliran sebelum kedaluwarsa dan hilang.

Menerapkan pemrosesan Kinesis Data Streams stateful di Lambda

Fungsi Lambda dapat menjalankan aplikasi pemrosesan aliran berkelanjutan. Aliran merupakan data tidak terbatas yang mengalir terus-menerus melalui aplikasi Anda. Untuk menganalisis informasi dari input yang terus diperbarui ini, Anda dapat mengikat catatan yang disertakan menggunakan jendela yang didefinisikan dalam hal waktu.

Jatuh jendela adalah jendela waktu yang berbeda yang membuka dan menutup secara berkala. Secara default, pemanggilan Lambda tidak memiliki status — Anda tidak dapat menggunakannya untuk memproses data di beberapa pemanggilan berkelanjutan tanpa database eksternal. Namun, dengan jendela yang jatuh, Anda dapat mempertahankan status Anda di seluruh pemanggilan. Status ini berisi hasil agregat pesan yang sebelumnya diproses untuk jendela saat ini. Status Anda maksimal bisa sebesar 1 MB per shard. Jika melebihi ukuran tersebut, Lambda mengakhiri jendela lebih awal.

Setiap rekaman dalam aliran milik jendela tertentu. Lambda akan memproses setiap rekaman setidaknya sekali, tetapi tidak menjamin bahwa setiap rekaman akan diproses hanya sekali. Dalam kasus yang jarang terjadi, seperti penanganan kesalahan, beberapa catatan mungkin diproses lebih dari sekali. Catatan selalu diproses secara berurutan pertama kali. Jika catatan diproses lebih dari satu kali, mereka mungkin diproses rusak.

Agregasi dan pemrosesan

Fungsi yang dikelola pengguna Anda dipanggil baik untuk agregasi maupun untuk memproses hasil akhir agregasi tersebut. Lambda mengumpulkan semua catatan yang diterima di jendela. Anda dapat menerima catatan ini dalam beberapa batch, masing-masing sebagai invokasi terpisah. Setiap invokasi menerima status. Jadi, saat menggunakan jendela tumbling, respons fungsi Lambda Anda harus berisi state properti. Jika respons tidak berisi state properti, Lambda menganggap ini sebagai pemanggilan yang gagal. Untuk memenuhi kondisi ini, fungsi Anda dapat mengembalikan `TimeWindowEventResponse` objek, yang memiliki bentuk JSON berikut:

Example Nilai `TimeWindowEventResponse`

```
{
```

```

    "state": {
      "1": 282,
      "2": 715
    },
    "batchItemFailures": []
  }
}

```

Note

Untuk fungsi Java, sebaiknya gunakan a `Map<String, String>` untuk mewakili status.

Di akhir jendela, tanda `isFinalInvokeForWindow` diatur ke `true` untuk menunjukkan bahwa ini adalah status akhir dan bahwa itu siap untuk diproses. Setelah pemrosesan, jendela selesai, dan invokasi akhir Anda selesai, lalu status dihapus.

Di akhir jendela Anda, Lambda menggunakan pemrosesan akhir untuk tindakan pada hasil agregasi. Pemrosesan akhir Anda dipanggil secara sinkron. Setelah pemanggilan berhasil, fungsi Anda memeriksa nomor urut dan pemrosesan aliran berlanjut. Jika invokasi tidak berhasil, fungsi Lambda Anda menunda pemrosesan lebih lanjut sampai invokasi sukses.

Example KinesisTimeWindowEvent

```

{
  "Records": [
    {
      "kinesis": {
        "kinesisSchemaVersion": "1.0",
        "partitionKey": "1",
        "sequenceNumber":
"49590338271490256608559692538361571095921575989136588898",
        "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
        "approximateArrivalTimestamp": 1607497475.000
      },
      "eventSource": "aws:kinesis",
      "eventVersion": "1.0",
      "eventID":
"shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
      "eventName": "aws:kinesis:record",
      "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-kinesis-role",

```

```
        "awsRegion": "us-east-1",
        "eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-
stream"
    }
],
"window": {
    "start": "2020-12-09T07:04:00Z",
    "end": "2020-12-09T07:06:00Z"
},
"state": {
    "1": 282,
    "2": 715
},
"shardId": "shardId-0000000000006",
"eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream",
"isFinalInvokeForWindow": false,
"isWindowTerminatedEarly": false
}
```

Konfigurasi

Anda dapat mengonfigurasi jendela berguling saat membuat atau memperbarui pemetaan sumber peristiwa. Untuk mengkonfigurasi jendela tumbling, tentukan jendela dalam hitungan detik ([TumblingWindowInSeconds](#)). Contoh berikut AWS Command Line Interface (AWS CLI) perintah membuat pemetaan sumber acara streaming yang memiliki jendela jatuh 120 detik. Fungsi Lambda yang didefinisikan untuk agregasi dan pemrosesan diberi nama `tumbling-window-example-function`.

```
aws lambda create-event-source-mapping \  
--event-source-arn arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream \  
--function-name tumbling-window-example-function \  
--starting-position TRIM_HORIZON \  
--tumbling-window-in-seconds 120
```

Lambda menentukan jatuh batas jendela berguling berdasarkan waktu ketika catatan dimasukkan ke dalam aliran. Semua catatan memiliki stempel waktu perkiraan yang tersedia yang digunakan Lambda dalam penentuan batas.

Agregasi jendela berguling tidak mendukung shard ulang. Ketika pecahan berakhir, Lambda menganggap jendela saat ini ditutup, dan setiap pecahan anak akan memulai jendela mereka sendiri dalam keadaan baru. Ketika tidak ada catatan baru yang ditambahkan ke jendela saat ini,

Lambda menunggu hingga 2 menit sebelum mengasumsikan bahwa jendela sudah selesai. Ini membantu memastikan bahwa fungsi membaca semua catatan di jendela saat ini, bahkan jika catatan ditambahkan sebentar-sebentar.

Jendela berguling sepenuhnya mendukung kebijakan coba lagi yang ada `maxRetryAttempts` dan `maxRecordAge`.

Example Handler.py - Agregasi dan pemrosesan

Fungsi Python berikut menunjukkan cara untuk menggabungkan, lalu memproses status akhir Anda:

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

    #Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
        print('Destination invoke')
    else:
        print('Aggregate invoke')

    #Check for early terminations
    if event['isWindowTerminatedEarly']:
        print('Window terminated early')

    #Aggregation logic
    state = event['state']
    for record in event['Records']:
        state[record['kinesis']['partitionKey']] = state.get(record['kinesis']
['partitionKey'], 0) + 1

    print('Returning state: ', state)
    return {'state': state}
```

Parameter Lambda untuk pemetaan sumber peristiwa Amazon Kinesis Data Streams

Semua pemetaan sumber acara Lambda berbagi hal yang sama dan operasi.

[CreateEventSourceMappingUpdateEventSourceMapping](#) API Namun, hanya beberapa parameter yang berlaku untuk Kinesis.

| Parameter | Diperlukan | Default | Catatan |
|--|------------|---------|---|
| BatchSize | T | 100 | Maksimum: 10.000. |
| BisectBatchOnFunctionError | T | false | none |
| DestinationConfig | T | N/A | SQSAntrian Amazon atau tujuan SNS topik Amazon untuk catatan yang dibuang. Untuk informasi selengkapnya, lihat Mengonfigurasi tujuan untuk pemanggilan yang gagal . |
| Diaktifkan | T | true | none |
| EventSourceArn | T | N/A | ARN dari aliran data atau konsumen aliran |
| FunctionName | T | N/A | none |
| FunctionResponseType | T | N/A | Agar fungsi Anda melaporkan kegagalan tertentu dalam satu batch, sertakan nilainya ReportBatchItemFailures FunctionResponseType. Untuk informasi selengkapnya, lihat Mengonfigurasi respons batch sebagian dengan |

| Parameter | Diperlukan | Default | Catatan |
|--|------------|---------|---|
| | | | Kinesis Data Streams dan Lambda . |
| MaximumBatchingWindowInSeconds | T | 0 | none |
| MaximumRecordAgeInSeconds | T | -1 | -1 berarti tak terbatas: Lambda tidak membuang catatan (pengaturan retensi data Kinesis Data Streams masih berlaku) Minimal: -1 Maksimal: 604.800 |
| MaximumRetryAttempts | T | -1 | -1 berarti tak terbatas: catatan gagal dicoba ulang sampai catatan kedaluwarsa Minimal: -1 Maksimum: 10.000. |
| ParallelizationFactor | T | 1 | Maksimal: 10 |
| StartingPosition | T | N/A | AT_TIMESTAMP, TRIM_HORIZON, atau LATEST |

| Parameter | Diperlukan | Default | Catatan |
|---|------------|---------|--|
| StartingPositionTimestamp | T | N/A | Hanya valid jika StartingPosition disetel ke AT_TIMESTAMP. Waktu untuk mulai membaca, dalam detik waktu Unix |
| TumblingWindowInSeconds | T | N/A | Minimal: 0 Maksimal: 900 |

Menggunakan pemfilteran acara dengan sumber acara Kinesis

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called “Penyaringan acara”](#).

Bagian ini berfokus pada penyaringan acara untuk sumber acara Kinesis.

Topik

- [Dasar-dasar penyaringan acara Kinesis](#)
- [Menyaring catatan agregat Kinesis](#)

Dasar-dasar penyaringan acara Kinesis

Misalkan produser memasukkan data JSON yang diformat ke dalam aliran data Kinesis Anda. Contoh catatan akan terlihat seperti berikut, dengan JSON data dikonversi ke string yang dikodekan Base64 di lapangan. data

```
{
  "kinesis": {
    "kinesisSchemaVersion": "1.0",
    "partitionKey": "1",
    "sequenceNumber": "49590338271490256608559692538361571095921575989136588898",
```

```

    "data":
      "eyJJSZWNvcnR0dWliZXIiOiAiMDAwMSIsICJJaWw1LU3RhbXAiOiAiAieXl5eS1tbS1kZFRoaDptbTpzcyIsICJSZXF1ZXN0Q
        "approximateArrivalTimestamp": 1545084650.987
      },
      "eventSource": "aws:kinesis",
      "eventVersion": "1.0",
      "eventID":
      "shardId-0000000000006:49590338271490256608559692538361571095921575989136588898",
      "eventName": "aws:kinesis:record",
      "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
      "awsRegion": "us-east-2",
      "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream"
    }
  }

```

Selama data yang dimasukkan produsen ke dalam aliran validJSON, Anda dapat menggunakan pemfilteran peristiwa untuk memfilter catatan menggunakan data kunci. Misalkan produser memasukkan catatan ke dalam aliran Kinesis Anda dalam format berikutJSON.

```

{
  "record": 12345,
  "order": {
    "type": "buy",
    "stock": "ANYCO",
    "quantity": 1000
  }
}

```

Untuk memfilter hanya catatan di mana jenis pesanan adalah “beli,” `FilterCriteria` objeknya adalah sebagai berikut.

```

{
  "Filters": [
    {
      "Pattern": "{ \"data\" : { \"order\" : { \"type\" : [ \"buy\" ] } } }"
    }
  ]
}

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```

{

```

```

    "data": {
      "order": {
        "type": [ "buy" ]
      }
    }
  }
}

```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "data" : { "order" : { "type" : [ "buy" ] } } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/my-stream \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type\" : [ \"buy\" ] } } }"}]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type\" : [ \"buy\" ] } } }"}]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
```

Filters:

```
- Pattern: '{ "data" : { "order" : { "type" : [ "buy" ] } } }'
```

Untuk memfilter peristiwa dengan benar dari sumber Kinesis, bidang data dan kriteria filter Anda untuk bidang data harus dalam format yang validJSON. Jika salah satu bidang tidak dalam JSON format yang valid, Lambda akan menghapus pesan atau melempar pengecualian. Tabel berikut merangkum perilaku spesifik:

| Format data masuk | Format pola filter untuk properti data | Tindakan yang dihasilkan |
|-------------------|---|--|
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Bukan- JSON | Lambda melempar pengecualian pada saat pembuatan atau pembaruan pemetaan sumber acara. Pola filter untuk properti data harus dalam JSON format yang valid. |
| Bukan- JSON | Valid JSON | Lambda menjatuhkan rekor. |
| Bukan- JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Bukan- JSON | Bukan- JSON | Lambda melempar pengecualian pada saat pembuatan atau pembaruan pemetaan sumber acara. Pola filter untuk |

| Format data masuk | Format pola filter untuk properti data | Tindakan yang dihasilkan |
|-------------------|--|---|
| | | properti data harus dalam JSON format yang valid. |

Menyaring catatan agregat Kinesis

Dengan Kinesis, Anda dapat menggabungkan beberapa catatan ke dalam satu catatan Kinesis Data Streams untuk meningkatkan throughput data Anda. [Lambda hanya dapat menerapkan kriteria filter ke rekaman agregat saat Anda menggunakan Kinesis yang ditingkatkan fan-out](#). Memfilter rekaman agregat dengan Kinesis standar tidak didukung. Saat menggunakan fan-out yang disempurnakan, Anda mengonfigurasi konsumen throughput khusus Kinesis untuk bertindak sebagai pemicu fungsi Lambda Anda. Lambda kemudian memfilter catatan agregat dan hanya meneruskan catatan yang memenuhi kriteria filter Anda.

Untuk mempelajari lebih lanjut tentang agregasi catatan Kinesis, lihat bagian [Agregasi](#) di halaman Konsep Kunci Perpustakaan Produsen Kinesis (). KPL Untuk mempelajari lebih lanjut tentang menggunakan Lambda dengan Kinesis yang ditingkatkan fan-out, lihat [Meningkatkan performa pemrosesan streaming real-time dengan Amazon Kinesis Data Streams yang disempurnakan oleh fan-out dan Lambda di blog komputasi](#). AWS AWS

Tutorial: Menggunakan Lambda dengan Kinesis Data Streams

Dalam tutorial ini, Anda membuat fungsi Lambda untuk mengkonsumsi peristiwa dari aliran data Amazon Kinesis.

1. Aplikasi kustom menulis rekaman ke aliran.
2. AWS Lambda polling aliran dan, ketika mendeteksi catatan baru dalam aliran, memanggil fungsi Lambda Anda.
3. AWS Lambda menjalankan fungsi Lambda dengan mengasumsikan peran eksekusi yang Anda tentukan pada saat Anda membuat fungsi Lambda.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```

Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (\) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh perintah CLI dalam panduan ini menggunakan pemformatan Linux. Perintah yang menyertakan dokumen JSON sebaris harus diformat ulang jika Anda menggunakan CLI Windows.

Buat peran eksekusi

Buat [peran eksekusi](#) yang memberikan izin fungsi Anda untuk mengakses AWS sumber daya.

Untuk membuat peran eksekusi

1. Buka [halaman peran](#) di konsol IAM.
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.

- Entitas tepercaya – AWS Lambda.
- Izin – AWSLambdaKinesisExecutionRole.
- Nama peran – **lambda-kinesis-role**.

AWSLambdaKinesisExecutionRoleKebijakan memiliki izin yang diperlukan fungsi untuk membaca item dari Kinesis dan menulis log ke Log CloudWatch .

Buat fungsi

Buat fungsi Lambda yang memproses pesan Kinesis Anda. Kode fungsi mencatat ID peristiwa dan data peristiwa dari catatan Kinesis ke CloudWatch Log.

Tutorial ini menggunakan runtime Node.js 18.x, tetapi kami juga menyediakan kode contoh dalam bahasa runtime lainnya. Anda dapat memilih tab di kotak berikut untuk melihat kode runtime yang Anda minati. JavaScript Kode yang akan Anda gunakan dalam langkah ini adalah pada contoh pertama yang ditunjukkan di JavaScripttab.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
into a .NET class.
```

```
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace KinesisIntegrationSampleCode;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
{record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
records.");
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
    }
}
```

```
    return data;
  }
}
```

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "log"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
    if len(kinesisEvent.Records) == 0 {
        log.Printf("empty Kinesis event received")
        return nil
    }

    for _, record := range kinesisEvent.Records {
        log.Printf("processed Kinesis event with EventId: %v", record.EventID)
        recordDataBytes := record.Kinesis.Data
        recordDataText := string(recordDataBytes)
        log.Printf("record data: %v", recordDataText)
        // TODO: Do interesting work based on the new data
    }
    log.Printf("successfully processed %v records", len(kinesisEvent.Records))
}
```

```
    return nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {
            logger.log("Empty Kinesis Event received");
            return null;
        }
        for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
            try {
                logger.log("Processed Event with EventId: "+record.getEventID());
                String data = new String(record.getKinesis().getData().array());
                logger.log("Data:"+ data);
            }
        }
    }
}
```

```
        // TODO: Do interesting work based on the new data
    }
    catch (Exception ex) {
        logger.log("An error occurred:"+ex.getMessage());
        throw ex;
    }
}
logger.log("Successfully processed:"+event.getRecords().size()+"
records");
return null;
}
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan menggunakan Lambda. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    for (const record of event.Records) {
        try {
            console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
            const recordData = await getRecordDataAsync(record.kinesis);
            console.log(`Record Data: ${recordData}`);
            // TODO: Do interesting work based on the new data
        } catch (err) {
            console.error(`An error occurred ${err}`);
            throw err;
        }
    }
    console.log(`Successfully processed ${event.Records.length} records.`);
}
```

```
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Mengonsumsi acara Kinesis dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      throw err;
    }
    logger.info(`Successfully processed ${event.Records.length} records.`);
  }
}
```

```
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }
}
```



```
}

/**
 * @throws JsonException
 * @throws \Bref\Event\InvalidLambdaEvent
 */
public function handleKinesis(KinesisEvent $event, Context $context): void
{
    $this->logger->info("Processing records");
    $records = $event->getRecords();
    foreach ($records as $record) {
        $data = $record->getData();
        $this->logger->info(json_encode($data));
        // TODO: Do interesting work based on the new data

        // Any exception thrown will be logged and the invocation will be
        marked as failed
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords records");
}

}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
```

```
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
end
```

```

end
puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
  here.
  return data
end

```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan Lambda menggunakan Rust.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
{
  if event.payload.records.is_empty() {
    tracing::info!("No records found. Exiting.");
    return Ok(());
  }

  event.payload.records.iter().for_each(|record| {
    tracing::info!("EventId:
    {}", record.event_id.as_deref().unwrap_or_default());

    let record_data = std::str::from_utf8(&record.kinesis.data);

```

```
        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
        time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Untuk membuat fungsi

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir kinesis-tutorial
cd kinesis-tutorial
```

2. Salin JavaScript kode sampel ke file baru bernama `index.js`.
3. Buat paket deployment.

```
zip function.zip index.js
```

4. Buat fungsi Lambda dengan perintah `create-function`.

```
aws lambda create-function --function-name ProcessKinesisRecords \  
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \  
--role arn:aws:iam::111122223333:role/lambda-kinesis-role
```

Uji fungsi Lambda

Panggil fungsi Lambda Anda secara manual menggunakan perintah `invoke` AWS Lambda CLI dan contoh peristiwa Kinesis.

Untuk menguji fungsi Lambda

1. Salin JSON berikut ke dalam file dan simpan sebagai `input.txt`.

```
{  
  "Records": [  
    {  
      "kinesis": {  
        "kinesisSchemaVersion": "1.0",  
        "partitionKey": "1",  
        "sequenceNumber":  
"49590338271490256608559692538361571095921575989136588898",  
        "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",  
        "approximateArrivalTimestamp": 1545084650.987  
      },  
      "eventSource": "aws:kinesis",  
      "eventVersion": "1.0",  
      "eventID":  
"shardId-000000000006:49590338271490256608559692538361571095921575989136588898",  
      "eventName": "aws:kinesis:record",  
      "invokeIdentityArn": "arn:aws:iam::111122223333:role/lambda-kinesis-  
role",  
      "awsRegion": "us-east-2",  
      "eventSourceARN": "arn:aws:kinesis:us-east-2:111122223333:stream/  
lambda-stream"  
    }  
  ]  
}
```

```
}
```

- Gunakan perintah `invoke` untuk mengirim kejadian ke fungsi.

```
aws lambda invoke --function-name ProcessKinesisRecords \  
--cli-binary-format raw-in-base64-out \  
--payload file://input.txt outputfile.txt
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Respons disimpan ke `out.txt`.

Buat aliran Kinesis

Gunakan perintah `create-stream` untuk membuat aliran.

```
aws kinesis create-stream --stream-name lambda-stream --shard-count 1
```

Jalankan perintah `describe-stream` berikut untuk mendapatkan ARN aliran.

```
aws kinesis describe-stream --stream-name lambda-stream
```

Anda akan melihat output berikut:

```
{  
  "StreamDescription": {  
    "Shards": [  
      {  
        "ShardId": "shardId-000000000000",  
        "HashKeyRange": {  
          "StartingHashKey": "0",  
          "EndingHashKey": "340282366920746074317682119384634633455"  
        },  
        "SequenceNumberRange": {  
          "StartingSequenceNumber":  
            "49591073947768692513481539594623130411957558361251844610"  
        }  
      ]  
    }  
  }  
}
```

```
    }
  ],
  "StreamARN": "arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream",
  "StreamName": "lambda-stream",
  "StreamStatus": "ACTIVE",
  "RetentionPeriodHours": 24,
  "EnhancedMonitoring": [
    {
      "ShardLevelMetrics": []
    }
  ],
  "EncryptionType": "NONE",
  "KeyId": null,
  "StreamCreationTimestamp": 1544828156.0
}
}
```

Anda menggunakan ARN aliran di langkah berikutnya untuk Anda mengasosiasikan aliran dengan fungsi Lambda Anda.

Tambahkan sumber peristiwa di AWS Lambda

Jalankan perintah AWS CLI `add-event-source` berikut.

```
aws lambda create-event-source-mapping --function-name ProcessKinesisRecords \
--event-source arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream \
--batch-size 100 --starting-position LATEST
```

Catat ID pemetaan untuk penggunaan selanjutnya. Anda bisa mendapatkan daftar pemetaan sumber kejadian dengan menjalankan perintah `list-event-source-mappings`.

```
aws lambda list-event-source-mappings --function-name ProcessKinesisRecords \
--event-source arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream
```

Dalam respons, Anda dapat memverifikasi nilai status adalah `enabled`. Pemetaan sumber peristiwa dapat dinonaktifkan untuk menjeda polling sementara tanpa kehilangan catatan.

Uji penyiapan

Untuk menguji pemetaan sumber kejadian, tambahkan rekaman kejadian ke aliran Kinesis Anda. Nilai `--data` adalah string yang diekodekan CLI ke base64 sebelum mengirimkannya ke Kinesis.

Anda dapat menjalankan perintah yang sama lebih dari satu kali untuk menambahkan beberapa rekaman ke aliran.

```
aws kinesys put-record --stream-name lambda-stream --partition-key 1 \  
--data "Hello, this is a test."
```

Lambda menggunakan peran eksekusi untuk membaca rekaman dari aliran. Kemudian, itu akan memanggil fungsi Lambda Anda, dengan mengirimkan batch rekaman. Fungsi ini menerjemahkan data dari setiap catatan dan mencatatnya, mengirimkan output ke CloudWatch Log. Lihat log di [konsol CloudWatch](#).

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus aliran Kinesis

1. [Masuk ke AWS Management Console dan buka konsol Kinesis di https://console.aws.amazon.com/kinesis.](https://console.aws.amazon.com/kinesis)
2. Pilih aliran yang Anda buat.
3. Pilih Tindakan, Hapus.

4. Masukkan **delete** di bidang input teks.
5. Pilih Hapus.

Menggunakan Lambda dengan Amazon MQ

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Amazon MQ adalah layanan broker pesan terkelola untuk [Apache ActiveMQ](#) dan [RabbitMQ](#). Broker pesan memungkinkan aplikasi dan komponen perangkat lunak untuk berkomunikasi menggunakan berbagai bahasa pemrograman, sistem operasi, dan protokol pesan formal baik melalui topik atau tujuan acara antrian.

Amazon MQ juga dapat mengelola instans Amazon Elastic Compute Cloud (AmazonEC2) atas nama Anda dengan menginstal broker ActiveMQ atau RabbitMQ dan dengan menyediakan berbagai topologi jaringan dan kebutuhan infrastruktur lainnya.

Anda dapat menggunakan fungsi Lambda untuk memproses rekaman dari broker pesan Amazon MQ Anda. [Lambda memanggil fungsi Anda melalui pemetaan sumber peristiwa, sumber daya Lambda yang membaca pesan dari broker Anda dan memanggil fungsi secara serempak.](#)

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Pemetaan sumber kejadian Amazon MQ memiliki pembatasan konfigurasi berikut:

- [Konkurensi - Fungsi Lambda yang menggunakan pemetaan sumber peristiwa Amazon MQ memiliki pengaturan konkurensi maksimum default.](#) Untuk ActiveMQ, layanan Lambda membatasi jumlah lingkungan eksekusi bersamaan hingga lima per pemetaan sumber peristiwa Amazon MQ. Untuk RabbitMQ, jumlah lingkungan eksekusi bersamaan dibatasi hingga 1 per pemetaan sumber peristiwa Amazon MQ. Bahkan jika Anda mengubah setelan konkurensi yang dicadangkan atau disediakan fungsi, layanan Lambda tidak akan membuat lebih banyak lingkungan eksekusi

tersedia. Untuk meminta peningkatan konkurensi maksimum default untuk satu pemetaan sumber peristiwa Amazon MQ, AWS Support hubungi UUID pemetaan sumber peristiwa, serta wilayah. Karena peningkatan diterapkan pada tingkat pemetaan sumber peristiwa tertentu, bukan tingkat akun atau wilayah, Anda perlu meminta peningkatan penskalaan secara manual untuk setiap pemetaan sumber peristiwa.

- Lintas akun — Lambda tidak mendukung pemrosesan lintas akun. Anda tidak dapat menggunakan Lambda untuk memproses catatan dari broker pesan Amazon MQ yang berbeda. Akun AWS
- Otentikasi - Untuk ActiveMQ, hanya ActiveMQ yang didukung. [SimpleAuthenticationPlugin](#) Untuk RabbitMQ, hanya mekanisme [PLAIN](#) otentikasi yang didukung. Pengguna harus menggunakan AWS Secrets Manager untuk mengelola kredensialnya. Untuk informasi selengkapnya tentang otentikasi ActiveMQ, lihat [Mengintegrasikan broker ActiveMQ dengan Panduan Pengembang Amazon MQ](#). LDAP
- Kuota koneksi – Broker memiliki jumlah maksimum koneksi yang diizinkan untuk setiap protokol wire-level. Kuota ini didasarkan pada jenis instans broker. Untuk informasi lebih lanjut, lihat bagian [Broker](#) dari Kuota di Amazon MQ dalam Panduan Developer Amazon MQ.
- Konektivitas — Anda dapat membuat broker di cloud pribadi virtual publik atau pribadi (VPC). Untuk pribadiVPCs, fungsi Lambda Anda memerlukan akses ke VPC untuk menerima pesan. Untuk informasi lebih lanjut, lihat [the section called “Konfigurasi akses jaringan”](#) nanti di bagian ini.
- Tujuan kejadian – Hanya tujuan antrean yang didukung. Namun, Anda dapat menggunakan topik virtual, yang berfungsi sebagai topik secara internal sambil berinteraksi dengan Lambda sebagai antrean. Untuk informasi lebih lanjut, lihat [Tujuan Virtual](#) di situs web Apache ActiveMQ, [dan Host Virtual](#) di situs web RabbitMQ.
- Topologi jaringan - Untuk ActiveMQ, hanya satu broker tunggal atau siaga yang didukung per pemetaan sumber peristiwa. Untuk RabbitMQ, hanya satu broker instans tunggal atau penerapan kluster yang didukung per pemetaan sumber peristiwa. Broker instans tunggal memerlukan titik akhir failover. Untuk informasi selengkapnya tentang mode penyebaran broker ini, lihat [Arsitektur Broker MQ Aktif dan Arsitektur Broker MQ Kelinci di Panduan Pengembang Amazon MQ](#).
- Protokol — Protokol yang didukung bergantung pada jenis integrasi Amazon MQ.
 - Untuk integrasi ActiveMQ, Lambda menggunakan pesan menggunakan OpenWire protokol / Java Message Service (). JMS Tidak ada protokol lain yang didukung untuk mengkonsumsi pesan. Dalam JMS protokol, hanya [TextMessage](#) dan [BytesMessage](#) didukung. Lambda juga mendukung properti JMS kustom. Untuk informasi lebih lanjut tentang OpenWire protokol, lihat [OpenWire](#) di situs web Apache ActiveMQ.

- Untuk integrasi RabbitMQ, Lambda mengkonsumsi pesan menggunakan protokol 0-9-1. AMQP Tidak ada protokol lain yang didukung untuk mengkonsumsi pesan. Untuk informasi lebih lanjut tentang implementasi protokol 0-9-1 RabbitMQ, lihat AMQP [AMQP0-9-1 Panduan Referensi Lengkap](#) di situs web RabbitMQ.

Lambda secara otomatis mendukung versi terbaru ActiveMQ dan RabbitMQ yang didukung Amazon MQ. Untuk versi terbaru yang didukung, lihat [catatan rilis Amazon MQ di Panduan Pengembang Amazon MQ](#).

Note

Secara default, Amazon MQ memiliki jangka waktu pemeliharaan mingguan untuk broker. Selama jangka waktu tersebut, broker tidak tersedia. Untuk broker tanpa standby, Lambda tidak dapat memproses pesan apa pun selama jangka waktu tersebut.

Topik

- [Memahami grup konsumen Lambda untuk Amazon MQ](#)
- [Memproses pesan Amazon MQ dengan Lambda](#)
- [Parameter pemetaan sumber peristiwa](#)
- [Filter peristiwa dari sumber acara Amazon MQ](#)
- [Memecahkan masalah kesalahan pemetaan sumber peristiwa Amazon MQ](#)

Memahami grup konsumen Lambda untuk Amazon MQ

Untuk berinteraksi dengan Amazon MQ, Lambda membuat grup konsumen yang dapat membaca dari broker Amazon MQ Anda. Grup konsumen dibuat dengan ID yang sama dengan pemetaan UUID sumber peristiwa.

Untuk sumber peristiwa Amazon MQ, Lambda mengumpulkan catatan bersama dan mengirimkannya ke fungsi Anda dalam satu muatan. Untuk mengontrol perilaku, Anda dapat mengonfigurasi jendela batching dan ukuran batch. Lambda menarik pesan hingga memproses ukuran muatan maksimum 6 MB, jendela batching kedaluwarsa, atau jumlah catatan mencapai ukuran batch penuh. Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Grup konsumen mengambil pesan sebagai BLOB byte, base64-mengkodekannya menjadi satu JSON muatan, dan kemudian memanggil fungsi Anda. Jika fungsi Anda mengembalikan kesalahan untuk salah satu pesan dalam batch, Lambda mencoba ulang seluruh batch pesan sampai berhasil diproses atau pesan berakhir.

Note

Sementara fungsi Lambda biasanya memiliki batas waktu tunggu maksimum 15 menit, pemetaan sumber acara untuk Amazon, Apache Kafka yang dikelola sendiri, MSK Amazon DocumentDB, dan Amazon MQ untuk ActiveMQ dan RabbitMQ hanya mendukung fungsi dengan batas waktu tunggu maksimum 14 menit. Kendala ini memastikan bahwa pemetaan sumber peristiwa dapat menangani kesalahan fungsi dan percobaan ulang dengan benar.

Anda dapat memantau penggunaan konkurensi fungsi tertentu menggunakan `ConcurrentExecutions` metrik di Amazon CloudWatch. Untuk informasi selengkapnya tentang konkurensi, lihat [the section called “Mengonfigurasi konkurensi terpesan”](#).

Example Acara rekam Amazon MQ

ActiveMQ

```
{
  "eventSource": "aws:mq",
  "eventSourceArn": "arn:aws:mq:us-east-2:111122223333:broker:test:b-9bcfa592-423a-4942-879d-eb284b418fc8",
  "messages": [
    {
      "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
      "messageType": "jms/text-message",
      "deliveryMode": 1,
      "replyTo": null,
      "type": null,
      "expiration": "60000",
      "priority": 1,
      "correlationId": "myJMScoID",
      "redelivered": false,
      "destination": {
        "physicalName": "testQueue"
      }
    },
  ],
}
```

```

    "data": "QUJD0kFBQUE=",
    "timestamp": 1598827811958,
    "brokerInTime": 1598827811958,
    "brokerOutTime": 1598827811959,
    "properties": {
      "index": "1",
      "doAlarm": "false",
      "myCustomProperty": "value"
    }
  },
  {
    "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
    "messageType": "jms/bytes-message",
    "deliveryMode": 1,
    "replyTo": null,
    "type": null,
    "expiration": "60000",
    "priority": 2,
    "correlationId": "myJMScoID1",
    "redelivered": false,
    "destination": {
      "physicalName": "testQueue"
    },
    "data": "LQaGQ82S48k=",
    "timestamp": 1598827811958,
    "brokerInTime": 1598827811958,
    "brokerOutTime": 1598827811959,
    "properties": {
      "index": "1",
      "doAlarm": "false",
      "myCustomProperty": "value"
    }
  }
]
}

```

RabbitMQ

```

{
  "eventSource": "aws:rmq",

```

```
"eventSourceArn": "arn:aws:mq:us-east-2:111122223333:broker:pizzaBroker:b-9bcfa592-423a-4942-879d-eb284b418fc8",
"rmqMessagesByQueue": {
  "pizzaQueue:./": [
    {
      "basicProperties": {
        "contentType": "text/plain",
        "contentEncoding": null,
        "headers": {
          "header1": {
            "bytes": [
              118,
              97,
              108,
              117,
              101,
              49
            ]
          },
          "header2": {
            "bytes": [
              118,
              97,
              108,
              117,
              101,
              50
            ]
          },
          "numberInHeader": 10
        },
        "deliveryMode": 1,
        "priority": 34,
        "correlationId": null,
        "replyTo": null,
        "expiration": "60000",
        "messageId": null,
        "timestamp": "Jan 1, 1970, 12:33:41 AM",
        "type": null,
        "userId": "AIDACKCEVSQ6C2EXAMPLE",
        "appId": null,
        "clusterId": null,
        "bodySize": 80
      },

```

```
    "redelivered": false,
    "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
  }
]
}
}
```

Note

Dalam contoh RabbitMQ, `pizzaQueue` adalah nama antrian RabbitMQ, dan `/` merupakan nama host virtual. Saat menerima pesan, sumber acara mencantumkan pesan di `bawahpizzaQueue::/`.

Memproses pesan Amazon MQ dengan Lambda

Topik

- [Konfigurasi akses jaringan](#)
- [Buat pemetaan sumber acara](#)

Konfigurasi akses jaringan

Untuk memberi Lambda akses penuh ke broker Anda melalui pemetaan sumber acara Anda, broker Anda harus menggunakan titik akhir publik (alamat IP publik), atau Anda harus memberikan akses ke Amazon tempat VPC Anda membuat broker.

Secara default, saat Anda membuat broker Amazon MQ, `PubliclyAccessible` bendera disetel ke `false`. Agar broker Anda menerima alamat IP publik, Anda harus mengatur `PubliclyAccessible` bendera ke `true`.

Praktik terbaik untuk menggunakan Amazon MQ dengan Lambda adalah dengan menggunakan AWS PrivateLink [VPCtitik akhir](#) dan memberikan akses fungsi Lambda Anda ke broker Anda. VPC Terapkan titik akhir untuk Lambda, dan, hanya untuk ActiveMQ, titik akhir untuk (). AWS Security Token Service AWS STS Jika broker Anda menggunakan otentikasi, gunakan juga titik akhir untuk AWS Secrets Manager Untuk mempelajari selengkapnya, lihat [the section called "Siapkan titik VPC akhir Amazon"](#).

Atau, konfigurasi NAT gateway di setiap subnet publik di yang VPC berisi broker Amazon MQ Anda. Untuk informasi selengkapnya, lihat [the section called “Akses internet untuk VPC fungsi”](#).

Saat Anda membuat pemetaan sumber acara untuk broker Amazon MQ, Lambda memeriksa apakah Antarmuka Jaringan Elastis ENIs () sudah ada untuk subnet dan grup keamanan broker Anda. VPC Jika Lambda menemukan yang ada ENIs, ia mencoba untuk menggunakannya kembali. Jika tidak, Lambda membuat yang baru ENIs untuk terhubung ke sumber acara dan memanggil fungsi Anda.

Note

Fungsi Lambda selalu berjalan di dalam yang VPCs dimiliki oleh layanan Lambda. Ini VPCs dikelola secara otomatis oleh layanan dan tidak terlihat oleh pelanggan. Anda juga dapat menghubungkan fungsi Anda ke Amazon VPC. Dalam kedua kasus tersebut, VPC konfigurasi fungsi Anda tidak memengaruhi pemetaan sumber peristiwa. Hanya konfigurasi sumber acara yang VPC menentukan bagaimana Lambda terhubung ke sumber acara Anda.

Mengonfigurasi aturan grup keamanan

Konfigurasi grup keamanan untuk Amazon yang VPC berisi Amazon MQ Anda.

Note

Secara default, Amazon MQ untuk ActiveMQ menggunakan port, dan 61617 Amazon MQ untuk port RabbitMQ. 5671

- Aturan masuk - Izinkan semua lalu lintas di port broker untuk grup keamanan yang terkait dengan sumber acara Anda dari dalam grup keamanannya sendiri.
- Aturan keluar - Izinkan semua lalu lintas di pelabuhan 443 untuk semua tujuan. Izinkan semua lalu lintas di port broker dari dalam grup keamanannya sendiri.
- Aturan masuk VPC titik akhir Amazon — Untuk grup keamanan yang terkait dengan VPC titik akhir Amazon Anda, izinkan lalu lintas masuk di port 443 dari grup keamanan broker

Siapkan titik VPC akhir Amazon

Saat Anda menggunakan VPC endpoint Amazon, AWS merutekan API panggilan Anda untuk menjalankan fungsi menggunakan Elastic Network Interface () titik akhir. ENI Kepala layanan Lambda

perlu memanggil `lambda:InvokeFunction` fungsi apa pun yang menggunakannya. ENIs Selain itu, untuk Amazon MQ untuk ActiveMQ, prinsipal layanan Lambda harus bekerja pada peran yang menggunakan `sts:AssumeRole` ENIs

Secara default, VPC titik akhir Amazon memiliki IAM kebijakan terbuka yang memungkinkan akses luas ke sumber daya. Untuk menggunakan Amazon MQ dengan Lambda dalam produksi, Anda dapat membatasi kebijakan ini untuk hanya mengizinkan prinsipal tertentu untuk hanya mengakses peran dan fungsi tertentu.

Contoh kebijakan VPC endpoint berikut menunjukkan cara memberikan akses yang diperlukan untuk AWS STS dan titik akhir Lambda.

Example Kebijakan titik akhir - AWS STS titik akhir (hanya ActiveMQ)

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "arn:aws::iam::123456789012:role/my-role"
    }
  ]
}
```

Example Kebijakan titik akhir — Titik akhir Lambda

```
{
  "Statement": [
    {
      "Action": "lambda:InvokeFunction",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "arn:aws::lambda:us-west-2:123456789012:function:my-function"
    }
  ]
}
```

```

    }
  ]
}

```

Jika broker Amazon MQ Anda menggunakan otentikasi, Anda juga dapat membatasi kebijakan titik akhir untuk titik akhir Secrets Manager. Untuk memanggil Secrets Manager API, Lambda menggunakan peran fungsi Anda, bukan kepala layanan Lambda. Contoh berikut menunjukkan kebijakan titik akhir Secrets Manager.

Example VPCkebijakan endpoint — titik akhir Secrets Manager

```

{
  "Statement": [
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws::iam::123456789012:role/my-role"
        ]
      },
      "Resource": "arn:aws::secretsmanager:us-west-2:123456789012:secret:my-secret"
    }
  ]
}

```

Warning

Membatasi kebijakan titik akhir Anda untuk hanya mengizinkan API panggilan yang berasal dari organisasi Anda mencegah pemetaan sumber peristiwa berfungsi dengan baik.


Buat pemetaan sumber acara

Buat [pemetaan sumber kejadian](#) untuk memberi tahu Lambda agar mengirim rekaman dari broker Amazon MQ ke fungsi Lambda. Anda dapat membuat beberapa pemetaan sumber kejadian untuk memproses data yang sama dengan beberapa fungsi, atau untuk memproses item dari beberapa sumber dengan satu fungsi.

Untuk mengonfigurasi fungsi agar dibaca dari Amazon MQ, tambahkan izin yang diperlukan dan buat pemicu MQ di konsol Lambda.

Untuk membaca catatan dari broker Amazon MQ, fungsi Lambda Anda memerlukan izin berikut. [Anda memberi Lambda izin untuk berinteraksi dengan broker Amazon MQ Anda dan sumber yang mendasarinya dengan menambahkan pernyataan izin ke peran eksekusi fungsi Anda:](#)

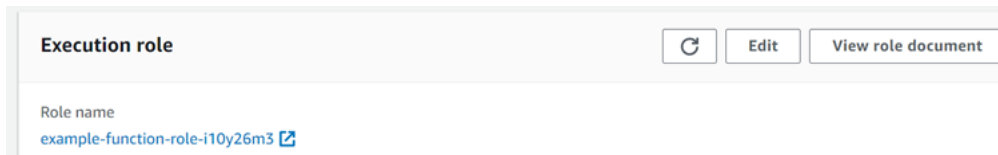
- [mq: DescribeBroker](#)
- [manajer rahasia: GetSecretValue](#)
- [EC2: CreateNetworkInterface](#)
- [EC2: DeleteNetworkInterface](#)
- [EC2: DescribeNetworkInterfaces](#)
- [EC2: DescribeSecurityGroups](#)
- [EC2: DescribeSubnets](#)
- [EC2: DescribeVpcs](#)
- [log: CreateLogGroup](#)
- [log: CreateLogStream](#)
- [log: PutLogEvents](#)

 Note

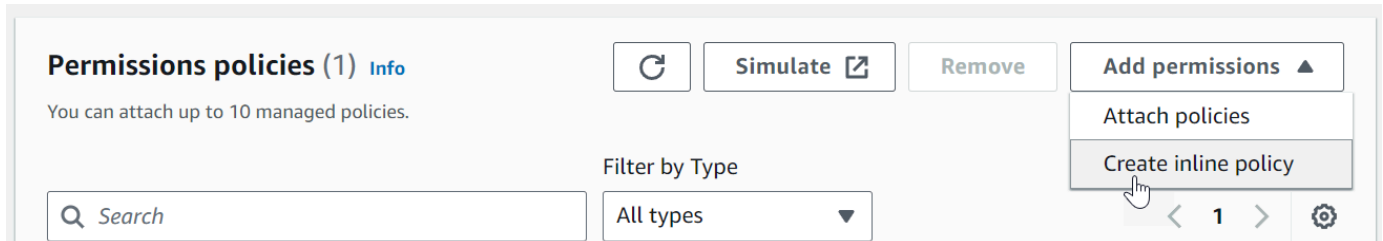
Saat menggunakan kunci terkelola pelanggan yang terenkripsi, tambahkan juga izin [kms:Decrypt](#).

Untuk menambahkan izin dan membuat pemicu

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih tab Konfigurasi, lalu pilih Izin.
4. Di bawah Nama peran, pilih tautan ke peran eksekusi Anda. Tautan ini membuka peran di IAM konsol.



5. Pilih Tambahkan izin, lalu pilih Buat kebijakan sebaris.



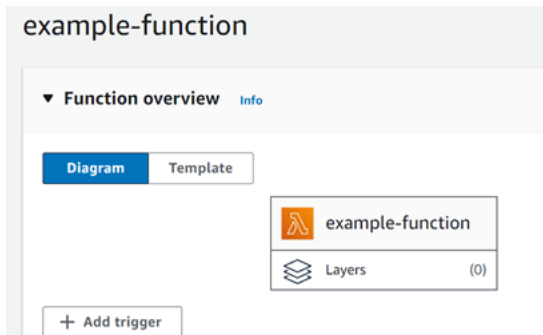
6. Di editor Kebijakan, pilih JSON. Masukkan kebijakan berikut. Fungsi Anda memerlukan izin ini untuk membaca dari broker Amazon MQ.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mq:DescribeBroker",
        "secretsmanager:GetSecretValue",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

Saat menggunakan kunci terkelola pelanggan terenkripsi, Anda juga harus menambahkan izin. `kms :Decrypt`

7. Pilih Berikutnya. Masukkan nama kebijakan, lalu pilih Buat kebijakan.
8. Kembali ke fungsi Anda di konsol Lambda. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.



9. Pilih jenis pemicu MQ.
10. Konfigurasi opsi yang diperlukan, lalu pilih Tambah.

Lambda mendukung opsi berikut untuk sumber kejadian Amazon MQ:

- MQ broker – Pilih broker Amazon MQ.
- Ukuran batch – Atur jumlah maksimum pesan yang akan diambil dalam satu batch.
- Nama antrean – Masukkan antrean Amazon MQ yang akan digunakan.
- Konfigurasi akses sumber — Masukkan informasi host virtual dan rahasia Secrets Manager yang menyimpan kredensi broker Anda.
- Aktifkan pemicu – Nonaktifkan pemicu untuk menghentikan pemrosesan rekaman.

Untuk mengaktifkan atau menonaktifkan pemicu (atau menghapusnya) pilih pemicu MQ di desainer. Untuk mengkonfigurasi ulang pemicu, gunakan operasi pemetaan API sumber peristiwa.

Parameter pemetaan sumber peristiwa

Semua jenis sumber acara Lambda berbagi hal yang sama [CreateEventSourceMapping](#) dan [UpdateEventSourceMapping](#) API operasi. Namun, hanya beberapa parameter yang berlaku untuk Amazon MQ dan RabbitMQ.

| Parameter | Diperlukan | Default | Catatan |
|--------------------------------|------------|---------|---|
| BatchSize | T | 100 | Maksimum: 10.000. |
| Diaktifkan | T | true | none |
| FunctionName | T | N/A | none |
| FilterCriteria | T | N/A | Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda |
| MaximumBatchingWindowInSeconds | T | 500 ms | Perilaku batching |
| Antrean | T | N/A | Nama antrean tujuan broker Amazon MQ yang akan digunakan. |
| SourceAccessConfigurations | T | N/A | Untuk ActiveMQ, _ BASIC kredensial. AUTH Untuk RabbitMQ, dapat berisi BASIC _ AUTH kredensi dan _ informasi. VIRTUAL HOST |

Filter peristiwa dari sumber acara Amazon MQ

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called "Penyaringan acara"](#).

Bagian ini berfokus pada pemfilteran acara untuk sumber acara Amazon MQ.

Topik

- [Dasar-dasar penyaringan acara Amazon MQ](#)

Dasar-dasar penyaringan acara Amazon MQ

Misalkan antrian pesan Amazon MQ Anda berisi pesan baik dalam JSON format yang valid atau sebagai string biasa. Contoh catatan akan terlihat seperti berikut, dengan data dikonversi ke string yang dikodekan Base64 di lapangan. data

ActiveMQ

```
{
  "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-east-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
  "messageType": "jms/text-message",
  "deliveryMode": 1,
  "replyTo": null,
  "type": null,
  "expiration": "60000",
  "priority": 1,
  "correlationId": "myJMScoID",
  "redelivered": false,
  "destination": {
    "physicalName": "testQueue"
  },
  "data": "QUJD0kFBQUE=",
  "timestamp": 1598827811958,
  "brokerInTime": 1598827811958,
  "brokerOutTime": 1598827811959,
  "properties": {
    "index": "1",
    "doAlarm": "false",
    "myCustomProperty": "value"
  }
}
```



```
}  
}
```

RabbitMQ

```
{  
  "basicProperties": {  
    "contentType": "text/plain",  
    "contentEncoding": null,  
    "headers": {  
      "header1": {  
        "bytes": [  
          118,  
          97,  
          108,  
          117,  
          101,  
          49  
        ]  
      },  
      "header2": {  
        "bytes": [  
          118,  
          97,  
          108,  
          117,  
          101,  
          50  
        ]  
      },  
      "numberInHeader": 10  
    },  
    "deliveryMode": 1,  
    "priority": 34,  
    "correlationId": null,  
    "replyTo": null,  
    "expiration": "60000",  
    "messageId": null,  
    "timestamp": "Jan 1, 1970, 12:33:41 AM",  
    "type": null,  
    "userId": "AIDACKCEVSQ6C2EXAMPLE",  
    "appId": null,  
    "clusterId": null,  
  },  
}
```

```

    "bodySize": 80
  },
  "redelivered": false,
  "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
}

```

Untuk broker MQ Aktif dan MQ Kelinci, Anda dapat menggunakan penyaringan acara untuk memfilter catatan menggunakan kunci. data Misalkan antrian Amazon MQ Anda berisi pesan dalam format berikut. JSON

```

{
  "timeout": 0,
  "IPAddress": "203.0.113.254"
}

```

Untuk memfilter hanya catatan yang timeout bidangnya lebih besar dari 0, FilterCriteria objeknya adalah sebagai berikut.

```

{
  "Filters": [
    {
      "Pattern": "{ \"data\" : { \"timeout\" : [ { \"numeric\" : [ \">\",
0] ] } ] } }"
    }
  ]
}

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```

{
  "data": {
    "timeout": [ { "numeric": [ ">", 0 ] } ]
  }
}

```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-  
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :  
[ { \"numeric\": [ \">\", 0 ] } ] } }"]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :  
[ { \"numeric\": [ \">\", 0 ] } ] } }"]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :  
[ { \"numeric\": [ \">\", 0 ] } ] } }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
```

Filters:

```
- Pattern: '{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }'
```

Dengan Amazon MQ, Anda juga dapat memfilter catatan di mana pesan adalah string biasa. Misalkan Anda hanya ingin memproses catatan di mana pesan dimulai dengan “Hasil:”. `FilterCriteriaObjek` akan terlihat sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"data\" : [ { \"prefix\": \"Result: \" } ] }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```
{
  "data": [
    {
      "prefix": "Result: "
    }
  ]
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "data" : [ { "prefix": "Result: " } ] }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
```

```
--event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-  
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \  
--filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":  
\"Result: \" } ] }"]}]'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \  
--uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \  
--filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":  
\"Result: \" } ] }"]}]'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:  
  Filters:  
    - Pattern: '{ "data" : [ { "prefix": "Result " } ] }'
```

Pesan Amazon MQ harus berupa UTF -8 string yang dikodekan, baik string biasa atau dalam format JSON. Itu karena Lambda menerjemahkan array byte Amazon MQ menjadi UTF -8 sebelum menerapkan kriteria filter. Jika pesan Anda menggunakan pengkodean lain, seperti UTF -16 atau ASCII, atau jika format pesan tidak cocok dengan format, Lambda FilterCriteria hanya memproses filter metadata. Tabel berikut merangkum perilaku spesifik:

| Format pesan masuk | Format pola filter untuk properti pesan | Tindakan yang dihasilkan |
|--------------------|---|--|
| Tali polos | Tali polos | Filter Lambda berdasarkan kriteria filter Anda. |
| Tali polos | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |

| Format pesan masuk | Format pola filter untuk properti pesan | Tindakan yang dihasilkan |
|------------------------------------|---|--|
| Tali polos | Valid JSON | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tali polos | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |
| String yang tidak dikodekan UTF -8 | JSON, string polos, atau tidak ada pola | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |

Memecahkan masalah kesalahan pemetaan sumber peristiwa Amazon MQ

Ketika fungsi Lambda mengalami kesalahan yang tidak dapat dipulihkan, konsumen Amazon MQ Anda menghentikan pemrosesan rekaman. Konsumen lain dapat melanjutkan pemrosesan, asalkan mereka tidak mengalami kesalahan yang sama. Untuk menentukan kemungkinan penyebab dari konsumen yang dihentikan, periksa bidang `StateTransitionReason` dalam detail pengembalian `EventSourceMapping` untuk salah satu kode berikut:

ESM_CONFIG_NOT_VALID

Konfigurasi pemetaan sumber kejadian tidak valid.

EVENT_SOURCE_AUTHN_ERROR

Lambda gagal mengautentikasi sumber kejadian.

EVENT_SOURCE_AUTHZ_ERROR

Lambda tidak memiliki izin yang diperlukan untuk mengakses sumber kejadian.

FUNCTION_CONFIG_NOT_VALID

Konfigurasi fungsi tidak valid.

Catatan juga tidak diproses jika Lambda menjatuhkannya karena ukurannya. Batas ukuran untuk rekaman Lambda adalah 6 MB. Untuk mengirim ulang pesan setelah kesalahan fungsi, Anda dapat menggunakan antrean huruf mati (DLQ). Untuk informasi selengkapnya, lihat [Pengiriman Ulang Pesan dan DLQ Penanganan](#) di situs web Apache ActiveMQ dan Panduan [Keandalan](#) di situs web RabbitMQ.

Note

Lambda tidak mendukung kebijakan pengiriman ulang khusus. Sebagai gantinya, Lambda menggunakan kebijakan dengan nilai default dari halaman [Kebijakan Pengiriman Ulang di situs](#) web Apache ActiveMQ, dengan disetel ke 6. `maximumRedeliveries`

Menggunakan Lambda dengan Amazon MSK

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

[Amazon Managed Streaming for Apache Kafka \(MSKAmazon\)](#) adalah layanan terkelola penuh yang dapat Anda gunakan untuk membangun dan menjalankan aplikasi yang menggunakan Apache Kafka untuk memproses data streaming. Amazon MSK menyederhanakan penyiapan, penskalaan, dan pengelolaan cluster yang menjalankan Kafka. Amazon MSK juga mempermudah konfigurasi aplikasi Anda untuk beberapa Availability Zone dan untuk keamanan dengan AWS Identity and Access Management (IAM). Amazon MSK mendukung beberapa versi open-source Kafka.

Amazon MSK sebagai sumber acara beroperasi mirip dengan menggunakan Amazon Simple Queue Service (AmazonSQS) atau Amazon Kinesis. Lambda melakukan polling secara internal untuk pesan baru dari sumber peristiwa, lalu memanggil fungsi Lambda target secara sinkron. Lambda membaca pesan dalam batch dan menyediakan ini untuk fungsi Anda sebagai muatan acara. Ukuran batch maksimum dapat dikonfigurasi (defaultnya adalah 100 pesan). Untuk informasi selengkapnya, lihat [Perilaku batching](#).

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Untuk contoh cara mengonfigurasi Amazon MSK sebagai sumber peristiwa, lihat [Menggunakan Amazon MSK sebagai sumber peristiwa AWS Lambda](#) di Blog AWS Komputasi. Untuk tutorial selengkapnya, lihat [Integrasi Amazon MSK Lambda](#) di Amazon MSK Labs.

Topik

- [Contoh peristiwa](#)
- [Mengonfigurasi sumber MSK acara Amazon untuk Lambda](#)

- [Memproses MSK pesan Amazon dengan Lambda](#)
- [Menggunakan pemfilteran acara dengan sumber MSK acara Amazon](#)
- [Menangkap batch yang dibuang untuk sumber acara Amazon MSK](#)
- [Tutorial: Menggunakan pemetaan sumber MSK peristiwa Amazon untuk menjalankan fungsi Lambda](#)

Contoh peristiwa

Lambda mengirimkan batch pesan dalam parameter peristiwa ketika memanggil fungsi Anda. Muatan peristiwa berisi array pesan. Setiap item array berisi detail MSK topik Amazon dan pengidentifikasi partisi, bersama dengan stempel waktu dan pesan yang disandikan base64.

```
{
  "eventSource": "aws:kafka",
  "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
  "bootstrapServers": "b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
  "records": {
    "mytopic-0": [
      {
        "topic": "mytopic",
        "partition": 0,
        "offset": 15,
        "timestamp": 1545084650987,
        "timestampType": "CREATE_TIME",
        "key": "abcDEFghiJKLmnoPQRstuVWXYZ1234==",
        "value": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
        "headers": [
          {
            "headerKey": [
              104,
              101,
              97,
              100,
              101,
              114,
              86,
              97,
              108,
            ]
          }
        ]
      }
    ]
  }
}
```

```
        117,  
        101  
    ]  
  }  
] }  
] }  
] }  
] }  
}
```

Mengonfigurasi sumber MSK acara Amazon untuk Lambda

Sebelum Anda membuat pemetaan sumber peristiwa untuk MSK klaster Amazon Anda, Anda perlu memastikan bahwa klaster Anda dan tempat VPC tinggalnya telah dikonfigurasi dengan benar. Anda juga perlu memastikan bahwa [peran eksekusi fungsi Lambda Anda memiliki izin](#) yang diperlukan IAM.

Ikuti petunjuk di bagian berikut untuk mengonfigurasi MSK klaster Amazon, VPC, dan fungsi Lambda. Untuk mempelajari cara membuat pemetaan sumber peristiwa, lihat [the section called “Menambahkan Amazon MSK sebagai sumber acara”](#).

Topik

- [MSK otentikasi cluster](#)
- [Mengelola API akses dan izin](#)
- [Kesalahan otentikasi dan otorisasi](#)
- [Konfigurasi jaringan](#)

MSK otentikasi cluster

Lambda memerlukan izin untuk mengakses MSK klaster Amazon, mengambil catatan, dan melakukan tugas lainnya. Amazon MSK mendukung beberapa opsi untuk mengontrol akses klien ke MSK cluster.

Opsi akses cluster

- [Akses tidak diautentikasi](#)
- [SASL/SCRAM otentikasi](#)
- [IAM otentikasi berbasis peran](#)
- [TLS otentikasi timbal balik](#)

- [Mengkonfigurasi rahasia m TLS](#)
- [Bagaimana Lambda memilih broker bootstrap](#)

Akses tidak diautentikasi

Jika tidak ada klien yang mengakses cluster melalui internet, Anda dapat menggunakan akses yang tidak diautentikasi.

SASL/SCRAMotentikasi

Amazon MSK mendukung otentikasi Simple Authentication and Security Layer/Salted Challenge Response Authentication Mechanism (SASL/SCRAM) otentikasi dengan enkripsi Transport Layer Security (). TLS Agar Lambda dapat terhubung ke cluster, Anda menyimpan kredensi otentikasi (nama pengguna dan kata sandi) secara rahasia. AWS Secrets Manager

Untuk informasi selengkapnya tentang menggunakan Secrets Manager, lihat [Autentikasi nama pengguna dan kata sandi dengan AWS Secrets Manager](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

Amazon MSK tidak mendukungSASL/PLAINotentikasi.

IAMotentikasi berbasis peran

Anda dapat menggunakan IAM untuk mengautentikasi identitas klien yang terhubung ke MSK cluster. Jika IAM auth aktif di MSK cluster Anda, dan Anda tidak memberikan rahasia untuk autentikasi, Lambda secara otomatis default menggunakan auth. IAM Untuk membuat dan menerapkan kebijakan berbasis pengguna atau peran, gunakan konsol atau IAM API Untuk informasi selengkapnya, lihat [kontrol IAM akses](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[Untuk mengizinkan Lambda terhubung ke MSK klaster, membaca catatan, dan melakukan tindakan lain yang diperlukan, tambahkan izin berikut ke peran eksekusi fungsi Anda.](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeGroup",
```

```

        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeClusterDynamicConfiguration"
    ],
    "Resource": [
        "arn:aws:kafka:region:account-id:cluster/cluster-name/cluster-uuid",
        "arn:aws:kafka:region:account-id:topic/cluster-name/cluster-uuid/topic-
name",
        "arn:aws:kafka:region:account-id:group/cluster-name/cluster-
uuid/consumer-group-id"
    ]
}
]
}

```

Anda dapat membuat cakupan izin ini ke klaster, topik, dan grup tertentu. Untuk informasi selengkapnya, lihat [tindakan Amazon MSK Kafka di Panduan Pengembang Amazon Managed Streaming for Apache Kafka](#).

TLS Otentikasi timbal balik

Mutual TLS (mTLS) menyediakan otentikasi dua arah antara klien dan server. Klien mengirimkan sertifikat ke server untuk server untuk memverifikasi klien, dan server mengirimkan sertifikat ke klien untuk klien untuk memverifikasi server.

Untuk AmazonMSK, Lambda bertindak sebagai klien. Anda mengonfigurasi sertifikat klien (sebagai rahasia di Secrets Manager) untuk mengautentikasi Lambda dengan broker di MSK klaster Anda. Sertifikat klien harus ditandatangani oleh CA di toko kepercayaan server. MSKCluster mengirimkan sertifikat server ke Lambda untuk mengautentikasi broker dengan Lambda. Sertifikat server harus ditandatangani oleh otoritas sertifikat (CA) yang ada di toko AWS kepercayaan.

Untuk petunjuk tentang cara membuat sertifikat klien, lihat [Memperkenalkan TLS autentikasi timbal balik untuk Amazon MSK sebagai sumber peristiwa](#).

Amazon MSK tidak mendukung sertifikat server yang ditandatangani sendiri, karena semua broker di Amazon MSK menggunakan [sertifikat publik](#) yang ditandatangani oleh [Amazon Trust Services CAs](#), yang dipercaya Lambda secara default.

Untuk informasi selengkapnya tentang m TLS untuk AmazonMSK, lihat [TLS Otentikasi Bersama](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka Kafka.

Mengkonfigurasi rahasia m TLS

AUTHRahasia CLIENT CERTIFICATE TLS __ memerlukan bidang sertifikat dan bidang kunci pribadi. Untuk kunci pribadi terenkripsi, rahasianya memerlukan kata sandi kunci pribadi. Baik sertifikat dan kunci pribadi harus dalam PEM format.

Note

Lambda mendukung [PBES1](#)(tetapi tidakPBES2) algoritma enkripsi kunci pribadi.

Bidang sertifikat harus berisi daftar sertifikat, dimulai dengan sertifikat klien, diikuti oleh sertifikat perantara, dan diakhiri dengan sertifikat root. Setiap sertifikat harus dimulai pada baris baru dengan struktur berikut:

```
-----BEGIN CERTIFICATE-----
    <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager mendukung rahasia hingga 65.536 byte, yang merupakan ruang yang cukup untuk rantai sertifikat yang panjang.

Kunci pribadi harus dalam format [PKCS#8](#), dengan struktur berikut:

```
-----BEGIN PRIVATE KEY-----
    <private key contents>
-----END PRIVATE KEY-----
```

Untuk kunci pribadi terenkripsi, gunakan struktur berikut:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
    <private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

Contoh berikut menunjukkan isi rahasia untuk m TLS otentikasi menggunakan kunci pribadi terenkripsi. Untuk kunci pribadi terenkripsi, Anda menyertakan kata sandi kunci pribadi dalam rahasia.

```
{
  "privateKeyPassword": "testpassword",
```

```

"certificate": "-----BEGIN CERTIFICATE-----
MII5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPim040s1cRqtFHxoa10QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFGjCCA2qgAwIBAgIQdJNZd6uFf9hbNC5RdfmHrzANBgkqhkiG9w0BAQsFADBb
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
-----END CERTIFICATE-----",
"privateKey": "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDANBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzg09IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}

```

Bagaimana Lambda memilih broker bootstrap

Lambda memilih [broker bootstrap](#) berdasarkan metode otentikasi yang tersedia di cluster Anda, dan apakah Anda memberikan rahasia untuk otentikasi. Jika Anda memberikan rahasia untuk mTLS atau SASL/SCRAM, Lambda secara otomatis memilih metode autentikasi itu. Jika Anda tidak memberikan rahasia, Lambda memilih metode autentikasi terkuat yang aktif di cluster Anda. Berikut ini adalah urutan prioritas di mana Lambda memilih broker, dari autentikasi terkuat hingga terlemah:

- mTLS (rahasia disediakan untuk mTLS)
- SASL/SCRAM (rahasia disediakan untuk SASL/SCRAM)
- SASLIAM (tidak ada rahasia yang disediakan, dan IAM autentikasi aktif)
- Tidak diautentikasi TLS (tidak ada rahasia yang disediakan, dan IAM autentikasi tidak aktif)
- Plaintext (tidak ada rahasia yang diberikan, dan autentikasi dan tidak IAM diautentikasi tidak aktif TLS)

Note

Jika Lambda tidak dapat terhubung ke jenis broker yang paling aman, Lambda tidak mencoba untuk terhubung ke jenis broker yang berbeda (lebih lemah). Jika Anda ingin

Lambda memilih jenis broker yang lebih lemah, nonaktifkan semua metode autentikasi yang lebih kuat di cluster Anda.

Mengelola API akses dan izin

Selain mengakses MSK klaster Amazon, fungsi Anda memerlukan izin untuk melakukan berbagai tindakan Amazon MSK API. Anda menambahkan izin ini ke peran eksekusi fungsi. Jika pengguna Anda memerlukan akses ke salah satu MSK API tindakan Amazon, tambahkan izin yang diperlukan ke kebijakan identitas untuk pengguna atau peran.

Anda dapat menambahkan setiap izin berikut ke peran eksekusi Anda secara manual. Atau, Anda dapat melampirkan kebijakan AWS terkelola [AWSLambdaMSKExecutionRole](#) ke peran eksekusi Anda. `AWSLambdaMSKExecutionRole` kebijakan ini berisi semua API tindakan dan VPC izin yang diperlukan yang tercantum di bawah ini.

Izin peran eksekusi fungsi Lambda yang diperlukan

Untuk membuat dan menyimpan log dalam grup log di Amazon CloudWatch Logs, fungsi Lambda Anda harus memiliki izin berikut dalam peran pelaksanaannya:

- [log: CreateLogGroup](#)
- [log: CreateLogStream](#)
- [log: PutLogEvents](#)

Agar Lambda dapat mengakses MSK klaster Amazon Anda atas nama Anda, fungsi Lambda Anda harus memiliki izin berikut dalam peran pelaksanaannya:

- [kafka: DescribeCluster](#)
- [kafka: DescribeCluster V2](#)
- [kafka: GetBootstrapBrokers](#)
- [kafka: DescribeVpcConnection](#): Hanya diperlukan untuk pemetaan [sumber acara lintas akun](#).
- [kafka: ListVpcConnections](#): Tidak diperlukan dalam peran eksekusi, tetapi diperlukan untuk IAM prinsipal yang membuat pemetaan [sumber peristiwa lintas akun](#).

Anda hanya perlu menambahkan salah satu `kafka:DescribeCluster` atau `kafka:DescribeClusterV2`. Untuk MSK cluster yang disediakan, salah satu izin berfungsi. Untuk MSK cluster tanpa server, Anda harus menggunakan `kafka:DescribeClusterV2`

Note

Lambda akhirnya berencana untuk menghapus `kafka:DescribeCluster` izin dari kebijakan `AWSLambdaMSKExecutionRole` terkelola terkait. Jika Anda menggunakan kebijakan ini, Anda harus memigrasikan aplikasi apa pun yang digunakan `kafka:DescribeCluster` untuk digunakan `kafka:DescribeClusterV2`.

VPC izin

Jika hanya pengguna dalam a yang VPC dapat mengakses MSK kluster Amazon Anda, fungsi Lambda Anda harus memiliki izin untuk mengakses sumber daya Amazon VPC Anda. Sumber daya ini termasuk Anda VPC, subnet, grup keamanan, dan antarmuka jaringan. Untuk mengakses sumber daya ini, peran eksekusi fungsi Anda harus memiliki izin berikut. Izin ini disertakan dalam kebijakan [AWSLambdaMSKExecutionRole](#) AWS terkelola.

- [EC2: CreateNetworkInterface](#)
- [EC2: DescribeNetworkInterfaces](#)
- [EC2: DescribeVpcs](#)
- [EC2: DeleteNetworkInterface](#)
- [EC2: DescribeSubnets](#)
- [EC2: DescribeSecurityGroups](#)

Izin fungsi Lambda opsional

Fungsi Lambda Anda mungkin juga memerlukan izin untuk:

- Akses SCRAM rahasia Anda, jika menggunakan SASL/SCRAM otentikasi.
- Jelaskan rahasia Secrets Manager Anda.
- Akses AWS Key Management Service (AWS KMS) kunci terkelola pelanggan Anda.
- Kirim catatan pemanggilan yang gagal ke tujuan.

Secrets Manager dan AWS KMS izin

Bergantung pada jenis kontrol akses yang Anda konfigurasi untuk MSK broker Amazon Anda, fungsi Lambda Anda mungkin memerlukan izin untuk mengakses rahasia Anda (jika SASL menggunakan SCRAM/otentikasi), atau rahasia Secrets Manager untuk mendekripsi AWS KMS kunci yang dikelola pelanggan SCRAM Anda. Untuk mengakses sumber daya ini, peran eksekusi fungsi Anda harus memiliki izin berikut:

- [kafka: ListScramSecrets](#)
- [manajer rahasia: GetSecretValue](#)
- [kms:Decrypt](#)

Menambahkan izin ke peran eksekusi

Ikuti langkah-langkah berikut untuk menambahkan kebijakan AWS terkelola [AWSLambdaMSKExecutionRole](#) ke peran eksekusi Anda menggunakan IAM konsol.

Untuk menambahkan kebijakan AWS terkelola

1. Buka [halaman Kebijakan](#) IAM konsol.
2. Dalam kotak pencarian kebijakan, masukkan nama kebijakan (`AWSLambdaMSKExecutionRole`).
3. Pilih kebijakan dari daftar, lalu pilih Tindakan kebijakan, Lampirkan.
4. Di halaman Lampirkan kebijakan, pilih peran eksekusi Anda dari daftar, lalu pilih Lampirkan kebijakan.

Memberikan akses kepada pengguna dengan kebijakan IAM

Secara default, pengguna dan peran tidak memiliki izin untuk melakukan MSK API operasi Amazon. Untuk memberikan akses ke pengguna di organisasi atau akun Anda, Anda dapat menambahkan atau memperbarui kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat [Contoh Kebijakan MSK Berbasis Identitas Amazon di Panduan Pengembang](#) Amazon Managed Streaming for Apache Kafka.

Kesalahan otentikasi dan otorisasi

Jika salah satu izin yang diperlukan untuk mengkonsumsi data dari MSK klaster Amazon tidak ada, Lambda menampilkan salah satu pesan galat berikut dalam pemetaan sumber peristiwa di bawah. LastProcessingResult

Pesan kesalahan

- [Cluster gagal mengotorisasi Lambda](#)
- [SASLotentikasi gagal](#)
- [Server gagal mengautentikasi Lambda](#)
- [Sertifikat atau kunci pribadi yang diberikan tidak valid](#)

Cluster gagal mengotorisasi Lambda

Untuk SASL/SCRAM atau mTLS, kesalahan ini menunjukkan bahwa pengguna yang disediakan tidak memiliki semua izin daftar kontrol akses (ACL) Kafka yang diperlukan berikut:

- DescribeConfigs Cluster
- Jelaskan Grup
- Baca Grup
- Jelaskan Topik
- Baca Topik

Untuk kontrol IAM akses, peran eksekusi fungsi Anda tidak memiliki satu atau beberapa izin yang diperlukan untuk mengakses grup atau topik. Tinjau daftar izin yang diperlukan di [the section called "IAM otentikasi berbasis peran"](#).

Saat Anda membuat Kafka ACLs atau IAM kebijakan dengan izin klaster Kafka yang diperlukan, tentukan topik dan kelompokkan sebagai sumber daya. Nama topik harus cocok dengan topik dalam pemetaan sumber acara. Nama grup harus cocok dengan pemetaan sumber acara. UUID

Setelah Anda menambahkan izin yang diperlukan ke peran eksekusi, mungkin perlu beberapa menit agar perubahan diterapkan.

SASLotentikasi gagal

Untuk SASL/SCRAM, kesalahan ini menunjukkan bahwa nama pengguna dan kata sandi yang diberikan tidak valid.

Untuk kontrol IAM akses, peran eksekusi tidak memiliki `kafka-cluster:Connect` izin untuk MSK cluster. Tambahkan izin ini ke peran dan tentukan Amazon Resource Name (ARN) cluster sebagai sumber daya.

Anda mungkin melihat kesalahan ini terjadi sebentar-sebentar. Cluster menolak koneksi setelah jumlah TCP koneksi melebihi [kuota MSK layanan Amazon](#). Lambda mundur dan mencoba lagi sampai koneksi berhasil. Setelah Lambda terhubung ke cluster dan polling untuk catatan, hasil pemrosesan terakhir berubah menjadi. OK

Server gagal mengautentikasi Lambda

Kesalahan ini menunjukkan bahwa broker Amazon MSK Kafka gagal mengautentikasi dengan Lambda. Ini dapat terjadi karena salah satu alasan berikut:

- Anda tidak memberikan sertifikat klien untuk TLS otentikasi m.
- Anda memberikan sertifikat klien, tetapi broker tidak dikonfigurasi untuk menggunakan mTLS.
- Sertifikat klien tidak dipercaya oleh broker.

Sertifikat atau kunci pribadi yang diberikan tidak valid

Kesalahan ini menunjukkan bahwa MSK konsumen Amazon tidak dapat menggunakan sertifikat atau kunci pribadi yang disediakan. Pastikan bahwa sertifikat dan PEM format penggunaan kunci, dan bahwa enkripsi kunci pribadi menggunakan PBES1 algoritma.

Konfigurasi jaringan

Agar Lambda dapat menggunakan cluster Kafka Anda sebagai sumber peristiwa, Lambda memerlukan akses ke Amazon tempat klaster VPC Anda berada. Kami menyarankan Anda menerapkan AWS PrivateLink [VPCtitik akhir](#) untuk Lambda untuk mengakses Anda. VPC Terapkan titik akhir untuk Lambda dan (). AWS Security Token Service AWS STS Jika broker menggunakan otentikasi, gunakan juga VPC endpoint untuk Secrets Manager. Jika Anda mengonfigurasi [tujuan saat kegagalan](#), gunakan juga VPC titik akhir untuk layanan tujuan.

Atau, pastikan bahwa yang VPC terkait dengan cluster Kafka Anda mencakup satu NAT gateway per subnet publik. Untuk informasi selengkapnya, lihat [the section called “Akses internet untuk VPC fungsi”](#).

Jika Anda menggunakan VPC titik akhir, Anda juga harus mengonfigurasinya untuk [mengaktifkan DNS nama pribadi](#).

Saat Anda membuat pemetaan sumber peristiwa untuk MSK klaster, Lambda memeriksa apakah Elastic Network Interfaces ENIs () sudah ada untuk subnet dan grup keamanan klaster Anda. VPC Jika Lambda menemukan yang ada ENIs, ia mencoba untuk menggunakannya kembali. Jika tidak, Lambda membuat yang baru ENIs untuk terhubung ke sumber acara dan memanggil fungsi Anda.

Note

Fungsi Lambda selalu berjalan di dalam yang VPCs dimiliki oleh layanan Lambda. Ini VPCs dikelola secara otomatis oleh layanan dan tidak terlihat oleh pelanggan. Anda juga dapat menghubungkan fungsi Anda ke Amazon VPC. Dalam kedua kasus tersebut, VPC konfigurasi fungsi Anda tidak memengaruhi pemetaan sumber peristiwa. Hanya konfigurasi sumber acara yang VPC menentukan bagaimana Lambda terhubung ke sumber acara Anda.

VPC [Konfigurasi Amazon Anda dapat ditemukan melalui Amazon. MSK API](#) Anda tidak perlu mengkonfigurasinya selama pengaturan menggunakan `create-event-source-mapping` perintah.

Untuk informasi selengkapnya tentang mengonfigurasi jaringan, lihat [Menyiapkan AWS Lambda dengan cluster Apache Kafka VPC di dalam Blog Komputasi AWS](#) .

VPC aturan kelompok keamanan

Konfigurasi grup keamanan untuk Amazon VPC yang berisi klaster Anda dengan aturan berikut (minimal):

- Aturan masuk - Izinkan semua lalu lintas di port MSK broker Amazon (9092 untuk teks biasa, 9094 untuk TLS, 9096 untuk SASL, 9098 untuk IAM) untuk SASL grup keamanan yang ditentukan untuk sumber acara Anda.
- Aturan keluar - Izinkan semua lalu lintas di port 443 untuk semua tujuan. Izinkan semua lalu lintas di port MSK broker Amazon (9092 untuk teks biasa, 9094 untuk TLS, 9096 untuk TLSSASL, 9098 untuk IAM) untuk grup keamanan yang ditentukan untuk sumber acara Anda.
- Jika Anda menggunakan VPC titik akhir alih-alih NAT gateway, grup keamanan yang terkait dengan VPC titik akhir harus mengizinkan semua lalu lintas masuk pada port 443 dari grup keamanan sumber acara.

Bekerja dengan titik VPC akhir

Saat Anda menggunakan VPC titik akhir, API panggilan untuk memanggil fungsi Anda dirutekan melalui titik akhir ini menggunakan ENIs Kepala layanan Lambda perlu memanggil

`sts:AssumeRole` dan `lambda:InvokeFunction` pada peran dan fungsi apa pun yang menggunakannya. ENIs

Secara default, VPC titik akhir memiliki IAM kebijakan yang terbuka. Praktik terbaik adalah membatasi kebijakan ini untuk memungkinkan hanya prinsipal tertentu untuk melakukan tindakan yang diperlukan menggunakan titik akhir itu. Untuk memastikan bahwa pemetaan sumber peristiwa Anda dapat menjalankan fungsi Lambda Anda, kebijakan VPC titik akhir harus mengizinkan prinsip layanan Lambda untuk memanggil dan. `sts:AssumeRole` `lambda:InvokeFunction` Membatasi kebijakan VPC titik akhir Anda untuk mengizinkan hanya API panggilan yang berasal dari organisasi Anda mencegah pemetaan sumber peristiwa berfungsi dengan baik.

Contoh kebijakan VPC endpoint berikut menunjukkan cara memberikan akses yang diperlukan ke prinsipal layanan Lambda untuk titik akhir AWS STS dan Lambda.

Example VPCkebijakan titik akhir - AWS STS titik akhir

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "*"
    }
  ]
}
```

Example VPCkebijakan titik akhir - Titik akhir Lambda

```
{
  "Statement": [
    {
      "Action": "lambda:InvokeFunction",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      }
    }
  ]
}
```

```

    },
    "Resource": "*"
  }
]
}

```

Jika broker Kafka Anda menggunakan otentikasi, Anda juga dapat membatasi kebijakan VPC titik akhir untuk titik akhir Secrets Manager. Untuk memanggil Secrets Manager API, Lambda menggunakan peran fungsi Anda, bukan kepala layanan Lambda. Contoh berikut menunjukkan kebijakan titik akhir Secrets Manager.

Example VPC kebijakan endpoint - titik akhir Secrets Manager

```

{
  "Statement": [
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "customer_function_execution_role_arn"
        ]
      },
      "Resource": "customer_secret_arn"
    }
  ]
}

```

Jika Anda memiliki tujuan pada kegagalan yang dikonfigurasi, Lambda juga menggunakan peran fungsi Anda untuk memanggil `s3:PutObject` salah satu `sns:Publish`, `sqs:sendMessage` atau menggunakan Lambda-managed. ENIs

Memproses MSK pesan Amazon dengan Lambda

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Topik

- [Menambahkan Amazon MSK sebagai sumber acara](#)
- [Parameter MSK konfigurasi Amazon](#)
- [Membuat pemetaan sumber peristiwa lintas akun](#)
- [Menggunakan MSK klaster Amazon sebagai sumber acara](#)
- [Posisi awal polling dan streaming](#)
- [CloudWatch Metrik Amazon](#)
- [Penskalaan otomatis sumber MSK acara Amazon](#)

Menambahkan Amazon MSK sebagai sumber acara

[Untuk membuat pemetaan sumber peristiwa, tambahkan Amazon MSK sebagai pemicu fungsi Lambda menggunakan konsol Lambda, AWS SDKsebuah, atau \(\).AWS Command Line InterfaceAWS CLI](#) Perhatikan bahwa saat Anda menambahkan Amazon MSK sebagai pemicu, Lambda mengasumsikan VPC pengaturan MSK klaster Amazon, bukan pengaturan fungsi Lambda. VPC

Bagian ini menjelaskan cara membuat pemetaan sumber peristiwa menggunakan konsol Lambda dan AWS CLI.

Prasyarat

- MSKCluster Amazon dan topik Kafka. Untuk informasi selengkapnya, lihat [Memulai Menggunakan Amazon MSK](#) di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.
- [Peran eksekusi](#) dengan izin untuk mengakses AWS sumber daya yang digunakan MSK klaster Anda.

ID grup konsumen yang dapat disesuaikan

Saat mengatur Kafka sebagai sumber acara, Anda dapat menentukan ID grup konsumen. ID grup konsumen ini adalah pengenal yang ada untuk grup konsumen Kafka yang Anda inginkan agar fungsi Lambda Anda bergabung. Anda dapat menggunakan fitur ini untuk memigrasikan pengaturan pemrosesan catatan Kafka yang sedang berlangsung dengan mulus dari konsumen lain ke Lambda.

Jika Anda menentukan ID grup konsumen dan ada poller aktif lainnya dalam grup konsumen tersebut, Kafka mendistribusikan pesan ke semua konsumen. Dengan kata lain, Lambda tidak menerima semua pesan untuk topik Kafka. Jika Anda ingin Lambda menangani semua pesan dalam topik, matikan poller lain di grup konsumen tersebut.

Selain itu, jika Anda menentukan ID grup konsumen, dan Kafka menemukan grup konsumen yang sudah ada yang valid dengan ID yang sama, Lambda mengabaikan parameter untuk `StartingPosition` pemetaan sumber peristiwa Anda. Sebaliknya, Lambda mulai memproses catatan sesuai dengan offset yang dilakukan dari kelompok konsumen. Jika Anda menentukan ID grup konsumen, dan Kafka tidak dapat menemukan grup konsumen yang ada, maka Lambda mengonfigurasi sumber acara Anda dengan yang ditentukan. `StartingPosition`

ID grup konsumen yang Anda tentukan harus unik di antara semua sumber acara Kafka Anda. Setelah membuat pemetaan sumber acara Kafka dengan ID grup konsumen yang ditentukan, Anda tidak dapat memperbarui nilai ini.

Menambahkan MSK pemicu Amazon (konsol)

Ikuti langkah-langkah berikut untuk menambahkan MSK klaster Amazon dan topik Kafka sebagai pemicu fungsi Lambda Anda.

Untuk menambahkan MSK pemicu Amazon ke fungsi Lambda Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi Lambda Anda.
3. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.
4. Pada Konfigurasi pemicu, lakukan hal berikut:
 - a. Pilih jenis MSKpemicu.
 - b. Untuk MSKcluster, pilih cluster Anda.
 - c. Untuk Ukuran batch, masukkan jumlah maksimum pesan yang akan diterima dalam satu batch.
 - d. Untuk jendela Batch, masukkan jumlah maksimum detik yang dihabiskan Lambda untuk mengumpulkan catatan sebelum menjalankan fungsi.
 - e. Untuk Nama topik, masukkan nama topik Kafka.
 - f. (Opsional) Untuk ID grup Konsumen, masukkan ID grup konsumen Kafka untuk bergabung.
 - g. (Opsional) Untuk posisi Mulai, pilih Terbaru untuk mulai membaca aliran dari catatan terbaru, Potong cakrawala untuk memulai pada catatan paling awal yang tersedia, atau Pada stempel waktu untuk menentukan stempel waktu untuk mulai membaca.
 - h. (Opsional) Untuk Otentikasi, pilih kunci rahasia untuk otentikasi dengan broker di cluster AndaMSK.

- i. Untuk membuat pemacu dalam status nonaktif untuk pengujian (disarankan), hapus Aktifkan pemacu. Atau, untuk segera mengaktifkan pemacu, pilih Aktifkan pemacu.
5. Untuk membuat pemacu, pilih Tambahkan.

Menambahkan MSK pemacu Amazon (AWS CLI)

Gunakan contoh AWS CLI perintah berikut untuk membuat dan melihat MSK pemacu Amazon untuk fungsi Lambda Anda.

Membuat pemacu menggunakan AWS CLI

Example — Buat pemetaan sumber acara untuk cluster yang menggunakan IAM otentikasi

Contoh berikut menggunakan [create-event-source-mapping](#) AWS CLI perintah untuk memetakan fungsi Lambda bernama `my-kafka-function` ke topik Kafka bernama `AWSKafkaTopic`. Posisi awal topik diatur ke `LATEST`. Saat cluster menggunakan [otentikasi IAM berbasis peran](#), Anda tidak memerlukan objek [SourceAccessConfiguration](#). Contoh:

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
```

Example — Buat pemetaan sumber acara untuk cluster yang SASL SCRAM menggunakan/otentikasi

Jika cluster menggunakan [SASL/SCRAMotentikasi](#), Anda harus menyertakan [SourceAccessConfiguration](#) objek yang menentukan `SASL_SCRAM_512_AUTH` dan rahasia Secrets Manager. ARN

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH", "URI":
"arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Example — Buat pemetaan sumber acara untuk cluster yang menggunakan otentikasi m TLS

Jika klaster menggunakan [TLSotentikasi m](#), Anda harus menyertakan

[SourceAccessConfiguration](#) objek yang menentukan CLIENT_CERTIFICATE_TLS_AUTH dan rahasia Secrets Manager. ARN

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-
fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH", "URI":
"arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Untuk informasi selengkapnya, lihat dokumentasi [CreateEventSourceMapping](#) API referensi.

Melihat status menggunakan AWS CLI

Contoh berikut menggunakan [get-event-source-mapping](#) AWS CLI perintah untuk menggambarkan status pemetaan sumber peristiwa yang Anda buat.

```
aws lambda get-event-source-mapping \
  --uuid 6d9bce8e-836b-442c-8070-74e77903c815
```

Parameter MSK konfigurasi Amazon

Semua jenis sumber acara Lambda berbagi hal yang sama [CreateEventSourceMapping](#) dan [UpdateEventSourceMapping](#) API operasi. Namun, hanya beberapa parameter yang berlaku untuk AmazonMSK.

| Parameter | Diperlukan | Default | Catatan |
|-------------------------------------|------------|--|--------------------------------|
| AmazonManagedKafkaEventSourceConfig | T | Berisi ConsumerGroupID bidang, yang default ke nilai unik. | Hanya dapat mengatur di Create |
| BatchSize | T | 100 | Maksimum: 10.000. |
| Diaktifkan | N | Diaktifkan | none |

| Parameter | Diperlukan | Default | Catatan |
|--------------------------------|------------|----------------------|--|
| EventSourceArn | T | N/A | Hanya dapat mengatur di Create |
| FunctionName | T | N/A | none |
| FilterCriteria | T | N/A | Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda |
| MaximumBatchingWindowInSeconds | T | 500 ms | Perilaku batching |
| SourceAccessConfigurations | T | Tidak ada kredensial | SASL/SCRAM atau CLIENT_CERTIFICATE_TLS_AUTH (Mutual TLS) kredensial otentikasi untuk sumber acara Anda |
| StartingPosition | T | N/A | AT_TIMESTAMP, TRIM_HORIZON, atau LATEST Hanya dapat mengatur di Create |
| StartingPositionTimestamp | T | N/A | Diperlukan jika StartingPosition disetel ke AT_TIMESTAMP |
| Topik | T | N/A | Nama topik Kafka Hanya dapat mengatur di Create |

Membuat pemetaan sumber peristiwa lintas akun

Anda dapat menggunakan [konektivitas VPC multi-pribadi](#) untuk menghubungkan fungsi Lambda ke MSK kluster yang disediakan di tempat yang berbeda. Akun AWS Penggunaan VPC multi-konektivitas AWS PrivateLink, yang menjaga semua lalu lintas dalam AWS jaringan.

Note

Anda tidak dapat membuat pemetaan sumber peristiwa lintas akun untuk kluster tanpa server. MSK

Untuk membuat pemetaan sumber peristiwa lintas akun, Anda harus terlebih dahulu [mengonfigurasi VPC multi-konektivitas untuk kluster](#). MSK Saat Anda membuat pemetaan sumber peristiwa, gunakan VPC koneksi terkelola ARN alih-alih klusterARN, seperti yang ditunjukkan pada contoh berikut. [CreateEventSourceMapping](#) Operasi juga berbeda tergantung pada jenis otentikasi yang digunakan MSK cluster.

Example — Buat pemetaan sumber peristiwa lintas akun untuk cluster yang menggunakan otentikasi IAM

Saat cluster menggunakan [otentikasi IAM berbasis peran](#), Anda tidak memerlukan objek. [SourceAccessConfiguration](#) Contoh:

```
aws lambda create-event-source-mapping \  
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/  
  my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \  
  --topics AWSKafkaTopic \  
  --starting-position LATEST \  
  --function-name my-kafka-function
```

Example — Buat pemetaan sumber peristiwa lintas akun untuk cluster yang SASL menggunakan/otentikasi SCRAM

Jika cluster menggunakan [SASL/SCRAMotentikasi](#), Anda harus menyertakan [SourceAccessConfiguration](#) objek yang menentukan SASL_SCRAM_512_AUTH dan rahasia Secrets Manager. ARN

Ada dua cara untuk menggunakan rahasia untuk pemetaan sumber MSK peristiwa Amazon lintas akun dengan SASL/otentikasi: SCRAM

- Buat rahasia di akun fungsi Lambda dan sinkronkan dengan rahasia cluster. [Buat rotasi](#) untuk menjaga kedua rahasia tetap sinkron. Opsi ini memungkinkan Anda untuk mengontrol rahasia dari akun fungsi.
- Gunakan rahasia yang terkait dengan MSK cluster. Rahasia ini harus memungkinkan akses lintas akun ke akun fungsi Lambda. Untuk informasi [selengkapnya, lihat Izin untuk AWS Secrets Manager](#) rahasia bagi pengguna di akun lain.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
  my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH", "URI":
  "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Example — Buat pemetaan sumber peristiwa lintas akun untuk cluster yang menggunakan otentikasi m TLS

Jika klaster menggunakan [TLSootentikasi m](#), Anda harus menyertakan [SourceAccessConfiguration](#) objek yang menentukan CLIENT_CERTIFICATE_TLS_AUTH dan rahasia Secrets Manager. ARN Rahasiannya dapat disimpan di akun cluster atau akun fungsi Lambda.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
  my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH", "URI":
  "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Menggunakan MSK klaster Amazon sebagai sumber acara

[Saat Anda menambahkan Apache Kafka atau MSK klaster Amazon sebagai pemicu fungsi Lambda Anda, cluster digunakan sebagai sumber peristiwa.](#)

Lambda membaca data peristiwa dari topik Kafka yang Anda tentukan seperti `Topics` dalam [CreateEventSourceMapping](#) permintaan, berdasarkan `StartingPosition` yang Anda tentukan. Setelah pemrosesan berhasil, topik Kafka Anda dijalankan untuk kluster Kafka Anda.

Jika Anda menentukan `StartingPosition` sebagai `LATEST`, Lambda mulai membaca dari pesan terbaru di setiap partisi milik topik. Karena mungkin ada beberapa penundaan setelah konfigurasi pemicu sebelum Lambda mulai membaca pesan, Lambda tidak membaca pesan apa pun yang dihasilkan selama jendela ini.

Lambda membaca pesan secara berurutan untuk setiap partisi topik Kafka. Payload Lambda tunggal dapat berisi pesan dari beberapa partisi. Bila lebih banyak rekaman tersedia, Lambda terus memproses catatan dalam batch, berdasarkan `BatchSize` nilai yang Anda tentukan dalam [CreateEventSourceMapping](#) permintaan, hingga fungsi Anda mengikuti topik.

Setelah Lambda memproses setiap batch, Lambda melakukan offset pesan dalam batch tersebut. Jika fungsi Anda mengembalikan kesalahan untuk salah satu pesan dalam batch, Lambda mencoba ulang seluruh batch pesan sampai berhasil diproses atau pesan berakhir. Anda dapat mengirim catatan yang gagal dalam semua upaya percobaan ulang ke [tujuan yang gagal untuk diproses](#) nanti.

Note

Sementara fungsi Lambda biasanya memiliki batas waktu tunggu maksimum 15 menit, pemetaan sumber acara untuk Amazon, Apache Kafka yang dikelola sendiri, MSK Amazon DocumentDB, dan Amazon MQ untuk ActiveMQ dan RabbitMQ hanya mendukung fungsi dengan batas waktu tunggu maksimum 14 menit. Kendala ini memastikan bahwa pemetaan sumber peristiwa dapat menangani kesalahan fungsi dan percobaan ulang dengan benar.

Posisi awal polling dan streaming

Ketahui bahwa polling streaming selama pembuatan dan pembaruan pemetaan sumber acara pada akhirnya konsisten.

- Selama pembuatan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk memulai acara polling dari aliran.
- Selama pembaruan pemetaan sumber acara, mungkin diperlukan beberapa menit untuk menghentikan dan memulai kembali acara pemungutan suara dari aliran.

Perilaku ini berarti bahwa jika Anda menentukan LATEST sebagai posisi awal untuk aliran, pemetaan sumber peristiwa dapat melewatkan peristiwa selama pembuatan atau pembaruan. Untuk memastikan bahwa tidak ada peristiwa yang terlewatkan, tentukan posisi awal aliran sebagai TRIM_HORIZON atau AT_TIMESTAMP.

CloudWatch Metrik Amazon

Lambda memancarkan `OffsetLag` metrik saat fungsi Anda memproses catatan. Nilai metrik ini adalah perbedaan offset antara catatan terakhir yang ditulis ke topik sumber peristiwa Kafka dan catatan terakhir yang diproses oleh grup konsumen fungsi Anda. Anda dapat menggunakan `OffsetLag` untuk memperkirakan latensi antara saat catatan ditambahkan dan kapan grup konsumen Anda memprosesnya.

Tren yang meningkat `OffsetLag` dapat menunjukkan masalah dengan poller dalam kelompok konsumen fungsi Anda. Untuk informasi selengkapnya, lihat [Lihat metrik untuk fungsi Lambda](#).

Penskalaan otomatis sumber MSK acara Amazon

Saat Anda awalnya membuat sumber MSK acara Amazon, Lambda mengalokasikan satu konsumen untuk memproses semua partisi dalam topik Kafka. Setiap konsumen memiliki beberapa prosesor yang berjalan secara paralel untuk menangani peningkatan beban kerja. Selain itu, Lambda secara otomatis meningkatkan atau menurunkan jumlah konsumen, berdasarkan beban kerja. Untuk mempertahankan pemesanan pesan di setiap partisi, jumlah maksimum konsumen adalah satu konsumen per partisi dalam topik.

Dalam interval satu menit, Lambda mengevaluasi lag offset konsumen dari semua partisi dalam topik. Jika lag terlalu tinggi, partisi menerima pesan lebih cepat daripada yang dapat diproses Lambda. Jika perlu, Lambda menambahkan atau menghapus konsumen dari topik tersebut. Proses penskalaan penambahan atau penghapusan konsumen terjadi dalam waktu tiga menit setelah evaluasi.

Jika fungsi Lambda target Anda dibatasi, Lambda mengurangi jumlah konsumen. Tindakan ini mengurangi beban kerja pada fungsi dengan mengurangi jumlah pesan yang dapat konsumen ambil dan kirim ke fungsi.

Untuk memantau throughput topik Kafka Anda, lihat [metrik Lambda Offset lag](#) yang dipancarkan saat fungsi Anda memproses catatan.

Untuk memeriksa berapa banyak fungsi invokasi yang terjadi secara paralel, Anda juga dapat memantau [metrik konkurensi](#) untuk fungsi Anda.

Menggunakan pemfilteran acara dengan sumber MSK acara Amazon

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called “Penyaringan acara”](#).

Bagian ini berfokus pada pemfilteran acara untuk sumber MSK acara Amazon.

Topik

- [Dasar-dasar pemfilteran MSK acara Amazon](#)

Dasar-dasar pemfilteran MSK acara Amazon

Misalkan produser menulis pesan ke topik di MSK klaster Amazon Anda, baik dalam JSON format yang valid atau sebagai string biasa. Contoh catatan akan terlihat seperti berikut, dengan pesan dikonversi ke string yang dikodekan Base64 di bidang `value`

```
{
  "mytopic-0": [
    {
      "topic": "mytopic",
      "partition": 0,
      "offset": 15,
      "timestamp": 1545084650987,
      "timestampType": "CREATE_TIME",
      "value": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
      "headers": []
    }
  ]
}
```

Misalkan produser Apache Kafka Anda menulis pesan ke topik Anda dalam format berikut JSON.

```
{
  "device_ID": "AB1234",
  "session": {
    "start_time": "yyyy-mm-ddThh:mm:ss",
    "duration": 162
  }
}
```


Anda dapat menggunakan `value` kunci untuk memfilter catatan. Misalkan Anda ingin memfilter hanya catatan-catatan di mana `device_ID` dimulai dengan huruf AB. `FilterCriteriaObjeknya` adalah sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang `Pattern` diperluas secara polosJSON.

```
{
  "value": {
    "device_ID": [ { "prefix": "AB" } ]
  }
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "value" : { "device_ID" : [ { "prefix": "AB" } ] } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/  
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : { "device_ID" : [ { "prefix": "AB" } ] } }'
```

Dengan AmazonMSK, Anda juga dapat memfilter catatan di mana pesan adalah string biasa. Misalkan Anda ingin mengabaikan pesan-pesan di mana string adalah “kesalahan”.

FilterCriteriaObjek akan terlihat sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"value\" : [ { \"anything-but\": [ \"error\" ] } ] }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```
{
  "value": [
    {
      "anything-but": [ "error" ]
    }
  ]
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "value" : [ { "anything-but": [ "error" ] } ] }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/  
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":  
[ \"error\" ] } ] }"]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":  
[ \"error\" ] } ] }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : [ { "anything-but": [ "error" ] } ] }'
```

MSKPesan Amazon harus berupa UTF -8 string yang dikodekan, baik string biasa atau dalam format. JSON Itu karena Lambda menerjemahkan array byte MSK Amazon UTF menjadi -8 sebelum menerapkan kriteria filter. Jika pesan Anda menggunakan pengkodean lain, seperti UTF -16

atauASCII, atau jika format pesan tidak cocok dengan format, Lambda `FilterCriteria` hanya memproses filter metadata. Tabel berikut merangkum perilaku spesifik:

| Format pesan masuk | Format pola filter untuk properti pesan | Tindakan yang dihasilkan |
|------------------------------------|---|--|
| Tali polos | Tali polos | Filter Lambda berdasarkan kriteria filter Anda. |
| Tali polos | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Tali polos | Valid JSON | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tali polos | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |
| String yang tidak dikodekan UTF -8 | JSON, string polos, atau tidak ada pola | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |

Menangkap batch yang dibuang untuk sumber acara Amazon MSK

Untuk menyimpan catatan pemanggilan pemetaan sumber peristiwa yang gagal, tambahkan tujuan ke pemetaan sumber peristiwa fungsi Anda. Setiap catatan yang dikirim ke tujuan adalah JSON dokumen dengan metadata tentang pemanggilan yang gagal. Anda dapat mengonfigurasi SNS topik Amazon, SQS antrian Amazon, atau bucket S3 sebagai tujuan. Peran eksekusi Anda harus memiliki izin untuk tujuan:

- Untuk SQS tujuan: [sqs: SendMessage](#)
- Untuk SNS tujuan: [SNS: Publikasikan](#)
- Untuk tujuan bucket S3: [s3: PutObject](#) dan [s3: ListBuckets](#)

Anda harus menerapkan VPC titik akhir untuk layanan tujuan saat kegagalan di dalam kluster Amazon Anda. MSK VPC

Selain itu, jika Anda mengonfigurasi KMS kunci tujuan, Lambda memerlukan izin berikut tergantung pada jenis tujuan:

- Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk tujuan S3, [kms: GenerateDataKey diperlukan](#). Jika tujuan bucket KMS kunci dan S3 berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi agar memungkinkan `kms: GenerateDataKey`
- [Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk SQS tujuan, KMS: Decrypt dan kms: diperlukan. GenerateDataKey](#) Jika tujuan KMS kunci dan SQS antrian berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi untuk mengizinkan `KMS:Decrypt`, `kms:`, `kms:`, dan `kms:GenerateDataKey`. `DescribeKey` `ReEncrypt`
- [Jika Anda telah mengaktifkan enkripsi dengan KMS kunci Anda sendiri untuk SNS tujuan, KMS: Decrypt dan kms: diperlukan. GenerateDataKey](#) Jika tujuan KMS kunci dan SNS topik berada di akun yang berbeda dari fungsi Lambda dan peran eksekusi, konfigurasi KMS kunci untuk mempercayai peran eksekusi untuk mengizinkan `KMS:Decrypt`, `kms:`, `kms:`, dan `kms:GenerateDataKey`. `DescribeKey` `ReEncrypt`

Mengonfigurasi tujuan saat gagal untuk pemetaan sumber MSK peristiwa Amazon

Untuk mengonfigurasi tujuan saat gagal menggunakan konsol, ikuti langkah-langkah berikut:

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Di bagian Gambaran umum fungsi, pilih Tambahkan tujuan.
4. Untuk Sumber, pilih Pemanggilan pemetaan sumber acara.
5. Untuk pemetaan sumber peristiwa, pilih sumber peristiwa yang dikonfigurasi untuk fungsi ini.
6. Untuk Kondisi, pilih On failure. Untuk pemanggilan pemetaan sumber peristiwa, ini adalah satu-satunya kondisi yang diterima.
7. Untuk tipe Tujuan, pilih tipe tujuan yang Lambda kirimkan catatan pemanggilan.
8. Untuk Tujuan, pilih sumber daya.
9. Pilih Simpan.

Anda juga dapat mengonfigurasi tujuan pada kegagalan menggunakan file. AWS CLI Misalnya, [create-event-source-mapping](#) perintah berikut menambahkan pemetaan sumber peristiwa dengan tujuan SQS kegagalan ke: MyFunction

```
aws lambda create-event-source-mapping \  
--function-name "MyFunction" \  
--event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/  
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2 \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-  
east-1:123456789012:dest-queue"}}'
```

[update-event-source-mapping](#) Perintah berikut menambahkan tujuan kegagalan S3 ke sumber acara yang terkait dengan input: uuid

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--destination-config '{"OnFailure": {"Destination": "arn:aws:s3:::dest-bucket"}}'
```

Untuk menghapus tujuan, berikan string kosong sebagai argumen ke `destination-config` parameter:

```
aws lambda update-event-source-mapping \  
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \  
--destination-config '{"OnFailure": {"Destination": ""}}'
```

SNS dan SQS contoh catatan pemanggilan

Contoh berikut menunjukkan apa yang Lambda kirim ke SNS topik atau tujuan SQS antrian untuk pemanggilan sumber acara Kafka yang gagal. Setiap kunci di bawah `recordsInfo` berisi topik dan partisi Kafka, dipisahkan oleh tanda hubung. Misalnya, untuk kuncinya `"Topic-0"`, `Topic` adalah topik Kafka, dan `0` merupakan partisi. Untuk setiap topik dan partisi, Anda dapat menggunakan data offset dan stempel waktu untuk menemukan catatan pemanggilan asli.

```
{
  "requestContext": {
    "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
    "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
    "approximateInvokeCount": 1
  },
  "responseContext": { // null if record is MaximumPayloadSizeExceeded
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T00:38:06.021Z",
  "KafkaBatchInfo": {
    "batchSize": 500,
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
    "bootstrapServers": "...",
    "payloadSize": 2039086, // In bytes
    "recordsInfo": {
      "Topic-0": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
      },
      "Topic-1": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
```

```

        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
    }
}
}
}

```

Catatan pemanggilan contoh tujuan S3

Untuk tujuan S3, Lambda mengirimkan seluruh catatan pemanggilan bersama dengan metadata ke tujuan. Contoh berikut menunjukkan bahwa Lambda mengirim ke tujuan bucket S3 untuk pemanggilan sumber peristiwa Kafka yang gagal. Selain semua bidang dari contoh sebelumnya untuk SQS dan SNS tujuan, payload bidang berisi catatan pemanggilan asli sebagai string yang JSON diloloskan.

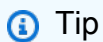
```

{
  "requestContext": {
    "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
    "condition": "RetryAttemptsExhausted | MaximumPayloadSizeExceeded",
    "approximateInvokeCount": 1
  },
  "responseContext": { // null if record is MaximumPayloadSizeExceeded
    "statusCode": 200,
    "executedVersion": "$LATEST",
    "functionError": "Unhandled"
  },
  "version": "1.0",
  "timestamp": "2019-11-14T00:38:06.021Z",
  "KafkaBatchInfo": {
    "batchSize": 500,
    "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
    "bootstrapServers": "...",
    "payloadSize": 2039086, // In bytes
    "recordsInfo": {
      "Topic-0": {
        "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
        "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
        "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
        "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
      }
    }
  },
}

```



```
    "Topic-1": {
      "firstRecordOffset":
"49601189658422359378836298521827638475320189012309704722",
      "lastRecordOffset":
"49601189658422359378836298522902373528957594348623495186",
      "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
      "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
    }
  },
  "payload": "<Whole Event>" // Only available in S3
}
```



Tip

Sebaiknya aktifkan versi S3 di bucket tujuan Anda.

Tutorial: Menggunakan pemetaan sumber MSK peristiwa Amazon untuk menjalankan fungsi Lambda

Dalam tutorial ini, Anda akan melakukan hal berikut:

- Buat fungsi Lambda di AWS akun yang sama dengan cluster Amazon MSK yang ada.
- Konfigurasi jaringan dan otentikasi untuk Lambda untuk berkomunikasi dengan Amazon. MSK
- Siapkan pemetaan sumber MSK peristiwa Lambda Amazon, yang menjalankan fungsi Lambda Anda saat peristiwa muncul di topik.

Setelah Anda selesai dengan langkah-langkah ini, ketika acara dikirim ke AmazonMSK, Anda akan dapat mengatur fungsi Lambda untuk memproses peristiwa tersebut secara otomatis dengan kode Lambda kustom Anda sendiri.

Apa yang dapat Anda lakukan dengan fitur ini?

Contoh solusi: Gunakan pemetaan sumber MSK acara untuk memberikan skor langsung kepada pelanggan Anda.

Pertimbangkan skenario berikut: Perusahaan Anda menghosting aplikasi web tempat pelanggan Anda dapat melihat informasi tentang acara langsung, seperti permainan olahraga. Pembaruan

informasi dari game disediakan untuk tim Anda melalui topik Kafka di AmazonMSK. Anda ingin merancang solusi yang menggunakan pembaruan dari MSK topik untuk memberikan tampilan terbaru dari acara langsung kepada pelanggan di dalam aplikasi yang Anda kembangkan. Anda telah memutuskan pendekatan desain berikut: Aplikasi klien Anda akan berkomunikasi dengan backend tanpa server yang dihosting. AWS Klien akan terhubung melalui sesi websocket menggunakan Amazon API Gateway WebSocket API.

Dalam solusi ini, Anda memerlukan komponen yang membaca MSK peristiwa, melakukan beberapa logika khusus untuk mempersiapkan peristiwa tersebut untuk lapisan aplikasi dan kemudian meneruskan informasi itu ke API GatewayAPI. Anda dapat mengimplementasikan komponen ini dengan AWS Lambda, dengan menyediakan logika kustom Anda dalam fungsi Lambda, lalu memanggilnya dengan pemetaan sumber MSK peristiwa AWS Lambda Amazon.

Untuk informasi selengkapnya tentang penerapan solusi menggunakan Amazon API Gateway WebSocket API, lihat [WebSocket API tutorial](#) di dokumentasi API Gateway.

Prasyarat

AWS Akun dengan sumber daya yang telah dikonfigurasi berikut:

Untuk memenuhi prasyarat ini, kami sarankan mengikuti [Memulai menggunakan Amazon di dokumentasi Amazon MSK](#). MSK

- MSKCluster Amazon. Lihat [Membuat MSK klaster Amazon](#) di Memulai menggunakan Amazon MSK.
- Konfigurasi berikut:
 - Pastikan otentikasi IAM berbasis peran Diaktifkan di pengaturan keamanan klaster Anda. Ini meningkatkan keamanan Anda dengan membatasi fungsi Lambda Anda untuk hanya mengakses MSK sumber daya Amazon yang dibutuhkan. Ini diaktifkan secara default di MSK cluster Amazon baru.
 - Pastikan akses Publik tidak aktif di pengaturan jaringan cluster Anda. Membatasi akses MSK klaster Amazon Anda ke internet meningkatkan keamanan Anda dengan membatasi berapa banyak perantara yang menangani data Anda. Ini diaktifkan secara default di MSK cluster Amazon baru.
- Topik Kafka di MSK cluster Amazon Anda untuk digunakan untuk solusi ini. Lihat [Membuat topik](#) di Memulai menggunakan Amazon MSK.
- Host admin Kafka disiapkan untuk mengambil informasi dari cluster Kafka Anda dan mengirim acara Kafka ke topik Anda untuk pengujian, seperti EC2 instans Amazon dengan admin Kafka CLI

dan perpustakaan Amazon diinstal. MSK IAM Lihat [Membuat mesin klien](#) di Memulai menggunakan Amazon MSK.

Setelah Anda menyiapkan sumber daya ini, kumpulkan informasi berikut dari AWS akun Anda untuk mengonfirmasi bahwa Anda siap untuk melanjutkan.

- Nama MSK cluster Amazon Anda. Anda dapat menemukan informasi ini di MSK konsol Amazon.
- ClusterUUID, bagian dari ARN untuk MSK cluster Amazon Anda, yang dapat Anda temukan di MSK konsol Amazon. Ikuti prosedur di [Daftar klaster](#) di MSK dokumentasi Amazon untuk menemukan informasi ini.
- Grup keamanan yang terkait dengan MSK cluster Amazon Anda. Anda dapat menemukan informasi ini di MSK konsol Amazon. Dalam langkah-langkah berikut, lihat ini sebagai *clusterSecurityGroups*.
- Id Amazon yang VPC berisi MSK cluster Amazon Anda. Anda dapat menemukan informasi ini dengan mengidentifikasi subnet yang terkait dengan MSK cluster Amazon Anda di MSK konsol Amazon, lalu mengidentifikasi Amazon yang VPC terkait dengan subnet di Konsol AmazonVPC.
- Nama topik Kafka yang digunakan dalam solusi Anda. Anda dapat menemukan informasi ini dengan menghubungi MSK cluster Amazon Anda dengan Kafka topics CLI dari host admin Kafka Anda. Untuk informasi selengkapnya tentang topikCLI, lihat [Menambahkan dan menghapus topik](#) dalam dokumentasi Kafka.
- Nama grup konsumen untuk topik Kafka Anda, cocok untuk digunakan oleh fungsi Lambda Anda. Grup ini dapat dibuat secara otomatis oleh Lambda, jadi Anda tidak perlu membuatnya dengan Kafka. CLI Jika Anda perlu mengelola grup konsumen, untuk mempelajari lebih lanjut tentang grup konsumenCLI, lihat [Mengelola Grup Konsumen di dokumentasi Kafka](#).

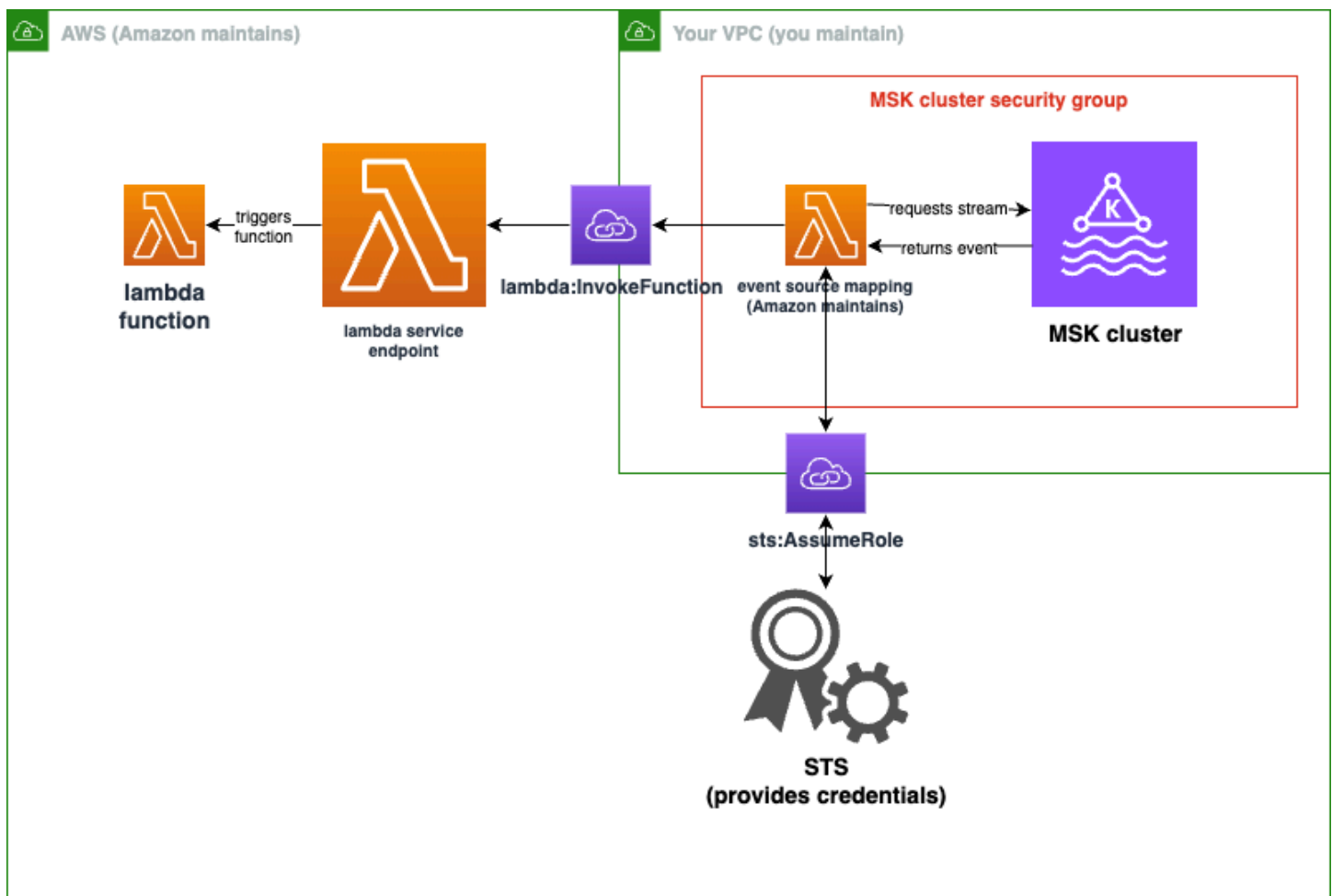
Izin berikut di AWS akun Anda:

- Izin untuk membuat dan mengelola fungsi Lambda.
- Izin untuk membuat IAM kebijakan dan mengaitkannya dengan fungsi Lambda Anda.
- Izin untuk membuat VPC endpoint Amazon dan mengubah konfigurasi jaringan di Amazon yang VPC menghosting cluster Amazon MSK Anda.

Konfigurasi konektivitas jaringan untuk Lambda untuk berkomunikasi dengan Amazon MSK

Gunakan AWS PrivateLink untuk menghubungkan Lambda dan Amazon MSK. Anda dapat melakukannya dengan membuat antarmuka VPC titik akhir Amazon di VPC konsol Amazon. Untuk informasi selengkapnya tentang konfigurasi jaringan, lihat [the section called “Konfigurasi jaringan”](#).

Saat pemetaan sumber MSK peristiwa Amazon berjalan atas nama fungsi Lambda, pemetaan tersebut akan mengasumsikan peran eksekusi fungsi Lambda. IAM Peran ini mengizinkan pemetaan untuk mengakses sumber daya yang diamankan IAM, seperti kluster Amazon MSK. Meskipun komponen berbagi peran eksekusi, MSK pemetaan Amazon dan fungsi Lambda Anda memiliki persyaratan konektivitas terpisah untuk tugasnya masing-masing, seperti yang ditunjukkan pada diagram berikut.



Pemetaan sumber acara Anda milik grup keamanan MSK kluster Amazon Anda. Pada langkah jaringan ini, buat VPC titik akhir Amazon dari MSK kluster Amazon Anda VPC untuk menghubungkan pemetaan sumber peristiwa ke Lambda dan layanan. STS Amankan titik akhir ini untuk menerima

lalu lintas dari grup keamanan MSK klaster Amazon Anda. Kemudian, sesuaikan grup keamanan MSK klaster Amazon untuk memungkinkan pemetaan sumber peristiwa berkomunikasi dengan MSK cluster Amazon.

Anda dapat mengonfigurasi langkah-langkah berikut menggunakan AWS Management Console.

Untuk mengonfigurasi antarmuka VPC titik akhir Amazon untuk menghubungkan Lambda dan Amazon MSK

1. Buat grup keamanan untuk antarmuka Anda VPC titik akhir Amazon, *endpointSecurityGroup*, yang memungkinkan TCP lalu lintas masuk pada 443 dari *clusterSecurityGroups*. Ikuti prosedur di [Buat grup keamanan](#) di EC2 dokumentasi Amazon untuk membuat grup keamanan. Kemudian, ikuti prosedur di [Tambahkan aturan ke grup keamanan](#) di EC2 dokumentasi Amazon untuk menambahkan aturan yang sesuai.

Buat grup keamanan dengan informasi berikut:

Saat menambahkan aturan masuk Anda, buat aturan untuk setiap grup keamanan di *clusterSecurityGroups*. Untuk setiap aturan:

- Untuk Jenis, pilih HTTPS.
 - Untuk Sumber, pilih salah satu *clusterSecurityGroups*.
2. Buat titik akhir yang menghubungkan layanan Lambda ke Amazon yang berisi klaster VPC Amazon MSK Anda. Ikuti prosedur di [Buat titik akhir antarmuka](#).

Buat titik akhir antarmuka dengan informasi berikut:

- Untuk nama Layanan, pilih `com.amazonaws.regionName.lambda`, di mana *regionName* host fungsi Lambda Anda.
- Untuk VPC, pilih Amazon yang VPC berisi MSK cluster Amazon Anda.
- Untuk grup Keamanan, pilih *endpointSecurityGroup*, yang Anda buat sebelumnya.
- Untuk Subnet, pilih subnet yang meng-host cluster Amazon MSK Anda.
- Untuk Kebijakan, berikan dokumen kebijakan berikut, yang mengamankan titik akhir untuk digunakan oleh kepala layanan Lambda untuk tindakan tersebut. `lambda:InvokeFunction`

```
{
  "Statement": [
    {
      "Action": "lambda:InvokeFunction",
```

```

        "Effect": "Allow",
        "Principal": {
            "Service": [
                "lambda.amazonaws.com"
            ]
        },
        "Resource": "*"
    }
]
}

```

- Pastikan DNSnama Aktifkan tetap disetel.
3. Buat titik akhir yang menghubungkan AWS STS layanan ke Amazon yang VPC berisi MSK kluster Amazon Anda. Ikuti prosedur di [Buat titik akhir antarmuka](#).

Buat titik akhir antarmuka dengan informasi berikut:

- Untuk nama Layanan, pilih AWS STS.
- Untuk VPC, pilih Amazon yang VPC berisi MSK cluster Amazon Anda.
- Untuk grup Keamanan, pilih *endpointSecurityGroup*.
- Untuk Subnet, pilih subnet yang meng-host cluster Amazon MSK Anda.
- Untuk Kebijakan, berikan dokumen kebijakan berikut, yang mengamankan titik akhir untuk digunakan oleh kepala layanan Lambda untuk tindakan tersebut. `sts:AssumeRole`

```

{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lambda.amazonaws.com"
        ]
      },
      "Resource": "*"
    }
  ]
}

```

- Pastikan DNSnama Aktifkan tetap disetel.

4. Untuk setiap grup keamanan yang terkait dengan MSK cluster Amazon Anda, yaitu, di *clusterSecurityGroups*, izinkan yang berikut ini:

- Izinkan semua TCP lalu lintas masuk dan keluar pada 9098 ke semua *clusterSecurityGroups*, termasuk di dalam dirinya sendiri.
- Izinkan semua TCP lalu lintas keluar di 443.

Beberapa lalu lintas ini diizinkan oleh aturan grup keamanan default, jadi jika klaster Anda dilampirkan ke satu grup keamanan, dan grup tersebut memiliki aturan default, aturan tambahan tidak diperlukan. Untuk menyesuaikan aturan grup keamanan, ikuti prosedur di [Tambahkan aturan ke grup keamanan](#) di EC2 dokumentasi Amazon.

Tambahkan aturan ke grup keamanan Anda dengan informasi berikut:

- Untuk setiap aturan masuk atau aturan keluar untuk port 9098, sediakan
 - Untuk Jenis, pilih Kustom TCP.
 - Untuk jangkauan Port, sediakan 9098.
 - Untuk Sumber, berikan salah satu *clusterSecurityGroups*.
- Untuk setiap aturan masuk untuk port 443, untuk Type, pilih. HTTPS

Buat IAM peran untuk dibaca Lambda dari topik Amazon Anda MSK

Identifikasi persyaratan autentikasi untuk dibaca Lambda dari topik MSK Amazon Anda, lalu tentukan dalam kebijakan. Buat peran, *lambdaAuthRole*, yang mengizinkan Lambda untuk menggunakan izin tersebut. Otorisasi tindakan di MSK klaster Amazon Anda menggunakan `kafka-cluster` IAM tindakan. Kemudian, otorisasi Lambda untuk melakukan tindakan Amazon MSK `kafka` dan EC2 Amazon yang diperlukan untuk menemukan dan terhubung ke cluster MSK Amazon Anda, CloudWatch serta tindakan agar Lambda dapat mencatat apa yang telah dilakukannya.

Untuk menjelaskan persyaratan autentikasi agar Lambda dapat dibaca dari Amazon MSK

1. Tulis dokumen IAM kebijakan (JSONdokumen), *clusterAuthPolicy*, yang memungkinkan Lambda membaca dari topik Kafka Anda di MSK cluster Amazon Anda menggunakan grup konsumen Kafka Anda. Lambda membutuhkan kelompok konsumen Kafka untuk diatur saat membaca.

Ubah template berikut agar selaras dengan prasyarat Anda:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeClusterDynamicConfiguration"
      ],
      "Resource": [
        "arn:aws:kafka:region:account-id:cluster/mskClusterName/cluster-uuid",
        "arn:aws:kafka:region:account-id:topic/mskClusterName/cluster-uuid/mskTopicName",
        "arn:aws:kafka:region:account-id:group/mskClusterName/cluster-uuid/mskGroupName"
      ]
    }
  ]
}

```

Untuk informasi lebih lanjut, konsultasikan [the section called “IAMotentikasi berbasis peran”](#). Saat menulis kebijakan Anda:

- Untuk *region* and *account-id*, berikan yang meng-host MSK cluster Amazon Anda.
 - Untuk *mskClusterName*, berikan nama MSK cluster Amazon Anda.
 - Untuk *cluster-uuid*, sediakan UUID di ARN untuk MSK cluster Amazon Anda.
 - Untuk *mskTopicName*, berikan nama topik Kafka Anda.
 - Untuk *mskGroupName*, berikan nama grup konsumen Kafka Anda.
2. Identifikasi AmazonMSK, Amazon, EC2 dan CloudWatch izin yang diperlukan Lambda untuk menemukan dan menghubungkan klaster MSK Amazon Anda, dan mencatat peristiwa tersebut.

Kebijakan AWSLambdaMSKExecutionRole dikelola secara permisif mendefinisikan izin yang diperlukan. Gunakan dalam langkah-langkah berikut.

Dalam lingkungan produksi, nilai `AWSLambdaMSKExecutionRole` untuk membatasi kebijakan peran eksekusi Anda berdasarkan prinsip hak istimewa terkecil, lalu tulis kebijakan untuk peran Anda yang menggantikan kebijakan terkelola ini.

Untuk detail tentang bahasa IAM kebijakan, lihat [IAM dokumentasi](#).

Sekarang setelah Anda menulis dokumen kebijakan Anda, buat IAM kebijakan sehingga Anda dapat melampirkannya ke peran Anda. Anda dapat melakukan ini menggunakan konsol dengan prosedur berikut.

Untuk membuat IAM kebijakan dari dokumen kebijakan Anda

1. Masuk ke AWS Management Console dan buka IAM konsol di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi sebelah kiri, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Di bagian Editor kebijakan, pilih JSONopsi.
5. Tempel `clusterAuthPolicy`.
6. Setelah selesai menambahkan izin ke kebijakan, pilih Berikutnya.
7. Pada halaman Tinjau dan buat, ketik Nama Kebijakan dan Deskripsi (opsional) untuk kebijakan yang Anda buat. Tinjau Izin yang ditentukan dalam kebijakan ini untuk melihat izin yang diberikan oleh kebijakan Anda.
8. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk informasi selengkapnya, lihat [Membuat IAM kebijakan](#) dalam IAM dokumentasi.

Sekarang setelah Anda memiliki IAM kebijakan yang sesuai, buat peran dan lampirkan padanya. Anda dapat melakukan ini menggunakan konsol dengan prosedur berikut.

Untuk membuat peran eksekusi di IAM konsol

1. Buka [halaman Peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Di bawah Jenis entitas tepercaya, pilih AWS layanan.
4. Di bawah Kasus penggunaan, pilih Lambda.

5. Pilih Berikutnya.
6. Pilih kebijakan berikut:
 - *clusterAuthPolicy*
 - *AWSLambdaMSKExecutionRole*
7. Pilih Berikutnya.
8. Untuk nama Peran, masukkan *lambdaAuthRole* dan kemudian pilih Buat peran.

Untuk informasi selengkapnya, lihat [the section called “Peran eksekusi \(izin untuk fungsi untuk mengakses sumber daya lain\)”](#).

Buat fungsi Lambda untuk membaca dari topik Amazon Anda MSK

Buat fungsi Lambda yang dikonfigurasi untuk menggunakan peran Anda IAM. Anda dapat membuat fungsi Lambda Anda menggunakan konsol.

Untuk membuat fungsi Lambda menggunakan konfigurasi autentikasi Anda

1. Buka konsol Lambda dan pilih Buat fungsi dari header.
2. Pilih Penulis dari awal.
3. Untuk nama Fungsi, berikan nama yang sesuai pilihan Anda.
4. Untuk Runtime, pilih versi terbaru yang didukung Node . js untuk menggunakan kode yang disediakan dalam tutorial ini.
5. Pilih Ubah peran eksekusi default.
6. Pilih Gunakan peran yang ada.
7. Untuk peran yang ada, pilih *lambdaAuthRole*.

Dalam lingkungan produksi, Anda biasanya perlu menambahkan kebijakan lebih lanjut ke peran eksekusi untuk fungsi Lambda Anda untuk memproses peristiwa Amazon Anda secara bermakna. MSK Untuk informasi selengkapnya tentang menambahkan kebijakan ke peran Anda, lihat [Menambahkan atau menghapus izin identitas](#) dalam IAM dokumentasi.

Buat pemetaan sumber acara ke fungsi Lambda Anda

Pemetaan sumber MSK peristiwa Amazon Anda memberikan layanan Lambda informasi yang diperlukan untuk memanggil Lambda Anda saat peristiwa Amazon yang sesuai terjadi. MSK Anda

dapat membuat MSK pemetaan Amazon menggunakan konsol. Buat pemicu Lambda, lalu pemetaan sumber peristiwa diatur secara otomatis.

Untuk membuat pemicu Lambda (dan pemetaan sumber peristiwa)

1. Arahkan ke halaman ikhtisar fungsi Lambda Anda.
2. Di bagian ikhtisar fungsi, pilih Tambahkan pemicu di kiri bawah.
3. Di menu tarik-turun Pilih sumber, pilih Amazon. MSK
4. Jangan mengatur otentikasi.
5. Untuk MSKcluster, pilih nama cluster Anda.
6. Untuk ukuran Batch, masukkan 1. Langkah ini membuat fitur ini lebih mudah untuk diuji, dan bukan merupakan nilai ideal dalam produksi.
7. Untuk nama Topik, berikan nama topik Kafka Anda.
8. Untuk ID grup Konsumen, berikan id grup konsumen Kafka Anda.

Perbarui fungsi Lambda Anda untuk membaca data streaming Anda

Lambda memberikan informasi tentang peristiwa Kafka melalui parameter metode acara. Untuk contoh struktur MSK acara Amazon, lihat [the section called “Contoh peristiwa”](#). Setelah Anda memahami cara menafsirkan peristiwa MSK Amazon yang diteruskan Lambda, Anda dapat mengubah kode fungsi Lambda Anda untuk menggunakan informasi yang mereka berikan.

Berikan kode berikut ke fungsi Lambda Anda untuk mencatat konten MSK acara Lambda Amazon untuk tujuan pengujian:

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan menggunakan Lambda. NET.

```
using System.Text;
```

```
using Amazon.Lambda.Core;
using Amazon.Lambda.KafkaEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace MSKLambda;

public class Function
{
    /// <param name="input">The event for the Lambda function handler to
    /// process.</param>
    /// <param name="context">The ILambdaContext that provides methods for
    /// logging and describing the Lambda environment.</param>
    /// <returns></returns>
    public void FunctionHandler(KafkaEvent evnt, ILambdaContext context)
    {
        foreach (var record in evnt.Records)
        {
            Console.WriteLine("Key:" + record.Key);
            foreach (var eventRecord in record.Value)
            {
                var valueBytes = eventRecord.Value.ToArray();
                var valueText = Encoding.UTF8.GetString(valueBytes);

                Console.WriteLine("Message:" + valueText);
            }
        }
    }
}
```

Java

SDKuntuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi MSK acara Amazon dengan Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent.KafkaEventRecord;

import java.util.Base64;
import java.util.Map;

public class Example implements RequestHandler<KafkaEvent, Void> {

    @Override
    public Void handleRequest(KafkaEvent event, Context context) {
        for (Map.Entry<String, java.util.List<KafkaEventRecord>> entry :
event.getRecords().entrySet()) {
            String key = entry.getKey();
            System.out.println("Key: " + key);

            for (KafkaEventRecord record : entry.getValue()) {
                System.out.println("Record: " + record);

                byte[] value = Base64.getDecoder().decode(record.getValue());
                String message = new String(value);
                System.out.println("Message: " + message);
            }
        }

        return null;
    }
}
```

JavaScript

SDKuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan menggunakan Lambda. JavaScript

```
exports.handler = async (event) => {
  // Iterate through keys
  for (let key in event.records) {
    console.log('Key: ', key)
    // Iterate through records
    event.records[key].map((record) => {
      console.log('Record: ', record)
      // Decode base64
      const msg = Buffer.from(record.value, 'base64').toString()
      console.log('Message:', msg)
    })
  }
}
```

Python

SDKuntuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi MSK acara Amazon dengan Lambda menggunakan Python.

```
import base64

def lambda_handler(event, context):
    # Iterate through keys
    for key in event['records']:
        print('Key:', key)
        # Iterate through records
        for record in event['records'][key]:
            print('Record:', record)
            # Decode base64
            msg = base64.b64decode(record['value']).decode('utf-8')
            print('Message:', msg)
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi MSK acara Amazon dengan Lambda menggunakan Ruby.

```
require 'base64'

def lambda_handler(event:, context:)
    # Iterate through keys
    event['records'].each do |key, records|
        puts "Key: #{key}"

        # Iterate through records
        records.each do |record|
            puts "Record: #{record}"

            # Decode base64
```

```
msg = Base64.decode64(record['value'])
puts "Message: #{msg}"
end
end
end
```

Anda dapat memberikan kode fungsi ke Lambda Anda menggunakan konsol.

Untuk memperbarui kode fungsi Lambda

1. Arahkan ke halaman ikhtisar fungsi Lambda Anda.
2. Pilih tab Kode.
3. Masukkan kode yang disediakan ke dalam sumber KodeIDE.
4. Di bilah navigasi sumber kode, pilih Deploy.

Uji fungsi Lambda Anda untuk memverifikasi bahwa itu terhubung ke topik Amazon MSK

Anda sekarang dapat memverifikasi apakah Lambda Anda sedang dipanggil oleh sumber peristiwa dengan memeriksa CloudWatch log peristiwa atau tidak.

Untuk memverifikasi apakah fungsi Lambda Anda sedang dipanggil

1. Gunakan host admin Kafka Anda untuk menghasilkan acara Kafka menggunakan `kafka-console-producer` CLI Untuk informasi lebih lanjut, lihat [Menulis beberapa peristiwa ke dalam topik](#) dalam dokumentasi Kafka. Kirim peristiwa yang cukup untuk mengisi batch yang ditentukan oleh ukuran batch untuk pemetaan sumber peristiwa yang ditentukan pada langkah sebelumnya, atau Lambda akan menunggu informasi lebih lanjut untuk dipanggil.
2. Jika fungsi Anda berjalan, Lambda menulis apa yang terjadi. CloudWatch Di konsol, navigasikan ke halaman detail fungsi Lambda Anda.
3. Pilih tab Konfigurasi.
4. Dari sidebar, pilih Alat pemantauan dan operasi.
5. Identifikasi grup CloudWatch log di bawah konfigurasi Logging. Grup log harus dimulai dengan `aws/lambda`. Pilih tautan ke grup log.
6. Di CloudWatch konsol, periksa peristiwa Log untuk peristiwa log yang dikirim Lambda ke aliran log. Identifikasi apakah ada peristiwa log yang berisi pesan dari acara Kafka Anda, seperti pada

gambar berikut. Jika ada, Anda telah berhasil menghubungkan fungsi Lambda ke Amazon MSK dengan pemetaan sumber peristiwa Lambda.

| | |
|-------------------------------|---|
| 2020-08-06T15:06:18.861-04:00 | START RequestId: 88ebae59-be0c-4e22-9db7-4154b437e43a Version: \$LATEST |
| 2020-08-06T15:06:18.866-04:00 | 2020-08-06T19:06:18.866Z 88ebae59-be0c-4e22-9db7-4154b437e43a INFO Key: mytopic-0 |
| 2020-08-06T15:06:18.866-04:00 | 2020-08-06T19:06:18.866Z 88ebae59-be0c-4e22-9db7-4154b437e43a INFO Record: { topic: 'mytopic', partition: 0, offset: 38, timestamp: 1596740777633, timestampType: 'CREATE_TIME', value: 'TwVzc2FnZSAjMQ==' } |
| 2020-08-06T15:06:18.866-04:00 | 2020-08-06T19:06:18.866Z 88ebae59-be0c-4e22-9db7-4154b437e43a INFO Message: Message #1 |
| 2020-08-06T15:06:18.890-04:00 | END RequestId: 88ebae59-be0c-4e22-9db7-4154b437e43a |

Menggunakan AWS Lambda dengan Amazon RDS

Anda dapat menghubungkan fungsi Lambda ke database Amazon Relational Database Service (AmazonRDS) secara langsung dan melalui Amazon Proxy. RDS Koneksi langsung berguna dalam skenario sederhana, dan proxy direkomendasikan untuk produksi. Proxy database mengelola kumpulan koneksi database bersama yang memungkinkan fungsi Anda mencapai tingkat konkurensi tinggi tanpa melelahkan koneksi database.

Sebaiknya gunakan Amazon RDS Proxy untuk fungsi Lambda yang sering membuat koneksi database pendek, atau membuka dan menutup sejumlah besar koneksi database. Untuk informasi selengkapnya, lihat [Menghubungkan fungsi Lambda dan instans DB secara otomatis](#) di Panduan Pengembangan Layanan Amazon Relational Database Service.

Mengkonfigurasi fungsi Anda untuk bekerja dengan sumber daya RDS

Di konsol Lambda, Anda dapat menyediakan, dan mengonfigurasi, instans RDS database Amazon dan sumber daya proxy. Anda dapat melakukan ini dengan menavigasi ke RDSdatabase di bawah tab Konfigurasi. Atau, Anda juga dapat membuat dan mengonfigurasi koneksi ke fungsi Lambda di konsol AmazonRDS. Saat mengonfigurasi instance RDS database untuk digunakan dengan Lambda, perhatikan kriteria berikut:

- Untuk terhubung ke database, fungsi Anda harus berada di Amazon yang sama VPC tempat database Anda berjalan.
- Anda dapat menggunakan RDS database Amazon dengan mesin MySQL, MariaDB, PostgreSQL, atau Microsoft Server. SQL
- Anda juga dapat menggunakan cluster Aurora DB dengan mesin My SQL atau Postgre. SQL
- Anda perlu memberikan rahasia Secrets Manager untuk otentikasi database.
- IAMPeran harus memberikan izin untuk menggunakan rahasia, dan kebijakan kepercayaan harus memungkinkan Amazon RDS untuk mengambil peran tersebut.
- IAMPrinsipal yang menggunakan konsol untuk mengonfigurasi RDS sumber daya Amazon, dan menghubungkannya ke fungsi Anda harus memiliki izin berikut:

Note

Anda memerlukan izin RDS Proxy Amazon hanya jika Anda mengonfigurasi RDS Proxy Amazon untuk mengelola kumpulan koneksi database Anda.

Example kebijakan izin

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds-db:connect",
        "rds:CreateDBProxy",
        "rds:CreateDBInstance",
        "rds:CreateDBSubnetGroup",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBProxyTargetGroups",
        "rds:RegisterDBProxyTargets",
        "rds:ModifyDBInstance",
        "rds:ModifyDBProxy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```

    "Action": [
      "lambda:CreateFunction",
      "lambda:ListFunctions",
      "lambda:UpdateFunctionConfiguration"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:AttachRolePolicy",
      "iam:AttachPolicy",
      "iam:CreateRole",
      "iam:CreatePolicy"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetResourcePolicy",
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret",
      "secretsmanager:ListSecretVersionIds",
      "secretsmanager:CreateSecret"
    ],
    "Resource": "*"
  }
]
}

```

Amazon RDS mengenakan tarif per jam untuk proxy berdasarkan ukuran instans database, lihat [Harga RDS proxy](#) untuk detailnya. Untuk informasi selengkapnya tentang koneksi proxy secara umum, lihat [Menggunakan Amazon RDS Proxy](#) di Panduan RDS Pengguna Amazon.

Pengaturan Lambda dan Amazon RDS

RDSKonsol Lambda dan Amazon akan membantu Anda mengonfigurasi beberapa sumber daya yang diperlukan secara otomatis untuk membuat koneksi antara Lambda dan Amazon RDS

Menghubungkan ke RDS database Amazon dalam fungsi Lambda

Contoh kode berikut menunjukkan cara menerapkan fungsi Lambda yang terhubung ke database AmazonRDS. Fungsi membuat permintaan database sederhana dan mengembalikan hasilnya.

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Go.

```
/*
Golang v2 code here.
*/

package main

import (
    "context"
    "database/sql"
    "encoding/json"
    "fmt"
    "os"

    "github.com/aws/aws-lambda-go/lambda"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
    _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
    Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {
```

```
var dbName string = os.Getenv("DatabaseName")
var dbUser string = os.Getenv("DatabaseUser")
var dbHost string = os.Getenv("DBHost") // Add hostname without https
var dbPort int = os.Getenv("Port")      // Add port number
var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
var region string = os.Getenv("AWS_REGION")

cfg, err := config.LoadDefaultConfig(context.TODO())
if err != nil {
    panic("configuration error: " + err.Error())
}

authenticationToken, err := auth.BuildAuthToken(
    context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
if err != nil {
    panic("failed to create authentication token: " + err.Error())
}

dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
    dbUser, authenticationToken, dbEndpoint, dbName,
)

db, err := sql.Open("mysql", dsn)
if err != nil {
    panic(err)
}

defer db.Close()

var sum int
err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
if err != nil {
    panic(err)
}
s := fmt.Sprint(sum)
message := fmt.Sprintf("The selected sum is: %s", s)

messageBytes, err := json.Marshal(message)
if err != nil {
    return nil, err
}

messageString := string(messageBytes)
return map[string]interface{}{
```

```
"statusCode": 200,  
"headers":    map[string]string{"Content-Type": "application/json"},  
"body":      messageString,  
}, nil  
}  
  
func main() {  
    lambda.Start(HandleRequest)  
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;  
import com.amazonaws.services.lambda.runtime.RequestHandler;  
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;  
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;  
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.rdsdata.RdsDataClient;  
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementRequest;  
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementResponse;  
import software.amazon.awssdk.services.rdsdata.model.Field;  
  
import java.sql.Connection;  
import java.sql.DriverManager;  
import java.sql.PreparedStatement;  
import java.sql.ResultSet;  
  
public class RdsLambdaHandler implements  
    RequestHandler<APIGatewayProxyRequestEvent, APIGatewayProxyResponseEvent> {
```

```
@Override
public APIGatewayProxyResponseEvent handleRequest(APIGatewayProxyRequestEvent
event, Context context) {
    APIGatewayProxyResponseEvent response = new
APIGatewayProxyResponseEvent();

    try {
        // Obtain auth token
        String token = createAuthToken();

        // Define connection configuration
        String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true",
            System.getenv("ProxyHostName"),
            System.getenv("Port"),
            System.getenv("DBName"));

        // Establish a connection to the database
        try (Connection connection =
DriverManager.getConnection(connectionString, System.getenv("DBUserName"),
token);
            PreparedStatement statement =
connection.prepareStatement("SELECT ? + ? AS sum")) {

            statement.setInt(1, 3);
            statement.setInt(2, 2);

            try (ResultSet resultSet = statement.executeQuery()) {
                if (resultSet.next()) {
                    int sum = resultSet.getInt("sum");
                    response.setStatusCode(200);
                    response.setBody("The selected sum is: " + sum);
                }
            }
        }
    } catch (Exception e) {
        response.setStatusCode(500);
        response.setBody("Error: " + e.getMessage());
    }

    return response;
}
```



```

private String createAuthToken() {
    // Create RDS Data Service client
    RdsDataClient rdsDataClient = RdsDataClient.builder()
        .region(Region.of(System.getenv("AWS_REGION")))
        .credentialsProvider(DefaultCredentialsProvider.create())
        .build();

    // Define authentication request
    ExecuteStatementRequest request = ExecuteStatementRequest.builder()
        .resourceArn(System.getenv("ProxyHostName"))
        .secretArn(System.getenv("DBUserName"))
        .database(System.getenv("DBName"))
        .sql("SELECT 'RDS IAM Authentication'")
        .build();

    // Execute request and obtain authentication token
    ExecuteStatementResponse response =
rdsDataClient.executeStatement(request);
    Field tokenField = response.records().get(0).get(0);

    return tokenField.stringValue();
}
}

```

JavaScript

SDKuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan JavaScript

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Node.js code here.
*/

```

```
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;
}

export const handler = async (event) => {
```

```
// Execute database flow
const result = await dbOps();
// Return result
return {
  statusCode: 200,
  body: JSON.stringify("The selected sum is: " + result[0].sum)
}
};
```

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan TypeScript

```
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

// RDS settings
// Using '!' (non-null assertion operator) to tell the TypeScript compiler that
// the DB settings are not null or undefined,
const proxy_host_name = process.env.PROXY_HOST_NAME!
const port = parseInt(process.env.PORT!)
const db_name = process.env.DB_NAME!
const db_user_name = process.env.DB_USER_NAME!
const aws_region = process.env.AWS_REGION!

async function createAuthToken(): Promise<string> {

  // Create RDS Signer object
  const signer = new Signer({
    hostname: proxy_host_name,
    port: port,
    region: aws_region,
    username: db_user_name
  });

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps(): Promise<mysql.QueryResult | undefined> {
  try {
```

```
// Obtain auth token
const token = await createAuthToken();
const conn = await mysql.createConnection({
  host: proxy_host_name,
  user: db_user_name,
  password: token,
  database: db_name,
  ssl: 'Amazon RDS' // Ensure you have the CA bundle for SSL connection
});
const [rows, fields] = await conn.execute('SELECT ? + ? AS sum', [3, 2]);
console.log('result:', rows);
return rows;
}
catch (err) {
  console.log(err);
}
}


export const lambdaHandler = async (event: any): Promise<{ statusCode: number;
body: string }> => {
  // Execute database flow
  const result = await dbOps();

  // Return error is result is undefined
  if (result == undefined)
    return {
      statusCode: 500,
      body: JSON.stringify(`Error with connection to DB host`)
    }

  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify(`The selected sum is: ${result[0].sum}`)
  };
};
```

PHP

SDK untuk PHP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan PHP

```
<?php
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;
use Aws\Rds\AuthTokenGenerator;
use Aws\Credentials\CredentialProvider;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    private function getAuthToken(): string {
        // Define connection authentication parameters
        $dbConnection = [
            'hostname' => getenv('DB_HOSTNAME'),
            'port' => getenv('DB_PORT'),
            'username' => getenv('DB_USERNAME'),
            'region' => getenv('AWS_REGION'),
        ];
    }
}
```

```
    // Create RDS AuthTokenGenerator object
    $generator = new
AuthTokenGenerator(CredentialProvider::defaultProvider());

    // Request authorization token from RDS, specifying the username
    return $generator->createToken(
        $dbConnection['hostname'] . ':' . $dbConnection['port'],
        $dbConnection['region'],
        $dbConnection['username']
    );
}

private function getQueryResults() {
    // Obtain auth token
    $token = $this->getAuthToken();

    // Define connection configuration
    $connectionConfig = [
        'host' => getenv('DB_HOSTNAME'),
        'user' => getenv('DB_USERNAME'),
        'password' => $token,
        'database' => getenv('DB_NAME'),
    ];

    // Create the connection to the DB
    $conn = new PDO(
        "mysql:host={$connectionConfig['host']};dbname={$connectionConfig['database']}",
        $connectionConfig['user'],
        $connectionConfig['password'],
        [
            PDO::MYSQL_ATTR_SSL_CA => '/path/to/rds-ca-2019-root.pem',
            PDO::MYSQL_ATTR_SSL_VERIFY_SERVER_CERT => true,
        ]
    );

    // Obtain the result of the query
    $stmt = $conn->prepare('SELECT ?+? AS sum');
    $stmt->execute([3, 2]);

    return $stmt->fetch(PDO::FETCH_ASSOC);
}
```

```
/**
 * @param mixed $event
 * @param Context $context
 * @return array
 */
public function handle(mixed $event, Context $context): array
{
    $this->logger->info("Processing query");

    // Execute database flow
    $result = $this->getQueryResults();

    return [
        'sum' => $result['sum']
    ];
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Python.

```
import json
import os
import boto3
import pymysql

# RDS settings
proxy_host_name = os.environ['PROXY_HOST_NAME']
port = int(os.environ['PORT'])
db_name = os.environ['DB_NAME']
```

```
db_user_name = os.environ['DB_USER_NAME']
aws_region = os.environ['AWS_REGION']

# Fetch RDS Auth Token
def get_auth_token():
    client = boto3.client('rds')
    token = client.generate_db_auth_token(
        DBHostname=proxy_host_name,
        Port=port
        DBUsername=db_user_name
        Region=aws_region
    )
    return token

def lambda_handler(event, context):
    token = get_auth_token()
    try:
        connection = pymysql.connect(
            host=proxy_host_name,
            user=db_user_name,
            password=token,
            db=db_name,
            port=port,
            ssl={'ca': 'Amazon RDS'} # Ensure you have the CA bundle for SSL
        )

        with connection.cursor() as cursor:
            cursor.execute('SELECT %s + %s AS sum', (3, 2))
            result = cursor.fetchone()

        return result

    except Exception as e:
        return (f"Error: {str(e)}") # Return an error message if an exception
    occurs
```


Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Ruby.

```
# Ruby code here.

require 'aws-sdk-rds'
require 'json'
require 'mysql2'

def lambda_handler(event:, context:)
  endpoint = ENV['DBEndpoint'] # Add the endpoint without https"
  port = ENV['Port']           # 3306
  user = ENV['DBUser']
  region = ENV['DBRegion']     # 'us-east-1'
  db_name = ENV['DBName']

  credentials = Aws::Credentials.new(
    ENV['AWS_ACCESS_KEY_ID'],
    ENV['AWS_SECRET_ACCESS_KEY'],
    ENV['AWS_SESSION_TOKEN']
  )
  rds_client = Aws::RDS::AuthTokenGenerator.new(
    region: region,
    credentials: credentials
  )

  token = rds_client.auth_token(
    endpoint: endpoint+ ':' + port,
    user_name: user,
    region: region
  )

  begin
    conn = Mysql2::Client.new(
```

```

    host: endpoint,
    username: user,
    password: token,
    port: port,
    database: db_name,
    sslca: '/var/task/global-bundle.pem',
    sslverify: true,
    enableCleartextPlugin: true
  )
  a = 3
  b = 2
  result = conn.query("SELECT #{a} + #{b} AS sum").first['sum']
  puts result
  conn.close
  {
    statusCode: 200,
    body: result.to_json
  }
rescue => e
  puts "Database connection failed due to #{e}"
end
end

```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Rust.

```

use aws_config::BehaviorVersion;
use aws_credential_types::provider::ProvideCredentials;
use aws_sigv4::{
    http_request::{sign, SignableBody, SignableRequest, SigningSettings},
    sign::v4,
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

```

```
use serde_json::{json, Value};
use sqlx::postgres::PgConnectOptions;
use std::env;
use std::time::{Duration, SystemTime};

const RDS_CERTS: &[u8] = include_bytes!("global-bundle.pem");

async fn generate_rds_iam_token(
    db_hostname: &str,
    port: u16,
    db_username: &str,
) -> Result<String, Error> {
    let config = aws_config::load_defaults(BehaviorVersion::v2024_03_28()).await;

    let credentials = config
        .credentials_provider()
        .expect("no credentials provider found")
        .provide_credentials()
        .await
        .expect("unable to load credentials");
    let identity = credentials.into();
    let region = config.region().unwrap().to_string();

    let mut signing_settings = SigningSettings::default();
    signing_settings.expires_in = Some(Duration::from_secs(900));
    signing_settings.signature_location =
aws_sigv4::http_request::SignatureLocation::QueryParams;

    let signing_params = v4::SigningParams::builder()
        .identity(&identity)
        .region(&region)
        .name("rds-db")
        .time(SystemTime::now())
        .settings(signing_settings)
        .build()?;

    let url = format!(
        "https://{db_hostname}:{port}/?Action=connect&DBUser={db_user}",
        db_hostname = db_hostname,
        port = port,
        db_user = db_username
    );

    let signable_request =
```

```

        SignableRequest::new("GET", &url, std::iter::empty(),
SignableBody::Bytes(&[]))
            .expect("signable request");

        let (signing_instructions, _signature) =
            sign(signable_request, &signing_params.into())?.into_parts();

        let mut url = url::Url::parse(&url).unwrap();
        for (name, value) in signing_instructions.params() {
            url.query_pairs_mut().append_pair(name, &value);
        }

        let response = url.to_string().split_off("https://".len());

        Ok(response)
    }

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(handler)).await
}

async fn handler(_event: LambdaEvent<Value>) -> Result<Value, Error> {
    let db_host = env::var("DB_HOSTNAME").expect("DB_HOSTNAME must be set");
    let db_port = env::var("DB_PORT")
        .expect("DB_PORT must be set")
        .parse:::<u16>()
        .expect("PORT must be a valid number");
    let db_name = env::var("DB_NAME").expect("DB_NAME must be set");
    let db_user_name = env::var("DB_USERNAME").expect("DB_USERNAME must be set");

    let token = generate_rds_iam_token(&db_host, db_port, &db_user_name).await?;

    let opts = PgConnectOptions::new()
        .host(&db_host)
        .port(db_port)
        .username(&db_user_name)
        .password(&token)
        .database(&db_name)
        .ssl_root_cert_from_pem(RDS_CERTS.to_vec())
        .ssl_mode(sqlx::postgres::PgSslMode::Require);

    let pool = sqlx::postgres::PgPoolOptions::new()
        .connect_with(opts)

```

```

        .await?;

let result: i32 = sqlx::query_scalar("SELECT $1 + $2")
    .bind(3)
    .bind(2)
    .fetch_one(&pool)
    .await?;

println!("Result: {:?}", result);

Ok(json!({
    "statusCode": 200,
    "content-type": "text/plain",
    "body": format!("The selected sum is: {result}")
}))
}

```

Memproses pemberitahuan acara dari Amazon RDS

Anda dapat menggunakan Lambda untuk memproses pemberitahuan peristiwa dari database AmazonRDS. Amazon RDS mengirimkan notifikasi ke topik Amazon Simple Notification Service (AmazonSNS), yang dapat Anda konfigurasi untuk menjalankan fungsi Lambda. Amazon SNS membungkus pesan dari Amazon RDS dalam dokumen acaranya sendiri dan mengirimkannya ke fungsi Anda.

Untuk informasi selengkapnya tentang mengonfigurasi RDS database Amazon untuk mengirim notifikasi, lihat [Menggunakan notifikasi RDS peristiwa Amazon](#).

Example RDS Pesan Amazon dalam SNS acara Amazon

```

{
  "Records": [
    {
      "EventVersion": "1.0",
      "EventSubscriptionArn": "arn:aws:sns:us-east-2:123456789012:rds-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
      "EventSource": "aws:sns",
      "Sns": {
        "SignatureVersion": "1",
        "Timestamp": "2023-01-02T12:45:07.000Z",

```

```

    "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi
+tE/1+82j...65r==",
    "SigningCertUrl": "https://sns.us-east-2.amazonaws.com/
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",
    "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
    "Message": "{\"Event Source\":\"db-instance\",\"Event Time\":\"2023-01-02
12:45:06.000\",\"Identifier Link\":\"https://console.aws.amazon.com/rds/home?
region=eu-west-1#dbinstance:id=dbinstanceid\",\"Source ID\":\"dbinstanceid\",\"Event ID
\":\"http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/USER_Events.html#RDS-
EVENT-0002\",\"Event Message\":\"Finished DB Instance backup\"}",
    "MessageAttributes": {},
    "Type": "Notification",
    "UnsubscribeUrl": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:sns-lambda",
    "Subject": "RDS Notification Message"
  }
}
]
}

```

Lengkap Lambda dan Amazon tutorial RDS

- [Menggunakan fungsi Lambda untuk mengakses RDS database Amazon](#) — Dari Panduan RDS Pengguna Amazon, pelajari cara menggunakan fungsi Lambda untuk menulis data ke database Amazon RDS melalui Proxy Amazon. RDS Fungsi Lambda Anda akan membaca catatan dari SQS antrian Amazon dan menulis item baru ke tabel di database Anda setiap kali pesan ditambahkan.

Memproses pemberitahuan acara Amazon S3 dengan Lambda

Anda dapat menggunakan Lambda untuk memproses [pemberitahuan kejadian](#) dari Amazon Simple Storage Service. Amazon S3 dapat mengirimkan kejadian ke fungsi Lambda saat objek dibuat atau dihapus. Anda mengonfigurasi pengaturan pemberitahuan di bucket, dan memberikan izin kepada Amazon S3 untuk memanggil fungsi di kebijakan izin berbasis sumber daya milik fungsi.

Warning

Jika fungsi Lambda Anda menggunakan bucket yang sama dengan bucket yang memicunya, hal ini dapat menyebabkan fungsi berjalan secara berulang-ulang. Misalnya, jika bucket memicu fungsi setiap kali suatu objek diunggah, dan fungsi mengunggah sebuah objek ke bucket, fungsi tersebut secara tidak langsung akan memicu dirinya sendiri. Untuk menghindari hal ini, gunakan dua bucket, atau konfigurasi pemicu agar hanya diterapkan ke awalan yang digunakan untuk objek masuk.

Amazon S3 memanggil fungsi Anda [secara asinkron](#) dengan kejadian yang berisi detail tentang objek. Contoh berikut menunjukkan kejadian yang dikirimkan Amazon S3 saat paket deployment diunggah ke Amazon S3.

Example Kejadian pemberitahuan Amazon S3

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-2",
      "eventTime": "2019-09-03T19:37:27.192Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "AWS:AIDAINPONIXQXHT3IKHL2"
      },
      "requestParameters": {
        "sourceIPAddress": "205.255.255.255"
      },
      "responseElements": {
        "x-amz-request-id": "D82B88E5F771F645",
        "x-amz-id-2":
"v1R7PnpV2Ce81l0PRw6jlUpck7Jo5ZsQjryTjK1c5aLWGVHPZLj5NeC6qMa0emYBDX0o6QBU0Wo="
      }
    }
  ]
}
```

```
  },
  "s3": {
    "s3SchemaVersion": "1.0",
    "configurationId": "828aa6fc-f7b5-4305-8584-487c791949c1",
    "bucket": {
      "name": "amzn-s3-demo-bucket",
      "ownerIdentity": {
        "principalId": "A3I5XTEXAMAI3E"
      },
      "arn": "arn:aws:s3:::lambda-artifacts-deafc19498e3f2df"
    },
    "object": {
      "key": "b21b84d653bb07b05b1e6b33684dc11b",
      "size": 1305107,
      "eTag": "b21b84d653bb07b05b1e6b33684dc11b",
      "sequencer": "0C0F6F405D6ED209E1"
    }
  }
}
```

Untuk memanggil fungsi Anda, Amazon S3 memerlukan izin dari [kebijakan berbasis sumber daya](#) milik fungsi. Saat Anda mengonfigurasi pemicu Amazon S3 di konsol Lambda, konsol memodifikasi kebijakan berbasis sumber daya untuk mengizinkan Amazon S3 memanggil fungsi jika nama bucket dan ID akun cocok. Jika Anda mengonfigurasi notifikasi di Amazon S3, Anda menggunakan Lambda API untuk memperbarui kebijakan. Anda juga dapat menggunakan Lambda API untuk memberikan izin ke akun lain, atau membatasi izin ke alias yang ditunjuk.

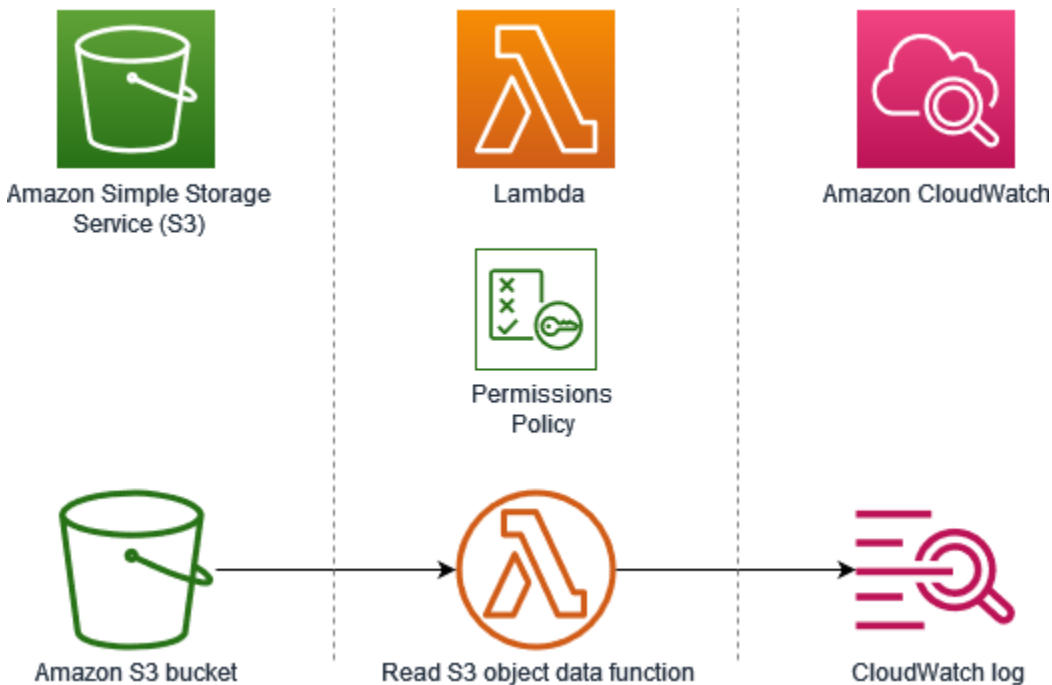
[Jika fungsi Anda menggunakan AWS SDK untuk mengelola sumber daya Amazon S3, fungsi tersebut juga memerlukan izin Amazon S3 dalam peran pelaksanaannya.](#)

Topik

- [Tutorial: Menggunakan pemicu Amazon S3 untuk memanggil fungsi Lambda](#)
- [Tutorial: Menggunakan pemicu Amazon S3 untuk membuat gambar thumbnail](#)

Tutorial: Menggunakan pemicu Amazon S3 untuk memanggil fungsi Lambda

Dalam tutorial ini, Anda menggunakan konsol untuk membuat fungsi Lambda dan mengonfigurasi pemicu untuk bucket Amazon Simple Storage Service (Amazon S3). Setiap kali Anda menambahkan objek ke bucket Amazon S3, fungsi Anda berjalan dan mengeluarkan jenis objek ke Amazon Logs. CloudWatch



Tutorial ini menunjukkan bagaimana untuk:

1. Buat bucket Amazon S3.
2. Buat fungsi Lambda yang mengembalikan jenis objek objek dalam bucket Amazon S3.
3. Konfigurasi pemicu Lambda yang memanggil fungsi Anda saat objek diunggah ke bucket Anda.
4. Uji fungsi Anda, pertama dengan acara dummy, dan kemudian gunakan pelatuknya.

Dengan menyelesaikan langkah-langkah ini, Anda akan mempelajari cara mengonfigurasi fungsi Lambda agar berjalan setiap kali objek ditambahkan atau dihapus dari bucket Amazon S3. Anda dapat menyelesaikan tutorial ini hanya dengan menggunakan AWS Management Console.

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

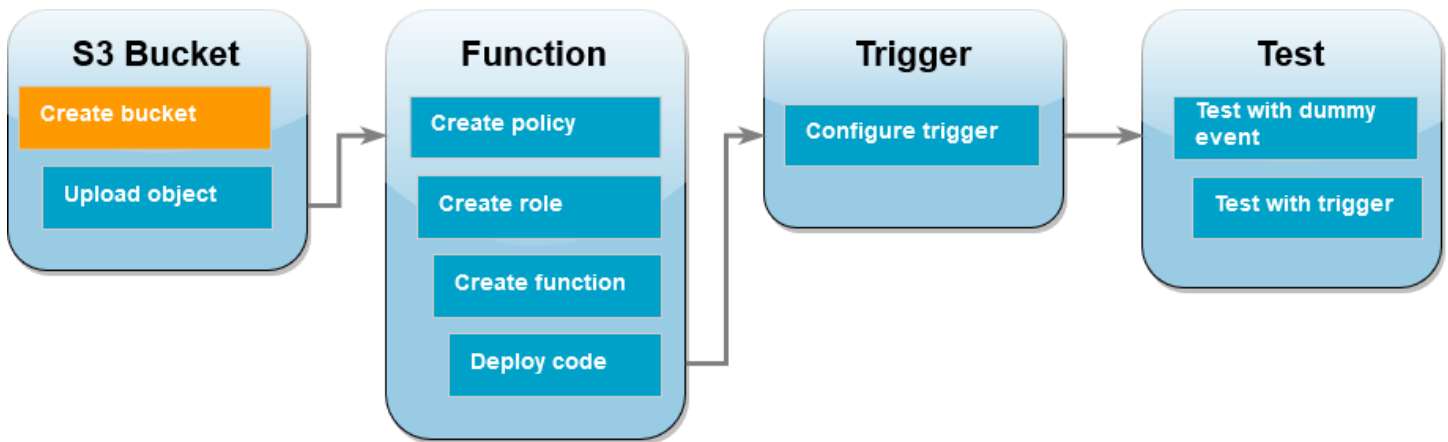
1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

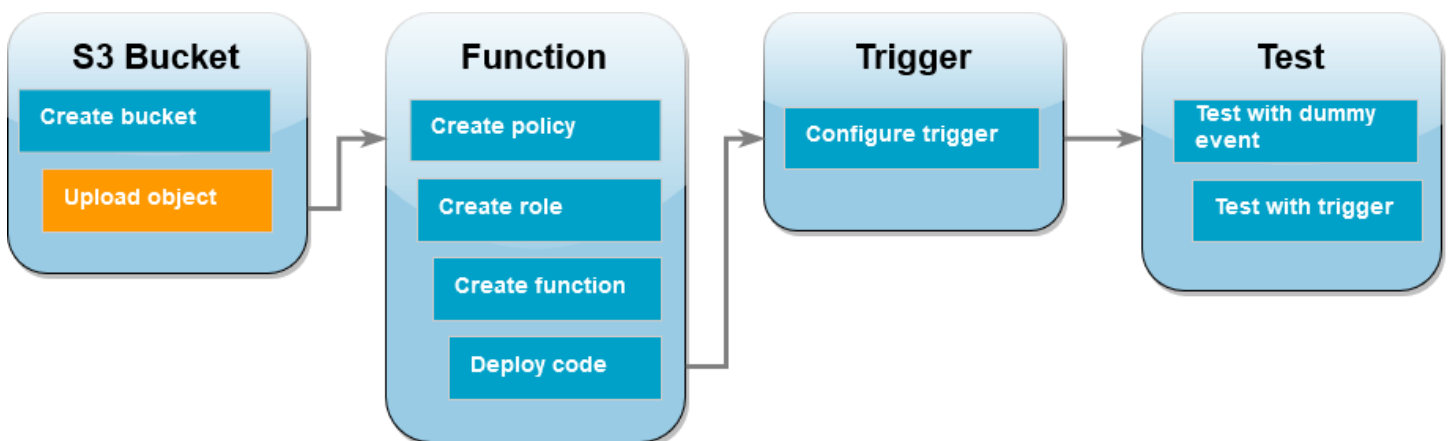
Buat bucket Amazon S3.



Untuk membuat bucket Amazon S3

1. Buka [konsol Amazon S3](#) dan pilih halaman Bucket.
2. Pilih Buat bucket.
3. Pada Konfigurasi umum, lakukan hal berikut:
 - a. Untuk nama Bucket, masukkan nama unik global yang memenuhi aturan [penamaan Amazon S3 Bucket](#). Nama bucket hanya dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-).
 - b. Untuk Wilayah AWS, pilih Wilayah. Kemudian dalam tutorial, Anda harus membuat fungsi Lambda Anda di Wilayah yang sama.
4. Biarkan semua opsi lain disetel ke nilai defaultnya dan pilih Buat bucket.

Unggah objek uji ke bucket Anda

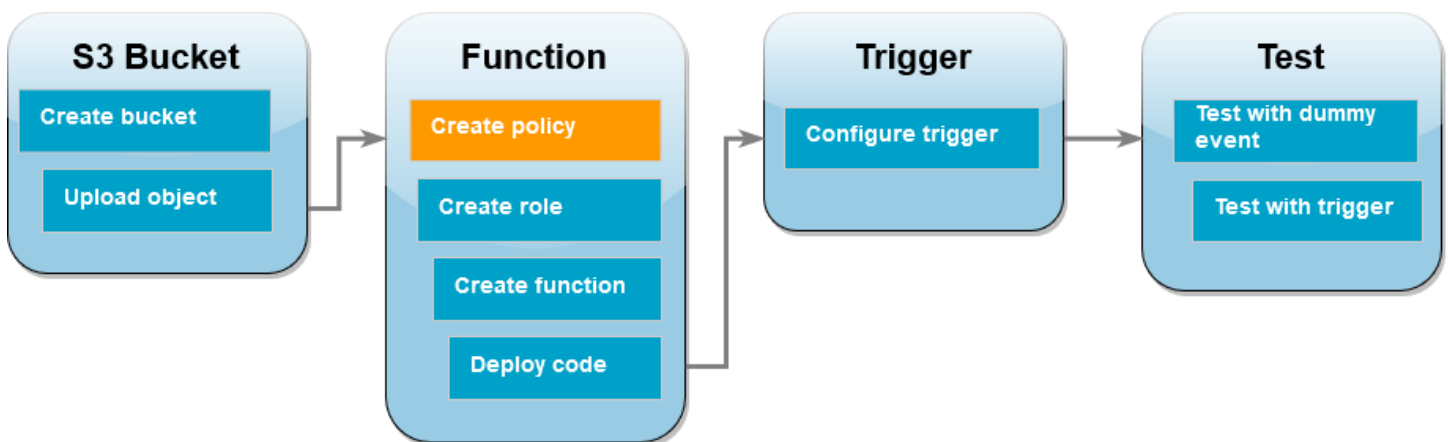


Untuk mengunggah objek uji

1. Buka halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket yang Anda buat selama langkah sebelumnya.
2. Pilih Unggah.
3. Pilih Tambahkan file dan pilih objek yang ingin Anda unggah. Anda dapat memilih file apa saja (misalnya, HappyFace .jpg).
4. Pilih Buka, lalu pilih Unggah.

Kemudian dalam tutorial, Anda akan menguji fungsi Lambda Anda menggunakan objek ini.

Membuat kebijakan izin



Buat kebijakan izin yang memungkinkan Lambda mendapatkan objek dari bucket Amazon S3 dan menulis ke Amazon Log. CloudWatch

Untuk membuat kebijakan

1. Buka [halaman Kebijakan](#) IAM konsol.
2. Pilih Buat Kebijakan.
3. Pilih JSONtab, lalu tempelkan kebijakan khusus berikut ke JSON editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

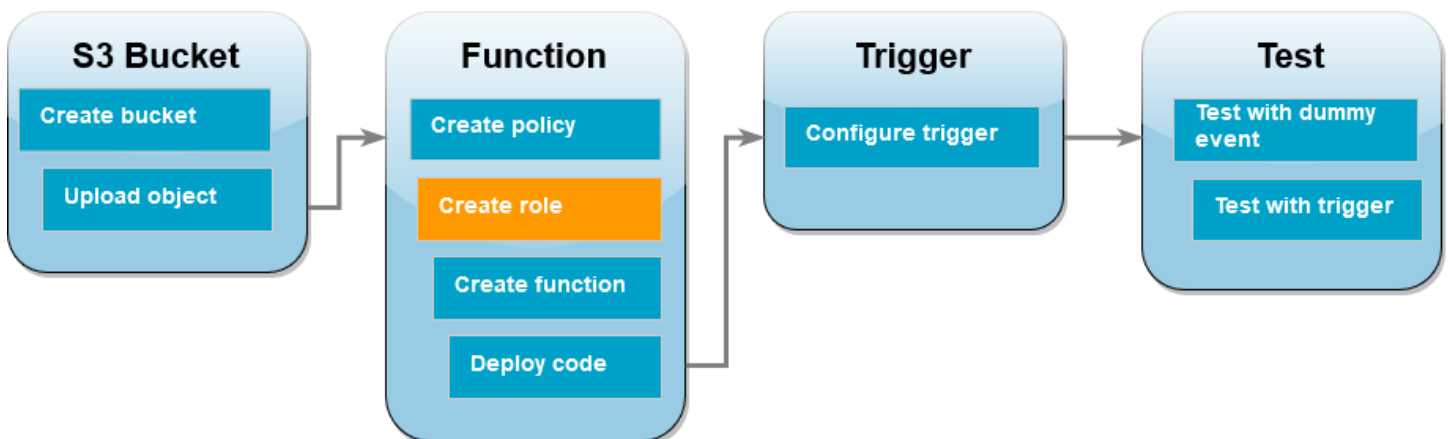
```

        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
    ],
    "Resource": "arn:aws:logs:*:*:*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::*/*"
}
]
}

```

4. Pilih Selanjutnya: Tag.
5. Pilih Berikutnya: Tinjau.
6. Di bawah Kebijakan peninjauan, untuk Nama kebijakan, masukkan **s3-trigger-tutorial**.
7. Pilih Buat kebijakan.

Membuat peran eksekusi



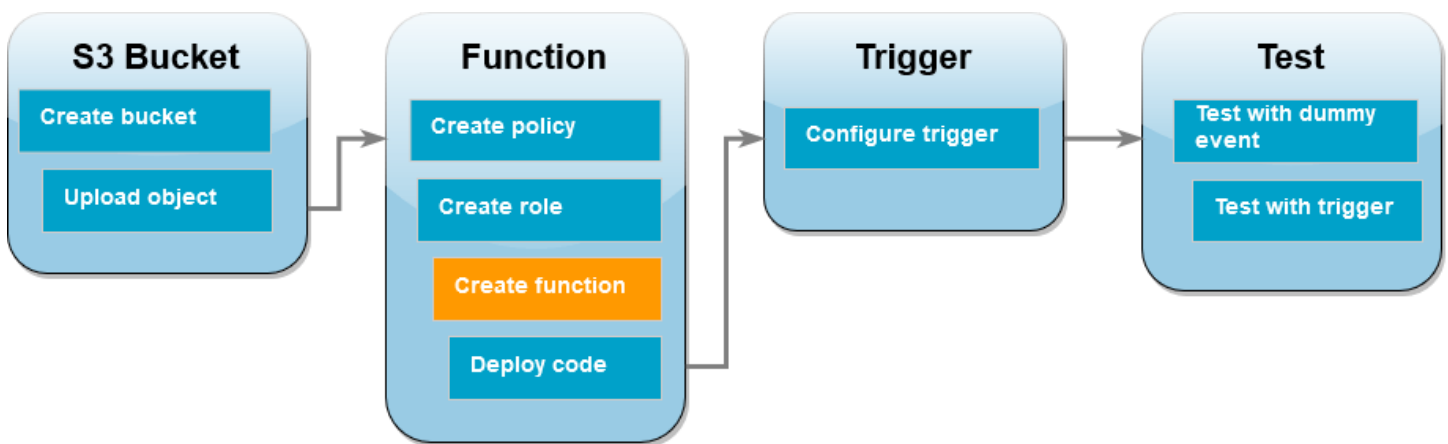
Peran [eksekusi adalah peran](#) AWS Identity and Access Management (IAM) yang memberikan izin fungsi Lambda untuk AWS mengakses layanan dan sumber daya. Pada langkah ini, buat peran eksekusi menggunakan kebijakan izin yang Anda buat di langkah sebelumnya.

Untuk membuat peran eksekusi dan melampirkan kebijakan izin kustom

1. Buka [halaman Peran](#) IAM konsol.

2. Pilih Buat peran.
3. Untuk jenis entitas tepercaya, pilih AWS layanan, lalu untuk kasus penggunaan, pilih Lambda.
4. Pilih Berikutnya.
5. Dalam kotak pencarian kebijakan, masukkan **s3-trigger-tutorial**.
6. Di hasil penelusuran, pilih kebijakan yang Anda buat (s3-trigger-tutorial), lalu pilih Berikutnya.
7. Di bawah Rincian peran, untuk nama Peran, masukkan **lambda-s3-trigger-role**, lalu pilih Buat peran.

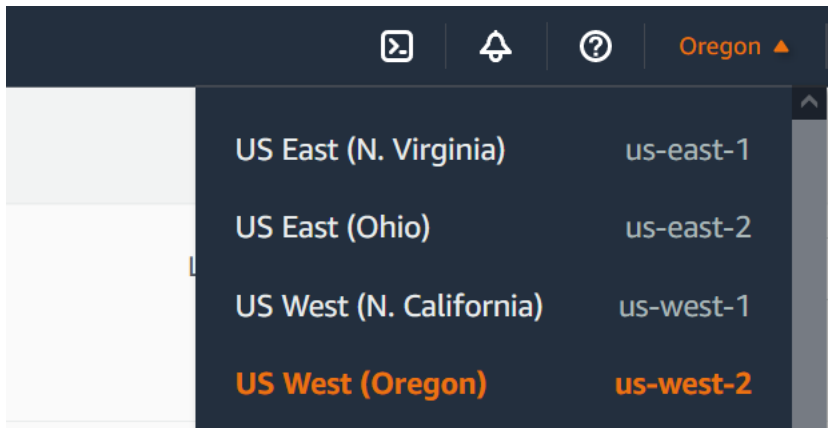
Buat fungsi Lambda



Buat fungsi Lambda di konsol menggunakan runtime Python 3.12.

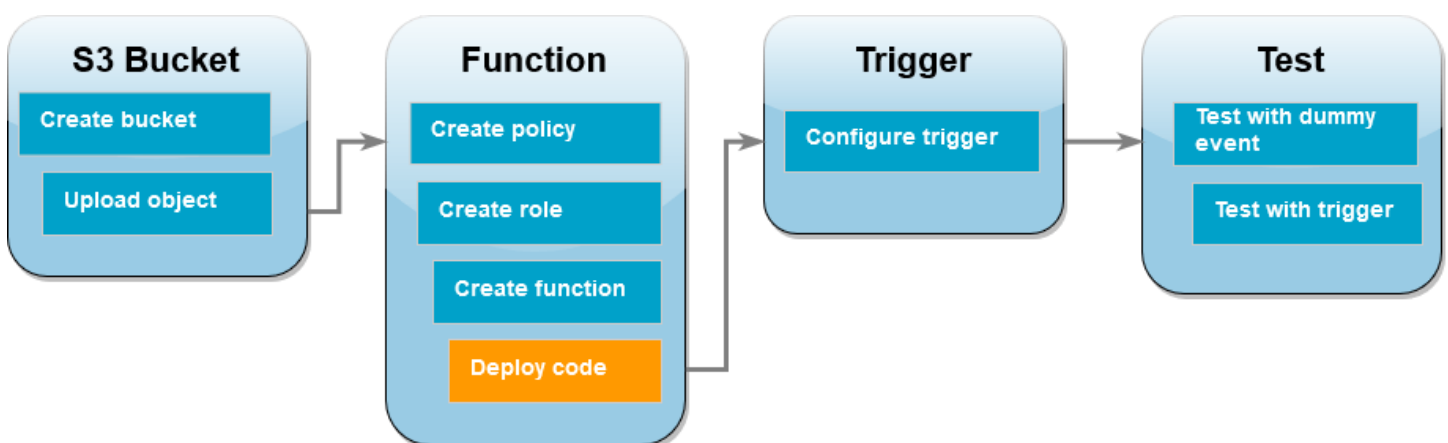
Untuk membuat fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pastikan Anda bekerja di tempat yang sama dengan saat Wilayah AWS Anda membuat bucket Amazon S3. Anda dapat mengubah Wilayah Anda menggunakan daftar drop-down di bagian atas layar.



3. Pilih Buat fungsi.
4. Pilih Penulis dari awal
5. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk nama Fungsi, masukkan `s3-trigger-tutorial`
 - b. Untuk Runtime, pilih Python 3.12.
 - c. Untuk Arsitektur, pilih `x86_64`.
6. Di tab Ubah peran eksekusi default, lakukan hal berikut:
 - a. Perluas tab, lalu pilih Gunakan peran yang ada.
 - b. Pilih yang `lambda-s3-trigger-role` Anda buat sebelumnya.
7. Pilih Buat fungsi.

Menyebarkan kode fungsi



Tutorial ini menggunakan runtime Python 3.12, tetapi kami juga menyediakan contoh file kode untuk runtime lainnya. Anda dapat memilih tab di kotak berikut untuk melihat kode runtime yang Anda minati.


Fungsi Lambda mengambil nama kunci objek yang diunggah dan nama bucket dari event parameter yang diterimanya dari Amazon S3. Fungsi kemudian menggunakan metode [get_object](#) dari AWS SDK for Python (Boto3) untuk mengambil metadata objek, termasuk tipe konten (MIMEtipe) dari objek yang diunggah.

Untuk menyebarkan kode fungsi

1. Pilih tab Python di kotak berikut dan salin kodenya.

.NET

AWS SDK for .NET

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be
// converted into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace S3Integration
{
```

```
public class Function
{
    private static AmazonS3Client _s3Client;
    public Function() : this(null)
    {
    }

    internal Function(AmazonS3Client s3Client)
    {
        _s3Client = s3Client ?? new AmazonS3Client();
    }

    public async Task<string> Handler(S3Event evt, ILambdaContext
context)
    {
        try
        {
            if (evt.Records.Count <= 0)
            {
                context.Logger.LogLine("Empty S3 Event received");
                return string.Empty;
            }

            var bucket = evt.Records[0].S3.Bucket.Name;
            var key =
HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

            context.Logger.LogLine($"Request is for {bucket} and {key}");

            var objectResult = await _s3Client.GetObjectAsync(bucket,
key);

            context.Logger.LogLine($"Returning {objectResult.Key}");


            return objectResult.Key;
        }
        catch (Exception e)
        {
            context.Logger.LogLine($"Error processing request -
{e.Message}");

            return string.Empty;
        }
    }
}
```

```
}  
}
```

Go

SDKuntuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
package main  
  
import (  
    "context"  
    "log"  
  
    "github.com/aws/aws-lambda-go/events"  
    "github.com/aws/aws-lambda-go/lambda"  
    "github.com/aws/aws-sdk-go-v2/config"  
    "github.com/aws/aws-sdk-go-v2/service/s3"  
)  
  
func handler(ctx context.Context, s3Event events.S3Event) error {  
    sdkConfig, err := config.LoadDefaultConfig(ctx)  
    if err != nil {  
        log.Printf("failed to load default config: %s", err)  
        return err  
    }  
    s3Client := s3.NewFromConfig(sdkConfig)  
  
    for _, record := range s3Event.Records {  
        bucket := record.S3.Bucket.Name  
        key := record.S3.Object.URLDecodedKey  
        headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
```

```
    Bucket: &bucket,
    Key:    &key,
  })
  if err != nil {
    log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
    return err
  }
  log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
*headOutput.ContentType)
}

return nil
}

func main() {
  lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
```

```
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
    com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNo

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger =
        LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
            S3EventNotificationRecord record = s3event.getRecords().get(0);
            String srcBucket = record.getS3().getBucket().getName();
            String srcKey = record.getS3().getObject().getUrlDecodedKey();

            S3Client s3Client = S3Client.builder().build();
            HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
srcKey);

            logger.info("Successfully retrieved " + srcBucket + "/" + srcKey +
" of type " + headObject.contentType());

            return "Ok";
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String
bucket, String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
            .bucket(bucket)
            .key(key)
            .build();
        return s3Client.headObject(headObjectRequest);
    }
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan menggunakan JavaScript Lambda.

```
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

export const handler = async (event, context) => {

  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, ' '));

  try {
    const { ContentType } = await client.send(new HeadObjectCommand({
      Bucket: bucket,
      Key: key,
    }));

    console.log('CONTENT TYPE:', ContentType);
    return ContentType;

  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}.
    Make sure they exist and your bucket is in the same region as this
    function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

Mengkonsumsi acara S3 dengan menggunakan TypeScript Lambda.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> =>
{
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, ' '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make
sure they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

PHP

SDKuntuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara S3 dengan menggunakan PHP Lambda.

```
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());
```



```
        try {
            $fileSize = urldecode($record->getObject()->getSize());
            echo "File Size: " . $fileSize . "\n";
            // TODO: Implement your custom processing logic here
        } catch (Exception $e) {
            echo $e->getMessage() . "\n";
            echo 'Error getting object ' . $key . ' from bucket ' .
            $bucket . '. Make sure they exist and your bucket is in the same region as
            this function.' . "\n";
            throw $e;
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')
```

```
def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']
['key'], encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they
exist and your bucket is in the same region as this function.'.format(key,
bucket))
        raise e
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan Lambda menggunakan Ruby.

```
require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'

def lambda_handler(event:, context:)
    s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
```

```
# puts "Received event: #{JSON.dump(event)}"

# Get the object from the event and show its content type
bucket = event['Records'][0]['s3']['bucket']['name']
key = URI.decode_www_form_component(event['Records'][0]['s3']['object']
['key'], Encoding::UTF_8)
begin
  response = s3.get_object(bucket: bucket, key: key)
  puts "CONTENT TYPE: #{response.content_type}"
  return response.content_type
rescue StandardError => e
  puts e.message
  puts "Error getting object #{key} from bucket #{bucket}. Make sure they
exist and your bucket is in the same region as this function."
  raise e
end
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Main function
#[tokio::main]
async fn main() -> Result<(), Error> {
```

```
tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

// Initialize the AWS SDK for Rust
let config = aws_config::load_from_env().await;
let s3_client = Client::new(&config);

let res = run(service_fn(|request: LambdaEvent<S3Event>| {
    function_handler(&s3_client, request)
})).await;

res
}

async fn function_handler(
    s3_client: &Client,
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request
from SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket =
    evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket name to
exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object
key to exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;

    match s3_get_object_result {
```

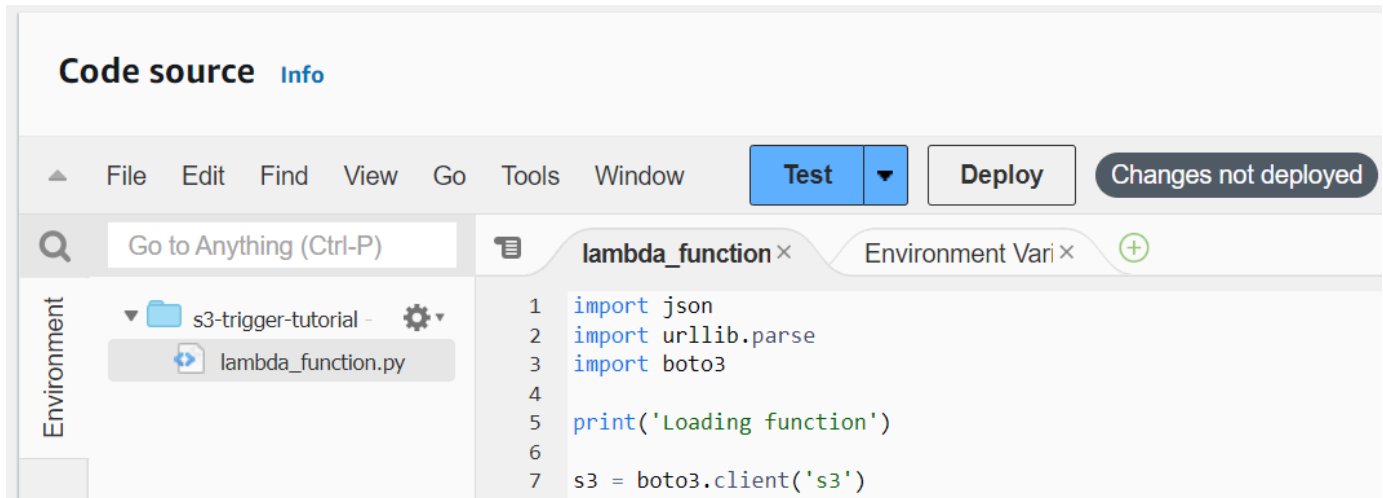
```

    Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
contains a 'body' property of type ByteStream"),
    Err(_) => tracing::info!("Failure with S3 Get Object request")
}

Ok(())
}

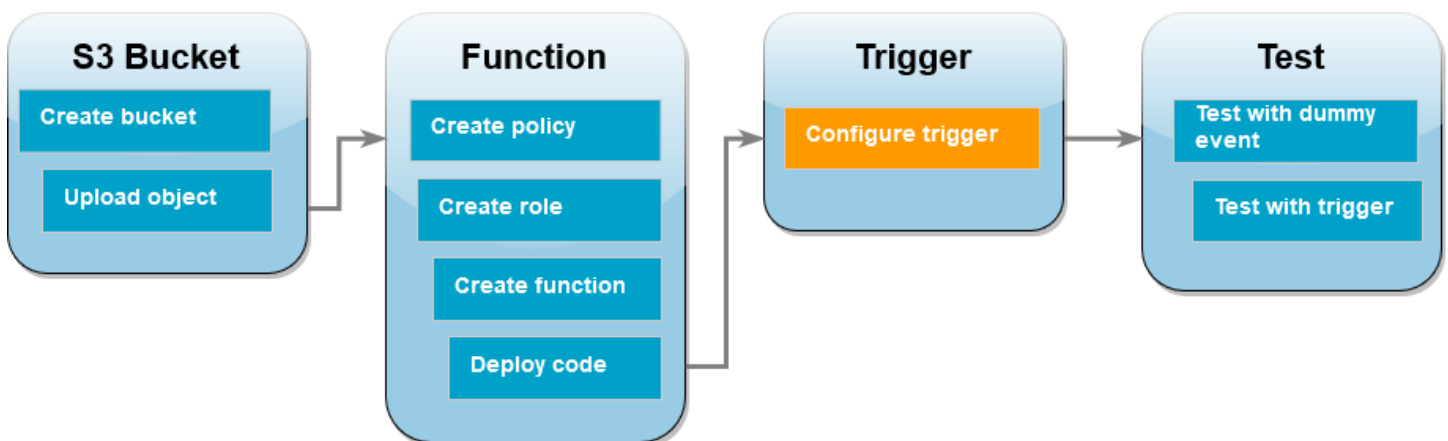
```

- Di panel Sumber kode di konsol Lambda, tempel kode ke file `lambda_function.py`.



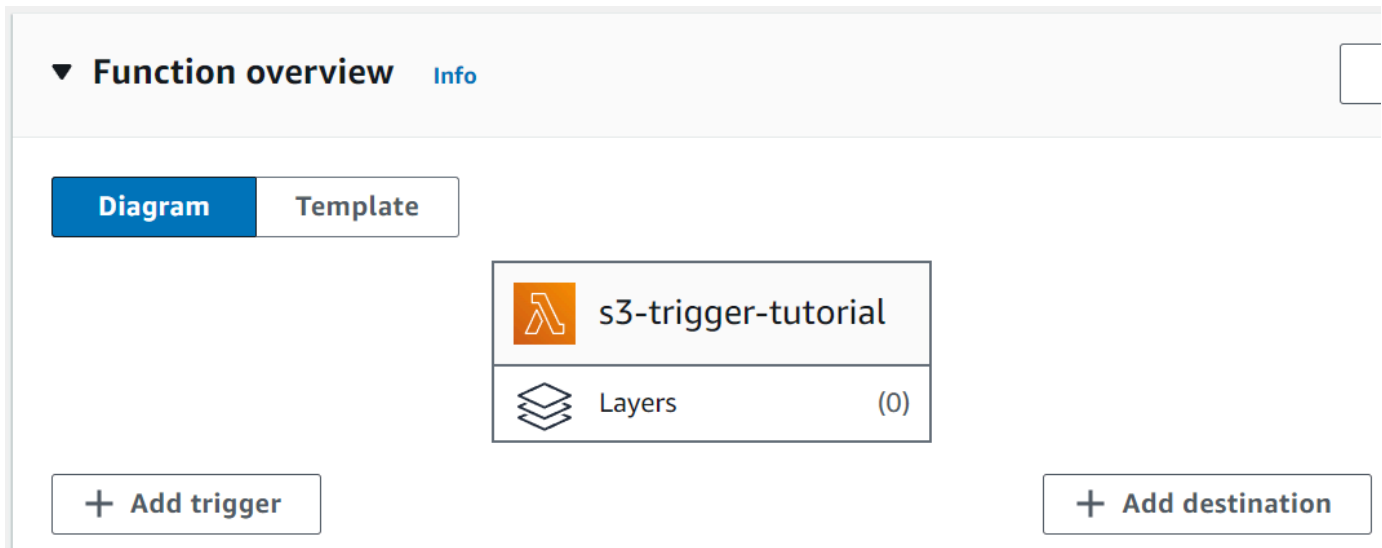
- Pilih Deploy.

Buat pemicu Amazon S3




Untuk membuat pemicu Amazon S3


- Di panel Ikhtisar fungsi, pilih Tambah pemicu.



▼ **Function overview** [Info](#)

Diagram Template

 s3-trigger-tutorial

 Layers (0)

+ Add trigger

+ Add destination

2. Pilih S3.
3. Di bawah Bucket, pilih bucket yang Anda buat sebelumnya di tutorial.
4. Di bawah Jenis acara, pastikan bahwa Semua peristiwa pembuatan objek dipilih.
5. Di bawah Pemanggilan rekursif, pilih kotak centang untuk mengetahui bahwa tidak disarankan menggunakan bucket Amazon S3 yang sama untuk input dan output.
6. Pilih Tambahkan.

Note

[Saat Anda membuat pemacu Amazon S3 untuk fungsi Lambda menggunakan konsol Lambda, Amazon S3 mengonfigurasi pemberitahuan peristiwa di bucket yang Anda tentukan.](#)

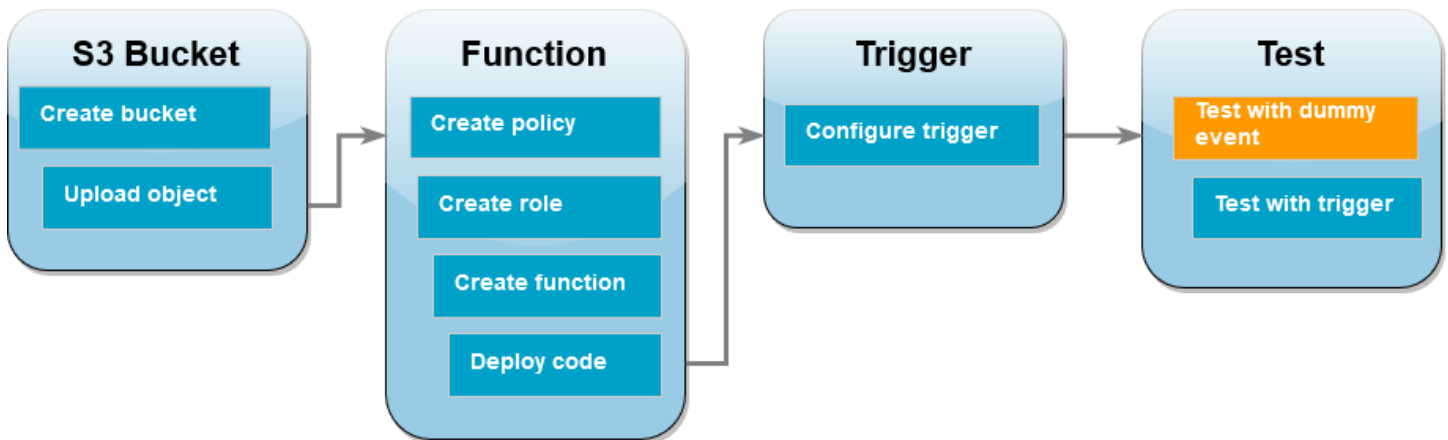
Sebelum mengonfigurasi pemberitahuan peristiwa ini, Amazon S3 melakukan serangkaian pemeriksaan untuk mengonfirmasi bahwa tujuan acara ada dan memiliki kebijakan yang IAM diperlukan. Amazon S3 juga melakukan pengujian ini pada notifikasi acara lain yang dikonfigurasi untuk bucket itu.

Karena pemeriksaan ini, jika bucket sebelumnya telah mengonfigurasi tujuan peristiwa untuk sumber daya yang tidak ada lagi, atau untuk sumber daya yang tidak memiliki kebijakan izin yang diperlukan, Amazon S3 tidak akan dapat membuat notifikasi peristiwa baru. Anda akan melihat pesan galat berikut yang menunjukkan bahwa pemacu Anda tidak dapat dibuat:

```
An error occurred when creating the trigger: Unable to validate the following destination configurations.
```

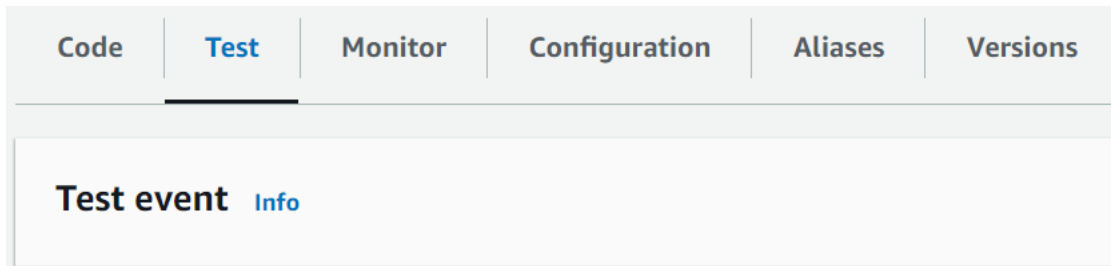
Anda dapat melihat kesalahan ini jika sebelumnya mengonfigurasi pemicu untuk fungsi Lambda lain menggunakan bucket yang sama, dan sejak itu Anda telah menghapus fungsi tersebut atau memodifikasi kebijakan izinnya.

Uji fungsi Lambda Anda dengan acara dummy



Untuk menguji fungsi Lambda dengan acara dummy

1. Di halaman konsol Lambda untuk fungsi Anda, pilih tab Uji.



2. Untuk Nama peristiwa, masukkan MyTestEvent.
3. Dalam Peristiwa tersebut JSON, tempel acara pengujian berikut. Pastikan untuk mengganti nilai-nilai ini:
 - Ganti us-east-1 dengan wilayah tempat Anda membuat bucket Amazon S3.
 - Ganti kedua instance amzn-s3-demo-bucket dengan nama bucket Amazon S3 Anda sendiri.
 - Ganti test%2FKey dengan nama objek pengujian yang Anda unggah ke bucket sebelumnya (misalnya,HappyFace.jpg).

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
  ]
}

```

4. Pilih Simpan.

5. Pilih Uji.
6. Jika fungsi Anda berjalan dengan sukses, Anda akan melihat output yang mirip dengan yang berikut ini di tab Hasil eksekusi.

Response

```
"image/jpeg"
```

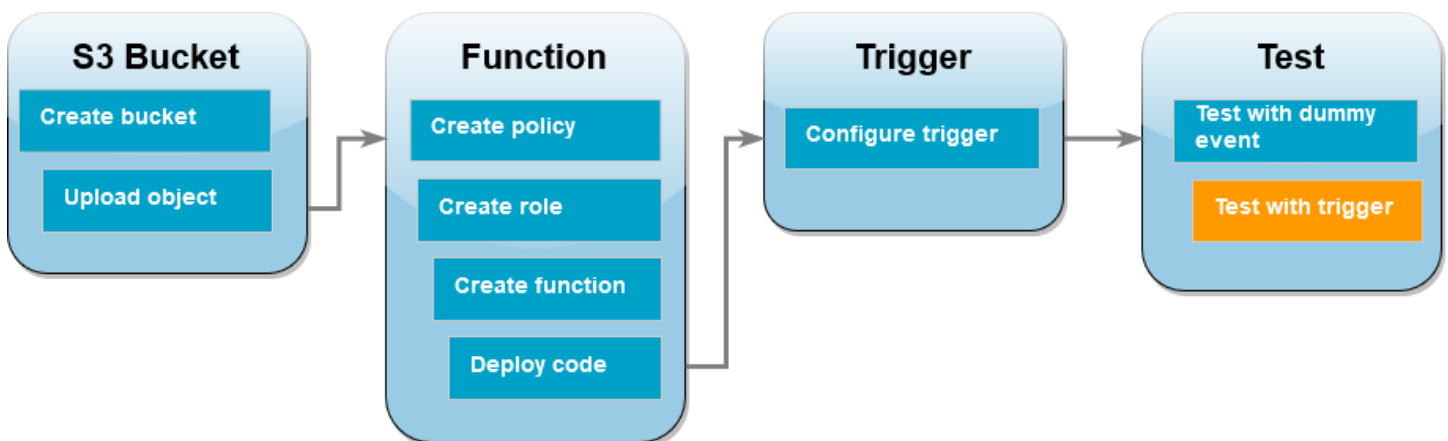
Function Logs

```
START RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6 Version: $LATEST
2021-02-18T21:40:59.280Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    INPUT
  BUCKET AND KEY:  { Bucket: 'amzn-s3-demo-bucket', Key: 'HappyFace.jpg' }
2021-02-18T21:41:00.215Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    CONTENT
  TYPE: image/jpeg
END RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6
REPORT RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6    Duration: 976.25 ms
  Billed Duration: 977 ms    Memory Size: 128 MB    Max Memory Used: 90 MB    Init
  Duration: 430.47 ms
```

Request ID

```
12b3cae7-5f4e-415e-93e6-416b8f8b66e6
```

Uji fungsi Lambda dengan pemicu Amazon S3



Untuk menguji fungsi Anda dengan pemicu yang dikonfigurasi, unggah objek ke bucket Amazon S3 menggunakan konsol. Untuk memverifikasi bahwa fungsi Lambda Anda berjalan seperti yang diharapkan, gunakan CloudWatch Log untuk melihat output fungsi Anda.

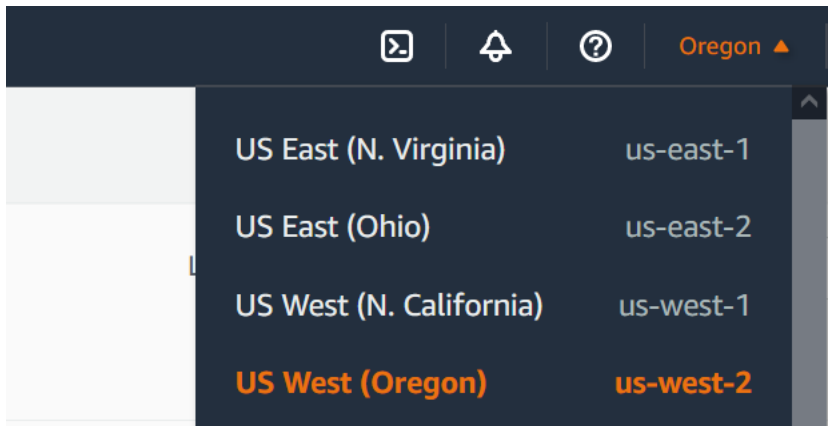
Untuk mengunggah objek ke bucket Amazon S3 Anda

1. Buka halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket yang Anda buat sebelumnya.

2. Pilih Unggah.
3. Pilih Tambahkan file dan gunakan pemilih file untuk memilih objek yang ingin Anda unggah. Objek ini dapat berupa file apa pun yang Anda pilih.
4. Pilih Buka, lalu pilih Unggah.

Untuk memverifikasi pemanggilan fungsi menggunakan Log CloudWatch

1. Buka [CloudWatch](#) konsol.
2. Pastikan Anda bekerja sama dengan saat Wilayah AWS Anda membuat fungsi Lambda Anda. Anda dapat mengubah Wilayah Anda menggunakan daftar drop-down di bagian atas layar.



3. Pilih Log, lalu pilih Grup log.
4. Pilih grup log untuk fungsi Anda (`/aws/lambda/s3-trigger-tutorial`).
5. Di bawah Aliran log, pilih aliran log terbaru.
6. Jika fungsi Anda dipanggil dengan benar sebagai respons terhadap pemicu Amazon S3 Anda, Anda akan melihat output yang mirip dengan berikut ini. Yang `CONTENT TYPE` Anda lihat tergantung pada jenis file yang Anda unggah ke bucket Anda.

```
2022-05-09T23:17:28.702Z 0cae7f5a-b0af-4c73-8563-a3430333cc10 INFO CONTENT  
TYPE: image/jpeg
```

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Akun AWS.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus bucket S3

1. Buka [konsol Amazon S3](#).
2. Pilih bucket yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama ember di bidang input teks.
5. Pilih Hapus bucket.

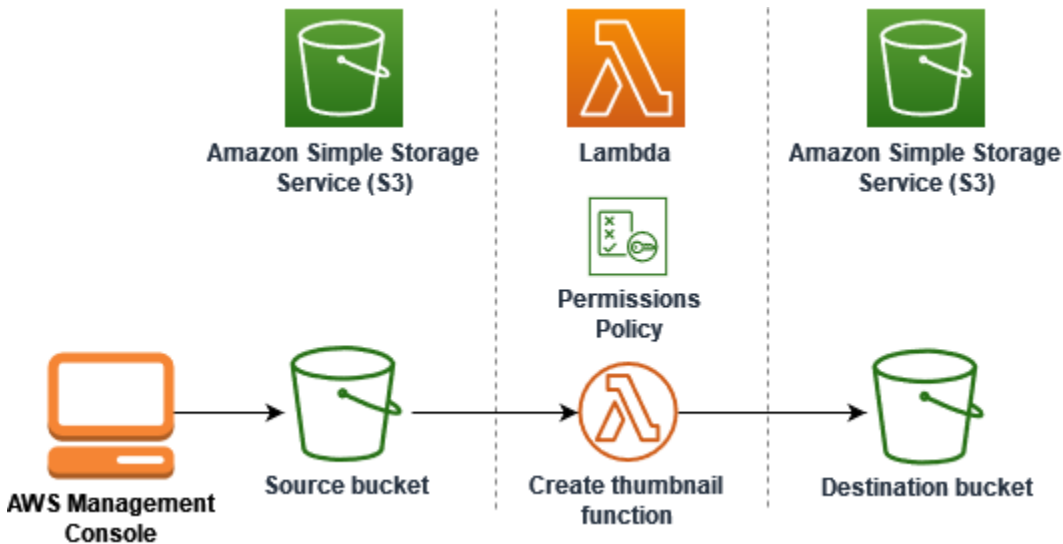
Langkah selanjutnya

Di [Tutorial: Menggunakan pemicu Amazon S3 untuk membuat gambar thumbnail](#), pemicu Amazon S3 memanggil fungsi yang membuat gambar thumbnail untuk setiap file gambar yang diunggah ke bucket. Tutorial ini membutuhkan pengetahuan domain Lambda AWS dan tingkat moderat. Ini menunjukkan cara membuat sumber daya menggunakan AWS Command Line Interface (AWS CLI) dan cara membuat paket penyebaran arsip file.zip untuk fungsi dan dependensinya.

Tutorial: Menggunakan pemicu Amazon S3 untuk membuat gambar thumbnail

Dalam tutorial ini, Anda membuat dan mengonfigurasi fungsi Lambda yang mengubah ukuran gambar yang ditambahkan ke bucket Amazon Simple Storage Service (Amazon S3). Saat

menambahkan file gambar ke bucket, Amazon S3 akan memanggil fungsi Lambda. Fungsi tersebut kemudian membuat versi thumbnail gambar dan mengeluarkannya ke bucket Amazon S3 yang berbeda.



Untuk menyelesaikan tutorial ini, Anda melakukan langkah-langkah berikut:

1. Buat bucket Amazon S3 sumber dan tujuan dan unggah gambar sampel.
2. Buat fungsi Lambda yang mengubah ukuran gambar dan mengeluarkan thumbnail ke bucket Amazon S3.
3. Konfigurasi pemicu Lambda yang memanggil fungsi Anda saat objek diunggah ke bucket sumber Anda.
4. Uji fungsi Anda, pertama dengan acara dummy, lalu dengan mengunggah gambar ke bucket sumber Anda.

Dengan menyelesaikan langkah-langkah ini, Anda akan mempelajari cara menggunakan Lambda untuk menjalankan tugas pemrosesan file pada objek yang ditambahkan ke bucket Amazon S3. Anda dapat menyelesaikan tutorial ini menggunakan AWS Command Line Interface (AWS CLI) atau AWS Management Console.

Jika Anda mencari contoh sederhana untuk mempelajari cara mengonfigurasi pemicu Amazon S3 untuk Lambda, Anda dapat mencoba [Tutorial: Menggunakan pemicu Amazon S3 untuk menjalankan fungsi Lambda](#).

Topik

- [Prasyarat](#)

- [Buat dua ember Amazon S3](#)
- [Unggah gambar uji ke bucket sumber Anda](#)
- [Membuat kebijakan izin](#)
- [Membuat peran eksekusi](#)
- [Buat paket penerapan fungsi](#)
- [Buat fungsi Lambda](#)
- [Konfigurasi Amazon S3 untuk menjalankan fungsi](#)
- [Uji fungsi Lambda Anda dengan acara dummy](#)
- [Uji fungsi Anda menggunakan pemicu Amazon S3](#)
- [Bersihkan sumber daya Anda](#)

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimkan Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi <https://aws.amazon.com/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftarkan Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

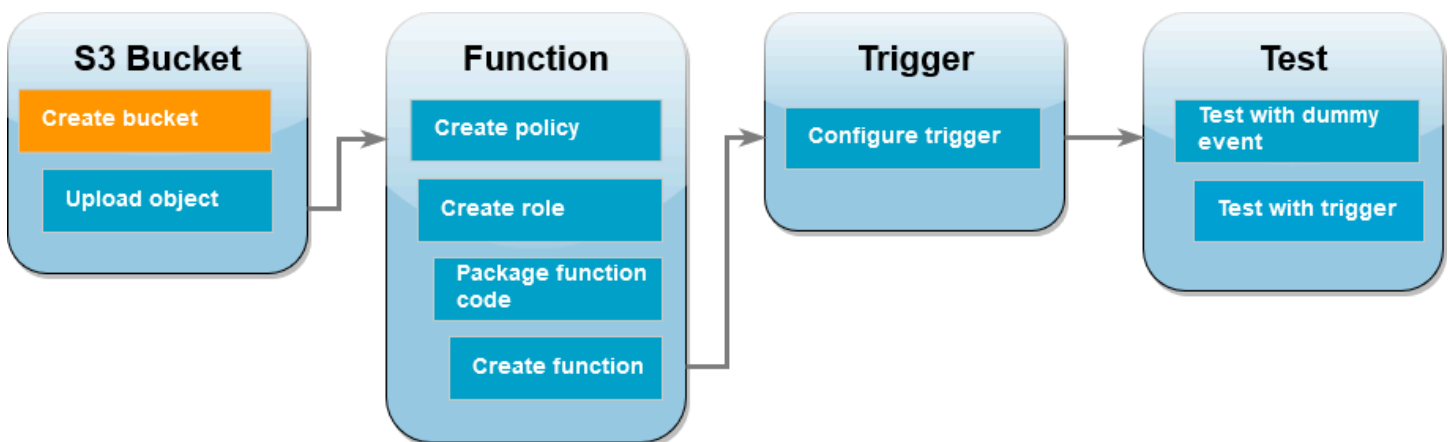
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Jika Anda ingin menggunakan AWS CLI untuk menyelesaikan tutorial, instal [versi terbaru dari AWS Command Line Interface](#).

Untuk kode fungsi Lambda Anda, Anda dapat menggunakan Python atau Node.js. Instal alat dukungan bahasa dan manajer paket untuk bahasa yang ingin Anda gunakan.

Buat dua ember Amazon S3



Pertama buat dua ember Amazon S3. Bucket pertama adalah bucket sumber tempat Anda akan mengunggah gambar Anda. Bucket kedua digunakan oleh Lambda untuk menyimpan thumbnail yang diubah ukurannya saat Anda menjalankan fungsi.

AWS Management Console

Untuk membuat bucket Amazon S3 (konsol)

1. Buka halaman [Bucket](#) konsol Amazon S3.
2. Pilih Buat bucket.
3. Pada Konfigurasi umum, lakukan hal berikut:

- a. Untuk nama Bucket, masukkan nama unik global yang memenuhi aturan [penamaan Amazon S3 Bucket](#). Nama bucket hanya dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-).
 - b. Untuk Wilayah AWS, pilih yang paling [Wilayah AWS](#)dekat dengan lokasi geografis Anda. Kemudian dalam tutorial, Anda harus membuat fungsi Lambda Anda dalam hal yang sama Wilayah AWS, jadi catat wilayah yang Anda pilih.
4. Biarkan semua opsi lain disetel ke nilai defaultnya dan pilih Buat bucket.
 5. Ulangi langkah 1 hingga 4 untuk membuat bucket tujuan Anda. Untuk nama Bucket **amzn-s3-demo-source-bucket-resized**, masukkan, di **amzn-s3-demo-source-bucket** mana nama bucket sumber yang baru saja Anda buat.

AWS CLI

Untuk membuat bucket Amazon S3 ()AWS CLI

1. Jalankan CLI perintah berikut untuk membuat bucket sumber Anda. Nama yang Anda pilih untuk bucket Anda harus unik secara global dan ikuti aturan [penamaan Amazon S3 Bucket](#). Nama hanya dapat berisi huruf kecil, angka, titik (.), dan tanda hubung (-). Untuk region dan LocationConstraint, pilih yang paling [Wilayah AWS](#)dekat dengan lokasi geografis Anda.

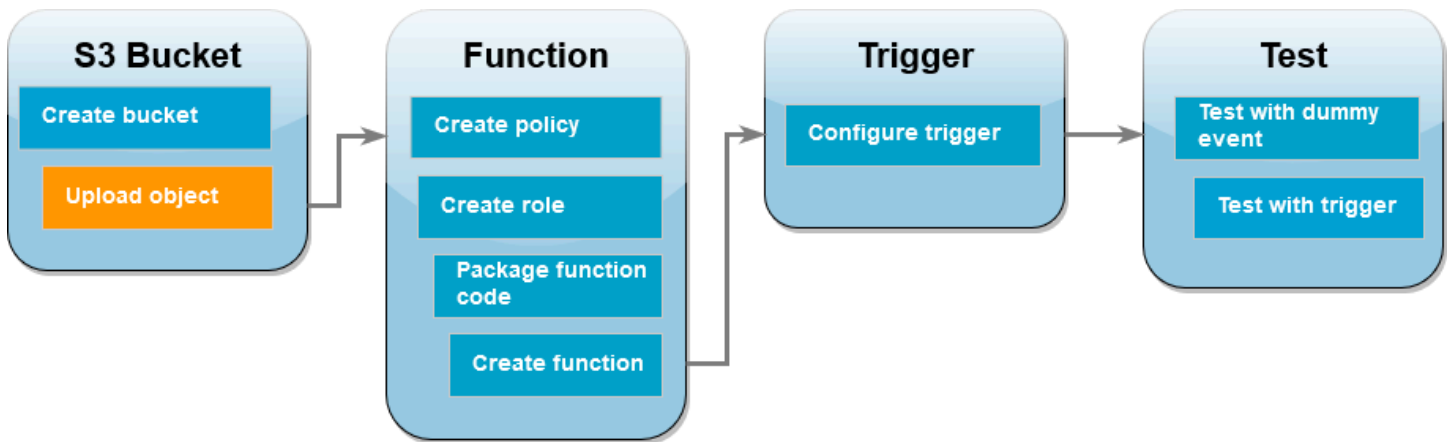
```
aws s3api create-bucket --bucket amzn-s3-demo-source-bucket --region us-east-1 \  
--create-bucket-configuration LocationConstraint=us-east-1
```

Kemudian dalam tutorial, Anda harus membuat fungsi Lambda Anda Wilayah AWS sama dengan bucket sumber Anda, jadi catat wilayah yang Anda pilih.

2. Jalankan perintah berikut untuk membuat bucket tujuan Anda. Untuk nama bucket, Anda harus menggunakan **amzn-s3-demo-source-bucket-resized**, di **amzn-s3-demo-source-bucket** mana nama bucket sumber yang Anda buat di langkah 1. Untuk region dan LocationConstraint, pilih yang sama dengan yang Wilayah AWS Anda gunakan untuk membuat bucket sumber Anda.

```
aws s3api create-bucket --bucket amzn-s3-demo-source-bucket-resized --region us-east-1 \  
--create-bucket-configuration LocationConstraint=us-east-1
```


Unggah gambar uji ke bucket sumber Anda



Kemudian dalam tutorial, Anda akan menguji fungsi Lambda Anda dengan memanggilnya menggunakan atau konsol Lambda. AWS CLI Untuk mengonfirmasi bahwa fungsi Anda beroperasi dengan benar, bucket sumber Anda harus berisi gambar uji. Gambar ini dapat berupa PNG file JPG atau apa saja yang Anda pilih.

AWS Management Console

Untuk mengunggah gambar uji ke bucket sumber Anda (konsol)

1. Buka halaman [Bucket](#) konsol Amazon S3.
2. Pilih bucket sumber yang Anda buat di langkah sebelumnya.
3. Pilih Unggah.
4. Pilih Tambahkan file dan gunakan pemilih file untuk memilih objek yang ingin Anda unggah.
5. Pilih Buka, lalu pilih Unggah.

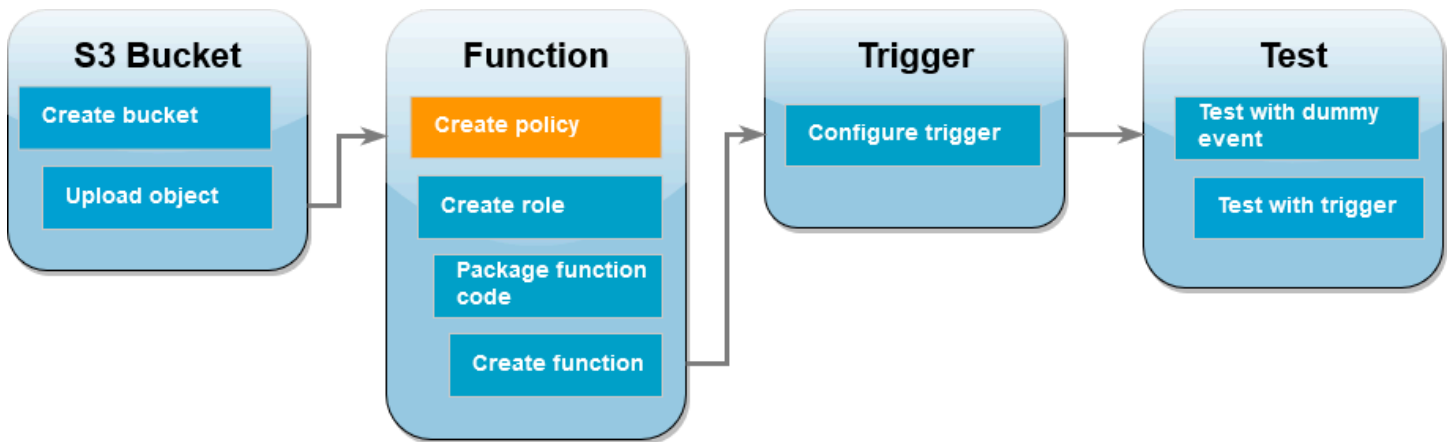
AWS CLI

Untuk mengunggah gambar uji ke bucket sumber Anda (AWS CLI)

- Dari direktori yang berisi gambar yang ingin Anda unggah, jalankan CLI perintah berikut. Ganti `--bucket` parameter dengan nama bucket sumber Anda. Untuk `--body` parameter `--key` dan, gunakan nama file gambar pengujian Anda.

```
aws s3api put-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg --body ./HappyFace.jpg
```

Membuat kebijakan izin



Langkah pertama dalam membuat fungsi Lambda Anda adalah membuat kebijakan izin. Kebijakan ini memberi fungsi Anda izin yang diperlukan untuk mengakses AWS sumber daya lain. Untuk tutorial ini, kebijakan memberikan izin baca dan tulis Lambda untuk bucket Amazon S3 dan memungkinkannya untuk menulis ke Amazon Log. CloudWatch

AWS Management Console

Untuk membuat kebijakan (konsol)

1. Buka halaman [Kebijakan](#) pada konsol AWS Identity and Access Management (IAM).
2. Pilih Buat kebijakan.
3. Pilih JSONtab, lalu tempelkan kebijakan khusus berikut ke JSON editor.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
  
```

```

        "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::*/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::*/*"
  }
]
}

```

4. Pilih Berikutnya.
5. Di bawah Detail kebijakan, untuk nama Kebijakan, masukkan **LambdaS3Policy**.
6. Pilih Buat kebijakan.

AWS CLI

Untuk membuat kebijakan (AWS CLI)

1. Simpan yang berikut ini JSON dalam file bernama `policy.json`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::*/*"
    }
  ]
}

```

```

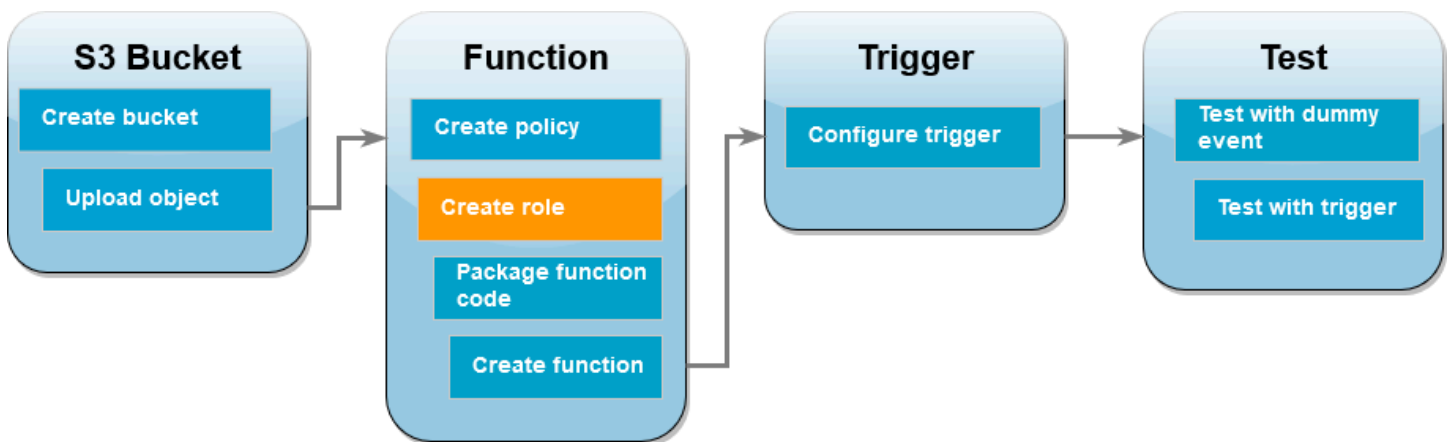
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::*/*"
    }
  ]
}

```

2. Dari direktori tempat Anda menyimpan dokumen JSON kebijakan, jalankan CLI perintah berikut.

```
aws iam create-policy --policy-name LambdaS3Policy --policy-document file://policy.json
```

Membuat peran eksekusi



Peran eksekusi adalah IAM peran yang memberikan izin fungsi Lambda untuk AWS layanan mengakses dan sumber daya. Untuk memberikan akses baca dan tulis fungsi ke bucket Amazon S3, Anda melampirkan kebijakan izin yang Anda buat di langkah sebelumnya.

AWS Management Console

Untuk membuat peran eksekusi dan melampirkan kebijakan izin Anda (konsol)

1. Buka halaman [Peran](#) pada konsol (IAM).
2. Pilih Buat peran.

3. Untuk jenis entitas Tepercaya, pilih AWS layanan, dan untuk kasus Penggunaan, pilih Lambda.
4. Pilih Berikutnya.
5. Tambahkan kebijakan izin yang Anda buat di langkah sebelumnya dengan melakukan hal berikut:
 - a. Dalam kotak pencarian kebijakan, masukkan **LambdaS3Policy**.
 - b. Dalam hasil pencarian, pilih kotak centang untuk **LambdaS3Policy**.
 - c. Pilih Berikutnya.
6. Di bawah Rincian peran, untuk nama Peran masuk **LambdaS3Role**.
7. Pilih Buat peran.

AWS CLI

Untuk membuat peran eksekusi dan melampirkan kebijakan izin Anda ()AWS CLI

1. Simpan yang berikut ini JSON dalam file bernama `trust-policy.json`. Kebijakan kepercayaan ini memungkinkan Lambda untuk menggunakan izin peran dengan memberikan `lambda.amazonaws.com` izin utama layanan untuk memanggil tindakan AWS Security Token Service ()AWS STS. `AssumeRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

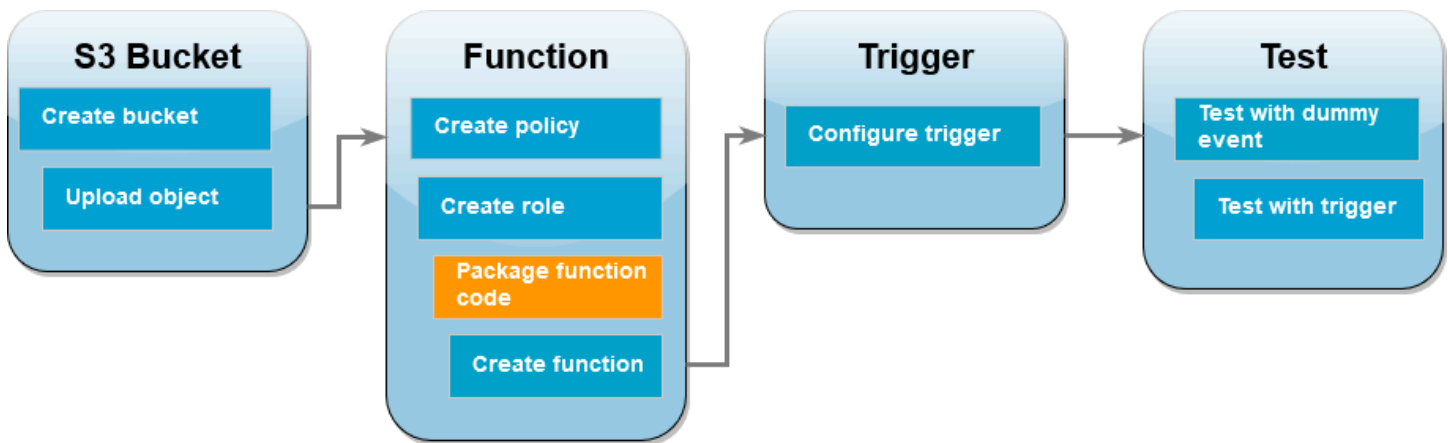
2. Dari direktori tempat Anda menyimpan dokumen kebijakan JSON kepercayaan, jalankan CLI perintah berikut untuk membuat peran eksekusi.

```
aws iam create-role --role-name LambdaS3Role --assume-role-policy-document
file://trust-policy.json
```

- Untuk melampirkan kebijakan izin yang Anda buat pada langkah sebelumnya, jalankan CLI perintah berikut. Ganti Akun AWS nomor dalam polis ARN dengan nomor akun Anda sendiri.

```
aws iam attach-role-policy --role-name LambdaS3Role --policy-arn
arn:aws:iam::123456789012:policy/LambdaS3Policy
```

Buat paket penerapan fungsi



Untuk membuat fungsi Anda, Anda membuat paket deployment yang berisi kode fungsi dan dependensinya. Untuk `CreateThumbnail` fungsi ini, kode fungsi Anda menggunakan pustaka terpisah untuk mengubah ukuran gambar. Ikuti instruksi untuk bahasa yang Anda pilih untuk membuat paket penyebaran yang berisi pustaka yang diperlukan.

Node.js

Untuk membuat paket penyebaran (Node.js)

- Buat direktori bernama `lambda-s3` untuk kode fungsi dan dependensi Anda dan navigasikan ke dalamnya.

```
mkdir lambda-s3
cd lambda-s3
```

- Buat proyek Node.js baru dengan `npm`. Untuk menerima opsi default yang disediakan dalam pengalaman interaktif, tekan `Enter`.

```
npm init
```

3. Simpan kode fungsi berikut dalam file bernama `index.mjs`. Pastikan untuk mengganti `us-east-1` dengan Wilayah AWS di mana Anda membuat ember sumber dan tujuan Anda sendiri.

```
// dependencies
import { S3Client, GetObjectCommand, PutObjectCommand } from '@aws-sdk/client-s3';

import { Readable } from 'stream';

import sharp from 'sharp';
import util from 'util';

// create S3 client
const s3 = new S3Client({region: 'us-east-1'});

// define the handler function
export const handler = async (event, context) => {

// Read options from the event parameter and get the source bucket
console.log("Reading options from event:\n", util.inspect(event, {depth: 5}));
  const srcBucket = event.Records[0].s3.bucket.name;

// Object key may have spaces or unicode non-ASCII characters
const srcKey = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, " "));
const dstBucket = srcBucket + "-resized";
const dstKey = "resized-" + srcKey;

// Infer the image type from the file suffix
const typeMatch = srcKey.match(/\.[^\.]*$/);
if (!typeMatch) {
  console.log("Could not determine the image type.");
  return;
}

// Check that the image type is supported
const imageType = typeMatch[1].toLowerCase();
if (imageType !== "jpg" && imageType !== "png") {
```

```
    console.log(`Unsupported image type: ${imageType}`);
    return;
}

// Get the image from the source bucket. GetObjectCommand returns a stream.
try {
    const params = {
        Bucket: srcBucket,
        Key: srcKey
    };
    var response = await s3.send(new GetObjectCommand(params));
    var stream = response.Body;

    // Convert stream to buffer to pass to sharp resize function.
    if (stream instanceof Readable) {
        var content_buffer = Buffer.concat(await stream.toArray());

    } else {
        throw new Error('Unknown object stream type');
    }

} catch (error) {
    console.log(error);
    return;
}

// set thumbnail width. Resize will set the height automatically to maintain
// aspect ratio.
const width = 200;

// Use the sharp module to resize the image and save in a buffer.
try {
    var output_buffer = await sharp(content_buffer).resize(width).toBuffer();

} catch (error) {
    console.log(error);
    return;
}

// Upload the thumbnail image to the destination bucket
try {
    const destparams = {
```



```

    Bucket: dstBucket,
    Key: dstKey,
    Body: output_buffer,
    ContentType: "image"
  };

  const putResult = await s3.send(new PutObjectCommand(destparams));

  } catch (error) {
    console.log(error);
    return;
  }

  console.log('Successfully resized ' + srcBucket + '/' + srcKey +
    ' and uploaded to ' + dstBucket + '/' + dstKey);
};

```

4. Di `lambda-s3` direktori Anda, instal perpustakaan tajam menggunakan `npm`. Perhatikan bahwa versi terbaru dari `sharp` (0.33) tidak kompatibel dengan Lambda. Instal versi 0.32.6 untuk menyelesaikan tutorial ini.

```
npm install sharp@0.32.6
```

`install`Perintah `npm` membuat `node_modules` direktori untuk modul Anda. Setelah langkah ini, struktur direktori Anda akan terlihat seperti berikut.

```

lambda-s3
|- index.mjs
|- node_modules
|  |- base64js
|  |- bl
|  |- buffer
...
|- package-lock.json
|- package.json

```

5. Buat paket deployment `.zip` yang berisi kode fungsi Anda dan dependensinya. Di `macOS` dan `Linux`, jalankan perintah berikut.

```
zip -r function.zip .
```

Di Windows, gunakan utilitas zip pilihan Anda untuk membuat file.zip. Pastikan bahwa `package-lock.json` file `index.mjspackage.json`, dan `node_modules` direktori Anda semuanya berada di root file.zip Anda.

Python

Untuk membuat paket penyebaran (Python)

1. Simpan kode contoh sebagai file bernama `lambda_function.py`.

```
import boto3
import os
import sys
import uuid
from urllib.parse import unquote_plus
from PIL import Image
import PIL.Image

s3_client = boto3.client('s3')

def resize_image(image_path, resized_path):
    with Image.open(image_path) as image:
        image.thumbnail(tuple(x / 2 for x in image.size))
        image.save(resized_path)

def lambda_handler(event, context):
    for record in event['Records']:
        bucket = record['s3']['bucket']['name']
        key = unquote_plus(record['s3']['object']['key'])
        tmpkey = key.replace('/', '')
        download_path = '/tmp/{}'.format(uuid.uuid4(), tmpkey)
        upload_path = '/tmp/resized-{}'.format(tmpkey)
        s3_client.download_file(bucket, key, download_path)
        resize_image(download_path, upload_path)
        s3_client.upload_file(upload_path, '{}-resized'.format(bucket), 'resized-{}'.format(key))
```

2. Di direktori yang sama di mana Anda membuat `lambda_function.py` file Anda, buat direktori baru bernama `package` dan instal pustaka [Pillow \(PIL\)](#) dan file AWS SDK for Python (Boto3). Meskipun runtime Lambda Python menyertakan versi Boto3SDK, kami menyarankan Anda menambahkan semua dependensi fungsi Anda ke paket penerapan Anda, bahkan jika

mereka disertakan dalam runtime. Untuk informasi selengkapnya, lihat [Dependensi runtime](#) dengan Python.

```
mkdir package
pip install \
--platform manylinux2014_x86_64 \
--target=package \
--implementation cp \
--python-version 3.12 \
--only-binary=:all: --upgrade \
pillow boto3
```

Pustaka Pillow berisi kode C/C ++. Dengan menggunakan `--only-binary=:all:` opsi `--platform manylinux_2014_x86_64` dan, pip akan mengunduh dan menginstal versi Pillow yang berisi binari pra-kompilasi yang kompatibel dengan sistem operasi Amazon Linux 2. Ini memastikan bahwa paket penerapan Anda akan berfungsi di lingkungan eksekusi Lambda, terlepas dari sistem operasi dan arsitektur mesin build lokal Anda.

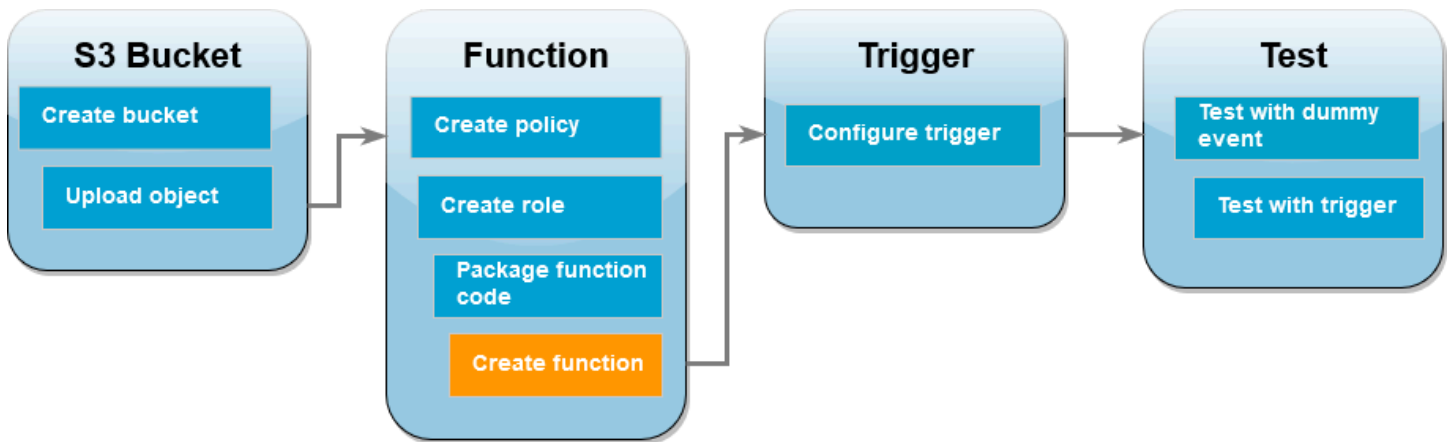
3. Buat file.zip yang berisi kode aplikasi Anda dan pustaka Pillow dan Boto3. Di Linux atau macOS, jalankan perintah berikut dari antarmuka baris perintah Anda.

```
cd package
zip -r ../lambda_function.zip .
cd ..
zip lambda_function.zip lambda_function.py
```

Di Windows, gunakan alat zip pilihan Anda untuk membuat file `lambda_function.zip`. Pastikan bahwa `lambda_function.py` file Anda dan folder yang berisi dependensi Anda semuanya berada di root file.zip.

Anda juga dapat membuat paket deployment menggunakan lingkungan virtual Python. Lihat [Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#)

Buat fungsi Lambda



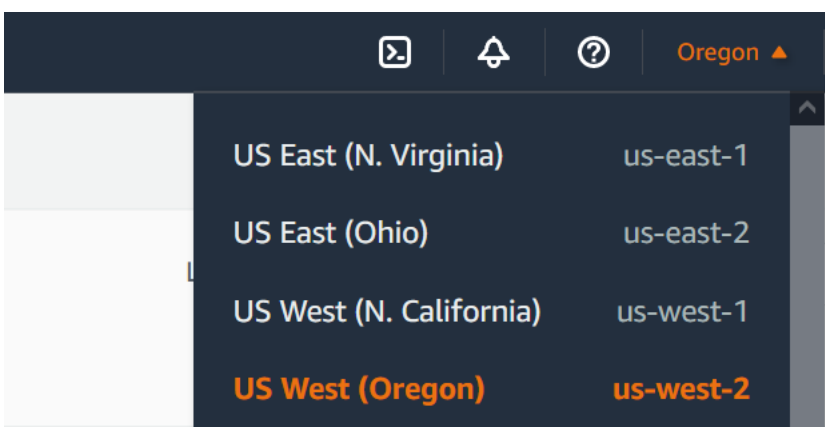
Anda dapat membuat fungsi Lambda menggunakan konsol Lambda AWS CLI atau Lambda. Ikuti instruksi untuk bahasa yang Anda pilih untuk membuat fungsi.

AWS Management Console

Untuk membuat fungsi (konsol)

Untuk membuat fungsi Lambda Anda menggunakan konsol, pertama-tama Anda membuat fungsi dasar yang berisi beberapa kode 'Hello world'. Anda kemudian mengganti kode ini dengan kode fungsi Anda sendiri dengan mengunggah the.zip atau JAR file yang Anda buat pada langkah sebelumnya.

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pastikan Anda bekerja di tempat yang sama dengan saat Wilayah AWS Anda membuat bucket Amazon S3. Anda dapat mengubah wilayah Anda menggunakan daftar drop-down di bagian atas layar.



3. Pilih Buat fungsi.

4. Pilih Penulis dari scratch.
5. Di bagian Informasi dasar, lakukan hal berikut:
 - a. Untuk Nama fungsi, masukkan **CreateThumbnail**.
 - b. Untuk Runtime pilih Node.js 20.x atau Python 3.12 sesuai dengan bahasa yang Anda pilih untuk fungsi Anda.
 - c. Untuk Arsitektur, pilih x86_64.
6. Di tab Ubah peran eksekusi default, lakukan hal berikut:
 - a. Perluas tab, lalu pilih Gunakan peran yang ada.
 - b. Pilih yang LambdaS3Role Anda buat sebelumnya.
7. Pilih Buat fungsi.

Untuk mengunggah kode fungsi (konsol)

1. Di panel Sumber kode, pilih Unggah dari.
2. Pilih file.zip.
3. Pilih Unggah.
4. Di pemilih file, pilih file.zip Anda dan pilih Buka.
5. Pilih Simpan.

AWS CLI

Untuk membuat fungsi (AWS CLI)

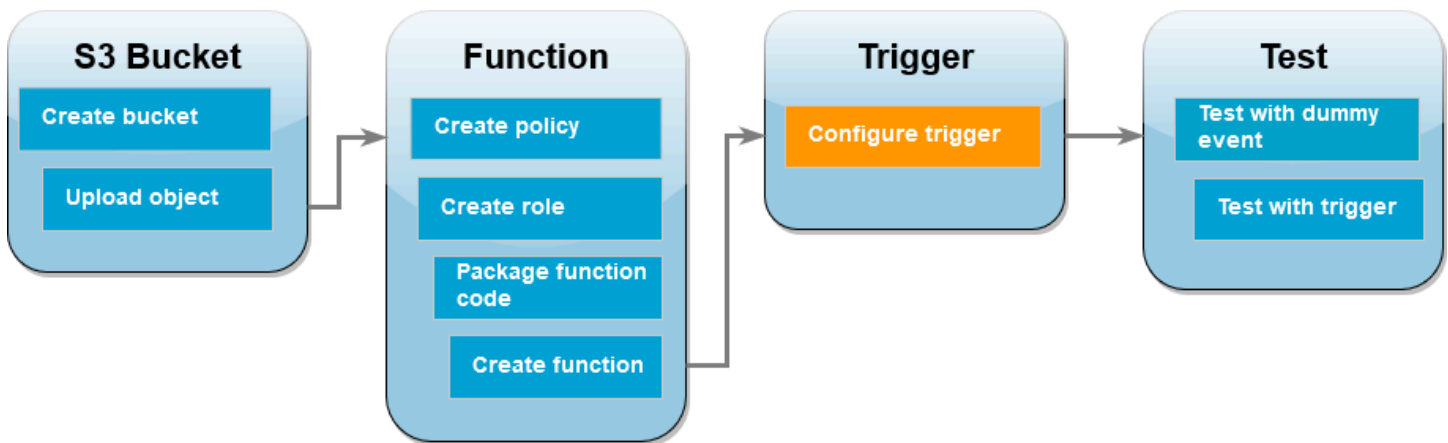
- Jalankan CLI perintah untuk bahasa yang Anda pilih. Untuk `role` parameter, pastikan untuk mengganti `123456789012` dengan Akun AWS ID Anda sendiri. Untuk `region` parameternya, ganti `us-east-1` dengan wilayah tempat Anda membuat bucket Amazon S3.
- Untuk Node.js, jalankan perintah berikut dari direktori yang berisi `function.zip` file Anda.

```
aws lambda create-function --function-name CreateThumbnail \  
--zip-file fileb://function.zip --handler index.handler --runtime nodejs20.x \  
--timeout 10 --memory-size 1024 \  
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-east-1
```

- Untuk Python, jalankan perintah berikut dari direktori yang berisi file `Andalambda_function.zip`.

```
aws lambda create-function --function-name CreateThumbnail \
--zip-file fileb://lambda_function.zip --handler
lambda_function.lambda_handler \
--runtime python3.12 --timeout 10 --memory-size 1024 \
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-east-1
```

Konfigurasi Amazon S3 untuk menjalankan fungsi



Agar fungsi Lambda dapat berjalan saat mengunggah gambar ke bucket sumber, Anda perlu mengonfigurasi pemicu untuk fungsi Anda. Anda dapat mengonfigurasi pemicu Amazon S3 menggunakan konsol atau AWS CLI

⚠ Important

Prosedur ini mengonfigurasi bucket Amazon S3 untuk menjalankan fungsi Anda setiap kali objek dibuat di bucket. Pastikan untuk mengonfigurasi ini hanya di bucket sumber. Jika fungsi Lambda Anda membuat objek dalam bucket yang sama yang memanggilnya, fungsi Anda dapat [dipanggil terus menerus](#) dalam satu loop. Hal ini dapat mengakibatkan biaya yang tidak diharapkan ditagih ke Anda Akun AWS.

AWS Management Console

Untuk mengonfigurasi pemicu Amazon S3 (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda (`CreateThumbnail`).
2. Pilih Tambahkan pemicu.
3. Pilih S3.
4. Di bawah Bucket, pilih bucket sumber Anda.
5. Di bawah Jenis acara, pilih Semua objek membuat acara.
6. Di bawah Pemanggilan rekursif, pilih kotak centang untuk mengetahui bahwa tidak disarankan menggunakan bucket Amazon S3 yang sama untuk input dan output. Anda dapat mempelajari lebih lanjut tentang pola pemanggilan rekursif di Lambda dengan membaca [pola rekursif yang menyebabkan fungsi Lambda yang tidak terkendali](#) di Tanah Tanpa Server.
7. Pilih Tambahkan.

Saat Anda membuat pemicu menggunakan konsol Lambda, Lambda secara otomatis membuat [kebijakan berbasis sumber daya](#) untuk memberikan layanan yang Anda pilih izin untuk menjalankan fungsi Anda.


AWS CLI

Untuk mengonfigurasi pemicu Amazon S3 (AWS CLI)

1. [Agar bucket sumber Amazon S3 menjalankan fungsi saat menambahkan file gambar, pertama-tama Anda harus mengonfigurasi izin untuk fungsi menggunakan kebijakan berbasis sumber daya.](#) Pernyataan kebijakan berbasis sumber daya memberikan AWS layanan izin lain untuk menjalankan fungsi Anda. Untuk memberikan izin Amazon S3 untuk menjalankan fungsi Anda, jalankan perintah berikut. CLI Pastikan untuk mengganti `source-account` parameter dengan Akun AWS ID Anda sendiri dan menggunakan nama bucket sumber Anda sendiri.

```
aws lambda add-permission --function-name CreateThumbnail \  
--principal s3.amazonaws.com --statement-id s3invoke --action \  
"lambda:InvokeFunction" \  
--source-arn arn:aws:s3:::amzn-s3-demo-source-bucket \  
--source-account 123456789012
```

Kebijakan yang Anda tetapkan dengan perintah ini memungkinkan Amazon S3 untuk menjalankan fungsi Anda hanya ketika tindakan dilakukan di bucket sumber Anda.

 Note

Meskipun nama bucket Amazon S3 unik secara global, saat menggunakan kebijakan berbasis sumber daya, praktik terbaik adalah menentukan bahwa bucket harus menjadi milik akun Anda. Ini karena jika Anda menghapus bucket, Anda dapat membuat bucket dengan Amazon Resource Name (ARN) yang sama. Akun AWS

2. Simpan yang berikut ini JSON dalam file bernama `notification.json`. Saat diterapkan ke bucket sumber Anda, ini akan JSON mengonfigurasi bucket untuk mengirim notifikasi ke fungsi Lambda Anda setiap kali objek baru ditambahkan. Ganti Akun AWS nomor dan Wilayah AWS dalam fungsi Lambda ARN dengan nomor akun dan wilayah Anda sendiri.

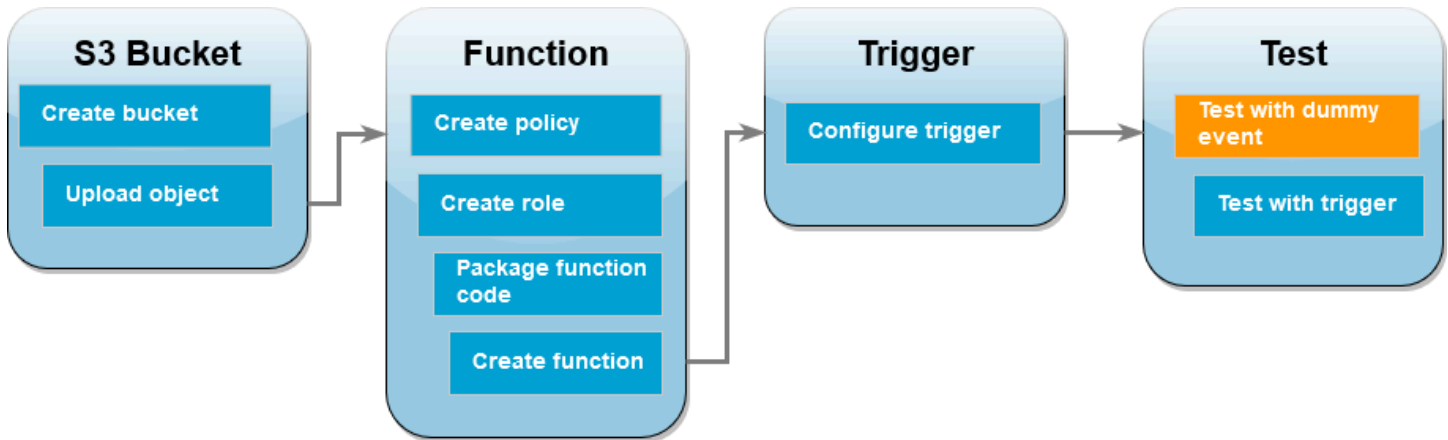
```
{
  "LambdaFunctionConfigurations": [
    {
      "Id": "CreateThumbnailEventConfiguration",
      "LambdaFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:CreateThumbnail",
      "Events": [ "s3:ObjectCreated:Put" ]
    }
  ]
}
```

3. Jalankan CLI perintah berikut untuk menerapkan pengaturan notifikasi dalam JSON file yang Anda buat ke bucket sumber Anda. Ganti `amzn-s3-demo-source-bucket` dengan nama bucket sumber Anda sendiri.

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-source-
bucket \
--notification-configuration file://notification.json
```

Untuk mempelajari lebih lanjut tentang `put-bucket-notification-configuration` perintah dan `notification-configuration` opsi, lihat [put-bucket-notification-configuration](#) di Referensi AWS CLI Perintah.

Uji fungsi Lambda Anda dengan acara dummy



Sebelum menguji seluruh penyiapan dengan menambahkan file gambar ke bucket sumber Amazon S3, Anda menguji apakah fungsi Lambda berfungsi dengan benar dengan memanggilnya dengan acara dummy. Peristiwa di Lambda adalah dokumen JSON berformat -yang berisi data untuk fungsi Anda untuk diproses. Saat fungsi Anda dipanggil oleh Amazon S3, peristiwa yang dikirim ke fungsi berisi informasi seperti nama bucket, ARN bucket, dan kunci objek.

AWS Management Console

Untuk menguji fungsi Lambda Anda dengan acara dummy (konsol)

1. Buka [halaman Fungsi](#) konsol Lambda dan pilih fungsi Anda (`CreateThumbnail`).
2. Pilih tab Uji.
3. Untuk membuat acara pengujian, di panel acara Uji, lakukan hal berikut:
 - a. Di bawah Uji tindakan peristiwa, pilih Buat acara baru.
 - b. Untuk Nama peristiwa, masukkan **myTestEvent**.
 - c. Untuk Template, pilih S3 Put.
 - d. Ganti nilai untuk parameter berikut dengan nilai Anda sendiri.
 - Untuk `awsRegion`, ganti `us-east-1` dengan bucket Amazon S3 yang Wilayah AWS Anda buat.
 - Untuk `name`, ganti `amzn-s3-demo-bucket` dengan nama bucket sumber Amazon S3 Anda sendiri.
 - Untuk `key`, ganti `test%2Fkey` dengan nama file objek pengujian yang Anda unggah ke bucket sumber di langkah tersebut. [Unggah gambar uji ke bucket sumber Anda](#)

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "amzn-s3-demo-bucket",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
  ]
}

```

e. Pilih Simpan.

4. Di panel acara Uji, pilih Uji.
5. Untuk memeriksa fungsi Anda telah membuat verison yang diubah ukurannya dari gambar Anda dan menyimpannya di bucket Amazon S3 target Anda, lakukan hal berikut:
 - a. Buka [halaman Bucket](#) konsol Amazon S3.
 - b. Pilih bucket target Anda dan konfirmasikan bahwa file yang diubah ukurannya tercantum di panel Objects.

AWS CLI

Untuk menguji fungsi Lambda Anda dengan acara dummy ()AWS CLI

1. Simpan yang berikut ini JSON dalam file bernama `dummyS3Event.json`. Ganti nilai untuk parameter berikut dengan nilai Anda sendiri:
 - Untuk `awsRegion`, ganti `us-east-1` dengan bucket Amazon S3 yang Wilayah AWS Anda buat.
 - Untuk `name`, ganti `amzn-s3-demo-bucket` dengan nama bucket sumber Amazon S3 Anda sendiri.
 - Untuk `key`, ganti `test%2Fkey` dengan nama file objek pengujian yang Anda unggah ke bucket sumber di langkah tersebut. [Unggah gambar uji ke bucket sumber Anda](#)

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
```

```

    "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
  },
  "s3": {
    "s3SchemaVersion": "1.0",
    "configurationId": "testConfigRule",
    "bucket": {
      "name": "amzn-s3-demo-bucket",
      "ownerIdentity": {
        "principalId": "EXAMPLE"
      },
      "arn": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    "object": {
      "key": "test%2Fkey",
      "size": 1024,
      "eTag": "0123456789abcdef0123456789abcdef",
      "sequencer": "0A1B2C3D4E5F678901"
    }
  }
}
]
}

```

2. Dari direktori tempat Anda menyimpan `dummyS3Event.json` file Anda, panggil fungsi dengan menjalankan CLI perintah berikut. Perintah ini memanggil fungsi Lambda Anda secara sinkron dengan `RequestResponse` menentukan sebagai nilai parameter tipe pemanggilan. [Untuk mempelajari lebih lanjut tentang pemanggilan sinkron dan asinkron, lihat Memanggil fungsi Lambda](#).

```

aws lambda invoke --function-name CreateThumbnail \
--invocation-type RequestResponse --cli-binary-format raw-in-base64-out \
--payload file://dummyS3Event.json outputfile.txt

```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan versi 2 dari AWS CLI. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#).

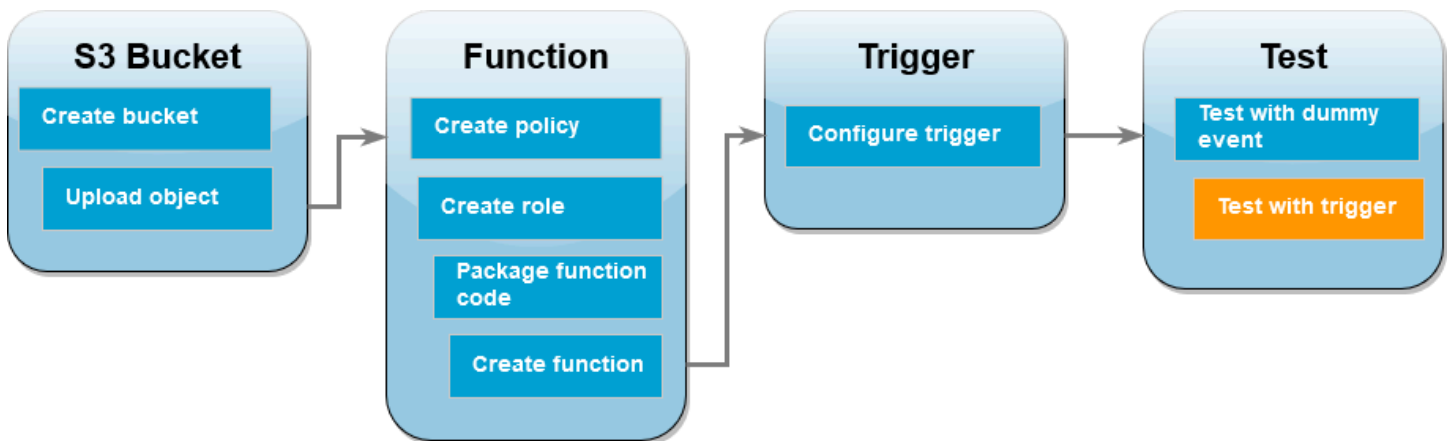
3. Verifikasi bahwa fungsi Anda telah membuat versi thumbnail gambar Anda dan menyimpannya ke bucket Amazon S3 target Anda. Jalankan CLI perintah berikut, ganti `amzn-s3-demo-source-bucket-resized` dengan nama bucket tujuan Anda sendiri.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-source-bucket-resized
```

Anda akan melihat output seperti yang berikut ini. KeyParameter menunjukkan nama file file gambar Anda yang diubah ukurannya.

```
{
  "Contents": [
    {
      "Key": "resized-HappyFace.jpg",
      "LastModified": "2023-06-06T21:40:07+00:00",
      "ETag": "\"d8ca652ffe83ba6b721ffc20d9d7174a\"",
      "Size": 2633,
      "StorageClass": "STANDARD"
    }
  ]
}
```

Uji fungsi Anda menggunakan pemacu Amazon S3



Sekarang setelah Anda mengonfirmasi bahwa fungsi Lambda Anda beroperasi dengan benar, Anda siap untuk menguji penyiapan lengkap Anda dengan menambahkan file gambar ke bucket sumber Amazon S3 Anda. Saat Anda menambahkan gambar ke bucket sumber, fungsi Lambda Anda akan dipanggil secara otomatis. Fungsi Anda membuat versi file yang diubah ukurannya dan menyimpannya di bucket target Anda.

AWS Management Console

Untuk menguji fungsi Lambda Anda menggunakan pemicu Amazon S3 (konsol)

1. Untuk mengunggah gambar ke bucket Amazon S3 Anda, lakukan hal berikut:
 - a. Buka halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket sumber Anda.
 - b. Pilih Unggah.
 - c. Pilih Tambahkan file dan gunakan pemilih file untuk memilih file gambar yang ingin Anda unggah. Objek gambar Anda dapat berupa file.jpg atau.png.
 - d. Pilih Buka, lalu pilih Unggah.
2. Verifikasi bahwa Lambda telah menyimpan versi file gambar yang diubah ukurannya di bucket target dengan melakukan hal berikut:
 - a. Arahkan kembali ke halaman [Bucket di](#) konsol Amazon S3 dan pilih bucket tujuan Anda.
 - b. Di panel Objects, Anda sekarang akan melihat dua file gambar yang diubah ukurannya, satu dari setiap pengujian fungsi Lambda Anda. Untuk mengunduh gambar yang diubah ukurannya, pilih file, lalu pilih Unduh.

AWS CLI

Untuk menguji fungsi Lambda Anda menggunakan pemicu Amazon S3 ()AWS CLI

1. Dari direktori yang berisi gambar yang ingin Anda unggah, jalankan CLI perintah berikut. Ganti `--bucket` parameter dengan nama bucket sumber Anda. Untuk `--body` parameter `--key` dan, gunakan nama file gambar pengujian Anda. Gambar uji Anda dapat berupa file.jpg atau.png.

```
aws s3api put-object --bucket amzn-s3-demo-source-bucket --key SmileyFace.jpg --body ./SmileyFace.jpg
```

2. Verifikasi bahwa fungsi Anda telah membuat versi thumbnail gambar Anda dan menyimpannya ke bucket Amazon S3 target Anda. Jalankan CLI perintah berikut, ganti `amzn-s3-demo-source-bucket-resized` dengan nama bucket tujuan Anda sendiri.

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-source-bucket-resized
```

Jika fungsi Anda berjalan dengan sukses, Anda akan melihat output yang mirip dengan berikut ini. Bucket target Anda sekarang harus berisi dua file yang diubah ukurannya.

```
{
  "Contents": [
    {
      "Key": "resized-HappyFace.jpg",
      "LastModified": "2023-06-07T00:15:50+00:00",
      "ETag": "\"7781a43e765a8301713f533d70968a1e\"",
      "Size": 2763,
      "StorageClass": "STANDARD"
    },
    {
      "Key": "resized-SmileyFace.jpg",
      "LastModified": "2023-06-07T00:13:18+00:00",
      "ETag": "\"ca536e5a1b9e32b22cd549e18792cdbc\"",
      "Size": 1245,
      "StorageClass": "STANDARD"
    }
  ]
}
```

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus kebijakan yang Anda buat.

1. Buka [halaman Kebijakan](#) IAM konsol.

2. Pilih kebijakan yang Anda buat (AWSLambdaS3Policy).
3. Pilih Tindakan kebijakan, Hapus.
4. Pilih Hapus.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus bucket S3

1. Buka [konsol Amazon S3](#).
2. Pilih bucket yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama ember di bidang input teks.
5. Pilih Hapus bucket.

Menggunakan Lambda dengan Amazon SQS

Note

[Jika Anda ingin mengirim data ke target selain fungsi Lambda atau memperkaya data sebelum mengirimnya, lihat Amazon Pipes. EventBridge](#)

Anda dapat menggunakan fungsi Lambda untuk memproses pesan dalam antrian Amazon Simple Queue Service (AmazonSQS). [Lambda mendukung antrian standar dan antrianfirst-in, first-out \(FIFO\) untuk pemetaan sumber acara.](#)

Topik

- [Memahami perilaku polling dan batching untuk pemetaan sumber SQS acara Amazon](#)
- [Contoh acara pesan antrian standar](#)
- [Contoh FIFO acara pesan antrian](#)
- [Membuat dan mengonfigurasi pemetaan sumber peristiwa Amazon SQS](#)
- [Mengonfigurasi perilaku penskalaan untuk pemetaan SQS sumber peristiwa](#)
- [Menangani kesalahan untuk sumber SQS peristiwa di Lambda](#)
- [Parameter Lambda untuk pemetaan sumber SQS acara Amazon](#)
- [Menggunakan pemfilteran acara dengan sumber SQS acara Amazon](#)
- [Tutorial: Menggunakan Lambda dengan Amazon SQS](#)
- [Tutorial: Menggunakan antrian Amazon SQS lintas akun sebagai sumber acara](#)

Memahami perilaku polling dan batching untuk pemetaan sumber SQS acara Amazon

[Dengan pemetaan sumber SQS peristiwa Amazon, Lambda melakukan polling antrian dan memanggil fungsi Anda secara sinkron dengan suatu peristiwa.](#) Setiap acara dapat berisi sekumpulan beberapa pesan dari antrian. Lambda menerima peristiwa ini satu batch pada satu waktu, dan memanggil fungsi Anda sekali untuk setiap batch. Ketika fungsi Anda berhasil memproses suatu batch, Lambda menghapus pesannya dari antrian.

[Saat Lambda menerima batch, pesan tetap berada dalam antrian tetapi disembunyikan selama batas waktu visibilitas antrian.](#) Jika fungsi Anda berhasil memproses semua pesan dalam batch,

Lambda menghapus pesan dari antrian. Secara default, jika fungsi Anda mengalami kesalahan saat memproses batch, semua pesan dalam kumpulan tersebut akan terlihat lagi dalam antrian setelah batas waktu visibilitas berakhir. Untuk alasan ini, kode fungsi Anda harus dapat memproses pesan yang sama beberapa kali tanpa efek samping yang tidak diinginkan.

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Untuk mencegah Lambda memproses pesan beberapa kali, Anda dapat mengonfigurasi pemetaan sumber peristiwa untuk menyertakan [kegagalan item batch](#) dalam respons fungsi Anda, atau Anda dapat menggunakan [DeleteMessageAPI](#) untuk menghapus pesan dari antrian karena fungsi Lambda berhasil memprosesnya.

Untuk informasi selengkapnya tentang parameter konfigurasi yang didukung Lambda untuk pemetaan sumber SQS peristiwa, lihat [the section called "Membuat pemetaan sumber acara SQS"](#)

Contoh acara pesan antrian standar

Example Acara SQS pesan Amazon (antrian standar)

```
{
  "Records": [
    {
      "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
      "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgXlaS3SLy0a...",
      "body": "Test message.",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOL023YVJ4V0",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
      },
      "messageAttributes": {},
      "md5fBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    }
  ]
}
```

```
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
    "awsRegion": "us-east-2"
  },
  {
    "messageId": "2e1424d4-f796-459a-8184-9c92662be6da",
    "receiptHandle": "AQEBzWwafTRI0KuVm4tP+/7q1rGgNqicHq...",
    "body": "Test message.",
    "attributes": {
      "ApproximateReceiveCount": "1",
      "SentTimestamp": "1545082650636",
      "SenderId": "AIDAIENQZJOL023YVJ4V0",
      "ApproximateFirstReceiveTimestamp": "1545082650649"
    },
    "messageAttributes": {},
    "md5fBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
    "awsRegion": "us-east-2"
  }
]
}
```

Secara default, Lambda melakukan polling hingga 10 pesan dalam antrian sekaligus dan mengirimkan batch tersebut ke fungsi Anda. Untuk menghindari menjalankan fungsi dengan sejumlah kecil catatan, Anda dapat mengonfigurasi sumber peristiwa untuk menyangga catatan hingga 5 menit dengan mengonfigurasi jendela batch. Sebelum menjalankan fungsi, Lambda melanjutkan polling pesan dari antrian standar hingga jendela batch kedaluwarsa, kuota [ukuran payload pemanggilan tercapai, atau ukuran](#) batch maksimum yang dikonfigurasi tercapai.

Jika Anda menggunakan jendela batch dan SQS antrian Anda berisi lalu lintas yang sangat rendah, Lambda mungkin menunggu hingga 20 detik sebelum menjalankan fungsi Anda. Ini benar bahkan jika Anda mengatur jendela batch lebih rendah dari 20 detik.

Note

Di Java, Anda mungkin mengalami kesalahan pointer null saat deserialisasi. JSON Ini bisa jadi karena bagaimana kasus "Records" dan "eventSourceARN" dikonversi oleh JSON object mapper.

Contoh FIFO acara pesan antrian

Untuk FIFO antrian, catatan berisi atribut tambahan yang terkait dengan deduplikasi dan pengurutan.

Example Acara SQS pesan Amazon (FIFOantrian)

```
{
  "Records": [
    {
      "messageId": "11d6ee51-4cc7-4302-9e22-7cd8afdaadf5",
      "receiptHandle": "AQEBBX8nesZEXmkhsmZeyIE8iQAMig7qw...",
      "body": "Test message.",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1573251510774",
        "SequenceNumber": "18849496460467696128",
        "MessageGroupId": "1",
        "SenderId": "AIDAI023YVJENQZJOL4V0",
        "MessageDeduplicationId": "1",
        "ApproximateFirstReceiveTimestamp": "1573251510774"
      },
      "messageAttributes": {},
      "md5ofBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
      "eventSource": "aws:sqs",
      "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:fifo.fifo",
      "awsRegion": "us-east-2"
    }
  ]
}
```

Membuat dan mengonfigurasi pemetaan sumber peristiwa Amazon SQS

Untuk memproses pesan Amazon SQS dengan Lambda, konfigurasi antrian Anda dengan pengaturan yang sesuai, lalu buat pemetaan sumber peristiwa Lambda.

Mengonfigurasi antrean untuk digunakan dengan Lambda

Jika Anda belum memiliki antrean Amazon SQS yang ada, [buat](#) antrean untuk berfungsi sebagai sumber acara untuk fungsi Lambda Anda. Kemudian konfigurasi antrian untuk memberikan waktu yang cukup bagi fungsi Lambda Anda untuk memproses setiap kumpulan peristiwa.

Untuk memungkinkan waktu fungsi Anda memproses setiap kumpulan rekaman, atur [batas waktu visibilitas](#) antrian sumber menjadi setidaknya enam kali batas [waktu konfigurasi](#) pada fungsi Anda. Waktu tambahan memungkinkan Lambda untuk mencoba lagi jika fungsi Anda dibatasi saat memproses batch sebelumnya.

Secara default, jika Lambda menemukan kesalahan di titik mana pun saat memproses batch, semua pesan dalam batch tersebut kembali ke antrian. Setelah [batas waktu visibilitas](#), pesan menjadi terlihat oleh Lambda lagi. Anda dapat mengonfigurasi pemetaan sumber peristiwa untuk menggunakan [respons batch sebagian](#) agar hanya mengembalikan pesan yang gagal kembali ke antrian. Selain itu, jika fungsi Anda gagal memproses pesan beberapa kali, Amazon SQS dapat mengirimkannya ke antrian huruf [mati](#). Sebaiknya setel [kebijakan redrive](#) antrian sumber Anda ke setidaknya 5. `maxReceiveCount` Ini memberi Lambda beberapa kesempatan untuk mencoba lagi sebelum mengirim pesan yang gagal langsung ke antrian surat mati.

Menyiapkan izin peran eksekusi Lambda

Kebijakan [AWSLambdaSQSQueueExecutionRole](#) AWS terkelola mencakup izin yang perlu dibaca Lambda dari antrian Amazon SQS Anda. Anda dapat menambahkan kebijakan terkelola ini ke [peran eksekusi](#) fungsi Anda.

Secara opsional, jika Anda menggunakan antrian terenkripsi, Anda juga perlu menambahkan izin berikut ke peran eksekusi Anda:

- [kms:Decrypt](#)

Membuat pemetaan sumber acara SQS

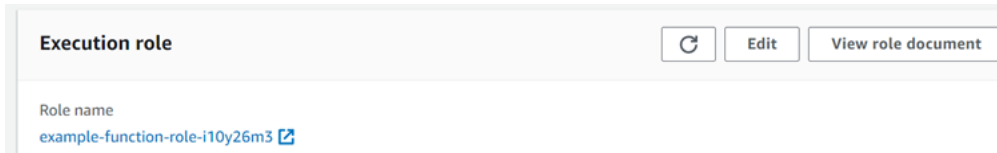
Buat pemetaan sumber kejadian untuk memberi tahu Lambda agar mengirim item dari antrian Anda ke fungsi Lambda. Anda dapat membuat beberapa pemetaan sumber kejadian untuk memproses item dari beberapa antrian dengan satu fungsi. Ketika Lambda memanggil fungsi target, kejadian dapat berisi beberapa item, hingga ukuran batch maksimum yang dapat dikonfigurasi.

Untuk mengonfigurasi fungsi agar dibaca dari Amazon SQS, lampirkan kebijakan [AWSLambdaSQSQueueExecutionRole](#) AWS terkelola ke peran eksekusi Anda. Kemudian, buat pemetaan sumber peristiwa SQS dari konsol menggunakan langkah-langkah berikut.

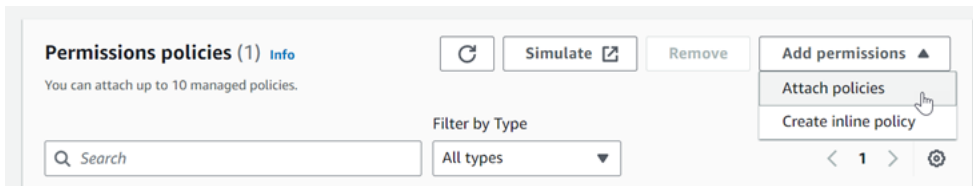
Untuk menambahkan izin dan membuat pemicu

1. Buka [Halaman fungsi](#) di konsol Lambda.

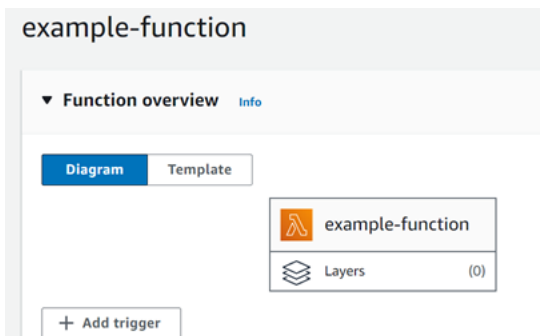
2. Pilih nama sebuah fungsi.
3. Pilih tab Konfigurasi, lalu pilih Izin.
4. Di bawah Nama peran, pilih tautan ke peran eksekusi Anda. Tautan ini membuka peran di konsol IAM.



5. Pilih Tambahkan izin, lalu pilih Lampirkan kebijakan.



6. Di bidang pencarian, masukkan `AWSLambdaSQSQueueExecutionRole`. Tambahkan kebijakan ini ke peran eksekusi Anda. Ini adalah kebijakan AWS terkelola yang berisi izin yang perlu dibaca fungsi Anda dari antrean Amazon SQS. Untuk informasi selengkapnya tentang kebijakan ini, lihat [AWSLambdaSQSQueueExecutionRole](#) di Referensi Kebijakan AWS Terkelola.
7. Kembali ke fungsi Anda di konsol Lambda. Di bagian Gambaran umum fungsi, pilih Tambah pemicu.



8. Pilih jenis pemicu.
9. Konfigurasi opsi yang diperlukan, lalu pilih Tambah.

Lambda mendukung opsi konfigurasi berikut untuk sumber peristiwa Amazon SQS:

Antrian SQS

Antrian Amazon SQS untuk membaca catatan dari.

Aktifkan pemicu

Status pemetaan sumber acara. Aktifkan pemicu dipilih secara default.

Ukuran batch

Jumlah maksimum catatan untuk dikirim ke fungsi di setiap batch. Untuk antrian standar, ini bisa mencapai 10.000 catatan. Untuk antrian FIFO, maksimum adalah 10. Untuk ukuran batch lebih dari 10, Anda juga harus mengatur batch window (`MaximumBatchingWindowInSeconds`) setidaknya 1 detik.

Konfigurasi [batas waktu fungsi](#) Anda untuk memberikan waktu yang cukup untuk memproses seluruh kumpulan item. Jika item membutuhkan waktu lama untuk diproses, pilih ukuran batch yang lebih kecil. Ukuran batch yang besar dapat meningkatkan efisiensi beban kerja yang sangat cepat atau memiliki banyak overhead. Jika Anda mengonfigurasi [konkurensi cadangan](#) pada fungsi Anda, setelah minimal lima eksekusi bersamaan untuk mengurangi kemungkinan kesalahan pelambatan saat Lambda memanggil fungsi Anda.

Lambda meneruskan semua catatan dalam batch ke fungsi dalam satu panggilan, selama ukuran total peristiwa tidak melebihi [kuota ukuran payload pemanggilan untuk pemanggilan sinkron](#) (6 MB). Baik Lambda dan Amazon SQS menghasilkan metadata untuk setiap catatan. Metadata tambahan ini dihitung terhadap ukuran muatan total dan dapat menyebabkan jumlah total catatan yang dikirim dalam batch menjadi lebih rendah dari ukuran batch yang dikonfigurasi. Bidang metadata yang dikirimkan Amazon SQS dapat bervariasi panjangnya. Untuk informasi selengkapnya tentang bidang metadata Amazon SQS, lihat dokumentasi operasi [ReceiveMessageAPI](#) di Referensi API Layanan Antrian Sederhana Amazon.

Jendela batch

Jumlah waktu maksimum untuk mengumpulkan rekaman sebelum memanggil fungsi, dalam hitungan detik. Ini hanya berlaku untuk antrian standar.

Jika Anda menggunakan jendela batch lebih dari 0 detik, Anda harus memperhitungkan peningkatan waktu pemrosesan dalam batas waktu [visibilitas](#) antrian Anda. Sebaiknya atur batas waktu visibilitas antrian Anda menjadi enam kali [batas waktu fungsi](#) Anda, ditambah nilai `MaximumBatchingWindowInSeconds`. Ini memungkinkan waktu untuk fungsi Lambda Anda memproses setiap batch peristiwa dan mencoba kembali jika terjadi kesalahan `throttling`.

Ketika pesan tersedia, Lambda mulai memproses pesan dalam batch. Lambda mulai memproses lima batch sekaligus dengan lima pemanggilan fungsi Anda secara bersamaan. Jika pesan masih tersedia, Lambda menambahkan hingga 300 instance fungsi Anda dalam satu menit, hingga

maksimum 1.000 instance fungsi. Untuk mempelajari lebih lanjut tentang penskalaan fungsi dan konkurensi, lihat Penskalaan fungsi [Lambda](#).

Untuk memproses lebih banyak pesan, Anda dapat mengoptimalkan fungsi Lambda untuk throughput yang lebih tinggi. Untuk informasi selengkapnya, lihat [Memahami cara AWS Lambda menskalakan dengan antrian standar Amazon SQS](#).

Konkurensi maksimum

Jumlah maksimum fungsi bersamaan yang dapat dipanggil sumber peristiwa. Untuk informasi selengkapnya, lihat [Mengonfigurasi konkurensi maksimum untuk sumber peristiwa Amazon SQS](#).

Kriteria filter

Tambahkan kriteria filter untuk mengontrol peristiwa yang dikirim Lambda ke fungsi Anda untuk diproses. Untuk informasi selengkapnya, lihat [Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda](#).

Mengonfigurasi perilaku penskalaan untuk pemetaan SQS sumber peristiwa

Untuk antrian standar, Lambda menggunakan polling [panjang untuk melakukan polling](#) antrian hingga menjadi aktif. Saat pesan tersedia, Lambda mulai memproses lima batch sekaligus dengan lima pemanggilan fungsi Anda secara bersamaan. Jika pesan masih tersedia, Lambda meningkatkan jumlah proses yang membaca batch hingga 300 instance lagi per menit. Jumlah maksimum batch yang dapat diproses oleh pemetaan sumber peristiwa secara bersamaan adalah 1.000.

Untuk FIFO antrian, Lambda mengirim pesan ke fungsi Anda dalam urutan yang diterimanya. Saat mengirim pesan ke FIFO antrian, Anda menentukan [ID grup pesan](#). Amazon SQS memastikan bahwa pesan dalam grup yang sama dikirim ke Lambda secara berurutan. Saat Lambda membaca pesan Anda ke dalam batch, setiap batch mungkin berisi pesan dari lebih dari satu grup pesan, tetapi urutan pesan tetap terjaga. Jika fungsi Anda menampilkan kesalahan, fungsi akan mencoba semua percobaan ulang pada pesan yang terpengaruh sebelum Lambda menerima pesan tambahan dari grup yang sama.

Mengonfigurasi konkurensi maksimum untuk sumber peristiwa Amazon SQS

Anda dapat menggunakan setelan konkurensi maksimum untuk mengontrol perilaku penskalaan untuk sumber SQS acara Anda. Setelan konkurensi maksimum membatasi jumlah instance bersamaan dari fungsi yang dapat dipanggil oleh sumber SQS peristiwa Amazon. Konkurensi maksimum adalah pengaturan tingkat sumber acara. Jika Anda memiliki beberapa sumber SQS

peristiwa Amazon yang dipetakan ke satu fungsi, setiap sumber peristiwa dapat memiliki setelan konkurensi maksimum yang terpisah. Anda dapat menggunakan konkurensi maksimum untuk mencegah satu antrian menggunakan semua [konkurensi cadangan fungsi atau sisa kuota konkurensi akun](#). Tidak ada biaya untuk mengonfigurasi konkurensi maksimum pada sumber SQS acara Amazon.

Yang penting, konkurensi maksimum dan konkurensi cadangan adalah dua pengaturan independen. Jangan setel konkurensi maksimum yang lebih tinggi dari konkurensi cadangan fungsi. Jika Anda mengonfigurasi konkurensi maksimum, pastikan bahwa konkurensi cadangan fungsi Anda lebih besar dari atau sama dengan total konkurensi maksimum untuk semua sumber SQS peristiwa Amazon pada fungsi tersebut. Jika tidak, Lambda dapat membatasi pesan Anda.

Jika kuota konkurensi akun Anda disetel ke nilai default 1.000, pemetaan sumber SQS peristiwa Amazon dapat menskalakan untuk memanggil instance fungsi hingga nilai ini, kecuali Anda menentukan konkurensi maksimum.

Jika Anda menerima peningkatan kuota konkurensi default akun Anda, Lambda mungkin tidak dapat menjalankan instans fungsi bersamaan hingga kuota baru Anda. Secara default, Lambda dapat menskalakan untuk menjalankan hingga 1.250 instance fungsi bersamaan untuk pemetaan sumber peristiwa Amazon. SQS Jika ini tidak cukup untuk kasus penggunaan Anda, hubungi AWS dukungan untuk mendiskusikan peningkatan konkurensi pemetaan sumber SQS peristiwa Amazon akun Anda.

Note

Untuk FIFO antrian, pemanggilan bersamaan dibatasi oleh jumlah [grup pesan IDs](#) (`messageGroupId`) atau pengaturan konkurensi maksimum—mana yang lebih rendah. Misalnya, jika Anda memiliki enam grup pesan IDs dan konkurensi maksimum disetel ke 10, fungsi Anda dapat memiliki maksimal enam pemanggilan bersamaan.

Anda dapat mengonfigurasi konkurensi maksimum pada pemetaan sumber SQS peristiwa Amazon yang baru dan yang sudah ada.

Konfigurasikan konkurensi maksimum menggunakan konsol Lambda

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Di bawah Ikhtisar fungsi, pilih SQS. Ini membuka tab Konfigurasi.

4. Pilih SQS pemicu Amazon dan pilih Edit.
5. Untuk Konkurensi maksimum, masukkan angka antara 2 dan 1.000. Untuk mematikan konkurensi maksimum, biarkan kotak kosong.
6. Pilih Simpan.

Konfigurasi konkurensi maksimum menggunakan AWS Command Line Interface (AWS CLI)

Gunakan [update-event-source-mapping](#) perintah dengan `--scaling-config` opsi. Contoh:

```
aws lambda update-event-source-mapping \  
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \  
  --scaling-config '{"MaximumConcurrency':5}'
```

Untuk mematikan konkurensi maksimum, masukkan nilai kosong untuk `--scaling-config`:

```
aws lambda update-event-source-mapping \  
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \  
  --scaling-config "{}"
```

Konfigurasi konkurensi maksimum menggunakan Lambda API

Gunakan [CreateEventSourceMapping](#) atau [UpdateEventSourceMapping](#) tindakan dengan [ScalingConfig](#) objek.

Menangani kesalahan untuk sumber SQS peristiwa di Lambda

Untuk menangani kesalahan yang terkait dengan sumber SQS peristiwa, Lambda secara otomatis menggunakan strategi coba lagi dengan strategi backoff. Anda juga dapat menyesuaikan perilaku penanganan kesalahan dengan mengonfigurasi pemetaan sumber SQS peristiwa Anda untuk mengembalikan respons [batch sebagian](#).

Strategi backoff untuk pemanggilan yang gagal

Ketika pemanggilan gagal, Lambda mencoba lagi pemanggilan sambil menerapkan strategi backoff. Strategi backoff sedikit berbeda tergantung pada apakah Lambda mengalami kegagalan karena kesalahan dalam kode fungsi Anda, atau karena pelambatan.

- Jika kode fungsi Anda menyebabkan kesalahan, Lambda akan berhenti memproses dan mencoba kembali pemanggilan. Sementara itu, Lambda secara bertahap mundur, mengurangi jumlah

konkurensi yang dialokasikan ke pemetaan sumber acara SQS Amazon Anda. Setelah batas waktu visibilitas antrian Anda habis, pesan akan muncul kembali dalam antrian.

- Jika pemanggilan gagal karena pembatasan, Lambda secara bertahap menghentikan percobaan ulang dengan mengurangi jumlah konkurensi yang dialokasikan ke pemetaan sumber peristiwa Amazon Anda. SQS Lambda terus mencoba lagi pesan hingga stempel waktu pesan melebihi batas waktu visibilitas antrian Anda, di mana Lambda menghapus pesan.

Menerapkan tanggapan batch sebagian

Saat fungsi Lambda Anda mengalami kesalahan saat memproses batch, semua pesan dalam kumpulan tersebut akan terlihat lagi dalam antrian secara default, termasuk pesan yang berhasil diproses Lambda. Akibatnya, fungsi Anda dapat memproses pesan yang sama beberapa kali.

Untuk menghindari pemrosesan ulang pesan yang berhasil diproses dalam kumpulan yang gagal, Anda dapat mengonfigurasi pemetaan sumber peristiwa agar hanya pesan yang gagal terlihat lagi. Ini disebut respon batch paral. Untuk mengaktifkan respons batch sebagian, tentukan `ReportBatchItemFailures` [FunctionResponseType](#) tindakan saat mengonfigurasi pemetaan sumber peristiwa Anda. Ini memungkinkan fungsi Anda mengembalikan sebagian keberhasilan, yang dapat membantu mengurangi jumlah percobaan ulang yang tidak perlu pada catatan.

Saat `ReportBatchItemFailures` diaktifkan, Lambda tidak [mengurangi polling pesan saat pemanggilan](#) fungsi gagal. Jika Anda mengharapkan beberapa pesan gagal—dan Anda tidak ingin kegagalan tersebut memengaruhi laju pemrosesan pesan—gunakan `ReportBatchItemFailures`

Note

Ingatlah hal berikut saat menggunakan respons batch sebagian:

- Jika fungsi Anda melempar pengecualian, seluruh batch dianggap gagal total.
- Jika Anda menggunakan fitur ini dengan FIFO antrian, fungsi Anda harus berhenti memproses pesan setelah kegagalan pertama dan mengembalikan semua pesan yang gagal dan belum diproses. `batchItemFailures` Ini membantu menjaga urutan pesan dalam antrian Anda.

Untuk mengaktifkan pelaporan batch sebagian

1. Tinjau [Praktik terbaik untuk menerapkan respons batch sebagian](#).

2. Jalankan perintah berikut `ReportBatchItemFailures` untuk mengaktifkan fungsi Anda. Untuk mengambil pemetaan sumber acara Anda UUID, jalankan perintah. [list-event-source-mappings](#)
AWS CLI

```
aws lambda update-event-source-mapping \  
--uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \  
--function-response-types "ReportBatchItemFailures"
```

3. Perbarui kode fungsi Anda untuk menangkap semua pengecualian dan mengembalikan pesan yang gagal dalam `batchItemFailures` JSON respons. `batchItemFailuresResponse` harus menyertakan daftar pesan IDs, sebagai `itemIdentifier` JSON nilai.

Misalnya, Anda memiliki sekumpulan lima pesan, dengan pesan IDs `id1`, `id2`, `id3`, `id4`, dan `id5`. Fungsi Anda berhasil memproses `id1`, `id3`, dan `id5`. Untuk membuat pesan `id2` dan `id4` terlihat lagi dalam antrian Anda, fungsi Anda harus mengembalikan respons berikut:

```
{  
  "batchItemFailures": [  
    {  
      "itemIdentifier": "id2"  
    },  
    {  
      "itemIdentifier": "id4"  
    }  
  ]  
}
```

Berikut adalah beberapa contoh kode fungsi yang mengembalikan daftar pesan gagal IDs dalam batch:

.NET

AWS SDK for .NET

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be
// converted into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
        ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
        List<SQSBatchResponse.BatchItemFailure>();
        foreach(var message in evnt.Records)
        {
            try
            {
                //process your message
                await ProcessMessageAsync(message, context);
            }
            catch (System.Exception)
            {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.Add(new
                SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
        ILambdaContext context)
    {
        if (String.IsNullOrEmpty(message.Body))
        {
```

```

        throw new Exception("No Body in SQS Message.");
    }
    context.Logger.LogInformation($"Processed message {message.Body}");
    // TODO: Do interesting work based on the new message
    await Task.CompletedTask;
}
}

```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Go.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "encoding/json"
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, sqsEvent events.SQSEvent)
(map[string]interface{}, error) {
    batchItemFailures := []map[string]interface{}{}

    for _, message := range sqsEvent.Records {

        if /* Your message processing condition here */ {
            batchItemFailures = append(batchItemFailures, map[string]interface{}{
                "itemIdentifier": message.MessageId})
        }
    }
}

```

```
    }  
  }  
  
  sqsBatchResponse := map[string]interface{}{  
    "batchItemFailures": batchItemFailures,  
  }  
  return sqsBatchResponse, nil  
}  
  
func main() {  
  lambda.Start(handler)  
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
import com.amazonaws.services.lambda.runtime.Context;  
import com.amazonaws.services.lambda.runtime.RequestHandler;  
import com.amazonaws.services.lambda.runtime.events.SQSEvent;  
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;  
  
import java.util.ArrayList;  
import java.util.List;  
  
public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,  
    SQSBatchResponse> {  
    @Override  
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context)  
    {
```

```

        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
ArrayList<SQSBatchResponse.BatchItemFailure>();
        String messageId = "";
        for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
            try {
                //process your message
                messageId = message.getMessageId();
            } catch (Exception e) {
                //Add failed message identifier to the batchItemFailures
list
                batchItemFailures.add(new
SQSBatchResponse.BatchItemFailure(messageId));
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }
}

```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. JavaScript

```

// Node.js 20.x Lambda runtime, AWS SDK for Javascript V3
export const handler = async (event, context) => {
    const batchItemFailures = [];
    for (const record of event.Records) {
        try {
            await processMessageAsync(record, context);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }
}

```



```
    return { batchItemFailures };
  };

  async function processMessageAsync(record, context) {
    if (record.body && record.body.includes("error")) {
      throw new Error("There is an error in the SQS Message.");
    }
    console.log(`Processed message: ${record.body}`);
  }
}
```

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure,
  SQSRecord } from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
  Promise<SQSBatchResponse> => {
  const batchItemFailures: SQSBatchItemFailure[] = [];

  for (const record of event.Records) {
    try {
      await processMessageAsync(record);
    } catch (error) {
      batchItemFailures.push({ itemIdentifier: record.messageId });
    }
  }

  return {batchItemFailures: batchItemFailures};
};

async function processMessageAsync(record: SQSRecord): Promise<void> {
  if (record.body && record.body.includes("error")) {
    throw new Error('There is an error in the SQS Message.');
```

PHP

SDKuntuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        $this->logger->info("Processing SQS records");
        $records = $event->getRecords();

        foreach ($records as $record) {
```

```
        try {
            // Assuming the SQS message is in JSON format
            $message = json_decode($record->getBody(), true);
            $this->logger->info(json_encode($message));
            // TODO: Implement your custom processing logic here
        } catch (Exception $e) {
            $this->logger->error($e->getMessage());
            // failed processing the record
            $this->markAsFailed($record);
        }
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords SQS
records");
}
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event, context):
    if event:
        batch_item_failures = []
        sqs_batch_response = {}
```

```
    for record in event["Records"]:
        try:
            # process message
        except Exception as e:
            batch_item_failures.append({"itemIdentifier":
record['messageId']})

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
  if event
    batch_item_failures = []
    sqs_batch_response = {}

    event["Records"].each do |record|
      begin
        # process message
      rescue StandardError => e
        batch_item_failures << {"itemIdentifier" => record['messageId']}
      end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
  end
end
```

```
end
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}

async fn function_handler(event: LambdaEvent<SqsEvent>) ->
Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }

    Ok(SqsBatchResponse {
```

```
        batch_item_failures,  
    })  
}  
  
#[tokio::main]  
async fn main() -> Result<(), Error> {  
    run(service_fn(function_handler)).await  
}
```

Jika peristiwa gagal tidak kembali ke antrian, lihat [Bagaimana cara memecahkan masalah fungsi Lambda? SQS ReportBatchItemFailures](#) di pusat AWS pengetahuan.

Status berhasil dan gagal

Lambda memperlakukan batch sebagai sukses total jika fungsi Anda mengembalikan salah satu dari berikut ini:

- Daftar `batchItemFailures` kosong
- Daftar `batchItemFailures` nol
- `EventResponse` kosong
- `EventResponse` nol

Lambda memperlakukan batch sebagai kegagalan total jika fungsi Anda mengembalikan salah satu dari berikut ini:

- Tanggapan yang tidak valid JSON
- String `itemIdentifier` kosong
- `itemIdentifier` nol
- `itemIdentifier` dengan nama kunci yang buruk
- `itemIdentifierNilai` dengan ID pesan yang tidak ada

CloudWatch metrik

Untuk menentukan apakah fungsi Anda melaporkan kegagalan item batch dengan benar, Anda dapat memantau SQS metrik `NumberOfMessagesDeleted` dan `ApproximateAgeOfOldestMessage` Amazon di Amazon CloudWatch.

- `NumberOfMessagesDeleted` melacak jumlah pesan yang dihapus dari antrian Anda. Jika ini turun ke 0, ini adalah tanda bahwa respons fungsi Anda tidak mengembalikan pesan yang gagal dengan benar.
- `ApproximateAgeOfOldestMessage` melacak berapa lama pesan tertua telah tinggal di antrian Anda. Peningkatan tajam dalam metrik ini dapat menunjukkan bahwa fungsi Anda tidak mengembalikan pesan yang gagal dengan benar.

Parameter Lambda untuk pemetaan sumber SQS acara Amazon

Semua jenis sumber acara Lambda berbagi hal yang sama [CreateEventSourceMapping](#) dan [UpdateEventSourceMapping](#) API operasi. Namun, hanya beberapa parameter yang berlaku untuk AmazonSQS.

| Parameter | Diperlukan | Default | Catatan |
|-----------------------------------|------------|---------|--|
| <code>BatchSize</code> | T | 10 | Untuk antrian standar, maksimum adalah 10.000. Untuk FIFO antrian, maksimum adalah 10. |
| Diaktifkan | T | true | none |
| <code>EventSourceArn</code> | T | N/A | Aliran data atau konsumen aliran ARN |
| <code>FunctionName</code> | T | N/A | none |
| <code>FilterCriteria</code> | T | N/A | Kontrol peristiwa mana yang dikirim Lambda ke fungsi Anda |
| <code>FunctionResponseType</code> | T | N/A | Agar fungsi Anda melaporkan kegagalan tertentu dalam satu batch, sertakan nilainya |

| Parameter | Diperlukan | Default | Catatan |
|--------------------------------|------------|---------|---|
| | | | ReportBatchItemFailures FunctionResponseTypes . Untuk informasi selengkapnya, lihat Menerapkan tanggapan batch sebagian . |
| MaximumBatchingWindowInSeconds | T | 0 | none |
| ScalingConfig | T | N/A | Mengonfigurasi konkurensi maksimum untuk sumber peristiwa Amazon SQS |

Menggunakan pemfilteran acara dengan sumber SQS acara Amazon

Anda dapat menggunakan pemfilteran peristiwa untuk mengontrol rekaman mana dari aliran atau antrian yang dikirim Lambda ke fungsi Anda. Untuk informasi umum tentang cara kerja penyaringan acara, lihat [the section called “Penyaringan acara”](#).

Bagian ini berfokus pada pemfilteran acara untuk sumber MSK acara Amazon.

Topik

- [Dasar-dasar pemfilteran SQS acara Amazon](#)

Dasar-dasar pemfilteran SQS acara Amazon

Misalkan SQS antrian Amazon Anda berisi pesan dalam JSON format berikut.

```
{
  "RecordNumber": 1234,
```



```

    "TimeStamp": "yyyy-mm-ddThh:mm:ss",
    "RequestCode": "AAAA"
  }

```

Contoh catatan untuk antrian ini akan terlihat sebagai berikut.

```

{
  "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
  "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgXlaS3SLy0a...",
  "body": "{\n  \"RecordNumber\": 1234,\n  \"TimeStamp\": \"yyyy-mm-ddThh:mm:ss\",\n  \"RequestCode\": \"AAAA\"\n}",
  "attributes": {
    "ApproximateReceiveCount": "1",
    "SentTimestamp": "1545082649183",
    "SenderId": "AIDAIENQZJOL023YVJ4V0",
    "ApproximateFirstReceiveTimestamp": "1545082649185"
  },
  "messageAttributes": {},
  "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
  "eventSource": "aws:sqs",
  "eventSourceARN": "arn:aws:sqs:us-west-2:123456789012:my-queue",
  "awsRegion": "us-west-2"
}

```

Untuk memfilter berdasarkan konten SQS pesan Amazon Anda, gunakan body kunci dalam catatan SQS pesan Amazon. Misalkan Anda hanya ingin memproses catatan-catatan RequestCode di mana SQS pesan Amazon Anda adalah "BBBB." FilterCriteriaObjeknya adalah sebagai berikut.

```

{
  "Filters": [
    {
      "Pattern": "{ \"body\" : { \"RequestCode\" : [ \"BBBB\" ] } }"
    }
  ]
}

```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```

{
  "body": {
    "RequestCode": [ "BBBB" ]
  }
}

```

```
}
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "body" : { "RequestCode" : [ "BBBB" ] } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" : [ \"BBBB\" ] } }"]}'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-1111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" : [ \"BBBB\" ] } }"]}'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RequestCode" : [ "BBBB" ] } }'
```

Misalkan Anda ingin fungsi Anda memproses hanya catatan yang RecordNumber lebih besar dari 9999. FilterCriteriaObjeknya adalah sebagai berikut.

```
{
  "Filters": [
    {
      "Pattern": "{ \"body\" : { \"RecordNumber\" : [ { \"numeric\" : [ \">\",
9999 ] } ] } }"
    }
  ]
}
```

Untuk kejelasan tambahan, berikut adalah nilai filter yang Pattern diperluas secara polosJSON.

```
{
  "body": {
    "RecordNumber": [
      {
        "numeric": [ ">", 9999 ]
      }
    ]
  }
}
```

Anda dapat menambahkan filter menggunakan konsol, AWS CLI atau AWS SAM templat.

Console

Untuk menambahkan filter ini menggunakan konsol, ikuti instruksi [Melampirkan kriteria filter ke pemetaan sumber peristiwa \(konsol\)](#) dan masukkan string berikut untuk kriteria Filter.

```
{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }
```

AWS CLI

Untuk membuat pemetaan sumber peristiwa baru dengan kriteria filter ini menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah berikut.

```
aws lambda create-event-source-mapping \
  --function-name my-function \
  --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
```

```
--filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" : [ { \"numeric\": [ \">\", 9999 ] } ] } }"]}]'
```

Untuk menambahkan kriteria filter ini ke pemetaan sumber peristiwa yang ada, jalankan perintah berikut.

```
aws lambda update-event-source-mapping \
  --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
  --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" : [ { \"numeric\": [ \">\", 9999 ] } ] } }"]}]'
```

AWS SAM

Untuk menambahkan filter ini menggunakan AWS SAM, tambahkan cuplikan berikut ke YAML template untuk sumber acara Anda.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }'
```

Untuk AmazonSQS, badan pesan dapat berupa string apa pun. Namun, ini bisa menjadi masalah jika Anda `FilterCriteria` body berharap berada dalam JSON format yang valid. Skenario sebaliknya juga benar—jika isi pesan yang masuk dalam JSON format tetapi kriteria filter Anda diharapkan menjadi string biasa, ini dapat body menyebabkan perilaku yang tidak diinginkan.

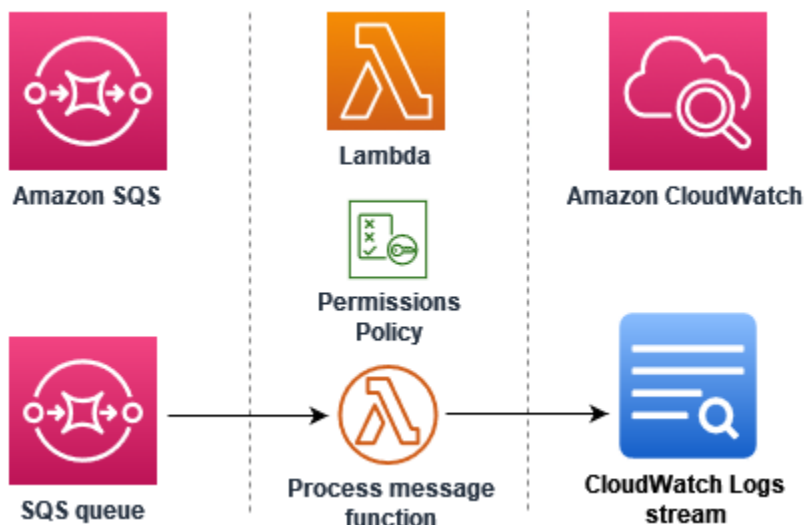
Untuk menghindari masalah ini, pastikan bahwa format isi dalam Anda `FilterCriteria` cocok dengan format yang diharapkan body dalam pesan yang Anda terima dari antrian Anda. Sebelum memfilter pesan Anda, Lambda secara otomatis mengevaluasi format badan pesan masuk dan pola filter Anda. body Jika ada ketidakcocokan, Lambda menjatuhkan pesan. Tabel berikut merangkum evaluasi ini:

| Format pesan body masuk | body Format pola filter | Tindakan yang dihasilkan |
|--------------------------------|---|--|
| Tali polos | Tali polos | Filter Lambda berdasarkan kriteria filter Anda. |
| Tali polos | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) |

| Format pesan body masuk | body Format pola filter | Tindakan yang dihasilkan |
|--------------------------------|---|--|
| | | berdasarkan kriteria filter Anda. |
| Tali polos | Valid JSON | Lambda menjatuhkan pesan. |
| Valid JSON | Tali polos | Lambda menjatuhkan pesan. |
| Valid JSON | Tidak ada pola filter untuk properti data | Filter Lambda (hanya pada properti metadata lainnya) berdasarkan kriteria filter Anda. |
| Valid JSON | Valid JSON | Filter Lambda berdasarkan kriteria filter Anda. |

Tutorial: Menggunakan Lambda dengan Amazon SQS

Dalam tutorial ini, Anda membuat fungsi Lambda yang menggunakan pesan dari antrian [Amazon Simple Queue Service \(Amazon SQS\)](#). Fungsi Lambda berjalan setiap kali pesan baru ditambahkan ke antrian. Fungsi ini menulis pesan ke aliran Amazon CloudWatch Logs. Diagram berikut menunjukkan sumber daya AWS yang Anda gunakan untuk menyelesaikan tutorial.



Untuk menyelesaikan tutorial ini, Anda melakukan langkah-langkah berikut:

1. Buat fungsi Lambda yang menulis pesan ke CloudWatch Log.

2. Membuat antrean Amazon SQS.
3. Buat pemetaan sumber acara Lambda. Pemetaan sumber peristiwa membaca antrian Amazon SQS dan memanggil fungsi Lambda Anda saat pesan baru ditambahkan.
4. Uji penyiapan dengan menambahkan pesan ke antrian Anda dan pantau hasilnya di CloudWatch Log.

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/signup>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi <https://aws.amazon.com/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Instal AWS Command Line Interface

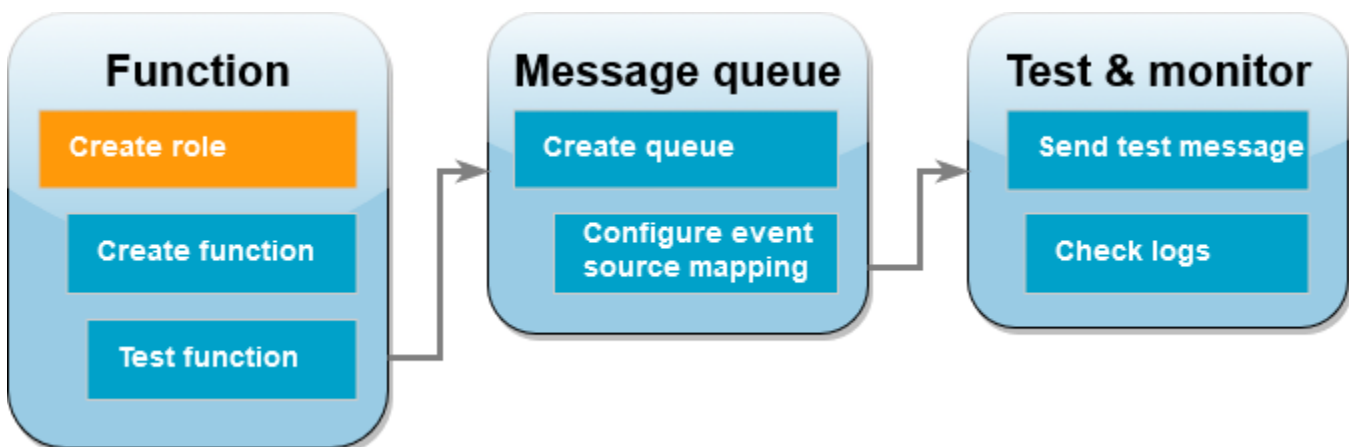
Jika Anda belum menginstal AWS Command Line Interface, ikuti langkah-langkah di [Menginstal atau memperbarui versi terbaru AWS CLI untuk menginstalnya](#).

Tutorial ini membutuhkan terminal baris perintah atau shell untuk menjalankan perintah. Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#).

Buat peran eksekusi



Peran [eksekusi adalah peran](#) AWS Identity and Access Management (IAM) yang memberikan izin fungsi Lambda untuk mengakses AWS layanan dan sumber daya. Untuk mengizinkan fungsi Anda membaca item dari Amazon SQS, lampirkan kebijakan `AWSLambdaSQSQueueExecutionRole` izin.

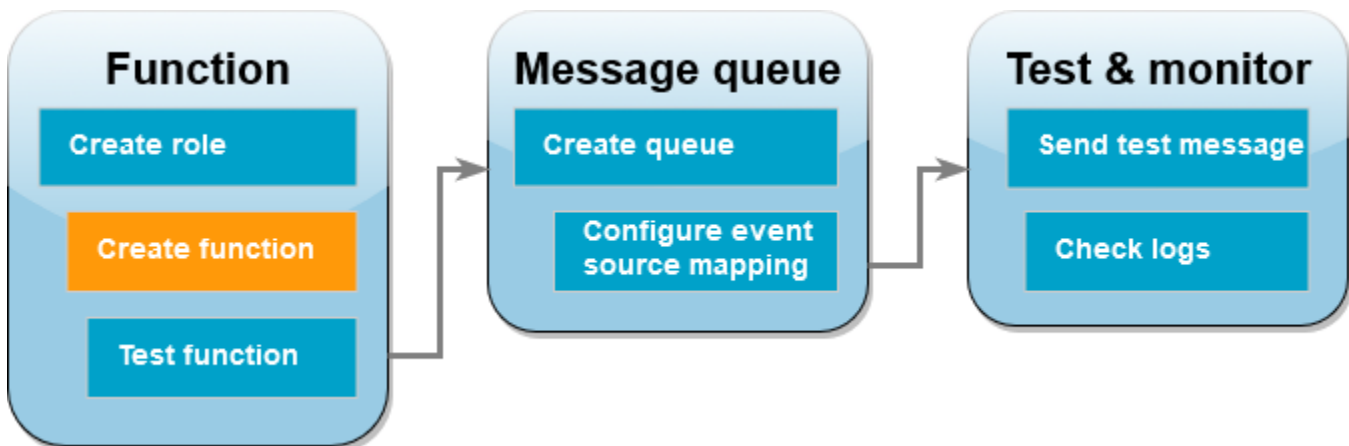
Untuk membuat peran eksekusi dan melampirkan kebijakan izin Amazon SQS

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih Buat peran.
3. Untuk jenis entitas Tepercaya, pilih AWS layanan.
4. Untuk kasus penggunaan, pilih Lambda.
5. Pilih Selanjutnya.

6. Di kotak pencarian Kebijakan izin, masukkan **AWSLambdaSQSQueueExecutionRole**.
7. Pilih **AWSLambdaSQSQueueExecutionRole** kebijakan, lalu pilih Berikutnya.
8. Di bawah Rincian peran, untuk nama Peran **lambda-sqs-role**, masukkan, lalu pilih Buat peran.

Setelah pembuatan peran, catat Nama Sumber Daya Amazon (ARN) peran eksekusi Anda. Anda akan membutuhkannya di langkah selanjutnya.

Buat fungsi



Buat fungsi Lambda yang memproses pesan Amazon SQS Anda. Kode fungsi mencatat isi pesan Amazon SQS ke CloudWatch Log.

Tutorial ini menggunakan runtime Node.js 18.x, tetapi kami juga menyediakan kode contoh dalam bahasa runtime lainnya. Anda dapat memilih tab di kotak berikut untuk melihat kode runtime yang Anda minati. JavaScript Kode yang akan Anda gunakan dalam langkah ini adalah pada contoh pertama yang ditunjukkan di JavaScript tab.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan Lambda menggunakan .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly: LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }


    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
    ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
            Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

```
}
```

Go

SDK untuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara SQS dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
    for _, record := range event.Records {
        err := processMessage(record)
        if err != nil {
            return err
        }
    }
    fmt.Println("done")
    return nil
}

func processMessage(record events.SQSMessage) error {
    fmt.Printf("Processed message %s\n", record.Body)
    // TODO: Do interesting work based on the new message
    return nil
}
```

```
func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
        }
    }
}
```

```
        throw e;
    }
}
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan JavaScript Lambda menggunakan.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message) {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Mengkonsumsi acara SQS dengan TypeScript Lambda menggunakan.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";

export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara SQS dengan Lambda menggunakan PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php
```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan Lambda menggunakan Ruby.


```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].each do |message|
    process_message(message)
  end
  puts "done"
end

def process_message(message)
  begin
    puts "Processed message #{message['body']}"
    # TODO: Do interesting work based on the new message
  rescue StandardError => err
    puts "An error occurred"
    raise err
  end
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara SQS dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
  event.payload.records.iter().for_each(|record| {
    // process the record
    tracing::info!("Message body: {}",
      record.body.as_deref().unwrap_or_default())
  })
}
```

```
});

Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Untuk membuat fungsi Lambda Node.js

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir sqs-tutorial
cd sqs-tutorial
```

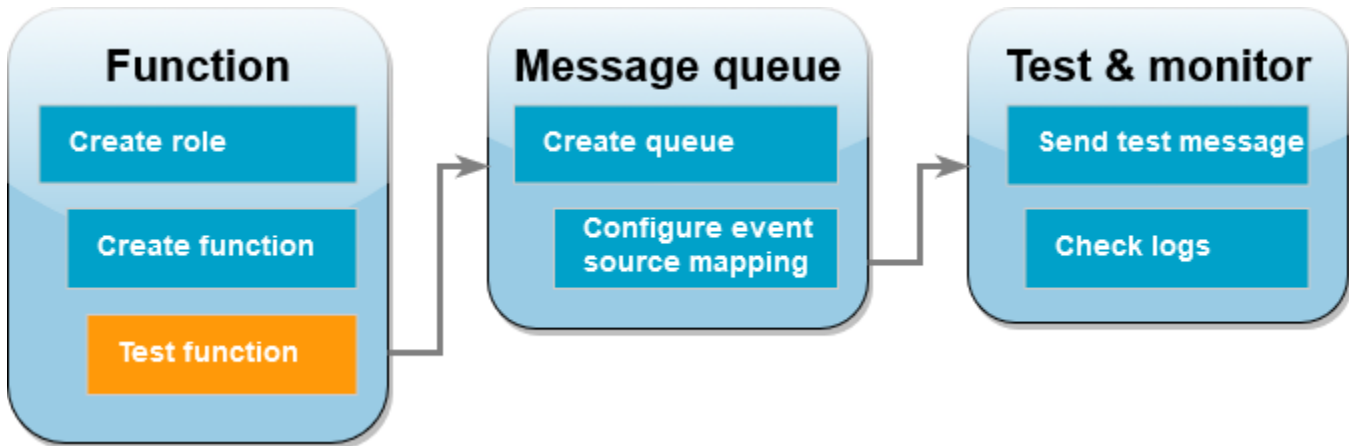
2. Salin JavaScript kode sampel ke file baru bernama `index.js`.
3. Buat paket penyebaran menggunakan zip perintah berikut.

```
zip function.zip index.js
```

4. Buat fungsi Lambda menggunakan perintah [AWS CLI create-function](#). Untuk parameter role, masukkan ARN peran eksekusi yang Anda buat sebelumnya.

```
aws lambda create-function --function-name ProcessSQSRecord \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
--role arn:aws:iam::111122223333:role/lambda-sqs-role
```

Uji fungsi



Memanggil fungsi Lambda Anda secara manual menggunakan `invoke` AWS CLI perintah dan contoh peristiwa Amazon SQS.

Untuk memanggil fungsi Lambda dengan contoh peristiwa

1. Simpan JSON berikut sebagai file bernama `input.json`. JSON ini mensimulasikan peristiwa yang mungkin dikirimkan Amazon SQS ke fungsi Lambda Anda, yang berisi pesan aktual dari "body" antrian. Dalam contoh ini, pesannya adalah "test".

Example Acara Amazon SQS

Ini adalah acara pengujian—Anda tidak perlu mengubah pesan atau nomor akun.

```

{
  "Records": [
    {
      "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
      "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgXlaS3SLy0a...",
      "body": "test",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOL023YVJ4V0",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
      },
      "messageAttributes": {},
      "md5ofBody": "098f6bcd4621d373cade4e832627b4f6",
      "eventSource": "aws:sqs",
      "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:my-queue",
    }
  ]
}
  
```

```

    "awsRegion": "us-east-1"
  }
]
}

```

2. Jalankan AWS CLI perintah [pemanggilan berikut](#). Perintah ini mengembalikan CloudWatch log dalam respon. Untuk informasi selengkapnya tentang mendapatkan log kembali, lihat [Mengakses log dengan AWS CLI](#).

```

aws lambda invoke --function-name ProcessSQSRecord --payload file://input.json out
--log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode

```

cli-binary-format Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

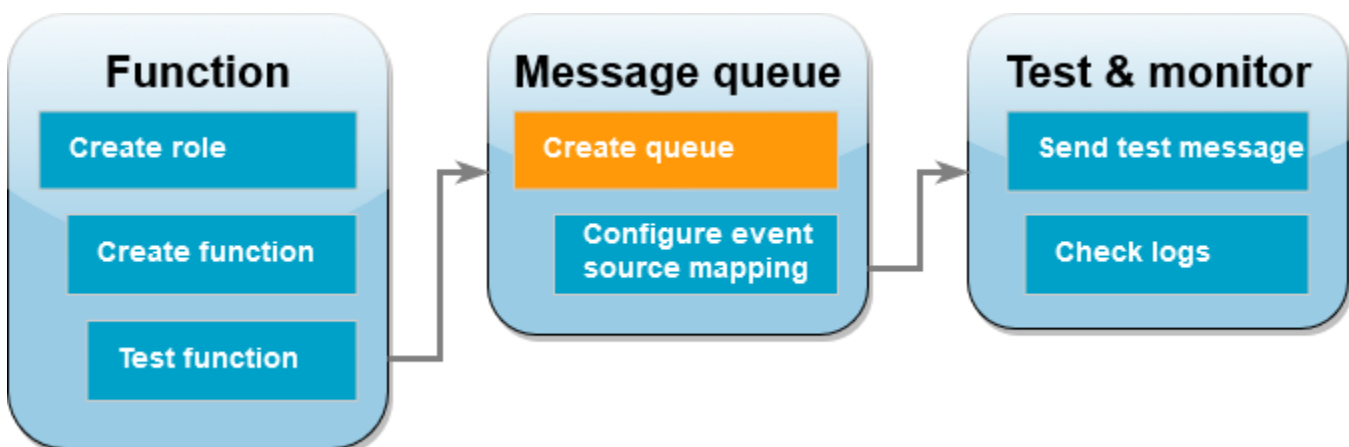
3. Temukan INFO log di respons. Di sinilah fungsi Lambda mencatat badan pesan. Anda akan melihat log yang terlihat seperti ini:

```

2023-09-11T22:45:04.271Z 348529ce-2211-4222-9099-59d07d837b60 INFO Processed
message test
2023-09-11T22:45:04.288Z 348529ce-2211-4222-9099-59d07d837b60 INFO done

```

Buat antrian Amazon SQS



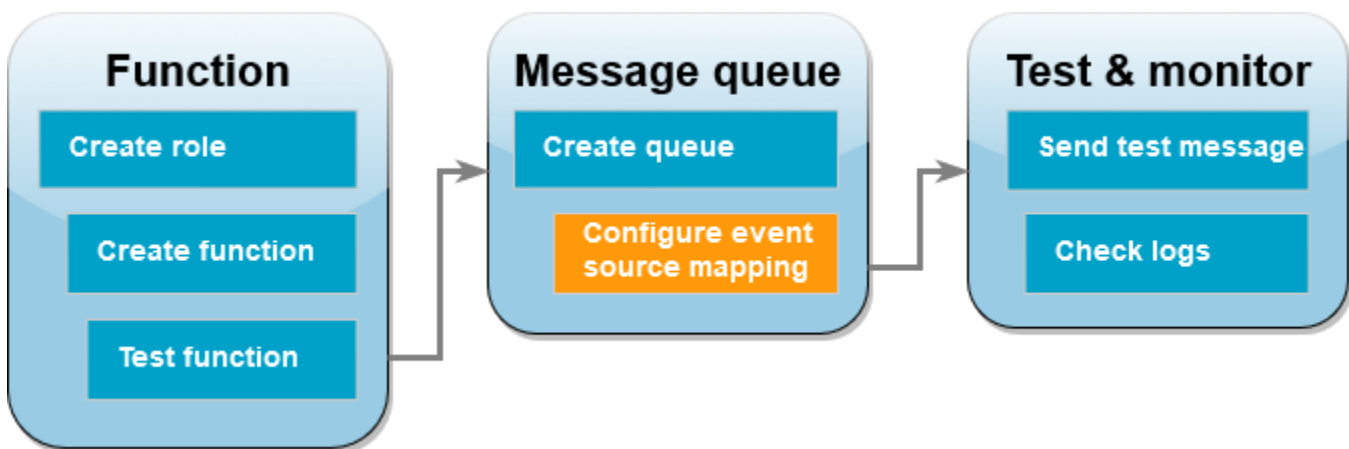
Buat antrian Amazon SQS yang dapat digunakan oleh fungsi Lambda sebagai sumber kejadian.

Untuk membuat antrian

1. Buka [konsol Amazon SQS](#).
2. Pilih Buat antrian.
3. Masukkan nama untuk antrian. Biarkan semua opsi lain di pengaturan default.
4. Pilih Buat antrian.

Setelah membuat antrian, catat ARN-nya. Anda memerlukan ini di langkah berikutnya ketika Anda mengasosiasikan antrian dengan fungsi Lambda Anda.

Konfigurasi sumber kejadian



[Hubungkan antrian Amazon SQS ke fungsi Lambda Anda dengan membuat pemetaan sumber peristiwa.](#) Pemetaan sumber peristiwa membaca antrian Amazon SQS dan memanggil fungsi Lambda Anda saat pesan baru ditambahkan.

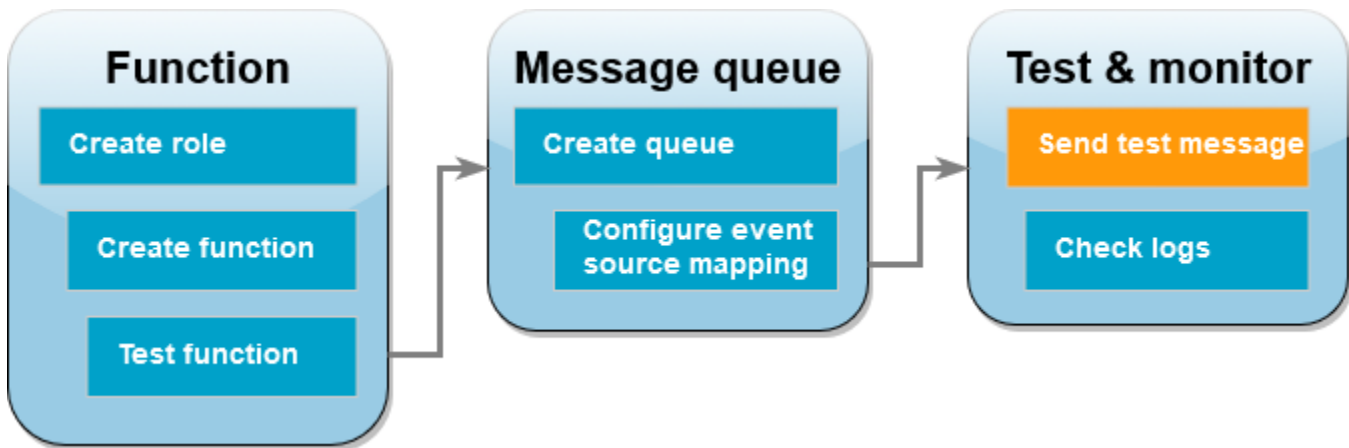
Untuk membuat pemetaan antara antrian Amazon SQS dan fungsi Lambda Anda, gunakan perintah [create-event-source-mapping](#) AWS CLI Contoh:

```
aws lambda create-event-source-mapping --function-name ProcessSQSRecord --batch-size 10 \
--event-source-arn arn:aws:sqs:us-east-1:111122223333:my-queue
```

Untuk mendapatkan daftar pemetaan sumber acara Anda, gunakan perintah [list-event-source-mappings](#) Contoh:

```
aws lambda list-event-source-mappings --function-name ProcessSQSRecord
```

Kirim pesan pengujian

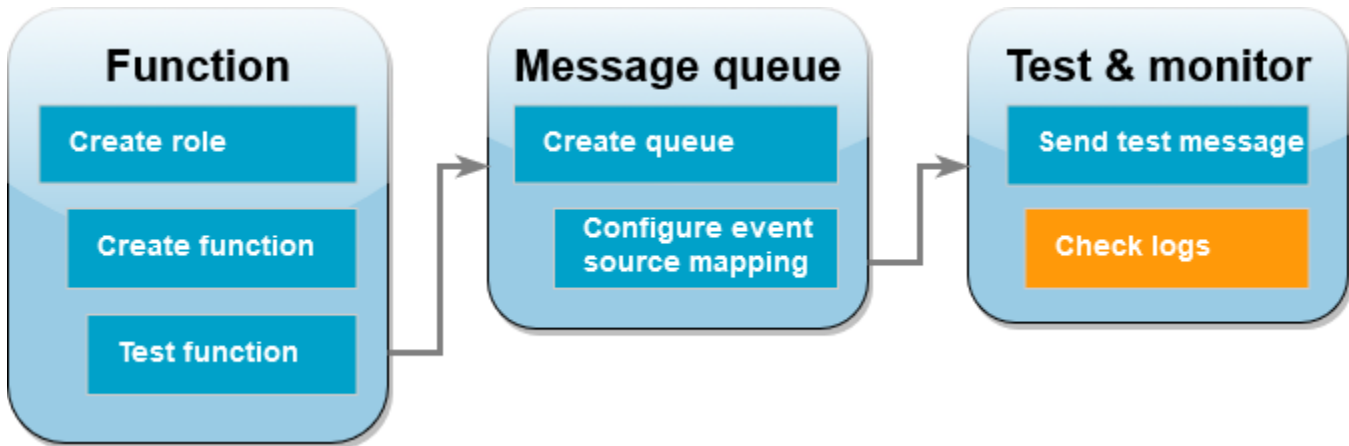


Untuk mengirim pesan Amazon SQS ke fungsi Lambda

1. Buka [konsol Amazon SQS](#).
2. Pilih antrian yang Anda buat sebelumnya.
3. Pilih Kirim dan terima pesan.
4. Di bawah Badan pesan, masukkan pesan pengujian, seperti "ini adalah pesan pengujian."
5. Pilih Kirim pesan.

Lambda melakukan polling antrian untuk pembaruan. Ketika ada pesan baru, Lambda memanggil fungsi Anda dengan data peristiwa baru ini dari antrian. Jika fungsi handler kembali tanpa pengecualian, Lambda menganggap pesan berhasil diproses dan mulai membaca pesan baru dalam antrian. Setelah berhasil memproses pesan, Lambda secara otomatis menghapusnya dari antrian. Jika handler melempar pengecualian, Lambda menganggap kumpulan pesan tidak berhasil diproses, dan Lambda memanggil fungsi dengan kumpulan pesan yang sama.

Periksa CloudWatch log



Untuk mengonfirmasi bahwa fungsi tersebut memproses pesan

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi ProcessSQSRecord.
3. Pilih Monitor.
4. Pilih Lihat CloudWatch log.
5. Di CloudWatch konsol, pilih aliran Log untuk fungsi tersebut.
6. Temukan INFO log. Di sinilah fungsi Lambda mencatat badan pesan. Anda akan melihat pesan yang Anda kirim dari antrian Amazon SQS. Contoh:

```
2023-09-11T22:49:12.730Z b0c41e9c-0556-5a8b-af83-43e59efeeec71 INFO Processed message this is a test message.
```

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.

4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus antrean Amazon SQS

1. [Masuk ke AWS Management Console dan buka konsol Amazon SQS di https://console.aws.amazon.com/sqs/.](https://console.aws.amazon.com/sqs/)
2. Pilih antrean yang Anda buat.
3. Pilih Hapus.
4. Masukkan **confirm** di bidang input teks.
5. Pilih Hapus.

Tutorial: Menggunakan antrian Amazon SQS lintas akun sebagai sumber acara

Dalam tutorial ini, Anda membuat fungsi Lambda yang menggunakan pesan dari antrian Amazon Simple Queue Service (Amazon SQS) di akun yang berbeda. AWS Tutorial ini melibatkan dua AWS akun: Akun A mengacu pada akun yang berisi fungsi Lambda Anda, dan Akun B mengacu pada akun yang berisi antrian Amazon SQS.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki pengetahuan tentang operasi Lambda dan konsol Lambda dasar. Jika belum, ikuti petunjuk di [Membuat fungsi Lambda dengan konsol](#) untuk membuat fungsi Lambda pertama Anda.

Untuk menyelesaikan langkah-langkah berikut, Anda memerlukan [AWS Command Line Interface \(AWS CLI\) versi 2](#). Perintah dan output yang diharapkan dicantumkan dalam blok terpisah:

```
aws --version
```


Anda akan melihat output berikut:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Untuk perintah panjang, karakter escape (\) digunakan untuk memisahkan perintah menjadi beberapa baris.

Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa perintah Bash CLI yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#). Contoh perintah CLI dalam panduan ini menggunakan pemformatan Linux. Perintah yang menyertakan dokumen JSON sebaris harus diformat ulang jika Anda menggunakan CLI Windows.

Buat peran eksekusi (Akun A)

Di Akun A, buat [peran eksekusi](#) yang memberikan izin fungsi Anda untuk mengakses AWS sumber daya yang diperlukan.

Untuk membuat peran eksekusi

1. Buka [halaman Peran](#) di konsol AWS Identity and Access Management (IAM).
2. Pilih Buat peran.
3. Buat peran dengan properti berikut.
 - Entitas tepercaya - AWS Lambda
 - Izin – `AWSLambdaSQSQueueExecutionRole`
 - Nama peran – **cross-account-lambda-sqs-role**

`AWSLambdaSQSQueueExecutionRole` Kebijakan ini memiliki izin yang diperlukan fungsi untuk membaca item dari Amazon SQS dan untuk menulis log ke Amazon CloudWatch Logs.

Buat fungsi (Akun A)

Di Akun A, buat fungsi Lambda yang memproses pesan Amazon SQS Anda. Contoh kode Node.js 18 berikut menulis setiap pesan ke log in CloudWatch Log.

Example index.mjs

```
export const handler = async function(event, context) {
  event.Records.forEach(record => {
    const { body } = record;
    console.log(body);
  });
  return {};
}
```

Untuk membuat fungsi

Note

Mengikuti langkah-langkah ini menciptakan fungsi di Node.js 18. Untuk bahasa lain, langkah-langkahnya serupa, tetapi beberapa detailnya berbeda.

1. Simpan contoh kode sebagai file bernama `index.mjs`.
2. Buat paket deployment.

```
zip function.zip index.mjs
```

3. Buat fungsi menggunakan perintah `create-function` AWS Command Line Interface (AWS CLI).

```
aws lambda create-function --function-name CrossAccountSQSExample \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
--role arn:aws:iam::<AccountA_ID>:role/cross-account-lambda-sqs-role
```

Uji fungsi (Akun A)

Di Akun A, uji fungsi Lambda Anda secara manual menggunakan `invoke` AWS CLI perintah dan contoh peristiwa Amazon SQS.

Jika handler kembali normal tanpa pengecualian, Lambda menganggap pesan berhasil diproses dan mulai membaca pesan baru dalam antrian. Setelah berhasil memproses pesan, Lambda secara otomatis menghapusnya dari antrian. Jika handler melempar pengecualian, Lambda menganggap kumpulan pesan tidak berhasil diproses, dan Lambda memanggil fungsi dengan kumpulan pesan yang sama.

1. Simpan JSON berikut sebagai file bernama `input.txt`.

```
{
  "Records": [
    {
      "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
      "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgXlaS3SLy0a...",
      "body": "test",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOL023YVJ4V0",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
      },
      "messageAttributes": {},
      "md5OfBody": "098f6bcd4621d373cade4e832627b4f6",
      "eventSource": "aws:sqs",
      "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:example-queue",
      "awsRegion": "us-east-1"
    }
  ]
}
```

JSON sebelumnya mensimulasikan peristiwa yang mungkin dikirimkan Amazon SQS ke fungsi Lambda Anda, yang berisi pesan aktual dari antrian. "body"

2. Jalankan perintah `invoke` AWS CLI berikut.

```
aws lambda invoke --function-name CrossAccountSQSExample \
  --cli-binary-format raw-in-base64-out \
  --payload file://input.txt outputfile.txt
```

`cli-binary-format` Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-`

base64-out. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

3. Verifikasikan output dalam `outputfile.txt` file.

Buat antrian Amazon SQS (Akun B)

Di Akun B, buat antrian Amazon SQS yang dapat digunakan oleh fungsi Lambda di Akun A sebagai sumber peristiwa.

Untuk membuat antrian

1. Buka [konsol Amazon SQS](#).
2. Pilih Buat antrian.
3. Buat antrian dengan properti berikut.
 - Jenis - Standar
 - Nama - LambdaCrossAccountQueue
 - Konfigurasi - Pertahankan pengaturan default.
 - Kebijakan akses — Pilih Lanjutan. Tempel dalam kebijakan JSON berikut:

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement": [{
    "Sid": "Queue1_AllActions",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::<AccountA_ID>:role/cross-account-lambda-sqs-role"
      ]
    },
    "Action": "sqs:*",
    "Resource": "arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue"
  ]
}
```

Kebijakan ini memberikan peran eksekusi Lambda dalam izin Akun A untuk menggunakan pesan dari antrian Amazon SQS ini.

4. Setelah membuat antrian, rekam Nama Sumber Daya Amazon (ARN). Anda memerlukan ini di langkah berikutnya ketika Anda mengasosiasikan antrian dengan fungsi Lambda Anda.

Konfigurasi sumber acara (Akun A)

Di Akun A, buat pemetaan sumber peristiwa antara antrian Amazon SQS di Akun B dan fungsi Lambda Anda dengan menjalankan perintah berikut. `create-event-source-mapping` AWS CLI

```
aws lambda create-event-source-mapping --function-name CrossAccountSQSExample --batch-size 10 \  
--event-source-arn arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue
```

Untuk mendapatkan daftar pemetaan sumber acara Anda, jalankan perintah berikut.

```
aws lambda list-event-source-mappings --function-name CrossAccountSQSExample \  
--event-source-arn arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue
```

Uji penyiapan

Anda sekarang dapat menguji pengaturan sebagai berikut:

1. Di Akun B, buka konsol [Amazon SQS](#).
2. Pilih `LambdaCrossAccountQueue`, yang Anda buat sebelumnya.
3. Pilih Kirim dan terima pesan.
4. Di bawah Badan pesan, masukkan pesan pengujian.
5. Pilih Kirim pesan.

Fungsi Lambda Anda di Akun A harus menerima pesan. Lambda akan terus melakukan polling antrian untuk pembaruan. Ketika ada pesan baru, Lambda memanggil fungsi Anda dengan data peristiwa baru ini dari antrian. Fungsi Anda berjalan dan membuat log di Amazon CloudWatch. Anda dapat melihat log di [CloudWatch konsol](#).

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Di Akun A, bersihkan peran eksekusi dan fungsi Lambda Anda.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Di Akun B, bersihkan antrian Amazon SQS.

Untuk menghapus antrean Amazon SQS

1. [Masuk ke AWS Management Console dan buka konsol Amazon SQS di https://console.aws.amazon.com/sqs/.](https://console.aws.amazon.com/sqs/)
2. Pilih antrean yang Anda buat.
3. Pilih Hapus.
4. Masukkan **confirm** di bidang input teks.
5. Pilih Hapus.

Memanggil fungsi Lambda dengan acara batch Amazon S3

Anda dapat menggunakan operasi batch Amazon S3 untuk memanggil fungsi Lambda pada serangkaian besar objek Amazon S3. Amazon S3 melacak kemajuan operasi batch, mengirimkan pemberitahuan, dan menyimpan laporan penyelesaian yang menunjukkan status setiap tindakan.

Untuk menjalankan operasi batch, Anda membuat [pekerjaan operasi batch](#) Amazon S3. Saat Anda membuat pekerjaan, Anda memberikan manifest (daftar objek) dan mengonfigurasi tindakan yang akan dilakukan pada objek tersebut.

Saat pekerjaan batch dimulai, Amazon S3 memanggil fungsi Lambda [secara sinkron](#) untuk setiap objek dalam manifest. Parameter kejadian mencakup nama bucket dan objek.

Contoh berikut menunjukkan peristiwa yang dikirimkan Amazon S3 ke fungsi Lambda untuk objek yang diberi nama `customerImage1.jpg` di bucket `amzn-s3-demo-bucket`.

Example Kejadian permintaan batch Amazon S3

```
{
  "invocationSchemaVersion": "1.0",
  "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "job": {
    "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
  },
  "tasks": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "s3Key": "customerImage1.jpg",
      "s3VersionId": "1",
      "s3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

Fungsi Lambda Anda harus mengembalikan JSON objek dengan bidang seperti yang ditunjukkan pada contoh berikut. Anda dapat menyalin `invocationId` dan `taskId` dari parameter kejadian. Anda dapat mengembalikan string di `resultString`. Amazon S3 menyimpan nilai `resultString` dalam laporan penyelesaian.

Example Respons permintaan batch Amazon S3

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Alice\", \"Bob\"]"
    }
  ]
}
```

Memanggil fungsi Lambda dari operasi batch Amazon S3

Anda dapat menjalankan fungsi Lambda dengan fungsi yang tidak memenuhi syarat atau memenuhi syarat. ARN Jika Anda ingin menggunakan versi fungsi yang sama untuk seluruh pekerjaan batch, konfigurasi versi fungsi tertentu di parameter `FunctionARN` saat membuat pekerjaan Anda. Jika Anda mengonfigurasi alias atau `$ LATEST` qualifier, pekerjaan batch segera mulai memanggil versi baru fungsi jika alias atau `$ LATEST` diperbarui selama eksekusi pekerjaan.

Perhatikan bahwa Anda tidak dapat menggunakan kembali fungsi berbasis kejadian Amazon S3 yang sudah ada untuk operasi batch. Ini karena operasi batch Amazon S3 meneruskan parameter peristiwa yang berbeda ke fungsi Lambda dan mengharapkan pesan kembali dengan struktur tertentu. JSON

Di [kebijakan berbasis sumber daya](#) yang Anda buat untuk pekerjaan batch Amazon S3, pastikan Anda menetapkan izin untuk pekerjaan tersebut untuk memanggil fungsi Lambda Anda.

Di [peran eksekusi](#) untuk fungsi tersebut, tetapkan kebijakan kepercayaan bagi Amazon S3 untuk mengambil peran tersebut saat menjalankan fungsi Anda.

Jika fungsi Anda menggunakan AWS SDK untuk mengelola sumber daya Amazon S3, Anda perlu menambahkan izin Amazon S3 dalam peran eksekusi.

Saat pekerjaan berjalan, Amazon S3 memulai beberapa instans fungsi untuk memproses objek Amazon S3 secara paralel, hingga mencapai [batas konkurensi](#) fungsi. Amazon S3 membatasi peningkatan instans awal guna menghindari biaya berlebih untuk pekerjaan kecil.

Jika fungsi Lambda mengembalikan kode respons `TemporaryFailure`, Amazon S3 akan mengulangi operasi.

Untuk informasi lebih lanjut tentang operasi batch Amazon S3, lihat [Melakukan operasi batch](#) dalam Panduan Developer Amazon S3.

Untuk contoh cara menggunakan fungsi Lambda di operasi batch Amazon S3, lihat [Memanggil fungsi Lambda dari operasi batch Amazon S3](#) dalam Panduan Developer Amazon S3.

Memanggil fungsi Lambda dengan notifikasi Amazon SNS

Anda dapat menggunakan fungsi Lambda untuk memproses notifikasi Amazon Simple Notification Service (Amazon SNS). Amazon SNS mendukung fungsi Lambda sebagai target untuk pesan yang dikirim ke topik. Anda dapat melanggan fungsi Anda ke topik di akun yang sama atau di akun AWS lainnya. Untuk panduan mendetail, lihat [the section called “Tutorial”](#)

Lambda mendukung pemicu SNS untuk topik SNS standar saja. Topik FIFO tidak didukung.

Untuk invokasi asinkron, Lambda mengantrekan pesan dan menangani percobaan ulang. Jika Amazon SNS tidak dapat mencapai Lambda atau pesan ditolak, Amazon SNS melakukan percobaan ulang dengan interval yang diperpanjang selama beberapa jam. Untuk perinciannya, lihat [Reliabilitas](#) di FAQ Amazon SNS.

Warning

Pemetaan sumber peristiwa Lambda memproses setiap peristiwa setidaknya sekali, dan pemrosesan duplikat catatan dapat terjadi. Untuk menghindari potensi masalah yang terkait dengan duplikat peristiwa, kami sangat menyarankan agar Anda membuat kode fungsi Anda idempoten. Untuk mempelajari lebih lanjut, lihat [Bagaimana cara membuat fungsi Lambda saya idempoten](#) di Pusat Pengetahuan. AWS

Topik

- [Menambahkan pemicu topik Amazon SNS untuk fungsi Lambda menggunakan konsol](#)
- [Menambahkan pemicu topik Amazon SNS secara manual untuk fungsi Lambda](#)
- [Contoh bentuk acara SNS](#)
- [Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service](#)

Menambahkan pemicu topik Amazon SNS untuk fungsi Lambda menggunakan konsol

Untuk menambahkan topik SNS sebagai pemicu fungsi Lambda, cara termudah adalah dengan menggunakan konsol Lambda. Saat Anda menambahkan pemicu melalui konsol, Lambda secara otomatis mengatur izin dan langganan yang diperlukan untuk mulai menerima acara dari topik SNS.

Untuk menambahkan topik SNS sebagai pemicu fungsi Lambda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih nama fungsi yang ingin Anda tambahkan pemicunya.
3. Pilih Konfigurasi, lalu pilih Pemicu.
4. Pilih Tambahkan pemicu.
5. Di bawah konfigurasi Trigger, di menu tarik-turun, pilih SNS.
6. Untuk topik SNS, pilih topik SNS untuk berlangganan.

Menambahkan pemicu topik Amazon SNS secara manual untuk fungsi Lambda

Untuk mengatur pemicu SNS untuk fungsi Lambda secara manual, Anda harus menyelesaikan langkah-langkah berikut:

- Tentukan kebijakan berbasis sumber daya untuk fungsi Anda agar SNS dapat memanggilmnya.
- Berlangganan fungsi Lambda Anda ke topik Amazon SNS.

Note

Jika topik SNS dan fungsi Lambda Anda berada di akun AWS yang berbeda, Anda juga perlu memberikan izin tambahan untuk mengizinkan langganan lintas akun ke topik SNS. Untuk informasi selengkapnya, lihat [Memberikan izin lintas akun untuk langganan Amazon SNS](#).

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk menyelesaikan kedua langkah ini. Pertama, untuk menentukan kebijakan berbasis sumber daya untuk fungsi Lambda yang memungkinkan pemanggilan SNS, gunakan perintah berikut. AWS CLI Pastikan untuk mengganti nilai `--function-name` dengan nama fungsi Lambda Anda, dan nilai `--source-arn` dengan ARN topik SNS Anda.

```
aws lambda add-permission --function-name example-function \  
  --source-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \  
  --statement-id function-with-sns --action "lambda:InvokeFunction" \  
  --principal sns.amazonaws.com
```

Untuk berlangganan fungsi Anda ke topik SNS, gunakan AWS CLI perintah berikut. Ganti nilai `--topic-arn` dengan ARN topik SNS Anda, dan nilai `--notification-endpoint` ARN dengan fungsi Lambda Anda.

```
aws sns subscribe --protocol lambda \  
  --region us-east-1 \  
  --topic-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \  
  --notification-endpoint arn:aws:lambda:us-east-1:123456789012:function:example-  
function
```

Contoh bentuk acara SNS

Amazon SNS memanggil fungsi Anda [secara asinkron](#) dengan kejadian yang berisi pesan dan metadata.

Example Kejadian pesan Amazon SNS

```
{  
  "Records": [  
    {  
      "EventVersion": "1.0",  
      "EventSubscriptionArn": "arn:aws:sns:us-east-1:123456789012:sns-lambda:21be56ed-  
a058-49f5-8c98-aedd2564c486",  
      "EventSource": "aws:sns",  
      "Sns": {  
        "SignatureVersion": "1",  
        "Timestamp": "2019-01-02T12:45:07.000Z",  
        "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi+tE/1+82j...65r==",  
        "SigningCertURL": "https://sns.us-east-1.amazonaws.com/  
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",  
        "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",  
        "Message": "Hello from SNS!",  
        "MessageAttributes": {  
          "Test": {  
            "Type": "String",  
            "Value": "TestString"  
          },  
          "TestBinary": {  
            "Type": "Binary",  
            "Value": "TestBinary"  
          }  
        }  
      },  
    }  
  ],  
}
```

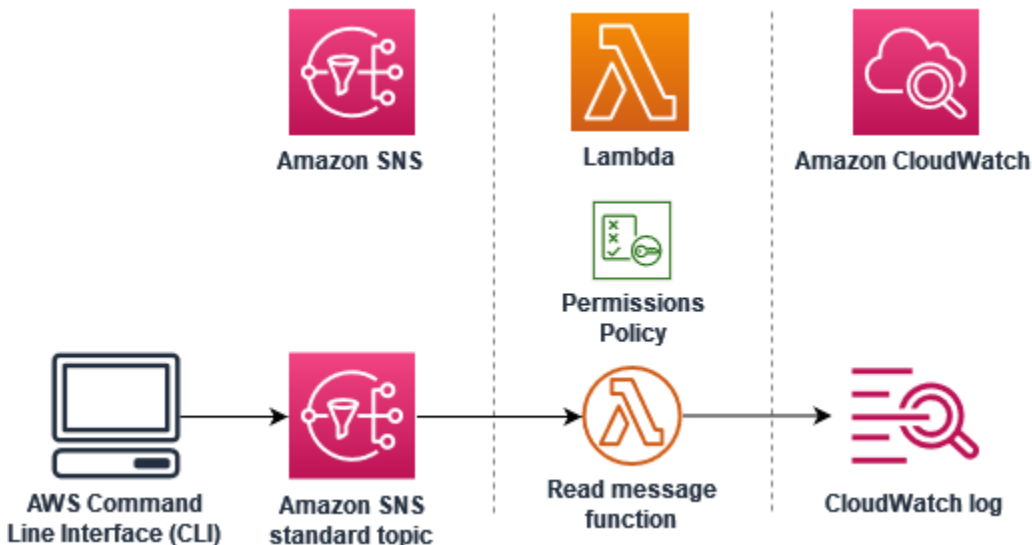
```

    "Type": "Notification",
    "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-1:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
    "TopicArn": "arn:aws:sns:us-east-1:123456789012:sns-lambda",
    "Subject": "TestInvoke"
  }
}
]
}

```

Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service

Dalam tutorial ini, Anda menggunakan fungsi Lambda dalam satu Akun AWS untuk berlangganan topik Amazon Simple Notification Service SNS (Amazon) secara terpisah. Akun AWS Saat Anda memublikasikan pesan ke SNS topik Amazon, fungsi Lambda Anda akan membaca konten pesan dan mengeluarkannya ke Amazon Logs. CloudWatch Untuk menyelesaikan tutorial ini, Anda menggunakan AWS Command Line Interface (AWS CLI).



Untuk menyelesaikan tutorial ini, Anda melakukan langkah-langkah berikut:

- Di akun A, buat SNS topik Amazon.
- Di akun B, buat fungsi Lambda yang akan membaca pesan dari topik.
- Di akun B, buat langganan ke topik.

- Publikasikan pesan ke SNS topik Amazon di akun A dan konfirmasikan bahwa fungsi Lambda di akun B mengeluarkannya ke Log. CloudWatch

Dengan menyelesaikan langkah-langkah ini, Anda akan belajar cara mengonfigurasi SNS topik Amazon untuk menjalankan fungsi Lambda. Anda juga akan mempelajari cara membuat kebijakan AWS Identity and Access Management (IAM) yang memberikan izin untuk sumber daya di sumber lain Akun AWS untuk memanggil Lambda.

Dalam tutorial, Anda menggunakan dua terpisah Akun AWS. AWS CLI Perintah mengilustrasikan hal ini dengan menggunakan dua profil bernama yang disebut `accountA` dan `accountB`, masing-masing dikonfigurasi untuk digunakan dengan yang berbeda Akun AWS. Untuk mempelajari cara mengonfigurasi penggunaan profil yang berbeda, lihat [Pengaturan file konfigurasi dan kredensi](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2. AWS CLI Pastikan untuk mengonfigurasi default yang sama Wilayah AWS untuk kedua profil.

Jika AWS CLI profil yang Anda buat untuk keduanya Akun AWS menggunakan nama yang berbeda, atau jika Anda menggunakan profil default dan satu profil bernama, ubah AWS CLI perintah dalam langkah-langkah berikut sesuai kebutuhan.

Prasyarat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirimkan Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi <https://aws.amazon.com/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftarkan Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan MFA perangkat virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

Instal AWS Command Line Interface

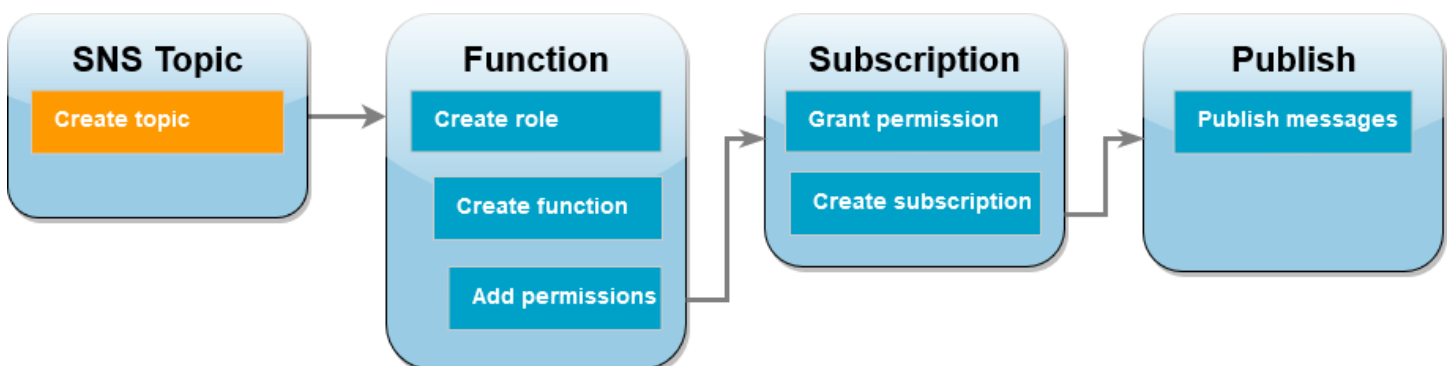
Jika Anda belum menginstal AWS Command Line Interface, ikuti langkah-langkah di [Menginstal atau memperbarui versi terbaru AWS CLI untuk menginstalnya](#).

Tutorial ini membutuhkan terminal baris perintah atau shell untuk menjalankan perintah. Di Linux dan macOS, gunakan shell dan manajer paket pilihan Anda.

Note

Di Windows, beberapa CLI perintah Bash yang biasa Anda gunakan dengan Lambda (zipseperti) tidak didukung oleh terminal bawaan sistem operasi. Untuk mendapatkan versi terintegrasi Windows dari Ubuntu dan Bash, [instal Windows Subsystem untuk Linux](#).

Buat SNS topik Amazon (akun A)



Untuk membuat topik

- Di akun A, buat topik SNS standar Amazon menggunakan AWS CLI perintah berikut.

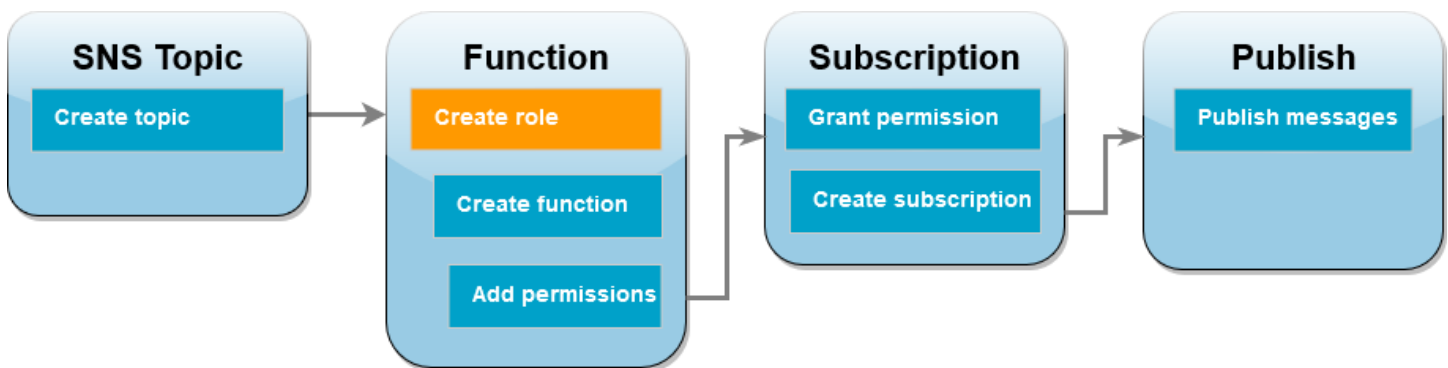
```
aws sns create-topic --name sns-topic-for-lambda --profile accountA
```

Anda akan melihat output seperti yang berikut ini.

```
{
  "TopicArn": "arn:aws:sns:us-west-2:123456789012:sns-topic-for-lambda"
}
```

Catat Nama Sumber Daya Amazon (ARN) topik Anda. Anda akan membutuhkannya nanti dalam tutorial ketika Anda menambahkan izin ke fungsi Lambda Anda untuk berlangganan topik.

Buat peran eksekusi fungsi (akun B)



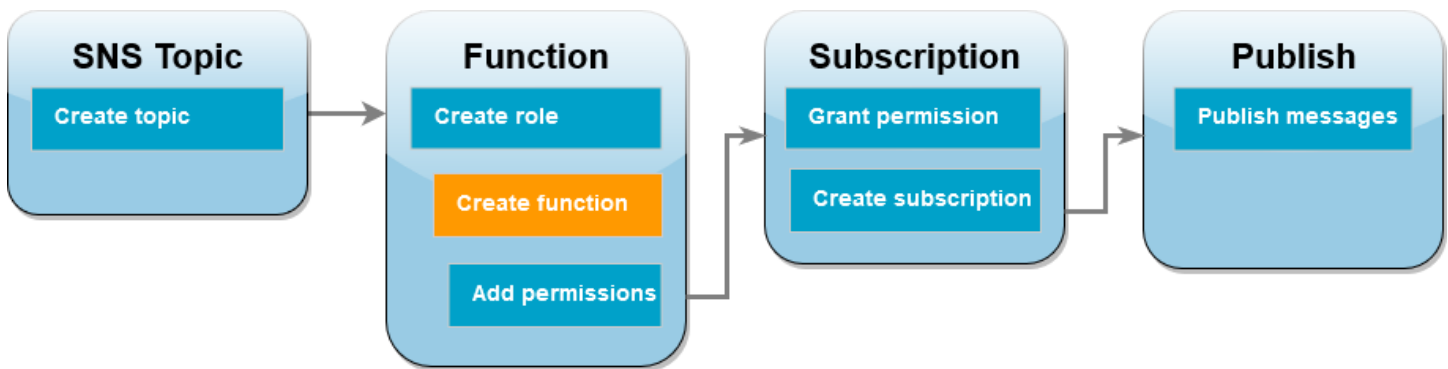
Peran eksekusi adalah IAM peran yang memberikan izin fungsi Lambda untuk AWS mengakses layanan dan sumber daya. Sebelum membuat fungsi di akun B, Anda membuat peran yang memberikan izin dasar fungsi untuk menulis CloudWatch log ke Log. Kami akan menambahkan izin untuk membaca dari SNS topik Amazon Anda di langkah selanjutnya.

Untuk membuat peran eksekusi

1. Di akun B buka [halaman peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Untuk jenis entitas Tepercaya, pilih AWS layanan.
4. Untuk kasus penggunaan, pilih Lambda.
5. Pilih Berikutnya.

6. Tambahkan kebijakan izin dasar ke peran dengan melakukan hal berikut:
 - a. Di kotak pencarian Kebijakan izin, masukkan **AWSLambdaBasicExecutionRole**.
 - b. Pilih Berikutnya.
7. Selesaikan pembuatan peran dengan melakukan hal berikut:
 - a. Di bawah Rincian peran, masukkan **lambda-sns-role** nama Peran.
 - b. Pilih Buat peran.

Buat fungsi Lambda (akun B)



Buat fungsi Lambda yang memproses pesan Amazon SNS Anda. Kode fungsi mencatat isi pesan dari setiap catatan ke Amazon CloudWatch Logs.

Tutorial ini menggunakan runtime Node.js 18.x, tetapi kami juga menyediakan kode contoh dalam bahasa runtime lainnya. Anda dapat memilih tab di kotak berikut untuk melihat kode runtime yang Anda minati. JavaScript Kode yang akan Anda gunakan dalam langkah ini adalah pada contoh pertama yang ditunjukkan di JavaScript tab.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly: LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace SnsIntegration;

public class Function
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
        foreach (var record in evnt.Records)
        {
            await ProcessRecordAsync(record, context);
        }
        context.Logger.LogInformation("done");
    }

    private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
    ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed record
            {record.Sns.Message}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
            Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

```
}
```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "fmt"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
    for _, record := range snsEvent.Records {
        processMessage(record)
    }
    fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
    message := record.SNS.Message
    fmt.Printf("Processed message: %s\n", message)
    // TODO: Process your record here
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;

import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }
}
```

```
    }

    public void processRecord(SNSRecord record) {
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan menggunakan Lambda. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    for (const record of event.Records) {
        await processMessageAsync(record);
    }
    console.info("done");
};

async function processMessageAsync(record) {
    try {
        const message = JSON.stringify(record.Sns.Message);
        console.log(`Processed message ${message}`);
    }
}
```

```
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Mengonsumsi SNS acara dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";

export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record: SNSEventRecord): Promise<any> {
  try {
    const message: string = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan menggunakan Lambda. PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
PHP functions runtime for AWS Lambda.
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-
lambda-custom-runtime-for-php-a-practical-example/
*/

// Additional composer packages may be required when using Bref or any other PHP
functions runtime.
// require __DIR__ . '/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Sns\SnsEvent;
use Bref\Event\Sns\SnsHandler;

class Handler extends SnsHandler
{
    public function handleSns(SnsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $message = $record->getMessage();

            // TODO: Implement your custom processing logic here
        }
    }
}
```



```
        // Any exception thrown will be logged and the invocation will be
        marked as failed

        echo "Processed Message: $message" . PHP_EOL;
    }
}

return new Handler();
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].map { |record| process_message(record) }
end

def process_message(record)
  message = record['Sns']['Message']
  puts("Processing message: #{message}")
rescue StandardError => e
  puts("Error processing message: #{e}")
  raise
end
```

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
// aws_lambda_events = { version = "0.10.0", default-features = false, features
// = ["sns"] }
// lambda_runtime = "0.8.1"
// tokio = { version = "1", features = ["macros"] }
// tracing = { version = "0.1", features = ["log"] }
// tracing-subscriber = { version = "0.3", default-features = false, features =
// ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for record in event.payload.records {
        process_record(&record)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);

    // Implement your record handling code here.

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Untuk membuat fungsi

1. Buat direktori untuk proyek, dan kemudian beralih ke direktori itu.

```
mkdir sns-tutorial
cd sns-tutorial
```

2. Salin JavaScript kode sampel ke file baru bernama `index.js`.
3. Buat paket penyebaran menggunakan zip perintah berikut.

```
zip function.zip index.js
```

4. Jalankan AWS CLI perintah berikut untuk membuat fungsi Lambda Anda di akun B.

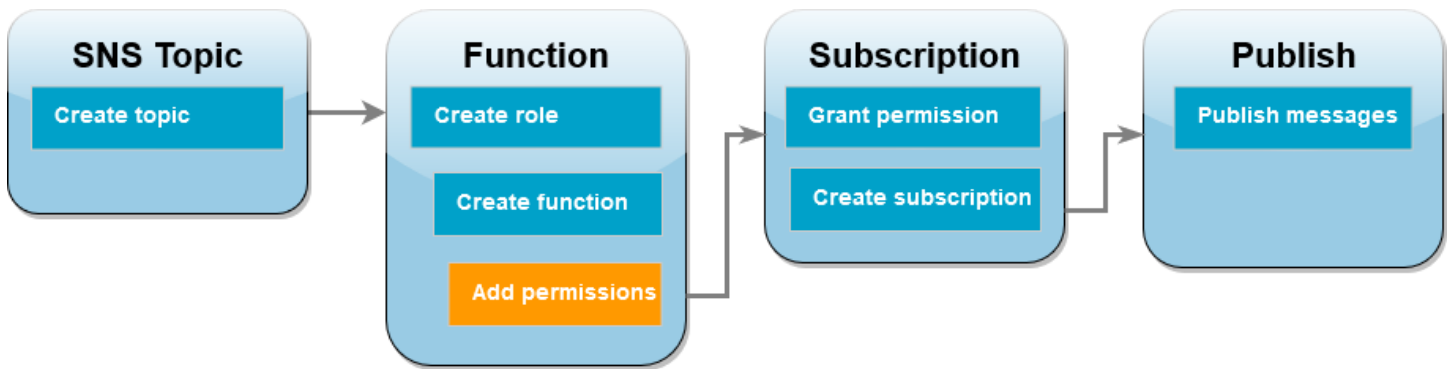
```
aws lambda create-function --function-name Function-With-SNS \
  --zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
  --role arn:aws:iam::<AccountB_ID>:role/lambda-sns-role \
  --timeout 60 --profile accountB
```

Anda akan melihat output seperti yang berikut ini.

```
{
  "FunctionName": "Function-With-SNS",
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:Function-With-SNS",
  "Runtime": "nodejs18.x",
  "Role": "arn:aws:iam::123456789012:role/lambda_basic_role",
  "Handler": "index.handler",
  ...
  "RuntimeVersionConfig": {
    "RuntimeVersionArn": "arn:aws:lambda:us-west-2::runtime:7d5f06b69c951da8a48b926ce280a9daf2e8bb1a74fc4a2672580c787d608206"
  }
}
```

5. Rekam Nama Sumber Daya Amazon (ARN) dari fungsi Anda. Anda akan membutuhkannya nanti dalam tutorial ketika Anda menambahkan izin untuk memungkinkan Amazon SNS menjalankan fungsi Anda.

Tambahkan izin ke fungsi (akun B)



SNS Agar Amazon dapat menjalankan fungsi Anda, Anda harus memberinya izin dalam pernyataan tentang kebijakan berbasis [sumber daya](#). Anda menambahkan pernyataan ini menggunakan AWS CLI `add-permission` perintah.

Untuk memberikan SNS izin Amazon untuk menjalankan fungsi Anda

- Di akun B, jalankan AWS CLI perintah berikut menggunakan SNS topik ARN untuk Amazon yang Anda rekam sebelumnya.

```
aws lambda add-permission --function-name Function-With-SNS \
  --source-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
  --statement-id function-with-sns --action "lambda:InvokeFunction" \
  --principal sns.amazonaws.com --profile accountB
```

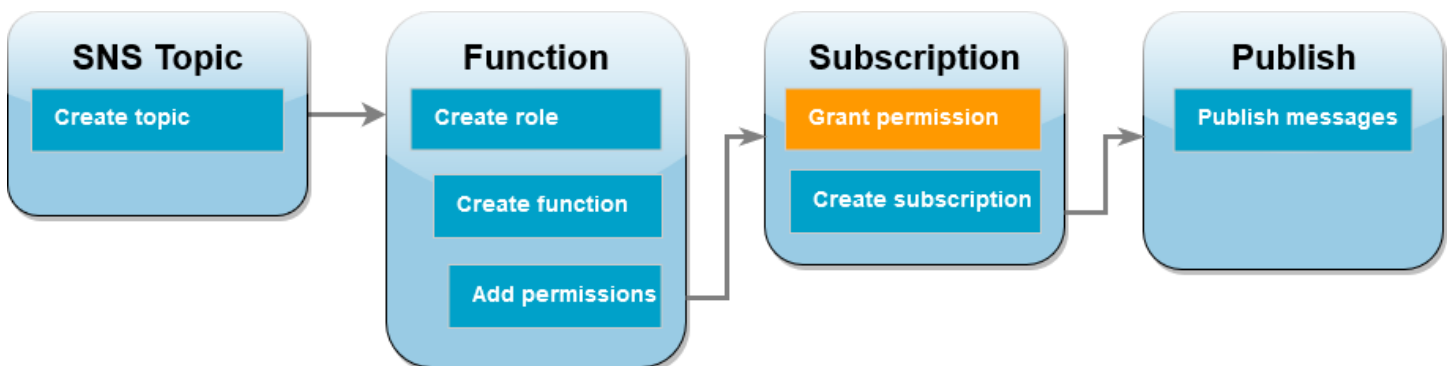
Anda akan melihat output seperti yang berikut ini.

```
{
  "Statement": [{"Condition":{"ArnLike":{"AWS:SourceArn":
    \"arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda\"}},
    \"Action\":[\"lambda:InvokeFunction\"],
    \"Resource\":\"arn:aws:lambda:us-east-1:<AccountB_ID>:function:Function-With-
    SNS\"},
    \"Effect\":\"Allow\", \"Principal\":{\"Service\":\"sns.amazonaws.com\"},
    \"Sid\":\"function-with-sns\"}]
}
```

Note

Jika akun dengan SNS topik Amazon di-host dalam [opt-in Wilayah AWS](#), Anda perlu menentukan wilayah di prinsipal. Misalnya, jika Anda bekerja dengan SNS topik Amazon di wilayah Asia Pasifik (Hong Kong), Anda harus menentukan `sns.ap-east-1.amazonaws.com` bukan `sns.amazonaws.com` untuk prinsipal.

Berikan izin lintas akun untuk SNS langganan Amazon (akun A)



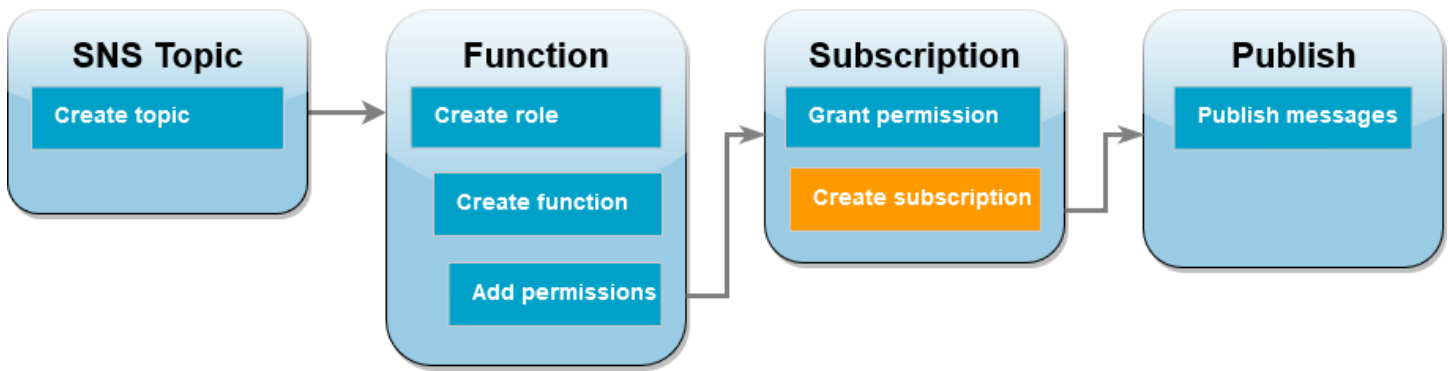
Agar fungsi Lambda Anda di akun B berlangganan SNS topik Amazon yang Anda buat di akun A, Anda harus memberikan izin untuk akun B untuk berlangganan topik Anda. Anda memberikan izin ini menggunakan AWS CLI `add-permission` perintah.

Untuk memberikan izin akun B untuk berlangganan topik

- Di akun A, jalankan AWS CLI perintah berikut. Gunakan ARN untuk SNS topik Amazon yang Anda rekam sebelumnya.

```
aws sns add-permission --label lambda-access --aws-account-id <AccountB_ID> \
  --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
  --action-name Subscribe ListSubscriptionsByTopic --profile accountA
```

Buat langganan (akun B)



Di akun B, Anda sekarang berlangganan fungsi Lambda Anda ke SNS topik Amazon yang Anda buat di awal tutorial di akun A. Saat pesan dikirim ke topik ini (`sns-topic-for-lambda`), Amazon akan SNS memanggil `Function-With-SNS` fungsi Lambda Anda di akun B.

Untuk membuat langganan

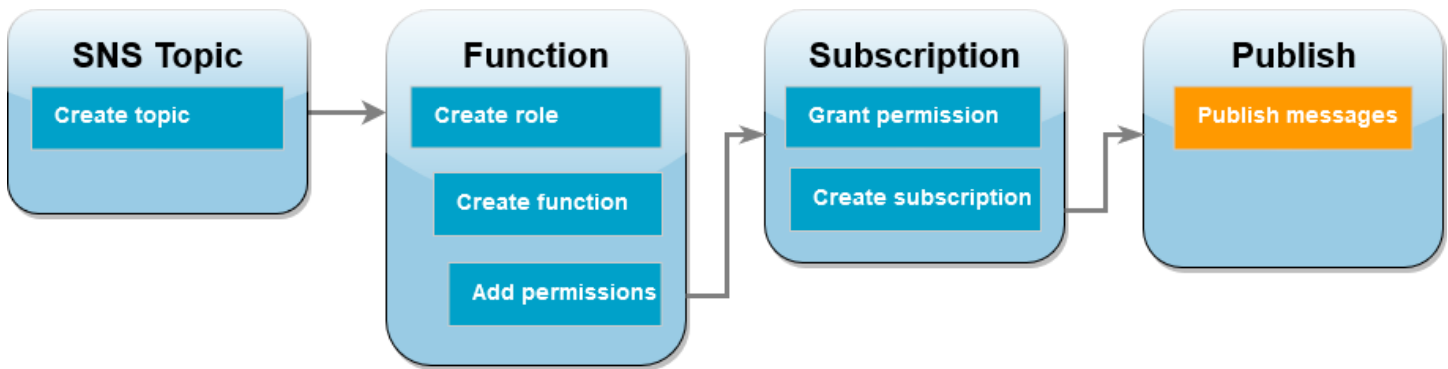
- Di akun B, jalankan AWS CLI perintah berikut. Gunakan wilayah default tempat Anda membuat topik dan ARNs untuk topik dan fungsi Lambda Anda.

```
aws sns subscribe --protocol lambda \
  --region us-east-1 \
  --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
  --notification-endpoint arn:aws:lambda:us-
east-1:<AccountB_ID>:function:Function-With-SNS \
  --profile accountB
```

Anda akan melihat output seperti yang berikut ini.

```
{
  "SubscriptionArn": "arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-
lambda:5d906xxxx-7c8x-45dx-a9dx-0484e31c98xx"
}
```

Publikasikan pesan ke topik (akun A dan akun B)



Sekarang fungsi Lambda Anda di akun B berlangganan SNS topik Amazon Anda di akun A, saatnya untuk menguji penyiapan Anda dengan menerbitkan pesan ke topik Anda. Untuk mengonfirmasi bahwa Amazon SNS telah memanggil fungsi Lambda Anda, Anda CloudWatch menggunakan Log untuk melihat output fungsi Anda.

Untuk memublikasikan pesan ke topik Anda dan melihat output fungsi Anda

1. Masukkan `Hello World` ke dalam file teks dan simpan sebagai `message.txt`.
2. Dari direktori yang sama tempat Anda menyimpan file teks Anda, jalankan AWS CLI perintah berikut di akun A. Gunakan ARN untuk topik Anda sendiri.

```
aws sns publish --message file://message.txt --subject Test \
  --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
  --profile accountA
```

Ini akan mengembalikan ID pesan dengan pengidentifikasi unik, yang menunjukkan bahwa Amazon SNS telah menerima pesan tersebut. Amazon SNS kemudian mencoba menyampaikan pesan ke pelanggan topik. Untuk mengonfirmasi bahwa Amazon SNS telah memanggil fungsi Lambda Anda, CloudWatch gunakan Log untuk melihat output fungsi Anda:

3. Di akun B, buka halaman [Grup log](#) di CloudWatch konsol Amazon.
4. Pilih grup log untuk fungsi Anda (`/aws/lambda/Function-With-SNS`).
5. Pilih aliran log terbaru.
6. Jika fungsi Anda dipanggil dengan benar, Anda akan melihat output yang mirip dengan berikut yang menunjukkan konten pesan yang Anda terbitkan ke topik Anda.

```
2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO Processed
message Hello World
```



```
2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO done
```

Bersihkan sumber daya Anda

Sekarang Anda dapat menghapus sumber daya yang Anda buat untuk tutorial ini, kecuali Anda ingin mempertahankannya. Dengan menghapus AWS sumber daya yang tidak lagi Anda gunakan, Anda mencegah tagihan yang tidak perlu ke Anda Akun AWS.

Di Akun A, bersihkan SNS topik Amazon Anda.

Untuk menghapus SNS topik Amazon

1. Buka [halaman Topik](#) SNS konsol Amazon.
2. Pilih topik yang Anda buat.
3. Pilih Hapus.
4. Masukkan **delete me** di bidang input teks.
5. Pilih Hapus.

Di Akun B, bersihkan peran eksekusi, fungsi Lambda, dan langganan AmazonSNS.

Untuk menghapus peran eksekusi

1. Buka [halaman Peran](#) IAM konsol.
2. Pilih peran eksekusi yang Anda buat.
3. Pilih Hapus.
4. Masukkan nama peran di bidang input teks dan pilih Hapus.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Untuk menghapus SNS langganan Amazon

1. Buka [halaman Langganan](#) SNS konsol Amazon.
2. Pilih langganan yang Anda buat.
3. Pilih Delete, Delete.

Mengelola izin di AWS Lambda

Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk mengelola izin di AWS Lambda. Ada dua kategori utama izin yang perlu Anda pertimbangkan saat bekerja dengan fungsi Lambda:

- Izin yang diperlukan fungsi Lambda Anda untuk API melakukan tindakan dan mengakses sumber daya lain AWS
- Izin yang dibutuhkan AWS pengguna dan entitas lain untuk mengakses fungsi Lambda Anda

Fungsi Lambda sering perlu mengakses AWS sumber daya lain, dan melakukan berbagai API operasi pada sumber daya tersebut. Misalnya, Anda mungkin memiliki fungsi Lambda yang merespons peristiwa dengan memperbarui entri dalam database Amazon DynamoDB. Dalam hal ini, fungsi Anda memerlukan izin untuk mengakses database, serta izin untuk menempatkan atau memperbarui item dalam database tersebut.

Anda menentukan izin yang dibutuhkan fungsi Lambda Anda dalam peran IAM khusus yang disebut [peran](#) eksekusi. Dalam peran ini, Anda dapat melampirkan kebijakan yang menentukan setiap izin yang diperlukan fungsi untuk mengakses AWS sumber daya lain, dan membaca dari sumber peristiwa. Setiap fungsi Lambda harus memiliki peran eksekusi. Minimal, peran eksekusi Anda harus memiliki akses ke Amazon CloudWatch karena fungsi Lambda masuk ke Log secara CloudWatch default. Anda dapat melampirkan [kebijakan AWSLambdaBasicExecutionRole terkelola](#) ke peran eksekusi Anda untuk memenuhi persyaratan ini.

Untuk memberikan izin lain Akun AWS, organisasi, dan layanan untuk mengakses sumber daya Lambda Anda, Anda memiliki beberapa opsi:

- Anda dapat menggunakan [kebijakan berbasis identitas](#) untuk memberi pengguna lain akses ke sumber daya Lambda Anda. Kebijakan berbasis identitas dapat berlaku untuk pengguna secara langsung, atau untuk kelompok dan peran yang terkait dengan pengguna.
- Anda dapat menggunakan [kebijakan berbasis sumber daya](#) untuk memberikan izin akun dan AWS layanan lain untuk mengakses sumber daya Lambda Anda. Saat pengguna mencoba mengakses sumber daya Lambda, Lambda mempertimbangkan kebijakan berbasis identitas pengguna dan kebijakan berbasis sumber daya. Saat AWS layanan seperti Amazon Simple Storage Service (Amazon S3) memanggil fungsi Lambda Anda, Lambda hanya mempertimbangkan kebijakan berbasis sumber daya.

- Anda dapat menggunakan model [access control \(ABAC\) berbasis atribut untuk mengontrol akses](#) ke fungsi Lambda Anda. Dengan ABAC, Anda dapat melampirkan tag ke fungsi Lambda, meneruskannya dalam API permintaan tertentu, atau melampirkannya ke IAM kepala sekolah yang membuat permintaan. Tentukan tag yang sama dalam elemen kondisi IAM kebijakan untuk mengontrol akses fungsi.

Di AWS, ini adalah praktik terbaik untuk hanya memberikan izin yang diperlukan untuk melakukan tugas (izin hak istimewa paling sedikit). Untuk menerapkan ini di Lambda, kami sarankan memulai dengan kebijakan [AWS terkelola](#). Anda dapat menggunakan kebijakan terkelola ini apa adanya, atau sebagai titik awal untuk menulis kebijakan Anda sendiri yang lebih ketat.

Untuk membantu Anda menyempurnakan izin untuk akses hak istimewa paling sedikit, Lambda menyediakan beberapa ketentuan tambahan yang dapat Anda sertakan dalam kebijakan Anda. Untuk informasi selengkapnya, lihat [the section called “Sumber Daya dan Kondisi”](#).

Untuk informasi selengkapnya IAM, lihat [Panduan IAM Pengguna](#).

Mendefinisikan izin fungsi Lambda dengan peran eksekusi

Peran eksekusi fungsi Lambda adalah peran AWS Identity and Access Management (IAM) yang memberikan izin fungsi untuk mengakses AWS layanan dan sumber daya. Misalnya, Anda dapat membuat peran eksekusi yang memiliki izin untuk mengirim log ke Amazon CloudWatch dan mengunggah data pelacakan AWS X-Ray. Halaman ini memberikan informasi tentang cara membuat, melihat, dan mengelola peran eksekusi fungsi Lambda.

Lambda secara otomatis mengasumsikan peran eksekusi Anda ketika Anda memanggil fungsi Anda. Anda harus menghindari panggilan manual `sts:AssumeRole` untuk mengambil peran eksekusi dalam kode fungsi Anda. Jika kasus penggunaan Anda mengharuskan peran tersebut mengasumsikan dirinya sendiri, Anda harus memasukkan peran itu sendiri sebagai prinsipal tepercaya dalam kebijakan kepercayaan peran Anda. Untuk informasi selengkapnya tentang cara mengubah kebijakan kepercayaan peran, lihat [Memodifikasi kebijakan kepercayaan peran \(konsol\)](#) di Panduan IAM Pengguna.

Agar Lambda dapat mengambil peran eksekusi Anda dengan benar, [kebijakan kepercayaan](#) peran harus menentukan prinsip layanan Lambda (`lambda.amazonaws.com`) sebagai layanan tepercaya.

Topik

- [Membuat peran eksekusi di IAM konsol](#)
- [Menciptakan dan mengelola peran dengan AWS CLI](#)
- [Berikan akses hak istimewa paling rendah ke peran eksekusi Lambda Anda](#)
- [Melihat dan memperbarui izin dalam peran eksekusi](#)
- [Bekerja dengan kebijakan AWS terkelola dalam peran eksekusi](#)
- [Menggunakan fungsi sumber ARN untuk mengontrol perilaku akses fungsi](#)

Membuat peran eksekusi di IAM konsol

Secara default, Lambda membuat peran eksekusi dengan izin minimal saat Anda [membuat fungsi di konsol Lambda](#). Secara khusus, peran eksekusi ini mencakup [kebijakan AWSLambdaBasicExecutionRole terkelola](#), yang memberikan izin dasar fungsi Anda untuk mencatat peristiwa ke Amazon CloudWatch Logs.

Fungsi Anda biasanya memerlukan izin tambahan untuk melakukan tugas yang lebih bermakna. Misalnya, Anda mungkin memiliki fungsi Lambda yang merespons peristiwa dengan memperbarui

entri dalam database Amazon DynamoDB. Anda dapat membuat peran eksekusi dengan izin yang diperlukan menggunakan IAM konsol.

Untuk membuat peran eksekusi di IAM konsol

1. Buka [halaman Peran](#) di IAM konsol.
2. Pilih Buat peran.
3. Di bawah Jenis entitas tepercaya, pilih AWS layanan.
4. Di bawah Kasus penggunaan, pilih Lambda.
5. Pilih Berikutnya.
6. Pilih kebijakan AWS terkelola yang ingin dilampirkan ke peran Anda. Misalnya, jika fungsi Anda perlu mengakses DynamoDB, pilih `AWSLambdaDynamoDBExecutionRole` kebijakan terkelola.
7. Pilih Berikutnya.
8. Masukkan nama Peran lalu pilih Buat peran.

Untuk petunjuk mendetail, lihat [Membuat peran untuk AWS layanan \(konsol\)](#) di Panduan IAM Pengguna.

Setelah Anda membuat peran eksekusi, lampirkan ke fungsi Anda. Saat Anda [membuat fungsi di konsol Lambda](#), Anda dapat melampirkan peran eksekusi apa pun yang sebelumnya Anda buat ke fungsi tersebut. Jika Anda ingin melampirkan peran eksekusi baru ke fungsi yang ada, ikuti langkah-langkahnya [the section called “Memperbarui peran eksekusi fungsi”](#).

Menciptakan dan mengelola peran dengan AWS CLI

Untuk membuat peran eksekusi dengan AWS Command Line Interface (AWS CLI), gunakan `create-role` perintah. Saat menggunakan perintah ini, Anda dapat menentukan kebijakan kepercayaan sebaris. Kebijakan kepercayaan peran memberikan izin kepada prinsipal yang ditentukan untuk mengambil peran tersebut. Dalam contoh berikut, Anda memberikan izin kepada kepala layanan Lambda untuk mengambil peran Anda. Perhatikan bahwa persyaratan untuk menghindari tanda kutip dalam JSON string dapat bervariasi tergantung pada shell Anda.

```
aws iam create-role \  
  --role-name lambda-ex \  
  --assume-role-policy-document '{"Version": "2012-10-17", "Statement":  
  [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action":  
  "sts:AssumeRole"}]}'
```

Anda juga dapat menentukan kebijakan kepercayaan untuk peran tersebut menggunakan JSON file terpisah. Dalam contoh berikut, `trust-policy.json` adalah file dalam direktori saat ini.

Example trust-policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
aws iam create-role \
  --role-name lambda-ex \
  --assume-role-policy-document file://trust-policy.json
```

Anda akan melihat output berikut:

```
{
  "Role": {
    "Path": "/",
    "RoleName": "lambda-ex",
    "RoleId": "AROAQFOXMPL6TZ6ITKWND",
    "Arn": "arn:aws:iam::123456789012:role/lambda-ex",
    "CreateDate": "2020-01-17T23:19:12Z",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "lambda.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

```
    }  
  }  
}
```

Untuk menambahkan izin peran, gunakan perintah `attach-policy-to-role`. Perintah berikut menambahkan kebijakan `AWSLambdaBasicExecutionRole` terkelola ke peran `lambda-ex` eksekusi.

```
aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/  
service-role/AWSLambdaBasicExecutionRole
```

Setelah Anda membuat peran eksekusi, lampirkan ke fungsi Anda. Saat Anda [membuat fungsi di konsol Lambda](#), Anda dapat melampirkan peran eksekusi apa pun yang sebelumnya Anda buat ke fungsi tersebut. Jika Anda ingin melampirkan peran eksekusi baru ke fungsi yang ada, ikuti langkah-langkahnya [the section called “Memperbarui peran eksekusi fungsi”](#).

Berikan akses hak istimewa paling rendah ke peran eksekusi Lambda Anda

Saat pertama kali membuat IAM peran untuk fungsi Lambda selama fase pengembangan, terkadang Anda dapat memberikan izin di luar yang diperlukan. Sebelum memublikasikan fungsi Anda di lingkungan produksi, sebagai praktik terbaik, sesuaikan kebijakan agar hanya menyertakan izin yang diperlukan. Untuk informasi selengkapnya, lihat [Menerapkan izin hak istimewa paling sedikit](#) di Panduan Pengguna. IAM

Gunakan IAM Access Analyzer untuk membantu mengidentifikasi izin yang diperlukan untuk kebijakan peran IAM eksekusi. IAM Access Analyzer meninjau AWS CloudTrail log Anda selama rentang tanggal yang Anda tentukan dan membuat templat kebijakan hanya dengan izin yang digunakan fungsi selama waktu tersebut. Anda dapat menggunakan templat untuk membuat kebijakan terkelola dengan izin berbutir halus, lalu melampirkannya ke peran. IAM Dengan begitu, Anda hanya memberikan izin yang diperlukan peran untuk berinteraksi dengan AWS sumber daya untuk kasus penggunaan spesifik Anda.

Untuk informasi selengkapnya, lihat [Menghasilkan kebijakan berdasarkan aktivitas akses](#) di Panduan IAM Pengguna.

Melihat dan memperbarui izin dalam peran eksekusi

Topik ini mencakup bagaimana Anda dapat melihat dan memperbarui [peran eksekusi](#) fungsi Anda.

Topik

- [Melihat peran eksekusi fungsi](#)
- [Memperbarui peran eksekusi fungsi](#)

Melihat peran eksekusi fungsi

Untuk melihat peran eksekusi fungsi, gunakan konsol Lambda.

Untuk melihat peran eksekusi fungsi (konsol)

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih Konfigurasi, lalu pilih Izin.
4. Di bawah Peran eksekusi, Anda dapat melihat peran yang saat ini digunakan sebagai peran eksekusi fungsi. Untuk kenyamanan, Anda dapat melihat semua sumber daya dan tindakan yang dapat diakses fungsi di bawah bagian Ringkasan sumber daya. Anda juga dapat memilih layanan dari daftar dropdown untuk melihat semua izin yang terkait dengan layanan tersebut.

Memperbarui peran eksekusi fungsi

Anda dapat menambahkan atau menghapus izin dari peran eksekusi fungsi kapan saja, atau mengonfigurasi fungsi Anda untuk menggunakan peran yang berbeda. Jika fungsi Anda memerlukan akses ke layanan atau sumber daya lain, Anda harus menambahkan izin yang diperlukan ke peran eksekusi.

Saat Anda menambahkan izin ke fungsi Anda, lakukan pembaruan sepele ke kode atau konfigurasinya juga. Ini memaksa instance menjalankan fungsi Anda, yang memiliki kredensialnya yang sudah ketinggalan zaman, untuk berhenti dan diganti.

Untuk memperbarui peran eksekusi fungsi, Anda dapat menggunakan konsol Lambda.

Untuk memperbarui peran eksekusi fungsi (konsol)

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih nama sebuah fungsi.
3. Pilih Konfigurasi, lalu pilih Izin.
4. Di bawah Peran eksekusi, pilih Edit.

5. Jika Anda ingin memperbarui fungsi Anda untuk menggunakan peran yang berbeda sebagai peran eksekusi, pilih peran baru di menu tarik-turun di bawah Peran yang ada.

 Note

Jika Anda ingin memperbarui izin dalam peran eksekusi yang ada, Anda hanya dapat melakukannya di konsol AWS Identity and Access Management (IAM).

Jika Anda ingin membuat peran baru untuk digunakan sebagai peran eksekusi, pilih Buat peran baru dari templat AWS kebijakan di bawah Peran eksekusi. Kemudian, masukkan nama untuk peran baru Anda di bawah Nama peran, dan tentukan kebijakan apa pun yang ingin Anda lampirkan ke peran baru di bawah Templat kebijakan.

6. Pilih Simpan.

Bekerja dengan kebijakan AWS terkelola dalam peran eksekusi

Kebijakan AWS terkelola berikut memberikan izin yang diperlukan untuk menggunakan fitur Lambda.

| Perubahan | Deskripsi | Tanggal |
|--|---|------------------|
| AWSLambdaMSKExecutionRole — Lambda menambahkan izin kafka:DescribeCluster V2 ke kebijakan ini. | AWSLambdaMSKExecutionRole memberikan izin untuk membaca dan mengakses catatan dari kluster Amazon Managed Streaming for Apache Kafka (Amazon MSK), mengelola antarmuka jaringan elastis (ENI), dan menulis ke Log. CloudWatch | Juni 17, 2022 |
| AWSLambdaBasicExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaBasicExecutionRole memberikan izin untuk mengunggah log ke CloudWatch | 14 Februari 2022 |

| Perubahan | Deskripsi | Tanggal |
|---|---|------------------|
| AWSLambdaDynamoDBExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaDynamoDBExecutionRole memberikan izin untuk membaca catatan dari aliran Amazon DynamoDB dan menulis ke Log. CloudWatch | 14 Februari 2022 |
| AWSLambdaKinesisExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaKinesisExecutionRole memberikan izin untuk membaca peristiwa dari aliran data Amazon Kinesis dan menulis ke Log. CloudWatch | 14 Februari 2022 |
| AWSLambdaMSKExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaMSKExecutionRole memberikan izin untuk membaca dan mengakses catatan dari kluster Amazon Managed Streaming for Apache Kafka (Amazon MSK), mengelola antarmuka jaringan elastis (ENI), dan menulis ke Log. CloudWatch | 14 Februari 2022 |
| AWSLambdaSQSQueueExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaSQSQueueExecutionRole memberikan izin untuk membaca pesan dari antrian Amazon Simple Queue Service (Amazon SQS) dan menulis ke Log. CloudWatch | 14 Februari 2022 |

| Perubahan | Deskripsi | Tanggal |
|---|---|------------------|
| AWSLambdaVPCAccess ExecutionRole — Lambda mulai melacak perubahan pada kebijakan ini. | AWSLambdaVPCAccess Execution Role memberikan izin untuk mengelola ENI dalam VPC Amazon dan menulis ke Log. CloudWatch | 14 Februari 2022 |
| AWSXRayDaemonWrite Access — Lambda mulai melacak perubahan pada kebijakan ini. | AWSXRayDaemonWrite Access memberikan izin untuk mengunggah data jejak ke X-Ray. | 14 Februari 2022 |
| CloudWatchLambdaInsightsExecutionRolePolicy — Lambda mulai melacak perubahan pada kebijakan ini. | CloudWatchLambdaInsightsExecutionRolePolicy memberikan izin untuk menulis metrik runtime ke Lambda Insights. CloudWatch | 14 Februari 2022 |
| Kebijakan AmazonS3 ObjectLambda Execution Role - Lambda mulai melacak perubahan pada kebijakan ini. | AmazonS3ObjectLambdaExecutionRolePolicy memberikan izin untuk berinteraksi dengan objek Amazon Simple Storage Service (Amazon S3) Lambda dan menulis ke Log. CloudWatch | 14 Februari 2022 |

Untuk beberapa fitur, konsol Lambda mencoba menambahkan izin yang hilang ke peran eksekusi Anda dalam kebijakan yang dikelola pelanggan. Kebijakan ini dapat menjadi beberapa. Untuk menghindari pembuatan kebijakan tambahan, tambahkan kebijakan yang dikelola AWS yang relevan ke peran eksekusi Anda sebelum mengaktifkan fitur.

Saat Anda menggunakan [pemetaan sumber peristiwa](#) untuk mengaktifkan fungsi Anda, Lambda menggunakan peran eksekusi untuk membaca data peristiwa. Misalnya, pemetaan sumber peristiwa

untuk Kinesis membaca peristiwa dari aliran data dan mengirimnya ke fungsi Anda dalam beberapa batch.

Saat layanan mengambil peran di akun Anda, Anda dapat menyertakan kunci konteks kondisi `aws:SourceArn` global `aws:SourceAccount` dan global dalam kebijakan kepercayaan peran untuk membatasi akses ke peran hanya pada permintaan yang dihasilkan oleh sumber daya yang diharapkan. Untuk informasi lebih lanjut, lihat [Pencegahan wakil kebingungan lintas layanan untuk AWS Security Token Service](#).

Selain kebijakan AWS terkelola, konsol Lambda menyediakan templat untuk membuat kebijakan khusus dengan izin untuk kasus penggunaan tambahan. Saat Anda membuat fungsi di konsol Lambda, Anda dapat memilih untuk membuat peran eksekusi baru dengan izin dari satu templat atau lebih. Templat ini juga diterapkan secara otomatis ketika Anda membuat fungsi dari cetak biru, atau ketika Anda mengonfigurasi opsi yang memerlukan akses ke layanan lain. Contoh templat tersedia di [GitHubrepositori](#) panduan ini.

Menggunakan fungsi sumber ARN untuk mengontrol perilaku akses fungsi

Biasanya kode fungsi Lambda Anda membuat permintaan API ke layanan lain AWS . Untuk membuat permintaan ini, Lambda menghasilkan seperangkat kredensial singkat dengan mengasumsikan peran eksekusi fungsi Anda. Kredensial ini tersedia sebagai variabel lingkungan selama pemanggilan fungsi Anda. Saat bekerja dengan AWS SDK, Anda tidak perlu memberikan kredensial untuk SDK secara langsung dalam kode. Secara default, rantai penyedia kredensial secara berurutan memeriksa setiap tempat di mana Anda dapat menyetel kredensial dan memilih yang pertama tersedia—biasanya variabel lingkungan (`AWSCredentialsProviderChain`, `AWSCredentialsProviderChain`, dan `AWSCredentialsProviderChain`). `AWSCredentialsProviderChain` `AWSCredentialsProviderChain` `AWSCredentialsProviderChain`

Lambda menyuntikkan ARN fungsi sumber ke dalam konteks kredensial jika permintaan tersebut adalah permintaan AWS API yang berasal dari dalam lingkungan eksekusi Anda. Lambda juga menyuntikkan ARN fungsi sumber untuk AWS permintaan API berikut yang dibuat Lambda atas nama Anda di luar lingkungan eksekusi Anda:

| Layanan | Tindakan | Alasan |
|----------------|--|--|
| CloudWatch Log | <code>CreateLogGroup</code> , <code>CreateLogStream</code> , <code>PutLogEvents</code> | Untuk menyimpan log ke dalam grup CloudWatch log Log |

| Layanan | Tindakan | Alasan |
|------------|------------------|--|
| X-Ray | PutTraceSegments | Untuk mengirim data jejak ke X-Ray |
| Amazon EFS | ClientMount | Untuk menghubungkan fungsi Anda ke sistem file Amazon Elastic File System (Amazon EFS) |

Panggilan AWS API lain yang dilakukan Lambda di luar lingkungan eksekusi Anda atas nama Anda menggunakan peran eksekusi yang sama tidak mengandung ARN fungsi sumber. Contoh panggilan API tersebut di luar lingkungan eksekusi meliputi:

- Panggilan ke AWS Key Management Service (AWS KMS) untuk mengenkripsi dan mendekripsi variabel lingkungan Anda secara otomatis.
- Panggilan ke Amazon Elastic Compute Cloud (Amazon EC2) untuk membuat antarmuka jaringan elastis (ENI) untuk fungsi berkemampuan VPC.
- [Panggilan ke AWS layanan, seperti Amazon Simple Queue Service \(Amazon SQS\), untuk membaca dari sumber peristiwa yang disiapkan sebagai pemetaan sumber peristiwa.](#)

Dengan fungsi sumber ARN dalam konteks kredensial, Anda dapat memverifikasi apakah panggilan ke sumber daya Anda berasal dari kode fungsi Lambda tertentu. Untuk memverifikasi ini, gunakan kunci `lambda:SourceFunctionArn` kondisi dalam kebijakan berbasis identitas IAM atau [kebijakan kontrol layanan](#) (SCP).

Note

Anda tidak dapat menggunakan kunci `lambda:SourceFunctionArn` kondisi dalam kebijakan berbasis sumber daya.

Dengan kunci kondisi ini dalam kebijakan berbasis identitas atau SCP, Anda dapat menerapkan kontrol keamanan untuk tindakan API yang dibuat kode fungsi Anda ke layanan lain. AWS Ini memiliki beberapa aplikasi keamanan utama, seperti membantu Anda mengidentifikasi sumber kebocoran kredensial.

Note

Kunci `lambda:SourceFunctionArn` kondisi berbeda dari tombol `lambda:FunctionArn` dan `aws:SourceArn` kondisi. Kunci `lambda:FunctionArn` kondisi hanya berlaku untuk [pemetaan sumber peristiwa](#) dan membantu menentukan fungsi mana yang dapat dipanggil sumber acara Anda. Kunci `aws:SourceArn` kondisi hanya berlaku untuk kebijakan di mana fungsi Lambda Anda adalah sumber daya target, dan membantu menentukan AWS layanan dan sumber daya lain mana yang dapat menjalankan fungsi tersebut. Kunci `lambda:SourceFunctionArn` kondisi dapat diterapkan pada kebijakan berbasis identitas atau SCP apa pun untuk menentukan fungsi Lambda tertentu yang memiliki izin untuk melakukan panggilan API tertentu ke sumber daya lain. AWS

Untuk digunakan `lambda:SourceFunctionArn` dalam polis Anda, sertakan sebagai syarat dengan salah satu operator [kondisi ARN](#). Nilai kunci harus berupa ARN yang valid.

Misalnya, misalkan kode fungsi Lambda Anda membuat `s3:PutObject` panggilan yang menargetkan bucket Amazon S3 tertentu. Anda mungkin ingin mengizinkan hanya satu fungsi Lambda tertentu untuk `s3:PutObject` mengakses bucket itu. Dalam hal ini, peran eksekusi fungsi Anda harus memiliki kebijakan yang dilampirkan yang terlihat seperti ini:

Example kebijakan yang memberikan akses fungsi Lambda tertentu ke sumber daya Amazon S3

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleSourceFunctionArn",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::lambda_bucket/*",
      "Condition": {
        "ArnEquals": {
          "lambda:SourceFunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:source_lambda"
        }
      }
    }
  ]
}
```

Kebijakan ini hanya mengizinkan `s3:PutObject` akses jika sumbernya adalah fungsi Lambda dengan ARN. `arn:aws:lambda:us-east-1:123456789012:function:source_lambda` Kebijakan ini tidak mengizinkan `s3:PutObject` akses ke identitas panggilan lainnya. Ini benar bahkan jika fungsi atau entitas yang berbeda membuat `s3:PutObject` panggilan dengan peran eksekusi yang sama.

Note

Kunci `lambda:SourceFunctionARN` kondisi tidak mendukung versi fungsi Lambda atau alias fungsi. Jika Anda menggunakan ARN untuk versi atau alias fungsi tertentu, fungsi Anda tidak akan memiliki izin untuk mengambil tindakan yang Anda tentukan. Pastikan untuk menggunakan ARN yang tidak memenuhi syarat untuk fungsi Anda tanpa versi atau akhiran alias.

Anda juga dapat menggunakannya `lambda:SourceFunctionArn` di SCP. Misalnya, Anda ingin membatasi akses ke bucket ke kode fungsi Lambda tunggal atau panggilan dari Amazon Virtual Private Cloud (VPC) tertentu. SCP berikut menggambarkan hal ini.

Example kebijakan yang menolak akses ke Amazon S3 dalam kondisi tertentu

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:*"
      ],
      "Resource": "arn:aws:s3:::lambda_bucket/*",
      "Effect": "Deny",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": [
            "vpc-12345678"
          ]
        }
      }
    },
    {
      "Action": [
        "s3:*"
      ]
    }
  ]
}
```



```
    ],
    "Resource": "arn:aws:s3:::lambda_bucket/*",
    "Effect": "Deny",
    "Condition": {
      "ArnNotEqualsIfExists": {
        "lambda:SourceFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:source_lambda"
      }
    }
  ]
}
```

Kebijakan ini menolak semua tindakan S3 kecuali berasal dari fungsi Lambda tertentu dengan ARN `arn:aws:lambda:*:123456789012:function:source_lambda`, atau kecuali berasal dari VPC yang ditentukan. `StringNotEqualsIfExistsOperator` memberitahu IAM untuk memproses kondisi ini hanya jika `aws:SourceVpc` kunci ada dalam permintaan. Demikian pula, IAM menganggap `ArnNotEqualsIfExists` operator hanya jika `lambda:SourceFunctionArn` ada.

Memberikan AWS entitas lain akses ke fungsi Lambda Anda

Untuk memberikan izin lain Akun AWS, organisasi, dan layanan untuk mengakses sumber daya Lambda Anda, Anda memiliki beberapa opsi:

- Anda dapat menggunakan [kebijakan berbasis identitas](#) untuk memberi pengguna lain akses ke sumber daya Lambda Anda. Kebijakan berbasis identitas dapat berlaku untuk pengguna secara langsung, atau untuk kelompok dan peran yang terkait dengan pengguna.
- Anda dapat menggunakan [kebijakan berbasis sumber daya](#) untuk memberikan izin akun dan AWS layanan lain untuk mengakses sumber daya Lambda Anda. Saat pengguna mencoba mengakses sumber daya Lambda, Lambda mempertimbangkan kebijakan berbasis identitas pengguna dan kebijakan berbasis sumber daya. Saat AWS layanan seperti Amazon Simple Storage Service (Amazon S3) memanggil fungsi Lambda Anda, Lambda hanya mempertimbangkan kebijakan berbasis sumber daya.
- Anda dapat menggunakan model [access control \(ABAC\) berbasis atribut untuk mengontrol akses](#) ke fungsi Lambda Anda. Dengan ABAC, Anda dapat melampirkan tag ke fungsi Lambda, meneruskannya dalam API permintaan tertentu, atau melampirkannya ke IAM kepala sekolah yang membuat permintaan. Tentukan tag yang sama dalam elemen kondisi IAM kebijakan untuk mengontrol akses fungsi.

Untuk membantu Anda menyempurnakan izin untuk akses hak istimewa paling sedikit, Lambda menyediakan beberapa ketentuan tambahan yang dapat Anda sertakan dalam kebijakan Anda. Untuk informasi selengkapnya, lihat [the section called “Sumber Daya dan Kondisi”](#).

Kebijakan berbasis identitas IAM untuk Lambda

Anda dapat menggunakan kebijakan berbasis identitas di AWS Identity and Access Management (IAM) untuk memberikan pengguna di akun Anda akses ke Lambda. Kebijakan berbasis identitas dapat diterapkan pada pengguna, grup pengguna, atau peran. Anda juga dapat memberi pengguna di akun lain izin untuk berperan di akun Anda dan mengakses sumber daya Lambda Anda.

Lambda menyediakan kebijakan AWS terkelola yang memberikan akses ke API tindakan Lambda dan, dalam beberapa kasus, akses ke AWS layanan lain yang digunakan untuk mengembangkan dan mengelola sumber daya Lambda. Lambda memperbarui kebijakan terkelola ini sesuai kebutuhan, untuk memastikan bahwa pengguna Anda memiliki akses ke fitur baru ketika dirilis.

- [AWSLambda_FullAccess](#) — Memberikan akses penuh ke tindakan Lambda dan layanan AWS lain yang digunakan untuk mengembangkan dan memelihara sumber daya Lambda.
- [AWSLambda_ReadOnlyAccess](#) — Memberikan akses hanya-baca ke sumber daya Lambda.
- [AWSLambdaRole](#)— Memberikan izin untuk memanggil fungsi Lambda.

AWS kebijakan terkelola memberikan izin untuk API tindakan tanpa membatasi fungsi atau lapisan Lambda yang dapat dimodifikasi pengguna. Untuk kontrol yang lebih cermat, Anda dapat membuat kebijakan Anda sendiri yang membatasi ruang lingkup izin pengguna.

Topik

- [Memberikan pengguna akses ke fungsi Lambda](#)
- [Memberikan pengguna akses ke lapisan Lambda](#)

Memberikan pengguna akses ke fungsi Lambda

Gunakan [kebijakan berbasis identitas](#) untuk mengizinkan pengguna, grup pengguna, atau peran menjalankan operasi pada fungsi Lambda.

Note

Untuk fungsi yang didefinisikan sebagai gambar kontainer, izin pengguna untuk mengakses gambar harus dikonfigurasi di Amazon Elastic Container Registry (Amazon ECR). Sebagai contoh, lihat Kebijakan [ECR repositori Amazon](#).

Berikut ini adalah contoh kebijakan izin dengan lingkup terbatas. Ini memungkinkan pengguna membuat dan mengelola fungsi Lambda yang diberi nama dengan awalan yang ditentukan (`intern-`), dan dikonfigurasi dengan peran eksekusi yang ditunjuk.

Example Kebijakan pengembangan fungsi

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
```

```

        "lambda:GetAccountSettings",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda>ListEventSourceMappings",
        "lambda>ListFunctions",
        "lambda>ListTags",
        "iam>ListRoles"
    ],
    "Resource": "*"
},
{
    "Sid": "DevelopFunctions",
    "Effect": "Allow",
    "NotAction": [
        "lambda:AddPermission",
        "lambda:PutFunctionConcurrency"
    ],
    "Resource": "arn:aws:lambda:*:*:function:intern-*"
},
{
    "Sid": "DevelopEventSourceMappings",
    "Effect": "Allow",
    "Action": [
        "lambda>DeleteEventSourceMapping",
        "lambda:UpdateEventSourceMapping",
        "lambda>CreateEventSourceMapping"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
        }
    }
},
{
    "Sid": "PassExecutionRole",
    "Effect": "Allow",
    "Action": [
        "iam>ListRolePolicies",
        "iam>ListAttachedRolePolicies",
        "iam:GetRole",

```

```

        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource": "arn:aws:iam::*:role/intern-lambda-execution-role"
},
{
    "Sid": "ViewLogs",
    "Effect": "Allow",
    "Action": [
        "logs:*"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*"
}
]
}

```

Izin dalam kebijakan disusun menjadi pernyataan berdasarkan [sumber daya dan kondisi](#) yang mereka dukung.

- `ReadOnlyPermissions` – Konsol Lambda menggunakan izin ini saat Anda menelusuri dan melihat fungsi. Mereka tidak mendukung pola atau kondisi sumber daya.

```

    "Action": [
        "lambda:GetAccountSettings",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda>ListEventSourceMappings",
        "lambda>ListFunctions",
        "lambda>ListTags",
        "iam>ListRoles"
    ],
    "Resource": "*"

```

- `DevelopFunctions`— Gunakan tindakan Lambda apa pun yang beroperasi pada fungsi yang diawali dengan `intern-`, kecuali `dan`. `AddPermission` `PutFunctionConcurrency` `AddPermission` memodifikasi [kebijakan berbasis sumber daya](#) pada fungsi dan dapat memiliki

implikasi keamanan. `PutFunctionConcurrency` cadangan kapasitas penskalaan untuk suatu fungsi dan dapat mengambil kapasitas dari fungsi lain.

```
"NotAction": [
    "lambda:AddPermission",
    "lambda:PutFunctionConcurrency"
],
"Resource": "arn:aws:lambda:*:*:function:intern-*
```

- `DevelopEventSourceMappings` – Mengelola pemetaan sumber peristiwa pada fungsi yang diawali dengan `intern-`. Tindakan ini beroperasi pada pemetaan sumber peristiwa, tetapi Anda dapat membatasinya menurut fungsi dengan syarat.

```
"Action": [
    "lambda:DeleteEventSourceMapping",
    "lambda:UpdateEventSourceMapping",
    "lambda>CreateEventSourceMapping"
],
"Resource": "*",
"Condition": {
    "StringLike": {
        "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
    }
}
```

- `PassExecutionRole`— Lihat dan berikan hanya peran bernama `intern-lambda-execution-role`, yang harus dibuat dan dikelola oleh pengguna dengan IAM izin. `PassRole` digunakan ketika Anda menetapkan peran eksekusi ke fungsi.

```
"Action": [
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:PassRole",
    "iam:SimulatePrincipalPolicy"
],
"Resource": "arn:aws:iam:*:*:role/intern-lambda-execution-role"
```

- **ViewLogs**— Gunakan CloudWatch Log untuk melihat log untuk fungsi yang diawali dengan `intern-`.

```
"Action": [
  "logs:*"
],
"Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*
```

Kebijakan ini memungkinkan pengguna untuk memulai dengan Lambda, tanpa menempatkan sumber daya pengguna lain dalam risiko. Itu tidak memungkinkan pengguna untuk mengonfigurasi fungsi yang akan dipicu oleh atau memanggil AWS layanan lain, yang memerlukan IAM izin yang lebih luas. Ini juga tidak termasuk izin untuk layanan yang tidak mendukung kebijakan lingkup terbatas, seperti dan CloudWatch X-Ray. Gunakan kebijakan hanya-baca untuk layanan ini agar pengguna dapat mengakses data metrik dan jejak.

Saat Anda mengonfigurasi pemicu untuk fungsi Anda, Anda memerlukan akses untuk menggunakan AWS layanan yang memanggil fungsi Anda. Misalnya, untuk mengonfigurasi pemicu Amazon S3, Anda memerlukan izin untuk menggunakan tindakan Amazon S3 yang mengelola pemberitahuan bucket. Banyak dari izin ini disertakan dalam kebijakan FullAccess terkelola [AWSLambda](#).

Memberikan pengguna akses ke lapisan Lambda

Gunakan [kebijakan berbasis identitas](#) untuk memungkinkan pengguna, grup pengguna, atau peran melakukan operasi pada lapisan Lambda. Kebijakan berikut memberikan izin pengguna untuk membuat lapisan dan menggunakan mereka dengan fungsi. Pola sumber daya memungkinkan pengguna untuk bekerja di setiap Wilayah AWS dan dengan versi lapisan apa pun, selama nama lapisan dimulai dengan `test-`.

Example kebijakan pengembangan lapisan

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublishLayers",
      "Effect": "Allow",
      "Action": [
        "lambda:PublishLayerVersion"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:lambda:*:*:layer:test-*"
  },
  {
    "Sid": "ManageLayerVersions",
    "Effect": "Allow",
    "Action": [
      "lambda:GetLayerVersion",
      "lambda>DeleteLayerVersion"
    ],
    "Resource": "arn:aws:lambda:*:*:layer:test-*:*"
  }
]
}

```

Anda juga dapat menerapkan penggunaan lapisan selama pembuatan fungsi dan konfigurasi dengan kondisi `lambda:Layer`. Misalnya, Anda dapat mencegah pengguna dari menggunakan lapisan yang diterbitkan oleh akun lain. Kebijakan berikut ini menambahkan kondisi ke `CreateFunction` dan `UpdateFunctionConfiguration` tindakan untuk mewajibkan setiap lapisan yang ditentukan berasal dari akun 123456789012.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfigureFunctions",
      "Effect": "Allow",
      "Action": [
        "lambda:CreateFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringLike": {
          "lambda:Layer": [
            "arn:aws:lambda:*:123456789012:layer:*:*"
          ]
        }
      }
    }
  ]
}

```


Untuk memastikan kondisi berlaku, verifikasi bahwa tidak ada pernyataan lain yang memberikan izin pengguna atas tindakan ini.

Bekerja dengan kebijakan berbasis sumber daya di Lambda IAM

Lambda mendukung kebijakan izin berbasis sumber daya untuk fungsi dan lapisan Lambda. [Anda dapat menggunakan kebijakan berbasis sumber daya untuk memberikan akses ke AWS akun, organisasi, atau layanan lain.](#) Kebijakan berbasis sumber daya berlaku untuk satu versi fungsi, versi, alias, atau lapisan.

Console

Untuk menampilkan kebijakan fungsi berbasis sumber daya

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi, lalu pilih Izin.
4. Gulir ke bawah ke Kebijakan berbasis sumber daya, lalu pilih Lihat dokumen kebijakan. Kebijakan berbasis sumber daya menunjukkan izin yang diterapkan saat akun atau AWS layanan lain mencoba mengakses fungsi tersebut. Contoh berikut menunjukkan pernyataan yang memungkinkan Amazon S3 memicu fungsi bernama `my-function` untuk bucket bernama `amzn-s3-demo-bucket` dalam akun `123456789012`.

Example Kebijakan berbasis sumber daya

```
{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "lambda-allow-s3-my-function",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-
function",
      "Condition": {
        "StringEquals": {
```

```

        "AWS:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "AWS:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
      }
    }
  ]
}

```

AWS CLI

Untuk melihat kebijakan berbasis sumber daya dari fungsi, gunakan perintah `get-policy`.

```

aws lambda get-policy \
  --function-name my-function \
  --output text

```

Anda akan melihat output berikut:

```

{"Version":"2012-10-17","Id":"default","Statement":
[{"Sid":"sns","Effect":"Allow","Principal":
{"Service":"s3.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:us-
east-2:123456789012:function:my-function","Condition":{"ArnLike":
{"AWS:SourceArn":"arn:aws:sns:us-east-2:123456789012:lambda*"}}}]}      7c681fc9-
b791-4e91-acdf-eb847fdaa0f0

```

Untuk versi dan alias, tambahkan nomor versi atau alias di akhir nama fungsi.

```

aws lambda get-policy --function-name my-function:PROD

```

Untuk menghapus izin dari fungsi, gunakan `remove-permission`.

```

aws lambda remove-permission \
  --function-name example \
  --statement-id sns

```

Gunakan perintah `get-layer-version-policy` untuk melihat izin pada lapisan.

```

aws lambda get-layer-version-policy \

```

```
--layer-name my-layer \  
--version-number 3 \  
--output text
```

Anda akan melihat output berikut:

```
b0cd9796-d4eb-4564-939f-de7fe0b42236 {"Sid":"engineering-  
org","Effect":"Allow","Principal":"*","Action":"lambda:GetLayerVersion","Resource":"arn:aws:  
west-2:123456789012:layer:my-layer:3","Condition":{"StringEquals":  
{"aws:PrincipalOrgID":"o-t194hfs8cz"}}}
```

Gunakan `remove-layer-version-permission` untuk menghapus pernyataan dari kebijakan.

```
aws lambda remove-layer-version-permission --layer-name my-layer --version-number 3  
--statement-id engineering-org
```

API Tindakan yang didukung

API Tindakan Lambda berikut mendukung kebijakan berbasis sumber daya:

- [CreateAlias](#)
- [DeleteAlias](#)
- [DeleteFunction](#)
- [DeleteFunctionConcurrency](#)
- [DeleteFunctionEventInvokeConfig](#)
- [DeleteProvisionedConcurrencyConfig](#)
- [GetAlias](#)
- [GetFunction](#)
- [GetFunctionConcurrency](#)
- [GetFunctionConfiguration](#)
- [GetFunctionEventInvokeConfig](#)
- [GetPolicy](#)
- [GetProvisionedConcurrencyConfig](#)
- [Memohon](#)
- [ListAliases](#)

- [ListFunctionEventInvokeConfigs](#)
- [ListProvisionedConcurrencyConfigs](#)
- [ListTags](#)
- [ListVersionsByFunction](#)
- [PublishVersion](#)
- [PutFunctionConcurrency](#)
- [PutFunctionEventInvokeConfig](#)
- [PutProvisionedConcurrencyConfig](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAlias](#)
- [UpdateFunctionCode](#)
- [UpdateFunctionEventInvokeConfig](#)

Memberikan akses fungsi Lambda ke layanan AWS

Saat Anda [menggunakan AWS layanan untuk menjalankan fungsi](#), Anda memberikan izin dalam pernyataan tentang kebijakan berbasis sumber daya. Anda dapat menerapkan pernyataan ke seluruh fungsi, atau membatasi pernyataan ke satu versi atau alias.

Note

Saat Anda menambahkan pemicu ke fungsi Anda dengan konsol Lambda, konsol memperbarui kebijakan berbasis sumber daya fungsi untuk memungkinkan layanan memicunya. Untuk memberikan izin ke akun atau layanan lain yang tidak tersedia di konsol Lambda, Anda dapat menggunakan AWS CLI.

Tambahkan pernyataan dengan perintah [add-permission](#). Pernyataan kebijakan berbasis sumber daya yang paling sederhana memungkinkan layanan untuk memicu fungsi. Perintah berikut memberikan izin Amazon Simple Notification Service untuk memanggil fungsi bernama. `my-function`

```
aws lambda add-permission \
```

```
--function-name my-function \  
--action lambda:InvokeFunction \  
--statement-id sns \  
--principal sns.amazonaws.com \  
--output text
```

Anda akan melihat output berikut:

```
{"Sid":"sns","Effect":"Allow","Principal":  
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:us-  
east-2:123456789012:function:my-function"}
```

Ini memungkinkan Amazon SNS memanggil API tindakan [Invoke](#) pada fungsi, tetapi tidak membatasi SNS topik Amazon yang memicu pemanggilan. Untuk memastikan bahwa fungsi Anda hanya dipanggil oleh sumber daya tertentu, tentukan Amazon Resource Name (ARN) sumber daya dengan `source-arn` opsi. Perintah berikut hanya memungkinkan Amazon SNS untuk memanggil fungsi untuk langganan ke topik bernama `my-topic`

```
aws lambda add-permission \  
--function-name my-function \  
--action lambda:InvokeFunction \  
--statement-id sns-my-topic \  
--principal sns.amazonaws.com \  
--source-arn arn:aws:sns:us-east-2:123456789012:my-topic
```

Beberapa layanan dapat melakukan invokasi fungsi di akun lain. Jika Anda menentukan sumber ARN yang memiliki ID akun di dalamnya, itu bukan masalah. Namun, untuk Amazon S3, sumbernya adalah ember yang ARN tidak memiliki ID akun di dalamnya. Anda mungkin bisa menghapus bucket, dan akun lain dapat membuat bucket dengan nama yang sama. Gunakan opsi `source-account` dengan ID akun Anda untuk memastikan hanya sumber daya di akun Anda yang dapat melakukan invokasi fungsi.

```
aws lambda add-permission \  
--function-name my-function \  
--action lambda:InvokeFunction \  
--statement-id s3-account \  
--principal s3.amazonaws.com \  
--source-arn arn:aws:s3::amzn-s3-demo-bucket \  
--source-account 123456789012
```

Memberikan akses fungsi ke organisasi

Untuk memberikan izin ke organisasi di [AWS Organizations](#), tentukan ID organisasi sebagai `principal-org-id`. Perintah [izin tambahan](#) berikut memberikan akses pemanggilan ke semua pengguna dalam organisasi. `o-a1b2c3d4e5f`

```
aws lambda add-permission \  
  --function-name example \  
  --statement-id PrincipalOrgIDExample \  
  --action lambda:InvokeFunction \  
  --principal * \  
  --principal-org-id o-a1b2c3d4e5f
```

Note

Dalam perintah ini, `Principal` adalah `*`. Ini berarti bahwa semua pengguna di organisasi `o-a1b2c3d4e5f` mendapatkan izin pemanggilan fungsi. Jika Anda menentukan peran Akun AWS atau sebagai `Principal`, maka hanya prinsipal yang mendapatkan izin pemanggilan fungsi, tetapi hanya jika mereka juga merupakan bagian dari organisasi. `o-a1b2c3d4e5f`

Perintah ini membuat kebijakan berbasis sumber daya yang terlihat seperti berikut:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PrincipalOrgIDExample",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "lambda:InvokeFunction",  
      "Resource": "arn:aws:lambda:us-east-2:123456789012:function:example",  
      "Condition": {  
        "StringEquals": {  
          "aws:PrincipalOrgID": "o-a1b2c3d4e5f"  
        }  
      }  
    }  
  ]  
}
```

Untuk informasi selengkapnya, lihat [aws: PrincipalOrg ID](#) di panduan IAM pengguna.

Memberikan akses fungsi Lambda ke akun lain

[Untuk berbagi fungsi dengan yang lain Akun AWS, tambahkan pernyataan izin lintas akun ke kebijakan berbasis sumber daya fungsi.](#) Jalankan perintah [add-permission](#) dan tentukan ID akun sebagai principal. Contoh berikut memberi izin 111122223333 akun untuk memanggil my-function dengan alias prod.

```
aws lambda add-permission \  
  --function-name my-function:prod \  
  --statement-id xaccount \  
  --action lambda:InvokeFunction \  
  --principal 111122223333 \  
  --output text
```

Anda akan melihat output berikut:

```
{"Sid": "xaccount", "Effect": "Allow", "Principal":  
{"AWS": "arn:aws:iam::111122223333:root"}, "Action": "lambda:InvokeFunction", "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function"}
```

Kebijakan berbasis sumber daya memberikan izin bagi akun lain untuk mengakses fungsi, tetapi tidak mengizinkan pengguna dalam akun tersebut untuk melebihi izin mereka. Pengguna di akun lain harus memiliki [izin pengguna](#) yang sesuai untuk menggunakan LambdaAPI.

Untuk membatasi akses ke pengguna atau peran di akun lain, tentukan ARN identitas penuh sebagai prinsipal. Misalnya, `arn:aws:iam::123456789012:user/developer`.

[Alias](#) membatasi versi mana yang dapat dilakukan invokasi oleh akun lain. Ini membutuhkan akun lain untuk memasukkan alias dalam fungsiARN.

```
aws lambda invoke \  
  --function-name arn:aws:lambda:us-east-2:123456789012:function:my-function:prod out
```

Anda akan melihat output berikut:

```
{  
  "StatusCode": 200,
```

```
"ExecutedVersion": "1"
}
```

Pemilik fungsi kemudian dapat memperbarui alias untuk menunjuk ke versi baru tanpa pemanggil perlu mengubah cara melakukan invokasi fungsi Anda. Ini memastikan akun lain tidak perlu mengubah kodenya untuk menggunakan versi baru, dan memiliki izin untuk melakukan invokasi versi fungsi yang terkait dengan alias.

Anda dapat memberikan akses lintas akun untuk sebagian besar API tindakan yang [beroperasi pada fungsi yang ada](#). Misalnya, Anda dapat memberikan akses ke `lambda:ListAliases` agar akun bisa mendapatkan daftar alias, atau `lambda:GetFunction` agar mengunduh kode fungsi Anda. Tambahkan setiap izin secara terpisah, atau gunakan `lambda:*` untuk memberikan akses ke semua tindakan untuk fungsi tertentu.

Untuk memberikan izin akun lain untuk beberapa fungsi, atau untuk tindakan yang tidak beroperasi pada suatu fungsi, sebaiknya gunakan [IAMperan](#).

Memberikan akses lapisan Lambda ke akun lain

[Untuk berbagi layer dengan yang lain Akun AWS, tambahkan pernyataan izin lintas akun ke kebijakan berbasis sumber daya lapisan](#). Jalankan [add-layer-version-permission](#) perintah dan tentukan ID akun sebagai `principal`. Dalam setiap pernyataan, Anda dapat memberikan izin ke satu akun, semua akun, atau organisasi di [AWS Organizations](#).

Contoh berikut memberikan akun 111122223333 akses ke versi 2 lapisan. `bash-runtime`

```
aws lambda add-layer-version-permission \
  --layer-name bash-runtime \
  --version-number 2 \
  --statement-id xaccount \
  --action lambda:GetLayerVersion \
  --principal 111122223333 \
  --output text
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:GetLayerVersion","Resource":"arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```


Izin hanya berlaku untuk satu versi lapisan. Ulangi proses ini tiap kali Anda membuat versi lapisan baru.

Untuk memberikan izin ke semua akun dalam suatu [AWS Organizations](#) organisasi, gunakan `organization-id` opsi ini. Contoh berikut memberikan semua akun dalam organisasi `o-t194hfs8cz` izin untuk menggunakan versi 3 dari `my-layer`

```
aws lambda add-layer-version-permission \  
  --layer-name my-layer \  
  --version-number 3 \  
  --statement-id engineering-org \  
  --principal '*' \  
  --action lambda:GetLayerVersion \  
  --organization-id o-t194hfs8cz \  
  --output text
```

Anda akan melihat output berikut:

```
{"Sid":"engineering-  
org","Effect":"Allow","Principal":"*","Action":"lambda:GetLayerVersion","Resource":"arn:aws:lam  
east-2:123456789012:layer:my-layer:3","Condition":{"StringEquals":  
{"aws:PrincipalOrgID":"o-t194hfs8cz"}}}
```

Untuk memberikan izin ke beberapa akun atau organisasi, Anda harus menambahkan beberapa pernyataan.

Menggunakan kontrol akses berbasis atribut di Lambda

Dengan [kontrol akses berbasis atribut \(ABAC\)](#), Anda dapat menggunakan tag untuk mengontrol akses ke fungsi Lambda Anda. Anda dapat melampirkan tag ke fungsi Lambda, meneruskannya dalam permintaan API tertentu, atau melampirkannya ke prinsipal AWS Identity and Access Management (IAM) yang membuat permintaan. Untuk informasi selengkapnya tentang cara AWS memberikan akses berbasis atribut, lihat [Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM](#).

Anda dapat menggunakan ABAC untuk [memberikan hak istimewa paling sedikit](#) tanpa menentukan pola Nama Sumber Daya Amazon (ARN) atau ARN dalam kebijakan IAM. Sebagai gantinya, Anda dapat menentukan tag dalam [elemen kondisi](#) kebijakan IAM untuk mengontrol akses. Penskalaan lebih mudah dengan ABAC karena Anda tidak perlu memperbarui kebijakan IAM saat membuat fungsi baru. Sebagai gantinya, tambahkan tag ke fungsi baru untuk mengontrol akses.

Di Lambda, tag bekerja pada tingkat fungsi. Tag tidak didukung untuk lapisan, konfigurasi penandatanganan kode, atau pemetaan sumber peristiwa. Saat Anda menandai fungsi, tag tersebut berlaku untuk semua versi dan alias yang terkait dengan fungsi tersebut. Untuk informasi tentang cara menandai fungsi, lihat [Menggunakan tag pada fungsi Lambda](#).

Anda dapat menggunakan tombol kondisi berikut untuk mengontrol tindakan fungsi:

- [aws: ResourceTag /tag-key](#): Kontrol akses berdasarkan tag yang dilampirkan ke fungsi Lambda.
- [aws: RequestTag /tag-key](#): Memerlukan tag untuk hadir dalam permintaan, seperti saat membuat fungsi baru.
- [aws: PrincipalTag /tag-key](#) : Kontrol apa yang boleh dilakukan oleh kepala sekolah IAM (orang yang membuat permintaan) berdasarkan tag yang dilampirkan ke pengguna atau peran IAM mereka.
- [aws: TagKeys](#): Kontrol apakah kunci tag tertentu dapat digunakan dalam permintaan.

Untuk daftar lengkap tindakan Lambda yang mendukung ABAC, lihat [Tindakan fungsi yang didukung](#) dan periksa kolom Kondisi dalam tabel.

Langkah-langkah berikut menunjukkan salah satu cara untuk mengatur izin menggunakan ABAC. Dalam skenario contoh ini, Anda akan membuat empat kebijakan izin IAM. Kemudian, Anda akan melampirkan kebijakan ini ke peran IAM baru. Terakhir, Anda akan membuat pengguna IAM dan memberikan izin kepada pengguna tersebut untuk mengambil peran baru.

Topik

- [Prasyarat](#)
- [Langkah 1: Memerlukan tag pada fungsi baru](#)
- [Langkah 2: Izinkan tindakan berdasarkan tag yang dilampirkan ke fungsi Lambda dan prinsip IAM](#)
- [Langkah 3: Berikan izin daftar](#)
- [Langkah 4: Berikan izin IAM](#)
- [Langkah 5: Buat peran IAM](#)
- [Langkah 6: Buat pengguna IAM](#)
- [Langkah 7: Uji izin](#)
- [Langkah 8: Bersihkan sumber daya Anda](#)

Prasyarat

Pastikan Anda memiliki peran [eksekusi Lambda](#). Anda akan menggunakan peran ini saat memberikan izin IAM dan saat membuat fungsi Lambda.

Langkah 1: Memerlukan tag pada fungsi baru

Saat menggunakan ABAC dengan Lambda, ini adalah praktik terbaik untuk mengharuskan semua fungsi memiliki tag. Ini membantu memastikan bahwa kebijakan izin ABAC Anda berfungsi seperti yang diharapkan.

[Buat kebijakan IAM](#) yang mirip dengan contoh berikut. Kebijakan ini menggunakan kunci TagKeys kondisi [aws: RequestTag /tag-key](#), [aws: ResourceTag /tag-key](#), dan [aws:](#) untuk mengharuskan fungsi baru dan prinsipal IAM yang membuat fungsi keduanya memiliki tag. `project` `ForAllValues` pengubah memastikan bahwa itu `project` adalah satu-satunya tag yang diizinkan. Jika Anda tidak menyertakan `ForAllValues` pengubah, pengguna dapat menambahkan tag lain ke fungsi selama mereka juga lulus `project`.

Example — Memerlukan tag pada fungsi baru

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction",
      "lambda:TagResource"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/project": "${aws:PrincipalTag/project}",
        "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": "project"
      }
    }
  }
}
```

Langkah 2: Izinkan tindakan berdasarkan tag yang dilampirkan ke fungsi Lambda dan prinsip IAM

Buat kebijakan IAM kedua menggunakan [ResourceTagkunci kondisi aws: /tag-key](#) untuk meminta tag prinsipal agar sesuai dengan tag yang dilampirkan ke fungsi. Contoh kebijakan berikut memungkinkan prinsipal dengan `project` tag untuk memanggil fungsi dengan tag. `project` Jika suatu fungsi memiliki tag lain, tindakan ditolak.

Example — Memerlukan tag yang cocok pada fungsi dan prinsip IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:*:function:*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

Langkah 3: Berikan izin daftar

Buat kebijakan yang memungkinkan prinsipal untuk mencantumkan fungsi Lambda dan peran IAM. Hal ini memungkinkan prinsipal untuk melihat semua fungsi Lambda dan peran IAM di konsol dan saat memanggil tindakan API.

Example — Berikan izin daftar Lambda dan IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AllResourcesLambdaNoTags",
    "Effect": "Allow",
    "Action": [
        "lambda:GetAccountSettings",
        "lambda:ListFunctions",
        "iam:ListRoles"
    ],
    "Resource": "*"
  }
]
}

```

Langkah 4: Berikan izin IAM

Buat kebijakan yang memungkinkan iam: PassRole. Izin ini diperlukan saat Anda menetapkan peran eksekusi ke suatu fungsi. Dalam contoh kebijakan berikut, ganti contoh ARN dengan ARN peran eksekusi Lambda Anda.

Note

Jangan menggunakan kunci ketentuan ResourceTag dalam sebuah kebijakan dengan tindakan iam:PassRole. Anda tidak dapat menggunakan tag pada peran IAM untuk mengontrol akses ke siapa yang dapat memberikan peran tersebut. Untuk informasi selengkapnya tentang izin yang diperlukan untuk meneruskan peran ke layanan, lihat [Memberikan izin pengguna untuk meneruskan peran ke layanan. AWS](#)

Example — Berikan izin untuk lulus peran eksekusi

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/lambda-ex"
    }
  ]
}

```

```
}
```

Langkah 5: Buat peran IAM

Ini adalah praktik terbaik untuk [menggunakan peran untuk mendelegasikan izin](#). [Buat peran IAM](#) yang disebut `abac-project-role`:

- Pada Langkah 1: Pilih entitas tepercaya: Pilih AWS akun dan kemudian pilih Akun ini.
- Pada Langkah 2: Tambahkan izin: Lampirkan empat kebijakan IAM yang Anda buat di langkah sebelumnya.
- Pada Langkah 3: Nama, tinjau, dan buat: Pilih Tambahkan tag. Untuk Kunci, masukkan `project`. Jangan masukkan Nilai.

Langkah 6: Buat pengguna IAM

[Buat pengguna IAM](#) yang dipanggil `abac-test-user`. Di bagian Setel izin, pilih Lampirkan kebijakan yang ada secara langsung, lalu pilih Buat kebijakan. Masukkan definisi kebijakan berikut. [Ganti `111122223333` dengan ID akun Anda.AWS](#) Kebijakan ini memungkinkan `abac-test-user` untuk berasumsi `abac-project-role`.

Example — Izinkan pengguna IAM untuk mengambil peran ABAC

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::111122223333:role/abac-project-role"
  }
}
```

Langkah 7: Uji izin

1. Masuk ke AWS konsol sebagai `abac-test-user`. Untuk informasi selengkapnya, lihat [Masuk sebagai pengguna IAM](#).
2. Beralih ke peran `abac-project-role`. Untuk informasi selengkapnya, lihat [Beralih ke peran \(konsol\)](#).

3. [Buat fungsi Lambda:](#)

- Di bawah Izin, pilih Ubah peran eksekusi default, lalu untuk peran Eksekusi, pilih Gunakan peran yang ada. Pilih peran eksekusi yang sama dengan yang Anda gunakan [Langkah 4: Berikan izin IAM](#).
- Di bawah Pengaturan lanjutan, pilih Aktifkan tag dan kemudian pilih Tambahkan tag baru. Untuk Kunci, masukkan project. Jangan masukkan Nilai.

4. [Uji fungsinya.](#)

5. Buat fungsi Lambda kedua dan tambahkan tag yang berbeda, seperti. environment Operasi ini akan gagal karena kebijakan ABAC yang Anda buat [Langkah 1: Memerlukan tag pada fungsi baru](#) hanya memungkinkan prinsipal untuk membuat fungsi dengan project tag.
6. Buat fungsi ketiga tanpa tag. Operasi ini akan gagal karena kebijakan ABAC yang Anda buat [Langkah 1: Memerlukan tag pada fungsi baru](#) tidak mengizinkan prinsipal untuk membuat fungsi tanpa tag.

Strategi otorisasi ini memungkinkan Anda untuk mengontrol akses tanpa membuat kebijakan baru untuk setiap pengguna baru. Untuk memberikan akses ke pengguna baru, cukup beri mereka izin untuk mengambil peran yang sesuai dengan proyek yang ditugaskan.

Langkah 8: Bersihkan sumber daya Anda

Untuk menghapus peran IAM

1. Buka [halaman Peran](#) dari konsol IAM.
2. Pilih peran yang Anda buat di [langkah 5](#).
3. Pilih Hapus.
4. Untuk mengonfirmasi penghapusan, masukkan nama peran di bidang input teks.
5. Pilih Hapus.

Untuk menghapus pengguna IAM

1. Buka [halaman Pengguna](#) konsol IAM.
2. Pilih pengguna IAM yang Anda buat di [langkah 6](#).
3. Pilih Hapus.
4. Untuk mengonfirmasi penghapusan, masukkan nama pengguna di bidang input teks.

5. Pilih Hapus pengguna.

Untuk menghapus fungsi Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang Anda buat.
3. Pilih Tindakan, Hapus.
4. Ketik **delete** kolom input teks dan pilih Hapus.

Menyesuaikan bagian Sumber Daya dan Ketentuan kebijakan

Anda dapat membatasi cakupan izin pengguna dengan menentukan sumber daya dan kondisi dalam kebijakan AWS Identity and Access Management (IAM). Setiap tindakan dalam kebijakan mendukung kombinasi sumber daya dan jenis kondisi yang bervariasi tergantung pada perilaku tindakan.

Setiap pernyataan IAM kebijakan memberikan izin untuk tindakan yang dilakukan pada sumber daya. Ketika tindakan tersebut tidak dilakukan berdasarkan sumber daya yang disebutkan, atau ketika Anda memberikan izin untuk melakukan tindakan pada semua sumber daya, nilai sumber daya dalam kebijakan tersebut adalah wildcard (*). Untuk banyak tindakan, Anda dapat membatasi sumber daya yang dapat dimodifikasi pengguna dengan menentukan Amazon Resource Name (ARN) sumber daya, atau ARN pola yang cocok dengan beberapa sumber daya.

Untuk membatasi izin berdasarkan sumber daya, tentukan sumber daya dengan. ARN

Format sumber daya Lambda ARN

- Fungsi – `arn:aws:lambda:us-west-2:123456789012:function:my-function`
- Versi fungsi – `arn:aws:lambda:us-west-2:123456789012:function:my-function:1`
- Alias fungsi – `arn:aws:lambda:us-west-2:123456789012:function:my-function:TEST`
- Pemetaan sumber kejadian – `arn:aws:lambda:us-west-2:123456789012:event-source-mapping:fa123456-14a1-4fd2-9fec-83de64ad683de6d47`
- Lapisan – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer`
- Versi lapisan – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer:1`

Misalnya, kebijakan berikut memungkinkan pengguna Akun AWS 123456789012 untuk memanggil fungsi bernama `my-function` di Wilayah Barat AS (Oregon) AWS .

Example aktifkan kebijakan fungsi

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Invoke",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:my-function"
    }
  ]
}
```

Ini adalah kasus khusus di mana pengidentifikasi tindakan (`lambda:InvokeFunction`) berbeda dari API operasi ([Invoke](#)). Untuk tindakan lainnya, pengidentifikasi tindakan adalah nama operasi yang diawali dengan `lambda:`.

Bagian-bagian

- [Memahami bagian Kondisi dalam kebijakan](#)
- [Fungsi referensi di bagian Sumber Daya kebijakan](#)
- [Tindakan fungsi yang didukung](#)
- [Tindakan pemetaan sumber peristiwa yang didukung](#)
- [Tindakan lapisan yang didukung](#)

Memahami bagian Kondisi dalam kebijakan

Kondisi adalah elemen kebijakan opsional yang menerapkan logika tambahan untuk menentukan apakah suatu tindakan diperbolehkan. Selain [kondisi](#) umum yang didukung semua tindakan, Lambda mendefinisikan jenis kondisi yang dapat Anda gunakan untuk membatasi nilai parameter tambahan pada beberapa tindakan.

[Misalnya, `lambda:Principal` kondisi ini memungkinkan Anda membatasi layanan atau akun tempat pengguna dapat memberikan akses pemanggilan pada kebijakan berbasis sumber daya fungsi.](#) Kebijakan berikut memungkinkan pengguna memberikan izin ke topik Amazon Simple Notification Service (AmazonSNS) untuk memanggil fungsi bernama `test`.

Example mengelola izin kebijakan fungsi

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageFunctionPolicy",
      "Effect": "Allow",
      "Action": [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:test:*",
      "Condition": {
        "StringEquals": {
          "lambda:Principal": "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Kondisi ini mengharuskan prinsipnya adalah Amazon SNS dan bukan layanan atau akun lain. Pola sumber daya mengharuskan nama fungsi test dan mencakup nomor versi atau alias. Misalnya, test:v1.

Untuk informasi selengkapnya tentang sumber daya dan ketentuan untuk Lambda dan AWS layanan lainnya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk AWS layanan](#) di Referensi Otorisasi Layanan.

Fungsi referensi di bagian Sumber Daya kebijakan

Anda mereferensikan fungsi Lambda dalam pernyataan kebijakan menggunakan Amazon Resource Name (ARN). Format fungsi ARN tergantung pada apakah Anda mereferensikan seluruh fungsi (tidak memenuhi syarat) atau [versi](#) fungsi atau [alias](#) (memenuhi syarat).

Saat melakukan API panggilan Lambda, pengguna dapat menentukan versi atau alias dengan meneruskan versi ARN atau alias ARN dalam [GetFunction](#) FunctionNameparameter, atau dengan menetapkan nilai dalam parameter. [GetFunctionQualifier](#) Lambda membuat keputusan otorisasi dengan membandingkan elemen sumber daya dalam IAM kebijakan dengan panggilan

FunctionName dan yang Qualifier diteruskan. API Jika ada ketidakcocokan, Lambda menolak permintaan tersebut.

Apakah Anda mengizinkan atau menolak tindakan pada fungsi Anda, Anda harus menggunakan ARN jenis fungsi yang benar dalam pernyataan kebijakan Anda untuk mencapai hasil yang Anda harapkan. Misalnya, jika kebijakan Anda mereferensikan yang tidak memenuhi syaratARN, Lambda menerima permintaan yang mereferensikan yang ARN tidak memenuhi syarat tetapi menolak permintaan yang mereferensikan kualifikasi. ARN

Note

Anda tidak dapat menggunakan karakter wildcard (*) untuk mencocokkan ID akun. Untuk informasi selengkapnya tentang sintaks yang diterima, lihat [referensi IAM JSON kebijakan](#) di Panduan IAM Pengguna.

Example memungkinkan pemanggilan yang tidak memenuhi syarat ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction"
    }
  ]
}
```

Jika kebijakan Anda mereferensikan kualifikasi tertentuARN, Lambda menerima permintaan yang mereferensikan ARN tetapi menolak permintaan yang mereferensikan yang tidak memenuhi syarat ARN atau kualifikasi ARN lain, misalnya,. myFunction:2

Example memungkinkan pemanggilan yang memenuhi syarat tertentu ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Action": "lambda:InvokeFunction",
        "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction:1"
    }
]
}

```

Jika kebijakan Anda mereferensikan ARN penggunaan yang memenuhi syarat: *, Lambda menerima permintaan yang memenuhi syarat ARN tetapi menolak permintaan yang merujuk kepada yang tidak memenuhi syarat. ARN

Example memungkinkan pemanggilan dari setiap yang memenuhi syarat ARN

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction:*"
    }
  ]
}

```

Jika kebijakan Anda mengacu pada ARN penggunaan apa pun*, Lambda menerima apa pun yang memenuhi syarat atau tidak memenuhi syarat. ARN

Example memungkinkan pemanggilan yang memenuhi syarat atau tidak memenuhi syarat ARN

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction*"
    }
  ]
}

```

Tindakan fungsi yang didukung

Tindakan yang beroperasi pada suatu fungsi dapat dibatasi untuk fungsi tertentu berdasarkan fungsi, versi, atau aliasARN, seperti yang dijelaskan dalam tabel berikut. Tindakan yang tidak mendukung pembatasan sumber daya diberikan untuk semua resource (*).

| Tindakan | Sumber Daya | Kondisi |
|--|--------------|---|
| AddPermission | Fungsi | lambda:Principal |
| RemovePermission | Versi fungsi | aws:ResourceTag/\${TagKey} |
| | Alias fungsi | lambda:FunctionUrl AuthType |
| Memohon Izin: lambda:InvokeFunction | Fungsi | aws:ResourceTag/\${TagKey} |
| | Versi fungsi | lambda:EventSourceToken |
| | Alias fungsi | |
| CreateFunction | Fungsi | lambda:CodeSigning ConfigArn |
| | | lambda:Layer |
| | | lambda:VpcIds |
| | | lambda:SubnetIds |
| | | lambda:SecurityGroupIds |
| | | aws:ResourceTag/\${TagKey} |
| | | aws:RequestTag/\${TagKey} |
| aws:TagKeys | | |
| UpdateFunctionConfiguration | Fungsi | lambda:CodeSigning ConfigArn lambda:Layer |

| Tindakan | Sumber Daya | Kondisi |
|----------|-------------|--|
| | | lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds aws:ResourceTag/\${TagKey} |

| Tindakan | Sumber Daya | Kondisi |
|---|-------------|---|
| CreateAlias | Fungsi | <code>aws:ResourceTag/\${TagKey}</code> |
| DeleteAlias | | |
| DeleteFunction | | |
| DeleteFunctionCodeSigningConfig | | |
| DeleteFunctionConcurrency | | |
| GetAlias | | |
| GetFunction | | |
| GetFunctionCodeSigningConfig | | |
| GetFunctionConcurrency | | |
| GetFunctionConfiguration | | |
| GetPolicy | | |
| ListProvisionedConcurrencyConfigs | | |
| ListAliases | | |
| ListTags | | |
| ListVersionsByFunction | | |
| PublishVersion | | |
| PutFunctionCodeSigningConfig | | |
| PutFunctionConcurrency | | |
| UpdateAlias | | |
| UpdateFunctionCode | | |

| Tindakan | Sumber Daya | Kondisi |
|--|--------------|--|
| CreateFunctionUrlConfig | Fungsi | lambda:FunctionUrl |
| DeleteFunctionUrlConfig | Alias fungsi | AuthType |
| GetFunctionUrlConfig | | aws:ResourceTag/\${TagKey} |
| UpdateFunctionUrlConfig | | |
| ListFunctionUrlConfigs | Fungsi | lambda:FunctionUrl AuthType |
| DeleteFunctionEventInvokeConfig | Fungsi | aws:ResourceTag/\${TagKey} |
| GetFunctionEventInvokeConfig | | |
| ListFunctionEventInvokeConfigs | | |
| PutFunctionEventInvokeConfig | | |
| UpdateFunctionEventInvokeConfig | | |
| DeleteProvisionedConcurrencyConfig | Alias fungsi | aws:ResourceTag/\${TagKey} |
| GetProvisionedConcurrencyConfig | Versi fungsi | |
| PutProvisionedConcurrencyConfig | | |
| GetAccountSettings | * | Tidak ada |
| ListFunctions | | |
| TagResource | Fungsi | aws:ResourceTag/\${TagKey} aws:RequestTag/\${TagKey} aws:TagKeys |
| UntagResource | Fungsi | aws:ResourceTag/\${TagKey} aws:TagKeys |

Tindakan pemetaan sumber peristiwa yang didukung

Untuk [pemetaan sumber peristiwa](#), Anda dapat membatasi menghapus dan memperbarui izin ke sumber peristiwa tertentu. Kondisi `lambda:FunctionArn` memungkinkan Anda membatasi fungsi mana yang dapat digunakan pengguna untuk mengonfigurasi sumber peristiwa yang akan diaktifkan.

Untuk tindakan ini, sumber daya adalah pemetaan sumber peristiwa, sehingga Lambda memberikan kondisi yang memungkinkan Anda membatasi izin berdasarkan fungsi yang diaktifkan oleh pemetaan sumber peristiwa.

Tindakan pemetaan sumber peristiwa

| Tindakan | Sumber Daya | Kondisi |
|--|---------------------------|---------------------------------|
| DeleteEventSourceMapping UpdateEventSourceMapping | Pemetaan sumber peristiwa | <code>lambda:FunctionArn</code> |
| CreateEventSourceMapping GetEventSourceMapping | * | <code>lambda:FunctionArn</code> |
| ListEventSourceMappings | * | Tidak ada |

Tindakan lapisan yang didukung

Tindakan berlapis memungkinkan Anda membatasi lapisan yang dapat dikelola dan digunakan dengan fungsi oleh pengguna. Tindakan yang berkaitan dengan penggunaan lapisan dan izin bertindak pada versi lapisan, selama `PublishLayerVersion` bekerja dengan nama lapisan. Anda dapat menggunakan wildcard untuk membatasi lapisan yang dapat pengguna gunakan untuk bekerja berdasarkan nama.

Note

[GetLayerVersion](#) Tindakan ini juga mencakup [GetLayerVersionByArn](#). Lambda tidak mendukung `GetLayerVersionByArn` sebagai tindakan IAM.

Tindakan berlapis

| Tindakan | Sumber Daya | Kondisi |
|--|---------------|-----------|
| AddLayerVersionPermission | Versi lapisan | Tidak ada |
| RemoveLayerVersionPermission | | |
| GetLayerVersion | | |
| GetLayerVersionPolicy | | |
| DeleteLayerVersion | | |
| ListLayerVersions | Lapisan | Tidak ada |
| PublishLayerVersion | | |
| ListLayers | * | Tidak ada |

Keamanan di AWS Lambda

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku AWS Lambda, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#).
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Lambda. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Lambda untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Lambda Anda.

Untuk informasi selengkapnya tentang penerapan prinsip keamanan pada aplikasi Lambda, lihat [Keamanan di Tanah Tanpa Server](#).

Topik

- [Perlindungan data di AWS Lambda](#)
- [Identity and Access Management untuk AWS Lambda](#)
- [Buat strategi tata kelola untuk fungsi dan lapisan Lambda](#)
- [Validasi kepatuhan untuk AWS Lambda](#)
- [Ketahanan di AWS Lambda](#)
- [Keamanan infrastruktur di AWS Lambda](#)
- [Menggunakan penandatanganan kode untuk memverifikasi integritas kode dengan Lambda](#)

Perlindungan data di AWS Lambda

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di AWS Lambda. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [Privasi Data FAQ](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Model Tanggung Jawab AWS Bersama dan](#) posting GDPR blog di Blog AWS Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat [Federal Information Processing Standard \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Lambda atau lainnya AWS layanan menggunakan konsol,, API AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar

Anda tidak menyertakan informasi kredensial dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Bagian-bagian

- [Enkripsi bergerak](#)
- [Enkripsi data saat istirahat untuk AWS Lambda](#)

Enkripsi bergerak

APIEndpoint Lambda hanya mendukung koneksi aman. HTTPS Saat Anda mengelola sumber daya Lambda dengan AWS Management Console, atau Lambda AWS SDKAPI, semua komunikasi dienkripsi dengan Transport Layer Security (TLS). Untuk daftar lengkap API titik akhir, lihat [AWS Wilayah dan titik akhir](#) di Referensi Umum AWS

Saat Anda [menghubungkan fungsi Anda ke sistem file](#), Lambda menggunakan enkripsi dalam perjalanan untuk semua koneksi. Untuk informasi selengkapnya, lihat [Enkripsi data di Amazon EFS](#) di Panduan Pengguna Amazon Elastic File System.

Saat Anda menggunakan [variabel lingkungan](#), Anda dapat mengaktifkan pembantu enkripsi konsol untuk menggunakan enkripsi sisi klien untuk melindungi variabel lingkungan yang sedang transit. Untuk informasi selengkapnya, lihat [Mengamankan variabel lingkungan Lambda](#).

Enkripsi data saat istirahat untuk AWS Lambda

Lambda selalu mengenkripsi variabel lingkungan saat istirahat. Secara default, Lambda menggunakan AWS KMS key Lambda yang dibuat di akun Anda untuk mengenkripsi variabel lingkungan Anda. Ini Kunci yang dikelola AWS dinamaiaws/Lambda.

Pada basis per-fungsi, Anda dapat secara opsional mengonfigurasi Lambda untuk menggunakan kunci yang dikelola pelanggan alih-alih default Kunci yang dikelola AWS untuk mengenkripsi variabel lingkungan Anda. Untuk informasi selengkapnya, lihat [Mengamankan variabel lingkungan Lambda](#).

Jika pemetaan sumber peristiwa fungsi Anda memiliki objek [kriteria filter](#), Lambda juga mengenkripsi kriteria filter menggunakan AWS KMS kunci secara default. Anda dapat menggunakan kunci yang dikelola pelanggan secara opsional untuk mengenkripsi kriteria filter.

Lambda selalu mengenkripsi file yang Anda unggah ke Lambda, termasuk [paket deployment](#) dan [arsip lapisan](#).

Amazon CloudWatch Logs dan AWS X-Ray juga mengenkripsi data secara default, dan dapat dikonfigurasi untuk menggunakan kunci yang dikelola pelanggan. Untuk detailnya, lihat [Mengenkripsi data CloudWatch log di Log](#) dan [Perlindungan data di AWS X-Ray](#).

Bagian-bagian

- [Memantau kunci enkripsi Anda untuk Lambda](#)

Memantau kunci enkripsi Anda untuk Lambda

Saat Anda menggunakan kunci yang dikelola AWS KMS pelanggan dengan Lambda, Anda dapat menggunakannya. [AWS CloudTrail](#) Contoh berikut adalah CloudTrail acara untuk `Decrypt`, `DescribeKey`, dan `GenerateDataKey` panggilan yang dilakukan oleh Lambda untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.

Decrypt

Jika Anda menggunakan kunci yang dikelola AWS KMS pelanggan untuk mengenkripsi objek [kriteria filter](#), Lambda mengirimkan `Decrypt` permintaan atas nama Anda saat Anda mencoba mengaksesnya dalam teks biasa (misalnya, dari panggilan). `ListEventSourceMappings` Contoh peristiwa berikut mencatat `Decrypt` operasi:

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI23456789EXAMPLE:example",
    "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI23456789EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/role-name",
        "accountId": "123456789012",
        "userName": "role-name"
      },
      "attributes": {
        "creationDate": "2024-05-30T00:45:23Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}
```

```
    },
    "invokedBy": "lambda.amazonaws.com"
  },
  "eventTime": "2024-05-30T01:05:46Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "lambda.amazonaws.com",
  "userAgent": "lambda.amazonaws.com",
  "requestParameters": {
    "keyId": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "encryptionContext": {
      "aws-crypto-public-key": "ABCD
+7876787678+CDEFGHIJKL/888666888999888555444111555222888333111==",
      "aws:lambda:EventSourceArn": "arn:aws:sqs:eu-west-1:123456789012:sample-
source",
      "aws:lambda:FunctionArn": "arn:aws:lambda:eu-
west-1:123456789012:function:sample-function"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEaaaaa",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEebbbbb",
  "readOnly": true,
  "resources": [
    {
      "accountId": "AWS Internal",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}
```

DescribeKey

Jika Anda menggunakan kunci terkelola AWS KMS pelanggan untuk mengenkripsi objek [kriteria filter](#), Lambda mengirimkan DescribeKey permintaan atas nama Anda saat Anda mencoba mengaksesnya (misalnya, dari GetEventSourceMapping panggilan). Contoh peristiwa berikut mencatat DescribeKey operasi:

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA123456789EXAMPLE:example",
    "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA123456789EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/role-name",
        "accountId": "123456789012",
        "userName": "role-name"
      },
      "attributes": {
        "creationDate": "2024-05-30T00:45:23Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2024-05-30T01:09:40Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DescribeKey",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "54.240.197.238",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36",
  "requestParameters": {
    "keyId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "responseElements": null,
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEaaaaa",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEebbbbb",
  "readOnly": true,
}
```



```

"resources": [
  {
    "accountId": "AWS Internal",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_256_GCM_SHA384",
  "clientProvidedHostHeader": "kms.eu-west-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}

```

GenerateDataKey

Saat Anda menggunakan kunci yang dikelola AWS KMS pelanggan untuk mengenkripsi objek [kriteria filter](#) Anda dalam UpdateEventSourceMapping panggilan CreateEventSourceMapping atau, Lambda mengirimkan GenerateDataKey permintaan atas nama Anda untuk menghasilkan kunci data untuk mengenkripsi kriteria filter (enkripsi amplop). Contoh peristiwa berikut mencatat GenerateDataKey operasi:

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA123456789EXAMPLE:example",
    "arn": "arn:aws:sts::123456789012:assumed-role/role-name/example",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA123456789EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/role-name",
        "accountId": "123456789012",
        "userName": "role-name"
      }
    }
  }
}

```

```

    },
    "attributes": {
      "creationDate": "2024-05-30T00:06:07Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "lambda.amazonaws.com"
},
"eventTime": "2024-05-30T01:04:18Z",
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKey",
"awsRegion": "eu-west-1",
"sourceIPAddress": "lambda.amazonaws.com",
"userAgent": "lambda.amazonaws.com",
"requestParameters": {
  "numberOfBytes": 32,
  "keyId": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "encryptionContext": {
    "aws-crypto-public-key": "ABCD
+7876787678+CDEFGHIJKL/888666888999888555444111555222888333111==",
    "aws:lambda:EventSourceArn": "arn:aws:sqs:eu-west-1:123456789012:sample-
source",
    "aws:lambda:FunctionArn": "arn:aws:lambda:eu-
west-1:123456789012:function:sample-function"
  },
},
},
"responseElements": null,
"requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEEaaaaa",
"eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEebbbbb",
"readOnly": true,
"resources": [
  {
    "accountId": "AWS Internal",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:eu-west-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"

```

```
}
```

Identity and Access Management untuk AWS Lambda

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAM administrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Lambda. IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Lambda bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)
- [Kebijakan terkelola AWS untuk AWS Lambda](#)
- [Memecahkan masalah AWS Lambda identitas dan akses](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Lambda.

Pengguna layanan – Jika Anda menggunakan layanan Lambda untuk melakukan tugas Anda, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Lambda untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara pengelolaan akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Lambda, lihat [Memecahkan masalah AWS Lambda identitas dan akses](#).

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Lambda di perusahaan Anda, Anda mungkin memiliki akses penuh ke Lambda. Tugas Anda adalah menentukan fitur dan sumber daya Lambda mana yang harus diakses pengguna layanan Anda. Anda kemudian harus

mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM Lambda, lihat [Bagaimana AWS Lambda bekerja dengan IAM](#)

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Lambda. Untuk melihat contoh kebijakan berbasis identitas Lambda yang dapat Anda gunakan, lihat IAM [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani AWS API permintaan](#) di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat [Autentikasi multi-faktor](#) di Panduan AWS IAM Identity Center Pengguna dan [Menggunakan otentikasi multi-faktor \(MFA\) AWS](#) di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensi pengguna root](#) di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat [Apa itu Pusat IAM Identitas?](#) dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

[IAMPengguna](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat [Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang](#) di IAMPanduan Pengguna.

[IAMGrup](#) adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdmins dan memberikan izin grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat [Kapan membuat IAM pengguna \(bukan peran\)](#) di Panduan IAM Pengguna.

IAMperan

[IAMPeran](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustom URL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat [Menggunakan IAM peran](#) di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengotentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai

proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM

- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur lain AWS layanan. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FAS permintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).
- Peran layanan — Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan](#) dalam IAM Panduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon](#) di IAM Panduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat [Kapan membuat IAM peran \(bukan pengguna\)](#) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat [Ringkasan JSON kebijakan](#) di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna IAM](#).

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam Akun AWS. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat [Memilih antara kebijakan terkelola dan kebijakan sebaris](#) di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau AWS layanan

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ikhtisar daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batas izin** — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat [Batas izin untuk IAM entitas](#) di [Panduan Pengguna IAM](#).
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations

adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP Membatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan IAM Pengguna.

Bagaimana AWS Lambda bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Lambda, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan Lambda.

| IAM fitur | Dukungan Lambda |
|--|-----------------|
| Kebijakan berbasis identitas | Ya |
| Kebijakan berbasis sumber daya | Ya |
| Tindakan kebijakan | Ya |
| Sumber daya kebijakan | Ya |
| kunci-kunci persyaratan kebijakan (spesifik layanan) | Ya |
| ACLs | Tidak |

| IAM fitur | Dukungan Lambda |
|---|-----------------|
| ABAC(tag dalam kebijakan) | Parsial |
| Kredensial sementara | Ya |
| Teruskan sesi akses (FAS) | Tidak |
| Peran layanan | Ya |
| Peran terkait layanan | Parsial |

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Lambda dan layanan AWS lainnya dengan IAM sebagian besar fitur, [AWS lihat layanan yang berfungsi](#) di IAM Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Lambda

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna IAM](#).

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat [referensi elemen IAM JSON kebijakan](#) di Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Lambda

Untuk melihat contoh kebijakan berbasis identitas Lambda, lihat. [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)

Kebijakan berbasis sumber daya dalam Lambda

Mendukung kebijakan berbasis sumber daya: Ya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau AWS layanan

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun IAM di](#) Panduan IAM Pengguna.

Anda dapat melampirkan kebijakan berbasis sumber daya ke fungsi atau lapisan Lambda. Kebijakan ini mendefinisikan prinsipal mana yang dapat melakukan tindakan pada fungsi atau lapisan.

Untuk mempelajari cara melampirkan kebijakan berbasis sumber daya ke fungsi atau lapisan, lihat [Bekerja dengan kebijakan berbasis sumber daya di Lambda IAM](#)

Tindakan kebijakan untuk Lambda

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

ActionElemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Lambda, lihat [Tindakan yang ditentukan oleh AWS Lambda](#) dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Lambda menggunakan awalan berikut sebelum tindakan:

```
lambda
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
  "lambda:action1",  
  "lambda:action2"  
]
```

Untuk melihat contoh kebijakan berbasis identitas Lambda, lihat. [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)

Sumber daya kebijakan untuk Lambda

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Lambda dan jenis sumber daya LambdaARNs, lihat [Jenis sumber daya yang ditentukan oleh AWS Lambda](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Lambda](#).

Untuk melihat contoh kebijakan berbasis identitas Lambda, lihat. [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)

Kunci kondisi kebijakan untuk Lambda

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen Condition (atau blok Condition) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen Condition bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat [elemen IAM kebijakan: variabel dan tag](#) di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi Lambda, lihat Kunci kondisi [untuk AWS Lambda Referensi](#) Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh AWS Lambda](#).

Untuk melihat contoh kebijakan berbasis identitas Lambda, lihat. [Contoh kebijakan berbasis identitas untuk AWS Lambda](#)

ACLs di Lambda

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABAC dengan Lambda

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABAC membantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi lebih lanjut tentang ABAC, lihat [Apa itu ABAC?](#) dalam IAM User Guide. Untuk melihat tutorial dengan langkah-langkah persiapan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) di IAM Panduan Pengguna.

Untuk informasi selengkapnya tentang menandai sumber daya Lambda, lihat [Menggunakan kontrol akses berbasis atribut di Lambda](#)

Menggunakan kredensi sementara dengan Lambda

Mendukung kredensi sementara: Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensi sementara, lihat [AWS layanan yang berfungsi IAM](#) di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat [Beralih ke peran \(konsol\)](#) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensi keamanan sementara](#) di. IAM

Teruskan sesi akses untuk Lambda

Mendukung sesi akses maju (FAS): Tidak

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FAS permintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

Peran layanan untuk Lambda

Mendukung peran layanan: Ya

Peran layanan adalah [IAM peran](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAM Administrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke AWS layanan](#) dalam IAMPanduan Pengguna.

Di Lambda, peran layanan dikenal sebagai peran [eksekusi](#).

⚠ Warning

Mengubah izin untuk peran eksekusi dapat merusak fungsionalitas Lambda.

Peran terkait layanan untuk Lambda

Mendukung peran terkait layanan: Sebagian

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Lambda tidak memiliki peran terkait layanan, tetapi Lambda @Edge memilikinya. Untuk informasi selengkapnya, lihat [Peran Tertaut Layanan untuk Lambda @Edge di Panduan Pengembang Amazon. CloudFront](#)

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat [AWS layanan yang berfungsi](#) dengannya. IAM Cari layanan dalam tabel yang memiliki Yes di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS Lambda

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Lambda. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat [Membuat JSON IAM kebijakan di Panduan Pengguna. IAM](#)

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Lambda, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi AWS Lambda](#) di Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)

- [Menggunakan konsol Lambda](#)
- [Perbolehkan pengguna untuk melihat izin mereka sendiri](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Lambda di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan AWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan](#) di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat [Kebijakan dan izin IAM di IAM](#) Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [elemen IAM JSON kebijakan: Kondisi](#) dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan IAM Access Analyzer](#) di IAMPanduan Pengguna.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat [Mengonfigurasi API akses MFA yang dilindungi](#) di IAMPanduan Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik di IAM, lihat [Praktik terbaik keamanan IAM di Panduan IAM Pengguna](#).

Menggunakan konsol Lambda

Untuk mengakses AWS Lambda konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Lambda di situs Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk contoh kebijakan yang memberikan akses minimal untuk pengembangan fungsi, lihat [Memberikan pengguna akses ke fungsi Lambda](#). Selain Lambda APIs, konsol Lambda menggunakan layanan lain untuk menampilkan konfigurasi pemicu dan memungkinkan Anda menambahkan pemicu baru. Jika pengguna Anda menggunakan Lambda dengan layanan lain, mereka juga memerlukan akses ke layanan tersebut. Untuk perincian konfigurasi layanan lain dengan Lambda, lihat [Memanggil Lambda dengan acara dari layanan lain AWS](#).

Perbolehkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan AWS CLI atau AWS API.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Sid": "ViewOwnUserInfo",
  "Effect": "Allow",
  "Action": [
    "iam:GetUserPolicy",
    "iam:ListGroupsWithUser",
    "iam:ListAttachedUserPolicies",
    "iam:ListUserPolicies",
    "iam:GetUser"
  ],
  "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
  "Sid": "NavigateInConsole",
  "Effect": "Allow",
  "Action": [
    "iam:GetGroupPolicy",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:ListAttachedGroupPolicies",
    "iam:ListGroupPolicies",
    "iam:ListPolicyVersions",
    "iam:ListPolicies",
    "iam:ListUsers"
  ],
  "Resource": "*"
}
]
```

Kebijakan terkelola AWS untuk AWS Lambda

Kebijakan terkelola AWS adalah kebijakan mandiri yang dibuat dan dikelola AWS. Kebijakan terkelola AWS dirancang untuk memberikan izin bagi banyak kasus penggunaan umum agar Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan yang dikelola AWS mungkin tidak memberikan izin hak akses paling rendah untuk kasus penggunaan spesifik Anda karena kebijakan ini tersedia untuk digunakan semua pelanggan AWS. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan yang dikelola AWS. Jika AWS memperbarui izin yang ditentukan dalam sebuah kebijakan yang dikelola AWS, maka pembaruan tersebut akan memengaruhi semua identitas prinsipal (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat sebuah AWS layanan baru diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada.

Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) dalam Panduan Pengguna IAM.

Topik

- [AWSkebijakan terkelola: AWSLambda_FullAccess](#)
- [AWSkebijakan terkelola: AWSLambda_ReadOnlyAccess](#)
- [AWSkebijakan terkelola: AWSLambdaBasicExecutionRole](#)
- [AWSkebijakan terkelola: AWSLambdaDynamoDBExecutionRole](#)
- [AWSkebijakan terkelola: AWSLambdaENIManagementAccess](#)
- [AWSkebijakan terkelola: AWSLambdaExecute](#)
- [AWSkebijakan terkelola: AWSLambdaInvocation -DynamoDB](#)
- [AWSkebijakan terkelola: AWSLambdaKinesisExecutionRole](#)
- [AWSkebijakan terkelola: AWSLambdaMSKExecutionRole](#)
- [AWSkebijakan terkelola: AWSLambdaRole](#)
- [AWSkebijakan terkelola: AWSLambdaSQSQueueExecutionRole](#)
- [AWSkebijakan terkelola: AWSLambdaVPCLambdaAccessExecutionRole](#)
- [Lambda memperbarui kebijakan terkelola AWS](#)

AWSkebijakan terkelola: AWSLambda_FullAccess

Kebijakan ini memberikan akses penuh ke tindakan Lambda. Ini juga memberikan izin ke AWS layanan lain yang digunakan untuk mengembangkan dan memelihara sumber daya Lambda.

Anda dapat melampirkan `AWSLambda_FullAccess` kebijakan ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- `lambda`— Memungkinkan kepala sekolah akses penuh ke Lambda.

- `cloudformation`— Memungkinkan kepala sekolah untuk menggambarkan AWS CloudFormation tumpukan dan daftar sumber daya di tumpukan tersebut.
- `cloudwatch`— Memungkinkan kepala sekolah untuk mencantumkan metrik Amazon dan mendapatkan CloudWatch data metrik.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan kelompok keamanan, subnet, dan VPC.
- `iam`— Memungkinkan prinsipal untuk mendapatkan kebijakan, versi kebijakan, peran, kebijakan peran, kebijakan peran terlampir, dan daftar peran. Kebijakan ini juga memungkinkan kepala sekolah untuk meneruskan peran ke Lambda. `PassRole` izin digunakan saat Anda menetapkan peran eksekusi ke fungsi.
- `kms`— Memungkinkan kepala sekolah untuk daftar alias.
- `logs`— Memungkinkan kepala sekolah untuk menggambarkan grup log Amazon CloudWatch . Untuk grup log yang terkait dengan fungsi Lambda, kebijakan ini memungkinkan prinsipal menjelaskan aliran log, mendapatkan peristiwa log, dan memfilter peristiwa log.
- `states`— Memungkinkan kepala sekolah untuk mendeskripsikan dan membuat daftar AWS Step Functions mesin negara.
- `tag`— Memungkinkan prinsipal untuk mendapatkan sumber daya berdasarkan tag mereka.
- `xray`— Memungkinkan kepala sekolah untuk mendapatkan ringkasan AWS X-Ray jejak dan mengambil daftar jejak yang ditentukan oleh ID.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambda_FullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambda_ReadOnlyAccess`

Kebijakan ini memberikan akses hanya-baca ke sumber daya Lambda dan AWS layanan lain yang digunakan untuk mengembangkan dan memelihara sumber daya Lambda.

Anda dapat melampirkan `AWSLambda_ReadOnlyAccess` kebijakan ke pengguna, grup, dan peran Anda.

Detail izin

Kebijakan ini mencakup izin berikut:

- `lambda`— Memungkinkan kepala sekolah untuk mendapatkan dan membuat daftar semua sumber daya.

- `cloudformation`— Memungkinkan kepala sekolah untuk mendeskripsikan dan daftar AWS CloudFormation tumpukan dan daftar sumber daya di tumpukan tersebut.
- `cloudwatch`— Memungkinkan kepala sekolah untuk mencantumkan metrik Amazon dan mendapatkan CloudWatch data metrik.
- `ec2`— Memungkinkan kepala sekolah untuk menggambarkan kelompok keamanan, subnet, dan VPC.
- `iam`— Memungkinkan prinsipal untuk mendapatkan kebijakan, versi kebijakan, peran, kebijakan peran, kebijakan peran terlampir, dan daftar peran.
- `kms`— Memungkinkan kepala sekolah untuk daftar alias.
- `logs`— Memungkinkan kepala sekolah untuk menggambarkan grup log Amazon CloudWatch . Untuk grup log yang terkait dengan fungsi Lambda, kebijakan ini memungkinkan prinsipal menjelaskan aliran log, mendapatkan peristiwa log, dan memfilter peristiwa log.
- `states`— Memungkinkan kepala sekolah untuk mendeskripsikan dan membuat daftar AWS Step Functions mesin negara.
- `tag`— Memungkinkan prinsipal untuk mendapatkan sumber daya berdasarkan tag mereka.
- `xray`— Memungkinkan kepala sekolah untuk mendapatkan ringkasan AWS X-Ray jejak dan mengambil daftar jejak yang ditentukan oleh ID.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambda_ReadOnlyAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaBasicExecutionRole`

Kebijakan ini memberikan izin untuk mengunggah log ke CloudWatch Log.

Anda dapat melampirkan `AWSLambdaBasicExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaBasicExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaDynamoDBExecutionRole`

Kebijakan ini memberikan izin untuk membaca catatan dari aliran Amazon DynamoDB dan menulis ke Log. CloudWatch

Anda dapat melampirkan `AWSLambdaDynamoDBExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaDynamoDBExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaENIManagementAccess`

Kebijakan ini memberikan izin untuk membuat, mendeskripsikan, dan menghapus antarmuka jaringan elastis yang digunakan oleh fungsi Lambda berkemampuan VPC.

Anda dapat melampirkan `AWSLambdaENIManagementAccess` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaENIManagementAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaExecute`

Kebijakan ini memberikan PUT dan GET akses ke Amazon Simple Storage Service dan akses penuh ke CloudWatch Log.

Anda dapat melampirkan `AWSLambdaExecute` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaExecute](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaInvocation-DynamoDB`

Kebijakan ini memberikan akses baca ke Amazon DynamoDB Streams.

Anda dapat melampirkan `AWSLambdaInvocation-DynamoDB` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaInvocation-DynamoDB](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaKinesisExecutionRole`

Kebijakan ini memberikan izin untuk membaca peristiwa dari aliran data Amazon Kinesis dan menulis ke Log. CloudWatch

Anda dapat melampirkan `AWSLambdaKinesisExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaKinesisExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaMSKExecutionRole`

Kebijakan ini memberikan izin untuk membaca dan mengakses catatan dari kluster Amazon Managed Streaming for Apache Kafka, mengelola antarmuka jaringan elastis, dan menulis ke Log. CloudWatch

Anda dapat melampirkan `AWSLambdaMSKExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaMSKExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaRole`

Kebijakan ini memberikan izin untuk menjalankan fungsi Lambda.

Anda dapat melampirkan `AWSLambdaRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaSQSQueueExecutionRole`

Kebijakan ini memberikan izin untuk membaca dan menghapus pesan dari antrian Layanan Antrian Sederhana Amazon, dan memberikan izin menulis ke Log. CloudWatch

Anda dapat melampirkan `AWSLambdaSQSQueueExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaSQSQueueExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: `AWSLambdaVPCAccessExecutionRole`

Kebijakan ini memberikan izin untuk mengelola antarmuka jaringan elastis dalam Amazon Virtual Private Cloud dan menulis ke Log. CloudWatch

Anda dapat melampirkan `AWSLambdaVPCAccessExecutionRole` kebijakan ke pengguna, grup, dan peran Anda.

Untuk informasi selengkapnya tentang kebijakan ini, termasuk dokumen kebijakan JSON dan versi kebijakan, lihat [AWSLambdaVPCAccessExecutionRole](#) di Panduan Referensi Kebijakan AWS Terkelola.

Lambda memperbarui kebijakan terkelola AWS

| Perubahan | Deskripsi | Tanggal |
|--|---|-----------------|
| AWSLambdaVPCAccessExecutionRole — Ubah | Lambda memperbarui <code>AWSLambdaVPCAccessExecutionRole</code> kebijakan untuk mengizinkan tindakan. <code>ec2:DescribeSubnets</code> | Januari 5, 2024 |
| AWSLambda_ReadOnlyAccess — Ubah | Lambda memperbarui <code>AWSLambda_ReadOnlyAccess</code> kebijakan untuk mengizinkan prinsipal membuat daftar tumpukan. <code>AWS CloudFormation</code> | Juli 27, 2023 |
| AWS Lambda mulai melacak perubahan | AWS Lambda mulai melacak perubahan untuk kebijakan terkelola AWS | Juli 27, 2023 |

Memecahkan masalah AWS Lambda identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Lambda dan IAM.

Topik

- [Saya tidak diotorisasi untuk melakukan tindakan di Lambda](#)
- [Saya tidak berwenang untuk melakukan `iam: PassRole`](#)

- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Lambda saya](#)

Saya tidak diotorisasi untuk melakukan tindakan di Lambda

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang `my-example-widget` sumber daya fiksi tetapi tidak memiliki izin `lambda:GetWidget` fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
lambda:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya `my-example-widget` dengan menggunakan tindakan `lambda:GetWidget`.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan `iam:PassRole`

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Lambda.

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Lambda. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Lambda saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Lambda mendukung fitur-fitur ini, lihat [Bagaimana AWS Lambda bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki](#) di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna yang diautentikasi secara eksternal \(federasi identitas\) di Panduan Pengguna](#). IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM

Buat strategi tata kelola untuk fungsi dan lapisan Lambda

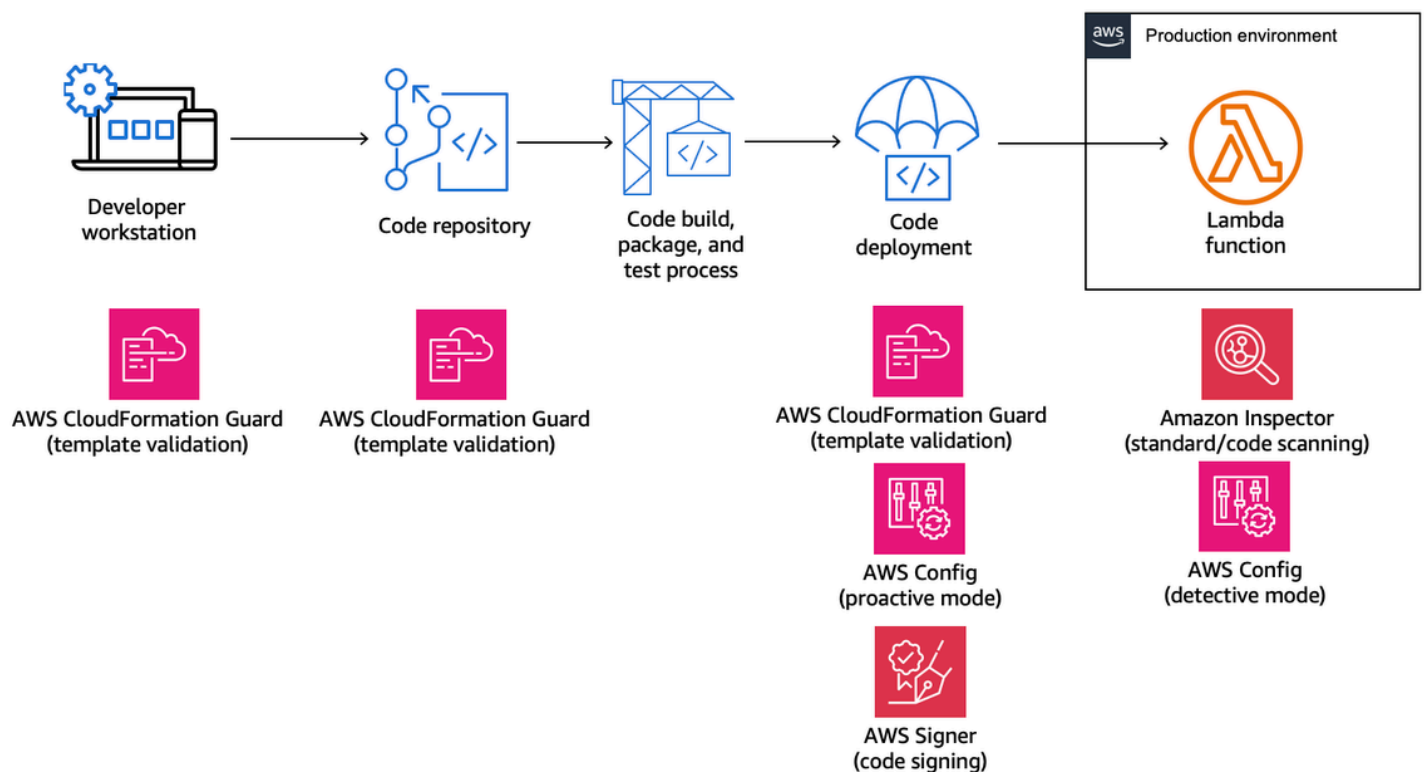
Untuk membangun dan menerapkan aplikasi cloud-native tanpa server, Anda harus mengizinkan kelincahan dan kecepatan ke pasar dengan tata kelola dan pagar pembatas yang sesuai. Anda menetapkan prioritas tingkat bisnis, mungkin menekankan kelincahan sebagai prioritas utama, atau sebagai alternatif menekankan penghindaran risiko melalui tata kelola, pagar pembatas, dan kontrol. Secara realistis, Anda tidak akan memiliki strategi “salah satu/atau” tetapi strategi “dan” yang menyeimbangkan kelincahan dan pagar pembatas dalam siklus hidup pengembangan perangkat lunak Anda. Di mana pun persyaratan ini termasuk dalam siklus hidup perusahaan Anda,

kemampuan tata kelola cenderung menjadi persyaratan implementasi dalam proses dan rantai alat Anda.

Berikut adalah beberapa contoh kontrol tata kelola yang mungkin diterapkan organisasi untuk Lambda:

- Fungsi Lambda tidak boleh diakses publik.
- Fungsi Lambda harus dilampirkan ke VPC.
- Fungsi Lambda tidak boleh menggunakan runtime yang tidak digunakan lagi.
- Fungsi Lambda harus ditandai dengan satu set tag yang diperlukan.
- Lapisan Lambda tidak boleh diakses di luar organisasi.
- Fungsi Lambda dengan grup keamanan terlampir harus memiliki tag yang cocok antara fungsi dan grup keamanan.
- Fungsi Lambda dengan lapisan terlampir harus menggunakan versi yang disetujui
- Variabel lingkungan Lambda harus dienkripsi saat istirahat dengan kunci yang dikelola pelanggan.

Diagram berikut adalah contoh strategi tata kelola mendalam yang mengimplementasikan kontrol dan kebijakan di seluruh proses pengembangan dan penyebaran perangkat lunak:



Topik berikut menjelaskan cara menerapkan kontrol untuk mengembangkan dan menerapkan fungsi Lambda di organisasi Anda, baik untuk startup maupun perusahaan. Organisasi Anda mungkin sudah memiliki alat di tempat. Topik berikut mengambil pendekatan modular untuk kontrol ini, sehingga Anda dapat memilih dan memilih komponen yang benar-benar Anda butuhkan.

Topik

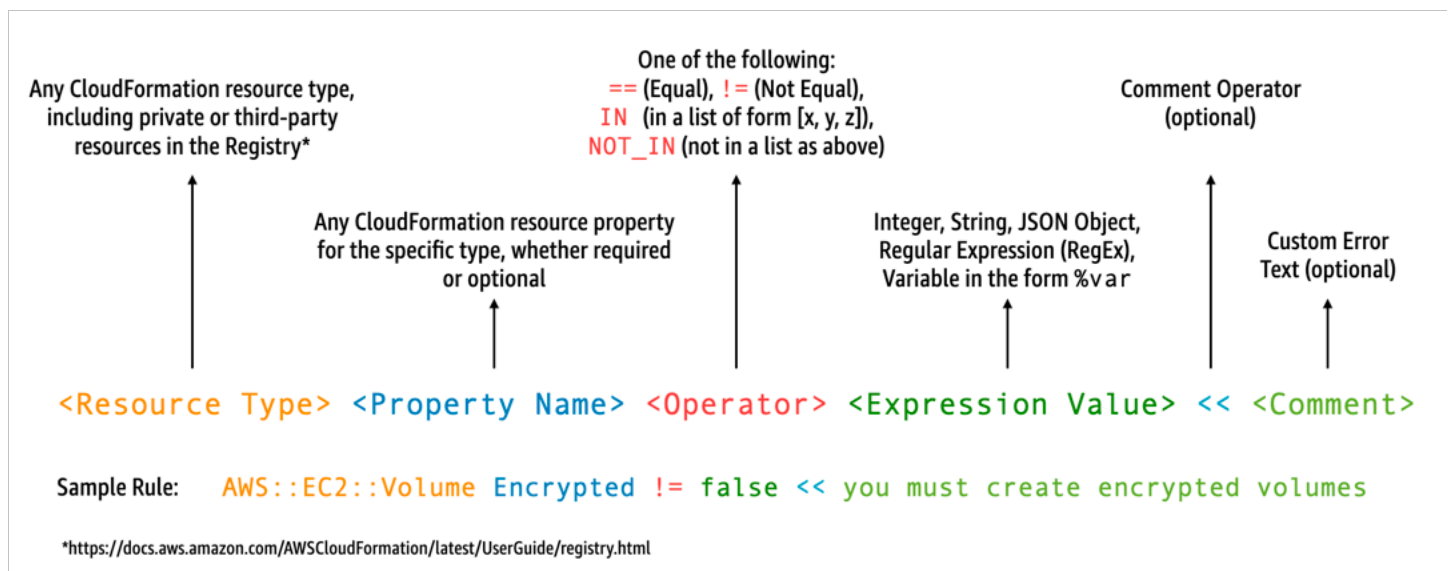
- [Kontrol proaktif untuk Lambda dengan AWS CloudFormation Guard](#)
- [Menerapkan kontrol pencegahan untuk Lambda dengan AWS Config](#)
- [Mendeteksi penerapan dan konfigurasi Lambda yang tidak sesuai dengan AWS Config](#)
- [Penandatanganan kode Lambda dengan AWS Signer](#)
- [Otomatisasikan penilaian keamanan untuk Lambda dengan Amazon Inspector](#)
- [Menerapkan observabilitas untuk keamanan dan kepatuhan Lambda](#)

Kontrol proaktif untuk Lambda dengan AWS CloudFormation Guard

[AWS CloudFormation Guard](#) adalah alat evaluasi open-source, tujuan umum, dan evaluasi. policy-as-code Ini dapat digunakan untuk tata kelola preventif dan kepatuhan dengan memvalidasi templat Infrastructure as Code (IaC) dan komposisi layanan terhadap aturan kebijakan. Aturan-aturan ini dapat disesuaikan berdasarkan persyaratan tim atau organisasi Anda. Untuk fungsi Lambda, aturan Penjaga dapat digunakan untuk mengontrol pembuatan sumber daya dan pembaruan konfigurasi dengan menentukan pengaturan properti yang diperlukan saat membuat atau memperbarui fungsi Lambda.

Administrator kepatuhan menentukan daftar kontrol dan kebijakan tata kelola yang diperlukan untuk menerapkan dan memperbarui fungsi Lambda. Administrator platform mengimplementasikan kontrol dalam pipeline CI/CD, sebagai webhook validasi pra-komit dengan repositori kode, dan menyediakan pengembang dengan alat baris perintah untuk memvalidasi template dan kode pada workstation lokal. Pengembang membuat kode, memvalidasi template dengan alat baris perintah, dan kemudian komit kode ke repositori, yang kemudian secara otomatis divalidasi melalui pipeline CI/CD sebelum penerapan ke lingkungan. AWS

Guard memungkinkan Anda untuk [menulis aturan](#) dan menerapkan kontrol Anda dengan bahasa khusus domain sebagai berikut.



Misalnya, Anda ingin memastikan bahwa pengembang hanya memilih runtime terbaru. Anda dapat menentukan dua kebijakan berbeda, satu untuk mengidentifikasi [runtime](#) yang sudah tidak digunakan lagi dan yang lain untuk mengidentifikasi runtime yang akan segera usang. Untuk melakukan ini, Anda dapat menulis `etc/rules.guard` file berikut:

```

let lambda_functions = Resources.*[
  Type == "AWS::Lambda::Function"
]

rule lambda_already_deprecated_runtime when %lambda_functions !empty {
  %lambda_functions {
    Properties {
      when Runtime exists {
        Runtime !in ["dotnetcore3.1", "nodejs12.x", "python3.6", "python2.7",
"dotnet5.0", "dotnetcore2.1", "ruby2.5", "nodejs10.x", "nodejs8.10", "nodejs4.3",
"nodejs6.10", "dotnetcore1.0", "dotnetcore2.0", "nodejs4.3-edge", "nodejs"] <<Lambda
function is using a deprecated runtime.>>
      }
    }
  }
}

rule lambda_soon_to_be_deprecated_runtime when %lambda_functions !empty {
  %lambda_functions {
    Properties {
      when Runtime exists {
        Runtime !in ["nodejs16.x", "nodejs14.x", "python3.7", "java8",
"dotnet7", "go1.x", "ruby2.7", "provided"] <<Lambda function is using a runtime that
is targeted for deprecation.>>
      }
    }
  }
}

```

Sekarang misalkan Anda menulis `iac/lambda.yaml` CloudFormation template berikut yang mendefinisikan fungsi Lambda:

```

Fn:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: python3.7
    CodeUri: src
    Handler: fn.handler
    Role: !GetAtt FnRole.Arn
    Layers:
      - arn:aws:lambda:us-east-1:111122223333:layer:LambdaInsightsExtension:35

```


Setelah [menginstal](#) utilitas Guard, validasi template Anda:

```
cfn-guard validate --rules etc/rules.guard --data iac/lambda.yaml
```

Keluaran terlihat seperti ini:

```
lambda.yaml Status = FAIL
FAILED rules
rules.guard/lambda_soon_to_be_deprecated_runtime
---
Evaluating data lambda.yaml against rules rules.guard
Number of non-compliant resources 1
Resource = Fn {
  Type      = AWS::Lambda::Function
  Rule = lambda_soon_to_be_deprecated_runtime {
    ALL {
      Check = Runtime not IN
["nodejs16.x", "nodejs14.x", "python3.7", "java8", "dotnet7", "go1.x", "ruby2.7", "provided"]
{
      ComparisonError {
        Message      = Lambda function is using a runtime that is targeted for
deprecation.
        Error         = Check was not compliant as property [/Resources/
Fn/Properties/Runtime[L:88,C:15]] was not present in [(resolved, Path=[L:0,C:0]
Value=["nodejs16.x", "nodejs14.x", "python3.7", "java8", "dotnet7", "go1.x", "ruby2.7", "provided"])]
      }
      PropertyPath   = /Resources/Fn/Properties/Runtime[L:88,C:15]
      Operator       = NOT IN
      Value          = "python3.7"
      ComparedWith  =
["nodejs16.x", "nodejs14.x", "python3.7", "java8", "dotnet7", "go1.x", "ruby2.7", "provided"]
      Code:
        86. Fn:
        87.   Type: AWS::Lambda::Function
        88.   Properties:
        89.     Runtime: python3.7
        90.     CodeUri: src
        91.     Handler: fn.handler
    }
  }
}
}
```

Guard memungkinkan pengembang Anda untuk melihat dari workstation pengembang lokal mereka bahwa mereka perlu memperbarui template untuk menggunakan runtime yang diizinkan oleh organisasi. Ini terjadi sebelum melakukan ke repositori kode dan kemudian gagal memeriksa dalam pipa CI/CD. Akibatnya, pengembang Anda mendapatkan umpan balik ini tentang cara mengembangkan templat yang sesuai dan mengalihkan waktu mereka untuk menulis kode yang memberikan nilai bisnis. Kontrol ini dapat diterapkan pada workstation pengembang lokal, dalam webhook validasi pra-komit, dan/atau di pipeline CI/CD sebelum penerapan.

Peringatan

Jika Anda menggunakan AWS Serverless Application Model (AWS SAM) template untuk menentukan fungsi Lambda, ketahuilah bahwa Anda perlu memperbarui aturan Guard untuk mencari jenis `AWS::Serverless::Function` sumber daya sebagai berikut.

```
let lambda_functions = Resources.*[
  Type == "AWS::Serverless::Function"
]
```

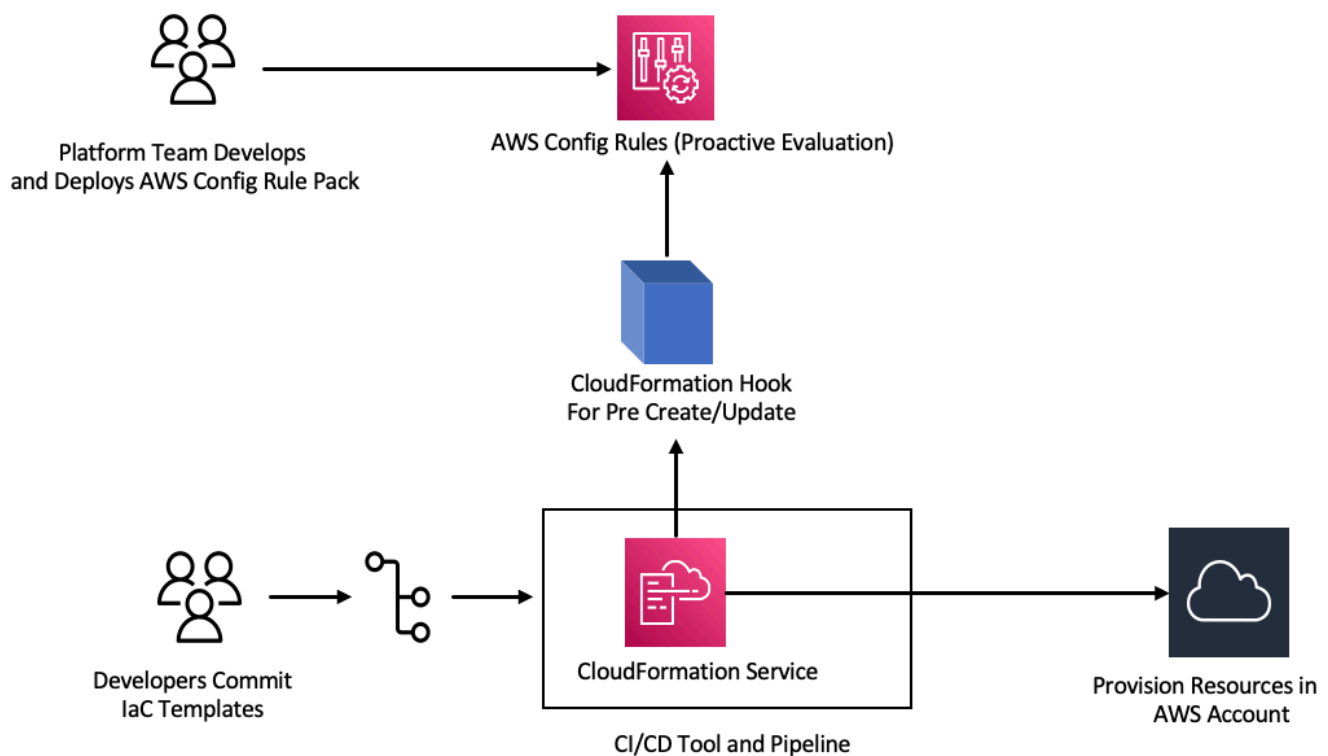
Guard juga mengharapkan properti untuk dimasukkan dalam definisi sumber daya. Sementara itu, AWS SAM template memungkinkan properti yang akan ditentukan di bagian [Globals](#) terpisah. Properti yang didefinisikan di bagian Globals tidak divalidasi dengan aturan Penjaga Anda.

Seperti yang diuraikan dalam [dokumentasi](#) pemecahan masalah Guard, ketahuilah bahwa Guard tidak mendukung intrinsik bentuk pendek seperti `!GetAtt` atau `!Sub` dan sebagai gantinya memerlukan penggunaan formulir yang diperluas: `and Fn::GetAtt Fn::Sub` ([Contoh sebelumnya](#) tidak mengevaluasi properti Peran, jadi intrinsik bentuk pendek digunakan untuk kesederhanaan.)

Menerapkan kontrol pencegahan untuk Lambda dengan AWS Config

Sangat penting untuk memastikan kepatuhan dalam aplikasi tanpa server Anda sedini mungkin dalam proses pengembangan. Dalam topik ini, kami membahas cara menerapkan kontrol pencegahan menggunakan [AWS Config](#). Ini memungkinkan Anda untuk menerapkan pemeriksaan kepatuhan sebelumnya dalam proses pengembangan dan memungkinkan Anda untuk menerapkan kontrol yang sama di saluran CI/CD Anda. Ini juga menstandarisasi kontrol Anda dalam repositori aturan yang dikelola secara terpusat sehingga Anda dapat menerapkan kontrol secara konsisten di seluruh akun Anda. AWS

Misalnya, administrator kepatuhan Anda menetapkan persyaratan untuk memastikan bahwa semua fungsi AWS X-Ray Lambda menyertakan penelusuran. Dengan AWS Config mode proaktif, Anda dapat menjalankan pemeriksaan kepatuhan pada sumber daya fungsi Lambda Anda sebelum penerapan, mengurangi risiko penerapan fungsi Lambda yang dikonfigurasi secara tidak benar dan menghemat waktu pengembang dengan memberi mereka umpan balik yang lebih cepat pada infrastruktur sebagai templat kode. Berikut ini adalah visualisasi aliran untuk kontrol pencegahan dengan: AWS Config



Pertimbangkan persyaratan bahwa semua fungsi Lambda harus mengaktifkan penelusuran. Sebagai tanggapan, tim platform mengidentifikasi perlunya AWS Config aturan tertentu untuk berjalan secara proaktif di semua akun. Aturan ini menandai fungsi Lambda apa pun yang tidak memiliki konfigurasi penelusuran X-Ray yang dikonfigurasi sebagai sumber daya yang tidak sesuai. Tim mengembangkan aturan, mengemasnya dalam paket [kesesuaian, dan menyebarkan paket](#) kesesuaian di semua AWS akun untuk memastikan bahwa semua akun dalam organisasi menerapkan kontrol ini secara seragam. Anda dapat menulis aturan dalam sintaks AWS CloudFormation Guard 2.xx, yang mengambil bentuk berikut:

```
rule name when condition { assertion }
```

Berikut ini adalah contoh aturan Penjaga yang memeriksa untuk memastikan fungsi Lambda mengaktifkan penelusuran:

```
rule lambda_tracing_check {
  when configuration.tracingConfig exists {
    configuration.tracingConfig.mode == "Active"
  }
}
```

[Tim platform mengambil tindakan lebih lanjut dengan mewajibkan bahwa setiap AWS CloudFormation penerapan memanggil kait pra-buat/pembaruan.](#) Mereka memikul tanggung jawab penuh untuk mengembangkan hook ini dan mengonfigurasi pipeline, memperkuat kontrol terpusat atas aturan kepatuhan dan mempertahankan aplikasi mereka yang konsisten di semua penerapan. Untuk mengembangkan, mengemas, dan mendaftarkan hook, lihat [Mengembangkan AWS CloudFormation Hooks](#) dalam dokumentasi CloudFormation Command Line Interface (CFN-CLI). Anda dapat menggunakan [CloudFormation CLI](#) untuk membuat proyek hook:

```
cfn init
```

Perintah ini meminta Anda untuk beberapa informasi dasar tentang proyek hook Anda dan membuat proyek dengan file berikut di dalamnya:

```
README.md
<hook-name>.json
rpdk.log
src/handler.py
template.yml
```

```
hook-role.yaml
```

Sebagai pengembang hook, Anda perlu menambahkan jenis sumber daya target yang diinginkan dalam file `<hook-name>.json` konfigurasi. Dalam konfigurasi di bawah ini, hook dikonfigurasi untuk mengeksekusi sebelum fungsi Lambda dibuat menggunakan CloudFormation Anda dapat menambahkan penanganan serupa untuk `preUpdate` dan `preDelete` tindakan juga.

```
"handlers": {
  "preCreate": {
    "targetNames": [
      "AWS::Lambda::Function"
    ],
    "permissions": []
  }
}
```

Anda juga perlu memastikan bahwa CloudFormation hook memiliki izin yang sesuai untuk memanggil file. AWS Config APIs Anda dapat melakukannya dengan memperbarui file definisi peran bernama `hook-role.yaml`. File definisi peran memiliki kebijakan kepercayaan berikut secara default, yang memungkinkan CloudFormation untuk mengambil peran.

```
AssumeRolePolicyDocument:
  Version: '2012-10-17'
  Statement:
    - Effect: Allow
      Principal:
        Service:
          - hooks.cloudformation.amazonaws.com
          - resources.cloudformation.amazonaws.com
```

Untuk mengizinkan hook ini memanggil config APIs, Anda harus menambahkan izin berikut ke pernyataan Policy. Kemudian Anda mengirimkan proyek hook menggunakan `cfn submit` perintah, di mana CloudFormation menciptakan peran untuk Anda dengan izin yang diperlukan.

```
Policies:
  - PolicyName: HookTypePolicy
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Action:
```

```

- "config:Describe*"
- "config:Get*"
- "config:List*"
- "config:SelectResourceConfig"
Resource: "*"

```

Selanjutnya, Anda perlu menulis fungsi Lambda dalam file `src/handler.py`. Dalam file ini, Anda menemukan metode bernama `preCreatepreUpdate`, dan `preDelete` sudah dibuat ketika Anda memulai proyek. Anda bertujuan untuk menulis fungsi umum yang dapat digunakan kembali yang memanggil AWS Config `StartResourceEvaluation` API dalam mode proaktif menggunakan AWS SDK for Python (Boto3) API. Panggilan ini mengambil properti sumber daya sebagai input dan mengevaluasi sumber daya terhadap definisi aturan.

```

def validate_lambda_tracing_config(resource_type, function_properties:
MutableMapping[str, Any]) -> ProgressEvent:
    LOG.info("Fetching proactive data")
    config_client = boto3.client('config')
    resource_specs = {
        'ResourceId': 'MyFunction',
        'ResourceType': resource_type,
        'ResourceConfiguration': json.dumps(function_properties),
        'ResourceConfigurationSchemaType': 'CFN_RESOURCE_SCHEMA'
    }
    LOG.info("Resource Specifications:", resource_specs)
    eval_response = config_client.start_resource_evaluation(EvaluationMode='PROACTIVE',
ResourceDetails=resource_specs, EvaluationTimeout=60)
    ResourceEvaluationId = eval_response.ResourceEvaluationId
    compliance_response =
config_client.get_compliance_details_by_resource(ResourceEvaluationId=ResourceEvaluationId)
    LOG.info("Compliance Verification:",
compliance_response.EvaluationResults[0].ComplianceType)
    if "NON_COMPLIANT" == compliance_response.EvaluationResults[0].ComplianceType:
        return ProgressEvent(status=OperationStatus.FAILED, message="Lambda function
found with no tracing enabled : FAILED", errorCode=HandlerErrorCode.NonCompliant)
    else:
        return ProgressEvent(status=OperationStatus.SUCCESS, message="Lambda function
found with tracing enabled : PASS.")

```

Sekarang Anda dapat memanggil fungsi umum dari handler untuk hook pra-buat. Berikut adalah contoh handler:

```
@hook.handler(HookInvocationPoint.CREATE_PRE_PROVISION)
```

```

def pre_create_handler(
    session: Optional[SessionProxy],
    request: HookHandlerRequest,
    callback_context: MutableMapping[str, Any],
    type_configuration: TypeConfigurationModel
) -> ProgressEvent:
    LOG.info("Starting execution of the hook")
    target_name = request.hookContext.targetName
    LOG.info("Target Name:", target_name)
    if "AWS::Lambda::Function" == target_name:
        return validate_lambda_tracing_config(target_name,
            request.hookContext.targetModel.get("resourceProperties"))
    )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")

```

Setelah langkah ini Anda dapat mendaftarkan hook dan mengkonfigurasinya untuk mendengarkan semua acara pembuatan AWS Lambda fungsi.

Pengembang menyiapkan template infrastruktur sebagai kode (IAC) untuk layanan mikro tanpa server menggunakan Lambda. Persiapan ini mencakup kepatuhan terhadap standar internal, diikuti dengan pengujian lokal dan melakukan template ke repositori. Berikut adalah contoh template IAC:

```

MyLambdaFunction:
  Type: 'AWS::Lambda::Function'
  Properties:
    Handler: index.handler
    Role: !GetAtt LambdaExecutionRole.Arn
    FunctionName: MyLambdaFunction
    Code:
      ZipFile: |
        import json

        def handler(event, context):
            return {
                'statusCode': 200,
                'body': json.dumps('Hello World!')}
    Runtime: python3.8
    TracingConfig:
      Mode: PassThrough
    MemorySize: 256

```

Timeout: 10

Sebagai bagian dari proses CI/CD, ketika CloudFormation template digunakan, CloudFormation layanan memanggil kait pra-buat/pembaruan tepat sebelum menyediakan jenis sumber daya. AWS::Lambda::Function Hook menggunakan AWS Config aturan yang berjalan dalam mode proaktif untuk memverifikasi bahwa konfigurasi fungsi Lambda menyertakan konfigurasi penelusuran yang diamankan. Respons dari hook menentukan langkah selanjutnya. Jika sesuai, hook menandakan keberhasilan, dan CloudFormation melanjutkan untuk menyediakan sumber daya. Jika tidak, penyebaran CloudFormation tumpukan gagal, pipeline segera berhenti, dan sistem mencatat detail untuk peninjauan berikutnya. Pemberitahuan kepatuhan dikirim ke pemangku kepentingan terkait.

Anda dapat menemukan informasi sukses/gagal hook di konsol: CloudFormation

| Stack info | Events | Resources | Outputs | Parameters | Template | Change sets |
|--|---------------------|----------------------|---|--|----------|-------------|
| Events (19) | | | | | | |
| <input type="text" value="Search events"/> | | | | | | |
| Timestamp | Logical ID | Status | Status reason | Hook invocations | | |
| 2023-08-29 23:50:23 UTC-0500 | HookTestStack | ROLLBACK_COMPLETE | - | - | | |
| 2023-08-29 23:50:22 UTC-0500 | LambdaExecutionRole | DELETE_COMPLETE | - | - | | |
| 2023-08-29 23:50:21 UTC-0500 | MyApi | DELETE_COMPLETE | - | - | | |
| 2023-08-29 23:50:20 UTC-0500 | LambdaExecutionRole | DELETE_IN_PROGRESS | - | - | | |
| 2023-08-29 23:50:20 UTC-0500 | MyLambdaFunction | DELETE_COMPLETE | - | - | | |
| 2023-08-29 23:50:20 UTC-0500 | MyApi | DELETE_IN_PROGRESS | - | - | | |
| 2023-08-29 23:50:18 UTC-0500 | HookTestStack | ROLLBACK_IN_PROGRESS | The following resource(s) failed to create: [MyLambdaFunction]. Rollback requested by user. | - | | |
| 2023-08-29 23:50:17 UTC-0500 | MyLambdaFunction | CREATE_FAILED | The following hook(s) failed: [AWS::Samples::LambdaTracingCheck::Hook] | - | | |
| 2023-08-29 23:50:17 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | AWS::Samples::LambdaTracingCheck::Hook | | |
| 2023-08-29 23:50:16 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | AWS::Samples::LambdaTracingCheck::Hook | | |
| 2023-08-29 23:50:15 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | - | | |
| 2023-08-29 23:50:14 UTC-0500 | LambdaExecutionRole | CREATE_COMPLETE | - | - | | |
| 2023-08-29 23:49:59 UTC-0500 | MyApi | CREATE_COMPLETE | - | - | | |
| 2023-08-29 23:49:59 UTC-0500 | MyApi | CREATE_IN_PROGRESS | Resource creation Initiated | - | | |
| 2023-08-29 23:49:58 UTC-0500 | LambdaExecutionRole | CREATE_IN_PROGRESS | Resource creation Initiated | - | | |
| 2023-08-29 23:49:58 UTC-0500 | LambdaExecutionRole | CREATE_IN_PROGRESS | - | - | | |
| 2023-08-29 23:49:58 UTC-0500 | MyApi | CREATE_IN_PROGRESS | - | - | | |
| 2023-08-29 23:49:55 UTC-0500 | HookTestStack | CREATE_IN_PROGRESS | User Initiated | - | | |
| 2023-08-29 23:49:50 UTC-0500 | HookTestStack | REVIEW_IN_PROGRESS | User Initiated | - | | |

Jika Anda mengaktifkan log untuk CloudFormation hook Anda, Anda dapat menangkap hasil evaluasi hook. Berikut adalah contoh log untuk hook dengan status gagal, yang menunjukkan bahwa fungsi Lambda tidak mengaktifkan X-Ray:

```

2023-08-29T23:50:17.574-05:00 ProgressEvent(status=<OperationStatus.FAILED: 'FAILED'>, errorCode=<HandlerErrorCode.NonCompliant: 'NonCompliant'...

ProgressEvent(status=<OperationStatus.FAILED: 'FAILED'>, errorCode=<HandlerErrorCode.NonCompliant: 'NonCompliant'>, message='Lambda
function found with no tracing enabled : FAILED', result=None, callbackContext=None, callbackDelaySeconds=0, resourceModel=None,
resourceModels=None, nextToken=None)
  
```

[Copy](#)

No newer events at this moment. [Auto retry paused.](#) [Resume](#)

Jika pengembang memilih untuk mengubah IAc untuk memperbarui TracingConfig Mode nilai dan menerapkan kembali, hook berhasil dijalankan Active dan tumpukan dilanjutkan dengan membuat sumber daya Lambda.

| Timestamp | Logical ID | Status | Status reason | Hook invocations |
|------------------------------|------------------------|--------------------|--|-----------------------------|
| 2023-08-29 23:56:52 UTC-0500 | LambdaApiGatewayInvoke | CREATE_IN_PROGRESS | - | - |
| 2023-08-29 23:56:52 UTC-0500 | MyLambdaFunction | CREATE_COMPLETE | - | - |
| 2023-08-29 23:56:44 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | Resource creation Initiated | - |
| 2023-08-29 23:56:44 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | Hook invocations complete. Resource creation initiated | - |
| 2023-08-29 23:56:43 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | AWS::Lambda::Function::Hook |
| 2023-08-29 23:56:41 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | - |
| 2023-08-29 23:56:41 UTC-0500 | MyLambdaFunction | CREATE_IN_PROGRESS | - | - |
| 2023-08-29 23:56:40 UTC-0500 | LambdaExecutionRole | CREATE_COMPLETE | - | - |
| 2023-08-29 23:56:25 UTC-0500 | MyApi | CREATE_COMPLETE | - | - |
| 2023-08-29 23:56:25 UTC-0500 | MyApi | CREATE_IN_PROGRESS | Resource creation Initiated | - |
| 2023-08-29 23:56:24 UTC-0500 | LambdaExecutionRole | CREATE_IN_PROGRESS | Resource creation Initiated | - |
| 2023-08-29 23:56:23 UTC-0500 | LambdaExecutionRole | CREATE_IN_PROGRESS | - | - |

Hook invocation details

Hook name
[AWS::Lambda::Function::Hook](#)

Hook status
HOOK_COMPLETE_SUCCEEDED

Hook failure mode
Fail

Hook invocation point
PRE_PROVISION

Hook status reason
Hook succeeded with message: Lambda function found with tracing enabled : PASS

Dengan cara ini, Anda dapat menerapkan kontrol pencegahan dengan AWS Config dalam mode proaktif saat mengembangkan dan menerapkan sumber daya tanpa server di akun Anda. AWS Dengan mengintegrasikan AWS Config aturan ke dalam pipeline CI/CD, Anda dapat mengidentifikasi

dan secara opsional memblokir penerapan sumber daya yang tidak sesuai, seperti fungsi Lambda yang tidak memiliki konfigurasi penelusuran aktif. Ini memastikan bahwa hanya sumber daya yang mematuhi kebijakan tata kelola terbaru yang diterapkan ke lingkungan Anda AWS .

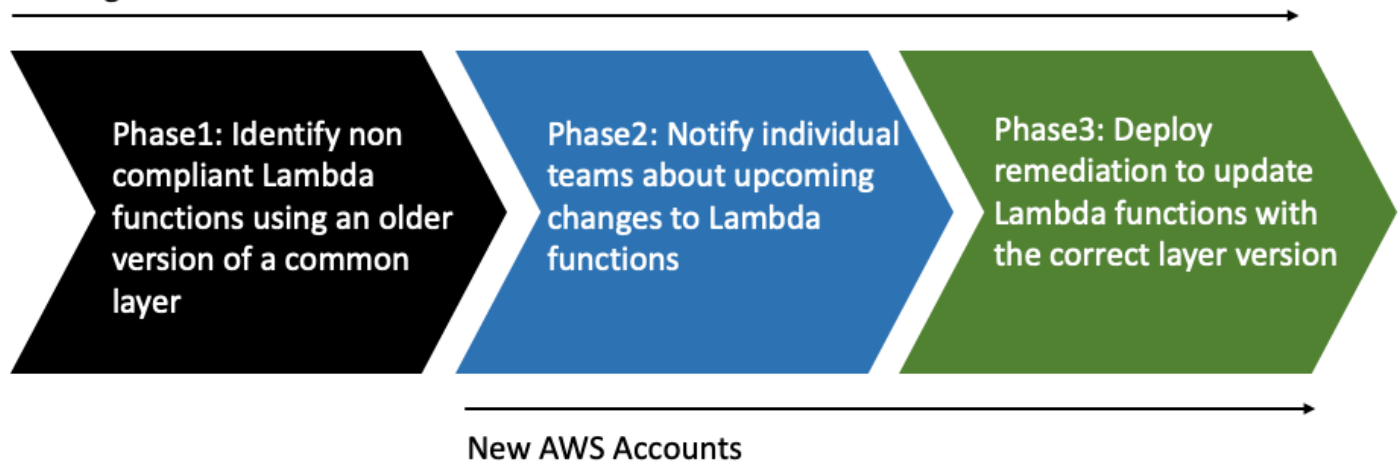
Mendeteksi penerapan dan konfigurasi Lambda yang tidak sesuai dengan AWS Config

Selain [evaluasi proaktif](#), juga AWS Config dapat secara reaktif mendeteksi penyebaran sumber daya dan konfigurasi yang tidak sesuai dengan kebijakan tata kelola Anda. Ini penting karena kebijakan tata kelola berkembang saat organisasi Anda belajar dan menerapkan praktik terbaik baru.

Pertimbangkan skenario di mana Anda menetapkan kebijakan baru saat menerapkan atau memperbarui fungsi Lambda: Semua fungsi Lambda harus selalu menggunakan versi lapisan Lambda tertentu yang disetujui. Anda dapat mengonfigurasi AWS Config untuk memantau fungsi baru atau yang diperbarui untuk konfigurasi lapisan. Jika AWS Config mendeteksi fungsi yang tidak menggunakan versi lapisan yang disetujui, ia menandai fungsi tersebut sebagai sumber daya yang tidak sesuai. Anda dapat mengonfigurasi secara opsional AWS Config untuk memulihkan sumber daya secara otomatis dengan menentukan tindakan remediasi menggunakan dokumen otomatisasi. AWS Systems Manager Misalnya, Anda dapat menulis dokumen otomatisasi dengan Python menggunakan AWS SDK for Python (Boto3), yang memperbarui fungsi yang tidak sesuai untuk menunjuk ke versi lapisan yang disetujui. Dengan demikian, AWS Config berfungsi sebagai kontrol detektif dan korektif, mengotomatiskan manajemen kepatuhan.

Mari kita uraikan proses ini menjadi tiga fase implementasi penting:

Existing AWS Accounts



Tahap 1: Identifikasi sumber daya akses

Mulailah dengan mengaktifkan AWS Config di seluruh akun Anda dan mengonfigurasinya untuk merekam fungsi Lambda AWS. Ini memungkinkan AWS Config untuk mengamati kapan fungsi Lambda dibuat atau diperbarui. Anda kemudian dapat mengonfigurasi [aturan kebijakan khusus](#) untuk

memeriksa pelanggaran kebijakan tertentu, yang menggunakan AWS CloudFormation Guard sintaks. Aturan penjaga mengambil bentuk umum berikut:

```
rule name when condition { assertion }
```

Di bawah ini adalah contoh aturan yang memeriksa untuk memastikan bahwa lapisan tidak diatur ke versi lapisan lama:

```
rule desiredlayer when configuration.layers != empty {  
    some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn  
}
```

Mari kita pahami sintaks aturan dan struktur:

- Nama aturan: Nama aturan dalam contoh yang diberikan adalah `desiredlayer`.
- Kondisi: Klausul ini menentukan kondisi di mana aturan harus diperiksa. Dalam contoh yang diberikan, kondisinya adalah `configuration.layers != empty`. Ini berarti sumber daya harus dievaluasi hanya ketika `layers` properti dalam konfigurasi tidak kosong.
- Pernyataan: Setelah `when` klausa, pernyataan menentukan apa yang diperiksa aturan. Pernyataan `some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn` memeriksa apakah ada ARN layer Lambda yang tidak cocok dengan nilainya. `OldLayerArn` Jika mereka tidak cocok, pernyataan itu benar dan aturan berlalu; jika tidak, itu gagal.

`CONFIG_RULE_PARAMETERS` adalah seperangkat parameter khusus yang dikonfigurasi dengan AWS Config aturan. Dalam hal ini, `OldLayerArn` adalah parameter di dalamnya `CONFIG_RULE_PARAMETERS`. Ini memungkinkan pengguna untuk memberikan nilai ARN tertentu yang mereka anggap lama atau tidak digunakan lagi, dan kemudian aturan memeriksa apakah ada fungsi Lambda yang menggunakan ARN lama ini.

Tahap 2: Visualisasikan dan desain

AWS Config mengumpulkan data konfigurasi dan menyimpan data tersebut di bucket Amazon Simple Storage Service (Amazon S3). Anda dapat menggunakan [Amazon Athena](#) untuk menanyakan data ini langsung dari bucket S3 Anda. Dengan Athena, Anda dapat menggabungkan data ini di tingkat organisasi, menghasilkan tampilan holistik dari konfigurasi sumber daya Anda di semua akun Anda. Untuk mengatur agregasi data konfigurasi sumber daya, lihat [Memvisualisasikan AWS Config data menggunakan Athena dan QuickSight Amazon](#) di blog Operasi dan AWS Manajemen Cloud.

Berikut ini adalah contoh query Athena untuk mengidentifikasi semua fungsi Lambda menggunakan ARN lapisan tertentu:

```
WITH unnested AS (  
  SELECT  
    item.awsaccountid AS account_id,  
    item.awsregion AS region,  
    item.configuration AS lambda_configuration,  
    item.resourceid AS resourceid,  
    item.resourcename AS resourcename,  
    item.configuration AS configuration,  
    json_parse(item.configuration) AS lambda_json  
  FROM  
    default.aws_config_configuration_snapshot,  
    UNNEST(configurationitems) as t(item)  
  WHERE  
    "dt" = 'latest'  
    AND item.resourcetype = 'AWS::Lambda::Function'  
)  
  
SELECT DISTINCT  
  region as Region,  
  resourcename as FunctionName,  
  json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,  
  json_extract_scalar(lambda_json, '$.timeout') AS timeout,  
  json_extract_scalar(lambda_json, '$.version') AS version  
FROM  
  unnested  
WHERE  
  lambda_configuration LIKE '%arn:aws:lambda:us-  
east-1:111122223333:layer:AnyGovernanceLayer:24%'
```

Berikut adalah hasil dari kueri:

Query results | Query stats

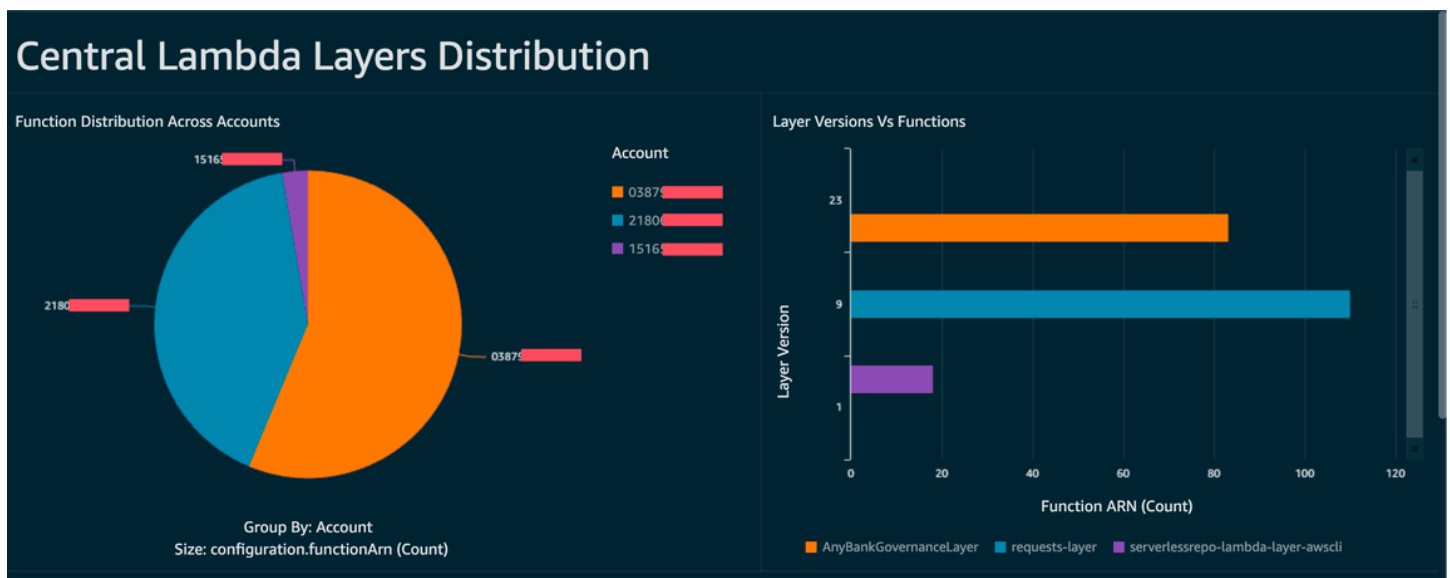
Completed Time in queue: 127 ms Run time: 1.803 sec Data scanned: 239.40 KB

Results (27) Copy Download results

Search rows

| # | Region | FunctionName | memory_size | timeout | version |
|---|-----------|--|-------------|---------|----------|
| 1 | us-east-1 | UpdateUIForPublishEvents | 128 | 18 | \$LATEST |
| 2 | us-east-1 | SchedulerCLI-InstanceSchedulerMain | 128 | 300 | \$LATEST |
| 3 | us-east-1 | my_functions_function10 | 128 | 3 | \$LATEST |
| 4 | us-east-1 | lex-web-ui-CognitoidentityP-CleanStackNameFunction-1TSORSH6L6YXQ | 128 | 300 | \$LATEST |
| 5 | us-east-1 | GetLatestArn | 128 | 3 | \$LATEST |
| 6 | us-east-1 | aws-python-http-api-project-dev-hello | 1024 | 6 | \$LATEST |
| 7 | us-east-1 | cloud9-MyTest-MyTest-688JGPVYP37L | 128 | 15 | \$LATEST |
| 8 | us-east-1 | my_functions_function1 | 128 | 3 | \$LATEST |
| 9 | us-east-1 | my_functions_function25 | 128 | 3 | \$LATEST |

Dengan AWS Config data yang dikumpulkan di seluruh organisasi, Anda kemudian dapat membuat dasbor menggunakan [Amazon QuickSight](#). Dengan mengimpor hasil Athena Anda ke QuickSight Amazon, Anda dapat memvisualisasikan seberapa baik fungsi Lambda Anda mematuhi aturan versi lapisan. [Dasbor ini dapat menyoroti sumber daya yang sesuai dan tidak sesuai, yang membantu Anda menentukan kebijakan penegakan hukum Anda, sebagaimana diuraikan di bagian berikutnya.](#) Gambar berikut adalah contoh dasbor yang melaporkan distribusi versi lapisan yang diterapkan pada fungsi dalam organisasi.



Tahap 3: Menerapkan dan menegakkan

Anda sekarang dapat secara opsional memasang aturan versi lapisan yang Anda buat di [fase 1](#) dengan tindakan remediasi melalui dokumen otomatisasi Systems Manager, yang Anda buat sebagai skrip Python yang ditulis dengan `AWS SDK for Python (Boto3)` Skrip memanggil tindakan

API [UpdateFunctionKonfigurasi](#) untuk setiap fungsi Lambda, memperbarui konfigurasi fungsi dengan lapisan ARN baru. Atau, Anda dapat meminta skrip mengirimkan permintaan tarik ke repositori kode untuk memperbarui lapisan ARN. Dengan cara ini penerapan kode future juga diperbarui dengan ARN lapisan yang benar.

Penandatanganan kode Lambda dengan AWS Signer

[AWS Signer](#) adalah layanan penandatanganan kode yang dikelola sepenuhnya yang memungkinkan Anda memvalidasi kode Anda terhadap tanda tangan digital untuk mengonfirmasi bahwa kode tidak berubah dan dari penerbit tepercaya. AWS Signer dapat digunakan bersama dengan AWS Lambda untuk memverifikasi bahwa fungsi dan lapisan tidak berubah sebelum penerapan ke lingkungan Anda. AWS Ini melindungi organisasi Anda dari pelaku jahat yang mungkin telah memperoleh kredensi untuk membuat fungsi baru atau memperbarui fungsi yang ada.

Untuk menyiapkan penandatanganan kode untuk fungsi Lambda Anda, mulailah dengan membuat bucket S3 dengan mengaktifkan versi. Setelah itu, buat profil penandatanganan dengan AWS Signer, tentukan Lambda sebagai platform dan kemudian tentukan periode hari di mana profil penandatanganan valid. Contoh:

```
Signer:
  Type: AWS::Signer::SigningProfile
  Properties:
    PlatformId: AWSLambda-SHA384-ECDSA
    SignatureValidityPeriod:
      Type: DAYS
      Value: !Ref pValidDays
```

Kemudian gunakan profil penandatanganan dan buat konfigurasi penandatanganan dengan Lambda. Anda harus menentukan apa yang harus dilakukan ketika konfigurasi penandatanganan melihat artefak yang tidak cocok dengan tanda tangan digital yang diharapkan: peringatkan (tetapi izinkan penerapan) atau terapkan (dan blokir penerapan). Contoh di bawah ini dikonfigurasi untuk menegakkan dan memblokir penerapan.

```
SigningConfig:
  Type: AWS::Lambda::CodeSigningConfig
  Properties:
    AllowedPublishers:
      SigningProfileVersionArns:
        - !GetAtt Signer.ProfileVersionArn
    CodeSigningPolicies:
      UntrustedArtifactOnDeployment: Enforce
```

Anda sekarang telah AWS Signer mengonfigurasi dengan Lambda untuk memblokir penerapan yang tidak tepercaya. Mari kita asumsikan Anda telah selesai mengkodekan permintaan fitur dan

sekarang siap untuk menerapkan fungsi. Langkah pertama adalah mem-zip kode dengan dependensi yang sesuai dan kemudian menandatangani artefak menggunakan profil penandatanganan yang Anda buat. Anda dapat melakukan ini dengan mengunggah artefak zip ke bucket S3 dan kemudian memulai pekerjaan penandatanganan.

```
aws signer start-signing-job \
--source 's3={bucketName=your-versioned-bucket,key=your-prefix/your-zip-artifact.zip,version=QyaJ3c4qa50LXV.9VaZgXHlsGbvCXpT}' \
--destination 's3={bucketName=your-versioned-bucket,prefix=your-prefix/}' \
--profile-name your-signer-id
```

Anda mendapatkan output sebagai berikut, di mana `jobId` adalah objek yang dibuat di bucket tujuan dan awalan dan `jobOwner` merupakan Akun AWS ID 12 digit tempat pekerjaan dijalankan.

```
{
  "jobId": "87a3522b-5c0b-4d7d-b4e0-4255a8e05388",
  "jobOwner": "111122223333"
}
```

Dan sekarang Anda dapat menerapkan fungsi Anda menggunakan objek S3 yang ditandatangani dan konfigurasi penandatanganan kode yang Anda buat.

```
Fn:
  Type: AWS::Serverless::Function
  Properties:
    CodeUri: s3://your-versioned-bucket/your-prefix/87a3522b-5c0b-4d7d-
b4e0-4255a8e05388.zip
    Handler: fn.handler
    Role: !GetAtt FnRole.Arn
    CodeSigningConfigArn: !Ref pSigningConfigArn
```

Sebagai alternatif, Anda dapat menguji penerapan fungsi dengan artefak zip sumber asli yang tidak ditandatangani. Penerapan akan gagal dengan pesan berikut:

```
Lambda cannot deploy the function. The function or layer might be signed using a
signature that the client is not configured to accept. Check the provided signature
for unsigned.
```

Jika Anda membangun dan menerapkan fungsi Anda menggunakan AWS Serverless Application Model (AWS SAM), perintah paket menangani pengunggahan artefak zip ke S3 dan juga memulai

pekerjaan penandatanganan dan mendapatkan artefak yang ditandatangani. Anda dapat melakukan ini dengan perintah dan parameter berikut:

```
aws s3 cp --recursive --acl public-read --signature-version s3sigv4 \
  --output-template-file your-output.yaml \
  --s3-bucket your-versioned-bucket \
  --s3-prefix your-prefix \
  --signing-profiles your-signer-id
```

AWS Signer membantu Anda memverifikasi bahwa artefak zip yang disebarkan ke akun Anda dipercaya untuk digunakan. Anda dapat menyertakan proses di atas dalam pipeline CI/CD Anda dan mengharuskan semua fungsi memiliki konfigurasi penandatanganan kode yang dilampirkan menggunakan teknik yang diuraikan dalam topik sebelumnya. Dengan menggunakan penandatanganan kode dengan penerapan fungsi Lambda, Anda mencegah pelaku jahat yang mungkin mendapatkan kredensi untuk membuat atau memperbarui fungsi agar tidak menyuntikkan kode berbahaya ke dalam fungsi Anda.

Otomatiskan penilaian keamanan untuk Lambda dengan Amazon Inspector

[Amazon Inspector](#) adalah layanan manajemen kerentanan yang terus-menerus memindai beban kerja untuk kerentanan perangkat lunak yang diketahui dan paparan jaringan yang tidak diinginkan. Amazon Inspector membuat temuan yang menjelaskan kerentanan, mengidentifikasi sumber daya yang terpengaruh, menilai tingkat keparahan kerentanan, dan memberikan panduan remediasi.

Dukungan Amazon Inspector menyediakan penilaian kerentanan keamanan otomatis yang berkelanjutan untuk fungsi dan lapisan Lambda. Amazon Inspector menyediakan dua jenis pemindaian untuk Lambda:

- Pemindaian standar Lambda (default): Memindai [dependensi aplikasi dalam fungsi Lambda dan lapisannya untuk kerentanan paket](#).
- Pemindaian kode Lambda: Memindai [kode aplikasi khusus di fungsi dan lapisan Anda untuk mencari kerentanan kode](#). Anda dapat mengaktifkan pemindaian standar Lambda atau mengaktifkan pemindaian standar Lambda bersama dengan pemindaian kode Lambda.

Untuk mengaktifkan Amazon Inspector, navigasikan ke konsol [Amazon Inspector](#), perluas bagian Pengaturan, dan pilih Manajemen Akun. Pada tab Akun, pilih Aktifkan, lalu pilih salah satu opsi pemindaian.

Anda dapat mengaktifkan Amazon Inspector untuk beberapa akun dan mendelegasikan izin untuk mengelola Amazon Inspector bagi organisasi ke akun tertentu saat menyiapkan Amazon Inspector. Saat mengaktifkan, Anda perlu memberikan izin Amazon Inspector dengan membuat peran: `AWSServiceRoleForAmazonInspector2`. Konsol Amazon Inspector memungkinkan Anda membuat peran ini menggunakan opsi sekali klik.

Untuk pemindaian standar Lambda, Amazon Inspector memulai pemindaian kerentanan fungsi Lambda dalam situasi berikut:

- Segera setelah Amazon Inspector menemukan fungsi Lambda yang ada.
- Saat Anda menerapkan fungsi Lambda baru.
- Saat Anda menerapkan pembaruan ke kode aplikasi atau dependensi fungsi Lambda yang ada atau lapisannya.
- Setiap kali Amazon Inspector menambahkan item common vulnerabilities and exposure (CVE) baru ke database-nya, dan CVE tersebut relevan dengan fungsi Anda.

Untuk pemindaian kode Lambda, Amazon Inspector mengevaluasi kode aplikasi fungsi Lambda Anda menggunakan penalaran otomatis dan pembelajaran mesin yang menganalisis kode aplikasi Anda untuk kepatuhan keamanan secara keseluruhan. Jika Amazon Inspector mendeteksi kerentanan dalam kode aplikasi fungsi Lambda Anda, Amazon Inspector menghasilkan temuan Kerentanan Kode yang terperinci. Untuk daftar kemungkinan deteksi, lihat [Perpustakaan CodeGuru Detektor Amazon](#).

Untuk melihat temuannya, buka konsol [Amazon Inspector](#). Pada menu Temuan, pilih Dengan fungsi Lambda untuk menampilkan hasil pemindaian keamanan yang dilakukan pada fungsi Lambda.

Untuk mengecualikan fungsi Lambda dari pemindaian standar, beri tag fungsi dengan pasangan kunci-nilai berikut:

- `Key:InspectorExclusion`
- `Value:LambdaStandardScanning`

Untuk mengecualikan fungsi Lambda dari pemindaian kode, beri tag fungsi dengan pasangan kunci-nilai berikut:

- `Key:InspectorCodeExclusion`
- `Value:LambdaCodeScanning`

Misalnya, seperti yang ditunjukkan pada gambar berikut, Amazon Inspector secara otomatis mendeteksi kerentanan dan mengategorikan temuan tipe Kerentanan Kode, yang menunjukkan bahwa kerentanan ada dalam kode fungsi, dan bukan di salah satu pustaka yang bergantung pada kode. Anda dapat memeriksa detail ini untuk fungsi tertentu atau beberapa fungsi sekaligus.

Findings (2)

Choose a row to view the finding details. All findings are related to this instance.

Active

Resource ID *EQUALS* `arn:aws:lambda:us-east-1:.....function:code_scanning_python:$LATEST`

< 1 >

| | Severity | Title | Type | Age | Status |
|-----------------------|----------|---|--------------------|------------|--------|
| <input type="radio"/> | High | CWE-200 - Insecure Socket Bind | Code Vulnerability | 10 minutes | Active |
| <input type="radio"/> | High | Overriding environment variables that are res | Code Vulnerability | 10 minutes | Active |

Anda dapat menyelam lebih jauh ke dalam masing-masing temuan ini dan belajar bagaimana memperbaiki masalah tersebut.

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior.



Finding ID: [arn:aws:inspector2:us-east-1: \[REDACTED\]:finding/\[REDACTED\]](#)

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior or failure of the Lambda function.

Finding overview

| | |
|---------------------------------|---|
| AWS account ID | [REDACTED] |
| Severity | High |
| Type | Code Vulnerability |
| Detector name ↗ | Override of reserved variable names in a Lambda function |
| Relevant CWE ↗ | -- |
| Rule ID ↗ | Rule-434311 |
| Detector tags | #availability, #aws-python-sdk, #aws-lambda, #data-integrity, #maintainability, #security, #security-context, #python |
| Fix available | Yes |
| Created at | March 29, 2023 10:08 AM (UTC-04:00) |

Vulnerability details

File path `lambda_function.py`

Vulnerability location

```

3 import socket
4
5 def lambda_handler(event, context):
6
7     # print("Scenario 1");
8     os.environ['_HANDLER'] = 'hello'
9     # print("Scenario 1 ends")
10
11     # print("Scenario 2");
12     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
13     s.bind(('',0))

```

Suggested remediation

Your code attempts to override an environment variable that is reserved by the Lambda runtime environment. This can lead to unexpected behavior and might break the execution of your Lambda function.

Saat bekerja dengan fungsi Lambda Anda, pastikan Anda mematuhi konvensi penamaan untuk fungsi Lambda Anda. Untuk informasi selengkapnya, lihat [Gunakan variabel lingkungan Lambda untuk mengonfigurasi nilai dalam kode](#).

Anda bertanggung jawab atas saran remediasi yang Anda terima. Selalu tinjau saran remediasi sebelum menerimanya. Anda mungkin perlu mengedit saran remediasi untuk memastikan bahwa kode Anda melakukan apa yang Anda inginkan.

Menerapkan observabilitas untuk keamanan dan kepatuhan Lambda

AWS Config adalah alat yang berguna untuk menemukan dan memperbaiki sumber daya Tanpa AWS Server yang tidak sesuai. Setiap perubahan yang Anda buat pada sumber daya tanpa server Anda dicatat. AWS Config Selain itu, AWS Config memungkinkan Anda untuk menyimpan data snapshot konfigurasi pada S3. Anda dapat menggunakan Amazon Athena dan Amazon QuickSight untuk membuat dashboard dan melihat data. AWS Config Pada tahun [Mendeteksi penerapan dan konfigurasi Lambda yang tidak sesuai dengan AWS Config](#), kita membahas bagaimana kita dapat memvisualisasikan konfigurasi tertentu seperti lapisan Lambda. Topik ini memperluas konsep-konsep ini.

Visibilitas ke konfigurasi Lambda

Anda dapat menggunakan kueri untuk menarik konfigurasi penting seperti Akun AWS ID, Wilayah, konfigurasi AWS X-Ray penelusuran, VPC konfigurasi, ukuran memori, runtime, dan tag. Berikut adalah contoh kueri yang dapat Anda gunakan untuk menarik informasi ini dari Athena:

```
WITH unnested AS (  
  SELECT  
    item.awsaccountid AS account_id,  
    item.awsregion AS region,  
    item.configuration AS lambda_configuration,  
    item.resourceid AS resourceid,  
    item.resourcename AS resourcename,  
    item.configuration AS configuration,  
    json_parse(item.configuration) AS lambda_json  
  FROM  
    default.aws_config_configuration_snapshot,  
    UNNEST(configurationitems) as t(item)  
  WHERE  
    "dt" = 'latest'  
    AND item.resourcetype = 'AWS::Lambda::Function'  
)  
  
SELECT DISTINCT  
  account_id,  
  tags,  
  region as Region,  
  resourcename as FunctionName,  
  json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,  
  json_extract_scalar(lambda_json, '$.timeout') AS timeout,  
  json_extract_scalar(lambda_json, '$.runtime') AS version
```



```

json_extract_scalar(lambda_json, '$.vpcConfig.SubnetIds') AS vpcConfig
json_extract_scalar(lambda_json, '$.tracingConfig.mode') AS tracingConfig
FROM
unnested

```

Anda dapat menggunakan kueri untuk membuat QuickSight dasbor Amazon dan memvisualisasikan data. Untuk menggabungkan data konfigurasi AWS sumber daya, membuat tabel di Athena, dan membuat dasbor QuickSight Amazon pada data dari Athena, lihat [Memvisualisasikan data AWS Config menggunakan Athena dan Amazon QuickSight di blog Operasi dan Manajemen Cloud](#). AWS Khususnya, kueri ini juga mengambil informasi tag untuk fungsi. Ini memungkinkan wawasan yang lebih dalam tentang beban kerja dan lingkungan Anda, terutama jika Anda menggunakan tag khusus.



Untuk informasi selengkapnya tentang tindakan yang dapat Anda lakukan, lihat [Mengatasi temuan observabilitas](#) bagian nanti dalam topik ini.

Visibilitas ke kepatuhan Lambda

Dengan data yang dihasilkan AWS Config, Anda dapat membuat dasbor tingkat organisasi untuk memantau kepatuhan. Hal ini memungkinkan pelacakan dan pemantauan yang konsisten terhadap:

- Paket kepatuhan berdasarkan skor kepatuhan

- Aturan oleh sumber daya yang tidak sesuai
- Status kepatuhan

AWS Config ×

[Dashboard](#)

[Conformance packs](#)

[Rules](#)

[Resources](#)

▼ [Aggregators](#)

- [Conformance packs](#)
- [Rules](#)
- [Resources](#)
- [Authorizations](#)

[Advanced queries](#)

[Settings](#)

[What's new](#)

[Documentation](#) ↗

[Partners](#) ↗

[FAQs](#) ↗

[Pricing](#) ↗

[AWS Config](#) > [Dashboard](#)

Dashboard

Conformance Packs by Compliance Score

| Conformance pack | Compliance score |
|----------------------|--|
| MyNewConformancePack | <div style="display: flex; align-items: center;"> <div style="flex-grow: 1; border: 1px solid #ccc; background-color: #e0e0e0; position: relative;"> <div style="background-color: #0070c0; width: 37%; height: 10px;"></div> </div> 37% </div> |

Compliance status

| Rules | Resources |
|---|---|
| ⚠ 6 Noncompliant rule(s) ✔ 7 Compliant rule(s) | ⚠ 100+ Noncompliant resource(s) ✔ 82 Compliant resource(s) |

Noncompliant rules by noncompliant resource count

| Name | Compliance |
|---|---|
| lambda-function-settings-ch... | ⚠ 25+ Noncompliant resource(s) |
| lambda-dlq-check-conforma... | ⚠ 25+ Noncompliant resource(s) |
| lambda-inside-vpc-conforma... | ⚠ 25+ Noncompliant resource(s) |
| lambda-vpc-multi-az-check-... | ⚠ 25+ Noncompliant resource(s) |
| lambda-function-settings-ch... | ⚠ 14 Noncompliant resource(s) |
| View all noncompliant rules | |

Periksa setiap aturan untuk mengidentifikasi sumber daya yang tidak sesuai untuk aturan itu. Misalnya, jika organisasi Anda mengamankan bahwa semua fungsi Lambda harus dikaitkan dengan VPC dan jika Anda telah menerapkan AWS Config aturan untuk mengidentifikasi kepatuhan, Anda dapat memilih aturan dalam daftar di `lambda-inside-vpc` atas.

Resources in scope

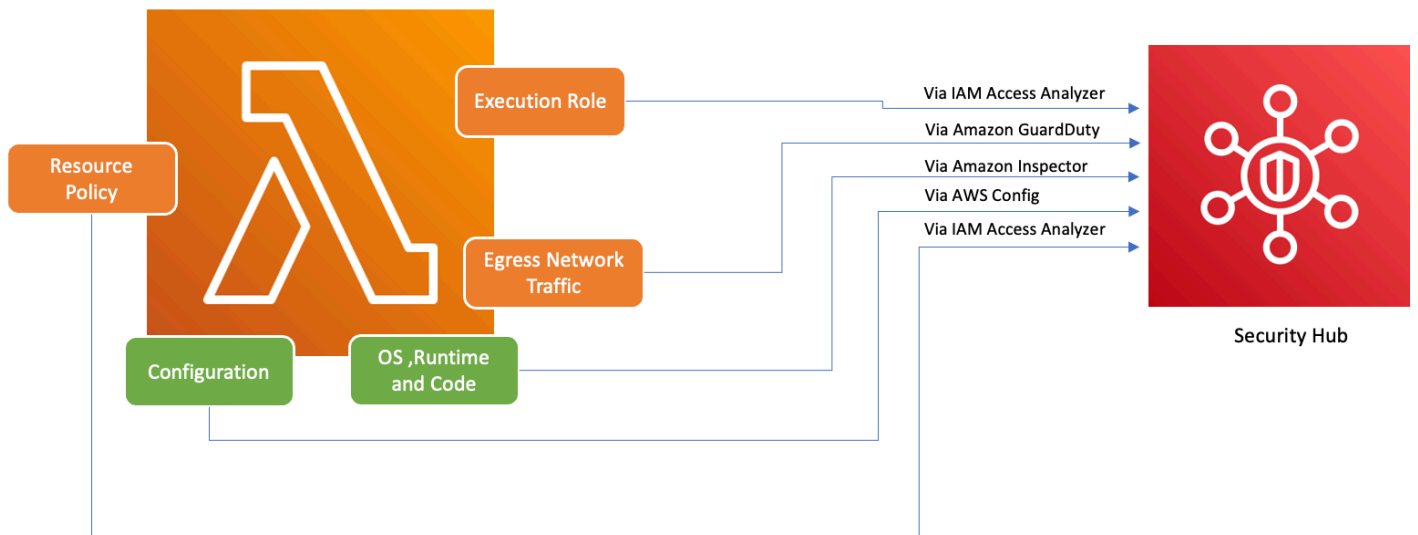
All

- All
- Compliant
- Noncompliant

| | Type | Annotation | Compliance |
|---|-----------------|--|----------------|
| <input type="radio"/> my_functions_function44 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function46 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function47 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function49 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function50 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function6 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function7 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> my_functions_function8 | Lambda Function | - | ✔ Compliant |
| <input type="radio"/> ConfigQueryLambda | Lambda Function | This AWS Lambda function is not in ... | ⚠ Noncompliant |
| <input type="radio"/> DormamuLambda | Lambda Function | This AWS Lambda function is not in ... | ⚠ Noncompliant |

Untuk informasi lebih lanjut tentang tindakan yang dapat Anda lakukan, lihat [Mengatasi temuan observabilitas](#) bagian di bawah ini.

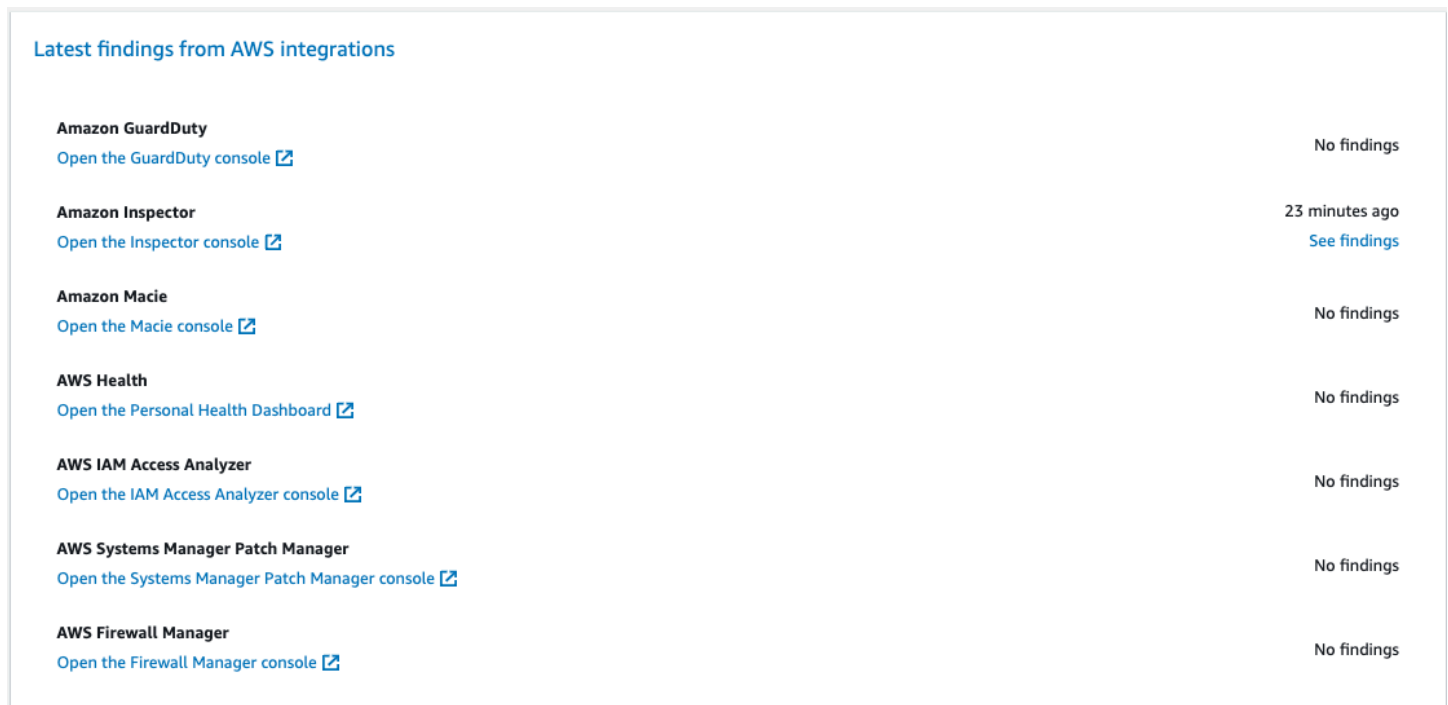
Visibilitas ke batas fungsi Lambda menggunakan Security Hub



Untuk memastikan bahwa AWS layanan termasuk Lambda digunakan dengan aman, AWS memperkenalkan Praktik Terbaik Keamanan Dasar v1.0.0. Serangkaian praktik terbaik ini memberikan pedoman yang jelas untuk mengamankan sumber daya dan data di AWS lingkungan, menekankan pentingnya mempertahankan postur keamanan yang kuat. Ini AWS Security Hub melengkapi ini dengan menawarkan pusat keamanan dan kepatuhan terpadu. Ini mengumpulkan,

mengatur, dan memprioritaskan temuan keamanan dari berbagai layanan seperti AWS Amazon Inspector,, dan Amazon. AWS Identity and Access Management Access Analyzer GuardDuty

Jika Anda memiliki Security Hub, Amazon Inspector, IAM Access Analyzer, dan GuardDuty diaktifkan dalam AWS organisasi Anda, Security Hub secara otomatis mengumpulkan temuan dari layanan ini. Misalnya, mari kita pertimbangkan Amazon Inspector. Menggunakan Security Hub, Anda dapat secara efisien mengidentifikasi kerentanan kode dan paket dalam fungsi Lambda. Di konsol Security Hub, navigasikan ke bagian bawah berlabel Temuan terbaru dari AWS integrasi. Di sini, Anda dapat melihat dan menganalisis temuan yang bersumber dari berbagai AWS layanan terintegrasi.



The screenshot displays a table titled "Latest findings from AWS integrations" with the following data:

| Service | Findings Status |
|---|--|
| Amazon GuardDuty Open the GuardDuty console | No findings |
| Amazon Inspector Open the Inspector console | 23 minutes ago See findings |
| Amazon Macie Open the Macie console | No findings |
| AWS Health Open the Personal Health Dashboard | No findings |
| AWS IAM Access Analyzer Open the IAM Access Analyzer console | No findings |
| AWS Systems Manager Patch Manager Open the Systems Manager Patch Manager console | No findings |
| AWS Firewall Manager Open the Firewall Manager console | No findings |

Untuk melihat detailnya, pilih tautan Lihat temuan di kolom kedua. Ini menampilkan daftar temuan yang disaring berdasarkan produk, seperti Amazon Inspector. Untuk membatasi pencarian Anda ke fungsi Lambda, setel Resource Type ke. AwsLambdaFunction Ini menampilkan temuan dari Amazon Inspector terkait dengan fungsi Lambda.

Security Hub > Findings

Findings (20+) Actions Workflow status Create insight

A finding is a security issue or a failed security check.

Q Add filter

Product name is Inspector X Resource type is AwsLambdaFunction X Workflow status is NEW X Workflow status is NOTIFIED X Record state is ACTIVE X Clear filters

< 1 ... >

| <input type="checkbox"/> | Severity | Workflow status | Record State | Region | Account Id | Company | Product | Title | Resource | Compliance Status | Updated at |
|--------------------------|----------|-----------------|--------------|-----------|------------|---------|-----------|-------------------------|-----------------------------|-------------------|----------------|
| <input type="checkbox"/> | HIGH | NEW | ACTIVE | us-east-1 | 218 | Amazon | Inspector | CWE-117 - Log injection | Lambda Function \$LATEST | | 27 minutes ago |
| <input type="checkbox"/> | HIGH | NEW | ACTIVE | us-east-1 | 218 | Amazon | Inspector | CWE-117 - Log injection | Lambda Function \$LATEST | | 27 minutes ago |
| <input type="checkbox"/> | HIGH | NEW | ACTIVE | us-east-1 | 218 | Amazon | Inspector | CWE-117 - Log injection | Lambda Function \$LATEST | | 27 minutes ago |
| <input type="checkbox"/> | HIGH | NEW | ACTIVE | us-east-1 | 218 | Amazon | Inspector | CWE-117 - Log injection | Lambda Function \$LATEST | | 27 minutes ago |

Untuk GuardDuty, Anda dapat mengidentifikasi pola lalu lintas jaringan yang mencurigakan. Anomali semacam itu mungkin menunjukkan adanya kode yang berpotensi berbahaya dalam fungsi Lambda Anda.

Dengan IAM Access Analyzer, Anda dapat memeriksa kebijakan, terutama kebijakan dengan pernyataan kondisi yang memberikan akses fungsi ke entitas eksternal. Selain itu, IAM Access Analyzer mengevaluasi izin yang ditetapkan saat menggunakan [AddPermission](#) operasi di Lambda bersama file. API EventSourceToken

Mengatasi temuan observabilitas

Mengingat konfigurasi luas yang mungkin untuk fungsi Lambda dan persyaratannya yang berbeda, solusi otomatisasi standar untuk remediasi mungkin tidak sesuai dengan setiap situasi. Selain itu, perubahan diterapkan secara berbeda di berbagai lingkungan. Jika Anda menemukan konfigurasi apa pun yang tampaknya tidak sesuai, pertimbangkan pedoman berikut:

1. Strategi penandaan

Kami merekomendasikan untuk menerapkan strategi penandaan yang komprehensif. Setiap fungsi Lambda harus ditandai dengan informasi kunci seperti:

- Pemilik: Orang atau tim yang bertanggung jawab atas fungsi tersebut.
- Lingkungan: Produksi, pementasan, pengembangan, atau kotak pasir.

- Aplikasi: Konteks yang lebih luas di mana fungsi ini berada, jika berlaku.

2. Penjangkauan pemilik

Alih-alih mengotomatiskan perubahan yang melanggar (seperti penyesuaian VPC konfigurasi), secara proaktif hubungi pemilik fungsi yang tidak sesuai (diidentifikasi oleh tag pemilik) dengan memberi mereka waktu yang cukup untuk:

- Sesuaikan konfigurasi yang tidak sesuai pada fungsi Lambda.
- Memberikan penjelasan dan meminta pengecualian, atau menyempurnakan standar kepatuhan.

3. Pertahankan database manajemen konfigurasi (CMDB)

Sementara tag dapat memberikan konteks langsung, mempertahankan terpusat CMDB dapat memberikan wawasan yang lebih dalam. Ini dapat menyimpan informasi yang lebih terperinci tentang setiap fungsi Lambda, dependensinya, dan metadata penting lainnya. A CMDB adalah sumber daya yang tak ternilai untuk audit, pemeriksaan kepatuhan, dan mengidentifikasi pemilik fungsi.

Karena lanskap infrastruktur tanpa server terus berkembang, penting untuk mengadopsi sikap proaktif terhadap pemantauan. Dengan alat seperti AWS Config, Security Hub, dan Amazon Inspector, kemungkinan anomali atau konfigurasi yang tidak sesuai dapat diidentifikasi dengan cepat. Namun, alat saja tidak dapat memastikan kepatuhan total atau konfigurasi optimal. Sangat penting untuk memasang alat-alat ini dengan proses dan praktik terbaik yang terdokumentasi dengan baik.

- Umpan balik loop: Setelah langkah-langkah remediasi dilakukan, pastikan ada loop umpan balik. Ini berarti meninjau kembali sumber daya yang tidak sesuai secara berkala untuk mengonfirmasi apakah sumber daya tersebut telah diperbarui atau masih berjalan dengan masalah yang sama.
- Dokumentasi: Selalu dokumentasikan pengamatan, tindakan yang diambil, dan pengecualian apa pun yang diberikan. Dokumentasi yang tepat tidak hanya membantu selama audit tetapi juga membantu dalam meningkatkan proses untuk kepatuhan dan keamanan yang lebih baik di masa depan.
- Pelatihan dan kesadaran: Memastikan bahwa semua pemangku kepentingan, terutama pemilik fungsi Lambda, secara teratur dilatih dan disadarkan akan praktik terbaik, kebijakan organisasi, dan mandat kepatuhan. Lokakarya reguler, webinar, atau sesi pelatihan dapat sangat membantu

dalam memastikan semua orang berada di halaman yang sama dalam hal keamanan dan kepatuhan.

Kesimpulannya, sementara alat dan teknologi memberikan kemampuan yang kuat untuk mendeteksi dan menandai masalah potensial, elemen manusia—pemahaman, komunikasi, pelatihan, dan dokumentasi—tetap penting. Bersama-sama, mereka membentuk kombinasi yang kuat untuk memastikan bahwa fungsi Lambda Anda dan infrastruktur yang lebih luas tetap sesuai, aman, dan dioptimalkan untuk kebutuhan bisnis Anda.

Validasi kepatuhan untuk AWS Lambda

Auditor pihak ketiga melakukan penilaian pada keamanan dan kepatuhan AWS Lambda sebagai bagian dari beberapa program kepatuhan AWS. Mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar layanan AWS dalam cakupan program kepatuhan khusus, lihat [Layanan AWS yang dicakup oleh program kepatuhan](#). Untuk informasi umum, lihat [Program kepatuhan AWS](#).

Anda bisa mengunduh laporan audit pihak ke tiga menggunakan AWS Artifact. Untuk informasi lebih lanjut, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Lambda ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. Anda dapat menerapkan kontrol tata kelola untuk memastikan bahwa fungsi Lambda perusahaan Anda memenuhi persyaratan kepatuhan Anda. Lihat informasi yang lebih lengkap di [Buat strategi tata kelola untuk fungsi dan lapisan Lambda](#).

Ketahanan di AWS Lambda

Infrastruktur global AWS dibangun di sekitar Wilayah dan Availability Zone AWS. AWS Kawasan menyediakan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang tersambung dengan jejaring jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripada infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [AWS Infrastruktur Global](#).

Selain infrastruktur global AWS, Lambda menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

- Versioning – Anda dapat menggunakan versioning di Lambda untuk menyimpan kode dan konfigurasi fungsi saat Anda mengembangkannya. Bersama dengan alias, Anda dapat menggunakan versioning untuk melakukan deployment blue/green dan rolling. Untuk detailnya, lihat [Kelola versi fungsi Lambda](#).

- **Penskalaan** – Ketika fungsi Anda menerima permintaan saat sedang memproses permintaan sebelumnya, Lambda meluncurkan instans lain dari fungsi Anda untuk menangani peningkatan beban. Lambda secara otomatis menyesuaikan skala untuk menangani 1.000 eksekusi bersamaan per Wilayah, dan [kuota](#) ini dapat ditingkatkan jika diperlukan. Untuk detailnya, lihat [Memahami penskalaan fungsi Lambda](#).
- **Ketersediaan tinggi** – Lambda menjalankan fungsi Anda di beberapa Availability Zone guna memastikannya tersedia untuk memproses kejadian jika terjadi gangguan layanan dalam satu zona. Jika Anda mengonfigurasi fungsi Anda agar terhubung ke virtual private cloud (VPC) di akun Anda, tentukan subnet di beberapa Availability Zone untuk memastikan ketersediaan yang tinggi. Untuk detailnya, lihat [Memberikan fungsi Lambda akses ke sumber daya di Amazon VPC](#).
- **Konkurensi cadangan** – Untuk memastikan bahwa fungsi Anda dapat selalu menskalakan untuk menangani permintaan tambahan, Anda dapat mencadangkan konkurensi untuk hal itu. Menetapkan konkurensi cadangan untuk suatu fungsi memastikan bahwa fungsi dapat menskalakan ke, tetapi tidak melebihi, jumlah invokasi bersamaan yang ditentukan. Hal ini memastikan bahwa Anda tidak kehilangan permintaan karena fungsi lain menggunakan semua konkurensi yang tersedia. Untuk detailnya, lihat [Mengkonfigurasi konkurensi cadangan untuk suatu fungsi](#).
- **Percobaan ulang** – Untuk invokasi asinkron dan subset invokasi yang dipicu oleh layanan lain, Lambda secara otomatis melakukan percobaan ulang terkait kesalahan dengan penundaan di antara percobaan. Klien dan layanan AWS lainnya yang memanggil fungsi secara sinkron bertanggung jawab untuk melakukan percobaan ulang. Untuk detailnya, lihat [Memahami perilaku coba lagi di Lambda](#).
- **Antrean surat mati** – Untuk invokasi asinkron, Anda dapat mengonfigurasi Lambda agar mengirim permintaan ke antrean surat gagal jika semua percobaan ulang gagal. Antrean surat mati adalah topik Amazon SNS atau antrean Amazon SQS yang menerima kejadian untuk pemecahan masalah atau pemrosesan ulang. Untuk detailnya, lihat [Menambahkan antrian huruf mati](#).

Keamanan infrastruktur di AWS Lambda

Sebagai layanan terkelola, AWS Lambda dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses Lambda melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Menggunakan penandatanganan kode untuk memverifikasi integritas kode dengan Lambda

Penandatanganan kode untuk AWS Lambda membantu memastikan bahwa hanya kode tepercaya yang berjalan di fungsi Lambda Anda. Saat Anda mengaktifkan penandatanganan kode untuk fungsi, Lambda memeriksa setiap deployment kode dan memverifikasi paket kode ditandatangani oleh sumber tepercaya.

Note

Fungsi yang ditentukan sebagai gambar kontainer tidak mendukung penandatanganan kode.

Untuk memverifikasi integrity kode, gunakan [AWS Signer](#) untuk membuat paket kode yang ditandatangani secara digital untuk fungsi dan lapisan. Saat pengguna mencoba men-deploy paket kode, Lambda melakukan pemeriksaan validasi pada paket kode sebelum menerima deployment. Karena pemeriksaan validasi penandatanganan kode berjalan pada waktu deployment, tidak ada dampak performa pada eksekusi fungsi.

Anda juga menggunakan AWS Penandatanganan untuk membuat profil penandatanganan. Anda menggunakan profil penandatanganan untuk membuat paket kode yang ditandatangani. Gunakan AWS Identity and Access Management (IAM) untuk mengontrol siapa yang dapat menandatangani

paket kode dan membuat profil penandatanganan. Untuk informasi selengkapnya, lihat [Autentikasi dan Kontrol Akses](#) dalam AWS Panduan Developer Signer.

Lapisan Lambda mengikuti format paket kode yang ditandatangani yang sama seperti paket kode fungsi. Saat Anda menambahkan lapisan ke fungsi yang telah mengaktifkan penandatanganan kode, Lambda memeriksa lapisan tersebut ditandatangani oleh profil penandatanganan yang diizinkan. Saat Anda mengaktifkan penandatanganan kode untuk fungsi, semua lapisan yang ditambahkan ke fungsi juga harus ditandatangani oleh salah satu profil penandatanganan yang diizinkan.

Anda dapat mengonfigurasi penandatanganan kode untuk mencatat perubahan ke AWS CloudTrail. Penerapan yang berhasil dan diblokir ke fungsi dicatat CloudTrail dengan informasi tentang tanda tangan dan pemeriksaan validasi.

Tidak ada biaya tambahan untuk menggunakan AWS Penandatanganan atau penandatanganan kode untuk AWS Lambda.

Validasi tanda tangan

Lambda melakukan pemeriksaan validasi berikut saat Anda men-deploy paket kode yang ditandatangani ke fungsi Anda:

1. Integrity – Memvalidasi paket kode belum dimodifikasi sejak ditandatangani. Lambda membandingkan hash paket dengan hash dari tanda tangan.
2. Expiry – Memvalidasi tanda tangan paket kode belum kedaluwarsa.
3. Mismatch – Memvalidasi paket kode ditandatangani dengan salah satu profil penandatanganan yang diizinkan untuk fungsi Lambda. Mismatch juga terjadi jika tanda tangan tidak ada.
4. Revocation – Memvalidasi tanda tangan paket kode belum dicabut.

Kebijakan validasi tanda tangan yang ditetapkan dalam konfigurasi penandatanganan kode menentukan tindakan mana yang diambil Lambda jika salah satu pemeriksaan validasi gagal:

- Warn – Lambda mengizinkan deployment paket kode, tetapi mengeluarkan peringatan. Lambda mengeluarkan CloudWatch metrik Amazon baru dan juga menyimpan peringatan di log. CloudTrail
- Enforce – Lambda mengeluarkan peringatan (sama seperti untuk tindakan Warn) dan memblokir deployment paket kode.

Anda dapat mengonfigurasi kebijakan untuk pemeriksaan validasi expiry, mismatch, dan revocation. Perhatikan bahwa Anda tidak dapat mengonfigurasi kebijakan untuk pemeriksaan integrity. Jika pemeriksaan integrity gagal, Lambda memblokir deployment.

Mengonfigurasi penandatanganan kode dengan Lambda API

Untuk mengelola konfigurasi penandatanganan kode dengan AWS CLI atau AWS SDK, gunakan API operasi berikut:

- [ListCodeSigningConfigs](#)
- [CreateCodeSigningConfig](#)
- [GetCodeSigningConfig](#)
- [UpdateCodeSigningConfig](#)
- [DeleteCodeSigningConfig](#)

Untuk mengelola konfigurasi penandatanganan kode untuk suatu fungsi, gunakan API operasi berikut:

- [CreateFunction](#)
- [GetFunctionCodeSigningConfig](#)
- [PutFunctionCodeSigningConfig](#)
- [DeleteFunctionCodeSigningConfig](#)
- [ListFunctionsByCodeSigningConfig](#)

Topik

- [Membuat konfigurasi penandatanganan kode untuk Lambda](#)
- [Memperbarui konfigurasi penandatanganan kode](#)
- [Mengonfigurasi IAM kebijakan untuk konfigurasi penandatanganan kode Lambda](#)

Membuat konfigurasi penandatanganan kode untuk Lambda

Untuk mengaktifkan penandatanganan kode untuk fungsi, Anda membuat konfigurasi penandatanganan kode dan melampirkannya ke fungsi. Konfigurasi penandatanganan kode

menetapkan daftar profil penandatanganan yang diizinkan dan tindakan kebijakan yang harus diambil jika pemeriksaan validasi gagal.

Bagian-bagian

- [Prasyarat konfigurasi](#)
- [Membuat konfigurasi penandatanganan kode](#)
- [Mengaktifkan penandatanganan kode untuk fungsi](#)

Prasyarat konfigurasi

Sebelum Anda dapat mengonfigurasi penandatanganan kode untuk fungsi Lambda, gunakan AWS Penandatanganan untuk melakukan hal berikut:

- Buat satu profil penandatanganan atau lebih.
- Gunakan profil penandatanganan untuk membuat paket kode yang ditandatangani untuk fungsi Anda.

Untuk informasi selengkapnya, lihat [Membuat Profil Penandatanganan \(Konsol\)](#) di AWS Panduan Developer Signer.

Membuat konfigurasi penandatanganan kode

Konfigurasi penandatanganan kode menetapkan daftar profil penandatanganan yang diizinkan dan kebijakan validasi tanda tangan.

Untuk membuat konfigurasi penandatanganan kode (konsol)

1. Buka [Halaman konfigurasi penandatanganan kode](#) di konsol Lambda.
2. Pilih Buat konfigurasi.
3. Untuk Deskripsi, masukkan nama deskriptif untuk konfigurasi.
4. Di bawah Profil penandatanganan, tambahkan hingga 20 profil penandatanganan ke konfigurasi.
 - a. Untuk Menandatangani versi profil ARN, pilih Amazon Resource Name (ARN) versi profil, atau masukkan ARN.
 - b. Untuk menambahkan profil penandatanganan tambahan, pilih Tambahkan profil penandatanganan.
5. Di bawah Kebijakan validasi tanda tangan, pilih Warn atau Enforce.

6. Pilih Buat konfigurasi.

Mengaktifkan penandatanganan kode untuk fungsi

Untuk mengaktifkan penandatanganan kode untuk fungsi, Anda mengaitkan konfigurasi penandatanganan kode dengan fungsi.

Untuk mengaitkan konfigurasi penandatanganan kode dengan fungsi (konsol)

1. Buka [Halaman fungsi](#) di konsol Lambda.
2. Pilih fungsi yang ingin Anda aktifkan penandatanganan kodenya.
3. Buka tab Konfigurasi.
4. Gulir ke bawah dan pilih Penandatanganan kode.
5. Pilih Edit.
6. Di Edit penandatanganan kode, pilih konfigurasi penandatanganan kode untuk fungsi ini.
7. Pilih Simpan.

Memperbarui konfigurasi penandatanganan kode

Saat Anda memperbarui [konfigurasi penandatanganan kode](#), perubahan akan memengaruhi penerapan fungsi di masa mendatang yang memiliki konfigurasi penandatanganan kode yang dilampirkan.

Untuk memperbarui konfigurasi penandatanganan kode (konsol)

1. Buka [Halaman konfigurasi penandatanganan kode](#) di konsol Lambda.
2. Pilih konfigurasi penandatanganan kode untuk diperbarui, lalu pilih Edit.
3. Untuk Deskripsi, masukkan nama deskriptif untuk konfigurasi.
4. Di bawah Profil penandatanganan, tambahkan hingga 20 profil penandatanganan ke konfigurasi.
 - a. Untuk Menandatangani versi profil ARN, pilih Amazon Resource Name (ARN) versi profil, atau masukkan ARN.
 - b. Untuk menambahkan profil penandatanganan tambahan, pilih Tambahkan profil penandatanganan.
5. Di bawah Kebijakan validasi tanda tangan, pilih Warn atau Enforce.

6. Pilih Simpan perubahan.

Mengonfigurasi IAM kebijakan untuk konfigurasi penandatanganan kode Lambda

Untuk memberikan izin bagi pengguna untuk mengakses [API operasi penandatanganan kode](#), lampirkan satu atau beberapa pernyataan kebijakan ke kebijakan pengguna. Untuk informasi selengkapnya tentang kebijakan pengguna, lihat [Kebijakan berbasis identitas IAM untuk Lambda](#).

Contoh pernyataan kebijakan berikut memberikan izin untuk membuat, memperbarui, dan mengambil konfigurasi penandatanganan kode.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:CreateCodeSigningConfig",
        "lambda:UpdateCodeSigningConfig",
        "lambda:GetCodeSigningConfig"
      ],
      "Resource": "*"
    }
  ]
}
```

Administrator dapat menggunakan kunci syarat `CodeSigningConfigArn` untuk menentukan konfigurasi penandatanganan kode yang harus digunakan developer untuk membuat atau memperbarui fungsi Anda.

Contoh pernyataan kebijakan berikut memberikan izin untuk membuat fungsi. Pernyataan kebijakan mencakup syarat `lambda:CodeSigningConfigArn` untuk menentukan konfigurasi penandatanganan kode yang diizinkan. Lambda memblokir `CreateFunction` API permintaan apa pun jika `CodeSigningConfigArn` parameternya hilang atau tidak cocok dengan nilai dalam kondisi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Sid": "AllowReferencingCodeSigningConfig",
"Effect": "Allow",
"Action": [
    "lambda:CreateFunction",
],
"Resource": "*",
"Condition": {
    "StringEquals": {
        "lambda:CodeSigningConfigArn":
            "arn:aws:lambda:us-west-2:123456789012:code-signing-
config:csc-0d4518bd353a0a7c6"
    }
}
]
```


Pemantauan dan pemecahan masalah fungsi Lambda

AWS Lambda terintegrasi dengan AWS layanan lain untuk membantu Anda memantau dan memecahkan masalah fungsi Lambda Anda. Lambda secara otomatis memantau fungsi Lambda atas nama Anda dan melaporkan metrik melalui Amazon CloudWatch. Untuk membantu Anda memantau kode ketika dijalankan, Lambda secara otomatis melacak jumlah permintaan, durasi invokasi per permintaan, dan jumlah permintaan yang menghasilkan kesalahan.

Anda dapat menggunakan AWS layanan lain untuk memecahkan masalah fungsi Lambda Anda. Bagian ini menjelaskan cara menggunakan layanan AWS ini untuk memantau, melacak, men-debug, dan memecahkan masalah fungsi dan aplikasi Lambda Anda. Untuk detail tentang pencatatan fungsi dan kesalahan di setiap runtime, lihat bagian runtime individual.

Untuk informasi selengkapnya tentang pemantauan aplikasi Lambda, lihat [Pemantauan dan pengamatan di Tanah Tanpa Server](#).

Bagian-bagian

- [Harga](#)
- [Lihat metrik untuk fungsi Lambda](#)
- [Menggunakan CloudWatch log Log dengan Lambda](#)
- [Logging panggilan AWS Lambda API menggunakan AWS CloudTrail](#)
- [Visualisasikan pemanggilan fungsi Lambda menggunakan AWS X-Ray](#)
- [Pantau kinerja fungsi dengan Amazon CloudWatch Lambda Insights](#)

Harga

CloudWatch memiliki tingkat bebas abadi. Di luar ambang batas tingkat gratis, CloudWatch biaya untuk metrik, dasbor, alarm, log, dan wawasan. Untuk informasi selengkapnya, lihat [CloudWatch harga Amazon](#).

Lihat metrik untuk fungsi Lambda

Saat AWS Lambda fungsi Anda selesai memproses peristiwa, Lambda mengirimkan metrik tentang pemanggilan ke Amazon. CloudWatch Tidak ada biaya untuk metrik ini.

Di CloudWatch konsol, Anda dapat membuat grafik dan dasbor dengan metrik ini. Anda dapat mengatur alarm untuk merespons perubahan dalam pemanfaatan, kinerja, atau tingkat kesalahan. Lambda mengirimkan data metrik ke CloudWatch dalam interval 1 menit. Untuk wawasan lebih cepat tentang fungsi Lambda Anda, Anda dapat membuat [metrik kustom](#) resolusi tinggi seperti yang dijelaskan di Tanah Tanpa Server. Biaya berlaku untuk metrik dan CloudWatch alarm khusus. Untuk informasi selengkapnya, lihat [CloudWatchHarga Amazon](#).

Halaman ini menjelaskan metrik pemanggilan, kinerja, dan konkurensi fungsi Lambda yang tersedia di konsol. CloudWatch

Bagian-bagian

- [Melihat metrik di konsol CloudWatch](#)
- [Tipe metrik](#)

Melihat metrik di konsol CloudWatch

Anda dapat menggunakan CloudWatch konsol untuk memfilter dan mengurutkan metrik fungsi berdasarkan nama fungsi, alias, atau versi.

Untuk melihat metrik di konsol CloudWatch

1. Buka [halaman Metrik](#) (AWS/Lambdamespace) konsol. CloudWatch
2. Pada tab Browse, di bawah Metrik, pilih salah satu dimensi berikut:
 - Menurut Nama Fungsi (FunctionName) – Lihat metrik gabungan untuk semua versi dan alias fungsi.
 - Menurut Sumber Daya (Resource) – Lihat metrik untuk versi atau alias fungsi.
 - Menurut Versi yang Dieksekusi (ExecutedVersion) – Lihat metrik untuk kombinasi alias dan versi. Gunakan dimensi ExecutedVersion untuk membandingkan tingkat kesalahan untuk dua versi fungsi yang keduanya adalah target [alias tertimbang](#).
 - Di Seluruh Fungsi (tidak ada) - Lihat metrik agregat untuk semua fungsi saat ini. Wilayah AWS
3. Pilih metrik, lalu pilih Tambahkan ke grafik atau opsi grafik lainnya.

Secara default, grafik menggunakan statistik Sum untuk semua metrik. Untuk memilih statistik yang berbeda dan menyesuaikan grafik, gunakan opsi pada tab Metrik bergrafik.

Note

Waktu yang tertera pada metrik mencerminkan saat fungsi diaktifkan. Tergantung pada durasi pemanggilan, ini bisa beberapa menit sebelum metrik dipancarkan. Misalnya, jika fungsi Anda memiliki batas waktu 10 menit, lihat lebih dari 10 menit sebelumnya untuk metrik yang akurat.

Untuk informasi selengkapnya CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).

Tipe metrik

Bagian berikut menjelaskan jenis metrik Lambda yang tersedia di konsol. CloudWatch

Metrik invokasi

Metrik pemanggilan adalah indikator biner dari hasil pemanggilan fungsi Lambda. Misalnya, jika fungsi mengembalikan kesalahan, maka Lambda mengirimkan `Errors` metrik dengan nilai 1. Untuk mendapatkan hitungan jumlah kesalahan fungsi yang terjadi setiap menit, lihat `Errors` metrik dengan jangka waktu 1 menit. Sum

Note

Lihat metrik pemanggilan berikut dengan statistik. Sum

- **Invocations**— Berapa kali kode fungsi Anda dipanggil, termasuk pemanggilan dan pemanggilan yang berhasil yang menghasilkan kesalahan fungsi. Pemanggilan tidak direkam jika permintaan pemanggilan dibatasi atau menghasilkan kesalahan pemanggilan. Nilai `Invocations` sama dengan jumlah permintaan yang ditagih.
- **Errors** – Jumlah invokasi yang mengakibatkan kesalahan fungsi. Kesalahan fungsi mencakup pengecualian yang dilemparkan kode Anda dan pengecualian yang dilemparkan oleh runtime Lambda. Runtime mengembalikan kesalahan untuk masalah seperti waktu habis dan kesalahan konfigurasi. Untuk menghitung tingkat kesalahan, bagi nilai `Errors` dengan nilai `Invocations`. Perhatikan bahwa stempel waktu pada metrik kesalahan mencerminkan ketika fungsi dipanggil, bukan ketika kesalahan terjadi.

- **DeadLetterErrors**— Untuk [pemanggilan asinkron](#), berapa kali Lambda mencoba mengirim acara ke antrian huruf mati () tetapi gagal. DLQ Kesalahan huruf mati dapat terjadi karena salah mengatur sumber daya atau batas ukuran.
- **DestinationDeliveryFailures**— Untuk [pemanggilan asinkron dan pemetaan sumber peristiwa yang didukung, berapa kali Lambda mencoba mengirim acara ke tujuan tetapi gagal](#). Untuk pemetaan sumber peristiwa, Lambda mendukung tujuan untuk sumber aliran (DynamoDB dan Kinesis). Kesalahan pengiriman dapat terjadi karena kesalahan izin, sumber daya yang tidak dikonfigurasi dengan benar, atau batas ukuran. Kesalahan juga dapat terjadi jika tujuan yang telah Anda konfigurasi adalah tipe yang tidak didukung seperti SQS FIFO antrian Amazon atau topik Amazon SNSFIFO.
- **Throttles** – Jumlah permintaan invokasi yang ditrotel. Ketika semua instance fungsi memproses permintaan dan tidak ada konkurensi yang tersedia untuk ditingkatkan, Lambda menolak permintaan tambahan dengan kesalahan. `TooManyRequestsException` Permintaan yang dibatasi dan kesalahan pemanggilan lainnya tidak dihitung sebagai salah satu atau. `Invocations Errors`
- **OversizedRecordCount**— Untuk sumber acara Amazon DocumentDB, jumlah peristiwa yang diterima fungsi Anda dari aliran perubahan Anda yang berukuran lebih dari 6 MB. Lambda menjatuhkan pesan dan memancarkan metrik ini.
- **ProvisionedConcurrencyInvocations**— Berapa kali kode fungsi Anda dipanggil menggunakan konkurensi yang [disediakan](#).
- **ProvisionedConcurrencySpilloverInvocations**— Berapa kali kode fungsi Anda dipanggil menggunakan konkurensi standar ketika semua konkurensi yang disediakan sedang digunakan.
- **RecursiveInvocationsDropped**— Berapa kali Lambda menghentikan pemanggilan fungsi Anda karena telah mendeteksi bahwa fungsi Anda adalah bagian dari loop rekursif tak terbatas. Deteksi loop rekursif memantau berapa kali fungsi dipanggil sebagai bagian dari rantai permintaan dengan melacak metadata yang ditambahkan oleh didukung. AWS SDKs Secara default, jika fungsi Anda dipanggil sebagai bagian dari rantai permintaan sekitar 16 kali, Lambda akan menghentikan pemanggilan berikutnya. Jika Anda menonaktifkan deteksi loop rekursif, metrik ini tidak dipancarkan. Untuk informasi selengkapnya tentang fitur ini, lihat [Gunakan deteksi loop rekursif Lambda untuk mencegah loop tak terbatas](#).

Metrik kinerja

Metrik kinerja memberikan detail kinerja tentang pemanggilan fungsi tunggal. Misalnya, metrik `Duration` menunjukkan jumlah waktu dalam milidetik yang digunakan oleh fungsi Anda untuk

memproses suatu acara. Untuk mengetahui seberapa cepat fungsi Anda memproses peristiwa, lihat metrik ini dengan statistik Average atau Max.

- `Duration` – Jumlah waktu yang digunakan kode fungsi Anda untuk memproses suatu peristiwa. Durasi tagihan untuk pemanggilan adalah nilai `Duration` dibulatkan ke milidetik terdekat. `Duration` tidak termasuk waktu mulai dingin.
- `PostRuntimeExtensionsDuration` – Jumlah kumulatif waktu yang runtime habiskan untuk menjalankan kode untuk ekstensi setelah kode fungsi selesai.
- `IteratorAge`— Untuk sumber acara DynamoDB, Kinesis, dan Amazon DocumentDB, usia rekor terakhir dalam acara tersebut. Metrik ini mengukur waktu antara saat aliran menerima rekaman dan saat pemetaan sumber peristiwa mengirimkan peristiwa ke fungsi.
- `OffsetLag`— Untuk sumber acara Apache Kafka dan Amazon Managed Streaming for Apache Kafka (MSK Amazon) yang dikelola sendiri, perbedaan offset antara catatan terakhir yang ditulis ke topik dan catatan terakhir yang diproses oleh grup konsumen fungsi Anda. Meskipun topik Kafka dapat memiliki beberapa partisi, metrik ini mengukur lag offset pada tingkat topik.

`Duration` juga mendukung statistik persentil (p). Gunakan persentil untuk mengecualikan nilai outlier yang miring dan statistik. Average Maximum Misalnya, p95 statistik menunjukkan durasi maksimum 95 persen pemanggilan, tidak termasuk 5 persen paling lambat. Untuk informasi selengkapnya, lihat [Persentil](#) di CloudWatch Panduan Pengguna Amazon.

Metrik konkurensi

Lambda melaporkan metrik konkurensi sebagai jumlah agregat dari jumlah instance yang memproses peristiwa di seluruh fungsi, versi, alias, atau. Wilayah AWS Untuk melihat seberapa dekat Anda dengan mencapai [batas konkurensi](#), lihat metrik ini dengan statistik. Max

- `ConcurrentExecutions` – Jumlah instans fungsi yang memproses peristiwa. Jika nomor ini mencapai [kuota eksekusi bersamaan](#) untuk Wilayah, atau batas [konkurensi cadangan](#) pada fungsi, maka Lambda membatasi permintaan pemanggilan tambahan.
- `ProvisionedConcurrentExecutions`— Jumlah instance fungsi yang memproses peristiwa menggunakan konkurensi yang [disediakan](#). Untuk setiap invokasi alias atau versi dengan konkurensi tersedia, Lambda mengeluarkan jumlah saat ini.
- `ProvisionedConcurrencyUtilization`— Untuk versi atau alias, nilai `ProvisionedConcurrentExecutions` dibagi dengan jumlah total konkurensi yang disediakan dikonfigurasi. Misalnya, jika Anda mengonfigurasi konkurensi 10 yang disediakan

untuk fungsi Anda, dan Anda `ProvisionedConcurrentExecutions` adalah 7, maka Anda `ProvisionedConcurrencyUtilization` adalah 0,7.

- `UnreservedConcurrentExecutions`— Untuk Wilayah, jumlah peristiwa yang berfungsi tanpa konkurensi cadangan sedang diproses.
- `ClaimedAccountConcurrency`— Untuk Wilayah, jumlah konkurensi yang tidak tersedia untuk pemanggilan sesuai permintaan. `ClaimedAccountConcurrency` sama dengan `UnreservedConcurrentExecutions` ditambah jumlah konkurensi yang dialokasikan (yaitu total konkurensi cadangan ditambah total konkurensi yang disediakan). Untuk informasi selengkapnya, lihat [Bekerja dengan `ClaimedAccountConcurrency` metrik](#).

Metrik pemanggilan asinkron

Metrik pemanggilan asinkron memberikan detail tentang pemanggilan asinkron dari sumber acara dan pemanggilan langsung. Anda dapat mengatur ambang batas dan alarm untuk memberi tahu Anda tentang perubahan tertentu. Misalnya, ketika ada peningkatan yang tidak diinginkan dalam jumlah acara yang diantri untuk pemrosesan (`AsyncEventsReceived` Atau, ketika suatu acara telah menunggu lama untuk diproses (`AsyncEventAge`).

- `AsyncEventsReceived`— Jumlah acara yang berhasil diantri Lambda untuk diproses. Metrik ini memberikan wawasan tentang jumlah peristiwa yang diterima fungsi Lambda. Pantau metrik ini dan setel alarm untuk ambang batas untuk memeriksa masalah. Misalnya, untuk mendeteksi sejumlah peristiwa yang tidak diinginkan yang dikirim ke Lambda, dan untuk dengan cepat mendiagnosis masalah yang dihasilkan dari pemicu atau konfigurasi fungsi yang salah. Ketidakcocokan antara `AsyncEventsReceived` dan `Invocations` dapat menunjukkan perbedaan dalam pemrosesan, peristiwa yang dijatuhkan, atau potensi backlog antrian.
- `AsyncEventAge`— Waktu antara ketika Lambda berhasil mengantri acara dan ketika fungsi dipanggil. Nilai metrik ini meningkat ketika peristiwa sedang dicoba ulang karena kegagalan pemanggilan atau pelambatan. Pantau metrik ini dan atur alarm untuk ambang batas pada statistik yang berbeda saat terjadi penumpukan antrian. Untuk memecahkan masalah peningkatan metrik ini, lihat metrik untuk mengidentifikasi kesalahan fungsi dan `Errors` metrik untuk mengidentifikasi masalah konkurensi. `Throttles`
- `AsyncEventsDropped`— Jumlah peristiwa yang dijatuhkan tanpa berhasil menjalankan fungsi. Jika Anda mengonfigurasi antrian huruf mati (DLQ) atau `OnFailure` tujuan, maka peristiwa akan dikirim ke sana sebelum dijatuhkan. Acara dijatuhkan karena berbagai alasan. Misalnya, peristiwa dapat melebihi usia peristiwa maksimum atau menghabiskan upaya percobaan ulang maksimum, atau konkurensi cadangan dapat disetel ke 0. Untuk memecahkan masalah mengapa peristiwa

dijatuhkan, lihat `Errors` metrik untuk mengidentifikasi kesalahan fungsi dan `Throttles` metrik untuk mengidentifikasi masalah konkurensi.

Menggunakan CloudWatch log Log dengan Lambda

AWS Lambda secara otomatis memonitor fungsi Lambda atas nama Anda untuk membantu Anda memecahkan masalah kegagalan dalam fungsi Anda. Selama [peran eksekusi](#) fungsi Anda memiliki izin yang diperlukan, Lambda menangkap log untuk semua permintaan yang ditangani oleh fungsi Anda dan mengirimkannya ke Amazon Logs. CloudWatch

Anda dapat menyisipkan pernyataan log masuk ke kode Anda untuk membantu memvalidasi bahwa kode Anda berfungsi seperti yang diharapkan. Lambda secara otomatis terintegrasi dengan CloudWatch Log dan mengirimkan semua log dari kode Anda ke grup CloudWatch log yang terkait dengan fungsi Lambda.

Secara default, Lambda mengirimkan log ke grup log bernama `/aws/lambda/<function name>`. Jika Anda ingin fungsi Anda mengirim log ke grup lain, Anda dapat mengonfigurasinya menggunakan konsol Lambda, AWS Command Line Interface (AWS CLI) atau Lambda. API Lihat [the section called “Mengkonfigurasi grup CloudWatch log”](#) untuk mempelajari selengkapnya.

Anda dapat melihat log untuk fungsi Lambda menggunakan konsol Lambda, konsol, AWS Command Line Interface (AWS CLI), atau. CloudWatch CloudWatch API

Note

Mungkin diperlukan 5 hingga 10 menit agar log muncul setelah pemanggilan fungsi.

Diperlukan izin IAM

[Peran eksekusi](#) Anda memerlukan izin berikut untuk mengunggah log ke CloudWatch Log:

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Untuk mempelajari selengkapnya, lihat [Menggunakan kebijakan \(IAMkebijakan\) berbasis identitas untuk CloudWatch Log di Panduan](#) Pengguna Amazon CloudWatch .

Anda dapat menambahkan izin CloudWatch Log ini menggunakan kebijakan `AWSLambdaBasicExecutionRole` AWS terkelola yang disediakan oleh Lambda. Untuk menambahkan kebijakan ini ke peran Anda, jalankan perintah berikut:


```
aws iam attach-role-policy --role-name your-role --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

Untuk informasi selengkapnya, lihat [the section called “AWS kebijakan terkelola”](#).

Harga

Tidak ada biaya tambahan untuk menggunakan log Lambda; namun, biaya CloudWatch Log standar berlaku. Untuk informasi lebih lanjut, lihat [CloudWatch harga](#).

Mengkonfigurasi kontrol logging lanjutan untuk fungsi Lambda

Untuk memberi Anda kontrol lebih besar atas bagaimana log fungsi Anda ditangkap, diproses, dan dikonsumsi, Lambda menawarkan opsi konfigurasi logging berikut:

- Format log - pilih antara teks biasa dan JSON format terstruktur untuk log fungsi Anda
- Tingkat log - untuk log JSON terstruktur, pilih tingkat detail log yang dikirim Lambda ke CloudWatch, seperti, ERROR, DEBUG atau INFO
- Grup log - pilih grup CloudWatch log yang dikirimkan oleh fungsi Anda

Untuk mempelajari lebih lanjut tentang mengonfigurasi kontrol logging lanjutan, lihat bagian berikut:

Topik

- [Mengkonfigurasi JSON dan format log teks biasa](#)
- [Pemfilteran tingkat log](#)
- [Mengkonfigurasi grup CloudWatch log](#)

Mengkonfigurasi JSON dan format log teks biasa

Menangkap output log Anda sebagai pasangan nilai JSON kunci membuatnya lebih mudah untuk mencari dan memfilter saat men-debug fungsi Anda. Dengan log JSON yang diformat, Anda juga dapat menambahkan tag dan informasi kontekstual ke log Anda. Ini dapat membantu Anda untuk melakukan analisis otomatis volume besar data log. Kecuali alur kerja pengembangan Anda bergantung pada alat yang ada yang menggunakan log Lambda dalam teks biasa, kami sarankan Anda memilih format log Anda. JSON

Untuk semua runtime terkelola Lambda, Anda dapat memilih apakah log sistem fungsi Anda dikirim ke CloudWatch Log dalam teks atau format biasa yang tidak terstruktur. JSON Log sistem adalah log yang dihasilkan Lambda dan kadang-kadang dikenal sebagai log peristiwa platform.

Untuk [runtime yang didukung](#), saat Anda menggunakan salah satu metode logging bawaan yang didukung, Lambda juga dapat menampilkan log aplikasi fungsi Anda (log yang dihasilkan kode fungsi Anda) dalam JSON format terstruktur. Saat Anda mengonfigurasi format log fungsi Anda untuk runtime ini, konfigurasi yang Anda pilih berlaku untuk log sistem dan aplikasi.

Untuk runtime yang didukung, jika fungsi Anda menggunakan pustaka atau metode logging yang didukung, Anda tidak perlu membuat perubahan apa pun pada kode yang ada untuk Lambda untuk menangkap log dalam struktur. JSON

Note

Menggunakan pemformatan JSON log menambahkan metadata tambahan dan mengkodekan pesan log sebagai JSON objek yang berisi serangkaian pasangan nilai kunci. Karena itu, ukuran pesan log fungsi Anda dapat meningkat.

Runtime dan metode logging yang didukung

Lambda saat ini mendukung opsi untuk menampilkan log aplikasi JSON terstruktur untuk runtime berikut.

| Waktu Aktif | Versi yang didukung |
|-------------|---|
| Java | Semua runtime Java kecuali Java 8 di Amazon Linux 1 |
| Node.js | Node.js 16 dan yang lebih baru |
| Python | Python 3.8 dan yang lebih baru |

Agar Lambda dapat mengirim log aplikasi fungsi Anda ke CloudWatch dalam JSON format terstruktur, fungsi Anda harus menggunakan alat logging bawaan berikut untuk mengeluarkan log:

- Java - `LambdaLogger` logger atau `log4j2`.

- Node.js - Metode `console.trace`, `console.debug`, `console.log`, `console.info`, `console.error`, dan `console.warn`
- Python - pustaka Python standar logging

Untuk informasi selengkapnya tentang menggunakan kontrol logging lanjutan dengan runtime yang didukung, lihat [the section called “Pencatatan log”](#), [the section called “Pencatatan log”](#), dan [the section called “Log dan pantau fungsi Python Lambda”](#).

Untuk runtime Lambda terkelola lainnya, Lambda saat ini hanya mendukung pengambilan log sistem dalam format terstruktur. JSON Namun, Anda masih dapat menangkap log aplikasi dalam JSON format terstruktur dalam runtime apa pun dengan menggunakan alat logging seperti Powertools untuk output log AWS Lambda yang JSON diformat.

Format log default

Saat ini, format log default untuk semua runtime Lambda adalah teks biasa.

Jika Anda sudah menggunakan pustaka logging seperti Powertools AWS Lambda untuk menghasilkan log fungsi dalam format JSON terstruktur, Anda tidak perlu mengubah kode jika memilih pemformatan JSON log. Lambda tidak menyandikan dua kali log apa pun yang sudah JSON dikodekan, sehingga log aplikasi fungsi Anda akan terus ditangkap seperti sebelumnya.

JSON format untuk log sistem

Saat Anda mengonfigurasi format log fungsi Anda sebagai JSON, setiap item log sistem (peristiwa platform) ditangkap sebagai JSON objek yang berisi pasangan nilai kunci dengan kunci berikut:

- `"time"`- waktu pesan log dihasilkan
- `"type"`- jenis acara yang dicatat
- `"record"`- isi dari output log

Format `"record"` nilai bervariasi sesuai dengan jenis peristiwa yang dicatat. Untuk informasi selengkapnya, lihat [the section called “Jenis objek telemetri API Event”](#). Untuk informasi selengkapnya tentang tingkat log yang ditetapkan ke peristiwa log sistem, lihat [the section called “Pemetaan peristiwa tingkat log sistem”](#).

Sebagai perbandingan, dua contoh berikut menunjukkan output log yang sama dalam teks biasa dan JSON format terstruktur. Perhatikan bahwa dalam kebanyakan kasus, peristiwa log sistem berisi lebih banyak informasi saat output dalam JSON format daripada saat output dalam teks biasa.

Example teks biasa:

```
2024-03-13 18:56:24.046000 fbe8c1 INIT_START Runtime Version:
python:3.12.v18 Runtime Version ARN: arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0
```

Example terstrukturJSON:

```
{
  "time": "2024-03-13T18:56:24.046Z",
  "type": "platform.initStart",
  "record": {
    "initializationType": "on-demand",
    "phase": "init",
    "runtimeVersion": "python:3.12.v18",
    "runtimeVersionArn": "arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0"
  }
}
```

Note

[the section called “Telemetry API”](#) Selalu memancarkan acara platform seperti START dan REPORT dalam JSON format. Mengonfigurasi format log sistem yang dikirim CloudWatch Lambda tidak memengaruhi perilaku Telemetry Lambda. API

JSONformat untuk log aplikasi

Saat Anda mengonfigurasi format log fungsi Anda sebagaiJSON, keluaran log aplikasi yang ditulis menggunakan pustaka dan metode logging yang didukung ditangkap sebagai JSON objek yang berisi pasangan nilai kunci dengan kunci berikut.

- "timestamp"- waktu pesan log dihasilkan
- "level"- tingkat log yang ditetapkan untuk pesan
- "message"- isi pesan log

- "requestId"(Python dan Node.js) atau "AWSrequestId" (Java) - ID permintaan unik untuk pemanggilan fungsi

Bergantung pada runtime dan metode logging yang digunakan fungsi Anda, JSON objek ini mungkin juga berisi pasangan kunci tambahan. Misalnya, di Node.js, jika fungsi Anda menggunakan console metode untuk mencatat objek kesalahan menggunakan beberapa argumen, JSON Objek akan berisi pasangan nilai kunci tambahan dengan kunci errorMessage, errorType, dan stackTrace. Untuk mempelajari lebih lanjut tentang log JSON yang diformat di runtime Lambda yang berbeda, [the section called "Log dan pantau fungsi Python Lambda"](#) lihat [the section called "Pencatatan log"](#), dan [the section called "Pencatatan log"](#)

Note

Kunci yang digunakan Lambda untuk nilai stempel waktu berbeda untuk log sistem dan log aplikasi. Untuk log sistem, Lambda menggunakan kunci "time" untuk menjaga konsistensi dengan Telemetry. API Untuk log aplikasi, Lambda mengikuti konvensi runtime dan penggunaan yang didukung. "timestamp"

Sebagai perbandingan, dua contoh berikut menunjukkan output log yang sama dalam teks biasa dan JSON format terstruktur.

Example teks biasa:

```
2024-10-27T19:17:45.586Z 79b4f56e-95b1-4643-9700-2807f4e68189 INFO some log message
```

Example terstrukturJSON:

```
{
  "timestamp":"2024-10-27T19:17:45.586Z",
  "level":"INFO",
  "message":"some log message",
  "requestId":"79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Mengatur format log fungsi Anda

Untuk mengonfigurasi format log untuk fungsi Anda, Anda dapat menggunakan konsol Lambda atau AWS Command Line Interface (AWS CLI). [Anda juga dapat mengonfigurasi format log fungsi](#)

[menggunakan API perintah CreateFunction dan UpdateFunctionConfigurationLambda](#), [sumber daya AWS Serverless Application Model \(AWS SAM\) AWS: :Serverless: :Function](#), dan [sumber daya: :Lambda: :Function](#). [AWS CloudFormation AWS](#)

Mengubah format log fungsi Anda tidak memengaruhi log yang ada yang disimpan di CloudWatch Log. Hanya log baru yang akan menggunakan format yang diperbarui.

Jika Anda mengubah format log fungsi Anda menjadi JSON dan tidak menyetel level log, maka Lambda secara otomatis menyetel level log aplikasi dan level log sistem fungsi Anda. INFO Ini berarti bahwa Lambda hanya mengirimkan output log tingkat INFO dan lebih rendah ke Log. CloudWatch Untuk mempelajari selengkapnya tentang pemfilteran tingkat log aplikasi dan sistem, lihat [the section called “Pemfilteran tingkat log”](#)

Note

Untuk runtime Python, ketika format log fungsi Anda diatur ke teks biasa, pengaturan tingkat log default adalah. WARN Ini berarti bahwa Lambda hanya mengirimkan output log level WARN dan lebih rendah ke Log. CloudWatch Mengubah format log fungsi Anda untuk JSON mengubah perilaku default ini. Untuk mempelajari lebih lanjut tentang login dengan Python, lihat. [the section called “Log dan pantau fungsi Python Lambda”](#)

Untuk fungsi Node.js yang memancarkan log format metrik (EMF) yang disematkan, mengubah format log fungsi Anda CloudWatch menjadi tidak dapat mengenali metrik Anda. JSON

Important

Jika fungsi Anda menggunakan Powertools for AWS Lambda (TypeScript) atau pustaka EMF klien bersumber terbuka untuk memancarkan EMF log, perbarui [Powertools](#) dan [EMF](#) pustaka Anda ke versi terbaru untuk memastikannya CloudWatch dapat terus mengurai log Anda dengan benar. Jika Anda beralih ke format JSON log, kami juga menyarankan Anda melakukan pengujian untuk memastikan kompatibilitas dengan metrik tertanam fungsi Anda. Untuk saran lebih lanjut tentang fungsi node.js yang memancarkan EMF log, lihat [the section called “Menggunakan pustaka klien format metrik tertanam \(EMF\) dengan log JSON terstruktur”](#).

Untuk mengkonfigurasi format log fungsi (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi
3. Pada halaman konfigurasi fungsi, pilih Alat pemantauan dan operasi.
4. Di panel konfigurasi Logging, pilih Edit.
5. Di bawah Konten log, untuk format Log pilih Teks atau JSON.
6. Pilih Simpan.

Untuk mengubah format log dari fungsi yang ada (AWS CLI)

- Untuk mengubah format log dari fungsi yang ada, gunakan [update-function-configuration](#) perintah. Atur LogFormat opsi LoggingConfig ke salah satu JSON atau Text.

```
aws lambda update-function-configuration \  
  --function-name myFunction \  
  --logging-config LogFormat=JSON
```

Untuk mengatur format log saat Anda membuat fungsi (AWS CLI)

- Untuk mengonfigurasi format log saat Anda membuat fungsi baru, gunakan `--logging-config` opsi dalam perintah [create-function](#). Setel LogFormat ke salah satu JSON atau Text. Contoh perintah berikut menciptakan fungsi Node.js yang output log dalam terstruktur JSON.

Jika Anda tidak menentukan format log saat membuat fungsi, Lambda akan menggunakan format log default untuk versi runtime yang Anda pilih. Untuk informasi tentang format logging default, lihat [the section called "Format log default"](#).

```
aws lambda create-function \  
  --function-name myFunction \  
  --runtime nodejs20.x \  
  --handler index.handler \  
  --zip-file fileb://function.zip \  
  --role arn:aws:iam::123456789012:role/LambdaRole \  
  --logging-config LogFormat=JSON
```

Pemfilteran tingkat log

Lambda dapat memfilter log fungsi Anda sehingga hanya log dengan tingkat detail tertentu atau lebih rendah yang dikirim ke CloudWatch Log. Anda dapat mengonfigurasi pemfilteran tingkat log secara terpisah untuk log sistem fungsi Anda (log yang dihasilkan Lambda) dan log aplikasi (log yang dihasilkan oleh kode fungsi Anda).

Untuk [the section called “Runtime dan metode logging yang didukung”](#), Anda tidak perlu membuat perubahan apa pun pada kode fungsi Anda agar Lambda memfilter log aplikasi fungsi Anda.

Untuk semua runtime dan metode logging lainnya, kode fungsi Anda harus menampilkan peristiwa log ke `stdout` atau `stderr` sebagai objek yang JSON diformat yang berisi pasangan nilai kunci dengan kunci. `level` Misalnya, Lambda menafsirkan output berikut `stdout` sebagai `DEBUG` log level.

```
print({'level': "debug", "msg": "my debug log", "timestamp":  
      "2024-11-02T16:51:31.587199Z"})
```

Jika bidang `level` nilai tidak valid atau hilang, Lambda akan menetapkan output log level. `INFO` [Agar Lambda dapat menggunakan bidang stempel waktu, Anda harus menentukan waktu dalam format stempel waktu 3339 yang validRFC](#). Jika Anda tidak menyediakan stempel waktu yang valid, Lambda akan menetapkan level log `INFO` dan menambahkan stempel waktu untuk Anda.

Saat memberi nama kunci stempel waktu, ikuti konvensi runtime yang Anda gunakan. Lambda mendukung konvensi penamaan yang paling umum digunakan oleh runtime terkelola. Misalnya, dalam fungsi yang menggunakan `NETruntime`, Lambda mengenali kuncinya. `Timestamp`

Note

Untuk menggunakan penyaringan tingkat log, fungsi Anda harus dikonfigurasi untuk menggunakan format log. JSON Format log default untuk semua runtime terkelola Lambda saat ini adalah teks biasa. Untuk mempelajari cara mengonfigurasi format log fungsi Anda JSON, lihat [the section called “Mengatur format log fungsi Anda”](#).

Untuk log aplikasi (log yang dihasilkan oleh kode fungsi Anda), Anda dapat memilih antara tingkat log berikut.

| Tingkat log | Penggunaan standar |
|----------------------|--|
| TRACE(paling detail) | Informasi paling halus yang digunakan untuk melacak jalur eksekusi kode Anda |
| DEBUG | Informasi terperinci untuk debugging sistem |
| INFO | Pesan yang merekam operasi normal fungsi Anda |
| WARN | Pesan tentang potensi kesalahan yang dapat menyebabkan perilaku tak terduga jika tidak ditangani |
| ERROR | Pesan tentang masalah yang mencegah kode berfungsi seperti yang diharapkan |
| FATAL(paling detail) | Pesan tentang kesalahan serius yang menyebabkan aplikasi berhenti berfungsi |

Ketika Anda memilih tingkat log, Lambda mengirimkan log pada tingkat itu dan lebih rendah ke CloudWatch Log. Misalnya, jika Anda menyetel level log aplikasi fungsi keWARN, Lambda tidak mengirim output log di level danINFO. DEBUG Level log aplikasi default untuk penyaringan log adalahINFO.

Ketika Lambda memfilter log aplikasi fungsi Anda, pesan log tanpa level akan ditetapkan tingkat log. INFO

Untuk log sistem (log yang dihasilkan oleh layanan Lambda), Anda dapat memilih antara tingkat log berikut.

| Tingkat log | Penggunaan |
|----------------------|---|
| DEBUG(paling detail) | Informasi terperinci untuk debugging sistem |
| INFO | Pesan yang merekam operasi normal fungsi Anda |

| Tingkat log | Penggunaan |
|---------------------|--|
| WARN(paling detail) | Pesan tentang potensi kesalahan yang dapat menyebabkan perilaku tak terduga jika tidak ditangani |

Ketika Anda memilih tingkat log, Lambda mengirimkan log pada tingkat itu dan lebih rendah. Misalnya, jika Anda menyetel level log sistem fungsi ke INFO, Lambda tidak mengirim output log pada level tersebut. DEBUG

Secara default, Lambda menyetel level log sistem ke. INFO Dengan pengaturan ini, Lambda secara otomatis mengirim "start" dan "report" mencatat pesan ke. CloudWatch Untuk menerima log sistem yang kurang lebih terperinci, ubah level log ke DEBUG atau WARN. Untuk melihat daftar level log tempat Lambda memetakan peristiwa log sistem yang berbeda, lihat. [the section called "Pemetaan peristiwa tingkat log sistem"](#)

Mengkonfigurasi penyaringan tingkat log

Untuk mengonfigurasi pemfilteran tingkat log aplikasi dan sistem untuk fungsi Anda, Anda dapat menggunakan konsol Lambda atau (). AWS Command Line Interface AWS CLI [Anda juga dapat mengonfigurasi tingkat log fungsi menggunakan API perintah CreateFunction dan UpdateFunctionConfigurationLambda, sumber daya AWS Serverless Application Model \(AWS SAM\) AWS: :Serverless: :Function, dan sumber daya: :Lambda: :Function. AWS CloudFormation AWS](#)

Perhatikan bahwa jika Anda menetapkan tingkat log fungsi Anda dalam kode Anda, pengaturan ini lebih diutamakan daripada setelan tingkat log lainnya yang Anda konfigurasi. Misalnya, jika Anda menggunakan `logging.setLevel()` metode Python untuk mengatur tingkat logging fungsi Anda ke INFO, pengaturan ini lebih diutamakan daripada pengaturan WARN yang Anda konfigurasi menggunakan konsol Lambda.

Untuk mengkonfigurasi aplikasi atau tingkat log sistem fungsi yang ada (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pada halaman konfigurasi fungsi, pilih Alat pemantauan dan operasi.
4. Di panel konfigurasi Logging, pilih Edit.
5. Di bawah Konten log, untuk format Log pastikan JSON dipilih.

6. Dengan menggunakan tombol radio, pilih level log Aplikasi yang Anda inginkan dan tingkat log sistem untuk fungsi Anda.
7. Pilih Simpan.

Untuk mengkonfigurasi aplikasi fungsi yang ada atau tingkat log sistem (AWS CLI)

- Untuk mengubah tingkat log aplikasi atau sistem dari fungsi yang ada, gunakan [update-function-configuration](#) perintah. Setel `--system-log-level` ke salah satu `DEBUG`, `INFO`, atau `WARN`. Setel `--application-log-level` ke salah satu `DEBUG`, `INFO`, `WARN`, `ERROR`, atau `FATAL`.

```
aws lambda update-function-configuration \  
  --function-name myFunction \  
  --system-log-level WARN \  
  --application-log-level ERROR
```

Untuk mengonfigurasi pemfilteran tingkat log saat Anda membuat fungsi

- [Untuk mengonfigurasi pemfilteran tingkat log saat Anda membuat fungsi baru, gunakan `--application-log-level` opsi `--system-log-level` dan dalam perintah `create-function`.](#) Setel `--system-log-level` ke salah satu `DEBUG`, `INFO`, atau `WARN`. Setel `--application-log-level` ke salah satu `DEBUG`, `INFO`, `WARN`, `WARN`, atau `FATAL`.

```
aws lambda create-function \  
  --function-name myFunction \  
  --runtime nodejs20.x \  
  --handler index.handler \  
  --zip-file fileb://function.zip \  
  --role arn:aws:iam::123456789012:role/LambdaRole \  
  --system-log-level WARN \  
  --application-log-level ERROR
```

Pemetaan peristiwa tingkat log sistem

Untuk peristiwa log tingkat sistem yang dihasilkan oleh Lambda, tabel berikut mendefinisikan tingkat log yang ditetapkan untuk setiap peristiwa. Untuk mempelajari lebih lanjut tentang peristiwa yang tercantum dalam tabel, lihat [the section called “Eventreferensi skema”](#)

| Nama peristiwa | Ketentuan | Tingkat log yang ditetapkan |
|--------------------|---------------------------------|-----------------------------|
| initStart | runtimeVersion diatur | INFO |
| initStart | runtimeVersion tidak diatur | DEBUG |
| initRuntimeDone | status=sukses | DEBUG |
| initRuntimeDone | status! = sukses | WARN |
| initReport | initializationType= snapstart | INFO |
| initReport | initializationType! = snapstart | DEBUG |
| initReport | status! = sukses | WARN |
| restoreStart | runtimeVersion diatur | INFO |
| restoreStart | runtimeVersion tidak diatur | DEBUG |
| restoreRuntimeDone | status=sukses | DEBUG |
| restoreRuntimeDone | status! = sukses | WARN |
| restoreReport | status=sukses | INFO |
| restoreReport | status! = sukses | WARN |
| start | - | INFO |
| runtimeDone | status=sukses | DEBUG |
| runtimeDone | status! = sukses | WARN |
| laporan | status=sukses | INFO |
| laporan | status! = sukses | WARN |
| luas | state=sukses | INFO |
| luas | negara! = sukses | WARN |

| Nama peristiwa | Ketentuan | Tingkat log yang ditetapkan |
|-----------------------|-----------|-----------------------------|
| logSubscription | - | INFO |
| telemetrySubscription | - | INFO |
| logsDropped | - | WARN |

Note

[the section called “Telemetry API”](#) Selalu memancarkan set lengkap acara platform. Mengonfigurasi level log sistem yang dikirim CloudWatch Lambda tidak memengaruhi perilaku Telemetry Lambda. API

Pemfilteran tingkat log aplikasi dengan runtime khusus

Saat Anda mengonfigurasi pemfilteran tingkat log aplikasi untuk fungsi Anda, di belakang layar Lambda menyetel level log aplikasi di runtime menggunakan variabel lingkungan. `AWS_LAMBDA_LOG_LEVEL` Lambda juga menetapkan format log fungsi Anda menggunakan variabel `AWS_LAMBDA_LOG_FORMAT` lingkungan. Anda dapat menggunakan variabel-variabel ini untuk mengintegrasikan kontrol logging lanjutan Lambda ke dalam runtime [kustom](#).

Untuk kemampuan mengonfigurasi pengaturan logging untuk fungsi menggunakan runtime kustom dengan konsol Lambda AWS CLI, dan APIs Lambda, konfigurasi runtime kustom Anda untuk memeriksa nilai variabel lingkungan ini. Anda kemudian dapat mengonfigurasi logger runtime Anda sesuai dengan format log dan level log yang Anda pilih.

Mengonfigurasi grup CloudWatch log

Secara default, CloudWatch secara otomatis membuat grup log bernama `/aws/lambda/<function name>` untuk fungsi Anda saat pertama kali dipanggil. Untuk mengonfigurasi fungsi Anda untuk mengirim log ke grup log yang ada, atau untuk membuat grup log baru untuk fungsi Anda, Anda dapat menggunakan konsol Lambda atau AWS CLI. Anda juga dapat mengonfigurasi grup log kustom menggunakan API perintah [CreateFunction](#) dan [UpdateFunctionConfiguration](#) Lambda dan sumber daya AWS Serverless Application Model (AWS SAM) [AWS::Serverless::Function](#).

Anda dapat mengonfigurasi beberapa fungsi Lambda untuk mengirim log ke grup log yang sama CloudWatch . Misalnya, Anda dapat menggunakan grup log tunggal untuk menyimpan log untuk semua fungsi Lambda yang membentuk aplikasi tertentu. Saat Anda menggunakan grup log kustom untuk fungsi Lambda, aliran log yang dibuat Lambda menyertakan nama fungsi dan versi fungsi. Ini memastikan bahwa pemetaan antara pesan log dan fungsi dipertahankan, bahkan jika Anda menggunakan grup log yang sama untuk beberapa fungsi.

Format penamaan aliran log untuk grup log kustom mengikuti konvensi ini:

```
YYYY/MM/DD/<function_name>[<function_version>][<execution_environment_GUID>]
```

Perhatikan bahwa saat mengonfigurasi grup log kustom, nama yang Anda pilih untuk grup log Anda harus mengikuti [aturan penamaan CloudWatch Log](#). Selain itu, nama grup log kustom tidak boleh dimulai dengan string `aws/`. Jika Anda membuat grup log kustom dimulai dengan `aws/`, Lambda tidak akan dapat membuat grup log. Akibatnya, log fungsi Anda tidak akan dikirim ke CloudWatch.

Untuk mengubah grup log fungsi (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pada halaman konfigurasi fungsi, pilih Alat pemantauan dan operasi.
4. Di panel konfigurasi Logging, pilih Edit.
5. Di panel grup Logging, untuk grup CloudWatch log, pilih Kustom.
6. Di bawah Grup log kustom, masukkan nama grup CloudWatch log yang Anda inginkan untuk mengirim log ke fungsi Anda. Jika Anda memasukkan nama grup log yang ada, maka fungsi Anda akan menggunakan grup itu. Jika tidak ada grup log dengan nama yang Anda masukkan, maka Lambda akan membuat grup log baru untuk fungsi Anda dengan nama itu.

Untuk mengubah grup log fungsi (AWS CLI)

- Untuk mengubah grup log dari fungsi yang ada, gunakan [update-function-configuration](#) perintah.

```
aws lambda update-function-configuration \  
  --function-name myFunction \  
  --logging-config LogGroup=myLogGroup
```

Untuk menentukan grup log kustom saat Anda membuat fungsi (AWS CLI)

- Untuk menentukan grup log kustom saat Anda membuat fungsi Lambda baru menggunakan AWS CLI, gunakan opsi. `--logging-config` Contoh perintah berikut menciptakan fungsi Lambda Node.js yang mengirimkan log ke grup log bernama. `myLogGroup`

```
aws lambda create-function \  
  --function-name myFunction \  
  --runtime nodejs20.x \  
  --handler index.handler \  
  --zip-file fileb://function.zip \  
  --role arn:aws:iam::123456789012:role/LambdaRole \  
  --logging-config LogGroup=myLogGroup
```

Izin peran eksekusi

Agar fungsi Anda mengirim CloudWatch log ke Log, itu harus memiliki `PutLogEvents` izin [log](#):. Saat Anda mengonfigurasi grup log fungsi menggunakan konsol Lambda, jika fungsi Anda tidak memiliki izin ini, Lambda menambahkannya ke peran [eksekusi](#) fungsi secara default. Ketika Lambda menambahkan izin ini, ia memberikan izin fungsi untuk mengirim log ke grup log Log apa pun CloudWatch .

Untuk mencegah Lambda memperbarui peran eksekusi fungsi secara otomatis dan mengeditnya secara manual, perluas Izin dan hapus centang Tambahkan izin yang diperlukan.

Saat Anda mengonfigurasi grup log fungsi Anda menggunakan AWS CLI, Lambda tidak akan secara otomatis menambahkan izin. `logs:PutLogEvents` Tambahkan izin ke peran eksekusi fungsi Anda jika belum memilikinya. Izin ini termasuk dalam kebijakan [AWSLambdaBasicExecutionRole](#)terkelola.

Melihat log fungsi Amazon CloudWatch Lambda

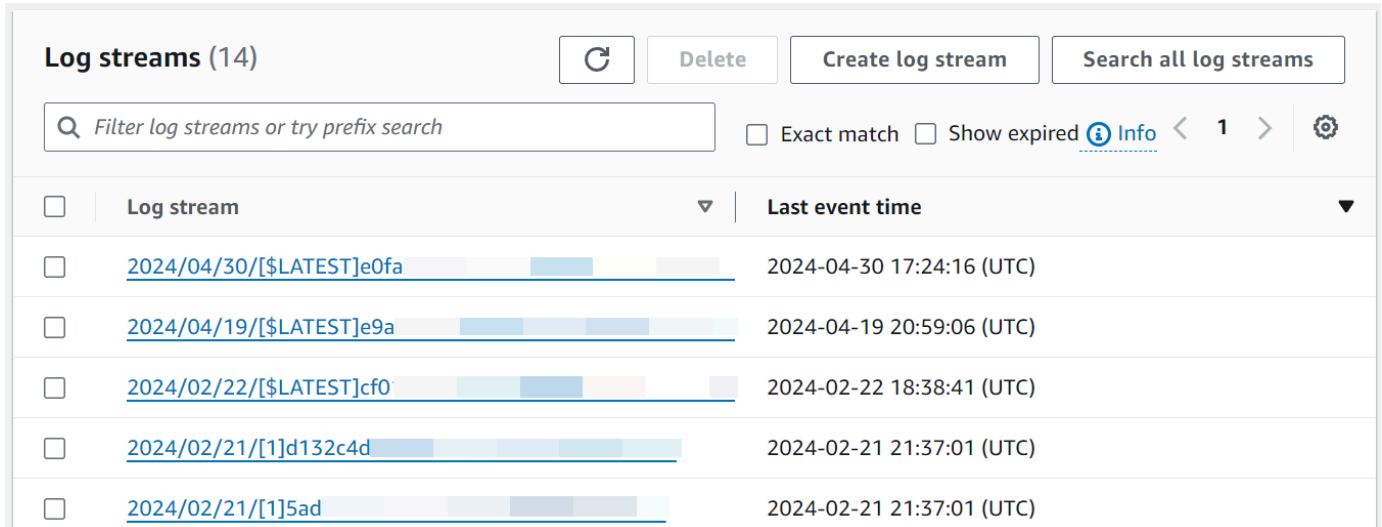
Anda dapat melihat CloudWatch log untuk fungsi Lambda menggunakan konsol Lambda, konsol CloudWatch Log, atau (). AWS Command Line Interface AWS CLI Ikuti petunjuk di bagian berikut untuk mengakses log fungsi Anda.

Mengakses log dengan konsol

Untuk melihat log menggunakan konsol Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.

2. Pilih fungsi.
3. Pilih tab Monitor.
4. Pilih Lihat CloudWatch log.
5. Gulir ke bawah dan pilih aliran Log untuk pemanggilan fungsi yang ingin Anda lihat.



| <input type="checkbox"/> | Log stream | Last event time |
|--------------------------|---|---------------------------|
| <input type="checkbox"/> | 2024/04/30/[\$LATEST]e0fa | 2024-04-30 17:24:16 (UTC) |
| <input type="checkbox"/> | 2024/04/19/[\$LATEST]e9a | 2024-04-19 20:59:06 (UTC) |
| <input type="checkbox"/> | 2024/02/22/[\$LATEST]cf0 | 2024-02-22 18:38:41 (UTC) |
| <input type="checkbox"/> | 2024/02/21/[1]d132c4d | 2024-02-21 21:37:01 (UTC) |
| <input type="checkbox"/> | 2024/02/21/[1]5ad | 2024-02-21 21:37:01 (UTC) |

Anda juga dapat mengakses log untuk fungsi Anda langsung dari CloudWatch konsol.

Untuk melihat log menggunakan CloudWatch konsol

1. Buka [halaman Grup log](#) CloudWatch konsol
2. Pilih grup Log fungsi Anda. Format nama default untuk grup CloudWatch log adalah `/aws/lambda/<function_name>`.
3. Pilih aliran Log untuk pemanggilan fungsi yang ingin Anda lihat.

Mengakses log dengan AWS CLI

AWS CLI Ini adalah alat sumber terbuka yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Untuk menyelesaikan langkah-langkah di bagian ini, Anda harus memiliki hal-hal berikut:

- [AWS Command Line Interface \(AWS CLI\) versi 2](#)
- [AWS CLI — Konfigurasi cepat dengan `aws configure`](#)

Anda dapat menggunakan [AWS CLI](#) untuk mengambil log untuk invokasi menggunakan opsi perintah `--log-type`. Respons berisi bidang `LogResult` yang memuat hingga 4 KB log berkode base64 dari invokasi.

Example mengambil ID log

Contoh berikut menunjukkan cara mengambil ID log dari `LogResult` untuk fungsi bernama `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Anda akan melihat output berikut:

```
{
  "StatusCode": 200,
  "LogResult":
  "U1RBULQgUmVxdWVzdElk0iA4N2QwNDRiOC1mMTU0LTExZTgt0GNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvc21vb... ",
  "ExecutedVersion": "$LATEST"
}
```

Example mendekode log

Pada prompt perintah yang sama, gunakan utilitas `base64` untuk mendekodekan log. Contoh berikut menunjukkan cara mengambil log berkode base64 untuk `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

`cli-binary-format`Opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Anda akan melihat output berikut:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ22luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
```

```
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Duration: 79.67 ms Billed
Duration: 80 ms Memory Size: 128 MB Max Memory Used: 73 MB
```

Utilitas base64 tersedia di Linux, macOS, dan [Ubuntu pada Windows](#). Pengguna macOS mungkin harus menggunakan `base64 -D`.

Example Skrip get-logs.sh

Pada prompt perintah yang sama, gunakan script berikut untuk mengunduh lima peristiwa log terakhir. Skrip menggunakan `sed` untuk menghapus kutipan dari file output, dan akan tidur selama 15 detik untuk memberikan waktu agar log tersedia. Output mencakup respons dari Lambda dan output dari perintah `get-log-events`.

Salin konten dari contoh kode berikut dan simpan dalam direktori proyek Lambda Anda sebagai `get-logs.sh`.

`cli-binary-format` opsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk menjadikan ini pengaturan default, jalankan `aws configure set cli-binary-format raw-in-base64-out`. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS dan Linux (khusus)

Pada prompt perintah yang sama, pengguna macOS dan Linux mungkin perlu menjalankan perintah berikut untuk memastikan skrip dapat dijalankan.

```
chmod -R 755 get-logs.sh
```

Example mengambil lima log acara terakhir

Pada prompt perintah yang sama, gunakan skrip berikut untuk mendapatkan lima log acara terakhir.

```
./get-logs.sh
```

Anda akan melihat output berikut:

```
{
  "statusCode": 200,
  "executedVersion": "$LATEST"
}
{
  "events": [
    {
      "timestamp": 1559763003171,
      "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
$LATEST\n",
      "ingestionTime": 1559763003309
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"\n$LATEST\n",
\r ...",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003173,
      "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
      "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
      "ingestionTime": 1559763018353
    },
    {
      "timestamp": 1559763003218,
      "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
MB\t\n",
      "ingestionTime": 1559763018353
    }
  ],
  "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
}
```

```
"nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"  
}
```

Logging panggilan AWS Lambda API menggunakan AWS CloudTrail

AWS Lambda terintegrasi dengan [AWS CloudTrail](#), layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap panggilan API untuk Lambda sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Lambda dan panggilan kode ke operasi API Lambda. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Lambda, alamat IP dari mana permintaan itu dibuat, kapan dibuat, dan detail tambahan.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut hal ini:

- Baik permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna.
- Apakah permintaan dibuat atas nama pengguna IAM Identity Center.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan tersebut dibuat oleh AWS layanan lain.

CloudTrail aktif di Anda Akun AWS ketika Anda membuat akun dan Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara. Riwayat CloudTrail Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk informasi selengkapnya, lihat [Bekerja dengan riwayat CloudTrail Acara](#) di Panduan AWS CloudTrail Pengguna. Tidak ada CloudTrail biaya untuk melihat riwayat Acara.

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara [CloudTrailDanau](#).

CloudTrail jalan setapak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Semua jalur yang dibuat menggunakan AWS Management Console Multi-region. Anda dapat membuat jalur Single-region atau Multi-region dengan menggunakan. AWS CLI Membuat jejak Multi-wilayah disarankan karena Anda menangkap aktivitas Wilayah AWS di semua akun Anda. Jika Anda membuat jejak wilayah Tunggal, Anda hanya dapat melihat peristiwa yang dicatat di jejak.

Wilayah AWS Untuk informasi selengkapnya tentang jejak, lihat [Membuat jejak untuk Anda Akun AWS](#) dan [Membuat jejak untuk organisasi](#) di Panduan AWS CloudTrail Pengguna.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#). Untuk informasi tentang harga Amazon S3, lihat [Harga Amazon S3](#).

CloudTrail Menyimpan data acara danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL pada acara Anda. CloudTrail [Lake mengubah peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC](#). ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara [tingkat lanjut](#). Penyeleksi yang Anda terapkan ke penyimpanan data acara mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihat [Bekerja dengan AWS CloudTrail Danau](#) di Panduan AWS CloudTrail Pengguna.

CloudTrail Penyimpanan data acara danau dan kueri menimbulkan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih [opsi harga](#) yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#).

Peristiwa data Lambda di CloudTrail

[Peristiwa data](#) memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya (misalnya, membaca atau menulis ke objek Amazon S3). Ini juga dikenal sebagai operasi bidang data. Peristiwa data seringkali merupakan aktivitas volume tinggi. Secara default, CloudTrail tidak mencatat sebagian besar peristiwa data, dan riwayat CloudTrail Peristiwa tidak merekamnya.

Satu peristiwa CloudTrail data yang dicatat secara default untuk layanan yang didukung adalah `LambdaESMDisabled`. Untuk mempelajari lebih lanjut tentang menggunakan acara ini untuk membantu memecahkan masalah dengan pemetaan sumber peristiwa Lambda, lihat [the section called “Menggunakan CloudTrail untuk memecahkan masalah sumber acara Lambda yang dinonaktifkan”](#)

Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya tentang CloudTrail harga, lihat [AWS CloudTrail Harga](#).

Anda dapat mencatat peristiwa data untuk jenis `AWS::Lambda::Function` sumber daya menggunakan CloudTrail konsol AWS CLI, atau operasi CloudTrail API. Untuk informasi selengkapnya tentang cara mencatat peristiwa data, lihat [Mencatat peristiwa data dengan AWS Management Console](#) dan [Logging peristiwa data dengan AWS Command Line Interface](#) di Panduan AWS CloudTrail Pengguna.

Tabel berikut mencantumkan jenis sumber daya Lambda yang dapat Anda log peristiwa data. Kolom tipe peristiwa data (konsol) menunjukkan nilai yang akan dipilih dari daftar tipe peristiwa Data di CloudTrail konsol. Kolom nilai `resources.type` menunjukkan **resources.type** nilai, yang akan Anda tentukan saat mengonfigurasi penyeleksi acara lanjutan menggunakan API atau AWS CLI CloudTrail CloudTrailKolom API Data yang dicatat ke menampilkan panggilan API yang dicatat CloudTrail untuk jenis sumber daya.

| Jenis peristiwa data (konsol) | nilai <code>resources.type</code> | API data masuk CloudTrail |
|-------------------------------|------------------------------------|---------------------------|
| Lambda | <code>AWS::Lambda::Function</code> | Memohon |

Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter pada `eventNamereadOnly`, dan `resources.ARN` bidang untuk mencatat hanya peristiwa yang penting bagi Anda. Contoh berikut adalah tampilan JSON dari konfigurasi peristiwa data yang mencatat peristiwa untuk fungsi tertentu saja. Untuk informasi selengkapnya tentang bidang ini, lihat [AdvancedFieldSelector](#) di Referensi AWS CloudTrail API.

```
[
  {
    "name": "function-invokes",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      }
    ],
  },
  {
    "field": "resources.type",
```

```
    "equals": [
      "AWS::Lambda::Function"
    ]
  },
  {
    "field": "resources.ARN",
    "equals": [
      "arn:aws:lambda:us-east-1:111122223333:function:hello-world"
    ]
  }
]
}
```

Acara manajemen Lambda di CloudTrail

[Acara manajemen](#) memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di Akun AWS. Ini juga dikenal sebagai operasi pesawat kontrol. Secara default, CloudTrail mencatat peristiwa manajemen.

Lambda mendukung pencatatan tindakan berikut sebagai peristiwa manajemen dalam file CloudTrail log.

Note

Dalam file CloudTrail log, eventName mungkin menyertakan informasi tanggal dan versi, tetapi masih mengacu pada tindakan API publik yang sama. Misalnya, GetFunction tindakan muncul sebagaiGetFunction20150331v2. Daftar berikut menentukan kapan nama acara berbeda dari nama tindakan API.

- [AddLayerVersionPermission](#)
- [AddPermission](#)(nama acara:AddPermission20150331v2)
- [CreateAlias](#)(nama acara:CreateAlias20150331)
- [CreateEventSourceMapping](#)(nama acara:CreateEventSourceMapping20150331)
- [CreateFunction](#)(nama acara:CreateFunction20150331)

(ZipFileParameter Environment dan dihilangkan dari CloudTrail log untukCreateFunction.)

- [CreateFunctionUrlConfig](#)

- [DeleteAlias](#)(nama acara:DeleteAlias20150331)
- [DeleteCodeSigningConfig](#)
- [DeleteEventSourceMapping](#)(nama acara:DeleteEventSourceMapping20150331)
- [DeleteFunction](#)(nama acara:DeleteFunction20150331)
- [DeleteFunctionKonkurensi](#) (nama acara:DeleteFunctionConcurrency20171031)
- [DeleteFunctionUrlConfig](#)
- [DeleteProvisionedConcurrencyConfig](#)
- [GetAlias](#)(nama acara:GetAlias20150331)
- [GetEventSourceMapping](#)
- [GetFunction](#)
- [GetFunctionUrlConfig](#)
- [GetFunctionKonfigurasi](#)
- [GetLayerVersionPolicy](#)
- [GetPolicy](#)
- [ListEventSourceMappings](#)
- [ListFunctions](#)
- [ListFunctionUrlConfigs](#)
- [PublishLayerVersi](#) (nama acara:PublishLayerVersion20181031)

(ZipFileParameter dihilangkan dari CloudTrail log untukPublishLayerVersion.)

- [PublishVersion](#)(nama acara:PublishVersion20150331)
- [PutFunctionKonkurensi](#) (nama acara:PutFunctionConcurrency20171031)
- [PutFunctionCodeSigningConfig](#)
- [PutFunctionEventInvokeConfig](#)
- [PutProvisionedConcurrencyConfig](#)
- [PutRuntimeManagementConfig](#)
- [RemovePermission](#)(nama acara:RemovePermission20150331v2)
- [TagResource](#)(nama acara:TagResource20170331v2)
- [UntagResource](#)(nama acara:UntagResource20170331v2)
- [UpdateAlias](#)(nama acara:UpdateAlias20150331)
- [UpdateCodeSigningConfig](#)

- [UpdateEventSourceMapping](#)(nama acara:UpdateEventSourceMapping20150331)
- [UpdateFunctionCode](#) (nama acara:UpdateFunctionCode20150331v2)
(ZipFileParameter dihilangkan dari CloudTrail log untukUpdateFunctionCode.)
- [UpdateFunctionKonfigurasi](#) (nama acara:UpdateFunctionConfiguration20150331v2)
(EnvironmentParameter dihilangkan dari CloudTrail log untukUpdateFunctionConfiguration.)
- [UpdateFunctionEventInvokeConfig](#)
- [UpdateFunctionUrlConfig](#)

Menggunakan CloudTrail untuk memecahkan masalah sumber acara Lambda yang dinonaktifkan

Saat Anda mengubah status pemetaan sumber peristiwa menggunakan tindakan [UpdateEventSourceMapping](#) API, panggilan API dicatat sebagai peristiwa manajemen. CloudTrail Pemetaan sumber peristiwa juga dapat bertransisi langsung ke Disabled status karena kesalahan.

Untuk layanan berikut, Lambda memublikasikan peristiwa LambdaESMDisabled data CloudTrail saat sumber peristiwa Anda beralih ke status Dinonaktifkan:

- Amazon Simple Queue Service (Amazon SQS)
- Amazon DynamoDB
- Amazon Kinesis

Lambda tidak mendukung acara ini untuk jenis pemetaan sumber peristiwa lainnya.

Untuk menerima peringatan saat pemetaan sumber peristiwa untuk layanan yang didukung beralih ke Disabled status, siapkan alarm di Amazon CloudWatch menggunakan acara tersebut. LambdaESMDisabled CloudTrail Untuk mempelajari lebih lanjut tentang mengatur CloudWatch alarm, lihat [Membuat CloudWatch alarm untuk CloudTrail acara: contoh](#).

serviceEventDetailsEntitas dalam pesan LambdaESMDisabled acara berisi salah satu kode kesalahan berikut.

RESOURCE_NOT_FOUND

Sumber daya yang ditentukan dalam permintaan tidak ada.

FUNCTION_NOT_FOUND

Fungsi yang dilampirkan pada sumber kejadian tidak ada.

REGION_NAME_NOT_VALID

Nama Wilayah yang diberikan ke sumber kejadian atau fungsi tidak valid.

AUTHORIZATION_ERROR

Izin belum diatur, atau tidak dikonfigurasi dengan benar.

FUNCTION_IN_FAILED_STATE

Kode fungsi tidak tersusun, mengalami pengecualian yang tidak dapat dipulihkan, atau terjadi deployment yang buruk.

Contoh acara Lambda

Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang operasi API yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untuk `GetFunction` dan `DeleteFunction` tindakan.

Note

`eventName` mungkin termasuk informasi tanggal dan versi, seperti `"GetFunction20150331"`, tetapi masih mengacu pada API publik yang sama.

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "userName": "myUserName"
  },
  "eventTime": "2015-03-18T19:03:36Z",
  "eventSource": "lambda.amazonaws.com",
  "eventName": "GetFunction",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "Python-httpplib2/0.8 (gzip)",
  "errorCode": "AccessDenied",
  "errorMessage": "User: arn:aws:iam::111122223333:user/myUserName is not
authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-
west-2:111122223333:function:other-acct-function",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
  "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
},
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "A1B2C3D4E5F6G7EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/myUserName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2015-03-18T19:04:42Z",
  "eventSource": "lambda.amazonaws.com",
  "eventName": "DeleteFunction20150331",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "Python-httpplib2/0.8 (gzip)",
  "requestParameters": {
    "functionName": "basic-node-task"
  },
  "responseElements": null,
  "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
  "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

```
]
}
```

Untuk informasi tentang konten CloudTrail rekaman, lihat [konten CloudTrail rekaman](#) di Panduan AWS CloudTrail Pengguna.

Visualisasikan pemanggilan fungsi Lambda menggunakan AWS X-Ray

Anda dapat menggunakan AWS X-Ray untuk memvisualisasikan komponen aplikasi Anda, mengidentifikasi kemacetan kinerja, dan memecahkan masalah permintaan yang mengakibatkan kesalahan. Fungsi Lambda Anda mengirimkan data jejak ke X-Ray, dan X-Ray memproses data untuk membuat peta layanan dan rangkuman jejak yang dapat dicari.

Jika Anda mengaktifkan pelacakan X-Ray di layanan yang memanggil fungsi Anda, Lambda mengirim jejak ke X-Ray secara otomatis. Layanan hulu, seperti Amazon API Gateway, atau aplikasi yang dihosting di Amazon EC2 yang diinstrumentasi dengan X-RaySDK, sampel permintaan masuk dan menambahkan header penelusuran yang memberi tahu Lambda untuk mengirim jejak atau tidak. Jejak dari produsen pesan hulu, seperti AmazonSQS, secara otomatis ditautkan ke jejak dari fungsi Lambda hilir, menciptakan end-to-end tampilan seluruh aplikasi. Untuk informasi selengkapnya, lihat [Menelusuri aplikasi berbasis peristiwa di Panduan Pengembang AWS X-Ray](#)

Note

Penelusuran X-Ray saat ini tidak didukung untuk fungsi Lambda dengan Amazon Managed Streaming for Apache Kafka MSK (Amazon), Apache Kafka yang dikelola sendiri, Amazon MQ dengan ActiveMQ dan RabbitMQ, atau pemetaan sumber acara Amazon DocumentDB.

Untuk mengaktifkan penelusuran aktif pada fungsi Lambda Anda dengan konsol, ikuti langkah-langkah berikut:

Untuk mengaktifkan penelusuran aktif

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih Konfigurasi dan kemudian pilih Alat Pemantauan dan operasi.
4. Pilih Edit.
5. Di bawah X-Ray, aktifkan penelusuran Aktif.
6. Pilih Simpan.

Fungsi Anda memerlukan izin untuk mengunggah data jejak ke X-Ray. [Saat Anda mengaktifkan penelusuran di konsol Lambda, Lambda menambahkan izin yang diperlukan ke peran eksekusi fungsi Anda.](#) Jika tidak, tambahkan [AWSXRayDaemonWriteAccess](#) kebijakan ke peran eksekusi.

X-Ray tidak melacak semua permintaan ke aplikasi Anda. X-Ray menerapkan algoritma pengambilan sampel untuk memastikan bahwa penelusuran efisien, sambil tetap memberikan sampel yang representatif dari semua permintaan. Tingkat pengambilan sampel adalah 1 permintaan per detik dan 5 persen dari permintaan tambahan. Anda tidak dapat mengonfigurasi laju pengambilan sampel X-Ray untuk fungsi Anda.

Memahami jejak X-Ray

Di X-Ray, jejak merekam informasi tentang permintaan yang diproses oleh satu atau beberapa layanan. Lambda mencatat 2 segmen per jejak, yang menciptakan dua node pada grafik layanan. Gambar berikut menyoroti dua node ini:



Node pertama di sebelah kiri mewakili layanan Lambda, yang menerima permintaan pemanggilan. Node kedua mewakili fungsi Lambda spesifik Anda.

Segmen yang direkam untuk layanan Lambda, `AWS::Lambda`, mencakup semua langkah yang diperlukan untuk mempersiapkan lingkungan eksekusi Lambda. Ini termasuk penjadwalan microVM, membuat atau mencairkan lingkungan eksekusi dengan sumber daya yang telah Anda konfigurasi, serta mengunduh kode fungsi Anda dan semua lapisan.

`AWS::Lambda::Function` Segmen ini untuk pekerjaan yang dilakukan oleh fungsi.

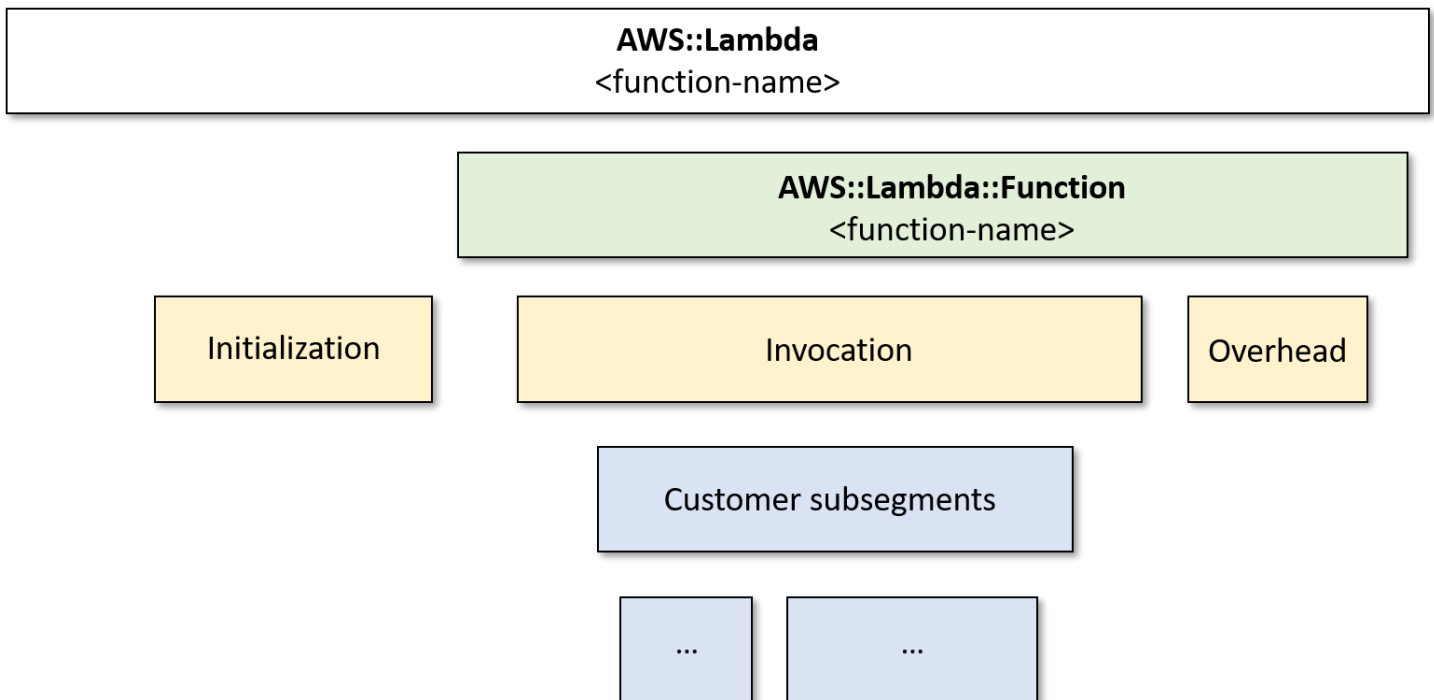
Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen pelacakan yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS Perubahan ini mempengaruhi subsegmen segmen fungsi. Paragraf berikut menjelaskan format lama dan baru untuk subsegmen ini.

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Struktur segmen Lambda gaya lama AWS X-Ray

Struktur X-Ray gaya lama untuk AWS : : Lambda segmen ini terlihat seperti berikut:



Dalam format ini, segmen fungsi memiliki subsegmen untuk `Initialization`, `Invocation`, dan `Overhead`. [Lambda SnapStart](#) Hanya saja, ada juga `Restore` subsegmen (tidak ditampilkan pada diagram ini).

Subsegmen `Initialization` merupakan fase init dari siklus hidup lingkungan eksekusi Lambda. Selama fase ini, Lambda menginisialisasi ekstensi, menginisialisasi runtime, dan menjalankan kode inisialisasi fungsi.

Subsegmen `Invocation` merupakan fase invocasi tempat Lambda memanggil handler fungsi. Ini dimulai dengan pendaftaran runtime dan ekstensi serta berakhir ketika runtime siap untuk mengirim respon.

(`SnapStart` Hanya Lambda) `Restore` Subsegmen menunjukkan waktu yang dibutuhkan Lambda untuk memulihkan snapshot, memuat runtime (JVM), dan menjalankan kait runtime apa pun. `afterRestore` Proses memulihkan snapshot dapat mencakup waktu yang dihabiskan untuk aktivitas di luar microVM. Kali ini dilaporkan di `Restore` subsegmen. Anda tidak dikenakan biaya untuk waktu yang dihabiskan di luar microVM untuk memulihkan snapshot.

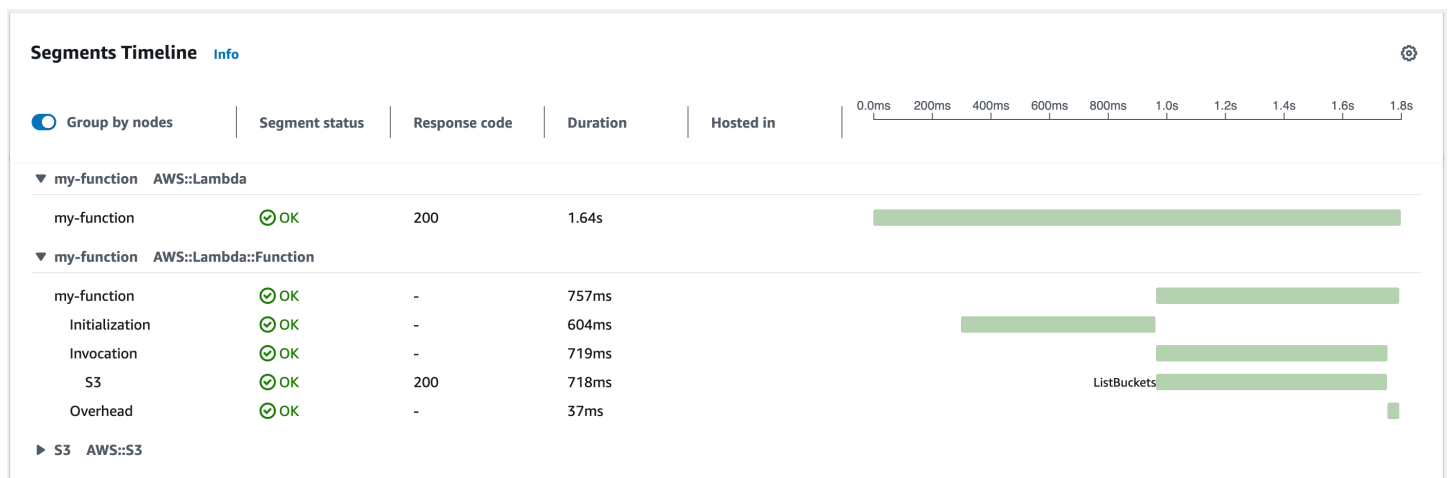
Subsegmen `Overhead` merupakan fase yang terjadi antara waktu ketika runtime mengirimkan respon dan sinyal untuk invocasi berikutnya. Selama waktu ini, runtime menyelesaikan semua tugas yang terkait dengan invocasi dan mempersiapkan untuk membekukan sandbox.

Important

Anda dapat menggunakan X-Ray SDK untuk memperluas `Invocation` subsegmen dengan subsegmen tambahan untuk panggilan hilir, anotasi, dan metadata. Anda tidak dapat mengakses segmen fungsi secara langsung atau merekam pekerjaan yang dilakukan di luar lingkup invocasi handler.

Untuk informasi selengkapnya tentang fase lingkungan eksekusi Lambda, lihat [Lingkungan eksekusi](#)

Contoh jejak menggunakan struktur X-Ray gaya lama ditunjukkan pada diagram berikut.



Perhatikan dua segmen dalam contoh. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal usul. `AWS::Lambda::Function` Jika

AWS::Lambda segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika

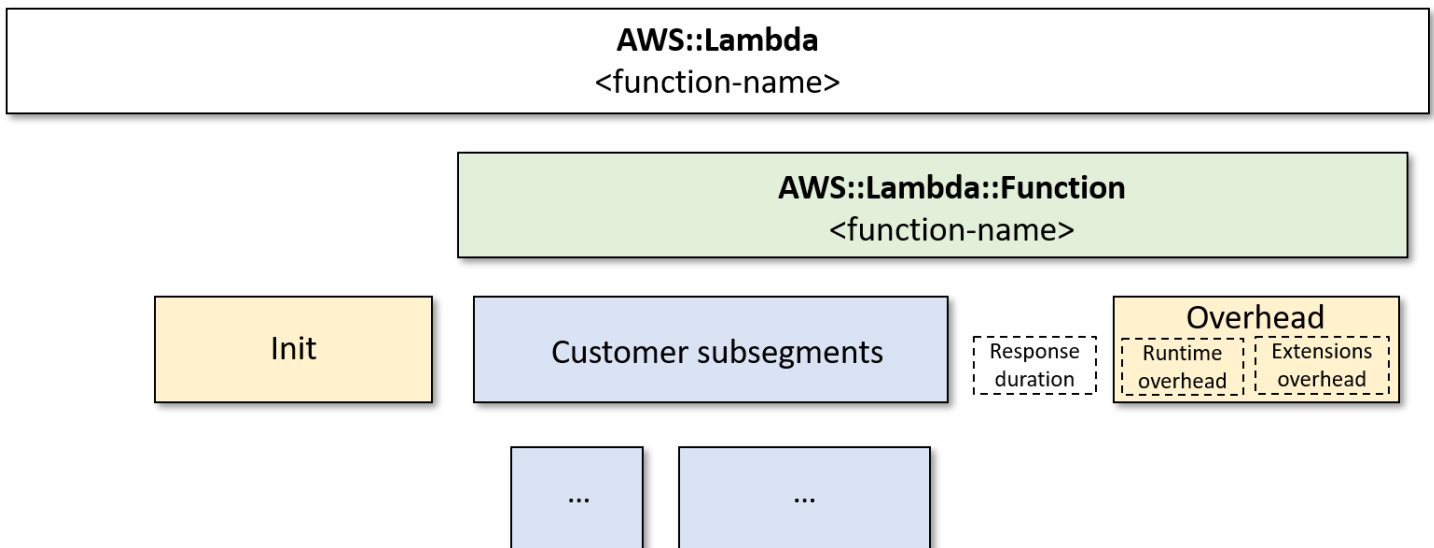
AWS::Lambda::Function segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.

Note

Kadang-kadang, Anda mungkin melihat kesenjangan besar antara inialisasi fungsi dan fase pemanggilan dalam jejak X-Ray Anda. Untuk fungsi yang menggunakan [konkurensi yang disediakan](#), ini karena Lambda menginisialisasi instance fungsi Anda jauh sebelum pemanggilan. Untuk fungsi [yang menggunakan konkurensi tanpa syarat \(sesuai permintaan\)](#), Lambda dapat secara proaktif menginisialisasi instance fungsi, meskipun tidak ada pemanggilan. Secara visual, kedua kasus ini muncul sebagai celah waktu antara fase inialisasi dan pemanggilan.

Struktur segmen Lambda gaya baru AWS X-Ray

Struktur X-Ray gaya baru untuk AWS::Lambda segmen ini terlihat seperti berikut:



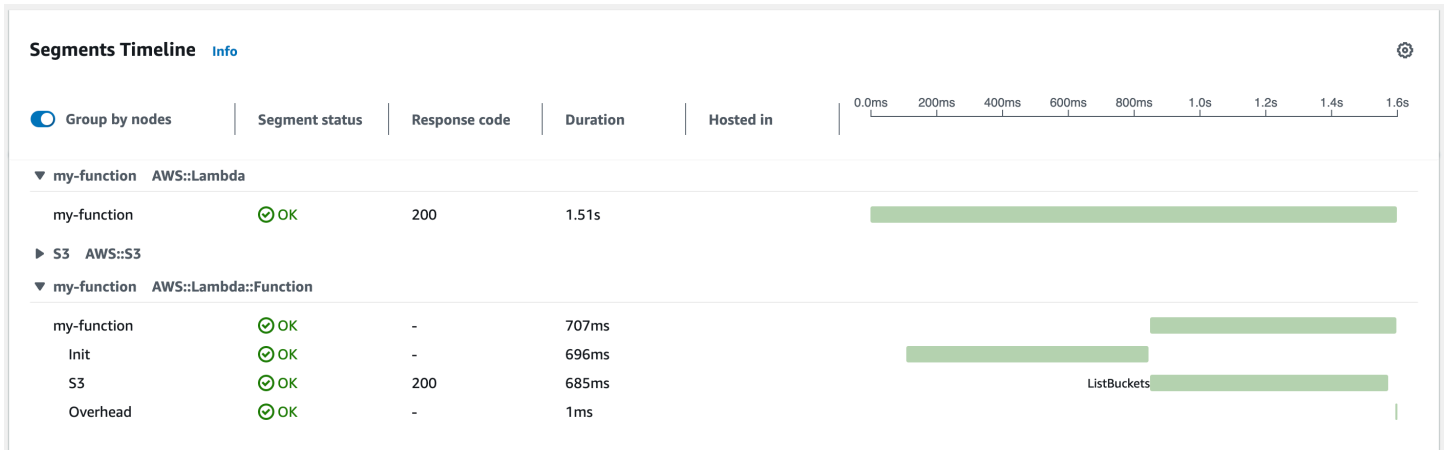
Dalam format baru ini, Init Subsegmen mewakili fase init dari siklus hidup lingkungan eksekusi Lambda seperti sebelumnya.

Tidak ada segmen pemanggilan dalam format baru. Sebaliknya, subsegmen pelanggan dilampirkan langsung ke AWS::Lambda::Function segmen. Segmen ini berisi metrik berikut sebagai anotasi:

- `aws.responseLatency`- waktu yang dibutuhkan untuk menjalankan fungsi
- `aws.responseDuration`- waktu yang dibutuhkan untuk mentransfer respons kepada pelanggan

- `aws.runtimeOverhead`- jumlah waktu tambahan runtime yang dibutuhkan untuk menyelesaikan
- `aws.extensionOverhead`- jumlah waktu tambahan ekstensi yang dibutuhkan untuk menyelesaikan

Contoh jejak menggunakan struktur X-Ray gaya baru ditunjukkan pada diagram berikut.



Perhatikan dua segmen dalam contoh. Keduanya bernama fungsi saya, tetapi yang satu memiliki asal `AWS::Lambda` dan yang lainnya memiliki asal `usul.AWS::Lambda::Function`. Jika `AWS::Lambda` segmen menunjukkan kesalahan, layanan Lambda mengalami masalah. Jika `AWS::Lambda::Function` segmen menunjukkan kesalahan, fungsi Anda mengalami masalah.

Lihat topik berikut untuk pengantar khusus bahasa tertentu terkait pelacakan di Lambda:

- [Menginstrumentasi kode Node.js di AWS Lambda](#)
- [Menginstrumentasi kode Python di AWS Lambda](#)
- [Menginstrumentasi kode Ruby di AWS Lambda](#)
- [Menginstrumentasi kode Java di AWS Lambda](#)
- [Menginstrumentasi kode Go di AWS Lambda](#)
- [Menginstrumentasi kode C # di AWS Lambda](#)

Untuk daftar lengkap layanan yang mendukung instrumentasi aktif, lihat [AWS Layanan yang didukung](#) di Panduan AWS X-Ray Pengembang.

Izin peran eksekusi

Lambda memerlukan izin berikut untuk mengirim data jejak ke X-Ray. Tambahkan izin ke [peran eksekusi](#) fungsi Anda.

- [xray: PutTraceSegments](#)
- [xray: PutTelemetryRecords](#)

Izin ini disertakan dalam kebijakan [AWSXRayDaemonWriteAccess](#)sterkelola.

AWS X-Ray Daemon

Alih-alih mengirim data jejak langsung ke X-RayAPI, X-Ray SDK menggunakan proses daemon. AWS X-Ray Daemon adalah aplikasi yang berjalan di lingkungan Lambda dan mendengarkan UDP lalu lintas yang berisi segmen dan subsegmen. Ini menyangga data masuk dan menuliskannya ke X-Ray dalam batch sehingga mengurangi pemrosesan dan overhead memori yang diperlukan untuk melacak invokasi.

Runtime Lambda memungkinkan daemon hingga 3 persen memori fungsi yang dikonfigurasi atau 16 MB, mana pun yang lebih besar. Jika fungsi Anda kehabisan memori selama invokasi, runtime mengakhiri proses daemon terlebih dahulu untuk mengosongkan memori.

Proses daemon dikelola penuh oleh Lambda dan tidak dapat dikonfigurasi oleh pengguna. Semua segmen yang dihasilkan oleh invokasi fungsi direkam dalam akun yang sama dengan fungsi Lambda. Daemon tidak dapat dikonfigurasi untuk mengalihkannya ke akun lain.

Untuk informasi lebih lanjut, lihat [Daemon X-Ray](#) dalam Panduan Developer X-Ray.

Mengaktifkan penelusuran aktif dengan Lambda API

Untuk mengelola konfigurasi penelusuran dengan AWS CLI atau AWS SDK, gunakan API operasi berikut:

- [UpdateFunctionConfiguration](#)
- [GetFunctionConfiguration](#)
- [CreateFunction](#)

Contoh AWS CLI perintah berikut memungkinkan penelusuran aktif pada fungsi bernama my-function.

```
aws lambda update-function-configuration --function-name my-function \  
--tracing-config Mode=Active
```

Mode penelusuran adalah bagian dari konfigurasi khusus versi saat Anda memublikasikan versi fungsi Anda. Anda tidak dapat mengubah mode pelacakan pada versi yang telah diterbitkan.

Mengaktifkan penelusuran aktif dengan AWS CloudFormation

Untuk mengaktifkan penelusuran pada `AWS::Lambda::Function` sumber daya dalam AWS CloudFormation templat, gunakan `TracingConfig` properti.

Example [function-inline.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Lambda::Function  
    Properties:  
      TracingConfig:  
        Mode: Active  
      ...
```

Untuk sumber `AWS::Serverless::Function` daya AWS Serverless Application Model (AWS SAM), gunakan `Tracing` properti.

Example [template.yml](#) – Konfigurasi pelacakan

```
Resources:  
  function:  
    Type: AWS::Serverless::Function  
    Properties:  
      Tracing: Active  
      ...
```

Pantau kinerja fungsi dengan Amazon CloudWatch Lambda Insights

Amazon CloudWatch Lambda Insights mengumpulkan dan menggabungkan metrik kinerja runtime fungsi Lambda dan log untuk aplikasi tanpa server Anda. Halaman ini menjelaskan cara mengaktifkan dan menggunakan Lambda Insights untuk mendiagnosis masalah dengan fungsi Lambda Anda.

Bagian

- [Cara kerja Lambda Insights memantau aplikasi nirserver](#)
- [Harga](#)
- [Runtime yang didukung](#)
- [Mengaktifkan Lambda Insights di konsol Lambda](#)
- [Mengaktifkan Lambda Insights secara terprogram](#)
- [Menggunakan dasbor Lambda Insights](#)
- [Contoh alur kerja untuk mendeteksi anomali fungsi](#)
- [Contoh alur kerja menggunakan kueri untuk memecahkan masalah fungsi](#)
- [Apa selanjutnya?](#)

Cara kerja Lambda Insights memantau aplikasi nirserver

CloudWatch Lambda Insights adalah solusi pemantauan dan pemecahan masalah untuk aplikasi tanpa server yang berjalan. AWS Lambda Solusi ini mengumpulkan, mengumpulkan, dan merangkum metrik tingkat sistem termasuk CPU waktu, memori, disk, dan penggunaan jaringan. Aplikasi ini juga mengumpulkan, menggabungkan, dan merangkum informasi diagnostik seperti proses mulai yang dingin dan penonaktifan pekerja Lambda untuk membantu Anda mengisolasi masalah dengan fungsi Lambda Anda dan menyelesaikan masalahnya segera.

[Lambda Insights menggunakan ekstensi CloudWatch Lambda Insights baru, yang disediakan sebagai lapisan Lambda.](#) Saat Anda mengaktifkan ekstensi ini pada fungsi Lambda untuk runtime yang didukung, ekstensi ini mengumpulkan metrik tingkat sistem dan memancarkan peristiwa log kinerja tunggal untuk setiap pemanggilan fungsi Lambda tersebut. CloudWatch menggunakan format metrik tertanam untuk mengekstrak metrik dari peristiwa log. Untuk informasi selengkapnya, lihat [Menggunakan AWS Lambda ekstensi](#).

Lapisan Lambda Insights memperluas CreateLogStream dan PutLogEvents untuk grup `/aws/lambda-insights/` log.

Harga

Saat Anda mengaktifkan Lambda Insights untuk fungsi Lambda Anda, Lambda Insights melaporkan 8 metrik per fungsi dan setiap pemanggilan fungsi mengirimkan sekitar 1KB data log ke CloudWatch. Anda hanya membayar metrik dan log yang dilaporkan untuk fungsi Anda oleh Lambda Insights. Tidak ada biaya minimum atau kebijakan penggunaan layanan wajib. Anda tidak membayar Lambda Insights jika fungsi tidak dipanggil. Untuk contoh penetapan harga, lihat [CloudWatch Harga Amazon](#).

Runtime yang didukung

Anda dapat menggunakan Lambda Insights dengan runtime mana pun yang mendukung [ekstensi Lambda](#).

Mengaktifkan Lambda Insights di konsol Lambda

Anda dapat mengaktifkan Lambda Insights dengan pemantauan ditingkatkan pada fungsi Lambda baru dan yang sudah ada. Saat Anda mengaktifkan Lambda Insights pada fungsi di konsol Lambda untuk runtime yang didukung, Lambda menambahkan [ekstensi](#) Lambda Insights sebagai lapisan untuk fungsi Anda, dan memverifikasi atau mencoba untuk memasang kebijakan [CloudWatchLambdaInsightsExecutionRolePolicy](#) ke [peran eksekusi](#) fungsi Anda.

Untuk mengaktifkan Lambda Insights di konsol Lambda

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi Anda.
3. Pilih tab Konfigurasi.
4. Di menu sebelah kiri, pilih Alat pemantauan dan operasi.
5. Pada panel Alat pemantauan tambahan, pilih Edit.
6. Di bawah CloudWatch Lambda Insights, aktifkan Pemantauan yang disempurnakan.
7. Pilih Simpan.

Mengaktifkan Lambda Insights secara terprogram

Anda juga dapat mengaktifkan Lambda Insights menggunakan AWS Command Line Interface (AWS CLI), AWS Serverless Application Model (SAM) CLI AWS CloudFormation,

atau. AWS Cloud Development Kit (AWS CDK) [Saat Anda mengaktifkan Lambda Insights secara terprogram pada fungsi untuk runtime yang didukung, CloudWatch lampirkan CloudWatchLambdaInsightsExecutionRolePolicy](#) kebijakan tersebut ke peran eksekusi fungsi Anda.

Untuk informasi selengkapnya, lihat [Memulai Wawasan Lambda](#) di Panduan Pengguna Amazon CloudWatch .

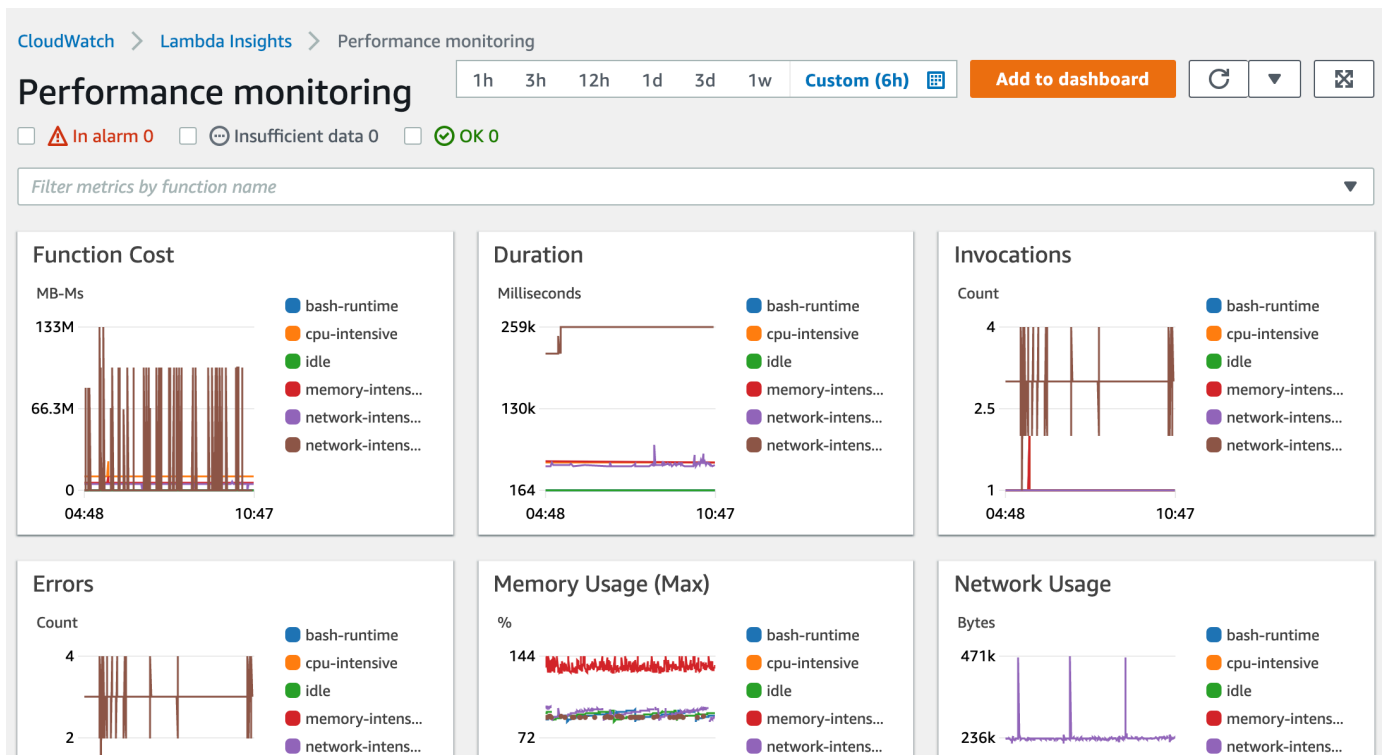
Menggunakan dasbor Lambda Insights

Dasbor Lambda Insights memiliki dua tampilan di CloudWatch konsol: ikhtisar multi-fungsi dan tampilan fungsi tunggal. Ikhtisar multi-fungsi menggabungkan metrik runtime untuk fungsi Lambda di akun saat ini dan Wilayah. AWS Tampilan fungsi tunggal menunjukkan metrik runtime yang tersedia untuk satu fungsi Lambda.

Anda dapat menggunakan ikhtisar multi-fungsi dasbor Lambda Insights di CloudWatch konsol untuk mengidentifikasi fungsi Lambda yang terlalu banyak dan kurang dimanfaatkan. Anda dapat menggunakan tampilan fungsi tunggal dasbor Lambda Insights di CloudWatch konsol untuk memecahkan masalah permintaan individual.

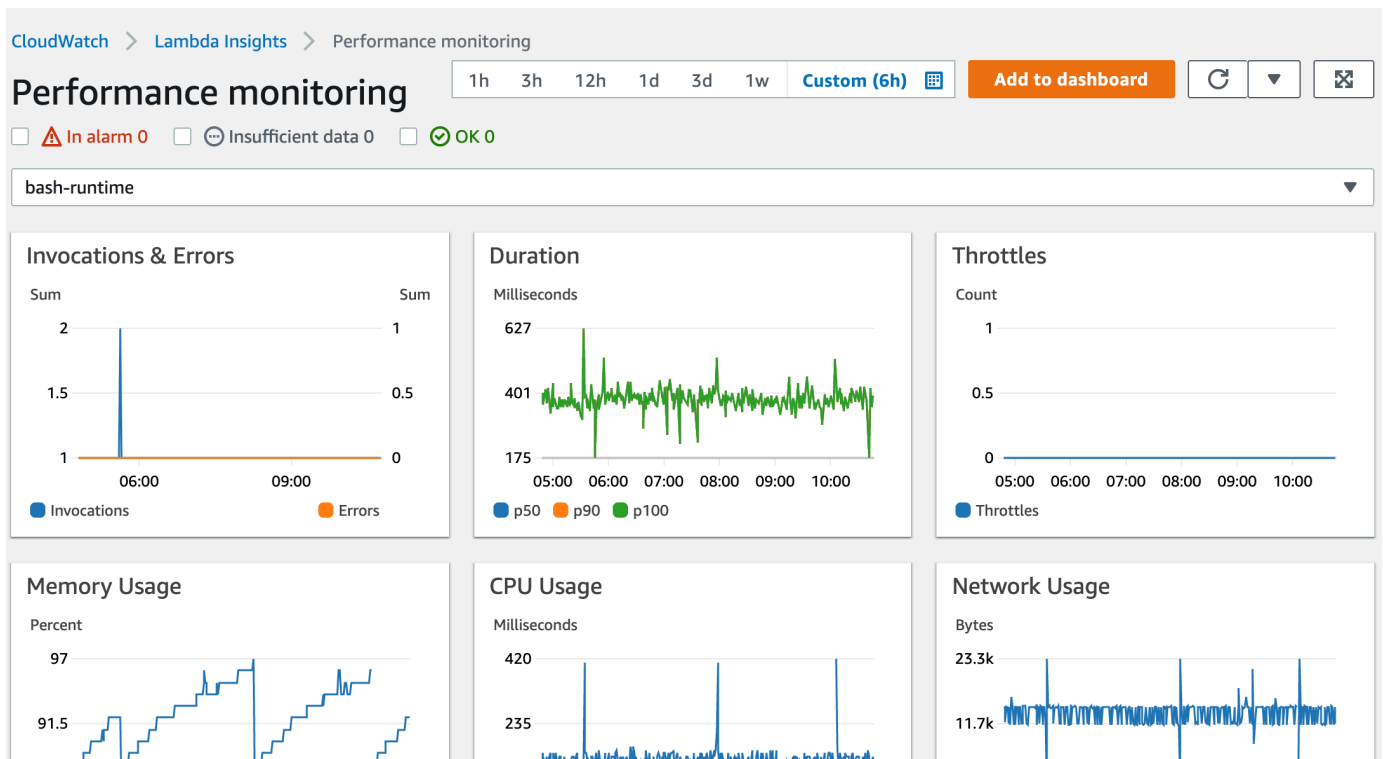
Untuk melihat metrik runtime untuk semua fungsi

1. Buka halaman [Multi-fungsi](#) di CloudWatch konsol.
2. Pilih dari rentang waktu yang sudah ditentukan, atau pilih rentang waktu kustom.
3. (Opsional) Pilih Tambahkan ke dasbor untuk menambahkan widget ke CloudWatch dasbor Anda.



Untuk melihat metrik runtime dari satu fungsi

1. Buka halaman [Single-function](#) di CloudWatch konsol.
2. Pilih dari rentang waktu yang sudah ditentukan, atau pilih rentang waktu kustom.
3. (Opsional) Pilih Tambahkan ke dasbor untuk menambahkan widget ke CloudWatch dasbor Anda.



Untuk informasi selengkapnya, lihat [Membuat dan bekerja dengan widget di CloudWatch dasbor](#).


Contoh alur kerja untuk mendeteksi anomali fungsi


Anda dapat menggunakan ikhtisar multifungsi pada dasbor Lambda Insights untuk mengidentifikasi dan mendeteksi anomali memori komputasi dengan fungsi Anda. Misalnya, jika ikhtisar multifungsi menunjukkan bahwa suatu fungsi menggunakan memori dalam jumlah besar, Anda dapat melihat metrik penggunaan memori yang terperinci dalam panel Penggunaan Memori. Kemudian, Anda dapat menuju dasbor Metrik untuk mengaktifkan deteksi anomali atau membuat alarm.

Untuk mengaktifkan deteksi anomali untuk fungsi

1. Buka halaman [Multi-fungsi](#) di CloudWatch konsol.
2. Di bawah Ringkasan fungsi, pilih nama fungsi Anda.

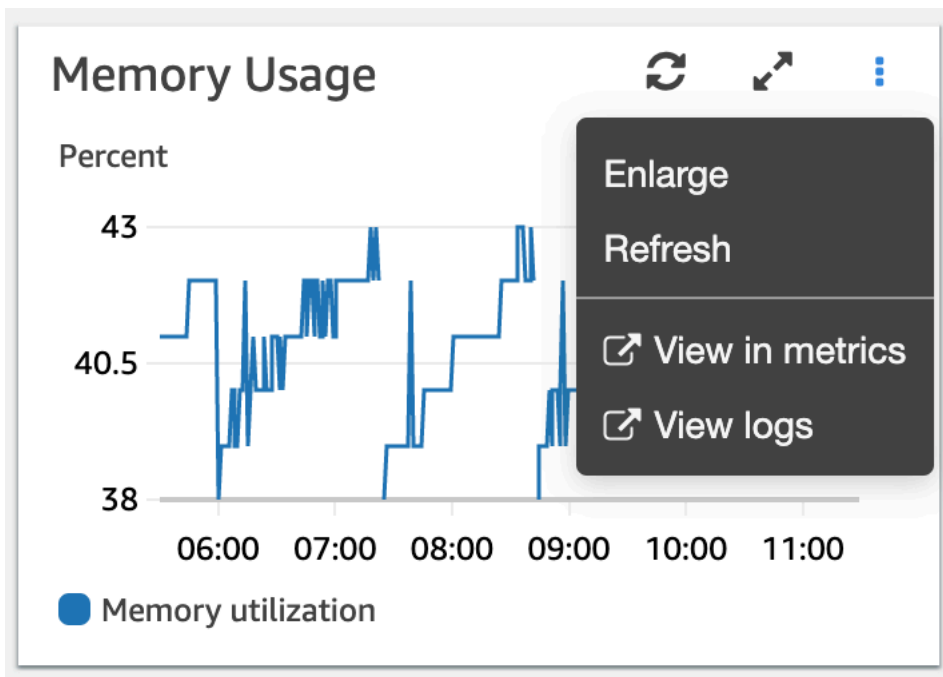
Tampilan fungsi tunggal terbuka dengan metrik runtime fungsi.

Function summary (6) Actions  ▼

< 1 > 

| <input type="checkbox"/> | Function name ▲ | Invocations ▼ | CPU time ▼ | Network IO ▼ | Max. memory ▼ | Cold starts ▼ |
|--------------------------|---------------------------------------|---------------|-------------|--------------|--|---------------|
| <input type="checkbox"/> | bash-runtime | 360 | 132.9167ms | 4770 kB | <div style="width: 97%;"><div style="width: 97%;"></div></div> 97% | 3 |
| <input type="checkbox"/> | cpu-intensive | 359 | 6714.2897ms | 4780 kB | <div style="width: 43%;"><div style="width: 43%;"></div></div> 43% | 4 |
| <input type="checkbox"/> | idle | 359 | 120.2507ms | 4746 kB | <div style="width: 96%;"><div style="width: 96%;"></div></div> 96% | 3 |
| <input type="checkbox"/> | memory-intensive | 358 | 2385.9497ms | 4794 kB | <div style="width: 44%;"><div style="width: 44%;"></div></div> 44% | 4 |
| <input type="checkbox"/> | network-intensive | 359 | 781.0585ms | 82008 kB | <div style="width: 99%;"><div style="width: 99%;"></div></div> 99% | 3 |
| <input type="checkbox"/> | network-intensive-vpc | 43 | 2730.6977ms | 95 kB | <div style="width: 91%;"><div style="width: 91%;"></div></div> 91% | 43 |

- Di panel Penggunaan Memori, pilih tiga titik vertikal, lalu pilih Lihat dalam metrik untuk membuka dasbor Metrik.



- Di tab Metrik bergrafik, di kolom Tindakan, pilih ikon pertama untuk mengaktifkan deteksi anomali untuk fungsi .

| All metrics | | Graphed metrics (6) | | Graph options | Source | | | | |
|-------------------------------------|------------------|--|-----------|-----------------------------------|---------------------------------|------------|--|--|--|
| Math expression ? | | Dynamic labels ? | | Statistic: Maximum ? | Period: 1 Minute ? | Remove all | | | |
| <input checked="" type="checkbox"/> | Label | Details | Statistic | Period | Y Axis | Actions | | | |
| <input checked="" type="checkbox"/> | bash-runtime | LambdaInsights * memory_utilization * functio... | Maximum | 1 Minute | < > | | | | |
| <input checked="" type="checkbox"/> | cpu-intensive | LambdaInsights * memory_utilization * functio... | Maximum | 1 Minute | < > | | | | |
| <input checked="" type="checkbox"/> | idle | LambdaInsights * memory_utilization * functio... | Maximum | 1 Minute | < > | | | | |
| <input checked="" type="checkbox"/> | memory-intensive | LambdaInsights * memory_utilization * functio... | Maximum | 1 Minute | < > | | | | |

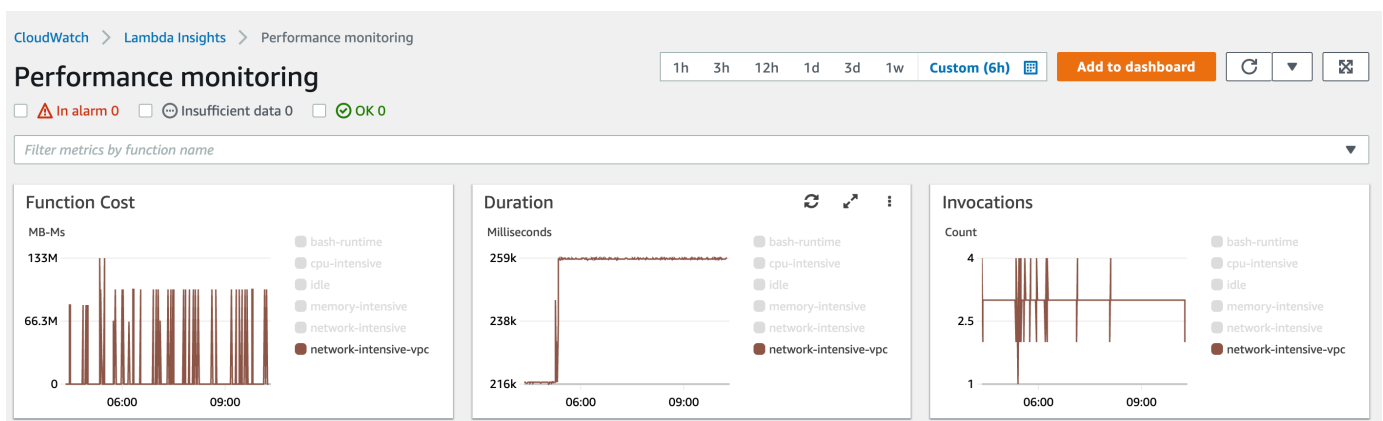
Untuk informasi lebih lanjut, lihat [Menggunakan Deteksi CloudWatch Anomali](#).

Contoh alur kerja menggunakan kueri untuk memecahkan masalah fungsi

Anda dapat menggunakan tampilan fungsi tunggal pada dasbor Lambda Insights untuk mengidentifikasi akar masalah dari lonjakan durasi fungsi. Misalnya, jika ikhtisar multifungsi menunjukkan peningkatan yang besar dalam durasi fungsi, Anda dapat menunda atau memilih setiap fungsi dalam panel Durasi untuk menentukan fungsi mana yang menyebabkan peningkatan. Kemudian, Anda dapat masuk ke tampilan fungsi tunggal dan meninjau Log aplikasi untuk menentukan akar masalah.

Untuk menjalankan kueri pada fungsi

1. Buka halaman [Multi-fungsi](#) di CloudWatch konsol.
2. Di panel Durasi, pilih fungsi Anda untuk memfilter metrik durasi.



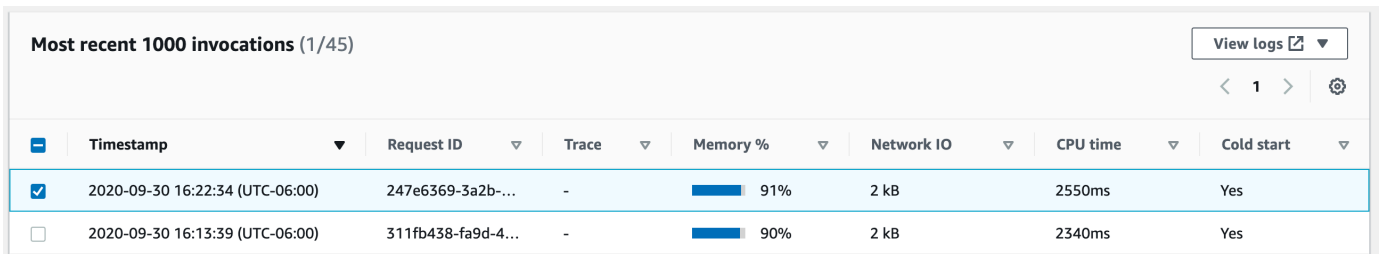
3. Membuka halaman [Fungsi tunggal](#).
4. Pilih daftar pilihan menurun Filter metrik berdasarkan nama fungsi, lalu pilih fungsi Anda.
5. Untuk melihat 1000 log aplikasi terbaru, pilih tab Log aplikasi.

- Meninjau Stempel waktu dan Pesan untuk mengidentifikasi permintaan invokasi yang ingin Anda pecahkan.



| Timestamp | Message |
|----------------------------|---|
| 2020-09-30T16:24:36.121-06 | 0 0 0 0 0 0 0 0 --:--:-- 0:03:06 --:--:-- 0 |
| 2020-09-30T16:24:34.917-06 | 0 0 0 0 0 0 0 0 --:--:-- 0:04:15 --:--:-- 0 |
| 2020-09-30T16:24:34.120-06 | 0 0 0 0 0 0 0 0 --:--:-- 0:03:04 --:--:-- 0 |
| 2020-09-30T16:24:33.033-06 | 0 0 0 0 0 0 0 0 --:--:-- 0:01:26 --:--:-- 0 |

- Untuk menampilkan 1000 invokasi terbaru, pilih tab Invokasi.
- Pilih Stempel waktu atau Pesan untuk permintaan invokasi yang ingin Anda pecahkan.



| | Timestamp | Request ID | Trace | Memory % | Network ID | CPU time | Cold start |
|-------------------------------------|---------------------------------|--------------------|-------|--|------------|----------|------------|
| <input checked="" type="checkbox"/> | 2020-09-30 16:22:34 (UTC-06:00) | 247e6369-3a2b-... | - | <div style="width: 91%; background-color: #0070C0; height: 10px;"></div> 91% | 2 kB | 2550ms | Yes |
| <input type="checkbox"/> | 2020-09-30 16:13:39 (UTC-06:00) | 311fb438-fa9d-4... | - | <div style="width: 90%; background-color: #0070C0; height: 10px;"></div> 90% | 2 kB | 2340ms | Yes |

- Pilih daftar pilihan menurun Lihat log, lalu pilih Lihat log kinerja.

Kueri yang dibuat secara otomatis untuk fungsi Anda terbuka di dasbor Logs Insights.

- Pilih Jalankan kueri untuk menghasilkan pesan Log untuk permintaan invokasi.

Select log group(s) 2020-09-30 (10:35:41) > 2020-09-30 (16:35:41)

/aws/lambda-insights X Clear

```
1 fields @timestamp, @message
2 | .filter function_name = "network-intensive-vpc"
3 | .filter request_id = "247e6369-3a2b-4ccf-9e95-fb80c6ba711f"
4 | sort @timestamp desc
```

Run query Save History

Logs Visualization Export results Add to dashboard Hide histogram

Showing 1 of 1 records matched ⓘ
1,856 records (2.0 MB) scanned in 4.0s @ 467 records/s (521.7 kB/s)

11 AM 12 PM 01 PM 02 PM 03 PM 04 PM

| # | @timestamp | @message |
|-----|-------------------------|--|
| ▶ 1 | 2020-09-30T16:22:34.... | {"cpu_system_time":1520,"shutdown":1,"cpu_user_time":1030,"agent_memory_avg":7487349,"used_memory... |

Apa selanjutnya?

- Pelajari cara membuat dasbor CloudWatch Log di [Membuat Dasbor](#) di Panduan CloudWatch Pengguna Amazon.
- Pelajari cara menambahkan kueri ke dasbor CloudWatch Log di [Tambahkan Kueri ke Dasbor atau Ekspor Hasil Kueri](#) di Panduan CloudWatch Pengguna Amazon.

Mengelola dependensi Lambda dengan lapisan

Lapisan Lambda adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi.

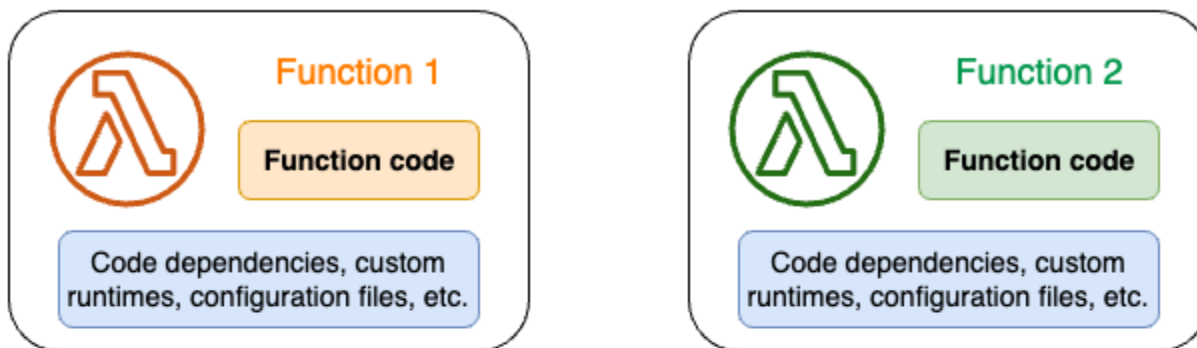
Ada beberapa alasan mengapa Anda mungkin mempertimbangkan untuk menggunakan lapisan:

- Untuk mengurangi ukuran paket penyebaran Anda. Alih-alih memasukkan semua dependensi fungsi Anda bersama dengan kode fungsi Anda dalam paket penerapan Anda, letakkan di lapisan. Ini membuat paket penerapan tetap kecil dan terorganisir.
- Untuk memisahkan logika fungsi inti dari dependensi. Dengan lapisan, Anda dapat memperbarui dependensi fungsi Anda secara independen dari kode fungsi Anda, dan sebaliknya. Ini mempromosikan pemisahan kekhawatiran dan membantu Anda fokus pada logika fungsi Anda.
- Untuk berbagi dependensi di beberapa fungsi. Setelah Anda membuat layer, Anda dapat menerapkannya ke sejumlah fungsi di akun Anda. Tanpa lapisan, Anda perlu menyertakan dependensi yang sama di setiap paket penerapan individu.
- Untuk menggunakan editor kode konsol Lambda. Editor kode adalah alat yang berguna untuk menguji pembaruan kode fungsi minor dengan cepat. Namun, Anda tidak dapat menggunakan editor jika ukuran paket penerapan Anda terlalu besar. Menggunakan lapisan mengurangi ukuran paket Anda dan dapat membuka kunci penggunaan editor kode.

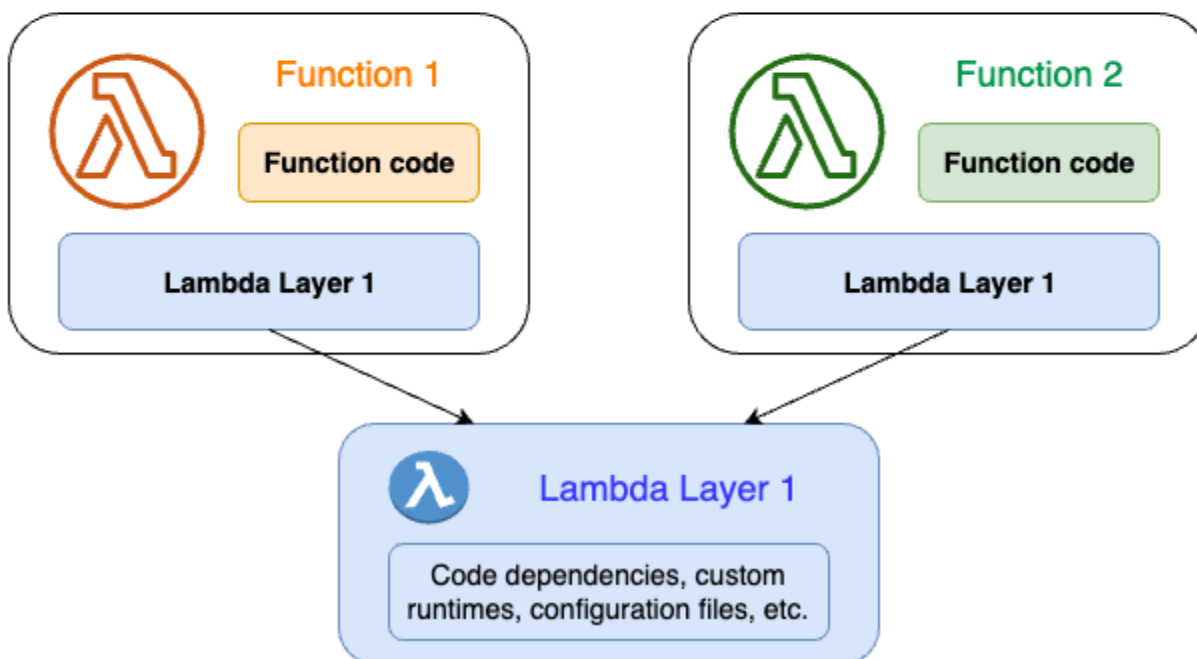
Jika Anda bekerja dengan fungsi Lambda di Go atau Rust, kami sarankan untuk tidak menggunakan lapisan. Untuk fungsi Go dan Rust, Anda memberikan kode fungsi Anda sebagai executable, yang mencakup kode fungsi yang dikompilasi bersama dengan semua dependensinya. Menempatkan dependensi Anda dalam lapisan memaksa fungsi Anda untuk memuat rakitan tambahan secara manual selama fase inisialisasi, yang dapat meningkatkan waktu mulai dingin. Untuk kinerja optimal untuk fungsi Go dan Rust, sertakan dependensi Anda bersama dengan paket penerapan Anda.

Diagram berikut menggambarkan perbedaan arsitektur tingkat tinggi antara dua fungsi yang berbagi dependensi. Satu menggunakan lapisan Lambda, dan yang lainnya tidak.

Lambda function components: Without layers



Lambda function components: With layers



Saat Anda menambahkan layer ke fungsi, Lambda mengekstrak konten layer ke dalam `/opt` direktori di lingkungan [eksekusi](#) fungsi Anda. Semua runtime Lambda yang didukung secara native menyertakan jalur ke direktori tertentu di dalam direktori. `/opt` Ini memberi fungsi Anda akses ke konten lapisan Anda. Untuk informasi selengkapnya tentang jalur spesifik ini dan cara mengemas layer Anda dengan benar, lihat [the section called "Lapisan kemasan"](#).

Anda dapat menyertakan hingga lima lapisan per fungsi. Selain itu, Anda dapat menggunakan lapisan hanya dengan fungsi Lambda yang [digunakan sebagai arsip file.zip](#). Untuk fungsi yang [didefinisikan sebagai gambar kontainer](#), paketkan runtime pilihan Anda dan semua dependensi kode

saat Anda membuat gambar kontainer. Untuk informasi selengkapnya, lihat [Bekerja dengan lapisan dan ekstensi Lambda dalam gambar kontainer di Blog AWS Komputasi](#).

Topik

- [Cara menggunakan lapisan](#)
- [Versi lapisan dan lapisan](#)
- [Kemasan konten lapisan Anda](#)
- [Membuat dan menghapus layer di Lambda](#)
- [Menambahkan lapisan ke fungsi](#)
- [Menggunakan AWS CloudFormation dengan lapisan](#)
- [Menggunakan AWS SAM dengan lapisan](#)

Cara menggunakan lapisan

Untuk membuat layer, paketkan dependensi Anda ke dalam file.zip, mirip dengan cara Anda [membuat paket penerapan normal](#). Lebih khusus lagi, proses umum membuat dan menggunakan lapisan melibatkan tiga langkah ini:

- Pertama, paketkan konten layer Anda. Ini berarti membuat arsip file.zip. Untuk informasi selengkapnya, lihat [the section called “Lapisan kemasan”](#).
- Selanjutnya, buat layer di Lambda. Untuk informasi selengkapnya, lihat [the section called “Membuat dan menghapus lapisan”](#).
- Tambahkan layer ke fungsi Anda. Untuk informasi selengkapnya, lihat [the section called “Menambahkan lapisan”](#).

Versi lapisan dan lapisan

Versi lapisan adalah snapshot yang tidak dapat diubah dari versi tertentu dari lapisan. Saat Anda membuat layer baru, Lambda membuat versi layer baru dengan nomor versi 1. Setiap kali Anda mempublikasikan pembaruan ke layer, Lambda menambah nomor versi dan membuat versi layer baru.

Setiap versi layer diidentifikasi oleh Amazon Resource Name (ARN) yang unik. Saat menambahkan lapisan ke fungsi, Anda harus menentukan versi lapisan yang tepat yang ingin Anda gunakan.

Kemasan konten lapisan Anda

Lapisan Lambda adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi.

Bagian ini menjelaskan cara mengemas konten layer Anda dengan benar. Untuk informasi konseptual lebih lanjut tentang lapisan dan mengapa Anda mungkin mempertimbangkan untuk menggunakannya, lihat [Lapisan Lambda](#).

Langkah pertama untuk membuat layer adalah untuk menggabungkan semua konten layer Anda ke dalam arsip file.zip. Karena fungsi Lambda berjalan di [Amazon Linux](#), konten layer Anda harus dapat dikompilasi dan dibangun di lingkungan Linux.

Untuk memastikan bahwa konten lapisan Anda berfungsi dengan baik di lingkungan Linux, kami sarankan untuk membuat konten lapisan Anda menggunakan alat seperti [Docker](#) atau [AWS Cloud9](#). AWS Cloud9 adalah lingkungan pengembangan terintegrasi berbasis cloud (IDE) yang menyediakan akses bawaan ke server Linux untuk menjalankan dan menguji kode. Untuk informasi selengkapnya, lihat [Menggunakan layer Lambda untuk menyederhanakan proses pengembangan Anda](#) di Compute Blog. AWS

Topik

- [Jalur lapisan untuk setiap runtime Lambda](#)

Jalur lapisan untuk setiap runtime Lambda

Saat Anda menambahkan lapisan ke fungsi, Lambda memuat konten lapisan ke dalam /opt direktori lingkungan eksekusi itu. Untuk setiap runtime Lambda, PATH variabel sudah menyertakan jalur folder tertentu dalam direktori. /opt Untuk memastikan bahwa PATH variabel mengambil konten lapisan Anda, file layer.zip Anda harus memiliki dependensi di jalur folder berikut:

| Runtime | Jalur |
|---------|---|
| Node.js | nodejs/node_modules |
| | nodejs/node16/node_modules (NODE_PATH) |
| | nodejs/node18/node_modules (NODE_PATH) |

| Runtime | Jalur |
|---------|---|
| | nodejs/node20/node_modules (NODE_PATH) |
| Python | python python/lib/ <i>python3.x</i> /site-packages (direktori situs) |
| Java | java/lib (CLASSPATH) |
| Ruby | ruby/gems/3.2.0 (GEM_PATH) ruby/lib (RUBYLIB) |
| Runtime | bin (PATH) lib (LD_LIBRARY_PATH) |

Contoh berikut menunjukkan cara Anda dapat menyusun folder dalam arsip .zip lapisan Anda.

Node.js

Example struktur file AWS X-Ray SDK untuk Node.js

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

Python

Example struktur file untuk pustaka Permintaan

```
layer_content.zip
# python
# lib
# python3.11
# site-packages
# requests
# <other_dependencies> (i.e. dependencies of the requests package)
# ...
```

Ruby

Example struktur file untuk JSON permata

```
json.zip
# ruby/gems/2.7.0/
| build_info
| cache
| doc
| extensions
| gems
| # json-2.1.0
# specifications
  # json-2.1.0.gemspec
```

Java

Example struktur file untuk JAR file Jackson

```
layer_content.zip
# java
  # lib
    # jackson-core-2.17.0.jar
    # <other potential dependencies>
    # ...
```

All

Example struktur file untuk pustaka jq

```
jq.zip
# bin/jq
```

Untuk instruksi khusus bahasa tentang pengemasan, pembuatan, dan penambahan lapisan, lihat halaman berikut:

- Python – [the section called “Lapisan”](#)
- Jawa — [the section called “Lapisan”](#)

Kami merekomendasikan untuk tidak menggunakan lapisan untuk bahasa berikut. Halaman yang ditautkan berisi informasi lebih lanjut.

- Go — [the section called “Lapisan”](#)
- Karat

Membuat dan menghapus layer di Lambda

Lapisan Lambda adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi.

Bagian ini menjelaskan cara membuat dan menghapus layer di Lambda. Untuk informasi konseptual lebih lanjut tentang lapisan dan mengapa Anda mungkin mempertimbangkan untuk menggunakannya, lihat [Lapisan Lambda](#).

Setelah Anda [mengemas konten layer Anda](#), langkah selanjutnya adalah membuat layer di Lambda. Bagian ini menunjukkan cara membuat dan menghapus lapisan menggunakan konsol Lambda atau API Lambda saja. Untuk membuat layer menggunakan AWS CloudFormation, lihat [the section called “Lapisan dengan AWS CloudFormation”](#). Untuk membuat layer menggunakan AWS Serverless Application Model (AWS SAM), lihat [the section called “Lapisan dengan AWS SAM”](#).

Topik

- [Membuat lapisan](#)
- [Menghapus versi lapisan](#)

Membuat lapisan

Untuk membuat layer, Anda dapat mengunggah arsip file.zip dari mesin lokal Anda atau dari Amazon Simple Storage Service (Amazon S3). Lambda mengekstrak konten lapisan ke dalam direktori /opt saat menyiapkan lingkungan eksekusi untuk fungsi.

Layers dapat memiliki satu atau lebih [versi layer](#). Saat Anda membuat lapisan, Lambda menetapkan versi lapisan ke versi 1. Anda dapat mengubah izin pada versi lapisan yang ada kapan saja. Namun, untuk memperbarui kode atau membuat perubahan konfigurasi lainnya, Anda harus membuat versi baru dari layer.

Untuk membuat lapisan (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih Buat lapisan.
3. Di bagian Konfigurasi lapisan, untuk Nama, masukkan nama untuk lapisan Anda.
4. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk lapisan Anda.
5. Untuk mengunggah kode lapisan Anda, lakukan salah satu hal berikut:

- Untuk mengunggah file .zip dari komputer Anda, pilih Unggah file .zip. Selanjutnya, pilih Unggah untuk memilih file .zip lokal Anda.
 - Untuk mengunggah file dari Amazon S3, pilih Unggah file dari Amazon S3. Kemudian, untuk URL tautan Amazon S3, masukkan tautan ke file.
6. (Opsional) Untuk arsitektur yang kompatibel, pilih satu nilai atau kedua nilai. Untuk informasi selengkapnya, lihat [the section called “Set instruksi \(ARM/x86\)”](#).
 7. (Opsional) Untuk runtime yang Kompatibel, pilih runtime yang kompatibel dengan layer Anda.
 8. (Opsional) Untuk lisensi, masukkan informasi lisensi yang diperlukan.
 9. Pilih Buat.

Atau, Anda juga dapat menggunakan [PublishLayerVersion](#) API untuk membuat layer. Misalnya, Anda dapat menggunakan perintah `publish-layer-version` AWS Command Line Interface (CLI) dengan nama, deskripsi, dan arsip file.zip yang ditentukan. Info lisensi, runtime yang kompatibel, dan parameter arsitektur yang kompatibel bersifat opsional.

```
aws lambda publish-layer-version --layer-name my-layer \  
  --description "My layer" \  
  --license-info "MIT" \  
  --zip-file fileb://layer.zip \  
  --compatible-runtimes python3.10 python3.11 \  
  --compatible-architectures "arm64" "x86_64"
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{  
  "Content": {  
    "Location": "https://awslambda-us-east-2-layers.s3.us-east-2.amazonaws.com/  
snapshots/123456789012/my-layer-4aaa2fbb-ff77-4b0a-ad92-5b78a716a96a?  
versionId=27iWyA73cCAYqyH...",  
    "CodeSha256": "tv9jJ0+rPbXUUXuRKi7CwHzKtLDkDRJLB3cC3Z/ouXo=",  
    "CodeSize": 169  
  },  
  "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",  
  "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:1",  
  "Description": "My layer",  
  "CreateDate": "2023-11-14T23:03:52.894+0000",  
  "Version": 1,  
  "CompatibleArchitectures": [  
    "arm64",
```

```
    "x86_64"  
  ],  
  "LicenseInfo": "MIT",  
  "CompatibleRuntimes": [  
    "python3.10",  
    "python3.11"  
  ]  
}
```

Setiap kali Anda menelepon `publish-layer-version`, Anda membuat versi baru dari layer.

Menghapus versi lapisan

Untuk menghapus versi layer, gunakan [DeleteLayerVersion](#) API. Misalnya, Anda dapat menggunakan perintah `delete-layer-version` CLI dengan nama lapisan dan versi lapisan yang ditentukan.

```
aws lambda delete-layer-version --layer-name my-layer --version-number 1
```

Saat menghapus versi lapisan, Anda tidak dapat lagi mengonfigurasi fungsi Lambda untuk menggunakannya. Namun, fungsi apa pun yang sudah menggunakan versi ini terus memiliki akses. Selain itu, Lambda tidak pernah menggunakan kembali nomor versi untuk nama lapisan.

Menambahkan lapisan ke fungsi

Lapisan Lambda adalah arsip file.zip yang berisi kode atau data tambahan. Lapisan biasanya berisi dependensi pustaka, [runtime kustom](#), atau file konfigurasi.

Bagian ini menjelaskan cara menambahkan layer ke fungsi Lambda. Untuk informasi konseptual lebih lanjut tentang lapisan dan mengapa Anda mungkin mempertimbangkan untuk menggunakannya, lihat [Lapisan Lambda](#).

Sebelum Anda dapat mengkonfigurasi fungsi Lambda untuk menggunakan lapisan, Anda harus:

- [Package konten layer Anda](#)
- [Buat layer di Lambda](#)
- Pastikan Anda memiliki izin untuk memanggil versi [GetLayerVersion](#) API on the layer. Untuk fungsi dalam Anda Akun AWS, Anda harus memiliki izin ini dalam [kebijakan pengguna](#) Anda. Untuk menggunakan lapisan di akun lain, pemilik akun tersebut harus memberi akun Anda izin dalam [kebijakan berbasis sumber daya](#). Sebagai contoh, lihat [the section called “Akses lapisan untuk akun lain”](#).

Anda dapat menambahkan hingga lima lapisan ke fungsi Lambda. Ukuran total fungsi yang belum di-zip dan semua lapisan tidak dapat melebihi kuota ukuran paket deployment yang belum di-zip sebesar 250 MB. Untuk informasi selengkapnya, lihat [Kuota Lambda](#).

Fungsi Anda dapat terus menggunakan versi lapisan apa pun yang telah Anda tambahkan, bahkan setelah versi lapisan itu dihapus, atau setelah izin Anda untuk mengakses lapisan dicabut. Namun, Anda tidak dapat membuat fungsi baru yang menggunakan versi lapisan yang dihapus.

Note

Pastikan bahwa layer yang Anda tambahkan ke fungsi kompatibel dengan runtime dan arsitektur set instruksi fungsi.

Untuk menambahkan lapisan ke fungsi (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang akan dikonfigurasi.

3. Di bawah Layers, pilih Add a layer
4. Di bawah Pilih layer, pilih sumber layer:
 - a. Untuk AWS layer atau sumber layer Custom layer, pilih layer dari menu pull-down. Di bawah Version, pilih versi layer dari menu pull-down.
 - b. Untuk Tentukan sumber ARN lapisan, masukkan ARN di kotak teks dan pilih Verifikasi. Kemudian, pilih Tambah.

Urutan di mana Anda menambahkan lapisan adalah urutan di mana Lambda menggabungkan konten lapisan ke dalam lingkungan eksekusi. Anda dapat mengubah urutan penggabungan lapisan menggunakan konsol.

Untuk memperbarui urutan penggabungan lapisan untuk fungsi Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi yang akan dikonfigurasi.
3. Di bawah Layers, pilih Edit
4. Pilih salah satu layer.
5. Pilih Merge sebelumnya atau Merge nanti untuk menyesuaikan urutan layer.
6. Pilih Simpan.

Lapisan berversi. Isi dari setiap versi lapisan tidak dapat diubah. Pemilik layer dapat merilis versi layer baru untuk menyediakan konten yang diperbarui. Anda dapat menggunakan konsol untuk memperbarui versi lapisan yang dilampirkan ke fungsi Anda.

Untuk memperbarui versi lapisan untuk fungsi Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih layer yang ingin Anda perbarui versinya.
3. Pilih tab Fungsi menggunakan versi ini.
4. Pilih fungsi yang ingin Anda ubah, lalu pilih Edit.
5. Untuk versi Layer, pilih versi layer yang akan diubah.
6. Pilih fungsi Perbarui.

Anda tidak dapat memperbarui versi lapisan fungsi di seluruh AWS akun.

Topik

- [Mengakses konten lapisan dari fungsi Anda](#)
- [Menemukan informasi lapisan](#)

Mengakses konten lapisan dari fungsi Anda

Jika fungsi Lambda Anda menyertakan lapisan, Lambda mengekstrak konten lapisan ke dalam `/opt` direktori di lingkungan eksekusi fungsi. Lambda mengekstrak lapisan dalam urutan (rendah ke tinggi) yang terdaftar oleh fungsi. Lambda menggabungkan folder dengan nama yang sama. Jika file yang sama muncul di beberapa lapisan, fungsi menggunakan versi di lapisan yang terakhir diekstrak.

Setiap runtime Lambda menambahkan folder `/opt` direktori tertentu ke variabel. `PATH` Kode fungsi Anda dapat mengakses konten lapisan tanpa harus menentukan jalur. Untuk informasi selengkapnya tentang pengaturan jalur di lingkungan eksekusi Lambda, lihat [the section called “Variabel lingkungan runtime yang ditetapkan”](#).

Lihat [the section called “Jalur lapisan untuk setiap runtime Lambda”](#) untuk mempelajari di mana harus menyertakan pustaka Anda saat membuat lapisan.

Jika Anda menggunakan runtime Node.js atau Python, Anda dapat menggunakan editor kode bawaan di konsol Lambda. Anda harus dapat mengimpor pustaka apa pun yang telah Anda tambahkan sebagai lapisan ke fungsi saat ini.

Menemukan informasi lapisan

Untuk menemukan lapisan di akun Anda yang kompatibel dengan runtime fungsi Anda, gunakan file. [ListLayers](#) API Misalnya, Anda dapat menggunakan perintah `list-layers` AWS Command Line Interface (CLI) berikut:

```
aws lambda list-layers --compatible-runtime python3.9
```

Anda akan melihat output yang serupa dengan yang berikut:

```
{
  "Layers": [
    {
      "LayerName": "my-layer",
      "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
```

```

    "LatestMatchingVersion": {
      "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
      "Version": 2,
      "Description": "My layer",
      "CreateDate": "2023-11-15T00:37:46.592+0000",
      "CompatibleRuntimes": [
        "python3.9",
        "python3.10",
        "python3.11",
      ]
    }
  ]
}

```

Untuk membuat daftar semua lapisan di akun Anda, hilangkan `--compatible-runtime` opsi. Detail respons menunjukkan versi terbaru dari setiap lapisan.

Anda juga bisa mendapatkan versi terbaru dari layer menggunakan file [ListLayerVersions](#) API. Misalnya, Anda dapat menggunakan `list-layer-versions` CLI perintah berikut:

```
aws lambda list-layer-versions --layer-name my-layer
```

Anda akan melihat output yang serupa dengan yang berikut:

```

{
  "LayerVersions": [
    {
      "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
      "Version": 2,
      "Description": "My layer",
      "CreateDate": "2023-11-15T00:37:46.592+0000",
      "CompatibleRuntimes": [
        "java11"
      ]
    },
    {
      "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:1",
      "Version": 1,

```

```
    "Description": "My layer",
    "CreateDate": "2023-11-15T00:27:46.592+0000",
    "CompatibleRuntimes": [
      "java11"
    ]
  }
]
```

Menggunakan AWS CloudFormation dengan lapisan

Anda dapat menggunakan AWS CloudFormation untuk membuat layer dan mengaitkan layer dengan fungsi Lambda Anda. Contoh template berikut membuat layer bernama **my-lambda-layer** dan melampirkan layer ke fungsi Lambda menggunakan properti Layers.

```
---
Description: CloudFormation Template for Lambda Function with Lambda Layer
Resources:
  MyLambdaLayer:
    Type: AWS::Lambda::LayerVersion
    Properties:
      LayerName: my-lambda-layer
      Description: My Lambda Layer
      Content:
        S3Bucket: amzn-s3-demo-bucket
        S3Key: my-layer.zip
      CompatibleRuntimes:
        - python3.9
        - python3.10
        - python3.11

  MyLambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-lambda-function
      Runtime: python3.9
      Handler: index.handler
      Timeout: 10
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
      Layers:
        - !Ref MyLambdaLayer
```

Menggunakan AWS SAM dengan lapisan

Anda dapat menggunakan AWS Serverless Application Model (AWS SAM) untuk mengotomatiskan pembuatan lapisan dalam aplikasi Anda. Tipe sumber daya `AWS::Serverless::LayerVersion` membuat versi lapisan yang dapat Anda referensikan dari konfigurasi fungsi Lambda Anda.

```
AWSTemplateFormatVersion: '2010-09-09'  
Transform: 'AWS::Serverless-2016-10-31'  
Description: AWS SAM Template for Lambda Function with Lambda Layer
```

Resources:

MyLambdaLayer:

```
Type: AWS::Serverless::LayerVersion
```

Properties:

```
LayerName: my-lambda-layer
```

```
Description: My Lambda Layer
```

```
ContentUri: s3://amzn-s3-demo-bucket/my-layer.zip
```

CompatibleRuntimes:

```
- python3.9
```

```
- python3.10
```

```
- python3.11
```

MyLambdaFunction:

```
Type: AWS::Serverless::Function
```

Properties:

```
FunctionName: MyLambdaFunction
```

```
Runtime: python3.9
```

```
Handler: app.handler
```

```
CodeUri: s3://amzn-s3-demo-bucket/my-function
```

Layers:

```
- !Ref MyLambdaLayer
```

Menambah fungsi Lambda menggunakan ekstensi Lambda

Anda dapat menggunakan ekstensi Lambda untuk memperbanyak fungsi Lambda. Misalnya, gunakan ekstensi Lambda untuk mengintegrasikan fungsi Anda dengan alat bantu pemantauan, pengamatan, keamanan, dan pengaturan pilihan Anda. Anda dapat memilih dari serangkaian luas alat yang disediakan oleh [AWS Lambda Mitra](#), atau Anda dapat [membuat ekstensi Lambda Anda sendiri](#).

Lambda mendukung ekstensi eksternal dan internal. Ekstensi eksternal berjalan sebagai proses independen di lingkungan eksekusi dan terus berjalan setelah invokasi fungsi diproses sepenuhnya. Karena ekstensi berjalan sebagai proses terpisah, Anda dapat menuliskannya dalam bahasa yang berbeda dari fungsi. Semua ekstensi [Runtime Lambda](#) dukungan.

Ekstensi internal berjalan sebagai bagian dari proses runtime. Fungsi Anda mengakses ekstensi internal dengan menggunakan skrip pembungkus atau mekanisme dalam proses seperti `JAVA_TOOL_OPTIONS`. Untuk informasi selengkapnya, lihat [Memodifikasi lingkungan waktu pengoperasian](#).

Anda dapat menambahkan ekstensi ke fungsi menggunakan konsol Lambda, layanan AWS Command Line Interface (AWS CLI), atau infrastruktur sebagai kode (IaC) dan alat seperti AWS CloudFormation, AWS Serverless Application Model (AWS SAM), dan Terraform.

Anda dikenakan biaya untuk waktu eksekusi yang digunakan oleh ekstensi (dengan penambahan 1 ms). Tidak ada biaya untuk menginstal ekstensi Anda sendiri. Untuk informasi harga ekstensi selengkapnya, lihat [AWS Lambda Harga](#). Untuk informasi harga ekstensi mitra, lihat situs web mitra tersebut. Lihat [the section called “Mitra ekstensi”](#) daftar ekstensi mitra resmi.

Untuk tutorial tentang ekstensi dan cara menggunakannya dengan fungsi Lambda Anda, lihat Lokakarya [AWS Lambda Ekstensi](#).

Topik

- [Lingkungan eksekusi](#)
- [Dampak pada performa dan sumber daya](#)
- [Izin](#)
- [Mengkonfigurasi ekstensi Lambda](#)
- [AWS Lambda mitra ekstensi](#)
- [Menggunakan Ekstensi Lambda API untuk membuat ekstensi](#)

- [Mengakses data telemetri real-time untuk ekstensi menggunakan Telemetri API](#)

Lingkungan eksekusi

Lambda memanggil fungsi dalam [lingkungan eksekusi](#), yang menyediakan lingkungan runtime yang aman dan terisolasi. Lingkungan eksekusi mengelola sumber daya yang diperlukan untuk menjalankan fungsi Anda dan menyediakan dukungan siklus hidup untuk runtime dan ekstensi fungsi.

Siklus hidup lingkungan eksekusi mencakup fase-fase berikut:

- **Init:** Dalam fase ini, Lambda membuat atau membatalkan pembekuan lingkungan eksekusi dengan sumber daya terkonfigurasi, mengunduh kode untuk fungsi dan semua lapisan, menginisialisasi ekstensi apa pun, menginisialisasi runtime, lalu menjalankan kode inisialisasi fungsi (yaitu kode di luar handler utama). Fase Init terjadi saat invokasi pertama, atau sebelum invokasi fungsi jika Anda telah mengaktifkan [konkurensi terprovisi](#).

Fase Init dibagi ke dalam tiga subfase: `Extension init`, `Runtime init`, dan `Function init`. Subfase ini memastikan semua ekstensi dan runtime menyelesaikan tugas penyiapan mereka sebelum kode fungsi berjalan.

Ketika [Lambda SnapStart](#) diaktifkan, Init fase terjadi ketika Anda menerbitkan versi fungsi. Lambda menyimpan snapshot memori dan status disk dari lingkungan eksekusi yang diinisialisasi, mempertahankan snapshot terenkripsi, dan menyimpannya dalam cache untuk akses latensi rendah. Jika Anda memiliki [hook beforeCheckpoint runtime](#), maka kode berjalan di akhir Init fase.

- **Restore**(SnapStart only): Saat Anda pertama kali memanggil [SnapStart](#) fungsi dan saat fungsi meningkat, Lambda melanjutkan lingkungan eksekusi baru dari snapshot yang bertahan alih-alih menginisialisasi fungsi dari awal. Jika Anda memiliki [hook afterRestore\(\) runtime](#), kode berjalan di akhir Restore fase. Anda dikenakan biaya untuk durasi kait `afterRestore()` runtime. Runtime (JVM) harus dimuat dan kait `afterRestore()` runtime harus selesai dalam batas waktu tunggu (10 detik). Jika tidak, Anda akan mendapatkan `SnapStartTimeoutException`. Ketika Restore fase selesai, Lambda memanggil fungsi handler (the). [Fase invokasi](#)
- **Invoke** Dalam fase ini, Lambda memicu handler fungsi. Setelah fungsi berjalan hingga selesai, Lambda bersiap untuk menangani invokasi fungsi lain.
- **Shutdown:** Fase ini dipicu jika fungsi Lambda tidak menerima invokasi apa pun selama jangka waktu tertentu. Di fase Shutdown, Lambda menonaktifkan runtime, memberi tahu ekstensi

agar mereka berhenti dengan bersih, lalu menghapus lingkungan. Lambda mengirim peristiwa Shutdown ke setiap ekstensi, yang memberi tahu ekstensi bahwa lingkungan akan dimatikan.

Selama fase `Init`, Lambda mengekstrak lapisan yang berisi ekstensi ke direktori `/opt` di lingkungan eksekusi. Lambda mencari ekstensi di direktori `/opt/extensions/`, menginterpretasikan setiap file sebagai bootstrap yang dapat dijalankan untuk meluncurkan ekstensi, dan memulai semua ekstensi secara paralel.

Dampak pada performa dan sumber daya

Ukuran jumlah ekstensi fungsi Anda dipertimbangkan untuk batasan ukuran paket deployment. Untuk arsip file `.zip`, ukuran total fungsi tanpa zip, dan semua ekstensi tidak boleh melebihi ukuran paket deployment tanpa zip sebesar 250 MB.

Ekstensi dapat memengaruhi kinerja fungsi Anda karena mereka berbagi sumber daya fungsi seperti CPU, memori, dan penyimpanan. Sebagai contoh, jika ekstensi melakukan operasi yang intensif-komputasi, Anda dapat melihat durasi eksekusi fungsi Anda meningkat.

Setiap ekstensi harus melengkapi inisialisasinya sebelum Lambda mengaktifkan fungsi. Oleh karena itu, ekstensi yang menggunakan waktu inisialisasi yang signifikan dapat meningkatkan latensi invokasi fungsi.

Untuk mengukur waktu ekstra yang diperlukan ekstensi setelah eksekusi fungsi, Anda dapat menggunakan [metrik fungsi](#) `PostRuntimeExtensionsDuration`. Untuk mengukur peningkatan memori yang digunakan, Anda dapat menggunakan metrik `MaxMemoryUsed`. Untuk memahami dampak dari ekstensi tertentu, Anda dapat menjalankan versi yang berbeda dari fungsi Anda secara berdampingan.

Izin

Ekstensi memiliki akses ke sumber daya yang sama dengan fungsi. Karena ekstensi dieksekusi dalam lingkungan yang sama dengan fungsi, izin dibagikan antara fungsi dan ekstensi.

Untuk arsip file `.zip`, Anda dapat membuat AWS CloudFormation template untuk menyederhanakan tugas melampirkan konfigurasi ekstensi yang sama—termasuk () AWS Identity and Access Management izin—ke beberapa fungsi. IAM

Mengonfigurasi ekstensi Lambda

Mengonfigurasi ekstensi (arsip file .zip)

Anda dapat menambahkan ekstensi ke fungsi Anda sebagai [lapisan Lambda](#). Dengan menggunakan lapisan, Anda dapat berbagi ekstensi di seluruh organisasi Anda atau ke seluruh komunitas developer Lambda. Anda dapat menambahkan satu ekstensi atau lebih ke satu lapisan. Anda dapat mendaftarkan hingga 10 ekstensi untuk satu fungsi.

Anda menambahkan ekstensi ke fungsi Anda menggunakan metode yang sama seperti yang Anda lakukan untuk setiap lapisan. Untuk informasi selengkapnya, lihat [Lapisan Lambda](#).

Menambahkan ekstensi ke fungsi Anda (konsol)

1. Buka [halaman Fungsi](#) di konsol Lambda.
2. Pilih fungsi.
3. Pilih tab Kode jika belum dipilih.
4. Di bagian Lapisan, pilih Edit.
5. Untuk Pilih lapisan, pilih Tentukan ARN.
6. Untuk Tentukan ARN, masukkan Amazon Resource Name (ARN) dari lapisan ekstensi.
7. Pilih Tambahkan.

Menggunakan ekstensi dalam gambar kontainer

Anda dapat menambahkan ekstensi ke [gambar kontainer](#) Anda. Pengaturan gambar kontainer ENTRYPOINT menentukan proses utama untuk fungsi. Konfigurasi pengaturan ENTRYPOINT di Dockerfile, atau sebagai penimpa dalam konfigurasi fungsi.

Anda dapat menjalankan beberapa proses dalam satu kontainer. Lambda mengelola siklus hidup proses utama dan proses tambahan. Lambda menggunakan [API Ekstensi](#) untuk mengelola siklus hidup ekstensi.

Contoh: Menambahkan ekstensi eksternal

Ekstensi eksternal berjalan dalam proses terpisah dari fungsi Lambda. Lambda memulai proses untuk setiap ekstensi di direktori `/opt/extensions/`. Lambda menggunakan API Ekstensi untuk

mengelola siklus hidup ekstensi. Setelah fungsi berjalan sampai selesai, Lambda mengirimkan peristiwa Shutdown untuk setiap ekstensi eksternal.

Example dari menambahkan ekstensi eksternal ke gambar dasar Python

```
FROM public.ecr.aws/lambda/python:3.11

# Copy and install the app
COPY /app /app
WORKDIR /app
RUN pip install -r requirements.txt

# Add an extension from the local directory into /opt
ADD my-extension.zip /opt
CMD python ./my-function.py
```

Langkah selanjutnya

Untuk mempelajari selengkapnya tentang ekstensi, kami merekomendasikan sumber daya berikut:

- Untuk contoh kerja dasar, lihat [Membangun Ekstensi untuk AWS Lambda](#) di Blog AWS Compute.
- Untuk informasi tentang ekstensi yang disediakan Mitra AWS Lambda, lihat [Memperkenalkan Ekstensi AWS Lambda](#) pada Blog AWS Compute.
- Untuk melihat contoh ekstensi dan skrip pembungkus yang tersedia, lihat [AWS Lambda Ekstensi](#) pada repositori AWS Sampel GitHub .

AWS Lambda mitra ekstensi

AWS Lambda telah bermitra dengan beberapa entitas pihak ketiga untuk menyediakan ekstensi untuk diintegrasikan dengan fungsi Lambda Anda. Daftar berikut merinci ekstensi pihak ketiga yang siap Anda gunakan kapan saja.

- [AppDynamics](#)— Menyediakan instrumentasi otomatis fungsi Node.js atau Python Lambda, memberikan visibilitas dan peringatan pada kinerja fungsi.
- [Axiom](#)— Menyediakan dasbor untuk memantau kinerja fungsi Lambda dan metrik tingkat sistem agregat.
- [Check Point CloudGuard](#)— Solusi runtime berbasis ekstensi yang menawarkan keamanan siklus hidup penuh untuk aplikasi tanpa server.
- [Datadog](#)— Menyediakan visibilitas real-time yang komprehensif ke aplikasi tanpa server Anda melalui penggunaan metrik, jejak, dan log.
- [Dynatrace](#)— Memberikan visibilitas ke dalam jejak dan metrik, dan memanfaatkan AI untuk deteksi kesalahan otomatis dan analisis akar penyebab di seluruh tumpukan aplikasi.
- [Elastic](#)— Menyediakan Application Performance Monitoring (APM) untuk mengidentifikasi dan menyelesaikan masalah akar penyebab menggunakan jejak, metrik, dan log yang berkorelasi.
- [Epsagon](#)— Mendengarkan acara pemanggilan, menyimpan jejak, dan mengirimkannya secara paralel dengan eksekusi fungsi Lambda.
- [Fastly](#)— Melindungi fungsi Lambda Anda dari aktivitas mencurigakan, seperti serangan gaya injeksi, pengambilalihan akun melalui isian kredensial, bot berbahaya, dan penyalahgunaan. API
- [HashiCorp Vault](#)— Mengelola rahasia dan membuatnya tersedia bagi pengembang untuk digunakan dalam kode fungsi, tanpa membuat fungsi Vault sadar.
- [Honeycomb](#)— Alat observabilitas untuk men-debug tumpukan aplikasi Anda.
- [Lumigo](#)— Profil Lambda memanggil fungsi dan mengumpulkan metrik untuk memecahkan masalah di lingkungan tanpa server dan layanan mikro.
- [New Relic](#)— Berjalan bersama fungsi Lambda, secara otomatis mengumpulkan, meningkatkan, dan mengangkut telemetri ke platform observabilitas terpadu New Relic.
- [Sedai](#)— Platform manajemen cloud otonom, didukung oleh AI/ML, yang memberikan optimasi berkelanjutan untuk tim operasi cloud untuk memaksimalkan penghematan biaya cloud, kinerja, dan ketersediaan dalam skala besar.
- [Sentry](#)— Mendiagnosis, memperbaiki, dan mengoptimalkan kinerja fungsi Lambda.
- [Site24x7](#)— Mencapai observabilitas waktu nyata ke lingkungan Lambda Anda

- [Splunk](#)— Mengumpulkan metrik resolusi tinggi, latensi rendah untuk pemantauan fungsi Lambda yang efisien dan efektif.
- [Sumo Logic](#)— Memberikan visibilitas ke dalam kesehatan dan kinerja aplikasi tanpa server.
- [Thundra](#)— Menyediakan pelaporan telemetri asinkron, seperti jejak, metrik, dan log.
- [Keamanan Garam](#) - Menyederhanakan tata kelola API postur dan API keamanan untuk fungsi Lambda melalui pengaturan otomatis dan dukungan untuk runtime yang beragam.

AWS ekstensi terkelola

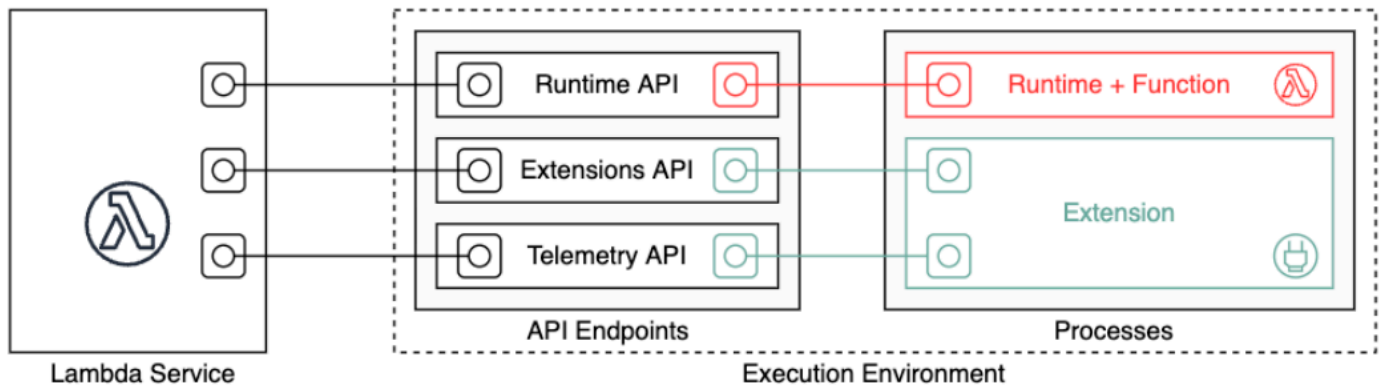
AWS menyediakan ekstensi terkelola sendiri, termasuk:

- [AWS AppConfig](#)— Gunakan bendera fitur dan data dinamis untuk memperbarui fungsi Lambda Anda. Anda juga dapat menggunakan ekstensi ini untuk memperbarui konfigurasi dinamis lainnya, seperti pelambatan operasi dan penyetelan.
- [Amazon CodeGuru Profiler](#) — Meningkatkan kinerja aplikasi dan mengurangi biaya dengan menentukan baris kode aplikasi yang paling mahal dan memberikan rekomendasi untuk meningkatkan kode.
- [CloudWatch Lambda Insights](#) — Pantau, pecahkan masalah, dan optimalkan kinerja fungsi Lambda Anda melalui dasbor otomatis.
- [AWS Distro for OpenTelemetry \(ADOT\)](#) - Memungkinkan fungsi untuk mengirim data jejak ke layanan AWS pemantauan seperti AWS X-Ray, dan ke tujuan yang mendukung OpenTelemetry seperti Honeycomb dan Lightstep.
- AWS Parameter dan Rahasia - Memungkinkan pelanggan untuk mengambil parameter dengan aman dari [AWS Systems Manager Parameter Store](#) dan rahasia dari [AWS Secrets Manager](#)

Untuk contoh ekstensi tambahan dan proyek demo, lihat [AWS Lambda Ekstensi](#).

Menggunakan Ekstensi Lambda API untuk membuat ekstensi

Penulis fungsi Lambda menggunakan ekstensi untuk mengintegrasikan Lambda Anda dengan alat pilihan mereka untuk pemantauan, pengamatan, keamanan, dan pengaturan. Penulis fungsi dapat menggunakan ekstensi dari AWS, [AWS Mitra](#), dan proyek sumber terbuka. Untuk informasi selengkapnya tentang penggunaan ekstensi, lihat [Memperkenalkan AWS Lambda Ekstensi](#) di Blog AWS Komputasi. Bagian ini menjelaskan cara menggunakan Ekstensi LambdaAPI, siklus hidup lingkungan eksekusi Lambda, dan referensi Ekstensi Lambda. API



[Sebagai pembuat ekstensi, Anda dapat menggunakan Ekstensi Lambda API untuk mengintegrasikan secara mendalam ke dalam lingkungan eksekusi Lambda.](#) Ekstensi Anda dapat mendaftar untuk fungsi dan peristiwa siklus hidup lingkungan eksekusi. Menanggapi peristiwa ini, Anda dapat memulai proses baru, menjalankan logika, dan mengontrol serta berpartisipasi dalam semua fase siklus hidup Lambda: inisialisasi, invokasi, dan penonaktifan. Selain itu, Anda dapat menggunakan [Runtime Logs API](#) untuk menerima aliran log.

Ekstensi berjalan sebagai proses independen di lingkungan eksekusi dan dapat terus berjalan setelah invokasi fungsi diproses sepenuhnya. Karena ekstensi berjalan sebagai proses, Anda dapat menuliskannya dalam bahasa yang berbeda dari fungsi. Sebaiknya terapkan ekstensi eksternal menggunakan bahasa terkompilasi. Dalam hal ini, ekstensi adalah biner mandiri yang kompatibel dengan runtime yang didukung. Semua ekstensi [Runtime Lambda](#) dukungan. Jika Anda menggunakan bahasa nonkompilasi, pastikan Anda memasukkan waktu pengoperasian yang kompatibel di ekstensi.

Lambda juga mendukung ekstensi internal. Ekstensi internal berjalan sebagai thread terpisah dari proses runtime. Runtime memulai dan menghentikan ekstensi internal. Cara alternatif untuk berintegrasi dengan lingkungan Lambda adalah dengan menggunakan [variabel lingkungan dan skrip](#)

[wrapper](#) khusus bahasa. Anda dapat menggunakan ini untuk mengonfigurasi lingkungan runtime dan memodifikasi perilaku startup proses runtime.

Anda dapat menambahkan ekstensi ke fungsi dengan dua cara. Untuk fungsi yang di-deploy sebagai [arsip file .zip](#), Anda men-deploy ekstensi sebagai [lapisan](#). Untuk fungsi yang didefinisikan sebagai gambar kontainer, Anda menambahkan [ekstensi](#) ke gambar kontainer Anda.

Note

Misalnya ekstensi dan skrip pembungkus, lihat [AWS Lambda Ekstensi](#) pada repositori AWS Sampel GitHub .

Topik

- [Siklus hidup lingkungan eksekusi Lambda](#)
- [API Referensi ekstensi](#)

Siklus hidup lingkungan eksekusi Lambda

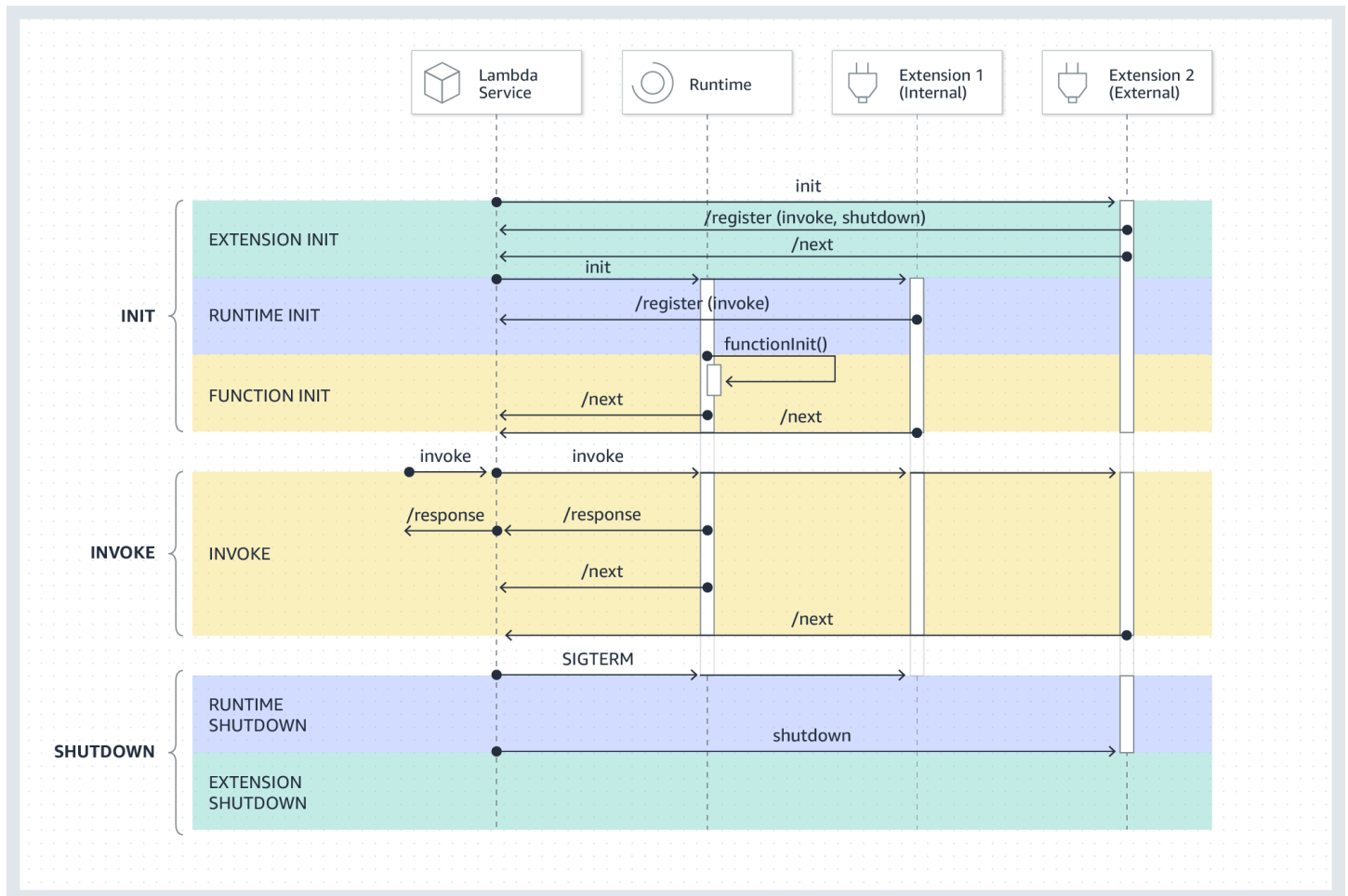
Siklus hidup lingkungan eksekusi mencakup fase-fase berikut:

- **Init:** Dalam fase ini, Lambda membuat atau membatalkan pembekuan lingkungan eksekusi dengan sumber daya terkonfigurasi, mengunduh kode untuk fungsi dan semua lapisan, menginisialisasi ekstensi apa pun, menginisialisasi runtime, lalu menjalankan kode inisialisasi fungsi (yaitu kode di luar handler utama). Fase Init terjadi saat invokasi pertama, atau sebelum invokasi fungsi jika Anda telah mengaktifkan [konkurensi terprovisi](#).

Fase Init dibagi ke dalam tiga subfase: `Extension init`, `Runtime init`, dan `Function init`. Subfase ini memastikan semua ekstensi dan runtime menyelesaikan tugas penyiapan mereka sebelum kode fungsi berjalan.

- **Invoke** Dalam fase ini, Lambda memicu handler fungsi. Setelah fungsi berjalan hingga selesai, Lambda bersiap untuk menangani invokasi fungsi lain.
- **Shutdown:** Fase ini dipicu jika fungsi Lambda tidak menerima invokasi apa pun selama jangka waktu tertentu. Di fase Shutdown, Lambda menonaktifkan runtime, memberi tahu ekstensi agar mereka berhenti dengan bersih, lalu menghapus lingkungan. Lambda mengirim kejadian Shutdown ke setiap ekstensi, yang memberi tahu ekstensi bahwa lingkungan akan dimatikan.

Setiap fase dimulai dengan peristiwa dari Lambda ke runtime dan ke semua ekstensi terdaftar. Runtime dan setiap ekstensi sinyal selesai dengan mengirimkan Next API permintaan. Lambda membekukan lingkungan eksekusi saat waktu proses telah selesai dan tidak ada kejadian yang tertunda.



Topik

- [Fase inisialisasi](#)
- [Fase invokasi](#)
- [Fase pematian](#)
- [Izin dan konfigurasi](#)
- [Penanganan kegagalan](#)
- [Pemecahan masalah ekstensi](#)

Fase inialisasi

Selama fase `Extension init`, setiap ekstensi perlu mendaftarkan dengan Lambda untuk menerima kejadian. Lambda menggunakan nama file ekstensi lengkap untuk memvalidasi bahwa ekstensi telah menyelesaikan sekuens bootstrap. Oleh karena itu, setiap `Register API` panggilan harus menyertakan `Lambda-Extension-Name` header dengan nama file lengkap ekstensi.

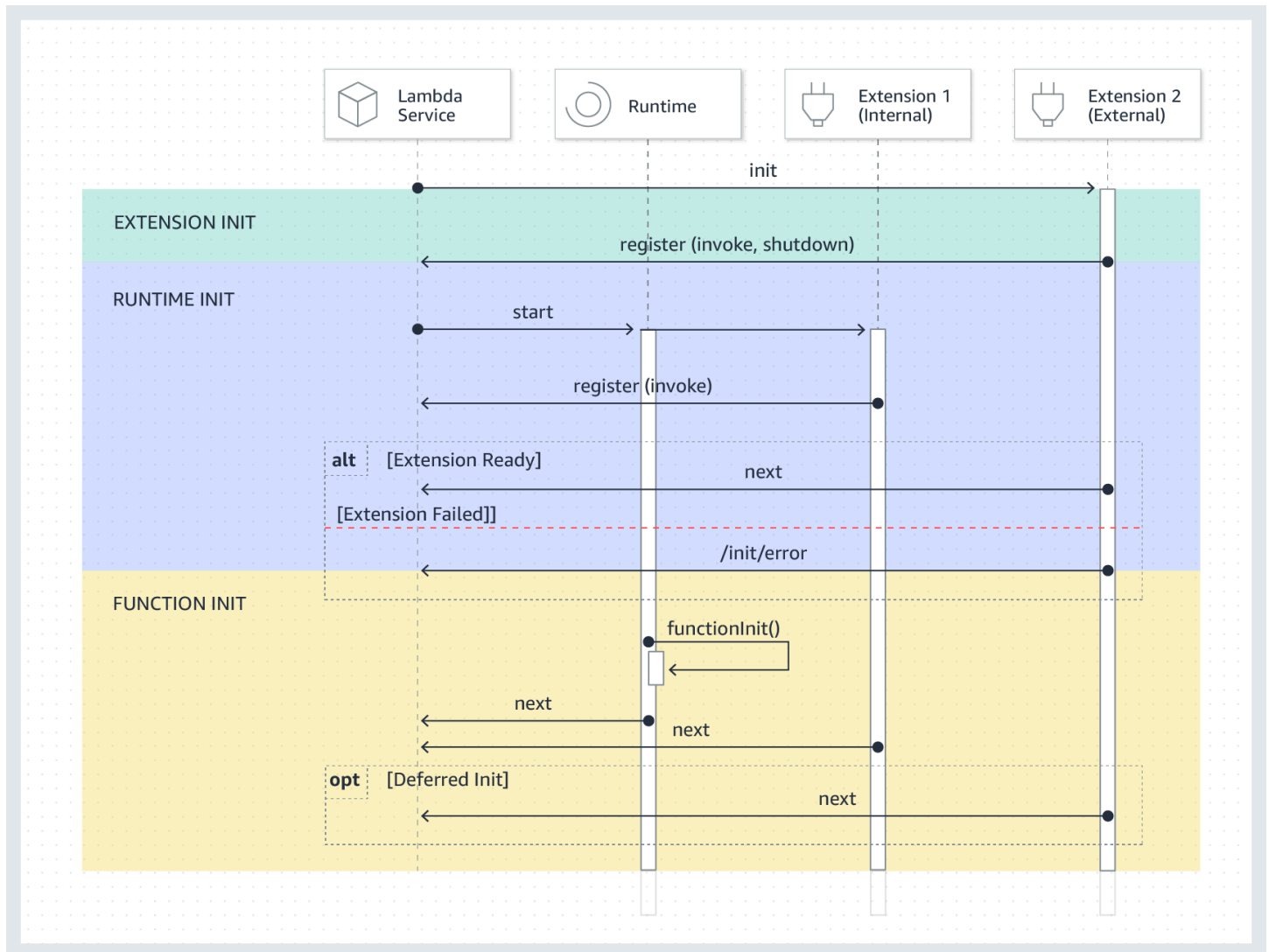
Anda dapat mendaftarkan hingga 10 ekstensi untuk satu fungsi. Batas ini diberlakukan melalui `Register API` panggilan.

Setelah setiap ekstensi mendaftar, Lambda memulai fase `Runtime init`. Proses runtime memanggil `functionInit` untuk memulai fase `Function init`.

`InitFase` selesai setelah runtime dan setiap ekstensi terdaftar menunjukkan penyelesaian dengan mengirimkan permintaan. `Next API`

Note

Ekstensi dapat menyelesaikan inialisasinya dalam fase `Init` kapan pun.



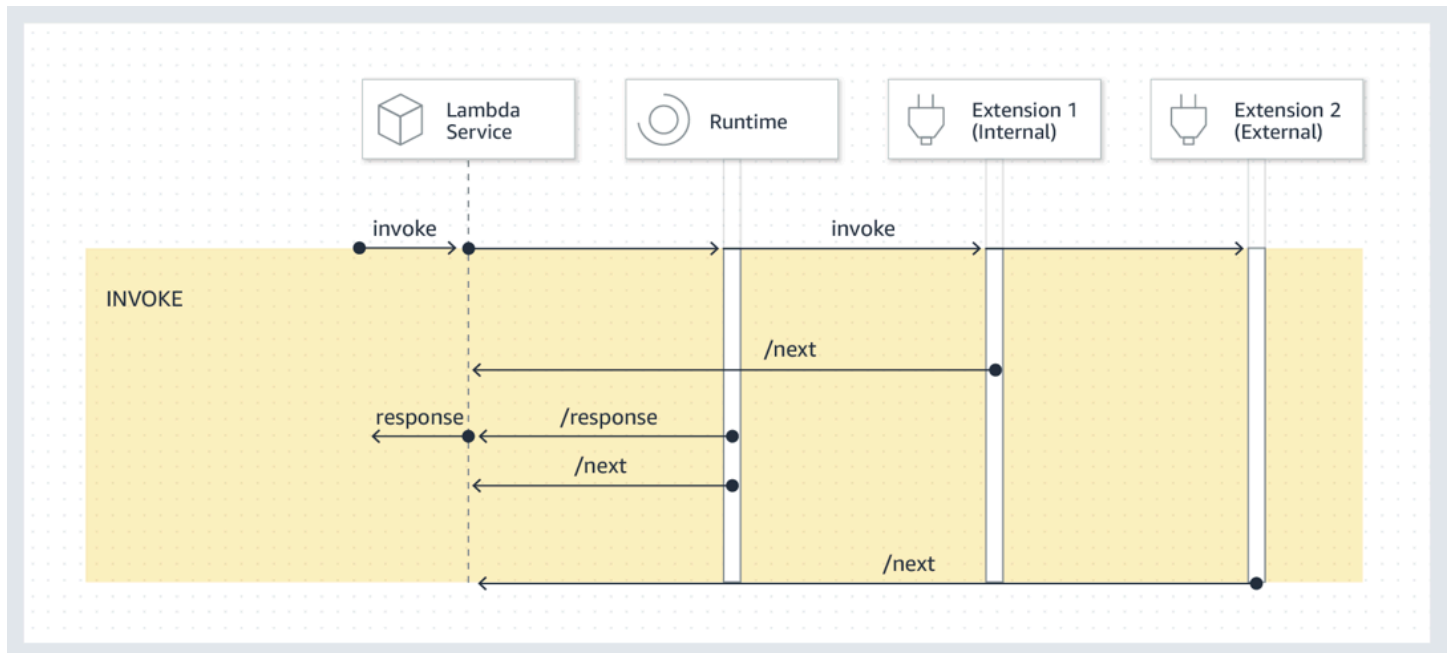
Fase invokasi

Ketika fungsi Lambda dipanggil sebagai respons terhadap permintaan NextAPI, Lambda mengirimkan Invoke acara ke runtime dan ke setiap ekstensi yang terdaftar untuk acara tersebut. Invoke

Selama invokasi, ekstensi eksternal berjalan secara paralel dengan fungsi. Ekstensi ini juga terus berjalan setelah fungsi selesai. Ini memungkinkan Anda menangkap informasi diagnostik atau mengirim log, metrik, dan jejak ke lokasi pilihan Anda.

Setelah menerima respon fungsi dari runtime, Lambda mengembalikan respon ke klien, bahkan jika ekstensi masih berjalan.

InvokeFase berakhir setelah runtime dan semua ekstensi memberi sinyal bahwa mereka dilakukan dengan mengirim Next API permintaan.



Muatan peristiwa: Peristiwa yang dikirim ke runtime (dan fungsi Lambda) memuat seluruh permintaan, header (seperti `RequestId`), dan muatan. Kejadian yang dikirim ke setiap ekstensi berisi metadata yang menjelaskan konten kejadian. Peristiwa siklus hidup ini mencakup jenis peristiwa, waktu fungsi times out (`deadlineMs`), Amazon Resource Name (ARN) fungsi yang dipanggil `requestId`, dan header penelusuran.

Ekstensi yang ingin mengakses badan acara fungsi dapat menggunakan in-runtime SDK yang berkomunikasi dengan ekstensi. Pengembang fungsi menggunakan in-runtime SDK untuk mengirim payload ke ekstensi saat fungsi dipanggil.

Berikut adalah contoh muatan:

```

{
  "eventType": "INVOKE",
  "deadlineMs": 676051,
  "requestId": "3da1f2dc-3222-475e-9205-e2e6c6318895",
  "invokedFunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:ExtensionTest",
  "tracing": {
    "type": "X-Amzn-Trace-Id",
    "value":
      "Root=1-5f35ae12-0c0fec141ab77a00bc047aa2;Parent=2be948a625588e32;Sampled=1"
  }
}
  
```

```
}  
}
```

Batas durasi: Pengaturan batas waktu fungsi membatasi durasi seluruh Invoke fase. Misalnya, jika Anda mengatur waktu fungsi habis sebagai 360 detik, fungsi dan semua ekstensi harus selesai dalam 360 detik. Perhatikan bahwa tidak ada fase pasca-invokasi yang independen. Durasi adalah total waktu yang dibutuhkan untuk runtime Anda dan semua pemanggilan ekstensi Anda selesai dan tidak dihitung sampai fungsi dan semua ekstensi selesai berjalan.

Dampak performa dan pengeluaran tambahan ekstensi: Ekstensi dapat memengaruhi performa fungsi. Sebagai penulis ekstensi, Anda memiliki kontrol atas dampak kinerja dari ekstensi Anda. Misalnya, jika ekstensi Anda melakukan operasi komputasi intensif, durasi fungsi meningkat karena ekstensi dan kode fungsi berbagi sumber daya yang sama. CPU Selain itu, jika ekstensi Anda melakukan operasi ekstensif setelah invokasi fungsi selesai, durasi fungsi meningkat karena fase Invoke berlanjut hingga semua sinyal ekstensi selesai.

Note

Lambda mengalokasikan CPU daya secara proporsional dengan pengaturan memori fungsi. Anda mungkin melihat peningkatan durasi eksekusi dan inisialisasi pada pengaturan memori yang lebih rendah karena fungsi dan proses ekstensi bersaing untuk sumber daya yang sama CPU. Untuk mengurangi eksekusi dan inisialisasi durasi, coba tingkatkan pengaturan memori.

Untuk membantu mengidentifikasi dampak performa yang muncul karena ekstensi di fase Invoke, Lambda mengeluarkan metrik `PostRuntimeExtensionsDuration`. Metrik ini mengukur waktu kumulatif yang dihabiskan antara permintaan runtime dan Next API permintaan ekstensi terakhir. Next API Untuk mengukur peningkatan memori yang digunakan, gunakan metrik `MaxMemoryUsed`. Untuk informasi selengkapnya tentang fungsi metrik, lihat [Lihat metrik untuk fungsi Lambda](#).

Pengembang fungsi dapat menjalankan versi fungsi yang berbeda secara berdampingan untuk memahami dampak ekstensi tertentu. Kami merekomendasikan agar penulis ekstensi memublikasikan konsumsi sumber daya yang diharapkan untuk mempermudah pengembang fungsi dalam memilih ekstensi yang sesuai.

Fase pematian

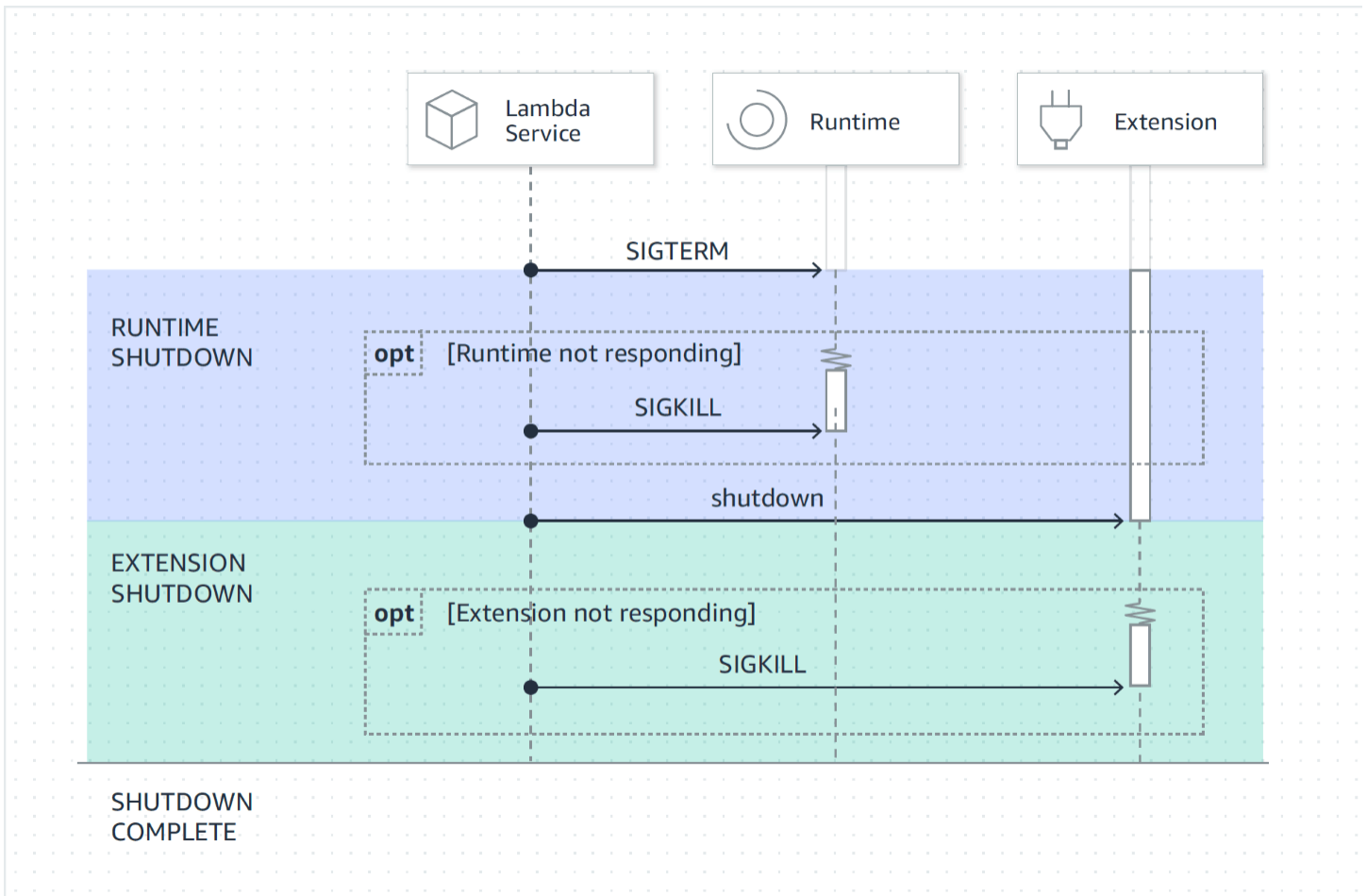
Ketika Lambda akan mematikan runtime, Lambda mengirimkan Shutdown ke setiap ekstensi eksternal terdaftar. Ekstensi dapat menggunakan waktu ini untuk tugas pembersihan akhir. Shutdown Acara dikirim sebagai tanggapan Next API atas permintaan.

Batas durasi: Durasi maksimum fase Shutdown bergantung pada konfigurasi ekstensi terdaftar:

- 0 ms - Fungsi tanpa ekstensi terdaftar
- 500 ms – Fungsi dengan ekstensi internal terdaftar.
- 2.000 ms – Fungsi dengan satu atau beberapa ekstensi eksternal terdaftar.

Untuk fungsi dengan ekstensi eksternal, Lambda mencadangkan hingga 300 ms (500 ms untuk waktu pengoperasian ekstensi internal) untuk proses waktu pengoperasian dalam melakukan pematian yang lancar. Lambda mengalokasikan sisa batas 2.000 ms untuk mematikan ekstensi eksternal.

Jika waktu pengoperasian atau ekstensi tidak merespons kejadian Shutdown dalam batasan, Lambda mengakhiri proses menggunakan sinyal SIGKILL.



Muatan peristiwa: Peristiwa Shutdown tersebut berisi alasan penonaktifan dan waktu yang tersisa dalam milidetik.

`shutdownReason` mencakup nilai-nilai berikut:

- `SPINDOWN`— Shutdown normal
- `TIMEOUT`— Batas durasi habis
- `FAILURE`— Kondisi kesalahan, seperti `out-of-memory` peristiwa

```
{
  "eventType": "SHUTDOWN",
  "shutdownReason": "reason for shutdown",
  "deadlineMs": "the time and date that the function times out in Unix time milliseconds"
}
```

Izin dan konfigurasi

Ekstensi berjalan di lingkungan eksekusi yang sama dengan fungsi Lambda. Ekstensi juga berbagi sumber daya dengan fungsi, seperti CPU, memori, dan penyimpanan /tmp disk. Selain itu, ekstensi menggunakan peran AWS Identity and Access Management (IAM) dan konteks keamanan yang sama dengan fungsi.

Sistem file dan izin akses jaringan: Ekstensi berjalan di namespace sistem file dan jaringan yang sama dengan runtime fungsi. Ini berarti ekstensi harus kompatibel dengan sistem operasi terkait. Jika ekstensi memerlukan aturan lalu lintas jaringan keluar, Anda harus menerapkan aturan ini ke konfigurasi fungsi.

Note

Karena direktori kode fungsi diatur ke baca-saja, ekstensi tidak dapat mengubah kode fungsi.

Variabel lingkungan: Ekstensi dapat mengakses [variabel lingkungan](#) fungsi, kecuali untuk variabel berikut yang spesifik untuk proses runtime:

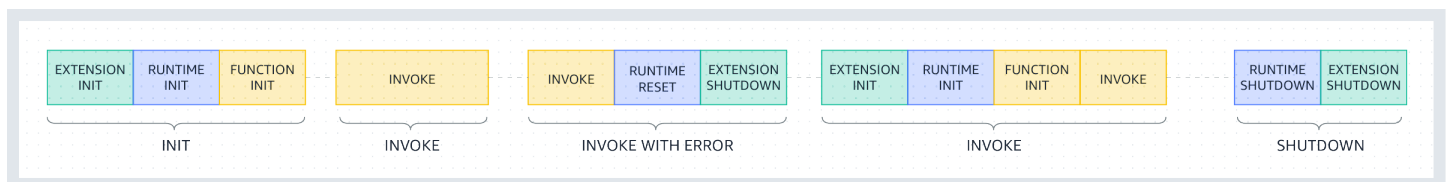
- AWS_EXECUTION_ENV
- AWS_LAMBDA_LOG_GROUP_NAME
- AWS_LAMBDA_LOG_STREAM_NAME
- AWS_XRAY_CONTEXT_MISSING
- AWS_XRAY_DAEMON_ADDRESS
- LAMBDA_RUNTIME_DIR
- LAMBDA_TASK_ROOT
- _AWS_XRAY_DAEMON_ADDRESS
- _AWS_XRAY_DAEMON_PORT
- _HANDLER

Penanganan kegagalan

Kegagalan inisialisasi: Jika ekstensi gagal, Lambda memulai ulang lingkungan eksekusi untuk memberlakukan perilaku yang konsisten dan mendorong kegagalan cepat untuk ekstensi. Selain itu, untuk beberapa pelanggan, ekstensi tersebut harus memenuhi kebutuhan kritis misi, seperti pencatatan log, keamanan, tata kelola, dan pengumpulan telemetri.

Memanggil kegagalan (seperti kehabisan memori, waktu habis fungsi): Karena ekstensi berbagi sumber daya dengan runtime, kehabisan dapat memengaruhi keduanya. Saat waktu pengoperasian gagal, semua ekstensi dan waktu pengoperasian sendiri ikut serta dalam fase Shut down. Selain itu, waktu pengoperasian dimulai ulang—baik otomatis sebagai bagian dari invokasi saat ini, atau melalui mekanisme inialisasi ulang yang ditangguhkan.

Jika ada kegagalan (seperti waktu fungsi habis atau kesalahan waktu pengoperasian) selama Invoke, layanan Lambda akan melakukan reset. Reset berperilaku seperti kejadian Shut down. Pertama, Lambda mematikan waktu pengoperasian, lalu ia mengirim kejadian Shut down untuk setiap ekstensi eksternal terdaftar. Kejadian ini mencakup alasan untuk pematian. Jika lingkungan ini digunakan untuk invokasi baru, ekstensi dan waktu pengoperasian diinisialisasi ulang sebagai bagian dari invokasi berikutnya.



Untuk penjelasan lebih rinci tentang diagram sebelumnya, lihat [Kegagalan selama fase pemanggilan](#).

Log ekstensi: Lambda mengirimkan keluaran log ekstensi ke CloudWatch Log. Lambda juga menghasilkan log acara tambahan untuk setiap ekstensi selama Init. Log acara mencatat preferensi nama dan registrasi (peristiwa, konfigurasi) saat berhasil, atau alasan kegagalan saat gagal.

Pemecahan masalah ekstensi

- Jika Register permintaan gagal, pastikan bahwa Lambda-Extension-Name header dalam Register API panggilan berisi nama file lengkap ekstensi.
- Jika permintaan Register gagal untuk ekstensi internal, pastikan permintaan tersebut tidak terdaftar untuk kejadian Shut down.

API Referensi ekstensi

API [Spesifikasi Terbuka untuk ekstensi API versi 2020-01-01](#) tersedia di sini: [extensions-api.zip](#)

Anda dapat mengambil nilai API endpoint dari variabel `AWS_LAMBDA_RUNTIME_API` lingkungan. Untuk mengirim `Register` permintaan, gunakan awalan `2020-01-01/` sebelum setiap API jalur. Sebagai contoh:

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
```

API metode

- [Pendaftaran](#)
- [Selanjutnya](#)
- [Kesalahan init](#)
- [Kesalahan keluar](#)

Pendaftaran

Selama `Extension init`, semua ekstensi perlu mendaftar dengan Lambda untuk menerima kejadian. Lambda menggunakan nama file ekstensi lengkap untuk memvalidasi bahwa ekstensi telah menyelesaikan sekuens bootstrap. Oleh karena itu, setiap `Register` API panggilan harus menyertakan `Lambda-Extension-Name` header dengan nama file lengkap ekstensi.

Ekstensi internal dimulai dan dihentikan oleh proses waktu pengoperasian sehingga tidak diizinkan untuk terdaftar untuk kejadian `Shutdown`.

Jalur – `/extension/register`

Metode - POST

Minta header

- `Lambda-Extension-Name` – Nama file lengkap ekstensi. Wajib: ya. Jenis: string.
- `Lambda-Extension-Accept-Feature`— Gunakan ini untuk menentukan fitur Ekstensi opsional selama pendaftaran. Wajib: tidak. Jenis: string dipisahkan koma. Fitur yang tersedia untuk ditentukan menggunakan pengaturan ini:
 - `accountId`— Jika ditentukan, respons pendaftaran Ekstensi akan berisi ID akun yang terkait dengan fungsi Lambda tempat Anda mendaftarkan Ekstensi.

Minta parameter tubuh

- `events` – Array kejadian yang akan didaftarkan. Wajib: tidak. Jenis: array string. String yang valid: `INVOKE`, `SHUTDOWN`.

Header respons

- `Lambda-Extension-Identifier`— Dihasilkan pengenal agen unik (UUIDstring) yang diperlukan untuk semua permintaan berikutnya.

Kode respons

- 200 – Isi respons berisi nama fungsi, versi fungsi, dan nama penanganan.
- 400 – Permintaan Buruk
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Ekstensi harus segera keluar.

Example Contoh isi permintaan

```
{
  'events': [ 'INVOKE', 'SHUTDOWN' ]
}
```

Example Contoh isi respons

```
{
  "functionName": "helloWorld",
  "functionVersion": "$LATEST",
  "handler": "lambda_function.lambda_handler"
}
```

Example Contoh badan respons dengan accountId fitur opsional

```
{
  "functionName": "helloWorld",
  "functionVersion": "$LATEST",
  "handler": "lambda_function.lambda_handler",
  "accountId": "123456789012"
}
```

```
}
```

Selanjutnya

Ekstensi mengirim Next API permintaan untuk menerima acara berikutnya, yang dapat berupa Invoke acara atau Shutdown acara. Badan respons berisi payload, yang merupakan JSON dokumen yang berisi data peristiwa.

Ekstensi mengirimkan Next API permintaan untuk memberi sinyal bahwa ia siap menerima acara baru. Ini adalah panggilan blokir.

Jangan mengatur batas waktu pada GET panggilan, karena ekstensi dapat ditangguhkan untuk jangka waktu tertentu sampai ada acara untuk kembali.

Jalur – `/extension/event/next`

Metode - GET

Minta header

- `Lambda-Extension-Identifier`— Pengidentifikasi unik untuk ekstensi (UUIDstring). Wajib: ya. Jenis: UUID string.

Header respons

- `Lambda-Extension-Event-Identifier`— Pengidentifikasi unik untuk acara (UUIDstring).

Kode respons

- 200 – Respons berisi informasi tentang kejadian berikutnya (EventInvoke atau EventShutdown).
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Ekstensi harus segera keluar.

Kesalahan init

Ekstensi menggunakan metode ini untuk melaporkan kesalahan inisialisasi ke Lambda. Panggil ini saat ekstensi gagal menginisialisasi setelah ia terdaftar. Setelah Lambda menerima kesalahan, tidak

ada API panggilan lebih lanjut yang berhasil. Ekstensi harus keluar setelah menerima respon dari Lambda.

Jalur – `/extension/init/error`

Metode - POST

Minta header

- `Lambda-Extension-Identifier` – Pengidentifikasi unik untuk ekstensi. Wajib: ya. Jenis: UUID string.
- `Lambda-Extension-Function-Error-Type` – Tipe kesalahan yang ekstensi ditemui. Wajib: ya. Header ini terdiri dari nilai string. Lambda menerima string apa pun, tetapi kami merekomendasikan format `<category.reason>`. Sebagai contoh:
 - Perpanjangan. `NoSuchHandler`
 - Perpanjangan. `APIKeyNotFound`
 - Perpanjangan. `ConfigInvalid`
 - Perpanjangan. `UnknownReason`

Minta parameter tubuh

- `ErrorRequest` – Informasi tentang kesalahan. Wajib: tidak.

Bidang ini adalah JSON objek dengan struktur sebagai berikut:

```
{
  errorMessage: string (text description of the error),
  errorType: string,
  stackTrace: array of strings
}
```

Perhatikan bahwa Lambda menerima nilai apa pun untuk `errorType`.

Contoh berikut menunjukkan pesan kesalahan fungsi Lambda ketika fungsi tidak dapat mengurai data peristiwa yang disediakan dalam invokasi.

Example Kesalahan fungsi

```
{
```

```
"errorMessage" : "Error parsing event data.",  
"errorType" : "InvalidEventDataException",  
"stackTrace": [ ]  
}
```

Kode respons

- 202 – Diterima
- 400 – Permintaan Buruk
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Ekstensi harus segera keluar.

Kesalahan keluar

Ekstensi menggunakan metode ini untuk melaporkan kesalahan ke Lambda sebelum keluar. Panggil ini saat Anda mengalami kegagalan tak terduga. Setelah Lambda menerima kesalahan, tidak ada API panggilan lebih lanjut yang berhasil. Ekstensi harus keluar setelah menerima respon dari Lambda.

Jalur – `/extension/exit/error`

Metode - POST

Minta header

- `Lambda-Extension-Identifier` – Pengidentifikasi unik untuk ekstensi. Wajib: ya. Jenis: UUID string.
- `Lambda-Extension-Function-Error-Type` – Tipe kesalahan yang ekstensi ditemui. Wajib: ya. Header ini terdiri dari nilai string. Lambda menerima string apa pun, tetapi kami merekomendasikan format `<category.reason>`. Sebagai contoh:
 - Perpanjangan. `NoSuchHandler`
 - Perpanjangan. `APIKeyNotFound`
 - Perpanjangan. `ConfigInvalid`
 - Perpanjangan. `UnknownReason`

Minta parameter tubuh

- `ErrorRequest` – Informasi tentang kesalahan. Wajib: tidak.

Bidang ini adalah JSON objek dengan struktur sebagai berikut:

```
{
  errorMessage: string (text description of the error),
  errorType: string,
  stackTrace: array of strings
}
```

Perhatikan bahwa Lambda menerima nilai apa pun untuk `errorType`.

Contoh berikut menunjukkan pesan kesalahan fungsi Lambda ketika fungsi tidak dapat mengurai data peristiwa yang disediakan dalam invokasi.

Example Kesalahan fungsi

```
{
  "errorMessage" : "Error parsing event data.",
  "errorType" : "InvalidEventDataException",
  "stackTrace": [ ]
}
```

Kode respons

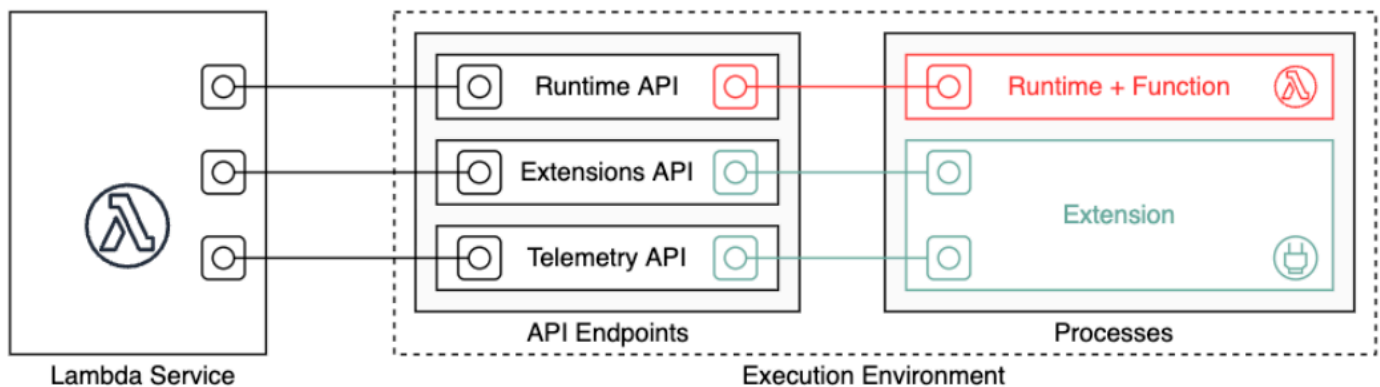
- 202 – Diterima
- 400 – Permintaan Buruk
- 403 – Dilarang
- 500 – Kesalahan penampung. Keadaan yang tidak dapat dipulihkan. Ekstensi harus segera keluar.

Mengakses data telemetri real-time untuk ekstensi menggunakan Telemetri API

Telemetri API memungkinkan ekstensi Anda menerima data telemetri langsung dari Lambda. Selama inialisasi dan pemanggilan fungsi, Lambda secara otomatis menangkap telemetri, termasuk log, metrik platform, dan jejak platform. Telemetri API memungkinkan ekstensi untuk mengakses data telemetri ini langsung dari Lambda dalam waktu dekat.

Dalam lingkungan eksekusi Lambda, Anda dapat berlangganan ekstensi Lambda Anda ke aliran telemetri. Setelah berlangganan, Lambda secara otomatis mengirimkan semua data telemetri ke ekstensi Anda. Anda kemudian memiliki fleksibilitas untuk memproses, memfilter, dan mengirimkan data ke tujuan pilihan Anda, seperti bucket Amazon Simple Storage Service (Amazon S3) atau penyedia alat observabilitas bagian ketiga.

Diagram berikut menunjukkan bagaimana Ekstensi API dan Telemetri API menghubungkan ekstensi ke Lambda dari dalam lingkungan eksekusi. Selain itu, Runtime API menghubungkan runtime dan fungsi Anda ke Lambda.



⚠ Important

Telemetri Lambda menggantikan Lambda API Log. API Meskipun Log API tetap berfungsi penuh, kami sarankan hanya menggunakan Telemetri di masa API mendatang. Anda dapat berlangganan ekstensi Anda ke aliran telemetri menggunakan Telemetri API atau Log. API Setelah berlangganan menggunakan salah satu dari ini APIs, setiap upaya untuk berlangganan menggunakan yang lain API mengembalikan kesalahan.

Ekstensi dapat menggunakan Telemetri API untuk berlangganan tiga aliran telemetri yang berbeda:

- Telemetri platform — Log, metrik, dan jejak, yang menjelaskan peristiwa dan kesalahan yang terkait dengan siklus hidup runtime lingkungan eksekusi, siklus hidup ekstensi, dan pemanggilan fungsi.
- Log fungsi - Log khusus yang dihasilkan oleh kode fungsi Lambda.
- Log ekstensi - Log khusus yang dihasilkan oleh kode ekstensi Lambda.

Note

Lambda mengirimkan log dan metrik ke CloudWatch, dan melacak ke X-Ray (jika Anda telah mengaktifkan penelusuran), bahkan jika ekstensi berlangganan aliran telemetri.

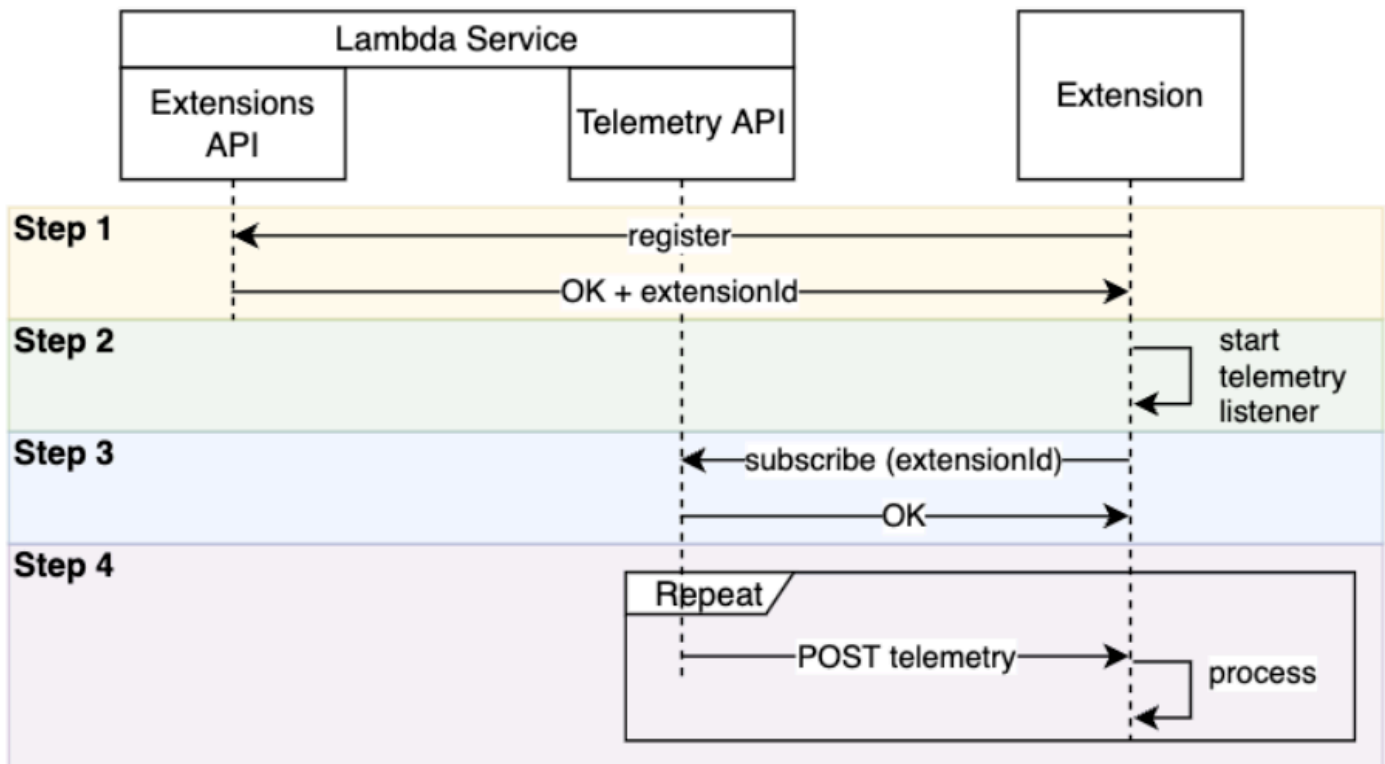
Bagian-bagian

- [Membuat ekstensi menggunakan Telemetri API](#)
- [Mendaftarkan ekstensi Anda](#)
- [Membuat pendengar telemetri](#)
- [Menentukan protokol tujuan](#)
- [Mengkonfigurasi penggunaan memori dan buffering](#)
- [Mengirim permintaan berlangganan ke Telemetri API](#)
- [Pesan API Telemetri Masuk](#)
- [Referensi API Telemetri Lambda](#)
- [Referensi skema API Event Telemetri Lambda](#)
- [Mengonversi objek API Event Telemetri Lambda ke Span OpenTelemetry](#)
- [Menggunakan Log Lambda API](#)

Membuat ekstensi menggunakan Telemetri API

Ekstensi Lambda berjalan sebagai proses independen di lingkungan eksekusi. Ekstensi dapat terus berjalan setelah pemanggilan fungsi selesai. Karena ekstensi adalah proses yang terpisah, Anda dapat menulisnya dalam bahasa yang berbeda dari kode fungsi. Kami merekomendasikan menulis ekstensi menggunakan bahasa yang dikompilasi seperti Golang atau Rust. Dengan cara ini, ekstensi adalah biner mandiri yang dapat kompatibel dengan runtime yang didukung.

Diagram berikut menggambarkan proses empat langkah untuk membuat ekstensi yang menerima dan memproses data telemetri menggunakan Telemetri API



Berikut adalah setiap langkah secara lebih rinci:

1. Daftarkan ekstensi Anda menggunakan [the section called “Ekstensi API”](#). Ini memberi Anda `Lambda-Extension-Identifier`, yang Anda perlukan dalam langkah-langkah berikut. Untuk informasi selengkapnya tentang cara mendaftarkan ekstensi Anda, lihat [the section called “Mendaftarkan ekstensi Anda”](#).
2. Buat pendengar telemetri. Ini bisa menjadi dasar HTTP atau TCP server. Lambda menggunakan URI pendengar telemetri untuk mengirim data telemetri ke ekstensi Anda. Untuk informasi selengkapnya, lihat [the section called “Membuat pendengar telemetri”](#).
3. Menggunakan Berlangganan API di TelemetriAPI, berlangganan ekstensi Anda ke aliran telemetri yang diinginkan. Anda akan memerlukan URI pendengar telemetri Anda untuk langkah ini. Untuk informasi selengkapnya, lihat [the section called “Mengirim permintaan berlangganan ke Telemetri API”](#).
4. Dapatkan data telemetri dari Lambda melalui pendengar telemetri. Anda dapat melakukan pemrosesan kustom data ini, seperti mengirimkan data ke Amazon S3 atau ke layanan observabilitas eksternal.

Note

Lingkungan eksekusi fungsi Lambda dapat dimulai dan berhenti beberapa kali sebagai bagian dari siklus hidupnya. Secara umum, kode ekstensi Anda berjalan selama pemanggilan fungsi, dan juga hingga 2 detik selama fase shutdown. Kami merekomendasikan pengelompokan telemetri saat sampai ke pendengar Anda. Kemudian, gunakan peristiwa Invoke dan Shutdown siklus hidup untuk mengirim setiap batch ke tujuan yang diinginkan.

Mendaftarkan ekstensi Anda

Sebelum Anda dapat berlangganan data telemetri, Anda harus mendaftarkan ekstensi Lambda Anda. Registrasi terjadi selama fase inisialisasi ekstensi. Contoh berikut menunjukkan HTTP permintaan untuk mendaftarkan ekstensi.

```
POST http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
Lambda-Extension-Name: lambda_extension_name
{
  'events': [ 'INVOKE', 'SHUTDOWN' ]
}
```

Jika permintaan berhasil, pelanggan menerima respons sukses HTTP 200. Header respon berisi `fileLambda-Extension-Identifier`. Badan respons mengandung sifat lain dari fungsi tersebut.

```
HTTP/1.1 200 OK
Lambda-Extension-Identifier: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
{
  "functionName": "lambda_function",
  "functionVersion": "$LATEST",
  "handler": "lambda_handler",
  "accountId": "123456789012"
}
```

Untuk informasi selengkapnya, lihat [the section called “APIReferensi ekstensi”](#).

Membuat pendengar telemetri

Ekstensi Lambda Anda harus memiliki pendengar yang menangani permintaan masuk dari Telemetri. API Kode berikut menunjukkan contoh implementasi pendengar telemetri di Golang:

```
// Starts the server in a goroutine where the log events will be sent
func (s *TelemetryApiListener) Start() (string, error) {
    address := listenOnAddress()
    l.Info("[listener:Start] Starting on address", address)
    s.httpServer = &http.Server{Addr: address}
    http.HandleFunc("/", s.http_handler)
    go func() {
        err := s.httpServer.ListenAndServe()
        if err != http.ErrServerClosed {
            l.Error("[listener:goroutine] Unexpected stop on Http Server:", err)
            s.Shutdown()
        } else {
            l.Info("[listener:goroutine] Http Server closed:", err)
        }
    }()
    return fmt.Sprintf("http://%s/", address), nil
}

// http_handler handles the requests coming from the Telemetry API.
// Everytime Telemetry API sends log events, this function will read them from the
// response body
// and put into a synchronous queue to be dispatched later.
// Logging or printing besides the error cases below is not recommended if you have
// subscribed to
// receive extension logs. Otherwise, logging here will cause Telemetry API to send new
// logs for
// the printed lines which may create an infinite loop.
func (s *TelemetryApiListener) http_handler(w http.ResponseWriter, r *http.Request) {
    body, err := ioutil.ReadAll(r.Body)
    if err != nil {
        l.Error("[listener:http_handler] Error reading body:", err)
        return
    }

    // Parse and put the log messages into the queue
    var slice []interface{}
    _ = json.Unmarshal(body, &slice)

    for _, el := range slice {
        s.LogEventsQueue.Put(el)
    }
}
```

```
1.Info("[listener:http_handler] logEvents received:", len(slice), " LogEventsQueue
length:", s.LogEventsQueue.Len())
slice = nil
}
```

Menentukan protokol tujuan

Saat Anda berlangganan untuk menerima telemetri menggunakan TelemetryAPI, Anda dapat menentukan protokol tujuan selain tujuan: URI

```
{
  "destination": {
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080"
  }
}
```

Lambda menerima dua protokol untuk menerima telemetri:

- HTTP(disarankan) - Lambda mengirimkan telemetri ke HTTP titik akhir lokal (`http://sandbox.localdomain:${PORT}/${PATH}`) sebagai larik catatan dalam format. JSON Parameter `$PATH` bersifat opsional. Lambda hanya mendukung HTTP, tidak. HTTPS Lambda memberikan telemetri melalui permintaan. POST
- TCP— Lambda mengirimkan telemetri ke TCP port dalam format [Newline](#) delimited (). JSON NDJSON

Note

Kami sangat menyarankan menggunakan HTTP daripada TCP. Dengan TCP, platform Lambda tidak dapat mengakui kapan mengirimkan telemetri ke lapisan aplikasi. Oleh karena itu, jika ekstensi Anda macet, Anda mungkin kehilangan telemetri. HTTP tidak memiliki batasan ini.

Sebelum berlangganan untuk menerima telemetri, buat HTTP pendengar atau port lokal. TCP Selama penyetulan, perhatikan hal berikut ini:

- Lambda mengirimkan telemetri hanya ke tujuan yang berada di dalam lingkungan eksekusi.

- Lambda mencoba lagi untuk mengirim telemetri (dengan backoff) tanpa adanya pendengar, atau jika permintaan mengalami kesalahan. POST Jika pendengar telemetri mogok, ia melanjutkan menerima telemetri setelah Lambda memulai ulang lingkungan eksekusi.
- Lambda mencadangkan port 9001. Tidak ada pembatasan atau rekomendasi nomor port lainnya.

Mengkonfigurasi penggunaan memori dan buffering

Penggunaan memori di lingkungan eksekusi tumbuh secara linier dengan jumlah pelanggan. Langgan mengkonsumsi sumber daya memori karena masing-masing membuka buffer memori baru untuk menyimpan data telemetri. Penggunaan memori buffer berkontribusi pada konsumsi memori secara keseluruhan di lingkungan eksekusi.

Saat berlangganan untuk menerima telemetri melalui TelemetriAPI, Anda memiliki opsi untuk menyangga data telemetri dan mengirimkannya ke pelanggan dalam batch. Untuk mengoptimalkan penggunaan memori, Anda dapat menentukan konfigurasi buffering:

```
{
  "buffering": {
    "maxBytes": 256*1024,
    "maxItems": 1000,
    "timeoutMs": 100
  }
}
```

| Parameter | Deskripsi | Default dan batas |
|-----------------------|---|---|
| <code>maxBytes</code> | Volume maksimum telemetri (dalam byte) untuk buffer dalam memori. | standar: 262.144 Minimal: 262.144 Maksimal: 1.048.576 |
| <code>maxItems</code> | Jumlah maksimum peristiwa untuk buffer dalam memori. | Default: 10.000 Minimal: 1.000 Maksimum: 10.000. |

| Parameter | Deskripsi | Default dan batas |
|------------------------|--|---|
| <code>timeoutMs</code> | Waktu maksimum (dalam milidetik) untuk buffer batch. | Default: 1.000 Minimal: 25 Maksimal: 30.000 |

Saat menyiapkan buffering, ingatlah poin-poin ini:

- Jika salah satu aliran input ditutup, Lambda akan menyiram log. Misalnya, ini dapat terjadi jika runtime mogok.
- Setiap pelanggan dapat menyesuaikan konfigurasi buffering mereka dalam permintaan berlangganan mereka.
- Saat menentukan ukuran buffer untuk membaca data, antisipasi menerima muatan sebesar $2 * \text{maxBytes} + \text{metadataBytes}$, di mana `maxBytes` merupakan komponen penyiapan buffering Anda. Untuk mengukur jumlah yang `metadataBytes` perlu dipertimbangkan, tinjau metadata berikut. Lambda menambahkan metadata yang mirip dengan ini ke setiap catatan:

```
{
  "time": "2022-08-20T12:31:32.123Z",
  "type": "function",
  "record": "Hello World"
}
```

- Jika pelanggan tidak dapat memproses telemetri masuk dengan cukup cepat, atau jika kode fungsi Anda menghasilkan volume log yang sangat tinggi, Lambda mungkin akan menjatuhkan catatan untuk menjaga pemanfaatan memori tetap terbatas. Ketika ini terjadi, Lambda mengirimkan acara `platform.logsDropped`

Mengirim permintaan berlangganan ke Telemetri API

Ekstensi Lambda dapat berlangganan untuk menerima data telemetri dengan mengirimkan permintaan berlangganan ke Telemetri. API Permintaan berlangganan harus berisi informasi tentang jenis acara yang Anda inginkan untuk berlangganan ekstensi. Selain itu, permintaan dapat berisi [informasi tujuan pengiriman](#) dan [konfigurasi buffering](#).

Sebelum mengirim permintaan berlangganan, Anda harus memiliki ID ekstensi (Lambda-Extension-Identifier). Saat Anda [mendaftarkan ekstensi Anda dengan Ekstensi API](#), Anda mendapatkan ID ekstensi dari API respons.

Langganan terjadi selama [fase inisialisasi ekstensi](#). Contoh berikut menunjukkan HTTP permintaan untuk berlangganan ketiga aliran telemetri: telemetri platform, log fungsi, dan log ekstensi.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
  "schemaVersion": "2022-12-13",
  "types": [
    "platform",
    "function",
    "extension"
  ],
  "buffering": {
    "maxItems": 1000,
    "maxBytes": 256*1024,
    "timeoutMs": 100
  },
  "destination": {
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080"
  }
}
```

Jika permintaan berhasil, maka pelanggan menerima HTTP 200 respons sukses.

```
HTTP/1.1 200 OK
"OK"
```

Pesan API Telemetri Masuk

Setelah berlangganan menggunakan TelemetriAPI, ekstensi secara otomatis mulai menerima telemetri dari Lambda melalui permintaan. POST Setiap badan POST permintaan berisi array Event objek. Masing-masing Event memiliki skema berikut:

```
{
  time: String,
  type: String,
```



```
record: Object
}
```

- `timeProperti` menentukan kapan platform Lambda menghasilkan acara. Ini berbeda dengan saat peristiwa itu benar-benar terjadi. Nilai string `time` adalah stempel waktu dalam format ISO 8601.
- `typeProperti` mendefinisikan jenis acara. Tabel berikut menjelaskan semua nilai yang mungkin.
- `recordProperti` mendefinisikan JSON objek yang berisi data telemetri. Skema JSON objek ini tergantung pada `type`

Tabel berikut merangkum semua jenis Event objek, dan tautan ke [referensi API Event skema Telemetri](#) untuk setiap jenis acara.

| Kategori | Jenis peristiwa | Deskripsi | Skema catatan acara |
|----------------|---------------------------------------|---|---|
| Acara platform | <code>platform.initStart</code> | Inisialisasi fungsi dimulai. | the section called "platform.initStart" skema |
| Acara platform | <code>platform.initRuntimeDone</code> | Inisialisasi fungsi selesai. | the section called "platform.initRuntimeDone" skema |
| Acara platform | <code>platform.initReport</code> | Laporan inisialisasi fungsi. | the section called "platform.initReport" skema |
| Acara platform | <code>platform.start</code> | Pemanggilan fungsi dimulai. | the section called "platform.start" skema |
| Acara platform | <code>platform.runtimeDone</code> | Runtime selesai memproses acara dengan keberhasilan atau kegagalan. | the section called "platform.runtimeDone" skema |

| Kategori | Jenis peristiwa | Deskripsi | Skema catatan acara |
|----------------|---|--------------------------------------|---|
| Acara platform | <code>platform.report</code> | Laporan pemanggilan fungsi. | the section called "platform.report" skema |
| Acara platform | <code>platform.restoreStart</code> | Pemulihan runtime dimulai. | the section called "platform.restoreStart" skema |
| Acara platform | <code>platform.restoreRuntimeDone</code> | Pemulihan runtime selesai. | the section called "platform.restoreRuntimeDone" skema |
| Acara platform | <code>platform.restoreReport</code> | Laporan pemulihan runtime. | the section called "platform.restoreReport" skema |
| Acara platform | <code>platform.telemetrySubscription</code> | Ekstensi berlangganan API Telemetry. | the section called "platform.telemetrySubscription" skema |
| Acara platform | <code>platform.logsDropped</code> | Lambda menjatuhkan entri log. | the section called "platform.logsDropped" skema |
| Log fungsi | <code>function</code> | Sebuah baris log dari kode fungsi. | the section called "function" skema |
| Log ekstensi: | <code>extension</code> | Sebuah baris log dari kode ekstensi. | the section called "extension" skema |

Referensi API Telemetry Lambda

Gunakan titik akhir API Telemetry Lambda untuk berlangganan ekstensi ke aliran telemetry. Anda dapat mengambil titik akhir API Telemetry dari variabel lingkungan. `AWS_LAMBDA_RUNTIME_API` Untuk mengirim permintaan API, tambahkan versi API (`2022-07-01/`) dan `telemetry/`. Sebagai contoh:

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Untuk definisi OpenAPI Specification (OAS) dari versi respons langganan 2022-12-13, lihat berikut ini:

- HTTP — [telemetry-api-http-schema.zip](#)
- TCP — [telemetry-api-tcp-schema .zip](#)

Operasi API

- [Langganan](#)

Langganan

Untuk berlangganan aliran telemetry, ekstensi Lambda dapat mengirim permintaan API Berlangganan.

- Jalur – `/telemetry`
- Metode - PUT
- Header
 - Content-Type: `application/json`
- Minta parameter tubuh
 - SchemaVersion
 - Wajib: Ya
 - Tipe: String
 - Nilai yang valid: `"2022-12-13"` atau `"2022-07-01"`
 - tujuan — Pengaturan konfigurasi yang menentukan tujuan acara telemetry dan protokol untuk pengiriman acara.
 - Diperlukan: Ya

- Tipe: Objek

```
{
  "protocol": "HTTP",
  "URI": "http://sandbox.localdomain:8080"
}
```

- Protokol — Protokol yang digunakan Lambda untuk mengirim data telemetri.
 - Wajib: Ya
 - Tipe: String
 - Nilai yang valid: "HTTP" | "TCP"
- URI — URI untuk mengirim data telemetri ke.
 - Wajib: Ya
 - Tipe: String
- Untuk informasi selengkapnya, lihat [the section called “Menentukan protokol tujuan”](#).
- jenis — Jenis telemetri yang Anda inginkan untuk berlangganan ekstensi.
 - Diperlukan: Ya
 - Tipe: Array string
 - Nilai yang valid: "platform" | "function" | "extension"
- buffering - Pengaturan konfigurasi untuk buffering acara.
 - Diperlukan: Tidak
 - Tipe: Objek

```
{
  "buffering": {
    "maxItems": 1000,
    "maxBytes": 256*1024,
    "timeoutMs": 100
  }
}
```

- maxItems – Jumlah maksimum peristiwa untuk buffer dalam memori.
 - Diperlukan: Tidak
 - Jenis: Integer

- Minimal: 1.000
- Maksimum: 10.000.
- MaxBytes — Volume maksimum telemetry (dalam byte) untuk buffer dalam memori.
 - Diperlukan: Tidak
 - Jenis: Integer
 - standar: 262.144
 - Minimal: 262.144
 - Maksimal: 1.048.576
- timeoutMs – Waktu maksimum (dalam milidetik) untuk mem-buffer batch.
 - Diperlukan: Tidak
 - Jenis: Integer
 - Default: 1.000
 - Minimal: 25
 - Maksimal: 30.000
- Untuk informasi selengkapnya, lihat [the section called “Mengkonfigurasi penggunaan memori dan buffering”](#).

Contoh Permintaan API Berlangganan

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
  "schemaVersion": "2022-12-13",
  "types": [
    "platform",
    "function",
    "extension"
  ],
  "buffering": {
    "maxItems": 1000,
    "maxBytes": 256*1024,
    "timeoutMs": 100
  },
  "destination": {
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080"
  }
}
```

```
}
```

Jika permintaan Berlangganan berhasil, ekstensi menerima respons sukses HTTP 200:

```
HTTP/1.1 200 OK  
"OK"
```

Jika permintaan Berlangganan gagal, ekstensi menerima respons kesalahan. Sebagai contoh:

```
HTTP/1.1 400 OK  
{  
  "errorType": "ValidationError",  
  "errorMessage": "URI port is not provided; types should not be empty"  
}
```

Berikut adalah beberapa kode respons tambahan yang dapat diterima ekstensi:

- 200 – Permintaan berhasil diselesaikan
- 202 – Permintaan diterima. Respons permintaan berlangganan di lingkungan pengujian lokal
- 400 — Permintaan buruk
- 500 – Kesalahan Layanan

Referensi skema API Event Telemetri Lambda

Gunakan API titik akhir Telemetri Lambda untuk berlangganan ekstensi ke aliran telemetri. Anda dapat mengambil API titik akhir Telemetri dari variabel lingkungan. `AWS_LAMBDA_RUNTIME_API` Untuk mengirim API permintaan, tambahkan API versi (`2022-07-01/`) dan `telemetry/`. Sebagai contoh:

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Untuk definisi Open API Specification (OAS) dari versi tanggapan langganan `2022-12-13`, lihat berikut ini:

- HTTP— [telemetry-api-http-schema.zip](#)
- TCP— [telemetry-api-tcp-schema.zip](#)

Tabel berikut adalah ringkasan dari semua jenis Event objek yang didukung TelemetriAPI.

| Kategori | Jenis peristiwa | Deskripsi | Skema catatan acara |
|----------------|---------------------------------------|------------------------------|---|
| Acara platform | <code>platform.initStart</code> | Inisialisasi fungsi dimulai. | the section called “platform.initStart” skema |
| Acara platform | <code>platform.initRuntimeDone</code> | Inisialisasi fungsi selesai. | the section called “platform.initRuntimeDone” skema |
| Acara platform | <code>platform.initReport</code> | Laporan inisialisasi fungsi. | the section called “platform.initReport” skema |
| Acara platform | <code>platform.start</code> | Pemanggilan fungsi dimulai. | the section called “platform.start” skema |

| Kategori | Jenis peristiwa | Deskripsi | Skema catatan acara |
|----------------|---|---|---|
| Acara platform | <code>platform.runtimeDone</code> | Runtime selesai memproses acara dengan keberhasilan atau kegagalan. | the section called "platform.runtimeDone" skema |
| Acara platform | <code>platform.report</code> | Laporan pemanggilan fungsi. | the section called "platform.report" skema |
| Acara platform | <code>platform.restoreStart</code> | Pemulihan runtime dimulai. | the section called "platform.restoreStart" skema |
| Acara platform | <code>platform.restoreRuntimeDone</code> | Pemulihan runtime selesai. | the section called "platform.restoreRuntimeDone" skema |
| Acara platform | <code>platform.restoreReport</code> | Laporan pemulihan runtime. | the section called "platform.restoreReport" skema |
| Acara platform | <code>platform.telemetrySubscription</code> | Ekstensi berlangganan API Telemetry. | the section called "platform.telemetrySubscription" skema |
| Acara platform | <code>platform.logsDropped</code> | Lambda menjatuhkan entri log. | the section called "platform.logsDropped" skema |

| Kategori | Jenis peristiwa | Deskripsi | Skema catatan acara |
|---------------|-----------------|--------------------------------------|---|
| Log fungsi | function | Sebuah baris log dari kode fungsi. | the section called “function” skema |
| Log ekstensi: | extension | Sebuah baris log dari kode ekstensi. | the section called “extension ” skema |

Daftar Isi

- [Jenis objek telemetri API Event](#)
 - [platform.initStart](#)
 - [platform.initRuntimeDone](#)
 - [platform.initReport](#)
 - [platform.start](#)
 - [platform.runtimeDone](#)
 - [platform.report](#)
 - [platform.restoreStart](#)
 - [platform.restoreRuntimeDone](#)
 - [platform.restoreReport](#)
 - [platform.extension](#)
 - [platform.telemetrySubscription](#)
 - [platform.logsDropped](#)
 - [function](#)
 - [extension](#)
- [Jenis objek bersama](#)
 - [InitPhase](#)
 - [InitReportMetrics](#)
 - [InitType](#)
 - [ReportMetrics](#)
 - [RestoreReportMetrics](#)
 - [RuntimeDoneMetrics](#)

- [Span](#)
- [Status](#)
- [TraceContext](#)
- [TracingType](#)

Jenis objek telemetri API **Event**

Bagian ini merinci jenis Event objek yang didukung API Telemetri Lambda. Dalam deskripsi peristiwa, tanda tanya (?) menunjukkan bahwa atribut mungkin tidak ada dalam objek.

platform.initStart

Sebuah `platform.initStart` peristiwa menunjukkan bahwa fase inisialisasi fungsi telah dimulai. Sebuah `platform.initStart` Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = platform.initStart
- record: PlatformInitStart
```

PlatformInitStartObjek memiliki atribut berikut:

- `functionName` – String
- `functionVersion` – String
- `initializationType`— [the section called “InitType”](#) objek
- `instanceId?` – String
- `instanceMaxMemory?` – Integer
- `fase` — [the section called “InitPhase”](#) objek
- `runtimeVersion?` – String
- `runtimeVersionArn?` – String

Berikut ini adalah contoh Event tipe `platform.initStart`:

```
{
  "time": "2022-10-12T00:00:15.064Z",
```

```

"type": "platform.initStart",
"record": {
  "initializationType": "on-demand",
  "phase": "init",
  "runtimeVersion": "nodejs-14.v3",
  "runtimeVersionArn": "arn",
  "functionName": "myFunction",
  "functionVersion": "$LATEST",
  "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
  "instanceMaxMemory": 256
}
}

```

platform.initRuntimeDone

Sebuah `platform.initRuntimeDone` peristiwa menunjukkan bahwa fase inisialisasi fungsi telah selesai. Sebuah `platform.initRuntimeDone` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.initRuntimeDone
- record: PlatformInitRuntimeDone

```

`PlatformInitRuntimeDone` objek memiliki atribut berikut:

- `initializationType`— [the section called “InitType”](#) objek
- `fase` — [the section called “InitPhase”](#) objek
- `status` - [the section called “Status”](#) objek
- `bentang?` — Daftar [the section called “Span”](#) objek

Berikut ini adalah contoh Event tipe `platform.initRuntimeDone`:

```

{
  "time": "2022-10-12T00:01:15.000Z",
  "type": "platform.initRuntimeDone",
  "record": {
    "initializationType": "on-demand"
    "status": "success",
    "spans": [
      {

```

```

        "name": "someTimeSpan",
        "start": "2022-06-02T12:02:33.913Z",
        "durationMs": 70.5
      }
    ]
  }
}

```

platform.initReport

Sebuah `platform.initReport` peristiwa berisi laporan keseluruhan dari fase inisialisasi fungsi. Sebuah `platform.initReport` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.initReport
- record: PlatformInitReport

```

PlatformInitReportObjek memiliki atribut berikut:

- `errorType?` — tali
- `initializationType`— [the section called "InitType"](#) objek
- `fase` — [the section called "InitPhase"](#) objek
- `metrik` — objek [the section called "InitReportMetrics"](#)
- `bentang?` — Daftar [the section called "Span"](#) objek
- `status` - [the section called "Status"](#) objek

Berikut ini adalah contoh Event tipe `platform.initReport`:

```

{
  "time": "2022-10-12T00:01:15.000Z",
  "type": "platform.initReport",
  "record": {
    "initializationType": "on-demand",
    "status": "success",
    "phase": "init",
    "metrics": {
      "durationMs": 125.33
    }
  }
}

```

```

    },
    "spans": [
      {
        "name": "someTimeSpan",
        "start": "2022-06-02T12:02:33.913Z",
        "durationMs": 90.1
      }
    ]
  }
}

```

platform.start

Sebuah `platform.start` peristiwa menunjukkan bahwa fase pemanggilan fungsi telah dimulai. Sebuah `platform.start` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.start
- record: PlatformStart

```

PlatformStartObjek memiliki atribut berikut:

- `requestId` – String
- `versi?` — String
- `menelusuri?` — [the section called "TraceContext"](#)

Berikut ini adalah contoh Event tipe `platform.start`:

```

{
  "time": "2022-10-12T00:00:15.064Z",
  "type": "platform.start",
  "record": {
    "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
    "version": "$LATEST",
    "tracing": {
      "spanId": "54565fb41ac79632",
      "type": "X-Amzn-Trace-Id",
      "value":
"Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
    }
  }
}

```

```

    }
  }
}

```

platform.runtimeDone

Sebuah `platform.runtimeDone` peristiwa menunjukkan bahwa fase pemanggilan fungsi telah selesai. Sebuah `platform.runtimeDone` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.runtimeDone
- record: PlatformRuntimeDone

```

PlatformRuntimeDoneObjek memiliki atribut berikut:

- `errorType?` – String
- `metrik?` — [the section called "RuntimeDoneMetrics"](#) objek
- `requestId` – String
- `status` - [the section called "Status"](#) objek
- `bentang?` — Daftar [the section called "Span"](#) objek
- `menelusuri?` — [the section called "TraceContext"](#) objek

Berikut ini adalah contoh Event tipe `platform.runtimeDone`:

```

{
  "time": "2022-10-12T00:01:15.000Z",
  "type": "platform.runtimeDone",
  "record": {
    "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
    "status": "success",
    "tracing": {
      "spanId": "54565fb41ac79632",
      "type": "X-Amzn-Trace-Id",
      "value":
"Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
    },
    "spans": [

```

```

    {
      "name": "someTimeSpan",
      "start": "2022-08-02T12:01:23:521Z",
      "durationMs": 80.0
    }
  ],
  "metrics": {
    "durationMs": 140.0,
    "producedBytes": 16
  }
}
}

```

platform.report

Sebuah `platform.report` peristiwa berisi laporan keseluruhan dari fase pemanggilan fungsi. Sebuah `platform.report` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.report
- record: PlatformReport

```

PlatformReportObjek memiliki atribut berikut:

- metrik — objek [the section called "ReportMetrics"](#)
- requestId - String
- bentang? — Daftar [the section called "Span"](#) objek
- status - [the section called "Status"](#) objek
- menelusuri? — [the section called "TraceContext"](#) objek

Berikut ini adalah contoh Event tipe `platform.report`:

```

{
  "time": "2022-10-12T00:01:15.000Z",
  "type": "platform.report",
  "record": {
    "metrics": {
      "billedDurationMs": 694,

```

```

        "durationMs": 693.92,
        "initDurationMs": 397.68,
        "maxMemoryUsedMB": 84,
        "memorySizeMB": 128
    },
    "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
}
}

```

platform.restoreStart

Sebuah `platform.restoreStart` peristiwa menunjukkan bahwa acara restorasi lingkungan fungsi dimulai. Dalam acara restorasi lingkungan, Lambda menciptakan lingkungan dari snapshot yang di-cache daripada menginisialisasi dari awal. Untuk informasi selengkapnya, lihat [Lambda SnapStart](#). Sebuah `platform.restoreStart` Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = platform.restoreStart
- record: PlatformRestoreStart

```

PlatformRestoreStartObjek memiliki atribut berikut:

- `functionName` – String
- `functionVersion` – String
- `instanceId?` – String
- `instanceMaxMemory?` – String
- `runtimeVersion?` – String
- `runtimeVersionArn?` – String

Berikut ini adalah contoh Event tipe `platform.restoreStart`:

```

{
  "time": "2022-10-12T00:00:15.064Z",
  "type": "platform.restoreStart",
  "record": {
    "runtimeVersion": "nodejs-14.v3",
    "runtimeVersionArn": "arn",

```



```
    "functionName": "myFunction",
    "functionVersion": "$LATEST",
    "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
    "instanceMaxMemory": 256
  }
}
```

platform.restoreRuntimeDone

Sebuah `platform.restoreRuntimeDone` peristiwa menunjukkan bahwa acara restorasi lingkungan fungsi selesai. Dalam acara restorasi lingkungan, Lambda menciptakan lingkungan dari snapshot yang di-cache daripada menginisialisasi dari awal. Untuk informasi selengkapnya, lihat [Lambda SnapStart](#). Sebuah `platform.restoreRuntimeDone` Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = platform.restoreRuntimeDone
- record: PlatformRestoreRuntimeDone
```

`PlatformRestoreRuntimeDone` objek memiliki atribut berikut:

- `errorType?` – String
- `bentang?` — Daftar [the section called “Span”](#) objek
- `status` - [the section called “Status”](#) objek

Berikut ini adalah contoh Event tipe `platform.restoreRuntimeDone`:

```
{
  "time": "2022-10-12T00:00:15.064Z",
  "type": "platform.restoreRuntimeDone",
  "record": {
    "status": "success",
    "spans": [
      {
        "name": "someTimeSpan",
        "start": "2022-08-02T12:01:23:521Z",
        "durationMs": 80.0
      }
    ]
  }
}
```

```
}  
}
```

platform.restoreReport

Sebuah `platform.restoreReport` peristiwa berisi laporan keseluruhan dari acara restorasi fungsi. Sebuah `platform.restoreReport` Event objek memiliki bentuk sebagai berikut:

```
Event: Object  
- time: String  
- type: String = platform.restoreReport  
- record: PlatformRestoreReport
```

PlatformRestoreReportObjek memiliki atribut berikut:

- `errorType?` — tali
- `metrik?` — [the section called "RestoreReportMetrics"](#) objek
- `bentang?` — Daftar [the section called "Span"](#) objek
- `status` - [the section called "Status"](#) objek

Berikut ini adalah contoh Event tipe `platform.restoreReport`:

```
{  
  "time": "2022-10-12T00:00:15.064Z",  
  "type": "platform.restoreReport",  
  "record": {  
    "status": "success",  
    "metrics": {  
      "durationMs": 15.19  
    },  
    "spans": [  
      {  
        "name": "someTimeSpan",  
        "start": "2022-08-02T12:01:23:521Z",  
        "durationMs": 30.0  
      }  
    ]  
  }  
}
```

platform.extension

Sebuah extension peristiwa berisi log dari kode ekstensi. Sebuah extension Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = extension
- record: {}
```

PlatformExtensionObjek memiliki atribut berikut:

- event — Daftar String
- nama — String
- negara — String

Berikut ini adalah contoh Event tipeplatform.extension:

```
{
  "time": "2022-10-12T00:02:15.000Z",
  "type": "platform.extension",
  "record": {
    "events": [ "INVOKE", "SHUTDOWN" ],
    "name": "my-telemetry-extension",
    "state": "Ready"
  }
}
```

platform.telemetrySubscription

Sebuah platform.telemetrySubscription acara berisi informasi tentang langganan ekstensi. Sebuah platform.telemetrySubscription Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = platform.telemetrySubscription
- record: PlatformTelemetrySubscription
```

PlatformTelemetrySubscriptionObjek memiliki atribut berikut:

- nama — String
- negara — String
- jenis — Daftar String

Berikut ini adalah contoh Event tipe `platform.telemetrySubscription`:

```
{
  "time": "2022-10-12T00:02:35.000Z",
  "type": "platform.telemetrySubscription",
  "record": {
    "name": "my-telemetry-extension",
    "state": "Subscribed",
    "types": [ "platform", "function" ]
  }
}
```

platform.logsDropped

Sebuah `platform.logsDropped` acara berisi informasi tentang peristiwa yang dijatuhkan. Lambda memancarkan `platform.logsDropped` peristiwa ketika suatu fungsi mengeluarkan log pada tingkat yang terlalu tinggi bagi Lambda untuk memprosesnya. Ketika Lambda tidak dapat mengirim log ke CloudWatch atau ke ekstensi yang berlangganan Telemetri API dengan kecepatan yang dihasilkannya, Lambda akan menjatuhkan log untuk mencegah eksekusi fungsi melambat. Sebuah `platform.logsDropped` Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = platform.logsDropped
- record: PlatformLogsDropped
```

`PlatformLogsDropped` objek memiliki atribut berikut:

- `droppedBytes` – Integer
- `droppedRecords` – Integer
- alasan — String

Berikut ini adalah contoh Event tipe `platform.logsDropped`:

```
{
  "time": "2022-10-12T00:02:35.000Z",
  "type": "platform.logsDropped",
  "record": {
    "droppedBytes": 12345,
    "droppedRecords": 123,
    "reason": "Some logs were dropped because the downstream consumer is slower
than the logs production rate"
  }
}
```

function

Sebuah function peristiwa berisi log dari kode fungsi. Sebuah function Event objek memiliki bentuk sebagai berikut:

```
Event: Object
- time: String
- type: String = function
- record: {}
```

Format record bidang tergantung pada apakah log fungsi Anda diformat dalam teks biasa atau JSON format. Untuk mempelajari lebih lanjut tentang opsi konfigurasi format log, lihat [the section called “Mengkonfigurasi JSON dan format log teks biasa”](#)

Berikut ini adalah contoh Event jenis function di mana format log adalah teks biasa:

```
{
  "time": "2022-10-12T00:03:50.000Z",
  "type": "function",
  "record": "[INFO] Hello world, I am a function!"
}
```

Berikut ini adalah contoh Event jenis function di mana format log adalah JSON:

```
{
  "time": "2022-10-12T00:03:50.000Z",
  "type": "function",
  "record": {
    "timestamp": "2022-10-12T00:03:50.000Z",
    "level": "INFO",
  }
}
```

```

    "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
    "message": "Hello world, I am a function!"
  }
}

```

Note

Jika versi skema yang Anda gunakan lebih lama dari 2022-12-13 versi, maka versi selalu "record" dirender sebagai string bahkan ketika format logging fungsi Anda dikonfigurasi sebagai JSON.

extension

Sebuah extension peristiwa berisi log dari kode ekstensi. Sebuah extension Event objek memiliki bentuk sebagai berikut:

```

Event: Object
- time: String
- type: String = extension
- record: {}

```

Format record bidang tergantung pada apakah log fungsi Anda diformat dalam teks biasa atau JSON format. Untuk mempelajari lebih lanjut tentang opsi konfigurasi format log, lihat [the section called "Mengkonfigurasi JSON dan format log teks biasa"](#)

Berikut ini adalah contoh Event jenis extension di mana format log adalah teks biasa:

```

{
  "time": "2022-10-12T00:03:50.000Z",
  "type": "extension",
  "record": "[INFO] Hello world, I am an extension!"
}

```

Berikut ini adalah contoh Event jenis extension di mana format log adalah JSON:

```

{
  "time": "2022-10-12T00:03:50.000Z",
  "type": "extension",
  "record": {
    "timestamp": "2022-10-12T00:03:50.000Z",

```

```
    "level": "INFO",
    "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
    "message": "Hello world, I am an extension!"
  }
}
```

Note

Jika versi skema yang Anda gunakan lebih lama dari 2022-12-13 versi, maka versi selalu "record" dirender sebagai string bahkan ketika format logging fungsi Anda dikonfigurasi sebagai JSON.

Jenis objek bersama

Bagian ini merinci jenis objek bersama yang didukung API Telemetry Lambda.

InitPhase

Sebuah string enum yang menggambarkan fase ketika langkah inisialisasi terjadi. Dalam kebanyakan kasus, Lambda menjalankan kode inisialisasi fungsi selama fase. `init` Namun, dalam beberapa kasus kesalahan, Lambda dapat menjalankan kembali kode inisialisasi fungsi selama fase. `invoke` (Ini disebut `init` yang ditekan.)

- Jenis - String
- Nilai yang valid - `init` | `invoke` | `snap-start`

InitReportMetrics

Objek yang berisi metrik tentang fase inisialisasi.

- Jenis - Object

Sebuah `InitReportMetrics` objek memiliki bentuk sebagai berikut:

```
InitReportMetrics: Object
- durationMs: Double
```

Berikut ini adalah contoh `InitReportMetrics` objek:

```
{
  "durationMs": 247.88
}
```

InitType

Sebuah string enum yang menjelaskan bagaimana Lambda menginisialisasi lingkungan.

- Jenis - String
- Nilai yang valid - on-demand | provisioned-concurrency

ReportMetrics

Objek yang berisi metrik tentang fase selesai.

- Jenis - Object

Sebuah ReportMetrics objek memiliki bentuk sebagai berikut:

```
ReportMetrics: Object
- billedDurationMs: Integer
- durationMs: Double
- initDurationMs?: Double
- maxMemoryUsedMB: Integer
- memorySizeMB: Integer
- restoreDurationMs?: Double
```

Berikut ini adalah contoh ReportMetrics objek:

```
{
  "billedDurationMs": 694,
  "durationMs": 693.92,
  "initDurationMs": 397.68,
  "maxMemoryUsedMB": 84,
  "memorySizeMB": 128
}
```

RestoreReportMetrics

Objek yang berisi metrik tentang fase restorasi selesai.

- **Jenis - Object**

Sebuah `RestoreReportMetrics` objek memiliki bentuk sebagai berikut:

```
RestoreReportMetrics: Object
- durationMs: Double
```

Berikut ini adalah contoh `RestoreReportMetrics` objek:

```
{
  "durationMs": 15.19
}
```

RuntimeDoneMetrics

Objek yang berisi metrik tentang fase pemanggilan.

- **Jenis - Object**

Sebuah `RuntimeDoneMetrics` objek memiliki bentuk sebagai berikut:

```
RuntimeDoneMetrics: Object
- durationMs: Double
- producedBytes?: Integer
```

Berikut ini adalah contoh `RuntimeDoneMetrics` objek:

```
{
  "durationMs": 200.0,
  "producedBytes": 15
}
```

Span

Objek yang berisi detail tentang rentang. Rentang mewakili unit kerja atau operasi dalam jejak. Untuk informasi selengkapnya tentang [rentang](#), lihat [Span](#) di API halaman Penelusuran situs web OpenTelemetry Dokumen.

Lambda mendukung rentang berikut untuk acara tersebut: `platform.RuntimeDone`

- `responseLatencyRentang` menjelaskan berapa lama waktu yang dibutuhkan fungsi Lambda Anda untuk mulai mengirim respons.
- `responseDurationRentang` menjelaskan berapa lama waktu yang dibutuhkan fungsi Lambda Anda untuk menyelesaikan pengiriman seluruh respons.
- `runtimeOverheadRentang` menjelaskan berapa lama waktu yang dibutuhkan runtime Lambda untuk memberi sinyal bahwa ia siap untuk memproses pemanggilan fungsi berikutnya. Ini adalah berapa lama waktu yang dibutuhkan untuk memanggil [pemanggilan berikutnya](#) API untuk mendapatkan acara berikutnya setelah mengembalikan respons fungsi Anda.

Berikut ini adalah contoh objek `responseLatency` span:

```
{
  "name": "responseLatency",
  "start": "2022-08-02T12:01:23.521Z",
  "durationMs": 23.02
}
```

Status

Objek yang menggambarkan status fase inisialisasi atau pemanggilan. Jika statusnya salah satu `failure` atau `error`, maka `Status` objek juga berisi `errorType` bidang yang menjelaskan kesalahan.

- Jenis - Object
- Nilai status yang valid - `success` | `failure` | `error` | `timeout`

TraceContext

Objek yang menggambarkan sifat-sifat jejak.

- Jenis - Object

Sebuah `TraceContext` objek memiliki bentuk sebagai berikut:

```
TraceContext: Object
- spanId?: String
- type: TracingType enum
```

```
- value: String
```

Berikut ini adalah contoh TraceContext objek:

```
{
  "spanId": "073a49012f3c312e",
  "type": "X-Amzn-Trace-Id",
  "value":
  "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
}
```

TracingType

Sebuah string enum yang menggambarkan jenis tracing dalam suatu [the section called "TraceContext"](#) objek.

- Jenis - String
- Nilai yang valid - X-Amzn-Trace-Id

Mengonversi objek API **Event** Telemetry Lambda ke Span OpenTelemetry

API Skema AWS Lambda Telemetry secara semantik kompatibel dengan (). OpenTelemetry OTel Ini berarti Anda dapat mengonversi API Event objek AWS Lambda Telemetry Anda ke OpenTelemetry (OTel) Rentang. Saat mengonversi, Anda tidak boleh memetakan satu Event objek ke satu OTel Span. Sebagai gantinya, Anda harus menyajikan ketiga peristiwa yang terkait dengan fase siklus hidup dalam satu OTel Span. Misalnya, `startRuntimeDone`, dan `runtimeReport` peristiwa mewakili pemanggilan fungsi tunggal. Hadirkan ketiga acara ini sebagai OTel Span tunggal.

Anda dapat mengonversi acara menggunakan Span Events atau Child (nested) Span. Tabel pada halaman ini menjelaskan pemetaan antara properti API skema Telemetry dan properti OTel Span untuk kedua pendekatan. Untuk informasi selengkapnya tentang OTel Span, lihat [Span](#) di API halaman Penelusuran situs web OpenTelemetry Dokumen.

Bagian-bagian

- [Peta ke OTel Bentang dengan Acara Span](#)
- [Peta ke OTel Bentang dengan Rentang Anak](#)

Peta ke OTel Bentang dengan Acara Span

Dalam tabel berikut, `e` mewakili peristiwa yang berasal dari sumber telemetry.

Memetakan acara *Mulai

| OpenTelemetry | Skema Telemetry Lambda API |
|-----------------------------|--|
| <code>Span.Name</code> | Ekstensi Anda menghasilkan nilai ini berdasarkan <code>type</code> bidang. |
| <code>Span.StartTime</code> | Gunakan <code>e.time</code> . |
| <code>Span.EndTime</code> | N/A, karena acara belum selesai. |
| <code>Span.Kind</code> | Setel ke <code>Server</code> . |
| <code>Span.Status</code> | Setel ke <code>Unset</code> . |

| OpenTelemetry | Skema Telemetry Lambda API |
|--|--|
| <code>Span.TraceId</code> | Parse AWS X-Ray header yang ditemukan <code>die.tracing.value</code> , lalu gunakan <code>TraceId</code> nilainya. |
| <code>Span.ParentId</code> | Parse header X-Ray yang ditemukan <code>die.tracing.value</code> , lalu gunakan <code>Parent</code> nilainya. |
| <code>Span.SpanId</code> | Gunakan <code>e.tracing.spanId</code> jika tersedia. Jika tidak, buat yang baru <code>SpanId</code> . |
| <code>Span.SpanContext.TraceState</code> | N/A untuk konteks jejak X-Ray. |
| <code>Span.SpanContext.TraceFlags</code> | Parse header X-Ray yang ditemukan <code>die.tracing.value</code> , lalu gunakan <code>Sampled</code> nilainya. |
| <code>Span.Attributes</code> | Ekstensi Anda dapat menambahkan nilai kustom apa pun di sini. |

Memetakan acara* `RuntimeDone`

| OpenTelemetry | Skema Telemetry Lambda API |
|-----------------------------|--|
| <code>Span.Name</code> | Ekstensi Anda menghasilkan nilai berdasarkan <code>type</code> bidang. |
| <code>Span.StartTime</code> | Gunakan <code>e.time</code> dari <code>*Start</code> acara yang cocok. Alternatif lainnya, gunakan <code>e.time - e.metrics.durationMs</code> . |
| <code>Span.EndTime</code> | N/A, karena acara belum selesai. |
| <code>Span.Kind</code> | Setel ke <code>Server</code> . |

| OpenTelemetry | Skema Telemetri Lambda API |
|--|--|
| <code>Span.Status</code> | Jika <code>e.status</code> tidak sama dengan <code>success</code> , maka atur <code>setError</code> . Jika tidak, atur ke <code>Ok</code> . |
| <code>Span.Events[]</code> | Gunakan <code>e.spans[]</code> . |
| <code>Span.Events[i].Name</code> | Gunakan <code>e.spans[i].name</code> . |
| <code>Span.Events[i].Time</code> | Gunakan <code>e.spans[i].start</code> . |
| <code>Span.TraceId</code> | Parse AWS X-Ray header yang ditemukan di <code>e.tracing.value</code> , lalu gunakan <code>TraceId</code> nilainya. |
| <code>Span.ParentId</code> | Parse header X-Ray yang ditemukan di <code>e.tracing.value</code> , lalu gunakan <code>Parent</code> nilainya. |
| <code>Span.SpanId</code> | Gunakan hal yang sama <code>SpanId</code> dari <code>*Start</code> acara tersebut. Jika tidak tersedia, maka gunakan <code>e.tracing.spanId</code> , atau buat yang baru <code>SpanId</code> . |
| <code>Span.SpanContext.TraceState</code> | N/A untuk konteks jejak X-Ray. |
| <code>Span.SpanContext.TraceFlags</code> | Parse header X-Ray yang ditemukan di <code>e.tracing.value</code> , lalu gunakan <code>Sampled</code> nilainya. |
| <code>Span.Attributes</code> | Ekstensi Anda dapat menambahkan nilai kustom apa pun di sini. |

Memetakan *Laporkan peristiwa

| OpenTelemetry | Skema Telemetri Lambda API |
|--|--|
| <code>Span.Name</code> | Ekstensi Anda menghasilkan nilai berdasarkan <code>type</code> bidang. |
| <code>Span.StartTime</code> | Gunakan <code>e.time</code> dari <code>*Start</code> acara yang cocok. Alternatif lainnya, gunakan <code>e.time - e.metrics.durationMs</code> . |
| <code>Span.EndTime</code> | Gunakan <code>e.time</code> . |
| <code>Span.Kind</code> | Setel ke <code>Server</code> . |
| <code>Span.Status</code> | Gunakan nilai yang sama dengan <code>*RuntimeDone</code> acara. |
| <code>Span.TraceId</code> | Parse AWS X-Ray header yang ditemukan di <code>die.tracing.value</code> , lalu gunakan <code>TraceId</code> nilainya. |
| <code>Span.ParentId</code> | Parse header X-Ray yang ditemukan di <code>die.tracing.value</code> , lalu gunakan <code>Parent</code> nilainya. |
| <code>Span.SpanId</code> | Gunakan hal yang sama <code>SpanId</code> dari <code>*Start</code> acara tersebut. Jika tidak tersedia, maka gunakan <code>e.tracing.spanId</code> , atau buat yang baru <code>SpanId</code> . |
| <code>Span.SpanContext.TraceState</code> | N/A untuk konteks jejak X-Ray. |
| <code>Span.SpanContext.TraceFlags</code> | Parse header X-Ray yang ditemukan di <code>die.tracing.value</code> , lalu gunakan <code>Sampled</code> nilainya. |
| <code>Span.Attributes</code> | Ekstensi Anda dapat menambahkan nilai kustom apa pun di sini. |

Peta ke OTEL Bentang dengan Rentang Anak

Tabel berikut menjelaskan cara mengonversi API peristiwa Telemetri Lambda menjadi OTEL Rentang dengan Rentang Anak (bersarang) untuk Rentang. *RuntimeDone Untuk *Start dan *Report pemetaan, lihat tabel di [the section called “Peta ke OTEL Bentang dengan Acara Span”](#), karena sama untuk Child Spans. Dalam tabel ini, e mewakili peristiwa yang berasal dari sumber telemetri.

Memetakan acara* RuntimeDone

| OpenTelemetry | Skema Telemetri Lambda API |
|----------------|---|
| Span.Name | Ekstensi Anda menghasilkan nilai berdasarkan type bidang. |
| Span.StartTime | Gunakan e.time dari *Start acara yang cocok. Alternatif lainnya, gunakan e.time - e.metrics.durationMs . |
| Span.EndTime | N/A, karena acara belum selesai. |
| Span.Kind | Setel keServer. |
| Span.Status | Jika e.status tidak sama success, maka atur keError. Jika tidak, atur keOk. |
| Span.TraceId | Parse AWS X-Ray header yang ditemukan die.tracing.value , lalu gunakan TraceId nilainya. |
| Span.ParentId | Parse header X-Ray yang ditemukan die.tracing.value , lalu gunakan Parent nilainya. |
| Span.SpanId | Gunakan hal yang sama SpanId dari *Start acara tersebut. Jika tidak tersedia, maka |

| OpenTelemetry | Skema Telemetri Lambda API |
|--|---|
| | gunakane <code>.tracing.spanId</code> , atau buat yang baru <code>SpanId</code> . |
| <code>Span.SpanContext.TraceState</code> | N/A untuk konteks jejak X-Ray. |
| <code>Span.SpanContext.TraceFlags</code> | Parse header X-Ray yang ditemukan die <code>.tracing.value</code> , lalu gunakan <code>Sampled</code> nilainya. |
| <code>Span.Attributes</code> | Ekstensi Anda dapat menambahkan nilai kustom apa pun di sini. |
| <code>ChildSpan[i].Name</code> | Gunakan <code>e.spans[i].name</code> . |
| <code>ChildSpan[i].StartTime</code> | Gunakan <code>e.spans[i].start</code> . |
| <code>ChildSpan[i].EndTime</code> | Gunakan <code>e.spans[i].start + e.spans[i].durations</code> . |
| <code>ChildSpan[i].Kind</code> | Sama seperti orang tua <code>Span.Kind</code> . |
| <code>ChildSpan[i].Status</code> | Sama seperti orang tua <code>Span.Status</code> . |
| <code>ChildSpan[i].TraceId</code> | Sama seperti orang tua <code>Span.TraceId</code> . |
| <code>ChildSpan[i].ParentId</code> | Gunakan orang tua <code>Span.SpanId</code> . |
| <code>ChildSpan[i].SpanId</code> | Hasilkan yang baru <code>SpanId</code> . |
| <code>ChildSpan[i].SpanContext.TraceState</code> | N/A untuk konteks jejak X-Ray. |
| <code>ChildSpan[i].SpanContext.TraceFlags</code> | Sama seperti orang tua <code>Span.SpanContext.TraceFlags</code> . |

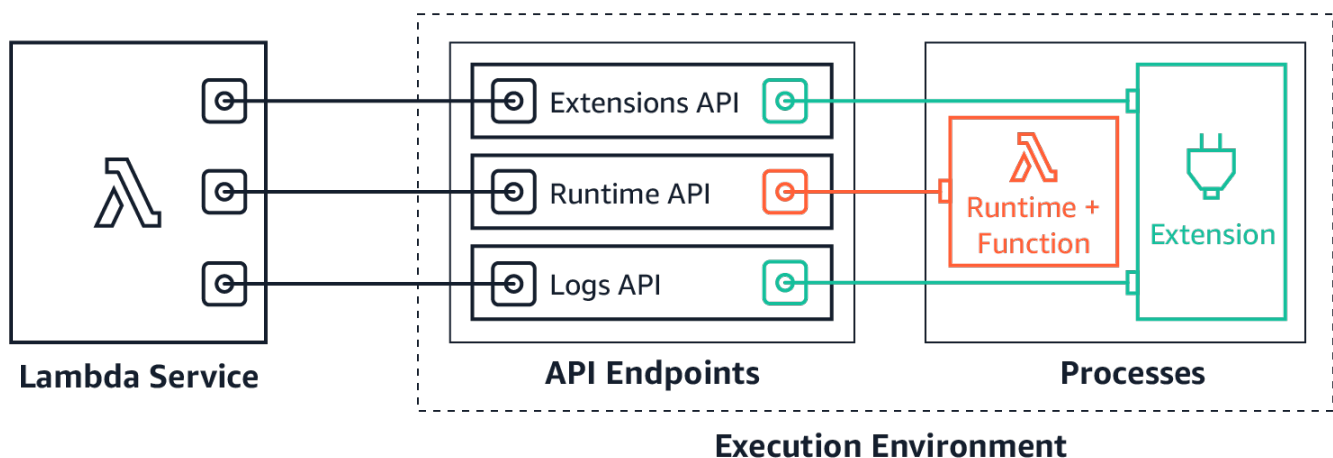
Menggunakan Log Lambda API

⚠ Important

Telemetri Lambda menggantikan Lambda API Log. API Meskipun Log API tetap berfungsi penuh, kami sarankan hanya menggunakan Telemetri API ke depan. Anda dapat berlangganan ekstensi Anda ke aliran telemetri menggunakan Telemetri API atau Log. API Setelah berlangganan menggunakan salah satu dari ini APIs, setiap upaya untuk berlangganan menggunakan yang lain API mengembalikan kesalahan.

Lambda secara otomatis menangkap log runtime dan mengalirkannya ke Amazon. CloudWatch Aliran log ini berisi log yang dibuat oleh kode fungsi dan ekstensi Anda, dan juga log yang dibuat oleh Lambda sebagai bagian dari invokasi fungsi.

[Ekstensi Lambda dapat menggunakan Lambda Runtime Logs API untuk berlangganan streaming log langsung dari dalam lingkungan eksekusi Lambda.](#) Lambda mengalirkan log ke ekstensi, dan ekstensi kemudian dapat memproses, memfilter, dan mengirim log ke tujuan yang diinginkan.



Log API memungkinkan ekstensi untuk berlangganan tiga aliran log yang berbeda:

- Log fungsi yang dibuat oleh fungsi Lambda dan ditulis ke `stdout` atau `stderr`.
- Log ekstensi yang dibuat kode ekstensi.
- Log platform Lambda, yang mencatat peristiwa dan kesalahan yang terkait dengan invokasi dan ekstensi.

 Note

Lambda mengirimkan semua log ke CloudWatch, bahkan ketika ekstensi berlangganan ke satu atau beberapa aliran log.


Topik

- [Berlangganan untuk menerima log](#)
- [Penggunaan memori](#)
- [Protokol tujuan](#)
- [Konfigurasi buffering](#)
- [Contoh berlangganan](#)
- [Contoh kode untuk Log API](#)
- [APIReferensi log](#)
- [Log pesan](#)

Berlangganan untuk menerima log

Ekstensi Lambda dapat berlangganan untuk menerima log dengan mengirimkan permintaan berlangganan ke Log. API

Untuk berlangganan guna menerima log, Anda memerlukan pengidentifikasi ekstensi (Lambda-Extension-Identifier). Pertama, [daftarkan ekstensi](#) untuk menerima pengidentifikasi ekstensi. Kemudian berlangganan Log API selama [inisialisasi](#). Setelah fase inisialisasi selesai, Lambda tidak memproses permintaan langganan.

 Note

APILangganan log idempoten. Permintaan berlangganan duplikat tidak menghasilkan langganan duplikat.

Penggunaan memori

Penggunaan memori meningkat secara linear seiring bertambahnya jumlah pelanggan. Langganan menghabiskan sumber daya memori karena setiap langganan membuka buffer memori baru untuk

menyimpan log. Untuk membantu mengoptimalkan penggunaan memori, Anda dapat menyesuaikan [konfigurasi buffering](#). Penggunaan memori buffer dihitung untuk konsumsi memori keseluruhan dalam lingkungan eksekusi.

Protokol tujuan

Anda dapat memilih salah satu protokol berikut untuk menerima log:

1. HTTP(disarankan) - Lambda mengirimkan log ke HTTP titik akhir lokal (`http://sandbox.localdomain:${PORT}/${PATH}`) sebagai larik catatan dalam format. JSON Parameter `$PATH` bersifat opsional. Perhatikan bahwa hanya HTTP didukung, tidak HTTPS. Anda dapat memilih untuk menerima log melalui PUT atau POST.
2. TCP— Lambda mengirimkan log ke TCP port dalam format [Newline JSON delimited](#) (). NDJSON

Kami merekomendasikan menggunakan HTTP daripada TCP. Dengan TCP, platform Lambda tidak dapat mengakui kapan mengirimkan log ke lapisan aplikasi. Oleh karena itu, Anda mungkin kehilangan log jika ekstensi Anda mengalami crash. HTTP tidak berbagi batasan ini.

Kami juga menyarankan untuk menyiapkan HTTP listener lokal atau TCP port sebelum berlangganan untuk menerima log. Selama penyetelan, perhatikan hal berikut ini:

- Lambda hanya mengirimkan log ke tujuan yang berada di lingkungan eksekusi.
- Lambda mencoba kembali upaya untuk mengirim log (dengan backoff) jika tidak ada pendengar, atau jika permintaan atau menghasilkan kesalahan POST. PUT Jika pelanggan log mengalami crash, pelanggan terus menerima log setelah Lambda memulai ulang lingkungan eksekusi.
- Lambda mencadangkan port 9001. Tidak ada pembatasan atau rekomendasi nomor port lainnya.

Konfigurasi buffering

Lambda dapat mem-buffer log dan mengirimkannya kepada pelanggan. Anda dapat mengonfigurasi perilaku ini dalam permintaan langganan dengan menentukan bidang opsional berikut. Perhatikan bahwa Lambda menggunakan nilai default untuk setiap bidang yang tidak Anda tentukan.

- `timeoutMs`— Waktu maksimum (dalam milidetik) untuk buffer batch. Default: 1.000. Minimum: 25. Maksimum: 30.000.
- `maxBytes`— Ukuran maksimum (dalam byte) dari log untuk buffer dalam memori. Default: 262.144. Minimum: 262.144. Maksimum: 1.048.576.

- `maxItems`— Jumlah maksimum peristiwa untuk buffer dalam memori. Default: 10.000. Minimum: 1.000. Maksimum: 10.000.

Selama konfigurasi buffering, perhatikan poin-poin berikut:

- Lambda membilas log jika salah satu aliran input tertutup, misalnya, jika waktu pengoperasian macet.
- Setiap pelanggan dapat menentukan konfigurasi buffering yang berbeda dalam permintaan langganan.
- Pertimbangkan ukuran buffer yang Anda butuhkan untuk membaca data. Perkirakan penerimaan muatan sebesar $2 * \text{maxBytes} + \text{metadata}$, dengan `maxBytes` dikonfigurasi dalam permintaan berlangganan. Misalnya, Lambda menambahkan byte metadata berikut ke setiap catatan:

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "function",
  "record": "Hello World"
}
```

- Jika pelanggan tidak dapat memproses log masuk dengan cukup cepat, Lambda mungkin akan menanggalkan log untuk menjaga pemanfaatan memori tetap terikat. Untuk menunjukkan jumlah catatan yang dihapus, Lambda mengirimkan log `platform.logsDropped`. Untuk informasi selengkapnya, lihat [the section called “Lambda: Tidak semua log fungsi saya muncul”](#).

Contoh berlangganan

Contoh berikut menunjukkan permintaan untuk berlangganan ke platform dan log fungsi.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs HTTP/1.1
{ "schemaVersion": "2020-08-15",
  "types": [
    "platform",
    "function"
  ],
  "buffering": {
    "maxItems": 1000,
    "maxBytes": 262144,
    "timeoutMs": 100
  },
}
```

```
"destination": {
  "protocol": "HTTP",
  "URI": "http://sandbox.localdomain:8080/lambda_logs"
}
}
```

Jika permintaan berhasil, pelanggan menerima respons sukses HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Contoh kode untuk Log API

Untuk kode contoh yang menunjukkan cara mengirim log ke tujuan kustom, lihat [Menggunakan AWS Lambda ekstensi untuk mengirim log ke tujuan khusus](#) di Blog AWS Komputasi.

Untuk contoh kode Python dan Go yang menunjukkan cara mengembangkan ekstensi Lambda dasar dan berlangganan LogAPI, lihat [AWS Lambda Ekstensi](#) pada repositori Sampel. AWS GitHub Untuk informasi lebih lanjut tentang membangun ekstensi Lambda, lihat [the section called “Ekstensi API”](#).

API Referensi log

Anda dapat mengambil API titik akhir Log dari variabel `AWS_LAMBDA_RUNTIME_API` lingkungan. Untuk mengirim API permintaan, gunakan awalan `2020-08-15/` sebelum API jalur. Sebagai contoh:

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs
```

API [Spesifikasi Terbuka untuk API versi Log 2020-08-15](#) tersedia di sini: [.zip logs-api-request](#)

Langganan

Untuk berlangganan satu atau beberapa aliran log yang tersedia di lingkungan eksekusi Lambda, ekstensi mengirimkan permintaan BerlanggananAPI.

Jalur – `/logs`

Metode - PUT

Parameter tubuh

`destination` – Lihat [the section called “Protokol tujuan”](#). Wajib: ya. Jenis: string.

`buffering` – Lihat [the section called “Konfigurasi buffering”](#). Wajib: tidak. Jenis: string.

`types` – Array jenis log yang akan diterima. Wajib: ya. Jenis: array string. Nilai valid: "platform", "function", "extension".

`schemaVersion` – Wajib: tidak. Nilai default: "2020-08-15". Atur ke "2021-03-18" untuk ekstensi untuk menerima pesan [platform.runtimeDone](#).

Parameter respons

APISpesifikasi Terbuka untuk respons langganan versi 2020-08-15 tersedia untuk HTTP dan TCP protokol:

- HTTP: [logs-api-http-response.zip](#)
- TCP: [logs-api-tcp-response.zip](#)

Kode respons

- 200 – Permintaan berhasil diselesaikan
- 202 – Permintaan diterima. Respons terhadap permintaan berlangganan selama pengujian lokal.
- 4XX – Permintaan Buruk
- 500 – Kesalahan Layanan

Jika permintaan berhasil, pelanggan menerima respons sukses HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Jika permintaan gagal, pelanggan akan menerima respons kesalahan. Sebagai contoh:

```
HTTP/1.1 400 OK
{
  "errorType": "Logs.ValidationError",
  "errorMessage": "URI port is not provided; types should not be empty"
}
```

Log pesan

Log API memungkinkan ekstensi untuk berlangganan tiga aliran log yang berbeda:

- Fungsi –Log dibuat oleh fungsi Lambda dan menulis ke `stdout` atau `stderr`.
- Ekstensi – Log yang dibuat kode ekstensi.
- Platform –Log yang dibuat platform runtime, yang mencatat peristiwa dan kesalahan yang terkait dengan invokasi dan ekstensi.

Topik

- [Log fungsi](#)
- [Log ekstensi:](#)
- [Log platform](#)

Log fungsi

Fungsi Lambda dan ekstensi internal yang menghasilkan log fungsi dan menuliskannya ke `stdout` atau `stderr`.

Contoh berikut menunjukkan format pesan log fungsi. {"time": "2020-08-20T 12:31:32.123 Z", "type": "function", "record": "ditemui. ERROR Stack trace:\n\nmy-function (line 10)\n" }

Log ekstensi:

Ekstensi dapat menghasilkan log ekstensi. Format log sama seperti untuk log fungsi.

Log platform

Lambda menghasilkan pesan log untuk peristiwa platform seperti `platform.start`, `platform.end`, dan `platform.fault`.

Secara opsional, Anda dapat berlangganan API skema Log versi 2021-03-18, yang menyertakan pesan log `platform.runtimeDone`

Contoh pesan log platform

Contoh berikut menunjukkan log awal platform dan akhir platform. Log ini menunjukkan waktu mulai pemanggilan dan waktu akhir pemanggilan untuk pemanggilan yang ditentukan. `requestId`

```
{
  "time": "2020-08-20T12:31:32.123Z",
```



```

    "type": "platform.start",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
  }
  {
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.end",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
  }

```

Platform. `initRuntimeDone` pesan log menunjukkan status Runtime `init` sub-fase, yang merupakan bagian dari fase [lifecycle Init](#). Runtime `init` kapan berhasil, runtime mengirimkan API permintaan `/next` runtime (untuk tipe `on-demand` dan `provisioned-concurrency` inisialisasi) atau `restore/next` (untuk tipe `snap-start` inisialisasi). Contoh berikut menunjukkan platform yang sukses. `initRuntimeDone` pesan log untuk jenis `snap-start` inisialisasi.

```

{
  "time": "2022-07-17T18:41:57.083Z",
  "type": "platform.initRuntimeDone",
  "record": {
    "initializationType": "snap-start",
    "status": "success"
  }
}

```

Platform. `initReport` pesan log menunjukkan berapa lama `Init` fase berlangsung dan berapa milidetik Anda ditagih selama fase ini. Ketika jenis inisialisasi `provisioned-concurrency`, Lambda mengirimkan pesan ini selama pemanggilan. Saat jenis inisialisasi `snap-start`, Lambda mengirimkan pesan ini setelah memulihkan snapshot. Contoh berikut menunjukkan platform. `initReport` pesan log untuk jenis `snap-start` inisialisasi.

```

{
  "time": "2022-07-17T18:41:57.083Z",
  "type": "platform.initReport",
  "record": {
    "initializationType": "snap-start",
    "metrics": {
      "durationMs": 731.79,
      "billedDurationMs": 732
    }
  }
}

```

Log laporan platform menyertakan metrik tentang pemanggilan yang ditentukan. `requestId` Bidang `initDurationMs` termasuk dalam log hanya jika invokasi termasuk mulai awal. Jika pelacakan AWS X-Ray aktif, log mencakup metadata X-Ray. Contoh berikut menunjukkan log laporan platform untuk invokasi yang mencakup mulai awal.

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "platform.report",
  "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56",
    "metrics": {"durationMs": 101.51,
      "billedDurationMs": 300,
      "memorySizeMB": 512,
      "maxMemoryUsedMB": 33,
      "initDurationMs": 116.67
    }
  }
}
```

Log kesalahan platform menangkap waktu pengoperasian atau kesalahan lingkungan eksekusi. Contoh berikut ini menunjukkan pesan log kesalahan platform.

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "platform.fault",
  "record": "RequestId: d783b35e-a91d-4251-af17-035953428a2c Process exited before
  completing request"
}
```

Note

AWS saat ini menerapkan perubahan pada layanan Lambda. Karena perubahan ini, Anda mungkin melihat perbedaan kecil antara struktur dan konten pesan log sistem dan segmen jejak yang dipancarkan oleh fungsi Lambda yang berbeda di Anda. Akun AWS

Salah satu output log yang terpengaruh oleh perubahan ini adalah `record` bidang log kesalahan platform. Contoh berikut menunjukkan `record` bidang ilustrasi dalam format lama dan baru. Gaya baru log kesalahan berisi pesan yang lebih ringkas

Perubahan ini akan diterapkan selama beberapa minggu mendatang, dan semua fungsi di semua Wilayah AWS kecuali China dan GovCloud wilayah akan bertransisi untuk menggunakan pesan log format baru dan segmen pelacakan.

Example catatan log kesalahan platform (gaya lama)

```
"record": "RequestId: ... \tError: Runtime exited with error: exit status 255\nRuntime.ExitError"
```

Example catatan log kesalahan platform (gaya baru)

```
"record": "RequestId: ... Status: error \tErrorType: Runtime.ExitError"
```

Lambda menghasilkan log ekstensi platform saat ekstensi mendaftar dengan ekstensi. API Contoh berikut ini menunjukkan pesan ekstensi platform.

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "platform.extension",
  "record": { "name": "Foo.bar",
    "state": "Ready",
    "events": ["INVOKE", "SHUTDOWN"]
  }
}
```

Lambda menghasilkan log langganan log platform saat ekstensi berlangganan log. API Contoh berikut menunjukkan pesan langganan Log.

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "platform.logsSubscription",
  "record": { "name": "Foo.bar",
    "state": "Subscribed",
    "types": ["function", "platform"],
  }
}
```

Lambda menghasilkan log yang dihapus log platform ketika ekstensi tidak dapat memproses jumlah log yang diterimanya. Contoh berikut menunjukkan pesan log platform.logsDropped.

```
{
  "time": "2020-08-20T12:31:32.123Z",
  "type": "platform.logsDropped",
```

```

    "record": {"reason": "Consumer seems to have fallen behind as it has not
acknowledged receipt of logs.",
      "droppedRecords": 123,
      "droppedBytes": 12345
    }
  }
}

```

Platform. `restoreStart` pesan log menunjukkan waktu Restore fase dimulai (hanya jenis `snap-start` inisialisasi). Contoh:

```

{
  "time": "2022-07-17T18:43:44.782Z",
  "type": "platform.restoreStart",
  "record": {}
}

```

Platform. `restoreReport` pesan log menunjukkan berapa lama Restore fase berlangsung dan berapa milidetik Anda ditagih selama fase ini (hanya jenis `snap-start` inisialisasi). Contoh:

```

{
  "time": "2022-07-17T18:43:45.936Z",
  "type": "platform.restoreReport",
  "record": {
    "metrics": {
      "durationMs": 70.87,
      "billedDurationMs": 13
    }
  }
}

```

Pesan `runtimeDone` platform

Jika Anda mengatur versi skema ke "2021-03-18" dalam permintaan berlangganan, Lambda mengirimkan pesan `platform.runtimeDone` setelah fungsi invokasi selesai baik berhasil maupun dengan kesalahan. Ekstensi dapat menggunakan pesan ini untuk menghentikan semua kumpulan telemetri untuk fungsi invokasi ini.

[API Spesifikasi Terbuka untuk jenis peristiwa Log dalam skema versi 2021-03-18 tersedia di sini: `schema-2021-03-18.zip`](#)

Lambda menghasilkan pesan `platform.runtimeDone` log saat runtime mengirim permintaan Next atau Error runtime. API `platform.runtimeDoneLog` menginformasikan konsumen tentang

Log API bahwa pemanggilan fungsi selesai. Ekstensi dapat menggunakan informasi ini untuk memutuskan kapan harus mengirim semua telemetri yang dikumpulkan selama invokasi tersebut.

Contoh

Lambda mengirimkan `platform.runtimeDone` pesan setelah runtime mengirimkan NEXT permintaan saat pemanggilan fungsi selesai. Contoh berikut menunjukkan pesan untuk masing-masing nilai status: sukses, kegagalan, dan waktu habis.

Example Contoh pesan sukses

```
{
  "time": "2021-02-04T20:00:05.123Z",
  "type": "platform.runtimeDone",
  "record": {
    "requestId": "6f7f0961f83442118a7af6fe80b88",
    "status": "success"
  }
}
```

Example Contoh pesan kegagalan

```
{
  "time": "2021-02-04T20:00:05.123Z",
  "type": "platform.runtimeDone",
  "record": {
    "requestId": "6f7f0961f83442118a7af6fe80b88",
    "status": "failure"
  }
}
```

Example Contoh pesan waktu habis

```
{
  "time": "2021-02-04T20:00:05.123Z",
  "type": "platform.runtimeDone",
  "record": {
    "requestId": "6f7f0961f83442118a7af6fe80b88",
    "status": "timeout"
  }
}
```

Example Contoh platform. restoreRuntimeDone pesan (hanya jenis **snap-start** inisialisasi)

Platform. restoreRuntimeDone pesan log menunjukkan apakah Restore fase berhasil atau tidak. Lambda mengirimkan pesan ini saat runtime mengirimkan permintaan runtime. `restore/next` API. Ada tiga kemungkinan status: sukses, gagal, dan batas waktu. Contoh berikut menunjukkan platform yang sukses. `restoreRuntimeDone` pesan log.

```
{
  "time": "2022-07-17T18:43:45.936Z",
  "type": "platform.restoreRuntimeDone",
  "record": {
    "status": "success"
  }
}
```

Memecahkan masalah di Lambda

Topik berikut memberikan saran pemecahan masalah untuk kesalahan dan masalah yang mungkin Anda temui saat menggunakan LambdaAPI, konsol, atau alat. Jika Anda menemukan masalah yang tidak tercantum di sini, Anda dapat menggunakan tombol Umpan Balik di halaman ini untuk melaporkannya.

Untuk saran pemecahan masalah selengkapnya dan jawaban atas pertanyaan dukungan umum, kunjungi [Pusat Pengetahuan AWS](#).

Untuk informasi selengkapnya tentang debugging dan pemecahan masalah aplikasi Lambda, [lihat Debugging di Tanah Tanpa Server](#).

Topik

- [Menyelesaikan masalah deployment di Lambda](#)
- [Menyelesaikan masalah invokasi di Lambda](#)
- [Menyelesaikan masalah eksekusi di Lambda](#)
- [Menyelesaikan masalah jaringan di Lambda](#)

Menyelesaikan masalah deployment di Lambda

Saat Anda memperbarui fungsi Anda, Lambda menerapkan perubahan dengan meluncurkan instans baru dari fungsi dengan kode atau pengaturan yang diperbarui. Kesalahan deployment menghambat penggunaan versi baru dan dapat disebabkan oleh masalah dengan paket deployment, kode, izin, atau alat Anda.

Saat Anda menerapkan pembaruan ke fungsi Anda secara langsung dengan API Lambda atau dengan klien seperti AWS CLI, Anda dapat melihat kesalahan dari Lambda langsung di output. Jika Anda menggunakan layanan seperti AWS CloudFormation, AWS CodeDeploy, atau AWS CodePipeline, cari respons dari Lambda di log atau aliran peristiwa untuk layanan tersebut.

Topik berikut memberikan saran pemecahan masalah untuk kesalahan dan masalah yang mungkin Anda temui saat menggunakan LambdaAPI, konsol, atau alat. Jika Anda menemukan masalah yang tidak tercantum di sini, Anda dapat menggunakan tombol Umpan Balik di halaman ini untuk melaporkannya.

Untuk saran pemecahan masalah selengkapnya dan jawaban atas pertanyaan dukungan umum, kunjungi [Pusat Pengetahuan AWS](#).

Untuk informasi selengkapnya tentang debugging dan pemecahan masalah aplikasi Lambda, [lihat](#) Debugging di Tanah Tanpa Server.

Topik

- [Umum: Izin ditolak/Tidak dapat memuat file tersebut](#)
- [Umum: Terjadi kesalahan saat memanggil UpdateFunctionCode](#)
- [Amazon S3: Kode Kesalahan. PermanentRedirect](#)
- [Umum: Tidak dapat menemukan, tidak dapat memuat, tidak dapat mengimpor, kelas tidak ditemukan, tidak ada file atau direktori tersebut](#)
- [Umum: Metode handler tidak didefinisikan](#)
- [Lambda: Konversi lapisan gagal](#)
- [Lambda: atau InvalidParameterValueException RequestEntityTooLargeException](#)
- [Lambda: InvalidParameterValueException](#)
- [Lambda: Konkurensi dan kuota memori](#)

Umum: Izin ditolak/Tidak dapat memuat file tersebut

Kesalahan: EACCES: izin ditolak, buka '/var/task/index.js'

Kesalahan: tidak dapat memuat file tersebut -- fungsi

Kesalahan: [Errno 13] Izin ditolak: '/var/task/function.py'

Runtime Lambda membutuhkan izin untuk membaca file dalam paket deployment Anda. Dalam notasi oktal izin Linux, Lambda membutuhkan 644 izin untuk file yang tidak dapat dieksekusi (rw-r - r--) dan 755 izin () untuk direktori dan file yang dapat dieksekusi. rwxr-xr-x

Di Linux dan macOS, gunakan `chmod` perintah untuk mengubah izin file pada file dan direktori dalam paket penyebaran Anda. Misalnya, untuk memberikan file yang dapat dieksekusi izin yang benar, jalankan perintah berikut.

```
chmod 755 <filepath>
```


Untuk mengubah izin file di Windows, lihat [Mengatur, Melihat, Mengubah, atau Menghapus Izin pada Objek](#) dalam dokumentasi Microsoft Windows.

Umum: Terjadi kesalahan saat memanggil UpdateFunctionCode

Kesalahan: Terjadi kesalahan (RequestEntityTooLargeException) saat memanggil UpdateFunctionCode operasi

Saat Anda mengunggah paket penyebaran atau arsip lapisan langsung ke Lambda, ukuran ZIP file dibatasi hingga 50 MB. Untuk mengunggah file yang lebih besar, simpan file di Amazon S3 dan gunakan parameter S3Bucket dan S3Key.

Note

Ketika Anda mengunggah file langsung dengan AWS CLI, AWS SDK, atau sebaliknya, ZIP file biner dikonversi ke base64, yang meningkatkan ukurannya sekitar 30%. Untuk memungkinkan hal ini, serta ukuran parameter lain dalam permintaan, batas ukuran permintaan aktual yang digunakan Lambda menjadi lebih besar. Oleh karena itu, batas sebesar 50 MB adalah perkiraan.

Amazon S3: Kode Kesalahan. PermanentRedirect

Kesalahan: Terjadi kesalahan saat GetObject. Kode Kesalahan S3: PermanentRedirect. Pesan Kesalahan S3: Bucket berada di wilayah: us-east-2. Harap gunakan wilayah ini untuk mencoba kembali permintaan ini

Saat Anda mengunggah paket deployment fungsi dari bucket Amazon S3, bucket harus berada di Wilayah yang sama dengan fungsi tersebut. Masalah ini dapat terjadi saat Anda menentukan objek Amazon S3 dalam panggilan ke [UpdateFunctionCode](#), atau menggunakan paket dan perintah penerapan di or. AWS CLI AWS SAM CLI Buat bucket artefak deployment untuk setiap Wilayah tempat Anda mengembangkan aplikasi.

Umum: Tidak dapat menemukan, tidak dapat memuat, tidak dapat mengimpor, kelas tidak ditemukan, tidak ada file atau direktori tersebut

Kesalahan: Tidak dapat menemukan modul 'function'

Kesalahan: tidak dapat memuat file tersebut -- fungsi

Kesalahan: Tidak dapat mengimpor modul 'function'

Kesalahan: Kelas tidak ditemukan: function.Handler

Kesalahan: fork/exec /var/task/function: tidak ada file atau direktori tersebut

Kesalahan: Tidak dapat memuat jenis 'Function.Handler' dari susunan 'Function'.

Nama file atau kelas dalam konfigurasi handler fungsi tidak cocok dengan kode. Lihat bagian berikut untuk informasi selengkapnya.

Umum: Metode handler tidak didefinisikan

Kesalahan: index.handler tidak ditentukan atau tidak terekspor

Kesalahan: Handler 'handler' hilang di modul 'function'

Kesalahan: metode penanganan yang tidak ditentukan untuk # <:0x000055b76cceb98>
LambdaHandler

Kesalahan: Tidak ada metode publik yang dinamai handleRequest dengan tanda tangan metode yang sesuai yang ditemukan di kelas Function.handler

Kesalahan: Tidak dapat menemukan metode " dalam tipe handleRequest 'Function.Handler' dari perakitan 'Fungsi'

Nama metode handler dalam konfigurasi handler fungsi tidak cocok dengan kode. Setiap runtime menentukan konvensi penamaan untuk handler, seperti *filename.methodname*. Handler adalah metode dalam kode fungsi Anda yang dijalankan oleh runtime saat fungsi Anda dipanggil.

Untuk beberapa bahasa, Lambda menyediakan pustaka dengan antarmuka yang mengharuskan metode handler memiliki nama tertentu. Untuk perincian tentang penamaan handler untuk setiap bahasa, lihat topik berikut.

- [Membangun fungsi Lambda dengan Node.js](#)
- [Membangun fungsi Lambda dengan Python](#)
- [Membangun fungsi Lambda dengan Ruby](#)
- [Membangun fungsi Lambda dengan Java](#)
- [Membangun fungsi Lambda dengan Go](#)
- [Membangun fungsi Lambda dengan C#](#)

- [Membangun fungsi Lambda dengan PowerShell](#)

Lambda: Konversi lapisan gagal

Kesalahan: Konversi lapisan Lambda gagal. Untuk saran tentang menyelesaikan masalah ini, lihat halaman Memecahkan masalah penerapan di Lambda di Panduan Pengguna Lambda.

Ketika Anda mengkonfigurasi fungsi Lambda dengan lapisan, Lambda menggabungkan layer dengan kode fungsi Anda. Jika proses ini gagal diselesaikan, Lambda mengembalikan kesalahan ini. Jika Anda mengalami kesalahan ini, lakukan langkah-langkah berikut:

- Hapus file yang tidak digunakan dari lapisan Anda
- Hapus tautan simbolis apa pun di lapisan Anda
- Ganti nama file yang memiliki nama yang sama dengan direktori di salah satu lapisan fungsi Anda

Lambda: atau InvalidParameterValueException RequestEntityTooLargeException

Kesalahan: InvalidParameterValueException: Lambda tidak dapat mengonfigurasi variabel lingkungan Anda karena variabel lingkungan yang Anda berikan melebihi batas 4KB. String diukur: {"A1": " uSFe Y5 cyPiPn 7ATnx5bsm...

Kesalahan: RequestEntityTooLargeException: Permintaan harus lebih kecil dari 5120 byte untuk operasi UpdateFunctionConfiguration

Ukuran maksimum objek variabel yang disimpan dalam konfigurasi fungsi tidak boleh melebihi 4096 byte. Ini termasuk nama kunci, nilai, tanda kutip, koma, dan tanda kurung. Ukuran total badan HTTP permintaan juga terbatas.

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
  "Runtime": "nodejs20.x",
  "Role": "arn:aws:iam::123456789012:role/lambda-role",
  "Environment": {
    "Variables": {
      "BUCKET": "amzn-s3-demo-bucket",
      "KEY": "file.txt"
    }
  }
}
```

```
    },  
    },  
    ...  
}
```

Dalam contoh ini, objek adalah 39 karakter dan menggunakan 39 byte ketika disimpan (tanpa spasi) sebagai string `{"BUCKET": "amzn-s3-demo-bucket", "KEY": "file.txt"}`. ASCII karakter standar dalam nilai variabel lingkungan masing-masing menggunakan satu byte. Karakter Extended ASCII dan Unicode dapat menggunakan antara 2 byte dan 4 byte per karakter.

Lambda: InvalidParameterValueException

Kesalahan: `InvalidParameterValueException`: Lambda tidak dapat mengonfigurasi variabel lingkungan Anda karena variabel lingkungan yang Anda berikan berisi kunci cadangan yang saat ini tidak didukung untuk modifikasi.

Lambda mencadangkan beberapa kunci variabel lingkungan untuk penggunaan internal. Misalnya, `AWS_REGION` digunakan oleh runtime untuk menentukan Wilayah saat ini dan tidak dapat dibatalkan. Variabel lainnya, seperti `PATH`, digunakan oleh runtime, tetapi dapat diperluas dalam konfigurasi fungsi Anda. Untuk daftar lengkap, lihat [Variabel lingkungan runtime yang ditetapkan](#).

Lambda: Konkurensi dan kuota memori

Kesalahan: Ditetapkan `ConcurrentExecutions` untuk fungsi mengurangi akun `UnreservedConcurrentExecution` di bawah nilai minimumnya

Kesalahan: Nilai `MemorySize` " gagal memenuhi kendala: Anggota harus memiliki nilai kurang dari atau sama dengan 3008

Kesalahan ini terjadi ketika Anda melebihi [kuota konkurensi atau memori untuk akun](#) Anda. AWS Akun baru telah mengurangi kuota konkurensi dan memori. Untuk mengatasi kesalahan yang terkait dengan konkurensi, Anda dapat [meminta peningkatan kuota](#). Anda tidak dapat meminta peningkatan kuota memori.

- **Konkurensi:** Anda mungkin mendapatkan kesalahan jika mencoba membuat fungsi menggunakan konkurensi cadangan atau ketentuan, atau jika permintaan konkurensi per fungsi ([PutFunctionConcurrency](#)) melebihi kuota konkurensi akun Anda.
- **Memori:** Kesalahan terjadi jika jumlah memori yang dialokasikan ke fungsi melebihi kuota memori akun Anda.

Menyelesaikan masalah invokasi di Lambda

Saat Anda memanggil fungsi Lambda, Lambda memvalidasi permintaan dan memeriksa kapasitas penskalaan sebelum mengirim kejadian ke fungsi Anda atau, untuk invokasi asinkron, ke antrean kejadian. Kesalahan invokasi dapat disebabkan oleh masalah parameter permintaan, struktur kejadian, pengaturan fungsi, izin pengguna, izin sumber daya, atau batas.

Jika Anda memanggil fungsi secara langsung, Anda melihat kesalahan invokasi apa pun dalam respons dari Lambda. Jika Anda memanggil fungsi secara asinkron dengan pemetaan sumber kejadian atau melalui layanan lain, Anda mungkin menemukan kesalahan di log, antrean surat gagal, atau tujuan kejadian-gagal. Opsi penanganan kesalahan dan perilaku percobaan ulang berbeda-beda tergantung pada cara Anda memanggil fungsi dan jenis kesalahan.

Untuk daftar tipe kesalahan yang dapat dikembalikan oleh operasi Invoke, lihat [Panggil](#).

IAM: lambda: InvokeFunction tidak diizinkan

Kesalahan: Pengguna: arn:aws:iam: :123456789012: pengguna/pengembang tidak berwenang untuk melakukan: lambda: on resource: my-function InvokeFunction

Pengguna Anda, atau peran yang Anda asumsikan, harus memiliki izin untuk menjalankan fungsi. Persyaratan ini juga berlaku untuk fungsi Lambda dan sumber daya komputasi lainnya yang memanggil fungsi. Tambahkan kebijakan AWS terkelola AWSLambdaRole ke pengguna Anda, atau tambahkan kebijakan khusus yang memungkinkan `lambda: InvokeFunction` tindakan pada fungsi target.

Note

Nama IAM action (`lambda: InvokeFunction`) mengacu pada operasi Invoke LambdaAPI.

Untuk informasi selengkapnya, lihat [Mengelola izin di AWS Lambda](#).

Lambda: Tidak dapat menemukan bootstrap yang valid (Runtime.InvalidEntryPoint)

Kesalahan: Tidak dapat menemukan bootstrap yang valid: [/var/task/bootstrap /opt/bootstrap]

Kesalahan ini biasanya terjadi ketika root paket penyebaran Anda tidak berisi file yang dapat dieksekusi bernama `bootstrap`. Misalnya, jika Anda menerapkan `provided.al2023` fungsi dengan `file.zip`, `bootstrap` file harus berada di root `file.zip`, bukan di direktori.

Lambda: Operasi tidak dapat dilakukan ResourceConflictException

Kesalahan `ResourceConflictException`:: Operasi tidak dapat dilakukan saat ini. Fungsi saat sedang dalam status: Tertunda

Saat Anda menghubungkan fungsi ke cloud pribadi virtual (VPC) pada saat pembuatan, fungsi memasuki `Pending` status sementara Lambda membuat antarmuka jaringan elastis. Selama waktu ini, Anda tidak dapat memanggil atau memodifikasi fungsi Anda. Jika Anda menghubungkan fungsi Anda ke VPC setelah pembuatan, Anda dapat memanggilnya saat pembaruan tertunda, tetapi Anda tidak dapat mengubah kode atau konfigurasinya.

Untuk informasi selengkapnya, lihat [Status fungsi Lambda](#).

Lambda: Fungsi tertahan dalam Tertunda

Kesalahan: Fungsi tertahan dalam status `Pending` selama beberapa menit.

Jika fungsi macet dalam `Pending` status selama lebih dari enam menit, panggil salah satu API operasi berikut untuk membuka blokir:

- [UpdateFunctionCode](#)
- [UpdateFunctionConfiguration](#)
- [PublishVersion](#)

Lambda membatalkan operasi yang tertunda dan menempatkan fungsi ke keadaan `Failed`. Anda kemudian dapat mencoba pembaruan lain.

Lambda: Salah satu fungsi menggunakan semua konkurensi

Masalah: Satu fungsi sedang menggunakan semua konkurensi yang tersedia, yang menyebabkan fungsi lain dibatasi.

Untuk membagi konkurensi AWS akun Anda yang tersedia di AWS Wilayah menjadi kumpulan, gunakan [konkurensi cadangan](#). Konkurensi cadangan memastikan fungsi dapat selalu menskalakan ke konkurensi yang ditetapkan, dan fungsi tidak menskalakan melebihi konkurensi yang ditetapkan.

Umum: Tidak dapat memanggil fungsi dengan akun atau layanan lain

Masalah: Anda dapat memanggil fungsi secara langsung, tetapi tidak dijalankan ketika layanan atau akun lain memanggilmnya.

Anda memberikan izin kepada akun dan [layanan lain](#) untuk memanggil fungsi dalam [kebijakan berbasis sumber daya](#) milik fungsi. Jika pemanggil ada di akun lain, pengguna tersebut juga harus memiliki [izin untuk memanggil fungsi](#).

Umum: Invokasi fungsi adalah perulangan

Masalah: Fungsi dipanggil secara berulang terus-menerus.

Ini biasanya terjadi ketika fungsi Anda mengelola sumber daya dalam AWS layanan yang sama yang memicunya. Misalnya, ini memungkinkan untuk membuat fungsi yang menyimpan objek dalam bucket Amazon Simple Storage Service (Amazon S3) yang dikonfigurasi dengan [notifikasi yang kembali memanggil fungsi](#). Untuk menghentikan fungsi agar tidak berjalan, kurangi [konkurensi](#) yang tersedia menjadi nol, yang membatasi semua pemanggilan future. Selanjutnya, identifikasi jalur kode atau kesalahan konfigurasi yang menyebabkan invokasi berulang. Lambda secara otomatis mendeteksi dan menghentikan loop rekursif untuk beberapa layanan dan. AWS SDKs Untuk informasi selengkapnya, lihat [the section called “Deteksi loop rekursif”](#).

Lambda: Perutean alias dengan konkurensi terprovisi

Masalah: Konkurensi terprovisi melimpahkan invokasi selama perutean alias.


Lambda menggunakan model probabilistik sederhana untuk mendistribusikan lalu lintas di antara dua versi fungsi. Pada tingkat lalu lintas rendah, Anda mungkin melihat varians tinggi di antara persentase lalu lintas yang dikonfigurasi dan aktual di setiap versi. Jika fungsi Anda menggunakan konkurensi terprovisi, Anda dapat menghindari [invokasi limpahan](#) dengan mengonfigurasi jumlah yang lebih tinggi dari instans konkurensi terprovisi selama perutean alias aktif.

Lambda: Mulai awal dengan konkurensi terprovisi

Masalah: Anda melihat mulai awal setelah mengaktifkan konkurensi terprovisi.

Ketika jumlah eksekusi bersamaan pada fungsi kurang dari atau sama dengan [tingkat konkurensi terprovisi yang dikonfigurasi](#), mulai awal seharusnya tidak ada. Untuk membantu Anda mengonfirmasi jika konkurensi terprovisi beroperasi secara normal, lakukan hal berikut:

- [Periksa apakah concurrency terprovisi diaktifkan](#) pada versi fungsi atau alias.

 Note

Konkurensi yang disediakan tidak dapat dikonfigurasi pada [versi fungsi yang tidak dipublikasikan \(\\$\) . LATEST](#)

- Pastikan pemicu Anda memanggil versi fungsi atau alias yang benar. Misalnya, jika Anda menggunakan Amazon API Gateway, periksa apakah API Gateway memanggil versi fungsi atau alias dengan konkurensi yang disediakan, bukan \$. LATEST [Untuk mengonfirmasi bahwa konkurensi yang disediakan sedang digunakan, Anda dapat memeriksa metrik AmazonProvisionedConcurrencyInvocations . CloudWatch](#) Nilai bukan nol menunjukkan fungsi ini memproses invokasi pada lingkungan eksekusi yang diinisialisasi.
- [Tentukan apakah konkurensi fungsi Anda melebihi tingkat konkurensi yang disediakan yang dikonfigurasi dengan memeriksa metrik. ProvisionedConcurrencySpilloverInvocations CloudWatch](#) Nilai bukan nol menunjukkan semua konkurensi terprovisi sedang digunakan dan beberapa invokasi terjadi dengan mulai awal.
- Periksa [frekuensi invokasi](#) (permintaan per detik). Fungsi dengan konkurensi terprovisi memiliki tingkat maksimum 10 permintaan per detik per konkurensi terprovisi. Misalnya, fungsi yang dikonfigurasi dengan 100 konkurensi terprovisi dapat menangani 1.000 permintaan per detik. Jika tingkat invokasi melebihi 1.000 permintaan per detik, beberapa mulai awal dapat terjadi.

Lambda: Mulai awal dengan versi baru

Masalah: Anda melihat mulai awal saat men-deploy versi baru dari fungsi Anda.

Ketika Anda memperbarui alias fungsi, Lambda secara otomatis menggeser konkurensi terprovisi ke versi baru berdasarkan bobot yang dikonfigurasi di alias.

Kesalahan:KMSDisabledException: Lambda tidak dapat mendekripsi variabel lingkungan karena KMS kunci yang digunakan dinonaktifkan. Silakan periksa pengaturan KMS tombol fungsi.

Kesalahan ini dapat terjadi jika kunci AWS Key Management Service (AWS KMS) Anda dinonaktifkan, atau jika hibah yang memungkinkan Lambda menggunakan kunci dicabut. Jika pemberian izin tidak ada, konfigurasi fungsi agar menggunakan kunci yang berbeda. Selanjutnya, atur ulang kunci kustom untuk membuat ulang pemberian izin.

EFS: Fungsi tidak dapat me-mount sistem EFS file

Kesalahan:EFSMountFailureException: Fungsi tidak dapat me-mount sistem EFS file dengan titik akses `arn:aws:elasticfilesystem:us-east-2:123456789012:access-point/fsap-015cxmplb72b405fd`.

Permintaan pemasangan untuk [sistem file](#) fungsi ditolak. Periksa izin fungsi, dan konfirmasi bahwa sistem file dan titik aksesnya sudah ada dan siap digunakan.

EFS: Fungsi tidak dapat terhubung ke sistem EFS file

Kesalahan:EFSMountConnectivityException: Fungsi tidak dapat terhubung ke sistem EFS file Amazon dengan titik akses `arn:aws:elasticfilesystem:us-east-2:123456789012:access-point/fsap-015cxmplb72b405fd`. Periksa konfigurasi jaringan Anda dan coba kembali.

Fungsi tidak dapat membuat koneksi ke [sistem file](#) fungsi dengan NFS protokol (TCPport 2049). Periksa [grup keamanan dan konfigurasi perutean](#) untuk VPC subnet.

Jika Anda mendapatkan kesalahan ini setelah memperbarui pengaturan VPC konfigurasi fungsi Anda, coba lepaskan dan atur ulang sistem file.

EFS: Fungsi tidak dapat me-mount sistem EFS file karena batas waktu

Kesalahan:EFSMountTimeoutException: Fungsi tidak dapat me-mount sistem EFS file dengan titik akses `{arn:aws:elasticfilesystem:us-east-2:123456789012:access-point/fsap-015cxmplb72b405fd}` karena waktu pemasangan habis.

Fungsi dapat terhubung ke [sistem file](#) fungsi, tetapi waktu operasi pemasangan habis. Coba lagi setelah beberapa saat dan pertimbangkan untuk membatasi [konkurensi](#) fungsi guna mengurangi beban sistem file.

Lambda: Lambda mendeteksi proses IO yang memakan waktu terlalu lama

EFSIOException: Instance fungsi ini dihentikan karena Lambda mendeteksi proses IO yang memakan waktu terlalu lama.

Waktu invokasi sebelumnya habis dan Lambda tidak dapat menghentikan handler fungsi. Masalah ini dapat terjadi ketika sistem file yang dilampirkan kehabisan kredit lonjakan dan throughput awal tidak cukup. Untuk meningkatkan throughput, Anda dapat meningkatkan ukuran sistem file atau menggunakan throughput terprovisi.

Menyelesaikan masalah eksekusi di Lambda

Ketika runtime Lambda menjalankan kode fungsi Anda, kejadian mungkin diproses pada instans fungsi yang sedang memproses kejadian selama beberapa saat, atau mungkin memerlukan instans baru untuk diinisialisasi. Kesalahan dapat terjadi selama inisialisasi fungsi, ketika kode handler Anda memproses kejadian, atau ketika fungsi Anda mengembalikan (atau gagal mengembalikan) respons.

Kesalahan eksekusi fungsi dapat disebabkan oleh masalah dengan kode, konfigurasi fungsi, sumber daya hilir, atau izin Anda. Jika Anda memanggil fungsi secara langsung, Anda melihat kesalahan fungsi dalam respons dari Lambda. Jika Anda memanggil fungsi Anda secara asinkron, dengan pemetaan sumber kejadian, atau melalui layanan lain, Anda mungkin menemukan kesalahan di log, antrean surat gagal, atau tujuan saat terjadi kegagalan. Opsi penanganan kesalahan dan perilaku percobaan ulang berbeda-beda tergantung pada cara Anda memanggil fungsi dan jenis kesalahan.

Saat kode fungsi atau runtime Lambda Anda memunculkan kesalahan, kode status di respons dari Lambda adalah 200 OK. Adanya kesalahan dalam respons ditunjukkan dengan header bernama `X-Amz-Function-Error`. Kode status seri 400 dan 500 dicadangkan untuk [kesalahan invokasi](#).

Lambda: Eksekusi memerlukan waktu yang lama

Masalah: Eksekusi fungsi membutuhkan waktu terlalu lama.

Jika kode Anda membutuhkan waktu lebih lama untuk dijalankan di Lambda daripada di mesin lokal Anda, kode mungkin dibatasi oleh memori atau daya pemrosesan yang tersedia untuk fungsi. [Konfigurasikan fungsi dengan memori tambahan](#) untuk menambah memori dan CPU.

Lambda: Log atau jejak tidak muncul

Masalah: Log tidak muncul di CloudWatch Log.

Masalah: Jejak tidak muncul di AWS X-Ray.

Fungsi Anda memerlukan izin untuk memanggil CloudWatch Log dan X-Ray. Perbarui [peran eksekusi](#) untuk memberikan izin. Tambahkan kebijakan terkelola berikut untuk mengaktifkan log dan pelacakan.

- `AWSLambdaBasicExecutionRole`
- `AWSXRayDaemonWriteAccess`

Saat Anda menambahkan izin ke fungsi Anda, lakukan pembaruan sepele ke kode atau konfigurasinya juga. Ini memaksa instance menjalankan fungsi Anda, yang memiliki kredensialnya yang sudah ketinggalan zaman, untuk berhenti dan diganti.

Note

Mungkin diperlukan 5 hingga 10 menit agar log muncul setelah pemanggilan fungsi.

Lambda: Tidak semua log fungsi saya muncul

Masalah: Log fungsi tidak ada di CloudWatch Log, meskipun izin saya benar

Jika Anda Akun AWS mencapai [batas kuota CloudWatch Log](#), fungsi CloudWatch throttles logging berfungsi. Ketika ini terjadi, beberapa log yang dihasilkan oleh fungsi Anda mungkin tidak muncul di CloudWatch Log.

Jika fungsi Anda mengeluarkan log pada tingkat yang terlalu tinggi bagi Lambda untuk memprosesnya, ini juga dapat menyebabkan keluaran log tidak muncul di Log. CloudWatch Ketika Lambda tidak dapat mengirim log CloudWatch pada tingkat yang dihasilkan oleh fungsi Anda, Lambda akan menjatuhkan log untuk mencegah eksekusi fungsi Anda melambat. Berharap untuk secara konsisten mengamati log yang dijatuhkan ketika throughput log Anda melebihi 2 MB/s untuk satu aliran log.

Jika fungsi Anda dikonfigurasi untuk menggunakan [log JSON yang diformat](#), Lambda mencoba mengirim [logsDropped](#) peristiwa CloudWatch ke Log saat menjatuhkan log. Namun, saat CloudWatch membatasi logging fungsi Anda, peristiwa ini mungkin tidak mencapai CloudWatch Log, sehingga Anda tidak akan selalu melihat catatan saat Lambda menjatuhkan log.

Untuk memeriksa apakah Anda Akun AWS telah mencapai batas kuota CloudWatch Log, lakukan hal berikut:

1. Buka [Konsol Service Quotas](#).
2. Di panel navigasi, pilih Layanan AWS .
3. Dari daftar AWS layanan, cari Amazon CloudWatch Logs.
4. Dalam daftar kuota Layanan, pilih `CreateLogGroup throttle limit in transactions per second`, `CreateLogStream throttle limit in transactions per second` dan `PutLogEvents throttle limit in transactions per second` kuota untuk melihat penggunaan Anda.

Anda juga dapat mengatur CloudWatch alarm untuk mengingatkan Anda ketika penggunaan akun Anda melebihi batas yang Anda tentukan untuk kuota ini. Lihat [Membuat CloudWatch alarm berdasarkan ambang batas statis](#) untuk mempelajari lebih lanjut.

Jika batas kuota default untuk CloudWatch Log tidak cukup untuk kasus penggunaan, Anda dapat [meminta peningkatan kuota](#).

Lambda: Fungsi kembali sebelum eksekusi selesai

Masalah: (Node.js) Fungsi kembali sebelum kode menyelesaikan eksekusi

Banyak perpustakaan, termasuk, beroperasi secara AWS SDK asinkron. Ketika Anda melakukan panggilan jaringan atau melakukan operasi lain yang perlu menunggu respons, pustaka mengembalikan objek yang disebut janji, yang melacak kemajuan operasi di latar belakang.

Untuk menunggu janji selesai menjadi respons, gunakan kata kunci `await`. Ini menghalangi kode handler Anda beroperasi hingga janji diselesaikan menjadi objek yang berisi respons. Jika Anda tidak perlu menggunakan data dari respons dalam kode, Anda dapat mengembalikan janji secara langsung ke runtime.

Beberapa pustaka tidak mengembalikan janji, tetapi dapat dirangkum dalam kode yang mengembalikan janji. Untuk informasi selengkapnya, lihat [Tentukan penanganan fungsi Lambda di Node.js](#).

AWS SDK: Versi dan pembaruan

Masalah: Yang AWS SDK disertakan pada runtime bukanlah versi terbaru

Masalah: Yang AWS SDK disertakan pada pembaruan runtime secara otomatis

Runtime untuk bahasa scripting termasuk AWS SDK dan diperbarui secara berkala ke versi terbaru. Versi terkini untuk setiap runtime tercantum di [halaman runtime](#). Untuk menggunakan versi yang lebih baru AWS SDK, atau untuk mengunci fungsi Anda ke versi tertentu, Anda dapat menggabungkan pustaka dengan kode fungsi Anda, atau [membuat lapisan Lambda](#). Untuk perincian tentang pembuatan paket deployment dengan dependensi, lihat topik berikut:

Node.js

[Deploy fungsi Lambda Node.js dengan arsip file .zip](#)

Python

[Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#)

Ruby

[Deploy fungsi Lambda Ruby dengan arsip file .zip](#)

Java

[Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file](#)

Go

[Deploy fungsi Go Lambda dengan arsip file .zip](#)

C#

[Bangun dan terapkan fungsi C# Lambda dengan arsip file.zip](#)

PowerShell

[Menyebarkan fungsi PowerShell Lambda dengan arsip file.zip](#)

Python: Pustaka memuat dengan tidak benar

Masalah: (Python) Beberapa pustaka tidak memuat dengan benar dari paket deployment

Pustaka dengan modul ekstensi yang tertulis dalam C atau C++ harus disusun dalam lingkungan dengan arsitektur prosesor yang sama dengan Lambda (Amazon Linux). Untuk informasi selengkapnya, lihat [Bekerja dengan arsip file.zip untuk fungsi Python Lambda](#).

Java: Fungsi Anda membutuhkan waktu lebih lama untuk memproses peristiwa setelah memperbarui ke Java 17 dari Java 11

Masalah: (Java) Fungsi Anda membutuhkan waktu lebih lama untuk memproses peristiwa setelah memperbarui ke Java 17 dari Java 11

Tune compiler Anda menggunakan `JAVA_TOOL_OPTIONS` parameter. Runtime Lambda untuk Java 17 dan versi Java yang lebih baru mengubah opsi kompiler default. Perubahan ini meningkatkan waktu mulai dingin untuk fungsi berumur pendek, tetapi perilaku sebelumnya lebih cocok untuk fungsi komputasi yang intensif dan berjalan lebih lama. Setel `JAVA_TOOL_OPTIONS -XX:-TieredCompilation` untuk kembali ke perilaku Java 11. Untuk informasi tentang parameter

JAVA_TOOL_OPTIONS, lihat [the section called “Memahami variabel JAVA_TOOL_OPTIONS lingkungan”](#).

Menyelesaikan masalah jaringan di Lambda

Secara default, Lambda menjalankan fungsi Anda di virtual private cloud (VPC) dengan konektivitas ke layanan AWS dan internet. Untuk mengakses sumber daya jaringan lokal, Anda dapat [mengonfigurasi fungsi Anda untuk terhubung ke VPC di akun Anda](#). Saat menggunakan fitur ini, Anda mengelola akses internet fungsi dan konektivitas jaringan dengan sumber daya Amazon Virtual Private Cloud (Amazon VPC).

Kesalahan konektivitas jaringan dapat diakibatkan oleh masalah dengan konfigurasi perutean VPC Anda, aturan grup keamanan, izin peran AWS Identity and Access Management (IAM), atau terjemahan alamat jaringan (NAT), atau dari ketersediaan sumber daya seperti alamat IP atau antarmuka jaringan. Bergantung pada masalahnya, Anda mungkin melihat kesalahan atau batas waktu tertentu jika permintaan tidak dapat mencapai tujuannya.

VPC: Fungsi kehilangan akses internet atau waktu habis

Masalah: Fungsi Lambda Anda kehilangan akses internet setelah tersambung ke VPC.

Kesalahan: Kesalahan: connect ETIMEDOUT 176.32.98.189:443

Kesalahan: Kesalahan: Batas waktu tugas berakhir setelah 10.00 detik

Kesalahan: ReadTimeoutError: Baca waktunya habis. (baca batas waktu = 15)

Saat Anda menghubungkan fungsi ke VPC, semua permintaan keluar melalui VPC. Untuk terhubung ke internet, konfigurasi VPC Anda agar mengirim lalu lintas keluar dari subnet fungsi ke gateway NAT di subnet publik. Untuk informasi lebih lanjut dan contoh konfigurasi VPC, lihat [the section called “Akses internet untuk VPC fungsi”](#).

Jika beberapa koneksi TCP Anda habis waktu, ini mungkin karena fragmentasi paket. Fungsi Lambda tidak dapat menangani permintaan TCP terfragmentasi yang masuk, karena Lambda tidak mendukung fragmentasi IP untuk TCP atau ICMP.

VPC: Fungsi membutuhkan akses ke AWS layanan tanpa menggunakan internet

Masalah: Fungsi Lambda Anda membutuhkan akses ke AWS layanan tanpa menggunakan internet.

Untuk menghubungkan fungsi ke AWS layanan dari subnet pribadi tanpa akses internet, gunakan titik akhir VPC.

VPC: Batas antarmuka jaringan elastis tercapai

Kesalahan: `ENILimitReachedException`: Batas antarmuka elastic network tercapai untuk VPC fungsi.

Saat Anda menghubungkan fungsi Lambda ke VPC, Lambda membuat elastic network interface untuk setiap kombinasi subnet dan grup keamanan yang terpasang pada fungsi tersebut. Kuota layanan default adalah 250 antarmuka jaringan per VPC. Untuk meminta peningkatan kuota, gunakan konsol [Service Quotas](#).

EC2: Antarmuka jaringan elastis dengan jenis “lambda”

Kode Kesalahan: `Klien. OperationNotPermitted`

Pesan galat: Grup keamanan tidak dapat dimodifikasi untuk jenis antarmuka ini

Anda akan menerima kesalahan ini jika Anda mencoba memodifikasi elastic network interface (ENI) yang dikelola oleh Lambda. `ModifyNetworkInterfaceAttribute` ini tidak termasuk dalam API Lambda untuk operasi pembaruan pada antarmuka jaringan elastis yang dibuat oleh Lambda.

DNS: Gagal terhubung ke host dengan UNKNOWNHOSTEXCEPTION

Pesan Kesalahan: `UNKNOWNHOSTEXCEPTION`

Fungsi Lambda mendukung maksimum 20 koneksi TCP bersamaan untuk resolusi DNS. Fungsi Anda mungkin melelahkan batas itu. Permintaan DNS yang paling umum dilakukan melalui UDP. Jika fungsi Anda hanya membuat koneksi DNS UDP, ini tidak mungkin menjadi masalah Anda. Kesalahan ini biasanya terjadi karena kesalahan konfigurasi atau infrastruktur yang terdegradasi, jadi sebelum memeriksa lalu lintas DNS Anda secara mendalam, konfirmasi bahwa infrastruktur DNS Anda dikonfigurasi dan sehat dengan benar dan bahwa fungsi Lambda Anda mengacu pada host yang ditentukan dalam DNS.

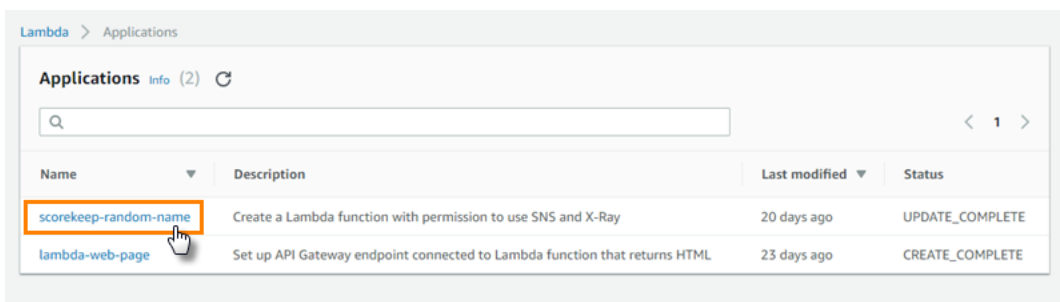
Jika Anda mendiagnosis masalah terkait dengan maksimum koneksi TCP, perhatikan bahwa Anda tidak dapat meminta peningkatan batas ini. Jika fungsi Lambda Anda kembali ke DNS TCP karena muatan DNS yang besar, konfirmasi bahwa solusi Anda menggunakan pustaka yang mendukung EDNS. Untuk informasi lebih lanjut tentang EDNS, lihat standar [RFC 6891](#). Jika muatan DNS Anda secara konsisten melebihi ukuran maks EDNS, solusi Anda mungkin masih menghabiskan batas DNS TCP.

Melihat aplikasi di AWS Lambda konsol

AWS Lambda Konsol membantu Anda memantau dan mengelola aplikasi Lambda Anda. Bagian Aplikasi mencantumkan AWS CloudFormation tumpukan dengan fungsi Lambda. Menu termasuk tumpukan yang Anda luncurkan AWS CloudFormation dengan menggunakan AWS CloudFormation konsol, AWS Serverless Application Repository, AWS CLI, atau AWS SAM CLI

Untuk melihat aplikasi Lambda

1. Buka konsol [halaman Aplikasi](#) konsol Lambda.
2. Pilih aplikasi.



Gambaran umum menampilkan informasi berikut tentang aplikasi Anda.

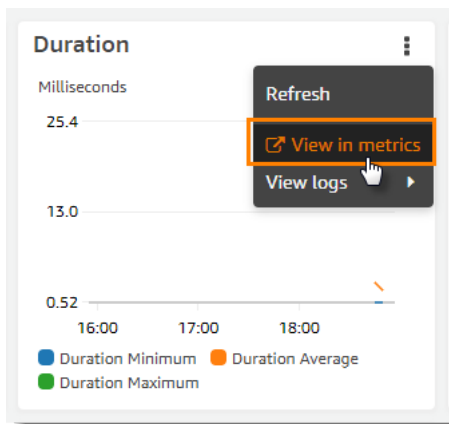
- AWS CloudFormation template atau SAMtemplate — Template yang mendefinisikan aplikasi Anda.
- AWS Resources — Sumber daya yang didefinisikan dalam template aplikasi Anda. Untuk mengelola fungsi Lambda aplikasi, pilih nama fungsi dari daftar.

Memantau aplikasi Lambda

Bagian Aplikasi pada konsol Lambda menyertakan tab Pemantauan tempat Anda dapat meninjau CloudWatch dasbor Amazon dengan metrik agregat untuk sumber daya dalam aplikasi Anda.

Untuk memantau aplikasi Lambda

1. Buka konsol [halaman Aplikasi](#) konsol Lambda.
2. Pilih Pemantauan.
3. Untuk melihat detail selengkapnya tentang metrik dalam grafik apa pun, pilih Lihat dalam metrik dari menu tarik-turun.



Grafik tersebut kemudian akan muncul di sebuah tab baru yang menampilkan metrik-metrik yang relevan yang tercantum di bawah grafik tersebut. Anda dapat menyesuaikan tampilan grafik ini, juga mengubah metrik-metrik dan sumber daya yang ditampilkan, statistik, periode, dan faktor lainnya yang ditampilkan untuk mendapatkan pemahaman lebih baik tentang situasi saat ini.

Secara default, konsol Lambda menunjukkan dasbor dasar. Anda dapat menyesuaikan halaman ini dengan menambahkan satu atau beberapa CloudWatch dasbor Amazon ke templat aplikasi Anda dengan jenis sumber daya [AWS:CloudWatch: :Dasbor](#). Ketika templat Anda mencakup satu dasbor atau lebih, halaman tersebut menampilkan dasbor Anda alih-alih dasbor default. Anda dapat beralih antara dasbor dengan menu tarik turun di kanan atas halaman. Contoh berikut membuat dasbor dengan satu widget yang membuat grafik jumlah invokasi fungsi yang dinamai `my-function`.

Example templat dasbor fungsi

```
Resources:
  MyDashboard:
```

```
Type: AWS::CloudWatch::Dashboard
Properties:
  DashboardName: my-dashboard
  DashboardBody: |
    {
      "widgets": [
        {
          "type": "metric",
          "width": 12,
          "height": 6,
          "properties": {
            "metrics": [
              [
                "AWS/Lambda",
                "Invocations",
                "FunctionName",
                "my-function",
                {
                  "stat": "Sum",
                  "label": "MyFunction"
                }
              ],
              [
                {
                  "expression": "SUM(METRICS())",
                  "label": "Total Invocations"
                }
              ]
            ],
            "region": "us-east-1",
            "title": "Invocations",
            "view": "timeSeries",
            "stacked": false
          }
        }
      ]
    }
  }
```

Untuk informasi selengkapnya tentang pembuatan CloudWatch dasbor dan widget, lihat [Struktur dan sintaks isi dasbor di Referensi Amazon. CloudWatch API](#)

Buat penerapan bergulir untuk fungsi Lambda

Gunakan deployment bergulir untuk mengontrol risiko yang berkaitan dengan memperkenalkan versi baru fungsi Lambda Anda. Dalam deployment bergulir, sistem secara otomatis men-deploy versi baru fungsi dan secara bertahap mengirimkan peningkatan jumlah lalu lintas ke versi baru. Jumlah lalu lintas dan tingkat peningkatan adalah parameter yang dapat Anda konfigurasi.

Anda mengonfigurasi penerapan bergulir dengan menggunakan AWS CodeDeploy dan AWS SAM. CodeDeploy adalah layanan yang mengotomatiskan penerapan aplikasi ke platform komputasi Amazon seperti Amazon EC2 dan AWS Lambda. Untuk informasi lebih lanjut, lihat [Apa itu CodeDeploy?](#) . Dengan menggunakan CodeDeploy untuk menyebarkan fungsi Lambda Anda, Anda dapat dengan mudah memantau status penerapan dan memulai rollback jika Anda mendeteksi masalah apa pun.

AWS SAM adalah kerangka kerja sumber terbuka untuk membangun aplikasi tanpa server. Anda membuat AWS SAM templat (dalam YAML format) untuk menentukan konfigurasi komponen yang diperlukan untuk penerapan bergulir. AWS SAM menggunakan template untuk membuat dan mengkonfigurasi komponen. Untuk informasi selengkapnya, lihat [Apa itu AWS SAM?](#).

Dalam penerapan bergulir, AWS SAM lakukan tugas-tugas ini:

- Mengonfigurasi fungsi Lambda Anda dan membuat alias.

Konfigurasi perutean alias adalah kemampuan dasar yang mengimplementasikan deployment bergulir.

- Ini menciptakan CodeDeploy aplikasi dan kelompok penyebaran.

Grup deployment mengelola deployment bergulir dan rollback (jika diperlukan).

- Mendeteksi ketika Anda membuat versi baru fungsi Lambda Anda.
- Ini memicu CodeDeploy untuk memulai penyebaran versi baru.

Contoh template AWS SAM Lambda

Contoh berikut menunjukkan [templat AWS SAM](#) untuk deployment bergulir sederhana.

```
AWSTemplateFormatVersion : '2010-09-09'  
Transform: AWS::Serverless-2016-10-31
```

```
Description: A sample SAM template for deploying Lambda functions.
```

```
Resources:
```

```
# Details about the myDateTimeFunction Lambda function
```

```
myDateTimeFunction:
```

```
  Type: AWS::Serverless::Function
```

```
  Properties:
```

```
    Handler: myDateTimeFunction.handler
```

```
    Runtime: nodejs18.x
```

```
# Creates an alias named "live" for the function, and automatically publishes when you update the function.
```

```
  AutoPublishAlias: live
```

```
  DeploymentPreference:
```

```
# Specifies the deployment configuration
```

```
  Type: Linear10PercentEvery2Minutes
```

Templat ini menentukan fungsi Lambda bernama `myDateTimeFunction` dengan properti berikut.

AutoPublishAlias

Properti `AutoPublishAlias` membuat alias bernama `live`. Selain itu, kerangka kerja AWS SAM secara otomatis mendeteksi saat Anda menyimpan kode baru untuk fungsi tersebut. Kerangka kerja kemudian menerbitkan versi fungsi baru dan memperbarui alias `live` untuk mengarah ke versi baru.

DeploymentPreference

`DeploymentPreference` Properti menentukan tingkat di mana `CodeDeploy` aplikasi menggeser lalu lintas dari versi asli fungsi Lambda ke versi baru. Nilai `Linear10PercentEvery2Minutes` menggeser sepuluh persen tambahan lalu lintas ke versi baru setiap dua menit.

Untuk daftar konfigurasi deployment yang ditetapkan sebelumnya, lihat [Konfigurasi deployment](#).

Untuk tutorial mendetail tentang cara menggunakan fungsi Lambda, lihat [Menerapkan fungsi Lambda yang diperbarui CodeDeploy](#) dengan `CodeDeploy`

Menggunakan Lambda dengan Kubernetes

[Anda dapat menerapkan dan mengelola fungsi Lambda dengan API Kubernetes AWS menggunakan Controllers for Kubernetes \(ACK\) atau Crossplane.](#)

AWS Pengontrol untuk Kubernetes (ACK)

Anda dapat menggunakan ACK untuk menyebarkan dan mengelola AWS sumber daya dari Kubernetes API. Melalui ACK, AWS menyediakan pengontrol kustom open-source untuk AWS layanan seperti Lambda, Amazon Elastic Container Registry (Amazon ECR), Amazon Simple Storage Service (Amazon S3), dan Amazon SageMaker. Setiap AWS layanan yang didukung memiliki pengontrol kustom sendiri. Di kluster Kubernetes Anda, instal pengontrol untuk setiap AWS layanan yang ingin Anda gunakan. Kemudian, buat [Definisi Sumber Daya Kustom \(CRD\)](#) untuk menentukan AWS sumber daya.

Kami menyarankan Anda menggunakan [Helm 3.8 atau yang lebih baru](#) untuk menginstal pengontrol ACK. Setiap pengontrol ACK dilengkapi dengan bagan Helm sendiri, yang menginstal controller, CRD, dan aturan RBAC Kubernetes. Untuk informasi selengkapnya, lihat [Menginstal ACK Controller](#) di dokumentasi ACK.

Setelah Anda membuat sumber daya khusus ACK, Anda dapat menggunakannya seperti objek Kubernetes bawaan lainnya. [Misalnya, Anda dapat menerapkan dan mengelola fungsi Lambda dengan toolchain Kubernetes pilihan Anda, termasuk kubectl.](#)

Berikut adalah beberapa contoh kasus penggunaan untuk menyediakan fungsi Lambda melalui ACK:

- Organisasi Anda menggunakan [peran kontrol akses berbasis peran \(RBAC\)](#) dan [IAM untuk akun layanan guna](#) membuat batas izin. Dengan ACK, Anda dapat menggunakan kembali model keamanan ini untuk Lambda tanpa harus membuat pengguna dan kebijakan baru.
- Organisasi Anda memiliki DevOps proses untuk menyebarkan sumber daya ke dalam kluster Amazon Elastic Kubernetes Service (Amazon EKS) menggunakan manifes Kubernetes. Dengan ACK, Anda dapat menggunakan manifes untuk menyediakan fungsi Lambda tanpa membuat infrastruktur terpisah sebagai templat kode.

Untuk informasi selengkapnya tentang penggunaan ACK, lihat [tutorial Lambda di dokumentasi ACK](#).

Crossplane

[Crossplane](#) adalah proyek Cloud Native Computing Foundation (CNCF) open-source yang menggunakan Kubernetes untuk mengelola sumber daya infrastruktur cloud. Dengan Crossplane, pengembang dapat meminta infrastruktur tanpa perlu memahami kompleksitasnya. Tim platform mempertahankan kendali atas bagaimana infrastruktur disediakan dan dikelola.

Menggunakan Crossplane, Anda dapat menerapkan dan mengelola fungsi Lambda dengan toolchain Kubernetes pilihan Anda seperti [kubectl](#), dan [pipeline CI/CD apa pun yang dapat menyebarkan manifes ke Kubernetes](#). Berikut adalah beberapa contoh kasus penggunaan untuk menyediakan fungsi Lambda melalui Crossplane:

- [Organisasi Anda ingin menegakkan kepatuhan dengan memastikan bahwa fungsi Lambda memiliki tag yang benar](#). Tim platform dapat menggunakan [Komposisi Crossplane](#) untuk menentukan kebijakan ini melalui abstraksi API. Pengembang kemudian dapat menggunakan abstraksi ini untuk menyebarkan fungsi Lambda dengan tag.
- Proyek Anda menggunakan GitOps Kubernetes. Dalam model ini, Kubernetes terus-menerus merekonsiliasi repositori git (status yang diinginkan) dengan sumber daya yang berjalan di dalam cluster (status saat ini). Jika ada perbedaan, GitOps proses secara otomatis membuat perubahan pada cluster. [Anda dapat menggunakan GitOps Kubernetes untuk menyebarkan dan mengelola fungsi Lambda melalui Crossplane, menggunakan alat dan konsep Kubernetes yang sudah dikenal seperti CRD dan Controller](#).

Untuk mempelajari lebih lanjut tentang menggunakan Crossplane dengan Lambda, lihat berikut ini:

- [AWSBlueprints for Crossplane](#): Repositori ini mencakup contoh cara menggunakan Crossplane untuk menyebarkan sumber daya, termasuk fungsi Lambda. AWS

Note

AWSCetak biru untuk Crossplane sedang dalam pengembangan aktif dan tidak boleh digunakan dalam produksi.

- [Menyebarkan Lambda dengan Amazon EKS dan Crossplane](#): Video ini menunjukkan contoh lanjutan dari penerapan AWS arsitektur tanpa server dengan Crossplane, mengeksplorasi desain dari perspektif pengembang dan platform.

Aplikasi sampel Lambda

GitHub Repositori untuk panduan ini mencakup contoh aplikasi yang menunjukkan penggunaan berbagai bahasa dan AWS layanan. Setiap aplikasi sampel menyertakan skrip untuk penyebaran dan pembersihan yang mudah serta sumber daya pendukung.

Node.js

Aplikasi sampel Lambda dalam Node.js

- [blank-nodejs](#) - Fungsi Node.js yang menunjukkan penggunaan logging, variabel lingkungan, AWS X-Ray tracing, lapisan, pengujian unit, dan SDK. AWS
- [nodejs-apig](#) – Fungsi dengan titik akhir API publik yang memproses peristiwa dari API Gateway dan mengembalikan respons HTTP.
- [efs-nodejs](#) – Fungsi yang menggunakan sistem file Amazon EFS di Amazon VPC. Sampel ini mencakup VPC, sistem file, target pemasangan, dan titik akses yang dikonfigurasi untuk penggunaan dengan Lambda.

Python

Aplikasi sampel Lambda di Python

- [blank-python](#) — Fungsi Python yang menunjukkan penggunaan logging, variabel lingkungan, AWS X-Ray tracing, lapisan, pengujian unit dan SDK. AWS

Ruby

Aplikasi sampel Lambda di Ruby

- [blank-ruby](#) — Fungsi Ruby yang menunjukkan penggunaan logging, variabel lingkungan, AWS X-Ray tracing, layer, pengujian unit, dan SDK. AWS
- [Sampel Kode Ruby untuk AWS Lambda](#) — Contoh kode yang ditulis dalam Ruby yang menunjukkan cara berinteraksi dengan Lambda. AWS

Java

Sampel aplikasi Lambda di Java

- [java17-examples](#) - Fungsi Java yang menunjukkan bagaimana menggunakan catatan Java untuk mewakili objek data peristiwa masukan.
- [java-basic](#) - Kumpulan fungsi Java minimal dengan pengujian unit dan konfigurasi logging variabel.
- [java-events](#) - Kumpulan fungsi Java yang berisi kode kerangka untuk cara menangani peristiwa dari berbagai layanan seperti Amazon API Gateway, Amazon SQS, dan Amazon Kinesis. Fungsi-fungsi ini menggunakan versi terbaru dari [aws-lambda-java-events](#) perpustakaan (3.0.0 dan yang lebih baru). Contoh-contoh ini tidak memerlukan AWS SDK sebagai dependensi.
- [s3-java](#) – Fungsi Java yang memproses kejadian pemberitahuan dari Amazon S3 dan menggunakan Java Class Library (JCL) untuk membuat thumbnail dari file gambar yang diunggah.
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#) — Fungsi Java yang memindai tabel Amazon DynamoDB yang berisi informasi karyawan. Kemudian menggunakan Amazon Simple Notification Service untuk mengirim pesan teks kepada karyawan yang merayakan ulang tahun kerja mereka. Contoh ini menggunakan API Gateway untuk menjalankan fungsi.

Menjalankan kerangka kerja Java populer di Lambda

- [spring-cloud-function-samples](#)— Contoh dari Spring yang menunjukkan cara menggunakan framework [Spring Cloud Function untuk membuat fungsi](#) AWS Lambda.
- [Demo Aplikasi Boot Spring Tanpa Server](#) - Contoh yang menunjukkan cara mengatur aplikasi Spring Boot khas dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime khusus.
- [Demo Aplikasi Micronaut Tanpa Server](#) - Contoh yang menunjukkan cara menggunakan Micronaut dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime kustom. Pelajari lebih lanjut di panduan [Micronaut/Lambda](#).
- [Demo Aplikasi Quarkus Tanpa Server](#) - Contoh yang menunjukkan cara menggunakan Quarkus dalam runtime Java yang dikelola dengan dan tanpa SnapStart, atau sebagai gambar asli GraalVM dengan runtime kustom. [Pelajari lebih lanjut di panduan Quarkus/Lambda dan panduan Quarkus/. SnapStart](#)

Go

Lambda menyediakan aplikasi contoh berikut untuk runtime Go:

Sampel aplikasi Lambda di Go

- [go-al2](#) - Fungsi hello world yang mengembalikan alamat IP publik. Aplikasi ini menggunakan runtime `provided.al2` khusus.
- [blank-go](#) — Fungsi Go yang menunjukkan penggunaan library Go Lambda, logging, variabel lingkungan, dan SDK. AWS Aplikasi ini menggunakan `go1.x` runtime.

C#

Aplikasi sampel Lambda dalam C#

- [blank-c-sharp](#) – Fungsi C# yang menunjukkan penggunaan pustaka NET Lambda, pencatatan, variabel lingkungan, pelacakan AWS X-Ray , uji unit, dan AWS SDK.
- [blank-csharp-with-layer](#)- Fungsi C# yang menggunakan CLI .NET untuk membuat lapisan yang mengemas dependensi fungsi.
- [ec2-spot](#) – Fungsi yang mengelola permintaan instans di Amazon EC2.

PowerShell

Lambda menyediakan contoh aplikasi berikut untuk: PowerShell

- [blank-powershell](#) — PowerShell Fungsi yang menunjukkan penggunaan logging, variabel lingkungan, dan SDK. AWS

Untuk men-deploy aplikasi sampel, ikuti petunjuk di file README.

Menggunakan Lambda dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDKs) tersedia untuk banyak bahasa pemrograman populer. Masing-masing SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan pengembang untuk membangun aplikasi dalam bahasa pilihan mereka.

| SDK dokumentasi | Contoh kode |
|--|--|
| AWS SDK for C++ | AWS SDK for C++ contoh kode |
| AWS CLI | AWS CLI contoh kode |
| AWS SDK for Go | AWS SDK for Go contoh kode |
| AWS SDK for Java | AWS SDK for Java contoh kode |
| AWS SDK for JavaScript | AWS SDK for JavaScript contoh kode |
| AWS SDK for Kotlin | AWS SDK for Kotlin contoh kode |
| AWS SDK for .NET | AWS SDK for .NET contoh kode |
| AWS SDK for PHP | AWS SDK for PHP contoh kode |
| AWS Tools for PowerShell | Alat untuk contoh PowerShell kode |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) contoh kode |
| AWS SDK for Ruby | AWS SDK for Ruby contoh kode |
| AWS SDK for Rust | AWS SDK for Rust contoh kode |
| AWS SDK untuk SAP ABAP | AWS SDK untuk SAP ABAP contoh kode |
| AWS SDK for Swift | AWS SDK for Swift contoh kode |

Untuk contoh khusus untuk Lambda, lihat. [Contoh kode untuk Lambda menggunakan AWS SDKs](#)

 Ketersediaan contoh

Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik di bagian bawah halaman ini.

Contoh kode untuk Lambda menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan Lambda dengan kit pengembangan AWS perangkat lunak (SDK).

Dasar-dasar adalah contoh kode yang menunjukkan kepada Anda bagaimana melakukan operasi penting dalam suatu layanan.

Tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Sementara tindakan menunjukkan cara memanggil fungsi layanan individual, Anda dapat melihat tindakan dalam konteks dalam skenario terkait.

Skenario adalah contoh kode yang menunjukkan kepada Anda bagaimana menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam layanan atau dikombinasikan dengan yang lain AWS layanan.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memulai

Halo Lambda

Contoh kode berikut menunjukkan cara memulai menggunakan Lambda.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
namespace LambdaActions;  
  
using Amazon.Lambda;
```

```
public class HelloLambda
{
    static async Task Main(string[] args)
    {
        var lambdaClient = new AmazonLambdaClient();

        Console.WriteLine("Hello AWS Lambda");
        Console.WriteLine("Let's get started with AWS Lambda by listing your
existing Lambda functions:");

        var response = await lambdaClient.ListFunctionsAsync();
        response.Functions.ForEach(function =>
        {

            Console.WriteLine($"{function.FunctionName}\t{function.Description}");
        });
    }
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Kode untuk CMakeLists file.txtCMake.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS lambda)
```

```
# Set this project's name.
project("hello_lambda")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
  libraries for the AWS SDK.
  string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
    "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
  list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
  # Copy relevant AWS SDK for C++ libraries into the current binary directory
  for running and debugging.

  # set(BIN_SUB_DIR "/Debug") # if you are building from the command line you
  may need to uncomment this
  # and set the proper subdirectory to the
  executables' location.

  AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
    ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
  hello_lambda.cpp)

target_link_libraries(${PROJECT_NAME}
  ${AWSSDK_LINK_LIBRARIES})
```

Kode untuk file sumber hello_lambda.cpp.

```
#include <aws/core/Aws.h>
```

```
#include <aws/lambda/LambdaClient.h>
#include <aws/lambda/model/ListFunctionsRequest.h>
#include <iostream>

/*
 * A "Hello Lambda" starter application which initializes an AWS Lambda (Lambda)
 client and lists the Lambda functions.
 *
 * main function
 *
 * Usage: 'hello_lambda'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
    // options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::Lambda::LambdaClient lambdaClient(clientConfig);
        std::vector<Aws::String> functions;
        Aws::String marker; // Used for pagination.

        do {
            Aws::Lambda::Model::ListFunctionsRequest request;
            if (!marker.empty()) {
                request.SetMarker(marker);
            }

            Aws::Lambda::Model::ListFunctionsOutcome outcome =
lambdaClient.ListFunctions(
                request);

            if (outcome.IsSuccess()) {
                const Aws::Lambda::Model::ListFunctionsResult
&listFunctionsResult = outcome.GetResult();
                std::cout << listFunctionsResult.GetFunctions().size()
<< " lambda functions were retrieved." << std::endl;
            }
        }
    }
}
```

```

        for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: listFunctionsResult.GetFunctions()) {
            functions.push_back(functionConfiguration.GetFunctionName());
            std::cout << functions.size() << " "
                << functionConfiguration.GetDescription() <<
std::endl;

            std::cout << " "
                <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                functionConfiguration.GetRuntime()) << ": "
                << functionConfiguration.GetHandler()
                << std::endl;
        }
        marker = listFunctionsResult.GetNextMarker();
    } else {
        std::cerr << "Error with Lambda::ListFunctions. "
            << outcome.GetError().GetMessage()
            << std::endl;
        result = 1;
        break;
    }
} while (!marker.empty());
}

Aws::ShutdownAPI(options); // Should only be called once.
return result;
}

```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for C++ API Referensi.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).


```
package main

import (
    "context"
    "fmt"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/lambda"
)

// main uses the AWS SDK for Go (v2) to create an AWS Lambda client and list up
// to 10
// functions in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
    sdkConfig, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        fmt.Println("Couldn't load default configuration. Have you set up your AWS
account?")
        fmt.Println(err)
        return
    }
    lambdaClient := lambda.NewFromConfig(sdkConfig)

    maxItems := 10
    fmt.Printf("Let's list up to %v functions for your account.\n", maxItems)
    result, err := lambdaClient.ListFunctions(context.TODO(),
&lambda.ListFunctionsInput{
    MaxItems: aws.Int32(int32(maxItems)),
})
    if err != nil {
        fmt.Printf("Couldn't list functions for your account. Here's why: %v\n", err)
        return
    }
    if len(result.Functions) == 0 {
        fmt.Println("You don't have any functions!")
    } else {
        for _, function := range result.Functions {
            fmt.Printf("\t\t%v\n", *function.FunctionName)
        }
    }
}
```

```
}  
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Go API Referensi.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
package com.example.lambda;  
  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.lambda.LambdaClient;  
import software.amazon.awssdk.services.lambda.model.LambdaException;  
import software.amazon.awssdk.services.lambda.model.ListFunctionsResponse;  
import software.amazon.awssdk.services.lambda.model.FunctionConfiguration;  
import java.util.List;  
  
/**  
 * Before running this Java V2 code example, set up your development  
 * environment, including your credentials.  
 *  
 * For more information, see the following documentation topic:  
 *  
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html  
 */  
public class ListLambdaFunctions {  
    public static void main(String[] args) {  
        Region region = Region.US_WEST_2;  
        LambdaClient awsLambda = LambdaClient.builder()  
            .region(region)  
            .build();  
    }  
}
```

```
        listFunctions(awsLambda);
        awsLambda.close();
    }

    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Java 2.x API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import { LambdaClient, paginateListFunctions } from "@aws-sdk/client-lambda";

const client = new LambdaClient({});

export const helloLambda = async () => {
    const paginator = paginateListFunctions({ client }, {});
    const functions = [];

    for await (const page of paginator) {
```

```
const funcNames = page.Functions.map((f) => f.FunctionName);
functions.push(...funcNames);
}

console.log("Functions:");
console.log(functions.join("\n"));
return functions;
};
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for JavaScript API Referensi.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import boto3

def main():
    """
    List the Lambda functions in your AWS account.
    """
    # Create the Lambda client
    lambda_client = boto3.client("lambda")

    # Use the paginator to list the functions
    paginator = lambda_client.get_paginator("list_functions")
    response_iterator = paginator.paginate()

    print("Here are the Lambda functions in your account:")
    for page in response_iterator:
        for function in page["Functions"]:
            print(f" {function['FunctionName']}")
```

```
if __name__ == "__main__":  
    main()
```

- Untuk API detailnya, lihat [ListFunctions AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
require 'aws-sdk-lambda'  
  
# Creates an AWS Lambda client using the default credentials and configuration  
def lambda_client  
  Aws::Lambda::Client.new  
end  
  
# Lists the Lambda functions in your AWS account, paginating the results if  
# necessary  
def list_lambda_functions  
  lambda = lambda_client  
  
  # Use a pagination iterator to list all functions  
  functions = []  
  lambda.list_functions.each_page do |page|  
    functions.concat(page.functions)  
  end  
  
  # Print the name and ARN of each function  
  functions.each do |function|  
    puts "Function name: #{function.function_name}"  
    puts "Function ARN: #{function.function_arn}"  
    puts  
  end  
end
```

```
end

puts "Total functions: #{functions.count}"
end

list_lambda_functions if __FILE__ == $PROGRAM_NAME
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Ruby API Referensi.

Contoh kode

- [Contoh dasar untuk penggunaan Lambda AWS SDKs](#)
 - [Halo Lambda](#)
 - [Tindakan untuk Lambda menggunakan AWS SDKs](#)
 - [Gunakan CreateAlias dengan AWS SDK atau CLI](#)
 - [Gunakan CreateFunction dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteAlias dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteFunction dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteFunctionConcurrency dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
 - [Gunakan GetAccountSettings dengan AWS SDK atau CLI](#)
 - [Gunakan GetAlias dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunction dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunctionConcurrency dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunctionConfiguration dengan AWS SDK atau CLI](#)
 - [Gunakan GetPolicy dengan AWS SDK atau CLI](#)
 - [Gunakan GetProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
 - [Gunakan Invoke dengan AWS SDK atau CLI](#)
 - [Gunakan ListFunctions dengan AWS SDK atau CLI](#)
 - [Gunakan ListProvisionedConcurrencyConfigs dengan AWS SDK atau CLI](#)
 - [Gunakan ListTags dengan AWS SDK atau CLI](#)
 - [Gunakan ListVersionsByFunction dengan AWS SDK atau CLI](#)

- [Gunakan PublishVersion dengan AWS SDK atau CLI](#)
- [Gunakan PutFunctionConcurrency dengan AWS SDK atau CLI](#)
- [Gunakan PutProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan RemovePermission dengan AWS SDK atau CLI](#)
- [Gunakan TagResource dengan AWS SDK atau CLI](#)
- [Gunakan UntagResource dengan AWS SDK atau CLI](#)
- [Gunakan UpdateAlias dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionCode dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionConfiguration dengan AWS SDK atau CLI](#)
- [Skenario untuk Lambda menggunakan AWS SDKs](#)
 - [Secara otomatis mengonfirmasi pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK](#)
 - [Secara otomatis memigrasikan pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK](#)
 - [Buat API Gateway REST API untuk melacak data COVID -19](#)
 - [Buat perpustakaan pinjaman REST API](#)
 - [Membuat aplikasi messenger dengan Step Functions](#)
 - [Membuat aplikasi manajemen aset foto yang memungkinkan pengguna mengelola foto menggunakan label](#)
 - [Buat aplikasi obrolan websocket dengan API Gateway](#)
 - [Buat aplikasi yang menganalisis umpan balik pelanggan dan mensintesis audio](#)
 - [Mulai membuat dan menjalankan fungsi Lambda menggunakan AWS SDK](#)
 - [Menginvokasi fungsi Lambda dari browser](#)
 - [Transformasi data untuk aplikasi Anda dengan S3 Object Lambda](#)
 - [Gunakan API Gateway untuk menjalankan fungsi Lambda](#)
 - [Menggunakan Step Functions untuk menginvokasi fungsi Lambda](#)
 - [Menggunakan peristiwa terjadwal untuk menginvokasi fungsi Lambda](#)
 - [Menulis data aktivitas kustom dengan fungsi Lambda setelah otentikasi pengguna Amazon Cognito menggunakan AWS SDK](#)
- [Contoh tanpa server untuk penggunaan Lambda AWS SDKs](#)
 - [Menghubungkan ke RDS database Amazon dalam fungsi Lambda](#)

- [Memanggil fungsi Lambda dari pemicu Kinesis](#)
- [Memanggil fungsi Lambda dari pemicu DynamoDB](#)
- [Memanggil fungsi Lambda dari pemicu Amazon DocumentDB](#)
- [Memanggil fungsi Lambda dari pemicu Amazon MSK](#)
- [Menginvokasi fungsi Lambda dari pemicu Amazon S3](#)
- [Memanggil fungsi Lambda dari pemicu Amazon SNS](#)
- [Memanggil fungsi Lambda dari pemicu Amazon SQS](#)
- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Kinesis](#)
- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu DynamoDB](#)
- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Amazon SQS](#)

Contoh dasar untuk penggunaan Lambda AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan dasar-dasar AWS Lambda dengan AWS SDKs.

Contoh

- [Halo Lambda](#)
- [Tindakan untuk Lambda menggunakan AWS SDKs](#)
 - [Gunakan CreateAlias dengan AWS SDK atau CLI](#)
 - [Gunakan CreateFunction dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteAlias dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteFunction dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteFunctionConcurrency dengan AWS SDK atau CLI](#)
 - [Gunakan DeleteProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
 - [Gunakan GetAccountSettings dengan AWS SDK atau CLI](#)
 - [Gunakan GetAlias dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunction dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunctionConcurrency dengan AWS SDK atau CLI](#)
 - [Gunakan GetFunctionConfiguration dengan AWS SDK atau CLI](#)
 - [Gunakan GetPolicy dengan AWS SDK atau CLI](#)

- [Gunakan GetProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan Invoke dengan AWS SDK atau CLI](#)
- [Gunakan ListFunctions dengan AWS SDK atau CLI](#)
- [Gunakan ListProvisionedConcurrencyConfigs dengan AWS SDK atau CLI](#)
- [Gunakan ListTags dengan AWS SDK atau CLI](#)
- [Gunakan ListVersionsByFunction dengan AWS SDK atau CLI](#)
- [Gunakan PublishVersion dengan AWS SDK atau CLI](#)
- [Gunakan PutFunctionConcurrency dengan AWS SDK atau CLI](#)
- [Gunakan PutProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan RemovePermission dengan AWS SDK atau CLI](#)
- [Gunakan TagResource dengan AWS SDK atau CLI](#)
- [Gunakan UntagResource dengan AWS SDK atau CLI](#)
- [Gunakan UpdateAlias dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionCode dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionConfiguration dengan AWS SDK atau CLI](#)

Halo Lambda

Contoh kode berikut menunjukkan cara memulai menggunakan Lambda.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
namespace LambdaActions;  
  
using Amazon.Lambda;  
  
public class HelloLambda
```

```
{
    static async Task Main(string[] args)
    {
        var lambdaClient = new AmazonLambdaClient();

        Console.WriteLine("Hello AWS Lambda");
        Console.WriteLine("Let's get started with AWS Lambda by listing your
existing Lambda functions:");

        var response = await lambdaClient.ListFunctionsAsync();
        response.Functions.ForEach(function =>
        {

            Console.WriteLine($"{function.FunctionName}\t{function.Description}");
        });
    }
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Kode untuk CMakeLists file.txtCMake.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS lambda)

# Set this project's name.
project("hello_lambda")
```

```
# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
  libraries for the AWS SDK.
  string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
    "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
  list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
  # Copy relevant AWS SDK for C++ libraries into the current binary directory
  for running and debugging.

  # set(BIN_SUB_DIR "/Debug") # if you are building from the command line you
  may need to uncomment this
  # and set the proper subdirectory to the
  executables' location.

  AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
    ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
  hello_lambda.cpp)

target_link_libraries(${PROJECT_NAME}
  ${AWSSDK_LINK_LIBRARIES})
```

Kode untuk file sumber hello_lambda.cpp.

```
#include <aws/core/Aws.h>
#include <aws/lambda/LambdaClient.h>
#include <aws/lambda/model/ListFunctionsRequest.h>
```

```
#include <iostream>

/*
 * A "Hello Lambda" starter application which initializes an AWS Lambda (Lambda)
 client and lists the Lambda functions.
 *
 * main function
 *
 * Usage: 'hello_lambda'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
    // options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::Lambda::LambdaClient lambdaClient(clientConfig);
        std::vector<Aws::String> functions;
        Aws::String marker; // Used for pagination.

        do {
            Aws::Lambda::Model::ListFunctionsRequest request;
            if (!marker.empty()) {
                request.SetMarker(marker);
            }

            Aws::Lambda::Model::ListFunctionsOutcome outcome =
lambdaClient.ListFunctions(
                request);

            if (outcome.IsSuccess()) {
                const Aws::Lambda::Model::ListFunctionsResult
&listFunctionsResult = outcome.GetResult();
                std::cout << listFunctionsResult.GetFunctions().size()
                    << " lambda functions were retrieved." << std::endl;
            }
        }
    }
}
```

```

        for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: listFunctionsResult.GetFunctions()) {
            functions.push_back(functionConfiguration.GetFunctionName());
            std::cout << functions.size() << " "
                << functionConfiguration.GetDescription() <<
std::endl;
            std::cout << " "
                <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                functionConfiguration.GetRuntime()) << ": "
                << functionConfiguration.GetHandler()
                << std::endl;
        }
        marker = listFunctionsResult.GetNextMarker();
    } else {
        std::cerr << "Error with Lambda::ListFunctions. "
            << outcome.GetError().GetMessage()
            << std::endl;
        result = 1;
        break;
    }
} while (!marker.empty());
}

Aws::ShutdownAPI(options); // Should only be called once.
return result;
}

```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for C++ API Referensi.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
package main

import (
    "context"
    "fmt"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/lambda"
)

// main uses the AWS SDK for Go (v2) to create an AWS Lambda client and list up
// to 10
// functions in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
    sdkConfig, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        fmt.Println("Couldn't load default configuration. Have you set up your AWS
account?")
        fmt.Println(err)
        return
    }
    lambdaClient := lambda.NewFromConfig(sdkConfig)

    maxItems := 10
    fmt.Printf("Let's list up to %v functions for your account.\n", maxItems)
    result, err := lambdaClient.ListFunctions(context.TODO(),
&lambda.ListFunctionsInput{
    MaxItems: aws.Int32(int32(maxItems)),
})
    if err != nil {
        fmt.Printf("Couldn't list functions for your account. Here's why: %v\n", err)
        return
    }
    if len(result.Functions) == 0 {
        fmt.Println("You don't have any functions!")
    } else {
        for _, function := range result.Functions {
            fmt.Printf("\t\t%v\n", *function.FunctionName)
        }
    }
}
```

```
}  
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Go API Referensi.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
package com.example.lambda;  
  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.lambda.LambdaClient;  
import software.amazon.awssdk.services.lambda.model.LambdaException;  
import software.amazon.awssdk.services.lambda.model.ListFunctionsResponse;  
import software.amazon.awssdk.services.lambda.model.FunctionConfiguration;  
import java.util.List;  
  
/**  
 * Before running this Java V2 code example, set up your development  
 * environment, including your credentials.  
 *  
 * For more information, see the following documentation topic:  
 *  
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html  
 */  
public class ListLambdaFunctions {  
    public static void main(String[] args) {  
        Region region = Region.US_WEST_2;  
        LambdaClient awsLambda = LambdaClient.builder()  
            .region(region)  
            .build();
```

```
        listFunctions(awsLambda);
        awsLambda.close();
    }

    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Java 2.x API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import { LambdaClient, paginateListFunctions } from "@aws-sdk/client-lambda";

const client = new LambdaClient({});

export const helloLambda = async () => {
    const paginator = paginateListFunctions({ client }, {});
    const functions = [];

    for await (const page of paginator) {
```



```
const funcNames = page.Functions.map((f) => f.FunctionName);
functions.push(...funcNames);
}

console.log("Functions:");
console.log(functions.join("\n"));
return functions;
};
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for JavaScript API Referensi.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import boto3

def main():
    """
    List the Lambda functions in your AWS account.
    """
    # Create the Lambda client
    lambda_client = boto3.client("lambda")

    # Use the paginator to list the functions
    paginator = lambda_client.get_paginator("list_functions")
    response_iterator = paginator.paginate()

    print("Here are the Lambda functions in your account:")
    for page in response_iterator:
        for function in page["Functions"]:
            print(f" {function['FunctionName']}")
```

```
if __name__ == "__main__":  
    main()
```

- Untuk API detailnya, lihat [ListFunctions AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
require 'aws-sdk-lambda'  
  
# Creates an AWS Lambda client using the default credentials and configuration  
def lambda_client  
  Aws::Lambda::Client.new  
end  
  
# Lists the Lambda functions in your AWS account, paginating the results if  
# necessary  
def list_lambda_functions  
  lambda = lambda_client  
  
  # Use a pagination iterator to list all functions  
  functions = []  
  lambda.list_functions.each_page do |page|  
    functions.concat(page.functions)  
  end  
  
  # Print the name and ARN of each function  
  functions.each do |function|  
    puts "Function name: #{function.function_name}"  
    puts "Function ARN: #{function.function_arn}"  
    puts  
  end  
end
```

```
end

puts "Total functions: #{functions.count}"
end

list_lambda_functions if __FILE__ == $PROGRAM_NAME
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Ruby API Referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Tindakan untuk Lambda menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara melakukan tindakan Lambda individu dengan AWS SDKs. Setiap contoh menyertakan tautan ke GitHub, di mana Anda dapat menemukan instruksi untuk mengatur dan menjalankan kode.

Kutipan ini memanggil Lambda API dan merupakan kutipan kode dari program yang lebih besar yang harus dijalankan dalam konteks. Anda dapat melihat tindakan dalam konteks di [Skenario untuk Lambda menggunakan AWS SDKs](#).

Contoh berikut hanya mencakup tindakan yang paling umum digunakan. Untuk daftar lengkap, lihat [AWS Lambda API Referensi](#).

Contoh

- [Gunakan CreateAlias dengan AWS SDK atau CLI](#)
- [Gunakan CreateFunction dengan AWS SDK atau CLI](#)
- [Gunakan DeleteAlias dengan AWS SDK atau CLI](#)
- [Gunakan DeleteFunction dengan AWS SDK atau CLI](#)
- [Gunakan DeleteFunctionConcurrency dengan AWS SDK atau CLI](#)
- [Gunakan DeleteProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan GetAccountSettings dengan AWS SDK atau CLI](#)
- [Gunakan GetAlias dengan AWS SDK atau CLI](#)

- [Gunakan GetFunction dengan AWS SDK atau CLI](#)
- [Gunakan GetFunctionConcurrency dengan AWS SDK atau CLI](#)
- [Gunakan GetFunctionConfiguration dengan AWS SDK atau CLI](#)
- [Gunakan GetPolicy dengan AWS SDK atau CLI](#)
- [Gunakan GetProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan Invoke dengan AWS SDK atau CLI](#)
- [Gunakan ListFunctions dengan AWS SDK atau CLI](#)
- [Gunakan ListProvisionedConcurrencyConfigs dengan AWS SDK atau CLI](#)
- [Gunakan ListTags dengan AWS SDK atau CLI](#)
- [Gunakan ListVersionsByFunction dengan AWS SDK atau CLI](#)
- [Gunakan PublishVersion dengan AWS SDK atau CLI](#)
- [Gunakan PutFunctionConcurrency dengan AWS SDK atau CLI](#)
- [Gunakan PutProvisionedConcurrencyConfig dengan AWS SDK atau CLI](#)
- [Gunakan RemovePermission dengan AWS SDK atau CLI](#)
- [Gunakan TagResource dengan AWS SDK atau CLI](#)
- [Gunakan UntagResource dengan AWS SDK atau CLI](#)
- [Gunakan UpdateAlias dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionCode dengan AWS SDK atau CLI](#)
- [Gunakan UpdateFunctionConfiguration dengan AWS SDK atau CLI](#)

Gunakan **CreateAlias** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `CreateAlias`.

CLI

AWS CLI

Untuk membuat alias untuk fungsi Lambda

`create-alias` Contoh berikut membuat alias bernama `LIVE` yang menunjuk ke versi 1 dari fungsi `my-function` Lambda.

```
aws lambda create-alias \  
  --function-name my-function \  
  --version 1 \  
  --alias LIVE \  
  --function-arn arn:aws:lambda:us-east-1:123456789012:function:my-function
```

```
--description "alias for live version of function" \
--function-version 1 \
--name LIVE
```

Output:

```
{
  "FunctionVersion": "1",
  "Name": "LIVE",
  "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
  "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
  "Description": "alias for live version of function"
}
```

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [CreateAlias](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini membuat Alias Lambda Baru untuk versi tertentu dan konfigurasi perutean untuk menentukan persentase permintaan pemanggilan yang diterimanya.

```
New-LMAlias -FunctionName "MylambdaFunction123" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6"} -Description "Alias
for version 4" -FunctionVersion 4 -Name "PowershellAlias"
```

- Untuk API detailnya, lihat [CreateAlias](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **CreateFunction** dengan AWS SDK atau CLI


Contoh kode berikut menunjukkan cara menggunakan `CreateFunction`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Creates a new Lambda function.
/// </summary>
/// <param name="functionName">The name of the function.</param>
/// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
/// bucket where the zip file containing the code is located.</param>
/// <param name="s3Key">The Amazon S3 key of the zip file.</param>
/// <param name="role">The Amazon Resource Name (ARN) of a role with the
/// appropriate Lambda permissions.</param>
/// <param name="handler">The name of the handler function.</param>
/// <returns>The Amazon Resource Name (ARN) of the newly created
/// Lambda function.</returns>
public async Task<string> CreateLambdaFunctionAsync(
    string functionName,
    string s3Bucket,
    string s3Key,
    string role,
    string handler)
{
    // Defines the location for the function code.
    // S3Bucket - The S3 bucket where the file containing
    //           the source code is stored.
    // S3Key    - The name of the file containing the code.
    var functionCode = new FunctionCode
    {
        S3Bucket = s3Bucket,
```

```

        S3Key = s3Key,
    };

    var createFunctionRequest = new CreateFunctionRequest
    {
        FunctionName = functionName,
        Description = "Created by the Lambda .NET API",
        Code = functionCode,
        Handler = handler,
        Runtime = Runtime.Dotnet6,
        Role = role,
    };

    var reponse = await
_lambdaService.CreateFunctionAsync(createFunctionRequest);
    return reponse.FunctionArn;
}

```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

    Aws::Client::ClientConfiguration clientConfig;
    // Optional: Set to the AWS Region in which the bucket was created
    (overrides config file).
    // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::CreateFunctionRequest request;
    request.SetFunctionName(LAMBDA_NAME);
    request.SetDescription(LAMBDA_DESCRIPTION); // Optional.

```

```
#if USE_CPP_LAMBDA_FUNCTION
    request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
    request.SetTimeout(15);
    request.SetMemorySize(128);

    // Assume the AWS Lambda function was built in Docker with same
    architecture
    // as this code.
#if defined(__x86_64__)
    request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
#elif defined(__aarch64__)
    request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
#else
#error "Unimplemented architecture"
#endif // defined(architecture)
#else
    request.SetRuntime(Aws::Lambda::Model::Runtime::python3_8);
#endif

    request.SetRole(roleArn);
    request.SetHandler(LAMBDA_HANDLER_NAME);
    request.SetPublish(true);
    Aws::Lambda::Model::FunctionCode code;
    std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                          std::ios_base::in | std::ios_base::binary);
    if (!ifstream.is_open()) {
        std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
std::endl;
    }

#if USE_CPP_LAMBDA_FUNCTION
    std::cerr
        << "The cpp Lambda function must be built following the
instructions in the cpp_lambda/README.md file. "
        << std::endl;
#endif

    deleteIamRole(clientConfig);
    return false;
}

    Aws::StringStream buffer;
    buffer << ifstream.rdbuf();

    code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
buffer.str().c_str(),
                                          buffer.str().length()));
```



```

    request.SetCode(code);

    Aws::Lambda::Model::CreateFunctionOutcome outcome =
client.CreateFunction(
    request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda function was successfully created. " <<
seconds
                << " seconds elapsed." << std::endl;
        break;
    }

    else {
        std::cerr << "Error with CreateFunction. "
                << outcome.GetError().GetMessage()
                << std::endl;
        deleteIamRole(clientConfig);
        return false;
    }

```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Untuk membuat fungsi Lambda

create-function Contoh berikut menciptakan fungsi Lambda bernama. my-function

```

aws lambda create-function \
  --function-name my-function \
  --runtime nodejs18.x \
  --zip-file fileb://my-function.zip \
  --handler my-function.handler \
  --role arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-tges6bf4

```

Isi dari my-function.zip:

This file is a deployment package that contains your function code and any dependencies.

Output:

```
{
  "TracingConfig": {
    "Mode": "PassThrough"
  },
  "CodeSha256": "PFn4S+er27qk+UuZSTKEQfNKG/XNn7QJs90mJgq6oH8=",
  "FunctionName": "my-function",
  "CodeSize": 308,
  "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
  "MemorySize": 128,
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
  "Version": "$LATEST",
  "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-zgur6bf4",
  "Timeout": 3,
  "LastModified": "2023-10-14T22:26:11.234+0000",
  "Handler": "my-function.handler",
  "Runtime": "nodejs18.x",
  "Description": ""
}
```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [CreateFunction](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
    LambdaClient *lambda.Client
}

// CreateFunction creates a new Lambda function from code contained in the
// zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
// until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(functionName string, handlerName
string,
iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
    var state types.State
    _, err := wrapper.LambdaClient.CreateFunction(context.TODO(),
&lambda.CreateFunctionInput{
        Code:          &types.FunctionCode{ZipFile: zipPackage.Bytes()},
        FunctionName:   aws.String(functionName),
        Role:           iamRoleArn,
        Handler:        aws.String(handlerName),
        Publish:        true,
        Runtime:        types.RuntimePython38,
    })
    if err != nil {
        var resConflict *types.ResourceConflictException
        if errors.As(err, &resConflict) {
            log.Printf("Function %v already exists.\n", functionName)
            state = types.StateActive
        } else {
            log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
        }
    } else {
        waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
        funcOutput, err := waiter.WaitForOutput(context.TODO(),
&lambda.GetFunctionInput{
            FunctionName: aws.String(functionName)}, 1*time.Minute)
        if err != nil {
```

```
    log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
functionName, err)
} else {
    state = funcOutput.Configuration.State
}
}
return state
}
```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for Go API Referensi.

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.CreateFunctionRequest;
import software.amazon.awssdk.services.lambda.model.FunctionCode;
import software.amazon.awssdk.services.lambda.model.CreateFunctionResponse;
import software.amazon.awssdk.services.lambda.model.GetFunctionRequest;
import software.amazon.awssdk.services.lambda.model.GetFunctionResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;
import software.amazon.awssdk.services.lambda.model.Runtime;
import software.amazon.awssdk.services.lambda.waiters.LambdaWaiter;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;

/**
 * This code example requires a ZIP or JAR that represents the code of the
 * Lambda function.
```

```
* If you do not have a ZIP or JAR, please refer to the following document:
*
* https://github.com/aws-doc-sdk-examples/tree/master/javav2/usecases/creating\_workflows\_stepfunctions
*
* Also, set up your development environment, including your credentials.
*
* For information, see this documentation topic:
*
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
*/
```

```
public class CreateFunction {
    public static void main(String[] args) {

        final String usage = ""

            Usage:
                <functionName> <filePath> <role> <handler>\s

            Where:
                functionName - The name of the Lambda function.\s
                filePath - The path to the ZIP or JAR where the code is
located.\s
                role - The role ARN that has Lambda permissions.\s
                handler - The fully qualified method name (for example,
example.Handler::handleRequest). \s
            """;

        if (args.length != 4) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        String filePath = args[1];
        String role = args[2];
        String handler = args[3];
        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
            .region(region)
            .build();
```

```
        createLambdaFunction(awsLambda, functionName, filePath, role, handler);
        awsLambda.close();
    }

    public static void createLambdaFunction(LambdaClient awsLambda,
        String functionName,
        String filePath,
        String role,
        String handler) {

        try {
            LambdaWaiter waiter = awsLambda.waiter();
            InputStream is = new FileInputStream(filePath);
            SdkBytes fileToUpload = SdkBytes.fromInputStream(is);

            FunctionCode code = FunctionCode.builder()
                .zipFile(fileToUpload)
                .build();

            CreateFunctionRequest functionRequest =
                CreateFunctionRequest.builder()
                    .functionName(functionName)
                    .description("Created by the Lambda Java API")
                    .code(code)
                    .handler(handler)
                    .runtime(Runtime.JAVA8)
                    .role(role)
                    .build();

            // Create a Lambda function using a waiter.
            CreateFunctionResponse functionResponse =
                awsLambda.createFunction(functionRequest);
            GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
                .functionName(functionName)
                .build();

            WaiterResponse<GetFunctionResponse> waiterResponse =
                waiter.waitUntilFunctionExists(getFunctionRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println("The function ARN is " +
                functionResponse.functionArn());

        } catch (LambdaException | FileNotFoundException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

```
    }  
  }  
}
```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for Java 2.x API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
const createFunction = async (funcName, roleArn) => {  
  const client = new LambdaClient({});  
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);  
  
  const command = new CreateFunctionCommand({  
    Code: { ZipFile: code },  
    FunctionName: funcName,  
    Role: roleArn,  
    Architectures: [Architecture.arm64],  
    Handler: "index.handler", // Required when sending a .zip file  
    PackageType: PackageType.Zip, // Required when sending a .zip file  
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file  
  });  
  
  return client.send(command);  
};
```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for JavaScript API Referensi.

Kotlin

SDKuntuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun createNewFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String,
): String? {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }

    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java8
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitUntilFunctionActive {
            functionName = myFunctionName
        }
        return functionResponse.functionArn
    }
}
```


- Untuk API detailnya, lihat [CreateFunction AWS SDK API referensi Kotlin](#).

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function createFunction($functionName, $role, $bucketName, $handler)
{
    //This assumes the Lambda function is in an S3 bucket.
    return $this->customWaiter(function () use ($functionName, $role,
$bucketName, $handler) {
        return $this->lambdaClient->createFunction([
            'Code' => [
                'S3Bucket' => $bucketName,
                'S3Key' => $functionName,
            ],
            'FunctionName' => $functionName,
            'Role' => $role['Arn'],
            'Runtime' => 'python3.9',
            'Handler' => "$handler.lambda_handler",
        ]);
    });
}
```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for PHP API Referensi.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini membuat fungsi C# (dotnetcore1.0 runtime) baru bernama MyFunction AWS Lambda, menyediakan binari yang dikompilasi untuk fungsi dari file zip pada sistem file lokal (jalur relatif atau absolut dapat digunakan). Fungsi C# Lambda

menentukan handler untuk fungsi menggunakan penunjukan: `:Namespace.AssemblyName.ClassName::MethodName`. Anda harus mengganti nama assembly (tanpa akhiran `.dll`), namespace, nama kelas dan bagian nama metode dari spesifikasi handler dengan tepat. Fungsi baru akan memiliki variabel lingkungan `'envvar1'` dan `'envvar2'` yang diatur dari nilai yang disediakan.

```
Publish-LMFunction -Description "My C# Lambda Function" `
  -FunctionName MyFunction `
  -ZipFilename .\MyFunctionBinaries.zip `
  -Handler "AssemblyName::Namespace.ClassName::MethodName" `
  -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
  -Runtime dotnetcore1.0 `
  -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

Output:

```
CodeSha256      : /NgBmd...gq71I=
CodeSize       : 214784
DeadLetterConfig :
Description     : My C# Lambda Function
Environment    : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn    : arn:aws:lambda:us-west-2:123456789012:function:ToUpper
FunctionName   : MyFunction
Handler        : AssemblyName::Namespace.ClassName::MethodName
KMSKeyArn     :
LastModified   : 2016-12-29T23:50:14.207+0000
MemorySize    : 128
Role           : arn:aws:iam::123456789012:role/LambdaFullExecRole
Runtime        : dotnetcore1.0
Timeout        : 3
Version        : $LATEST
VpcConfig      :
```

Contoh 2: Contoh ini mirip dengan yang sebelumnya kecuali binari fungsi pertama kali diunggah ke bucket Amazon S3 (yang harus berada di wilayah yang sama dengan fungsi Lambda yang dimaksud) dan objek S3 yang dihasilkan kemudian direferensikan saat membuat fungsi.

```
Write-S3Object -BucketName mybucket -Key MyFunctionBinaries.zip -File .
  \MyFunctionBinaries.zip
Publish-LMFunction -Description "My C# Lambda Function" `
```

```
-FunctionName MyFunction `
-BucketName mybucket `
-Key MyFunctionBinaries.zip `
-Handler "AssemblyName::Namespace.ClassName::MethodName" `
-Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
-Runtime dotnetcore1.0 `
-Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS Tools for PowerShell Referensi Cmdlet.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def create_function(
        self, function_name, handler_name, iam_role, deployment_package
    ):
        """
        Deploys a Lambda function.

        :param function_name: The name of the Lambda function.
        :param handler_name: The fully qualified name of the handler function.
        This
                               must include the file name and the function name.
        :param iam_role: The IAM role to use for the function.
        :param deployment_package: The deployment package that contains the
        function
                               code in .zip format.
        :return: The Amazon Resource Name (ARN) of the newly created function.
        """
```

```
try:
    response = self.lambda_client.create_function(
        FunctionName=function_name,
        Description="AWS Lambda doc example",
        Runtime="python3.8",
        Role=iam_role.arn,
        Handler=handler_name,
        Code={"ZipFile": deployment_package},
        Publish=True,
    )
    function_arn = response["FunctionArn"]
    waiter = self.lambda_client.get_waiter("function_active_v2")
    waiter.wait(FunctionName=function_name)
    logger.info(
        "Created function '%s' with ARN: '%s'.",
        function_name,
        response["FunctionArn"],
    )
except ClientError:
    logger.error("Couldn't create function %s.", function_name)
    raise
else:
    return function_arn
```

- Untuk API detailnya, lihat [CreateFunction AWS SDK Referensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
```

```

@lambda_client = Aws::Lambda::Client.new
@logger = Logger.new($stdout)
@logger.level = Logger::WARN
end

# Deploys a Lambda function.
#
# @param function_name: The name of the Lambda function.
# @param handler_name: The fully qualified name of the handler function. This
#                       must include the file name and the function name.
# @param role_arn: The IAM role to use for the function.
# @param deployment_package: The deployment package that contains the function
#                             code in .zip format.
# @return: The Amazon Resource Name (ARN) of the newly created function.
def create_function(function_name, handler_name, role_arn, deployment_package)
  response = @lambda_client.create_function({
    role: role_arn.to_s,
    function_name: function_name,
    handler: handler_name,
    runtime: "ruby2.7",
    code: {
      zip_file: deployment_package
    },
    environment: {
      variables: {
        "LOG_LEVEL" => "info"
      }
    }
  })

  @lambda_client.wait_until(:function_active_v2, { function_name:
function_name}) do |w|
    w.max_attempts = 5
    w.delay = 5
  end
  response
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error creating #{function_name}:\n #{e.message}")
rescue Aws::Waiters::Errors::WaiterFailed => e
  @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
end
end

```

- Untuk API detailnya, lihat [CreateFunction](#) di AWS SDK for Ruby API Referensi.

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/**
 * Create a function, uploading from a zip file.
 */
pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
anyhow::Error> {
    let code = self.prepare_function(zip_file, None).await?;

    let key = code.s3_key().unwrap().to_string();

    let role = self.create_role().await.map_err(|e| anyhow!(e))?;

    info!("Created iam role, waiting 15s for it to become active");
    tokio::time::sleep(Duration::from_secs(15)).await;

    info!("Creating lambda function {}", self.lambda_name);
    let _ = self
        .lambda_client
        .create_function()
        .function_name(self.lambda_name.clone())
        .code(code)
        .role(role.arn())
        .runtime(aws_sdk_lambda::types::Runtime::ProvidedAl2)
        .handler("_unused")
        .send()
        .await
        .map_err(anyhow::Error::from)?;

    self.wait_for_function_ready().await?;

    self.lambda_client
        .publish_version()
        .function_name(self.lambda_name.clone())
```

```

        .send()
        .await?;

    Ok(key)
}

/**
 * Upload function code from a path to a zip file.
 * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
 * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
 */
async fn prepare_function(
    &self,
    zip_file: PathBuf,
    key: Option<String>,
) -> Result<FunctionCode, anyhow::Error> {
    let body = ByteStream::from_path(zip_file).await?;

    let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

    info!("Uploading function code to s3://{}/{}", self.bucket, key);
    let _ = self
        .s3_client
        .put_object()
        .bucket(self.bucket.clone())
        .key(key.clone())
        .body(body)
        .send()
        .await?;

    Ok(FunctionCode::builder()
        .s3_bucket(self.bucket.clone())
        .s3_key(key)
        .build())
}

```

- Untuk API detailnya, lihat [CreateFunction AWSSDK](#) untuk API referensi Rust.

SAP ABAP

SDKuntuk SAP ABAP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
TRY.
  lo_lmd->createfunction(
    iv_functionname = iv_function_name
    iv_runtime = `python3.9`
    iv_role = iv_role_arn
    iv_handler = iv_handler
    io_code = io_zip_file
    iv_description = 'AWS Lambda code example'
  ).
  MESSAGE 'Lambda function created.' TYPE 'I'.
CATCH /aws1/cx_lmdcodesigningcfn00.
  MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdcodestorageexcdex.
  MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
CATCH /aws1/cx_lmdcodeverification00.
  MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
CATCH /aws1/cx_lmdinvalidcodesigex.
  MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
CATCH /aws1/cx_lmdinvparamvalueex.
  MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
CATCH /aws1/cx_lmdresourceconflictex.
  MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
CATCH /aws1/cx_lmdresourcenotfoundex.
  MESSAGE 'The requested resource does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdserviceexception.
  MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
CATCH /aws1/cx_lmdtoomanyrequestsex.
  MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
ENDTRY.
```


- Untuk API detailnya, lihat [CreateFunction AWS SDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **DeleteAlias** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteAlias`.

CLI

AWS CLI

Untuk menghapus alias fungsi Lambda

`delete-alias` Contoh berikut menghapus alias bernama LIVE dari fungsi `my-function`.

```
aws lambda delete-alias \  
  --function-name my-function \  
  --name LIVE
```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [DeleteAlias](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menghapus fungsi Lambda Alias yang disebutkan dalam perintah.

```
Remove-LMAlias -FunctionName "MyLambdaFunction123" -Name "NewAlias"
```

- Untuk API detailnya, lihat [DeleteAlias](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **DeleteFunction** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteFunction`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Delete an AWS Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function to
/// delete.</param>
/// <returns>A Boolean value that indicates the success of the action.</
returns>
public async Task<bool> DeleteFunctionAsync(string functionName)
{
    var request = new DeleteFunctionRequest
    {
        FunctionName = functionName,
    };

    var response = await _lambdaService.DeleteFunctionAsync(request);

    // A return value of NoContent means that the request was processed.
    // In this case, the function was deleted, and the return value
```

```
// is intentionally blank.  
return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;  
}
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
Aws::Client::ClientConfiguration clientConfig;  
// Optional: Set to the AWS Region in which the bucket was created  
(overrides config file).  
// clientConfig.region = "us-east-1";  
  
Aws::Lambda::LambdaClient client(clientConfig);  
  
Aws::Lambda::Model::DeleteFunctionRequest request;  
request.SetFunctionName(LAMBDA_NAME);  
  
Aws::Lambda::Model::DeleteFunctionOutcome outcome = client.DeleteFunction(  
    request);  
  
if (outcome.IsSuccess()) {  
    std::cout << "The lambda function was successfully deleted." <<  
std::endl;  
}  
else {  
    std::cerr << "Error with Lambda::DeleteFunction. "  
        << outcome.GetError().GetMessage()  
        << std::endl;  
}
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Contoh 1: Untuk menghapus fungsi Lambda dengan nama fungsi

`delete-function` Contoh berikut menghapus fungsi Lambda `my-function` bernama dengan menentukan nama fungsi.

```
aws lambda delete-function \  
  --function-name my-function
```

Perintah ini tidak menghasilkan output.

Contoh 2: Untuk menghapus fungsi Lambda berdasarkan fungsi ARN

`delete-function` Contoh berikut menghapus fungsi Lambda `my-function` bernama dengan menentukan fungsi. ARN

```
aws lambda delete-function \  
  --function-name arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Perintah ini tidak menghasilkan output.

Contoh 3: Untuk menghapus fungsi Lambda dengan fungsi sebagian ARN

`delete-function` Contoh berikut menghapus fungsi Lambda `my-function` bernama dengan menentukan sebagian fungsi. ARN

```
aws lambda delete-function \  
  --function-name 123456789012:function:my-function
```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [DeleteFunction](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
    LambdaClient *lambda.Client
}

// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(functionName string) {
    _, err := wrapper.LambdaClient.DeleteFunction(context.TODO(),
        &lambda.DeleteFunctionInput{
            FunctionName: aws.String(functionName),
        })
    if err != nil {
        log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
    }
}
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for Go API Referensi.

Java

SDK untuk Java 2.x

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.model.DeleteFunctionRequest;
import software.amazon.awssdk.services.lambda.model.LambdaException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 */
public class DeleteFunction {
    public static void main(String[] args) {
        final String usage = ""

                Usage:
                <functionName>\s

                Where:
                functionName - The name of the Lambda function.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        Region region = Region.US_EAST_1;
```

```

        LambdaClient awsLambda = LambdaClient.builder()
            .region(region)
            .build();

        deleteLambdaFunction(awsLambda, functionName);
        awsLambda.close();
    }

    public static void deleteLambdaFunction(LambdaClient awsLambda, String
functionName) {
        try {
            DeleteFunctionRequest request = DeleteFunctionRequest.builder()
                .functionName(functionName)
                .build();

            awsLambda.deleteFunction(request);
            System.out.println("The " + functionName + " function was deleted");

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}

```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for Java 2.x API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/**
 * @param {string} funcName
 */
const deleteFunction = (funcName) => {

```

```
const client = new LambdaClient({});
const command = new DeleteFunctionCommand({ FunctionName: funcName });
return client.send(command);
};
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for JavaScript API Referensi.

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun dellambdaFunction(myFunctionName: String) {
    val request =
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

- Untuk API detailnya, lihat [DeleteFunction AWS SDK API Referensi Kotlin](#).

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function deleteFunction($functionName)
{
    return $this->lambdaClient->deleteFunction([
        'FunctionName' => $functionName,
    ]);
}
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for PHP API Referensi.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menghapus versi tertentu dari fungsi Lambda

```
Remove-LMFunction -FunctionName "MyLambdaFunction123" -Qualifier '3'
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS Tools for PowerShell Referensi Cmdlet.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def delete_function(self, function_name):
        """
        Deletes a Lambda function.

        :param function_name: The name of the function to delete.
        """
        try:
            self.lambda_client.delete_function(FunctionName=function_name)
        except ClientError:
            logger.exception("Couldn't delete function %s.", function_name)
            raise

```

- Untuk API detailnya, lihat [DeleteFunction AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

```

```
# Deletes a Lambda function.
# @param function_name: The name of the function to delete.
def delete_function(function_name)
  print "Deleting function: #{function_name}..."
  @lambda_client.delete_function(
    function_name: function_name
  )
  print "Done!".green
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
end
```

- Untuk API detailnya, lihat [DeleteFunction](#) di AWS SDK for Ruby API Referensi.

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
pub async fn delete_function(
  &self,
  location: Option<String>,
) -> (
  Result<DeleteFunctionOutput, anyhow::Error>,
  Result<DeleteRoleOutput, anyhow::Error>,
  Option<Result<DeleteObjectOutput, anyhow::Error>>,
) {
  info!("Deleting lambda function {}", self.lambda_name);
  let delete_function = self
    .lambda_client
    .delete_function()
    .function_name(self.lambda_name.clone())
    .send()
    .await
```

```
        .map_err(anyhow::Error::from);

    info!("Deleting iam role {}", self.role_name);
    let delete_role = self
        .iam_client
        .delete_role()
        .role_name(self.role_name.clone())
        .send()
        .await
        .map_err(anyhow::Error::from);

    let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
        if let Some(location) = location {
            info!("Deleting object {location}");
            Some(
                self.s3_client
                    .delete_object()
                    .bucket(self.bucket.clone())
                    .key(location)
                    .send()
                    .await
                    .map_err(anyhow::Error::from),
            )
        } else {
            info!(?location, "Skipping delete object");
            None
        };

    (delete_function, delete_role, delete_object)
}
```

- Untuk API detailnya, lihat [DeleteFunction AWS SDK](#) untuk API referensi Rust.

SAP ABAP

SDK untuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

TRY.
  lo_lmd->deletefunction( iv_functionname = iv_function_name ).
  MESSAGE 'Lambda function deleted.' TYPE 'I'.
CATCH /aws1/cx_lmdinvparamvalueex.
  MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
CATCH /aws1/cx_lmdresourceconflictex.
  MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
CATCH /aws1/cx_lmdresourcenotfoundex.
  MESSAGE 'The requested resource does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdserviceexception.
  MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
CATCH /aws1/cx_lmdtoomanyrequestsex.
  MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
ENDTRY.

```

- Untuk API detailnya, lihat [DeleteFunction AWS SDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **DeleteFunctionConcurrency** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteFunctionConcurrency`.

CLI

AWS CLI

Untuk menghapus batas eksekusi bersamaan yang dicadangkan dari suatu fungsi

`delete-function-concurrency` Contoh berikut menghapus batas eksekusi bersamaan yang dicadangkan dari fungsi `my-function`

```

aws lambda delete-function-concurrency \
  --function-name my-function

```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Reservasi Konkurensi untuk Fungsi Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [DeleteFunctionConcurrency](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menghapus Function Concurrency dari Fungsi Lambda.

```
Remove-LMFunctionConcurrency -FunctionName "MyLambdaFunction123"
```

- Untuk API detailnya, lihat [DeleteFunctionConcurrency](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **DeleteProvisionedConcurrencyConfig** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `DeleteProvisionedConcurrencyConfig`.

CLI

AWS CLI

Untuk menghapus konfigurasi konkurensi yang disediakan

`delete-provisioned-concurrency-config` Contoh berikut menghapus konfigurasi konkurensi yang disediakan untuk GREEN alias fungsi yang ditentukan.

```
aws lambda delete-provisioned-concurrency-config \  
  --function-name my-function \  
  --qualifier GREEN
```

- Untuk API detailnya, lihat [DeleteProvisionedConcurrencyConfig](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menghapus Konfigurasi Konkurensi yang Disediakan untuk Alias tertentu.

```
Remove-LMProvisionedConcurrencyConfig -FunctionName "MyLambdaFunction123" -
Qualifier "NewAlias1"
```

- Untuk API detailnya, lihat [DeleteProvisionedConcurrencyConfig](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetAccountSettings** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetAccountSettings`.

CLI

AWS CLI

Untuk mengambil detail tentang akun Anda di suatu Wilayah AWS

`get-account-settings` Contoh berikut menampilkan batas Lambda dan informasi penggunaan untuk akun Anda.

```
aws lambda get-account-settings
```

Output:

```
{
  "AccountLimit": {
    "CodeSizeUnzipped": 262144000,
    "UnreservedConcurrentExecutions": 1000,
    "ConcurrentExecutions": 1000,
    "CodeSizeZipped": 52428800,
    "TotalCodeSize": 80530636800
  }
}
```

```
    },
    "AccountUsage": {
      "FunctionCount": 4,
      "TotalCodeSize": 9426
    }
  }
}
```

Untuk informasi selengkapnya, lihat [Batas AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [GetAccountSettings](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini ditampilkan untuk membandingkan Batas Akun dan Penggunaan Akun

```
Get-LMAccountSetting | Select-Object
@{Name="TotalCodeSizeLimit";Expression={$_.AccountLimit.TotalCodeSize}},
@{Name="TotalCodeSizeUsed";Expression={$_.AccountUsage.TotalCodeSize}}
```

Output:

```
TotalCodeSizeLimit TotalCodeSizeUsed
-----
            80530636800            15078795
```

- Untuk API detailnya, lihat [GetAccountSettings](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetAlias** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetAlias`.

CLI

AWS CLI

Untuk mengambil rincian tentang alias fungsi

`get-alias` Contoh berikut menampilkan rincian untuk alias bernama LIVE pada fungsi `my-function` Lambda.

```
aws lambda get-alias \  
  --function-name my-function \  
  --name LIVE
```

Output:

```
{  
  "FunctionVersion": "3",  
  "Name": "LIVE",  
  "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-  
function:LIVE",  
  "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",  
  "Description": "alias for live version of function"  
}
```

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [GetAlias](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mengambil bobot Routing Config untuk Alias Fungsi Lambda tertentu.

```
Get-LMAlias -FunctionName "MylambdaFunction123" -Name "newlabel1" -Select  
RoutingConfig
```

Output:

```
AdditionalVersionWeights
```

```
-----  
{[1, 0.6]}
```

- Untuk API detailnya, lihat [GetAlias](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetFunction** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetFunction`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>  
/// Gets information about a Lambda function.  
/// </summary>  
/// <param name="functionName">The name of the Lambda function for  
/// which to retrieve information.</param>  
/// <returns>Async Task.</returns>  
public async Task<FunctionConfiguration> GetFunctionAsync(string  
functionName)  
{  
    var functionRequest = new GetFunctionRequest  
    {  
        FunctionName = functionName,
```

```
};

var response = await _lambdaService.GetFunctionAsync(functionRequest);
return response.Configuration;
}
```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
Aws::Client::ClientConfiguration clientConfig;
// Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
// clientConfig.region = "us-east-1";

Aws::Lambda::LambdaClient client(clientConfig);

Aws::Lambda::Model::GetFunctionRequest request;
request.SetFunctionName(functionName);

Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

if (outcome.IsSuccess()) {
    std::cout << "Function retrieve.\n" <<
outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
    << std::endl;
}
else {
    std::cerr << "Error with Lambda::GetFunction. "
    << outcome.GetError().GetMessage()
```

```
        << std::endl;
    }
```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Untuk mengambil informasi tentang suatu fungsi

`get-function` Contoh berikut menampilkan informasi tentang `my-function` fungsi.

```
aws lambda get-function \
  --function-name my-function
```

Output:

```
{
  "Concurrency": {
    "ReservedConcurrentExecutions": 100
  },
  "Code": {
    "RepositoryType": "S3",
    "Location": "https://awslambda-us-west-2-tasks.s3.us-west-2.amazonaws.com/snapshots/123456789012/my-function..."
  },
  "Configuration": {
    "TracingConfig": {
      "Mode": "PassThrough"
    },
    "Version": "$LATEST",
    "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJm1KidWaaCgk=",
    "FunctionName": "my-function",
    "VpcConfig": {
      "SubnetIds": [],
      "VpcId": "",
      "SecurityGroupIds": []
    },
    "MemorySize": 128,
    "RevisionId": "28f0fb31-5c5c-43d3-8955-03e76c5c1075",
```

```

    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
    "Handler": "index.handler",
    "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qq",
    "Timeout": 3,
    "LastModified": "2019-09-24T18:20:35.054+0000",
    "Runtime": "nodejs10.x",
    "Description": ""
  }
}

```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [GetFunction](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh selengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
  LambdaClient *lambda.Client
}

// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(functionName string) types.State {
  var state types.State
  funcOutput, err := wrapper.LambdaClient.GetFunction(context.TODO(),
    &lambda.GetFunctionInput{

```

```
    FunctionName: aws.String(functionName),
  })
  if err != nil {
    log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
  } else {
    state = funcOutput.Configuration.State
  }
  return state
}
```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for Go API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
const getFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new GetFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for JavaScript API Referensi.

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function getFunction($functionName)
{
    return $this->lambdaClient->getFunction([
        'FunctionName' => $functionName,
    ]);
}
```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for PHP API Referensi.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def get_function(self, function_name):
        """
        Gets data about a Lambda function.
```

```
    :param function_name: The name of the function.
    :return: The function data.
    """
    response = None
    try:
        response =
self.lambda_client.get_function(FunctionName=function_name)
    except ClientError as err:
        if err.response["Error"]["Code"] == "ResourceNotFoundException":
            logger.info("Function %s does not exist.", function_name)
        else:
            logger.error(
                "Couldn't get function %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
    return response
```

- Untuk API detailnya, lihat [GetFunction AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end
end
```



```

# Gets data about a Lambda function.
#
# @param function_name: The name of the function.
# @return response: The function data, or nil if no such function exists.
def get_function(function_name)
  @lambda_client.get_function(
    {
      function_name: function_name
    }
  )
rescue Aws::Lambda::Errors::ResourceNotFoundException => e
  @logger.debug("Could not find function: #{function_name}:\n #{e.message}")
  nil
end

```

- Untuk API detailnya, lihat [GetFunction](#) di AWS SDK for Ruby API Referensi.

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/** Get the Lambda function with this Manager's name. */
pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
  info!("Getting lambda function");
  self.lambda_client
    .get_function()
    .function_name(self.lambda_name.clone())
    .send()
    .await
    .map_err(anyhow::Error::from)
}

```

- Untuk API detailnya, lihat [GetFunction AWSSDK](#) untuk API referensi Rust.

SAP ABAP

SDK untuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
TRY.  
    oo_result = lo_lmd->getfunction( iv_functionname = iv_function_name ).  
    " oo_result is returned for testing purposes. "  
    MESSAGE 'Lambda function information retrieved.' TYPE 'I'.  
CATCH /aws1/cx_lmdinvparamvalueex.  
    MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.  
CATCH /aws1/cx_lmdserviceexception.  
    MESSAGE 'An internal problem was encountered by the AWS Lambda service.'  
TYPE 'E'.  
CATCH /aws1/cx_lmdtoomanyrequestsex.  
    MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.  
ENDTRY.
```

- Untuk API detailnya, lihat [GetFunction AWSSDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetFunctionConcurrency** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetFunctionConcurrency`.

CLI

AWS CLI

Untuk melihat setelan konkurensi cadangan untuk suatu fungsi

`get-function-concurrency` Contoh berikut mengambil pengaturan konkurensi cadangan untuk fungsi yang ditentukan.

```
aws lambda get-function-concurrency \  
  --function-name my-function
```

Output:

```
{  
  "ReservedConcurrentExecutions": 250  
}
```

- Untuk API detailnya, lihat [GetFunctionConcurrency](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mendapatkan konkurensi Cadangan untuk Fungsi Lambda

```
Get-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -Select *
```

Output:

```
ReservedConcurrentExecutions  
-----  
100
```

- Untuk API detailnya, lihat [GetFunctionConcurrency](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetFunctionConfiguration** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetFunctionConfiguration`.

CLI

AWS CLI

Untuk mengambil pengaturan khusus versi dari fungsi Lambda

`get-function-configuration` Contoh berikut menampilkan pengaturan untuk versi 2 dari `my-function` fungsi.

```
aws lambda get-function-configuration \  
  --function-name my-function:2
```

Output:

```
{  
  "FunctionName": "my-function",  
  "LastModified": "2019-09-26T20:28:40.438+0000",  
  "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",  
  "MemorySize": 256,  
  "Version": "2",  
  "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy3l9qyq",  
  "Timeout": 3,  
  "Runtime": "nodejs10.x",  
  "TracingConfig": {  
    "Mode": "PassThrough"  
  },  
  "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmLKidWoaCgk=",  
  "Description": "",  
  "VpcConfig": {  
    "SubnetIds": [],  
    "VpcId": "",  
    "SecurityGroupIds": []  
  },  
  "CodeSize": 304,  
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function:2",  
  "Handler": "index.handler"  
}
```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [GetFunctionConfiguration](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mengembalikan konfigurasi spesifik versi dari Fungsi Lambda.

```
Get-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Qualifier "PowershellAlias"
```

Output:

```
CodeSha256           : uW0W0R7z+f0VyLuUg7+/D08hkMFsq0SF4seuyUZJ/R8=
CodeSize             : 1426
DeadLetterConfig     : Amazon.Lambda.Model.DeadLetterConfig
Description          : Verson 3 to test Aliases
Environment          : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn          : arn:aws:lambda:us-east-1:123456789012:function:MylambdaFunction123
                    : PowershellAlias
FunctionName         : MylambdaFunction123
Handler              : lambda_function.launch_instance
KMSKeyArn            :
LastModified         : 2019-12-25T09:52:59.872+0000
LastUpdateStatus    : Successful
LastUpdateStatusReason :
LastUpdateStatusReasonCode :
Layers               : {}
MasterArn            :
MemorySize           : 128
RevisionId           : 5d7de38b-87f2-4260-8f8a-e87280e10c33
Role                 : arn:aws:iam::123456789012:role/service-role/lambda
Runtime              : python3.8
State                : Active
StateReason          :
StateReasonCode      :
Timeout              : 600
TracingConfig        : Amazon.Lambda.Model.TracingConfigResponse
Version              : 4
```

```
VpcConfig : Amazon.Lambda.Model.VpcConfigDetail
```

- Untuk API detailnya, lihat [GetFunctionConfiguration](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetPolicy** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetPolicy`.

CLI

AWS CLI

Untuk mengambil IAM kebijakan berbasis sumber daya untuk fungsi, versi, atau alias

`get-policy` Contoh berikut menampilkan informasi kebijakan tentang fungsi `my-function` Lambda.

```
aws lambda get-policy \  
  --function-name my-function
```

Output:

```
{  
  "Policy": {  
    "Version": "2012-10-17",  
    "Id": "default",  
    "Statement": [  
      {  
        "Sid": "iot-events",  
        "Effect": "Allow",  
        "Principal": {"Service": "iotevents.amazonaws.com"},  
        "Action": "lambda:InvokeFunction",  
        "Resource": "arn:aws:lambda:us-west-2:123456789012:function:my-  
function"  
      }  
    ]  
  }  
}
```

```
    ],  
    },  
    "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668"  
  }  
}
```

Untuk informasi selengkapnya, lihat [Menggunakan Kebijakan Berbasis Sumber Daya untuk Lambda AWS di Panduan Pengembang Lambda.AWS](#)

- Untuk API detailnya, lihat [GetPolicy](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menampilkan kebijakan Fungsi dari fungsi Lambda

```
Get-LMPolicy -FunctionName test -Select Policy
```

Output:

```
{"Version":"2012-10-17","Id":"default","Statement":  
[{"Sid":"xxxx","Effect":"Allow","Principal":  
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:  
east-1:123456789102:function:test"}]}
```

- Untuk API detailnya, lihat [GetPolicy](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **GetProvisionedConcurrencyConfig** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `GetProvisionedConcurrencyConfig`.

CLI

AWS CLI

Untuk melihat konfigurasi konkurensi yang disediakan

`get-provisioned-concurrency-config` Contoh berikut menampilkan detail untuk konfigurasi konkurensi yang disediakan untuk BLUE alias fungsi yang ditentukan.

```
aws lambda get-provisioned-concurrency-config \
  --function-name my-function \
  --qualifier BLUE
```

Output:

```
{
  "RequestedProvisionedConcurrentExecutions": 100,
  "AvailableProvisionedConcurrentExecutions": 100,
  "AllocatedProvisionedConcurrentExecutions": 100,
  "Status": "READY",
  "LastModified": "2019-12-31T20:28:49+0000"
}
```

- Untuk API detailnya, lihat [GetProvisionedConcurrencyConfig](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mendapatkan Konfigurasi Konkurensi yang disediakan untuk Alias yang ditentukan dari Fungsi Lambda.

```
C:\>Get-LMProvisionedConcurrencyConfig -FunctionName "MyLambdaFunction123" -
Qualifier "NewAlias1"
```

Output:

```
AllocatedProvisionedConcurrentExecutions : 0
AvailableProvisionedConcurrentExecutions : 0
LastModified                             : 2020-01-15T03:21:26+0000
RequestedProvisionedConcurrentExecutions : 70
Status                                    : IN_PROGRESS
StatusReason                              :
```

- Untuk API detailnya, lihat [GetProvisionedConcurrencyConfig](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **Invoke** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `Invoke`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
/// Invoke a Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function to
/// invoke.</param>
/// <param name="parameters">The parameter values that will be passed to the
function.</param>
/// <returns>A System Threading Task.</returns>
public async Task<string> InvokeFunctionAsync(
    string functionName,
    string parameters)
{
    var payload = parameters;
    var request = new InvokeRequest
    {
        FunctionName = functionName,
        Payload = payload,
    };
};
```

```

    var response = await _lambdaService.InvokeAsync(request);
    MemoryStream stream = response.Payload;
    string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
    return returnValue;
}

```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for .NET API Referensi](#).

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

    Aws::Client::ClientConfiguration clientConfig;
    // Optional: Set to the AWS Region in which the bucket was created
    (overrides config file).
    // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::InvokeRequest request;
    request.SetFunctionName(LAMBDA_NAME);
    request.SetLogType(logType);
    std::shared_ptr<Aws::IOStream> payload =
    Aws::MakeShared<Aws::StringStream>(
        "FunctionTest");
    *payload << jsonPayload.View().WriteReadable();
    request.SetBody(payload);
    request.SetContentType("application/json");
    Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

    if (outcome.IsSuccess()) {
        invokeResult = std::move(outcome.GetResult());
    }

```

```
        result = true;
        break;
    }

    else {
        std::cerr << "Error with Lambda::InvokeRequest. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
        break;
    }
}
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for C++ API Referensi](#).

CLI

AWS CLI

Contoh 1: Untuk menjalankan fungsi Lambda secara sinkron

invokeContoh berikut memanggil my-function fungsi sinkron. cli-binary-formatOpsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan Pengguna Antarmuka Baris AWS Perintah.

```
aws lambda invoke \  
  --function-name my-function \  
  --cli-binary-format raw-in-base64-out \  
  --payload '{ "name": "Bob" }' \  
  response.json
```

Output:

```
{  
  "ExecutedVersion": "$LATEST",  
  "StatusCode": 200  
}
```

Untuk informasi selengkapnya, lihat [Pemanggilan Sinkron di Panduan Pengembang Lambda AWS](#).

Contoh 2: Untuk menjalankan fungsi Lambda secara asinkron

invokeContoh berikut memanggil my-function fungsi asinkron. cli-binary-formatOpsi ini diperlukan jika Anda menggunakan AWS CLI versi 2. Untuk informasi selengkapnya, lihat [opsi baris perintah global yang AWS CLI didukung](#) di Panduan Pengguna Antarmuka Baris AWS Perintah.

```
aws lambda invoke \  
  --function-name my-function \  
  --invocation-type Event \  
  --cli-binary-format raw-in-base64-out \  
  --payload '{ "name": "Bob" }' \  
  response.json
```

Output:

```
{  
  "statusCode": 202  
}
```

Untuk informasi selengkapnya, lihat [Pemanggilan Asinkron](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [Memanggil di Referensi AWS CLI Perintah](#).

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
// FunctionWrapper encapsulates function actions used in the examples.  
// It contains an AWS Lambda service client that is used to perform user actions.  
type FunctionWrapper struct {  
  LambdaClient *lambda.Client  
}
```

```
// Invoke invokes the Lambda function specified by functionName, passing the
// parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
// tells
// Lambda to include the last few log lines in the returned result.
func (wrapper FunctionWrapper) Invoke(functionName string, parameters any, getLog
bool) *lambda.InvokeOutput {
    logType := types.LogTypeNone
    if getLog {
        logType = types.LogTypeTail
    }
    payload, err := json.Marshal(parameters)
    if err != nil {
        log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
    }
    invokeOutput, err := wrapper.LambdaClient.Invoke(context.TODO(),
&lambda.InvokeInput{
        FunctionName: aws.String(functionName),
        LogType:      logType,
        Payload:      payload,
    })
    if err != nil {
        log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
    }
    return invokeOutput
}
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for Go API Referensi](#).

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import org.json.JSONObject;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.model.InvokeRequest;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.services.lambda.model.InvokeResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;

public class LambdaInvoke {

    /*
     * Function names appear as
     * arn:aws:lambda:us-west-2:335556666777:function:HelloFunction
     * you can retrieve the value by looking at the function in the AWS Console
     *
     * Also, set up your development environment, including your credentials.
     *
     * For information, see this documentation topic:
     *
     * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.
     * html
     */

    public static void main(String[] args) {
        final String usage = ""

            Usage:
            <functionName>\s

            Where:
            functionName - The name of the Lambda function\s

            """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
```

```
        .region(region)
        .build();

    invokeFunction(awsLambda, functionName);
    awsLambda.close();
}

public static void invokeFunction(LambdaClient awsLambda, String
functionName) {

    InvokeResponse res = null;
    try {
        // Need a SdkBytes instance for the payload.
        JSONObject jsonObj = new JSONObject();
        jsonObj.put("inputValue", "2000");
        String json = jsonObj.toString();
        SdkBytes payload = SdkBytes.fromUtf8String(json);

        // Setup an InvokeRequest.
        InvokeRequest request = InvokeRequest.builder()
            .functionName(functionName)
            .payload(payload)
            .build();

        res = awsLambda.invoke(request);
        String value = res.payload().asUtf8String();
        System.out.println(value);

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for Java 2.x API Referensi](#).

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for JavaScript API Referensi](#).

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun invokeFunction(functionNameVal: String) {
  val json = """"{"inputValue":"1000}""""
  val byteArray = json.trimIndent().encodeToByteArray()
```



```
val request =
    InvokeRequest {
        functionName = functionNameVal
        logType = LogType.Tail
        payload = byteArray
    }

LambdaClient { region = "us-west-2" }.use { awsLambda ->
    val res = awsLambda.invoke(request)
    println("${res.payload?.toString(Charsets.UTF_8)}")
    println("The log result is ${res.logResult}")
}
}
```

- Untuk API detailnya, lihat [Memanggil AWS SDK referensi Kotlin API](#).

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function invoke($functionName, $params, $logType = 'None')
{
    return $this->lambdaClient->invoke([
        'FunctionName' => $functionName,
        'Payload' => json_encode($params),
        'LogType' => $logType,
    ]);
}
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for PHP API Referensi](#).

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def invoke_function(self, function_name, function_params, get_log=False):
        """
        Invokes a Lambda function.

        :param function_name: The name of the function to invoke.
        :param function_params: The parameters of the function as a dict. This
        dict
                               is serialized to JSON before it is sent to
        Lambda.
        :param get_log: When true, the last 4 KB of the execution log are
        included in
                               the response.
        :return: The response from the function invocation.
        """
        try:
            response = self.lambda_client.invoke(
                FunctionName=function_name,
                Payload=json.dumps(function_params),
                LogType="Tail" if get_log else "None",
            )
            logger.info("Invoked function %s.", function_name)
        except ClientError:
            logger.exception("Couldn't invoke function %s.", function_name)
            raise
        return response
```

- Untuk API detailnya, lihat [Memanggil AWS SDK Referensi Python \(APIBoto3\)](#).

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Invokes a Lambda function.
  # @param function_name [String] The name of the function to invoke.
  # @param payload [nil] Payload containing runtime parameters.
  # @return [Object] The response from the function invocation.
  def invoke_function(function_name, payload = nil)
    params = { function_name: function_name }
    params[:payload] = payload unless payload.nil?
    @lambda_client.invoke(params)
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n#{e.message}")
  end
end
```

- Untuk API detailnya, lihat [Memanggil di AWS SDK for Ruby API Referensi](#).

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/** Invoke the lambda function using calculator InvokeArgs. */
pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
anyhow::Error> {
    info!(?args, "Invoking {}", self.lambda_name);
    let payload = serde_json::to_string(&args)?;
    debug!(?payload, "Sending payload");
    self.lambda_client
        .invoke()
        .function_name(self.lambda_name.clone())
        .payload(Blob::new(payload))
        .send()
        .await
        .map_err(anyhow::Error::from)
}

fn log_invoke_output(invoke: &InvokeOutput, message: &str) {
    if let Some(payload) = invoke.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
        info!("Could not extract payload")
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}
```

- Untuk API detailnya, lihat [Memanggil AWS](#) SDKuntuk API referensi Rust.

SAP ABAP

SDKuntuk SAP ABAP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

TRY.
  DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
    `{` &&
    ` "action": "increment",` &&
    ` "number": 10` &&
    `}`
  ).
  oo_result = lo_lmd->invoke(
    " oo_result is returned for
testing purposes. "
    iv_functionname = iv_function_name
    iv_payload = lv_json
  ).
  MESSAGE 'Lambda function invoked.' TYPE 'I'.
CATCH /aws1/cx_lmdinvparamvalueex.
  MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
CATCH /aws1/cx_lmdinvrequestcontex.
  MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
CATCH /aws1/cx_lmdinvalidzipfileex.
  MESSAGE 'The deployment package could not be unzipped.' TYPE 'E'.
CATCH /aws1/cx_lmdrequesttoolargeex.
  MESSAGE 'Invoke request body JSON input limit was exceeded by the request
payload.' TYPE 'E'.
CATCH /aws1/cx_lmdresourceconflictex.
  MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
CATCH /aws1/cx_lmdresourcenotfoundex.
  MESSAGE 'The requested resource does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdserviceexception.
  MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
CATCH /aws1/cx_lmdtoomanyrequestsex.
  MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.

```

```
CATCH /aws1/cx_lmdunsuppedmediatyp00.  
    MESSAGE 'Invoke request body does not have JSON as its content type.'  
TYPE 'E'.  
ENDTRY.
```

- Untuk API detailnya, lihat [Memanggil AWS SDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **ListFunctions** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListFunctions`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>  
/// Get a list of Lambda functions.  
/// </summary>  
/// <returns>A list of FunctionConfiguration objects.</returns>  
public async Task<List<FunctionConfiguration>> ListFunctionsAsync()  
{  
    var functionList = new List<FunctionConfiguration>();  
  
    var functionPaginator =
```

```
        _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
    await foreach (var function in functionPaginator.Functions)
    {
        functionList.Add(function);
    }

    return functionList;
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
Aws::Client::ClientConfiguration clientConfig;
// Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
// clientConfig.region = "us-east-1";

Aws::Lambda::LambdaClient client(clientConfig);

std::vector<Aws::String> functions;
Aws::String marker;

do {
    Aws::Lambda::Model::ListFunctionsRequest request;
    if (!marker.empty()) {
        request.SetMarker(marker);
    }

    Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
        request);
```

```

    if (outcome.IsSuccess()) {
        const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
        std::cout << result.GetFunctions().size()
            << " lambda functions were retrieved." << std::endl;

        for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
            functions.push_back(functionConfiguration.GetFunctionName());
            std::cout << functions.size() << " "
                << functionConfiguration.GetDescription() << std::endl;
            std::cout << " "
                <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                functionConfiguration.GetRuntime()) << ": "
                << functionConfiguration.GetHandler()
                << std::endl;
        }
        marker = result.GetNextMarker();
    }
    else {
        std::cerr << "Error with Lambda::ListFunctions. "
            << outcome.GetError().GetMessage()
            << std::endl;
    }
} while (!marker.empty());

```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Untuk mengambil daftar fungsi Lambda

`list-functions` Contoh berikut menampilkan daftar semua fungsi untuk pengguna saat ini.

```
aws lambda list-functions
```

Output:

```
{
```



```
"Functions": [
  {
    "TracingConfig": {
      "Mode": "PassThrough"
    },
    "Version": "$LATEST",
    "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbl/RMr0fT/I=",
    "FunctionName": "helloworld",
    "MemorySize": 128,
    "RevisionId": "1718e831-badf-4253-9518-d0644210af7b",
    "CodeSize": 294,
    "FunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:helloworld",
    "Handler": "helloworld.handler",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-
role-zgur6bf4",
    "Timeout": 3,
    "LastModified": "2023-09-23T18:32:33.857+0000",
    "Runtime": "nodejs18.x",
    "Description": ""
  },
  {
    "TracingConfig": {
      "Mode": "PassThrough"
    },
    "Version": "$LATEST",
    "CodeSha256": "sU0cJ2/h0ZevwV/1TxCuQqK3gDZP3i8gUoqUUVRmY6E=",
    "FunctionName": "my-function",
    "VpcConfig": {
      "SubnetIds": [],
      "VpcId": "",
      "SecurityGroupIds": []
    },
    "MemorySize": 256,
    "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
    "CodeSize": 266,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
    "Handler": "index.handler",
    "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy319qqq",
    "Timeout": 3,
    "LastModified": "2023-10-01T16:47:28.490+0000",
    "Runtime": "nodejs18.x",
```

```

        "Description": ""
    },
    {
        "Layers": [
            {
                "CodeSize": 41784542,
                "Arn": "arn:aws:lambda:us-
west-2:420165488524:layer:AWSLambda-Python37-SciPy1x:2"
            },
            {
                "CodeSize": 4121,
                "Arn": "arn:aws:lambda:us-
west-2:123456789012:layer:pythonLayer:1"
            }
        ],
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "$LATEST",
        "CodeSha256": "ZQukCqxtkqFgyF2cU41Avj99TKQ/hNihPtDtRcc08mI=",
        "FunctionName": "my-python-function",
        "VpcConfig": {
            "SubnetIds": [],
            "VpcId": "",
            "SecurityGroupIds": []
        },
        "MemorySize": 128,
        "RevisionId": "80b4eabc-acf7-4ea8-919a-e874c213707d",
        "CodeSize": 299,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
python-function",
        "Handler": "lambda_function.lambda_handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/my-python-
function-role-z5g7dr6n",
        "Timeout": 3,
        "LastModified": "2023-10-01T19:40:41.643+0000",
        "Runtime": "python3.11",
        "Description": ""
    }
]
}

```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [ListFunctions](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh selengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
    LambdaClient *lambda.Client
}

// ListFunctions lists up to maxItems functions for the account. This function
// uses a
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(maxItems int)
[]types.FunctionConfiguration {
    var functions []types.FunctionConfiguration
    paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
    &lambda.ListFunctionsInput{
        MaxItems: aws.Int32(int32(maxItems)),
    })
    for paginator.HasMorePages() && len(functions) < maxItems {
        pageOutput, err := paginator.NextPage(context.TODO())
        if err != nil {
            log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
        }
        functions = append(functions, pageOutput.Functions...)
    }
    return functions
}
```

```
}
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Go API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
const listFunctions = () => {  
  const client = new LambdaClient({});  
  const command = new ListFunctionsCommand({});  
  
  return client.send(command);  
};
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for JavaScript API Referensi.

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function listFunctions($maxItems = 50, $marker = null)  
{
```

```

    if (is_null($marker)) {
        return $this->lambdaClient->listFunctions([
            'MaxItems' => $maxItems,
        ]);
    }

    return $this->lambdaClient->listFunctions([
        'Marker' => $marker,
        'MaxItems' => $maxItems,
    ]);
}

```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for PHP API Referensi.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menampilkan semua fungsi Lambda dengan ukuran kode yang diurutkan

```

Get-LMFunctionList | Sort-Object -Property CodeSize | Select-Object FunctionName,
    RunTime, Timeout, CodeSize

```

Output:

| FunctionName CodeSize | Runtime | Timeout |
|----------------------------|-----------|---------|
| ----- ----- | ----- | ----- |
| test 243 | python2.7 | 3 |
| MylambdaFunction123 659 | python3.8 | 600 |
| myfuncpython1 675 | python3.8 | 303 |

- Untuk API detailnya, lihat [ListFunctions](#) di AWS Tools for PowerShell Referensi Cmdlet.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def list_functions(self):
        """
        Lists the Lambda functions for the current account.
        """
        try:
            func_paginator = self.lambda_client.get_paginator("list_functions")
            for func_page in func_paginator.paginate():
                for func in func_page["Functions"]:
                    print(func["FunctionName"])
                    desc = func.get("Description")
                    if desc:
                        print(f"\t{desc}")
                        print(f"\t{func['Runtime']}: {func['Handler']}")
        except ClientError as err:
            logger.error(
                "Couldn't list functions. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- Untuk API detailnya, lihat [ListFunctions AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Lists the Lambda functions for the current account.
  def list_functions
    functions = []
    @lambda_client.list_functions.each do |response|
      response["functions"].each do |function|
        functions.append(function["function_name"])
      end
    end
    functions
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n#{e.message}")
  end
end
```

- Untuk API detailnya, lihat [ListFunctions](#) di AWS SDK for Ruby API Referensi.

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/** List all Lambda functions in the current Region. */
pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
    info!("Listing lambda functions");
    self.lambda_client
        .list_functions()
        .send()
        .await
        .map_err(anyhow::Error::from)
}
```

- Untuk API detailnya, lihat [ListFunctions AWS SDKuntuk API referensi Rust](#).

SAP ABAP

SDKuntuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
TRY.
    oo_result = lo_lmd->listfunctions( ).      " oo_result is returned for
testing purposes. "
    DATA(lt_functions) = oo_result->get_functions( ).
    MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
CATCH /aws1/cx_lmdinvparamvalueex.
```



```

    MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
  CATCH /aws1/cx_lmdserviceexception.
    MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
  TYPE 'E'.
  CATCH /aws1/cx_lmdtoomanyrequestsex.
    MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
  ENDTRY.

```

- Untuk API detailnya, lihat [ListFunctions AWS SDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **ListProvisionedConcurrencyConfigs** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListProvisionedConcurrencyConfigs`.

CLI

AWS CLI

Untuk mendapatkan daftar konfigurasi konkurensi yang disediakan

`list-provisioned-concurrency-configs` Contoh berikut mencantumkan konfigurasi konkurensi yang disediakan untuk fungsi yang ditentukan.

```

aws lambda list-provisioned-concurrency-configs \
  --function-name my-function

```

Output:

```

{
  "ProvisionedConcurrencyConfigs": [
    {
      "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:GREEN",
      "RequestedProvisionedConcurrentExecutions": 100,
      "AvailableProvisionedConcurrentExecutions": 100,
      "AllocatedProvisionedConcurrentExecutions": 100,
    }
  ]
}

```

```

        "Status": "READY",
        "LastModified": "2019-12-31T20:29:00+0000"
    },
    {
        "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:BLUE",
        "RequestedProvisionedConcurrentExecutions": 100,
        "AvailableProvisionedConcurrentExecutions": 100,
        "AllocatedProvisionedConcurrentExecutions": 100,
        "Status": "READY",
        "LastModified": "2019-12-31T20:28:49+0000"
    }
]
}

```

- Untuk API detailnya, lihat [ListProvisionedConcurrencyConfigs](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mengambil daftar konfigurasi konkurensi yang disediakan untuk fungsi Lambda.

```
Get-LMProvisionedConcurrencyConfigList -FunctionName "MyLambdaFunction123"
```

- Untuk API detailnya, lihat [ListProvisionedConcurrencyConfigs](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **ListTags** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListTags`.

CLI

AWS CLI

Untuk mengambil daftar tag untuk fungsi Lambda

`list-tags` Contoh berikut menampilkan tag yang dilampirkan ke fungsi `my-function` Lambda.

```
aws lambda list-tags \  
  --resource arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Output:

```
{  
  "Tags": {  
    "Category": "Web Tools",  
    "Department": "Sales"  
  }  
}
```

Untuk informasi selengkapnya, lihat [Menandai Fungsi Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [ListTags](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Mengambil tag dan nilainya saat ini ditetapkan pada fungsi yang ditentukan.

```
Get-LMResourceTag -Resource "arn:aws:lambda:us-  
west-2:123456789012:function:MyFunction"
```

Output:

| Key | Value |
|------------|------------|
| --- | ----- |
| California | Sacramento |
| Oregon | Salem |

Washington Olympia

- Untuk API detailnya, lihat [ListTags](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **ListVersionsByFunction** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `ListVersionsByFunction`.

CLI

AWS CLI

Untuk mengambil daftar versi fungsi

`list-versions-by-function` Contoh berikut menampilkan daftar versi untuk fungsi `my-function` Lambda.

```
aws lambda list-versions-by-function \  
--function-name my-function
```

Output:

```
{  
  "Versions": [  
    {  
      "TracingConfig": {  
        "Mode": "PassThrough"  
      },  
      "Version": "$LATEST",  
      "CodeSha256": "sU0cJ2/h0ZevwV/1TxCuQqK3gDZP3i8gUoqUUVRmY6E=",  
      "FunctionName": "my-function",  
      "VpcConfig": {  
        "SubnetIds": [],  
        "VpcId": "",  
        "SecurityGroupIds": []  
      },  
      "MemorySize": 256,  
      "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
```

```

        "CodeSize": 266,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:$LATEST",
        "Handler": "index.handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qq",
        "Timeout": 3,
        "LastModified": "2019-10-01T16:47:28.490+0000",
        "Runtime": "nodejs10.x",
        "Description": ""
    },
    {
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "1",
        "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
        "FunctionName": "my-function",
        "VpcConfig": {
            "SubnetIds": [],
            "VpcId": "",
            "SecurityGroupIds": []
        },
        "MemorySize": 256,
        "RevisionId": "949c8914-012e-4795-998c-e467121951b1",
        "CodeSize": 304,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:1",
        "Handler": "index.handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qq",
        "Timeout": 3,
        "LastModified": "2019-09-26T20:28:40.438+0000",
        "Runtime": "nodejs10.x",
        "Description": "new version"
    },
    {
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "2",
        "CodeSha256": "sU0cJ2/h0ZevwV/1TxCuQqK3gDZP3i8gUoqUUVRmY6E=",
        "FunctionName": "my-function",
        "VpcConfig": {

```

```

        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "MemorySize": 256,
    "RevisionId": "cd669f21-0f3d-4e1c-9566-948837f2e2ea",
    "CodeSize": 266,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
    "Handler": "index.handler",
    "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9yq",
    "Timeout": 3,
    "LastModified": "2019-10-01T16:47:28.490+0000",
    "Runtime": "nodejs10.x",
    "Description": "newer version"
    }
]
}

```

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [ListVersionsByFunction](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini mengembalikan daftar konfigurasi spesifik versi untuk setiap versi Fungsi Lambda.

```
Get-LMVersionsByFunction -FunctionName "MylambdaFunction123"
```

Output:

| FunctionName RoleName | Runtime | MemorySize | Timeout | CodeSize | LastModified |
|--------------------------|-----------|------------|---------|----------|------------------------------|
| MylambdaFunction123 | python3.8 | 128 | 600 | 659 | 2020-01-10T03:20:56.390+0000 |
| | lambda | | | | |

```

MyLambdaFunction123 python3.8      128      5      1426
2019-12-25T09:19:02.238+0000 lambda
MyLambdaFunction123 python3.8      128      5      1426
2019-12-25T09:39:36.779+0000 lambda
MyLambdaFunction123 python3.8      128      600     1426
2019-12-25T09:52:59.872+0000 lambda

```

- Untuk API detailnya, lihat [ListVersionsByFunction](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **PublishVersion** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `PublishVersion`.

CLI

AWS CLI

Untuk mempublikasikan versi baru dari suatu fungsi

`publish-version` Contoh berikut menerbitkan versi baru dari fungsi `my-function` Lambda.

```

aws lambda publish-version \
  --function-name my-function

```

Output:

```

{
  "TracingConfig": {
    "Mode": "PassThrough"
  },
  "CodeSha256": "dBG9m8SGdm1Ejw/JYX1hhvCrAv5TxvXsbL/RM1r0fT/I=",
  "FunctionName": "my-function",
  "CodeSize": 294,
  "RevisionId": "f31d3d39-cc63-4520-97d4-43cd44c94c20",
  "MemorySize": 128,
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:3",

```

```
"Version": "2",
"Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-zgur6bf4",
"Timeout": 3,
"LastModified": "2019-09-23T18:32:33.857+0000",
"Handler": "my-function.handler",
"Runtime": "nodejs10.x",
"Description": ""
}
```

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [PublishVersion](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini membuat versi untuk snapshot Kode Fungsi Lambda yang ada

```
Publish-LMVersion -FunctionName "MylambdaFunction123" -Description "Publishing Existing Snapshot of function code as a new version through Powershell"
```

- Untuk API detailnya, lihat [PublishVersion](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **PutFunctionConcurrency** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `PutFunctionConcurrency`.

CLI

AWS CLI

Untuk mengonfigurasi batas konkurensi cadangan untuk suatu fungsi

`put-function-concurrency` Contoh berikut mengonfigurasi 100 eksekusi bersamaan yang dicadangkan untuk fungsi tersebut. `my-function`


```
aws lambda put-function-concurrency \  
  --function-name my-function \  
  --reserved-concurrent-executions 100
```

Output:

```
{  
  "ReservedConcurrentExecutions": 100  
}
```

Untuk informasi selengkapnya, lihat [Reservasi Konkurensi untuk Fungsi Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [PutFunctionConcurrency](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menerapkan pengaturan konkurensi untuk Fungsi secara keseluruhan.

```
Write-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -  
ReservedConcurrentExecution 100
```

- Untuk API detailnya, lihat [PutFunctionConcurrency](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **PutProvisionedConcurrencyConfig** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `PutProvisionedConcurrencyConfig`.

CLI

AWS CLI

Untuk mengalokasikan konkurensi yang disediakan

put-provisioned-concurrency-config Contoh berikut mengalokasikan 100 konkurensi yang disediakan untuk BLUE alias fungsi yang ditentukan.

```
aws lambda put-provisioned-concurrency-config \  
  --function-name my-function \  
  --qualifier BLUE \  
  --provisioned-concurrent-executions 100
```

Output:

```
{  
  "Requested ProvisionedConcurrentExecutions": 100,  
  "Allocated ProvisionedConcurrentExecutions": 0,  
  "Status": "IN_PROGRESS",  
  "LastModified": "2019-11-21T19:32:12+0000"  
}
```

- Untuk API detailnya, lihat [PutProvisionedConcurrencyConfig](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menambahkan konfigurasi konkurensi yang disediakan ke Alias Fungsi

```
Write-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -  
ProvisionedConcurrentExecution 20 -Qualifier "NewAlias1"
```

- Untuk API detailnya, lihat [PutProvisionedConcurrencyConfig](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **RemovePermission** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `RemovePermission`.

CLI

AWS CLI

Untuk menghapus izin dari fungsi Lambda yang ada

`remove-permission` Contoh berikut menghapus izin untuk memanggil fungsi bernama `my-function`.

```
aws lambda remove-permission \  
  --function-name my-function \  
  --statement-id sns
```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Menggunakan Kebijakan Berbasis Sumber Daya untuk Lambda AWS di Panduan Pengembang Lambda.AWS](#)

- Untuk API detailnya, lihat [RemovePermission](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini menghapus kebijakan fungsi untuk yang ditentukan `StatementId` dari Fungsi Lambda.

```
$policy = Get-LMPolicy -FunctionName "MylambdaFunction123" -Select Policy |  
  ConvertFrom-Json | Select-Object -ExpandProperty Statement  
Remove-LMPermission -FunctionName "MylambdaFunction123" -StatementId  
  $policy[0].Sid
```

- Untuk API detailnya, lihat [RemovePermission](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **TagResource** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `TagResource`.

CLI

AWS CLI

Untuk menambahkan tag ke fungsi Lambda yang ada

tag-resource Contoh berikut menambahkan tag dengan nama kunci `DEPARTMENT` dan nilai `Department A` untuk fungsi Lambda tertentu.

```
aws lambda tag-resource \  
  --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \  
  --tags "DEPARTMENT=Department A"
```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Menandai Fungsi Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [TagResource](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Menambahkan tiga tag (Washington, Oregon dan California) dan nilai terkaitnya ARN ke fungsi tertentu yang diidentifikasi olehnya.

```
Add-LMResourceTag -Resource "arn:aws:lambda:us-  
west-2:123456789012:function:MyFunction" -Tag @{ "Washington" = "Olympia";  
  "Oregon" = "Salem"; "California" = "Sacramento" }
```

- Untuk API detailnya, lihat [TagResource](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **UntagResource** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `UntagResource`.

CLI

AWS CLI

Untuk menghapus tag dari fungsi Lambda yang ada

`untag-resource` Contoh berikut menghapus tag dengan DEPARTMENT tag nama kunci dari fungsi `my-function` Lambda.

```
aws lambda untag-resource \  
  --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \  
  --tag-keys DEPARTMENT
```

Perintah ini tidak menghasilkan output.

Untuk informasi selengkapnya, lihat [Menandai Fungsi Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [UntagResource](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Menghapus tag yang disediakan dari fungsi. Cmdlet akan meminta konfirmasi sebelum melanjutkan kecuali sakelar `-Force` ditentukan. Satu panggilan dilakukan ke layanan untuk menghapus tag.

```
Remove-LMResourceTag -Resource "arn:aws:lambda:us-  
west-2:123456789012:function:MyFunction" -TagKey  
  "Washington","Oregon","California"
```

Contoh 2: Menghapus tag yang disediakan dari fungsi. Cmdlet akan meminta konfirmasi sebelum melanjutkan kecuali sakelar `-Force` ditentukan. Setelah panggilan ke layanan dilakukan per tag yang disediakan.

```
"Washington","Oregon","California" | Remove-LMResourceTag -Resource
"arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
```

- Untuk API detailnya, lihat [UntagResource](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **UpdateAlias** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `UpdateAlias`.

CLI

AWS CLI

Untuk memperbarui alias fungsi

`update-alias` Contoh berikut memperbarui alias bernama LIVE untuk menunjuk ke versi 3 dari fungsi `my-function` Lambda.

```
aws lambda update-alias \
  --function-name my-function \
  --function-version 3 \
  --name LIVE
```

Output:

```
{
  "FunctionVersion": "3",
  "Name": "LIVE",
  "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
  "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",
  "Description": "alias for live version of function"
}
```

Untuk informasi selengkapnya, lihat [Mengonfigurasi Alias Fungsi AWS Lambda](#) di Panduan Pengembang AWS Lambda.

- Untuk API detailnya, lihat [UpdateAlias](#) di Referensi AWS CLI Perintah.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini memperbarui Konfigurasi Alias fungsi Lambda yang ada. Ini memperbarui RoutingConfiguration nilai untuk menggeser 60% (0,6) lalu lintas ke versi 1

```
Update-LMAlias -FunctionName "MyLambdaFunction123" -Description  
" Alias for version 2" -FunctionVersion 2 -Name "newlabel1" -  
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6"}
```

- Untuk API detailnya, lihat [UpdateAlias](#) di AWS Tools for PowerShell Referensi Cmdlet.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **UpdateFunctionCode** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan UpdateFunctionCode.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>
```

```

    /// Update an existing Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to update.</
param>
    /// <param name="bucketName">The bucket where the zip file containing
    /// the Lambda function code is stored.</param>
    /// <param name="key">The key name of the source code file.</param>
    /// <returns>Async Task.</returns>
    public async Task UpdateFunctionCodeAsync(
        string functionName,
        string bucketName,
        string key)
    {
        var functionCodeRequest = new UpdateFunctionCodeRequest
        {
            FunctionName = functionName,
            Publish = true,
            S3Bucket = bucketName,
            S3Key = key,
        };

        var response = await
_lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
        Console.WriteLine($"The Function was last modified at
{response.LastModified}.");
    }

```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
Aws::Client::ClientConfiguration clientConfig;
```



```
    // Optional: Set to the AWS Region in which the bucket was created
    (overrides config file).
    // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::UpdateFunctionCodeRequest request;
    request.SetFunctionName(LAMBDA_NAME);
    std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
                          std::ios_base::in | std::ios_base::binary);
    if (!ifstream.is_open()) {
        std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
std::endl;
}

#ifdef USE_CPP_LAMBDA_FUNCTION
    std::cerr
        << "The cpp Lambda function must be built following the
instructions in the cpp_lambda/README.md file. "
        << std::endl;
#endif

    deleteLambdaFunction(client);
    deleteIamRole(clientConfig);
    return false;
}

    Aws::StringStream buffer;
    buffer << ifstream.rdbuf();
    request.SetZipFile(
        Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                               buffer.str().length()));

    request.SetPublish(true);

    Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
client.UpdateFunctionCode(
    request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda code was successfully updated." <<
std::endl;
    }
    else {
        std::cerr << "Error with Lambda::UpdateFunctionCode. "
        << outcome.GetError().GetMessage()
        << std::endl;
    }
}
```

```
}
```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Untuk memperbarui kode fungsi Lambda

update-function-code Contoh berikut menggantikan kode versi my-function fungsi yang tidak dipublikasikan (\$LATEST) dengan isi file zip yang ditentukan.

```
aws lambda update-function-code \  
  --function-name my-function \  
  --zip-file fileb://my-function.zip
```

Output:

```
{  
  "FunctionName": "my-function",  
  "LastModified": "2019-09-26T20:28:40.438+0000",  
  "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",  
  "MemorySize": 256,  
  "Version": "$LATEST",  
  "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy3l9qqq",  
  "Timeout": 3,  
  "Runtime": "nodejs10.x",  
  "TracingConfig": {  
    "Mode": "PassThrough"  
  },  
  "CodeSha256": "5tT2qgzYUHaqWR716pZ2dpkn/0J1FrzJm1KidWoaCgk=",  
  "Description": "",  
  "VpcConfig": {  
    "SubnetIds": [],  
    "VpcId": "",  
    "SecurityGroupIds": []  
  },  
  "CodeSize": 304,  
  "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
```

```
"Handler": "index.handler"
}
```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh selengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
    LambdaClient *lambda.Client
}

// UpdateFunctionCode updates the code for the Lambda function specified by
// functionName.
// The existing code for the Lambda function is entirely replaced by the code in
// the
// zipPackage buffer. After the update action is called, a
// lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(functionName string, zipPackage
*bytes.Buffer) types.State {
    var state types.State
    _, err := wrapper.LambdaClient.UpdateFunctionCode(context.TODO(),
&lambda.UpdateFunctionCodeInput{
    FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
})
    if err != nil {
```

```

log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
functionName, err)
} else {
waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
funcOutput, err := waiter.WaitForOutput(context.TODO(),
&lambda.GetFunctionInput{
FunctionName: aws.String(functionName)}, 1*time.Minute)
if err != nil {
log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
functionName, err)
} else {
state = funcOutput.Configuration.State
}
}
return state
}

```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for Go API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

const updateFunctionCode = async (funcName, newFunc) => {
const client = new LambdaClient({});
const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
const command = new UpdateFunctionCodeCommand({
ZipFile: code,
FunctionName: funcName,
Architectures: [Architecture.arm64],
Handler: "index.handler", // Required when sending a .zip file
PackageType: PackageType.Zip, // Required when sending a .zip file
Runtime: Runtime.nodejs16x, // Required when sending a .zip file
});

```

```
return client.send(command);
};
```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for JavaScript API Referensi.

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function updateFunctionCode($functionName, $s3Bucket, $s3Key)
{
    return $this->lambdaClient->updateFunctionCode([
        'FunctionName' => $functionName,
        'S3Bucket' => $s3Bucket,
        'S3Key' => $s3Key,
    ]);
}
```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for PHP API Referensi.

PowerShell

Alat untuk PowerShell

Contoh 1: Memperbarui fungsi bernama 'MyFunction' dengan konten baru yang terkandung dalam file zip yang ditentukan. Untuk C#.NET Fungsi Core Lambda file zip harus berisi rakitan yang dikompilasi.

```
Update-LMFunctionCode -FunctionName MyFunction -ZipFilename .\UpdatedCode.zip
```

Contoh 2: Contoh ini mirip dengan yang sebelumnya tetapi menggunakan objek Amazon S3 yang berisi kode yang diperbarui untuk memperbarui fungsi.

```
Update-LMFunctionCode -FunctionName MyFunction -BucketName mybucket -Key
UpdatedCode.zip
```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS Tools for PowerShell Referensi Cmdlet.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def update_function_code(self, function_name, deployment_package):
        """
        Updates the code for a Lambda function by submitting a .zip archive that
        contains
        the code for the function.

        :param function_name: The name of the function to update.
        :param deployment_package: The function code to update, packaged as bytes
        in
                               .zip format.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_code(
                FunctionName=function_name, ZipFile=deployment_package
            )
```

```
except ClientError as err:
    logger.error(
        "Couldn't update function %s. Here's why: %s: %s",
        function_name,
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
else:
    return response
```

- Untuk API detailnya, lihat [UpdateFunctionCode AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the code for a Lambda function by submitting a .zip archive that
  # contains
  # the code for the function.

  # @param function_name: The name of the function to update.
  # @param deployment_package: The function code to update, packaged as bytes in
  #                               .zip format.
  # @return: Data about the update, including the status.
```

```

def update_function_code(function_name, deployment_package)
  @lambda_client.update_function_code(
    function_name: function_name,
    zip_file: deployment_package
  )
  @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
    w.max_attempts = 5
    w.delay = 5
  end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating function code for:
#{function_name}:\n #{e.message}")
    nil
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
  end
end

```

- Untuk API detailnya, lihat [UpdateFunctionCode](#) di AWS SDK for Ruby API Referensi.

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/** Given a Path to a zip file, update the function's code and wait for the
update to finish. */
pub async fn update_function_code(
  &self,
  zip_file: PathBuf,
  key: String,
) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
  let function_code = self.prepare_function(zip_file, Some(key)).await?;

  info!("Updating code for {}", self.lambda_name);

```



```

    let update = self
        .lambda_client
        .update_function_code()
        .function_name(self.lambda_name.clone())
        .s3_bucket(self.bucket.clone())
        .s3_key(function_code.s3_key().unwrap().to_string())
        .send()
        .await
        .map_err( anyhow::Error::from );

    self.wait_for_function_ready().await?;

    Ok(update)
}

/**
 * Upload function code from a path to a zip file.
 * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
 * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
 */
async fn prepare_function(
    &self,
    zip_file: PathBuf,
    key: Option<String>,
) -> Result<FunctionCode, anyhow::Error> {
    let body = ByteStream::from_path(zip_file).await?;

    let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

    info!("Uploading function code to s3://{}/{}", self.bucket, key);
    let _ = self
        .s3_client
        .put_object()
        .bucket(self.bucket.clone())
        .key(key.clone())
        .body(body)
        .send()
        .await?;

    Ok(FunctionCode::builder()
        .s3_bucket(self.bucket.clone())
        .s3_key(key)
        .build())
}

```

```
}

```

- Untuk API detailnya, lihat [UpdateFunctionCode AWSSDK](#) untuk API referensi Rust.

SAP ABAP

SDK untuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
TRY.
    oo_result = lo_lmd->updatefunctioncode( " oo_result is returned for
testing purposes. "
        iv_functionname = iv_function_name
        iv_zipfile = io_zip_file
    ).

    MESSAGE 'Lambda function code updated.' TYPE 'I'.
CATCH /aws1/cx_lmdcodesigningcfgno00.
    MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdcodestorageexcdex.
    MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
CATCH /aws1/cx_lmdcodeverification00.
    MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
CATCH /aws1/cx_lmdinvalidcodesigex.
    MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
CATCH /aws1/cx_lmdinvparamvalueex.
    MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
CATCH /aws1/cx_lmdresourceconflictex.
    MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
CATCH /aws1/cx_lmdresourcenotfoundex.
    MESSAGE 'The requested resource does not exist.' TYPE 'E'.
CATCH /aws1/cx_lmdserviceexception.
    MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.

```

```
CATCH /aws1/cx_lmdtoomanyrequestsex.  
    MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.  
ENDTRY.
```

- Untuk API detailnya, lihat [UpdateFunctionCode AWSSDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan **UpdateFunctionConfiguration** dengan AWS SDK atau CLI

Contoh kode berikut menunjukkan cara menggunakan `UpdateFunctionConfiguration`.

Contoh tindakan adalah kutipan kode dari program yang lebih besar dan harus dijalankan dalam konteks. Anda dapat melihat tindakan ini dalam konteks dalam contoh kode berikut:

- [Memulai dengan fungsi](#)

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/// <summary>  
/// Update the code of a Lambda function.  
/// </summary>  
/// <param name="functionName">The name of the function to update.</param>  
/// <param name="functionHandler">The code that performs the function's  
actions.</param>  
/// <param name="environmentVariables">A dictionary of environment  
variables.</param>  
/// <returns>A Boolean value indicating the success of the action.</returns>  
public async Task<bool> UpdateFunctionConfigurationAsync(  

```

```

    string functionName,
    string functionHandler,
    Dictionary<string, string> environmentVariables)
    {
        var request = new UpdateFunctionConfigurationRequest
        {
            Handler = functionHandler,
            FunctionName = functionName,
            Environment = new Amazon.Lambda.Model.Environment { Variables =
environmentVariables },
        };

        var response = await
_lambdaService.UpdateFunctionConfigurationAsync(request);

        Console.WriteLine(response.LastModified);

        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for .NET API Referensi.

C++

SDK untuk C++

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

    Aws::Client::ClientConfiguration clientConfig;
    // Optional: Set to the AWS Region in which the bucket was created
    (overrides config file).
    // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;

```

```

request.SetFunctionName(LAMBDA_NAME);
Aws::Lambda::Model::Environment environment;
environment.AddVariables("LOG_LEVEL", "DEBUG");
request.SetEnvironment(environment);

Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
client.UpdateFunctionConfiguration(
    request);

if (outcome.IsSuccess()) {
    std::cout << "The lambda configuration was successfully updated."
              << std::endl;
    break;
}

else {
    std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
              << outcome.GetError().GetMessage()
              << std::endl;
}

```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for C++ API Referensi.

CLI

AWS CLI

Untuk memodifikasi konfigurasi suatu fungsi

update-function-configuration Contoh berikut memodifikasi ukuran memori menjadi 256 MB untuk versi fungsi yang tidak dipublikasikan (\$LATEST). my-function

```

aws lambda update-function-configuration \
  --function-name my-function \
  --memory-size 256

```

Output:

```

{
  "FunctionName": "my-function",
  "LastModified": "2019-09-26T20:28:40.438+0000",

```

```

    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-uy319qq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
      "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJm1KidWoaCgk=",
    "Description": "",
    "VpcConfig": {
      "SubnetIds": [],
      "VpcId": "",
      "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
  }

```

Untuk informasi selengkapnya, lihat [Konfigurasi Fungsi AWS Lambda di Panduan Pengembang AWS Lambda](#).

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di Referensi AWS CLI Perintah.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
  LambdaClient *lambda.Client

```

```

}

// UpdateFunctionConfiguration updates a map of environment variables configured
// for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(functionName string,
    envVars map[string]string) {
    _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(context.TODO(),
        &lambda.UpdateFunctionConfigurationInput{
            FunctionName: aws.String(functionName),
            Environment: &types.Environment{Variables: envVars},
        })
    if err != nil {
        log.Panicf("Couldn't update configuration for %v. Here's why: %v",
            functionName, err)
    }
}
}

```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for Go API Referensi.

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

const updateFunctionConfiguration = (funcName) => {
    const client = new LambdaClient({});
    const config = readFileSync(`${dirname}../functions/config.json`).toString();
    const command = new UpdateFunctionConfigurationCommand({
        ...JSON.parse(config),
        FunctionName: funcName,
    });
    return client.send(command);
}

```

```
};
```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for JavaScript API Referensi.

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
public function updateFunctionConfiguration($functionName, $handler,
$environment = '')
{
    return $this->lambdaClient->updateFunctionConfiguration([
        'FunctionName' => $functionName,
        'Handler' => "$handler.lambda_handler",
        'Environment' => $environment,
    ]);
}
```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for PHP API Referensi.

PowerShell

Alat untuk PowerShell

Contoh 1: Contoh ini memperbarui Konfigurasi Fungsi Lambda yang ada

```
Update-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Handler
"lambda_function.launch_instance" -Timeout 600 -Environment_Variable
@{ "envvar1"="value";"envvar2"="value" } -Role arn:aws:iam::123456789101:role/
service-role/lambda -DeadLetterConfig_TargetArn arn:aws:sns:us-east-1:
123456789101:MyfirstTopic
```


- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS Tools for PowerShell Referensi Cmdlet.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    def update_function_configuration(self, function_name, env_vars):
        """
        Updates the environment variables for a Lambda function.

        :param function_name: The name of the function to update.
        :param env_vars: A dict of environment variables to update.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_configuration(
                FunctionName=function_name, Environment={"Variables": env_vars}
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function configuration %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration AWSSDKReferensi Python \(Boto3\)](#). API

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the environment variables for a Lambda function.
  # @param function_name: The name of the function to update.
  # @param log_level: The log level of the function.
  # @return: Data about the update, including the status.
  def update_function_configuration(function_name, log_level)
    @lambda_client.update_function_configuration({
      function_name: function_name,
      environment: {
        variables: {
          "LOG_LEVEL" => log_level
        }
      }
    })

    @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
      w.max_attempts = 5
    end
  end
end
```

```

    w.delay = 5
  end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
end

```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration](#) di AWS SDK for Ruby API Referensi.

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

/** Update the environment for a function. */
pub async fn update_function_configuration(
    &self,
    environment: Environment,
) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
    info!(
        ?environment,
        "Updating environment for {}", self.lambda_name
    );
    let updated = self
        .lambda_client
        .update_function_configuration()
        .function_name(self.lambda_name.clone())
        .environment(environment)
        .send()
        .await
        .map_err(anyhow::Error::from)?;

    self.wait_for_function_ready().await?;
}

```

```
    Ok(updated)
  }
```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration AWSSDK](#) untuk API referensi Rust.

SAP ABAP

SDK untuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
TRY.
    oo_result = lo_lmd->updatefunctionconfiguration(      " oo_result is
returned for testing purposes. "
        iv_functionname = iv_function_name
        iv_runtime       = iv_runtime
        iv_description   = 'Updated Lambda function'
        iv_memorysize   = iv_memory_size
    ).

    MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
    CATCH /aws1/cx_lmdcodesigningcfn00.
    MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
    CATCH /aws1/cx_lmdcodeverification00.
    MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
    CATCH /aws1/cx_lmdinvalidcodesigex.
    MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
    CATCH /aws1/cx_lmdinvparamvalueex.
    MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_lmdresourceconflictex.
    MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
    CATCH /aws1/cx_lmdresourcenotfoundex.
    MESSAGE 'The requested resource does not exist.' TYPE 'E'.
    CATCH /aws1/cx_lmdserviceexception.
```

```
MESSAGE 'An internal problem was encountered by the AWS Lambda service.'  
TYPE 'E'.  
CATCH /aws1/cx_lmdtoomanyrequestsex.  
MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.  
ENDTRY.
```

- Untuk API detailnya, lihat [UpdateFunctionConfiguration AWSSDK](#) untuk SAP ABAP API referensi.

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Skenario untuk Lambda menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menerapkan skenario umum di Lambda dengan AWS SDKs. Skenario ini menunjukkan kepada Anda cara menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam Lambda atau dikombinasikan dengan yang lain. AWS layanan Setiap skenario menyertakan tautan ke kode sumber lengkap, di mana Anda dapat menemukan instruksi tentang cara mengatur dan menjalankan kode.

Skenario menargetkan tingkat pengalaman menengah untuk membantu Anda memahami tindakan layanan dalam konteks.

Contoh

- [Secara otomatis mengonfirmasi pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK](#)
- [Secara otomatis memigrasikan pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK](#)
- [Buat API Gateway REST API untuk melacak data COVID -19](#)
- [Buat perpustakaan pinjaman REST API](#)
- [Membuat aplikasi messenger dengan Step Functions](#)
- [Membuat aplikasi manajemen aset foto yang memungkinkan pengguna mengelola foto menggunakan label](#)
- [Buat aplikasi obrolan websocket dengan API Gateway](#)
- [Buat aplikasi yang menganalisis umpan balik pelanggan dan mensintesis audio](#)

- [Mulai membuat dan menjalankan fungsi Lambda menggunakan AWS SDK](#)
- [Menginvokasi fungsi Lambda dari browser](#)
- [Transformasi data untuk aplikasi Anda dengan S3 Object Lambda](#)
- [Gunakan API Gateway untuk menjalankan fungsi Lambda](#)
- [Menggunakan Step Functions untuk menginvokasi fungsi Lambda](#)
- [Menggunakan peristiwa terjadwal untuk menginvokasi fungsi Lambda](#)
- [Menulis data aktivitas kustom dengan fungsi Lambda setelah otentikasi pengguna Amazon Cognito menggunakan AWS SDK](#)

Secara otomatis mengonfirmasi pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK

Contoh kode berikut menunjukkan cara mengonfirmasi pengguna Amazon Cognito yang diketahui secara otomatis dengan fungsi Lambda.

- Konfigurasi kumpulan pengguna untuk memanggil fungsi Lambda untuk PreSignUp pemicunya.
- Daftarkan pengguna dengan Amazon Cognito.
- Fungsi Lambda memindai tabel DynamoDB dan secara otomatis mengonfirmasi pengguna yang dikenal.
- Masuk sebagai pengguna baru, lalu bersihkan sumber daya.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Jalankan skenario interaktif di pengunggah/prompt perintah.

```
// AutoConfirm separates the steps of this scenario into individual functions so
// that
// they are simpler to read and understand.
type AutoConfirm struct {
    helper      IScenarioHelper
    questioner  demotools.IQuestioner
    resources   Resources
    cognitoActor *actions.CognitoActions
}

// NewAutoConfirm constructs a new auto confirm runner.
func NewAutoConfirm(sdkConfig aws.Config, questioner demotools.IQuestioner,
    helper IScenarioHelper) AutoConfirm {
    scenario := AutoConfirm{
        helper:      helper,
        questioner:  questioner,
        resources:   Resources{},
        cognitoActor: &actions.CognitoActions{CognitoClient:
    cognitoidentityprovider.NewFromConfig(sdkConfig)},
    }
    scenario.resources.init(scenario.cognitoActor, questioner)
    return scenario
}

// AddPreSignUpTrigger adds a Lambda handler as an invocation target for the
// PreSignUp trigger.
func (runner *AutoConfirm) AddPreSignUpTrigger(userPoolId string, functionArn
    string) {
    log.Printf("Let's add a Lambda function to handle the PreSignUp trigger from
    Cognito.\n" +
        "This trigger happens when a user signs up, and lets your function take action
    before the main Cognito\n" +
        "sign up processing occurs.\n")
    err := runner.cognitoActor.UpdateTriggers(
        userPoolId,
        actions.TriggerInfo{Trigger: actions.PreSignUp, HandlerArn:
    aws.String(functionArn)})
    if err != nil {
        panic(err)
    }
    log.Printf("Lambda function %v added to user pool %v to handle the PreSignUp
    trigger.\n",
        functionArn, userPoolId)
}
```

```

// SignUpUser signs up a user from the known user table with a password you
// specify.
func (runner *AutoConfirm) SignUpUser(clientId string, usersTable string)
(string, string) {
log.Println("Let's sign up a user to your Cognito user pool. When the user's
email matches an email in the\n" +
"DynamoDB known users table, it is automatically verified and the user is
confirmed.")

knownUsers, err := runner.helper.GetKnownUsers(usersTable)
if err != nil {
panic(err)
}
userChoice := runner.questioner.AskChoice("Which user do you want to use?\n",
knownUsers.UserNameList())
user := knownUsers.Users[userChoice]

var signedUp bool
var userConfirmed bool
password := runner.questioner.AskPassword("Enter a password that has at least
eight characters, uppercase, lowercase, numbers and symbols.\n"+
"(the password will not display as you type):", 8)
for !signedUp {
log.Printf("Signing up user '%v' with email '%v' to Cognito.\n", user.UserName,
user.UserEmail)
userConfirmed, err = runner.cognitoActor.SignUp(clientId, user.UserName,
password, user.UserEmail)
if err != nil {
var invalidPassword *types.InvalidPasswordException
if errors.As(err, &invalidPassword) {
password = runner.questioner.AskPassword("Enter another password:", 8)
} else {
panic(err)
}
} else {
signedUp = true
}
}
log.Printf("User %v signed up, confirmed = %v.\n", user.UserName, userConfirmed)

log.Println(strings.Repeat("-", 88))

return user.UserName, password

```



```
}

// SignInUser signs in a user.
func (runner *AutoConfirm) SignInUser(clientId string, userName string, password
string) string {
runner.questioner.Ask("Press Enter when you're ready to continue.")
log.Printf("Let's sign in as %v...\n", userName)
authResult, err := runner.cognitoActor.SignIn(clientId, userName, password)
if err != nil {
panic(err)
}
log.Printf("Successfully signed in. Your access token starts with: %v...\n",
(*authResult.AccessToken)[:10])
log.Println(strings.Repeat("-", 88))
return *authResult.AccessToken
}

// Run runs the scenario.
func (runner *AutoConfirm) Run(stackName string) {
defer func() {
if r := recover(); r != nil {
log.Println("Something went wrong with the demo.")
runner.resources.Cleanup()
}
}()

log.Println(strings.Repeat("-", 88))
log.Printf("Welcome\n")

log.Println(strings.Repeat("-", 88))

stackOutputs, err := runner.helper.GetStackOutputs(stackName)
if err != nil {
panic(err)
}
runner.resources.userPoolId = stackOutputs["UserPoolId"]
runner.helper.PopulateUserTable(stackOutputs["TableName"])

runner.AddPreSignUpTrigger(stackOutputs["UserPoolId"],
stackOutputs["AutoConfirmFunctionArn"])
runner.resources.triggers = append(runner.resources.triggers, actions.PreSignUp)
userName, password := runner.SignUpUser(stackOutputs["UserPoolClientId"],
stackOutputs["TableName"])
runner.helper.ListRecentLogEvents(stackOutputs["AutoConfirmFunction"])
```

```

runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
runner.SignInUser(stackOutputs["UserPoolClientId"], userName, password))

runner.resources.Cleanup()

log.Println(strings.Repeat("-", 88))
log.Println("Thanks for watching!")
log.Println(strings.Repeat("-", 88))
}

```

Tangani PreSignUp pelatuk dengan fungsi Lambda.

```

const TABLE_NAME = "TABLE_NAME"

// UserInfo defines structured user data that can be marshalled to a DynamoDB
// format.
type UserInfo struct {
    UserName string `dynamodbav:"UserName"`
    UserEmail string `dynamodbav:"UserEmail"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
    userEmail, err := attributevalue.Marshal(user.UserEmail)
    if err != nil {
        panic(err)
    }
    return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
    dynamoClient *dynamodb.Client
}

// HandleRequest handles the PreSignUp event by looking up a user in an Amazon
// DynamoDB table and
// specifying whether they should be confirmed and verified.
func (h *handler) HandleRequest(ctx context.Context, event
events.CognitoEventUserPoolsPreSignup) (events.CognitoEventUserPoolsPreSignup,
error) {

```

```
log.Printf("Received presignup from %v for user '%v'", event.TriggerSource,
event.UserName)
if event.TriggerSource != "PreSignUp_SignUp" {
    // Other trigger sources, such as PreSignUp_AdminInitiateAuth, ignore the
    response from this handler.
    return event, nil
}
tableName := os.Getenv(TABLE_NAME)
user := UserInfo{
    UserEmail: event.Request.UserAttributes["email"],
}
log.Printf("Looking up email %v in table %v.\n", user.UserEmail, tableName)
output, err := h.dynamoClient.GetItem(ctx, &dynamodb.GetItemInput{
    Key:      user.GetKey(),
    TableName: aws.String(tableName),
})
if err != nil {
    log.Printf("Error looking up email %v.\n", user.UserEmail)
    return event, err
}
if output.Item == nil {
    log.Printf("Email %v not found. Email verification is required.\n",
user.UserEmail)
    return event, err
}

err = attributevalue.UnmarshalMap(output.Item, &user)
if err != nil {
    log.Printf("Couldn't unmarshal DynamoDB item. Here's why: %v\n", err)
    return event, err
}

if user.UserName != event.UserName {
    log.Printf("UserEmail %v found, but stored UserName '%v' does not match
supplied UserName '%v'. Verification is required.\n",
    user.UserEmail, user.UserName, event.UserName)
} else {
    log.Printf("UserEmail %v found with matching UserName %v. User is confirmed.
\n", user.UserEmail, user.UserName)
    event.Response.AutoConfirmUser = true
    event.Response.AutoVerifyEmail = true
}

return event, err
```

```

}

func main() {
    sdkConfig, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        log.Panicln(err)
    }
    h := handler{
        dynamoClient: dynamodb.NewFromConfig(sdkConfig),
    }
    lambda.Start(h.HandleRequest)
}

```

Buat struct yang melakukan tugas-tugas umum.

```

// IScenarioHelper defines common functions used by the workflows in this
// example.
type IScenarioHelper interface {
    Pause(secs int)
    GetStackOutputs(stackName string) (actions.StackOutputs, error)
    PopulateUserTable(tableName string)
    GetKnownUsers(tableName string) (actions.UserList, error)
    AddKnownUser(tableName string, user actions.User)
    ListRecentLogEvents(functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
// example.
type ScenarioHelper struct {
    questioner demotools.IQuestioner
    dynamoActor *actions.DynamoActions
    cfnActor *actions.CloudFormationActions
    cwActor *actions.CloudWatchLogsActions
    isTestRun bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
    ScenarioHelper {
    scenario := ScenarioHelper{

```

```

    questioner: questioner,
    dynamoActor: &actions.DynamoActions{DynamoClient:
dynamodb.NewFromConfig(sdkConfig)},
    cfnActor: &actions.CloudFormationActions{CfnClient:
cloudformation.NewFromConfig(sdkConfig)},
    cwlActor: &actions.CloudWatchLogsActions{CwlClient:
cloudwatchlogs.NewFromConfig(sdkConfig)},
}
return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
    if !helper.isTestRun {
        time.Sleep(time.Duration(secs) * time.Second)
    }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
(actions.StackOutputs, error) {
    return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
    log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
this example.\n", tableName)
    err := helper.dynamoActor.PopulateTable(tableName)
    if err != nil {
        panic(err)
    }
}

// GetKnownUsers gets the users from the known users table in a structured
format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
error) {
    knownUsers, err := helper.dynamoActor.Scan(tableName)
    if err != nil {
        log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
tableName, err)
    }
}

```

```
    return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
    log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
table...\n",
        user.UserName, user.UserEmail)
    err := helper.dynamoActor.AddUser(tableName, user)
    if err != nil {
        panic(err)
    }
}

// ListRecentLogEvents gets the most recent log stream and events for the
specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
    log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
    helper.Pause(10)
    log.Println("Okay, let's check the logs to find what's happened recently with
your Lambda function.")
    logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
    if err != nil {
        panic(err)
    }
    log.Printf("Getting some recent events from log stream %v\n",
        *logStream.LogStreamName)
    events, err := helper.cwlActor.GetLogEvents(functionName,
        *logStream.LogStreamName, 10)
    if err != nil {
        panic(err)
    }
    for _, event := range events {
        log.Printf("\t%v", *event.Message)
    }
    log.Println(strings.Repeat("-", 88))
}
```

Buat struct yang membungkus tindakan Amazon Cognito.

```
type CognitoActions struct {
    CognitoClient *cognitoidentityprovider.Client
}

// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
// trigger.
type Trigger int

const (
    PreSignUp Trigger = iota
    UserMigration
    PostAuthentication
)

type TriggerInfo struct {
    Trigger    Trigger
    HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
// is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
    triggers ...TriggerInfo) error {
    output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
        &cognitoidentityprovider.DescribeUserPoolInput{
            UserPoolId: aws.String(userPoolId),
        })
    if err != nil {
        log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
            userPoolId, err)
        return err
    }
    lambdaConfig := output.UserPool.LambdaConfig
    for _, trigger := range triggers {
        switch trigger.Trigger {
        case PreSignUp:
            lambdaConfig.PreSignUp = trigger.HandlerArn
        case UserMigration:
            lambdaConfig.UserMigration = trigger.HandlerArn
        case PostAuthentication:
```

```
    lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
}
_, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
&cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:  aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
})
if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
}
return err
}

// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(clientId string, userName string, password
string, userEmail string) (bool, error) {
  confirmed := false
  output, err := actor.CognitoClient.SignUp(context.TODO(),
&cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
    {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
})
if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
    log.Println(*invalidPassword.Message)
  } else {
    log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
} else {
  confirmed = output.UserConfirmed
}
return confirmed, err
}
```



```
// SignIn signs in a user to Amazon Cognito using a username and password
authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
string) (*types.AuthenticationResultType, error) {
    var authResult *types.AuthenticationResultType
    output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
    &cognitoidentityprovider.InitiateAuthInput{
        AuthFlow:      "USER_PASSWORD_AUTH",
        ClientId:      aws.String(clientId),
        AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
    })
    if err != nil {
        var resetRequired *types.PasswordResetRequiredException
        if errors.As(err, &resetRequired) {
            log.Println(*resetRequired.Message)
        } else {
            log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
        }
    } else {
        authResult = output.AuthenticationResult
    }
    return authResult, err
}

// ForgotPassword starts a password recovery flow for a user. This flow typically
sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
(*types.CodeDeliveryDetailsType, error) {
    output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
    &cognitoidentityprovider.ForgotPasswordInput{
        ClientId: aws.String(clientId),
        Username: aws.String(userName),
    })
    if err != nil {
        log.Printf("Couldn't start password reset for user '%v'. Here's why: %v\n",
        userName, err)
    }
    return output.CodeDeliveryDetails, err
}
```

```
// ConfirmForgotPassword confirms a user with a confirmation code and a new
password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
  userName string, password string) error {
  _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
    &cognitoidentityprovider.ConfirmForgotPasswordInput{
      ClientId:      aws.String(clientId),
      ConfirmationCode: aws.String(code),
      Password:      aws.String(password),
      Username:      aws.String(userName),
    })
  if err != nil {
    var invalidPassword *types.InvalidPasswordException
    if errors.As(err, &invalidPassword) {
      log.Println(*invalidPassword.Message)
    } else {
      log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
    }
  }
  return err
}

// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
  _, err := actor.CognitoClient.DeleteUser(context.TODO(),
    &cognitoidentityprovider.DeleteUserInput{
      AccessToken: aws.String(userAccessToken),
    })
  if err != nil {
    log.Printf("Couldn't delete user. Here's why: %v\n", err)
  }
  return err
}

// AdminCreateUser uses administrator credentials to add a user to a user pool.
This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
  userEmail string) error {
```

```

_, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
&cognitoidentityprovider.AdminCreateUserInput{
    UserPoolId:    aws.String(userPoolId),
    Username:      aws.String(userName),
    MessageAction: types.MessageActionTypeSuppress,
    UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
aws.String(userEmail)}}},
})
if err != nil {
    var userExists *types.UsernameExistsException
    if errors.As(err, &userExists) {
        log.Printf("User %v already exists in the user pool.", userName)
        err = nil
    } else {
        log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
    }
}
return err
}

// AdminSetUserPassword uses administrator credentials to set a password for a
// user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
string, password string) error {
_, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
&cognitoidentityprovider.AdminSetUserPasswordInput{
    Password:    aws.String(password),
    UserPoolId: aws.String(userPoolId),
    Username:    aws.String(userName),
    Permanent:   true,
})
if err != nil {
    var invalidPassword *types.InvalidPasswordException
    if errors.As(err, &invalidPassword) {
        log.Println(*invalidPassword.Message)
    } else {
        log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
err)
    }
}
return err
}

```

```
}
```

Buat struct yang membungkus tindakan DynamoDB.

```
// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
// actions
// used in the examples.
type DynamoActions struct {
    DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
    UserName string
    UserEmail string
    LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
    UserPoolId string
    ClientId string
    Time string
}

// UserList defines a list of users.
type UserList struct {
    Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
// strings.
func (users *UserList) UserNameList() []string {
    names := make([]string, len(users.Users))
    for i := 0; i < len(users.Users); i++ {
        names[i] = users.Users[i].UserName
    }
    return names
}
```

```
// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
    var err error
    var item map[string]types.AttributeValue
    var writeReqs []types.WriteRequest
    for i := 1; i < 4; i++ {
        item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
        %v", i), userEmail: fmt.Sprintf("test_email_%v@example.com", i)})
        if err != nil {
            log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
            err)
            return err
        }
        writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
        &types.PutRequest{Item: item}})
    }
    _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
    &dynamodb.BatchWriteItemInput{
        RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
    })
    if err != nil {
        log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
        tableName, err)
    }
    return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
    var userList UserList
    output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
        err)
    } else {
        err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
        if err != nil {
            log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
        }
    }
    return userList, err
}
```

```
// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
    userItem, err := attributevalue.MarshalMap(user)
    if err != nil {
        log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
    }
    _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
        Item:      userItem,
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
    }
    return err
}
```

Buat struct yang membungkus tindakan CloudWatch Log.

```
type CloudWatchLogsActions struct {
    CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
(types.LogStream, error) {
    var logStream types.LogStream
    logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
    output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
&cloudwatchlogs.DescribeLogStreamsInput{
    Descending:  aws.Bool(true),
    Limit:       aws.Int32(1),
    LogGroupName: aws.String(logGroupName),
    OrderBy:    types.OrderByLastEventTime,
})
    if err != nil {
        log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
logGroupName, err)
    } else {
        logStream = output.LogStreams[0]
    }
}
```

```

    }
    return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
// stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
logStreamName string, eventCount int32) (
[]types.OutputLogEvent, error) {
var events []types.OutputLogEvent
logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
output, err := actor.CwlClient.GetLogEvents(context.TODO(),
&cloudwatchlogs.GetLogEventsInput{
    LogStreamName: aws.String(logStreamName),
    Limit:         aws.Int32(eventCount),
    LogGroupName:  aws.String(logGroupName),
})
if err != nil {
    log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
logStreamName, err)
} else {
    events = output.Events
}
return events, err
}

```

Buat struct yang membungkus tindakan AWS CloudFormation .

```

// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
    CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
// structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
output, err := actor.CfnClient.DescribeStacks(context.TODO(),
&cloudformation.DescribeStacksInput{

```

```

    StackName: aws.String(stackName),
  })
  if err != nil || len(output.Stacks) == 0 {
    log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
      stackName, err)
  }
  stackOutputs := StackOutputs{}
  for _, out := range output.Stacks[0].Outputs {
    stackOutputs[*out.OutputKey] = *out.OutputValue
  }
  return stackOutputs
}

```

Pembersihan sumber daya

```

// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
  userPoolId      string
  userAccessTokens []string
  triggers        []actions.Trigger

  cognitoActor *actions.CognitoActions
  questioner   demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
  demotools.IQuestioner) {
  resources.userAccessTokens = []string{}
  resources.triggers = []actions.Trigger{}
  resources.cognitoActor = cognitoActor
  resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
  defer func() {
    if r := recover(); r != nil {
      log.Printf("Something went wrong during cleanup.\n%v\n", r)
    }
  }()
}

```



```
    log.Println("Use the AWS Management Console to remove any remaining resources\n" +\n        "that were created for this scenario.")\n    }\n    }()\n\n    wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS\n    resources that were created "+\n        "during this demo (y/n)?", "y")\n    if wantDelete {\n        for _, accessToken := range resources.userAccessTokens {\n            err := resources.cognitoActor.DeleteUser(accessToken)\n            if err != nil {\n                log.Println("Couldn't delete user during cleanup.")\n                panic(err)\n            }\n            log.Println("Deleted user.")\n        }\n        triggerList := make([]actions.TriggerInfo, len(resources.triggers))\n        for i := 0; i < len(resources.triggers); i++ {\n            triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],\n            HandlerArn: nil}\n        }\n        err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,\n        triggerList...)\n        if err != nil {\n            log.Println("Couldn't update Cognito triggers during cleanup.")\n            panic(err)\n        }\n        log.Println("Removed Cognito triggers from user pool.")\n    } else {\n        log.Println("Be sure to remove resources when you're done with them to avoid\n        unexpected charges!")\n    }\n}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Go API Referensi.
 - [DeleteUser](#)
 - [InitiateAuth](#)
 - [SignUp](#)

- [UpdateUserPool](#)

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Secara otomatis memigrasikan pengguna Amazon Cognito yang dikenal dengan fungsi Lambda menggunakan AWS SDK

Contoh kode berikut menunjukkan cara memigrasi pengguna Amazon Cognito yang dikenal secara otomatis dengan fungsi Lambda.

- Konfigurasi kumpulan pengguna untuk memanggil fungsi Lambda untuk `MigrateUser` pemicunya.
- Masuk ke Amazon Cognito dengan nama pengguna dan email yang tidak ada di kumpulan pengguna.
- Fungsi Lambda memindai tabel DynamoDB dan secara otomatis memigrasikan pengguna yang dikenal ke kumpulan pengguna.
- Lakukan alur lupa kata sandi untuk mengatur ulang kata sandi untuk pengguna yang dimigrasi.
- Masuk sebagai pengguna baru, lalu bersihkan sumber daya.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

Jalankan skenario interaktif di pengunggah/prompt perintah.

```
import (  
  "errors"  
  "fmt"
```

```
"log"
"strings"
"user_pools_and_lambda_triggers/actions"

"github.com/aws/aws-sdk-go-v2/aws"
"github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
"github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
"github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// MigrateUser separates the steps of this scenario into individual functions so
// that
// they are simpler to read and understand.
type MigrateUser struct {
    helper      IScenarioHelper
    questioner  demotools.IQuestioner
    resources   Resources
    cognitoActor *actions.CognitoActions
}

// NewMigrateUser constructs a new migrate user runner.
func NewMigrateUser(sdkConfig aws.Config, questioner demotools.IQuestioner,
    helper IScenarioHelper) MigrateUser {
    scenario := MigrateUser{
        helper:      helper,
        questioner:  questioner,
        resources:   Resources{},
        cognitoActor: &actions.CognitoActions{CognitoClient:
            cognitoidentityprovider.NewFromConfig(sdkConfig)},
    }
    scenario.resources.init(scenario.cognitoActor, questioner)
    return scenario
}

// AddMigrateUserTrigger adds a Lambda handler as an invocation target for the
// MigrateUser trigger.
func (runner *MigrateUser) AddMigrateUserTrigger(userPoolId string, functionArn
    string) {
    log.Printf("Let's add a Lambda function to handle the MigrateUser trigger from
        Cognito.\n" +
        "This trigger happens when an unknown user signs in, and lets your function
        take action before Cognito\n" +
        "rejects the user.\n\n")
    err := runner.cognitoActor.UpdateTriggers(
```

```

    userPoolId,
    actions.TriggerInfo{Trigger: actions.UserMigration, HandlerArn:
aws.String(functionArn)}}
if err != nil {
    panic(err)
}
log.Printf("Lambda function %v added to user pool %v to handle the MigrateUser
trigger.\n",
    functionArn, userPoolId)

log.Println(strings.Repeat("-", 88))
}

// SignInUser adds a new user to the known users table and signs that user in to
Amazon Cognito.
func (runner *MigrateUser) SignInUser(usersTable string, clientId string) (bool,
actions.User) {
log.Println("Let's sign in a user to your Cognito user pool. When the username
and email matches an entry in the\n" +
    "DynamoDB known users table, the email is automatically verified and the user
is migrated to the Cognito user pool.")

user := actions.User{}
user.UserName = runner.questioner.Ask("\nEnter a username:")
user.UserEmail = runner.questioner.Ask("\nEnter an email that you own. This
email will be used to confirm user migration\n" +
    "during this example:")

runner.helper.AddKnownUser(usersTable, user)

var err error
var resetRequired *types.PasswordResetRequiredException
var authResult *types.AuthenticationResultType
signedIn := false
for !signedIn && resetRequired == nil {
    log.Printf("Signing in to Cognito as user '%v'. The expected result is a
PasswordResetRequiredException.\n\n", user.UserName)
    authResult, err = runner.cognitoActor.SignIn(clientId, user.UserName, "_")
    if err != nil {
        if errors.As(err, &resetRequired) {
            log.Printf("\nUser '%v' is not in the Cognito user pool but was found in the
DynamoDB known users table.\n"+
                "User migration is started and a password reset is required.",
                user.UserName)

```

```

    } else {
        panic(err)
    }
} else {
    log.Printf("User '%v' successfully signed in. This is unexpected and probably
means you have not\n"+
        "cleaned up a previous run of this scenario, so the user exist in the Cognito
user pool.\n"+
        "You can continue this example and select to clean up resources, or manually
remove\n"+
        "the user from your user pool and try again.", user.UserName)
    runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
*authResult.AccessToken)
    signedIn = true
}
}

log.Println(strings.Repeat("-", 88))
return resetRequired != nil, user
}

// ResetPassword starts a password recovery flow.
func (runner *MigrateUser) ResetPassword(clientId string, user actions.User) {
    wantCode := runner.questioner.AskBool(fmt.Sprintf("In order to migrate the user
to Cognito, you must be able to receive a confirmation\n"+
        "code by email at %v. Do you want to send a code (y/n)?", user.UserEmail), "y")
    if !wantCode {
        log.Println("To complete this example and successfully migrate a user to
Cognito, you must enter an email\n" +
            "you own that can receive a confirmation code.")
        return
    }
    codeDelivery, err := runner.cognitoActor.ForgotPassword(clientId, user.UserName)
    if err != nil {
        panic(err)
    }
    log.Printf("\nA confirmation code has been sent to %v.",
*codeDelivery.Destination)
    code := runner.questioner.Ask("Check your email and enter it here:")

    confirmed := false
    password := runner.questioner.AskPassword("\nEnter a password that has at least
eight characters, uppercase, lowercase, numbers and symbols.\n"+
        "(the password will not display as you type):", 8)

```

```

for !confirmed {
    log.Printf("\nConfirming password reset for user '%v'.\n", user.UserName)
    err = runner.cognitoActor.ConfirmForgotPassword(clientId, code, user.UserName,
password)
    if err != nil {
        var invalidPassword *types.InvalidPasswordException
        if errors.As(err, &invalidPassword) {
            password = runner.questioner.AskPassword("\nEnter another password:", 8)
        } else {
            panic(err)
        }
    } else {
        confirmed = true
    }
}
log.Printf("User '%v' successfully confirmed and migrated.\n", user.UserName)
log.Println("Signing in with your username and password...")
authResult, err := runner.cognitoActor.SignIn(clientId, user.UserName, password)
if err != nil {
    panic(err)
}
log.Printf("Successfully signed in. Your access token starts with: %v...\n",
(*authResult.AccessToken)[:10])
runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
*authResult.AccessToken)

log.Println(strings.Repeat("-", 88))
}

// Run runs the scenario.
func (runner *MigrateUser) Run(stackName string) {
    defer func() {
        if r := recover(); r != nil {
            log.Println("Something went wrong with the demo.")
            runner.resources.Cleanup()
        }
    }()

    log.Println(strings.Repeat("-", 88))
    log.Printf("Welcome\n")

    log.Println(strings.Repeat("-", 88))

    stackOutputs, err := runner.helper.GetStackOutputs(stackName)

```

```

if err != nil {
    panic(err)
}
runner.resources.userPoolId = stackOutputs["UserPoolId"]

runner.AddMigrateUserTrigger(stackOutputs["UserPoolId"],
stackOutputs["MigrateUserFunctionArn"])
runner.resources.triggers = append(runner.resources.triggers,
actions.UserMigration)
resetNeeded, user := runner.SignInUser(stackOutputs["TableName"],
stackOutputs["UserPoolClientId"])
if resetNeeded {
    runner.helper.ListRecentLogEvents(stackOutputs["MigrateUserFunction"])
    runner.ResetPassword(stackOutputs["UserPoolClientId"], user)
}

runner.resources.Cleanup()

log.Println(strings.Repeat("-", 88))
log.Println("Thanks for watching!")
log.Println(strings.Repeat("-", 88))
}

```

Tangani MigrateUser pelatuk dengan fungsi Lambda.

```

const TABLE_NAME = "TABLE_NAME"

// UserInfo defines structured user data that can be marshalled to a DynamoDB
format.
type UserInfo struct {
    UserName string `dynamodbav:"UserName"`
    UserEmail string `dynamodbav:"UserEmail"`
}

type handler struct {
    dynamoClient *dynamodb.Client
}

// HandleRequest handles the MigrateUser event by looking up a user in an Amazon
DynamoDB table and

```

```
// specifying whether they should be migrated to the user pool.
func (h *handler) HandleRequest(ctx context.Context, event
events.CognitoEventUserPoolsMigrateUser)
(events.CognitoEventUserPoolsMigrateUser, error) {
log.Printf("Received migrate trigger from %v for user '%v'",
event.TriggerSource, event.UserName)
if event.TriggerSource != "UserMigration_Authentication" {
return event, nil
}
tableName := os.Getenv(TABLE_NAME)
user := UserInfo{
UserName: event.UserName,
}
log.Printf("Looking up user '%v' in table %v.\n", user.UserName, tableName)
filterEx := expression.Name("UserName").Equal(expression.Value(user.UserName))
expr, err := expression.NewBuilder().WithFilter(filterEx).Build()
if err != nil {
log.Printf("Error building expression to query for user '%v'.\n",
user.UserName)
return event, err
}
output, err := h.dynamoClient.Scan(ctx, &dynamodb.ScanInput{
TableName:          aws.String(tableName),
FilterExpression:   expr.Filter(),
ExpressionAttributeNames: expr.Names(),
ExpressionAttributeValues: expr.Values(),
})
if err != nil {
log.Printf("Error looking up user '%v'.\n", user.UserName)
return event, err
}
if output.Items == nil || len(output.Items) == 0 {
log.Printf("User '%v' not found, not migrating user.\n", user.UserName)
return event, err
}

var users []UserInfo
err = attributevalue.UnmarshalListOfMaps(output.Items, &users)
if err != nil {
log.Printf("Couldn't unmarshal DynamoDB items. Here's why: %v\n", err)
return event, err
}

user = users[0]
```



```

log.Printf("UserName '%v' found with email %v. User is migrated and must reset
password.\n", user.UserName, user.UserEmail)
event.CognitoEventUserPoolsMigrateUserResponse.UserAttributes =
map[string]string{
    "email":          user.UserEmail,
    "email_verified": "true", // email_verified is required for the forgot password
flow.
}
event.CognitoEventUserPoolsMigrateUserResponse.FinalUserStatus =
"RESET_REQUIRED"
event.CognitoEventUserPoolsMigrateUserResponse.MessageAction = "SUPPRESS"

return event, err
}

func main() {
    sdkConfig, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        log.Panicln(err)
    }
    h := handler{
        dynamoClient: dynamodb.NewFromConfig(sdkConfig),
    }
    lambda.Start(h.HandleRequest)
}

```

Buat struct yang melakukan tugas-tugas umum.

```

// IScenarioHelper defines common functions used by the workflows in this
example.
type IScenarioHelper interface {
    Pause(secs int)
    GetStackOutputs(stackName string) (actions.StackOutputs, error)
    PopulateUserTable(tableName string)
    GetKnownUsers(tableName string) (actions.UserList, error)
    AddKnownUser(tableName string, user actions.User)
    ListRecentLogEvents(functionName string)
}

```

```
// ScenarioHelper contains AWS wrapper structs used by the workflows in this
// example.
type ScenarioHelper struct {
    questioner demotools.IQuestioner
    dynamoActor *actions.DynamoActions
    cfnActor     *actions.CloudFormationActions
    cwActor     *actions.CloudWatchLogsActions
    isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
    ScenarioHelper {
    scenario := ScenarioHelper{
        questioner: questioner,
        dynamoActor: &actions.DynamoActions{DynamoClient:
            dynamodb.NewFromConfig(sdkConfig)},
        cfnActor: &actions.CloudFormationActions{CfnClient:
            cloudformation.NewFromConfig(sdkConfig)},
        cwActor: &actions.CloudWatchLogsActions{CwlClient:
            cloudwatchlogs.NewFromConfig(sdkConfig)},
    }
    return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
    if !helper.isTestRun {
        time.Sleep(time.Duration(secs) * time.Second)
    }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
// structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
    (actions.StackOutputs, error) {
    return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
    log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
    this example.\n", tableName)
    err := helper.dynamoActor.PopulateTable(tableName)
}
```

```
    if err != nil {
        panic(err)
    }
}

// GetKnownUsers gets the users from the known users table in a structured
// format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
error) {
    knownUsers, err := helper.dynamoActor.Scan(tableName)
    if err != nil {
        log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
            tableName, err)
    }
    return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
    log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
        table...\n",
        user.UserName, user.UserEmail)
    err := helper.dynamoActor.AddUser(tableName, user)
    if err != nil {
        panic(err)
    }
}

// ListRecentLogEvents gets the most recent log stream and events for the
// specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
    log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
    helper.Pause(10)
    log.Println("Okay, let's check the logs to find what's happened recently with
        your Lambda function.")
    logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
    if err != nil {
        panic(err)
    }
    log.Printf("Getting some recent events from log stream %v\n",
        *logStream.LogStreamName)
    events, err := helper.cwlActor.GetLogEvents(functionName,
        *logStream.LogStreamName, 10)
    if err != nil {
```

```

panic(err)
}
for _, event := range events {
    log.Printf("\t%v", *event.Message)
}
log.Println(strings.Repeat("-", 88))
}

```

Buat struct yang membungkus tindakan Amazon Cognito.

```

type CognitoActions struct {
    CognitoClient *cognitoidentityprovider.Client
}

// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
// trigger.
type Trigger int

const (
    PreSignUp Trigger = iota
    UserMigration
    PostAuthentication
)

type TriggerInfo struct {
    Trigger    Trigger
    HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
// is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
    triggers ...TriggerInfo) error {
    output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
    &cognitoidentityprovider.DescribeUserPoolInput{
        UserPoolId: aws.String(userPoolId),
    })
}

```

```
    })
    if err != nil {
        log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
            userPoolId, err)
        return err
    }
    lambdaConfig := output.UserPool.LambdaConfig
    for _, trigger := range triggers {
        switch trigger.Trigger {
        case PreSignUp:
            lambdaConfig.PreSignUp = trigger.HandlerArn
        case UserMigration:
            lambdaConfig.UserMigration = trigger.HandlerArn
        case PostAuthentication:
            lambdaConfig.PostAuthentication = trigger.HandlerArn
        }
    }
    _, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
        &cognitoidentityprovider.UpdateUserPoolInput{
            UserPoolId:    aws.String(userPoolId),
            LambdaConfig: lambdaConfig,
        })
    if err != nil {
        log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
    }
    return err
}

// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(clientId string, userName string, password
string, userEmail string) (bool, error) {
    confirmed := false
    output, err := actor.CognitoClient.SignUp(context.TODO(),
        &cognitoidentityprovider.SignUpInput{
            ClientId: aws.String(clientId),
            Password: aws.String(password),
            Username: aws.String(userName),
            UserAttributes: []types.AttributeType{
                {Name: aws.String("email"), Value: aws.String(userEmail)},
            },
        })
    if err != nil {
```

```
var invalidPassword *types.InvalidPasswordException
if errors.As(err, &invalidPassword) {
    log.Println(*invalidPassword.Message)
} else {
    log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
}
} else {
    confirmed = output.UserConfirmed
}
return confirmed, err
}

// SignIn signs in a user to Amazon Cognito using a username and password
authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
string) (*types.AuthenticationResultType, error) {
    var authResult *types.AuthenticationResultType
    output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
&cognitoidentityprovider.InitiateAuthInput{
        AuthFlow:      "USER_PASSWORD_AUTH",
        ClientId:      aws.String(clientId),
        AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
    })
    if err != nil {
        var resetRequired *types.PasswordResetRequiredException
        if errors.As(err, &resetRequired) {
            log.Println(*resetRequired.Message)
        } else {
            log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
        }
    } else {
        authResult = output.AuthenticationResult
    }
    return authResult, err
}

// ForgotPassword starts a password recovery flow for a user. This flow typically
sends a confirmation code
// to the user's configured notification destination, such as email.
```

```
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
(*types.CodeDeliveryDetailsType, error) {
    output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
&cognitoidentityprovider.ForgotPasswordInput{
    ClientId: aws.String(clientId),
    Username: aws.String(userName),
})
    if err != nil {
        log.Printf("Couldn't start password reset for user '%v'. Here's why: %v\n",
userName, err)
    }
    return output.CodeDeliveryDetails, err
}

// ConfirmForgotPassword confirms a user with a confirmation code and a new
password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
userName string, password string) error {
    _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
&cognitoidentityprovider.ConfirmForgotPasswordInput{
    ClientId:      aws.String(clientId),
    ConfirmationCode: aws.String(code),
    Password:      aws.String(password),
    Username:      aws.String(userName),
})
    if err != nil {
        var invalidPassword *types.InvalidPasswordException
        if errors.As(err, &invalidPassword) {
            log.Println(*invalidPassword.Message)
        } else {
            log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
        }
    }
    return err
}

// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
    _, err := actor.CognitoClient.DeleteUser(context.TODO(),
&cognitoidentityprovider.DeleteUserInput{
```

```
    AccessToken: aws.String(userAccessToken),
  })
  if err != nil {
    log.Printf("Couldn't delete user. Here's why: %v\n", err)
  }
  return err
}

// AdminCreateUser uses administrator credentials to add a user to a user pool.
// This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
userEmail string) error {
  _, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
&cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:      aws.String(userPoolId),
  Username:        aws.String(userName),
  MessageAction:   types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
aws.String(userEmail)}}},
  })
  if err != nil {
    var userExists *types.UsernameExistsException
    if errors.As(err, &userExists) {
      log.Printf("User %v already exists in the user pool.", userName)
      err = nil
    } else {
      log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
    }
  }
  return err
}

// AdminSetUserPassword uses administrator credentials to set a password for a
// user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
string, password string) error {
  _, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
&cognitoidentityprovider.AdminSetUserPasswordInput{
```



```

Password:  aws.String(password),
UserPoolId: aws.String(userPoolId),
Username:  aws.String(userName),
Permanent: true,
})
if err != nil {
    var invalidPassword *types.InvalidPasswordException
    if errors.As(err, &invalidPassword) {
        log.Println(*invalidPassword.Message)
    } else {
        log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
err)
    }
}
return err
}

```

Buat struct yang membungkus tindakan DynamoDB.

```

// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
actions
// used in the examples.
type DynamoActions struct {
    DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
    UserName string
    UserEmail string
    LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
    UserPoolId string
    ClientId string
    Time string
}

```

```
// userList defines a list of users.
type userList struct {
    Users []User
}

// UserNameList returns the usernames contained in a userList as a list of
strings.
func (users *UserList) UserNameList() []string {
    names := make([]string, len(users.Users))
    for i := 0; i < len(users.Users); i++ {
        names[i] = users.Users[i].UserName
    }
    return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
    var err error
    var item map[string]types.AttributeValue
    var writeReqs []types.WriteRequest
    for i := 1; i < 4; i++ {
        item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
        %v", i), userEmail: fmt.Sprintf("test_email_%v@example.com", i)})
        if err != nil {
            log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
            err)
            return err
        }
        writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
        &types.PutRequest{Item: item}})
    }
    _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
    &dynamodb.BatchWriteItemInput{
        RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
    })
    if err != nil {
        log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
        tableName, err)
    }
    return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
```

```

var userList UserList
output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
    TableName: aws.String(tableName),
})
if err != nil {
    log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
err)
} else {
    err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
    if err != nil {
        log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
    }
}
return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
    userItem, err := attributevalue.MarshalMap(user)
    if err != nil {
        log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
    }
    _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
        Item:      userItem,
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
    }
    return err
}

```

Buat struct yang membungkus tindakan CloudWatch Log.

```

type CloudWatchLogsActions struct {
    CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.

```

```
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
(types.LogStream, error) {
    var logStream types.LogStream
    logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
    output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
&cloudwatchlogs.DescribeLogStreamsInput{
    Descending:    aws.Bool(true),
    Limit:         aws.Int32(1),
    LogGroupName: aws.String(logGroupName),
    OrderBy:      types.OrderByLastEventTime,
})
    if err != nil {
        log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
logGroupName, err)
    } else {
        logStream = output.LogStreams[0]
    }
    return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
logStreamName string, eventCount int32) (
[]types.OutputLogEvent, error) {
    var events []types.OutputLogEvent
    logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
    output, err := actor.CwlClient.GetLogEvents(context.TODO(),
&cloudwatchlogs.GetLogEventsInput{
    LogStreamName: aws.String(logStreamName),
    Limit:         aws.Int32(eventCount),
    LogGroupName:  aws.String(logGroupName),
})
    if err != nil {
        log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
logStreamName, err)
    } else {
        events = output.Events
    }
    return events, err
}
```

Buat struct yang membungkus tindakan AWS CloudFormation .

```
// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
    CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
// structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
    output, err := actor.CfnClient.DescribeStacks(context.TODO(),
        &cloudformation.DescribeStacksInput{
            StackName: aws.String(stackName),
        })
    if err != nil || len(output.Stacks) == 0 {
        log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
            stackName, err)
    }
    stackOutputs := StackOutputs{}
    for _, out := range output.Stacks[0].Outputs {
        stackOutputs[*out.OutputKey] = *out.OutputValue
    }
    return stackOutputs
}
```

Pembersihan sumber daya

```
// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
    userPoolId      string
    userAccessTokens []string
    triggers        []actions.Trigger

    cognitoActor *actions.CognitoActions
    questioner   demotools.IQuestioner
}
```

```
func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
demotools.IQuestioner) {
    resources.userAccessTokens = []string{}
    resources.triggers = []actions.Trigger{}
    resources.cognitoActor = cognitoActor
    resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
    defer func() {
        if r := recover(); r != nil {
            log.Printf("Something went wrong during cleanup.\n%v\n", r)
            log.Println("Use the AWS Management Console to remove any remaining resources
\n" +
                "that were created for this scenario.")
        }
    }()

    wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
resources that were created "+
        "during this demo (y/n)?", "y")
    if wantDelete {
        for _, accessToken := range resources.userAccessTokens {
            err := resources.cognitoActor.DeleteUser(accessToken)
            if err != nil {
                log.Println("Couldn't delete user during cleanup.")
                panic(err)
            }
            log.Println("Deleted user.")
        }
        triggerList := make([]actions.TriggerInfo, len(resources.triggers))
        for i := 0; i < len(resources.triggers); i++ {
            triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
HandlerArn: nil}
        }
        err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,
triggerList...)
        if err != nil {
            log.Println("Couldn't update Cognito triggers during cleanup.")
            panic(err)
        }
        log.Println("Removed Cognito triggers from user pool.")
    }
}
```

```
} else {  
    log.Println("Be sure to remove resources when you're done with them to avoid  
unexpected charges!")  
}  
}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Go API Referensi.
 - [ConfirmForgotPassword](#)
 - [DeleteUser](#)
 - [ForgotPassword](#)
 - [InitiateAuth](#)
 - [SignUp](#)
 - [UpdateUserPool](#)

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Buat API Gateway REST API untuk melacak data COVID -19

Contoh kode berikut menunjukkan cara membuat REST API yang mensimulasikan sistem untuk melacak kasus harian COVID -19 di Amerika Serikat, menggunakan data fiksi.

Python

SDK untuk Python (Boto3)

Menunjukkan cara menggunakan AWS Chalice dengan membuat tanpa server AWS SDK for Python (Boto3) yang REST API menggunakan Amazon API Gateway, AWS Lambda dan Amazon DynamoDB. Ini REST API mensimulasikan sistem yang melacak kasus harian COVID -19 di Amerika Serikat, menggunakan data fiksi. Pelajari cara:

- Gunakan AWS Chalice untuk menentukan rute dalam fungsi Lambda yang dipanggil untuk menangani REST permintaan yang datang melalui Gateway. API
- Gunakan fungsi Lambda untuk mengambil dan menyimpan data dalam tabel DynamoDB untuk melayani permintaan. REST

- Tentukan struktur tabel dan sumber daya peran keamanan dalam AWS CloudFormation template.
- Gunakan AWS Chalice dan CloudFormation untuk mengemas dan menyebarkan semua sumber daya yang diperlukan.
- Gunakan CloudFormation untuk membersihkan semua sumber daya yang dibuat.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- AWS CloudFormation
- DynamoDB
- Lambda

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Buat perpustakaan pinjaman REST API

Contoh kode berikut menunjukkan cara membuat pustaka pinjaman tempat pelanggan dapat meminjam dan mengembalikan buku dengan menggunakan basis data Amazon Aurora yang REST API didukung.

Python

SDK untuk Python (Boto3)

Menunjukkan cara menggunakan AWS SDK for Python (Boto3) dengan Amazon Relational Database Service API (RDS Amazon) dan AWS Chalice untuk membuat database Amazon Aurora REST API yang didukung. Layanan web sepenuhnya nirserver dan mewakili pustaka peminjaman sederhana tempat pelanggan dapat meminjam dan mengembalikan buku.

Pelajari cara:

- Membuat dan mengelola kluster basis data Aurora nirserver.
- Gunakan AWS Secrets Manager untuk mengelola kredensial database.

- Menerapkan lapisan penyimpanan data yang menggunakan Amazon RDS untuk memindahkan data masuk dan keluar dari database.
- Gunakan AWS Chalice untuk menyebarkan tanpa server REST API ke Amazon Gateway dan. API AWS Lambda
- Menggunakan paket Permintaan untuk mengirim permintaan ke layanan web.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- APIGateway
- Aurora
- Lambda
- Secrets Manager

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Membuat aplikasi messenger dengan Step Functions

Contoh kode berikut menunjukkan cara membuat aplikasi AWS Step Functions messenger yang mengambil catatan pesan dari tabel database.

Python

SDK untuk Python (Boto3)

Menunjukkan cara menggunakan AWS SDK for Python (Boto3) with AWS Step Functions untuk membuat aplikasi messenger yang mengambil catatan pesan dari tabel Amazon DynamoDB dan mengirimkannya dengan Amazon Simple Queue Service (Amazon). SQS Mesin state terintegrasi dengan AWS Lambda fungsi untuk memindai database untuk pesan yang tidak terkirim.

- Buat mesin status yang mengambil dan memperbarui catatan pesan dari tabel Amazon DynamoDB.
- Perbarui definisi mesin status untuk juga mengirim pesan ke Amazon Simple Queue Service (AmazonSQS).

- Mulai dan hentikan berjalannya mesin status.
- Connect ke Lambda, DynamoDB, dan SQS Amazon dari mesin status dengan menggunakan integrasi layanan.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- Lambda
- Amazon SQS
- Step Functions

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Membuat aplikasi manajemen aset foto yang memungkinkan pengguna mengelola foto menggunakan label

Contoh kode berikut ini menunjukkan cara membuat aplikasi nirserver yang memungkinkan pengguna mengelola foto menggunakan label.

.NET

AWS SDK for .NET

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang

- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

C++

SDK untuk C++

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Java

SDK untuk Java 2.x

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

JavaScript

SDK untuk JavaScript (v3)

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Kotlin

SDKuntuk Kotlin

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

PHP

SDKuntuk PHP

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB

- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Rust

SDK untuk Rust

Menunjukkan cara mengembangkan aplikasi manajemen aset foto yang mendeteksi label dalam gambar menggunakan Amazon Rekognition dan menyimpannya untuk pengambilan nanti.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Untuk mendalami tentang asal usul contoh ini, lihat postingan di [Komunitas AWS](#).

Layanan yang digunakan dalam contoh ini

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Buat aplikasi obrolan websocket dengan API Gateway

Contoh kode berikut menunjukkan cara membuat aplikasi obrolan yang dilayani oleh websocket yang API dibangun di Amazon API Gateway.

Python

SDK untuk Python (Boto3)

Menunjukkan cara menggunakan AWS SDK for Python (Boto3) dengan Amazon API Gateway V2 untuk membuat websocket API yang terintegrasi dengan AWS Lambda dan Amazon DynamoDB.

- Buat websocket yang API dilayani oleh API Gateway.
- Tentukan penanganan Lambda yang menyimpan koneksi di DynamoDB dan memposting pesan ke peserta obrolan lainnya.
- Hubungkan ke aplikasi obrolan websocket dan kirim pesan dengan paket WebSocket.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- API Gateway
- DynamoDB
- Lambda

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Buat aplikasi yang menganalisis umpan balik pelanggan dan mensintesis audio

Contoh kode berikut menunjukkan cara membuat aplikasi yang menganalisis kartu komentar pelanggan, menerjemahkannya dari bahasa aslinya, menentukan sentimen mereka, dan menghasilkan file audio dari teks yang diterjemahkan.

.NET

AWS SDK for .NET

Aplikasi contoh ini menganalisis dan menyimpan kartu umpan balik pelanggan. Secara khusus, ini memenuhi kebutuhan hotel fiktif di New York City. Hotel menerima umpan balik dari para tamu dalam berbagai bahasa dalam bentuk kartu komentar fisik. Umpan balik itu

diunggah ke aplikasi melalui klien web. Setelah gambar kartu komentar diunggah, langkah-langkah berikut terjadi:

- Teks diekstraksi dari gambar menggunakan Amazon Textract.
- Amazon Comprehend menentukan sentimen teks yang diekstraksi dan bahasanya.
- Teks yang diekstraksi diterjemahkan ke bahasa Inggris menggunakan Amazon Translate.
- Amazon Polly mensintesis file audio dari teks yang diekstraksi.

Aplikasi lengkap dapat digunakan dengan. AWS CDK Untuk kode sumber dan petunjuk penerapan, lihat proyek di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Java

SDK untuk Java 2.x

Aplikasi contoh ini menganalisis dan menyimpan kartu umpan balik pelanggan. Secara khusus, ini memenuhi kebutuhan hotel fiktif di New York City. Hotel menerima umpan balik dari para tamu dalam berbagai bahasa dalam bentuk kartu komentar fisik. Umpan balik itu diunggah ke aplikasi melalui klien web. Setelah gambar kartu komentar diunggah, langkah-langkah berikut terjadi:

- Teks diekstraksi dari gambar menggunakan Amazon Textract.
- Amazon Comprehend menentukan sentimen teks yang diekstraksi dan bahasanya.
- Teks yang diekstraksi diterjemahkan ke bahasa Inggris menggunakan Amazon Translate.
- Amazon Polly mensintesis file audio dari teks yang diekstraksi.

Aplikasi lengkap dapat digunakan dengan. AWS CDK Untuk kode sumber dan petunjuk penerapan, lihat proyek di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- Amazon Comprehend

- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

JavaScript

SDK untuk JavaScript (v3)

Aplikasi contoh ini menganalisis dan menyimpan kartu umpan balik pelanggan. Secara khusus, ini memenuhi kebutuhan hotel fiktif di New York City. Hotel menerima umpan balik dari para tamu dalam berbagai bahasa dalam bentuk kartu komentar fisik. Umpan balik itu diunggah ke aplikasi melalui klien web. Setelah gambar kartu komentar diunggah, langkah-langkah berikut terjadi:

- Teks diekstraksi dari gambar menggunakan Amazon Textract.
- Amazon Comprehend menentukan sentimen teks yang diekstraksi dan bahasanya.
- Teks yang diekstraksi diterjemahkan ke bahasa Inggris menggunakan Amazon Translate.
- Amazon Polly mensintesis file audio dari teks yang diekstraksi.

Aplikasi lengkap dapat digunakan dengan AWS CDK Untuk kode sumber dan petunjuk penerapan, lihat proyek di [GitHub](#). Kutipan berikut menunjukkan bagaimana yang AWS SDK for JavaScript digunakan di dalam fungsi Lambda.

```
import {
  ComprehendClient,
  DetectDominantLanguageCommand,
  DetectSentimentCommand,
} from "@aws-sdk/client-comprehend";

/**
 * Determine the language and sentiment of the extracted text.
 *
 * @param {{ source_text: string }} extractTextOutput
 */
export const handler = async (extractTextOutput) => {
  const comprehendClient = new ComprehendClient({});

  const detectDominantLanguageCommand = new DetectDominantLanguageCommand({
    Text: extractTextOutput.source_text,
```

```
});

// The source language is required for sentiment analysis and
// translation in the next step.
const { Languages } = await comprehendClient.send(
  detectDominantLanguageCommand,
);

const languageCode = Languages[0].LanguageCode;

const detectSentimentCommand = new DetectSentimentCommand({
  Text: extractTextOutput.source_text,
  LanguageCode: languageCode,
});

const { Sentiment } = await comprehendClient.send(detectSentimentCommand);

return {
  sentiment: Sentiment,
  language_code: languageCode,
};
};
```

```
import {
  DetectDocumentTextCommand,
  TextractClient,
} from "@aws-sdk/client-textract";

/**
 * Fetch the S3 object from the event and analyze it using Amazon Textract.
 *
 * @param {import("@types/aws-lambda").EventBridgeEvent<"Object Created">}
  eventBridgeS3Event
 */
export const handler = async (eventBridgeS3Event) => {
  const textractClient = new TextractClient();

  const detectDocumentTextCommand = new DetectDocumentTextCommand({
    Document: {
      S3Object: {
        Bucket: eventBridgeS3Event.bucket,
        Name: eventBridgeS3Event.object,
      },
    },
  },
```

```
    },
  });

  // Textract returns a list of blocks. A block can be a line, a page, word, etc.
  // Each block also contains geometry of the detected text.
  // For more information on the Block type, see https://docs.aws.amazon.com/
  // textract/latest/dg/API_Block.html.
  const { Blocks } = await textractClient.send(detectDocumentTextCommand);

  // For the purpose of this example, we are only interested in words.
  const extractedWords = Blocks.filter((b) => b.BlockType === "WORD").map(
    (b) => b.Text,
  );

  return extractedWords.join(" ");
};
```

```
import { PollyClient, SynthesizeSpeechCommand } from "@aws-sdk/client-polly";
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

/**
 * Synthesize an audio file from text.
 *
 * @param {{ bucket: string, translated_text: string, object: string }}
 * sourceDestinationConfig
 */
export const handler = async (sourceDestinationConfig) => {
  const pollyClient = new PollyClient({});

  const synthesizeSpeechCommand = new SynthesizeSpeechCommand({
    Engine: "neural",
    Text: sourceDestinationConfig.translated_text,
    VoiceId: "Ruth",
    OutputFormat: "mp3",
  });

  const { AudioStream } = await pollyClient.send(synthesizeSpeechCommand);

  const audioKey = `${sourceDestinationConfig.object}.mp3`;

  // Store the audio file in S3.
  const s3Client = new S3Client();
```

```
const upload = new Upload({
  client: s3Client,
  params: {
    Bucket: sourceDestinationConfig.bucket,
    Key: audioKey,
    Body: AudioStream,
    ContentType: "audio/mp3",
  },
});

await upload.done();
return audioKey;
};
```

```
import {
  TranslateClient,
  TranslateTextCommand,
} from "@aws-sdk/client-translate";

/**
 * Translate the extracted text to English.
 *
 * @param {{ extracted_text: string, source_language_code: string }}
  textAndSourceLanguage
 */
export const handler = async (textAndSourceLanguage) => {
  const translateClient = new TranslateClient({});

  const translateCommand = new TranslateTextCommand({
    SourceLanguageCode: textAndSourceLanguage.source_language_code,
    TargetLanguageCode: "en",
    Text: textAndSourceLanguage.extracted_text,
  });

  const { TranslatedText } = await translateClient.send(translateCommand);

  return { translated_text: TranslatedText };
};
```

Layanan yang digunakan dalam contoh ini

- Amazon Comprehend
- Lambda

- Amazon Polly
- Amazon Textract
- Amazon Translate

Ruby

SDK untuk Ruby

Aplikasi contoh ini menganalisis dan menyimpan kartu umpan balik pelanggan. Secara khusus, ini memenuhi kebutuhan hotel fiktif di New York City. Hotel menerima umpan balik dari para tamu dalam berbagai bahasa dalam bentuk kartu komentar fisik. Umpan balik itu diunggah ke aplikasi melalui klien web. Setelah gambar kartu komentar diunggah, langkah-langkah berikut terjadi:

- Teks diekstraksi dari gambar menggunakan Amazon Textract.
- Amazon Comprehend menentukan sentimen teks yang diekstraksi dan bahasanya.
- Teks yang diekstraksi diterjemahkan ke bahasa Inggris menggunakan Amazon Translate.
- Amazon Polly mensintesis file audio dari teks yang diekstraksi.

Aplikasi lengkap dapat digunakan dengan AWS CDK Untuk kode sumber dan petunjuk penerapan, lihat proyek di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Mulai membuat dan menjalankan fungsi Lambda menggunakan AWS SDK

Contoh kode berikut ini menunjukkan cara:

- Buat IAM peran dan fungsi Lambda, lalu unggah kode handler.
- Panggil fungsi dengan satu parameter dan dapatkan hasil.
- Perbarui kode fungsi dan konfigurasi dengan variabel lingkungan.
- Panggil fungsi dengan parameter baru dan dapatkan hasil. Tampilkan log eksekusi yang dikembalikan.
- Buat daftar fungsi untuk akun Anda, lalu bersihkan sumber daya.

Untuk informasi selengkapnya, lihat [Membuat fungsi Lambda dengan konsol](#).

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

Buat metode yang melakukan tindakan Lambda.

```
namespace LambdaActions;

using Amazon.Lambda;
using Amazon.Lambda.Model;

/// <summary>
/// A class that implements AWS Lambda methods.
/// </summary>
public class LambdaWrapper
{
    private readonly IAmazonLambda _lambdaService;

    /// <summary>
    /// Constructor for the LambdaWrapper class.
    /// </summary>
    /// <param name="lambdaService">An initialized Lambda service client.</param>
    public LambdaWrapper(IAmazonLambda lambdaService)
    {
        _lambdaService = lambdaService;
    }
}
```

```
}

/// <summary>
/// Creates a new Lambda function.
/// </summary>
/// <param name="functionName">The name of the function.</param>
/// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
/// bucket where the zip file containing the code is located.</param>
/// <param name="s3Key">The Amazon S3 key of the zip file.</param>
/// <param name="role">The Amazon Resource Name (ARN) of a role with the
/// appropriate Lambda permissions.</param>
/// <param name="handler">The name of the handler function.</param>
/// <returns>The Amazon Resource Name (ARN) of the newly created
/// Lambda function.</returns>
public async Task<string> CreateLambdaFunctionAsync(
    string functionName,
    string s3Bucket,
    string s3Key,
    string role,
    string handler)
{
    // Defines the location for the function code.
    // S3Bucket - The S3 bucket where the file containing
    //           the source code is stored.
    // S3Key    - The name of the file containing the code.
    var functionCode = new FunctionCode
    {
        S3Bucket = s3Bucket,
        S3Key = s3Key,
    };

    var createFunctionRequest = new CreateFunctionRequest
    {
        FunctionName = functionName,
        Description = "Created by the Lambda .NET API",
        Code = functionCode,
        Handler = handler,
        Runtime = Runtime.Dotnet6,
        Role = role,
    };

    var reponse = await
_lambdaService.CreateFunctionAsync(createFunctionRequest);
    return reponse.FunctionArn;
}
```

```
}

/// <summary>
/// Delete an AWS Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function to
/// delete.</param>
/// <returns>A Boolean value that indicates the success of the action.</
returns>
public async Task<bool> DeleteFunctionAsync(string functionName)
{
    var request = new DeleteFunctionRequest
    {
        FunctionName = functionName,
    };

    var response = await _lambdaService.DeleteFunctionAsync(request);

    // A return value of NoContent means that the request was processed.
    // In this case, the function was deleted, and the return value
    // is intentionally blank.
    return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;
}

/// <summary>
/// Gets information about a Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function for
/// which to retrieve information.</param>
/// <returns>Async Task.</returns>
public async Task<FunctionConfiguration> GetFunctionAsync(string
functionName)
{
    var functionRequest = new GetFunctionRequest
    {
        FunctionName = functionName,
    };

    var response = await _lambdaService.GetFunctionAsync(functionRequest);
    return response.Configuration;
}
```



```
/// <summary>
/// Invoke a Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function to
/// invoke.</param>
/// <param name="parameters">The parameter values that will be passed to the
function.</param>
/// <returns>A System Threading Task.</returns>
public async Task<string> InvokeFunctionAsync(
    string functionName,
    string parameters)
{
    var payload = parameters;
    var request = new InvokeRequest
    {
        FunctionName = functionName,
        Payload = payload,
    };

    var response = await _lambdaService.InvokeAsync(request);
    MemoryStream stream = response.Payload;
    string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
    return returnValue;
}

/// <summary>
/// Get a list of Lambda functions.
/// </summary>
/// <returns>A list of FunctionConfiguration objects.</returns>
public async Task<List<FunctionConfiguration>> ListFunctionsAsync()
{
    var functionList = new List<FunctionConfiguration>();

    var functionPaginator =
        _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
    await foreach (var function in functionPaginator.Functions)
    {
        functionList.Add(function);
    }

    return functionList;
}
```

```
}

/// <summary>
/// Update an existing Lambda function.
/// </summary>
/// <param name="functionName">The name of the Lambda function to update.</
param>
/// <param name="bucketName">The bucket where the zip file containing
/// the Lambda function code is stored.</param>
/// <param name="key">The key name of the source code file.</param>
/// <returns>Async Task.</returns>
public async Task UpdateFunctionCodeAsync(
    string functionName,
    string bucketName,
    string key)
{
    var functionCodeRequest = new UpdateFunctionCodeRequest
    {
        FunctionName = functionName,
        Publish = true,
        S3Bucket = bucketName,
        S3Key = key,
    };

    var response = await
_lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
    Console.WriteLine($"The Function was last modified at
{response.LastModified}.");
}

/// <summary>
/// Update the code of a Lambda function.
/// </summary>
/// <param name="functionName">The name of the function to update.</param>
/// <param name="functionHandler">The code that performs the function's
actions.</param>
/// <param name="environmentVariables">A dictionary of environment
variables.</param>
/// <returns>A Boolean value indicating the success of the action.</returns>
public async Task<bool> UpdateFunctionConfigurationAsync(
    string functionName,
    string functionHandler,
```

```
Dictionary<string, string> environmentVariables)
{
    var request = new UpdateFunctionConfigurationRequest
    {
        Handler = functionHandler,
        FunctionName = functionName,
        Environment = new Amazon.Lambda.Model.Environment { Variables =
environmentVariables },
    };

    var response = await
_lambdaService.UpdateFunctionConfigurationAsync(request);

    Console.WriteLine(response.LastModified);

    return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
}
}
```

Buat fungsi yang menjalankan skenario.

```
global using System.Threading.Tasks;
global using Amazon.IdentityManagement;
global using Amazon.Lambda;
global using LambdaActions;
global using LambdaScenarioCommon;
global using Microsoft.Extensions.DependencyInjection;
global using Microsoft.Extensions.Hosting;
global using Microsoft.Extensions.Logging;
global using Microsoft.Extensions.Logging.Console;
global using Microsoft.Extensions.Logging.Debug;

using Amazon.Lambda.Model;
using Microsoft.Extensions.Configuration;

namespace LambdaBasics;

public class LambdaBasics
```

```
{
    private static ILogger logger = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
                        LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
                        LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonLambda>()
                    .AddAWSService<IAmazonIdentityManagementService>()
                    .AddTransient<LambdaWrapper>()
                    .AddTransient<LambdaRoleWrapper>()
                    .AddTransient<UIWrapper>()
            )
            .Build();

        var configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load test settings from .json file.
            .AddJsonFile("settings.local.json",
                true) // Optionally load local settings.
            .Build();

        logger = LoggerFactory.Create(builder => { builder.AddConsole(); })
            .CreateLogger<LambdaBasics>();

        var lambdaWrapper = host.Services.GetRequiredService<LambdaWrapper>();
        var lambdaRoleWrapper =
            host.Services.GetRequiredService<LambdaRoleWrapper>();
        var uiWrapper = host.Services.GetRequiredService<UIWrapper>();

        string functionName = configuration["FunctionName"]!;
        string roleName = configuration["RoleName"]!;
        string policyDocument = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\": [ " +
            "    {" +
```

```
        "        \"Effect\": \"Allow\", \" +
        \"Principal\": { \" +
        \"Service\": \"lambda.amazonaws.com\" \" +
        }, \" +
        \"Action\": \"sts:AssumeRole\" \" +
        } \" +
    ] \" +
}";

var incrementHandler = configuration["IncrementHandler"];
var calculatorHandler = configuration["CalculatorHandler"];
var bucketName = configuration["BucketName"];
var incrementKey = configuration["IncrementKey"];
var calculatorKey = configuration["CalculatorKey"];
var policyArn = configuration["PolicyArn"];

uiWrapper.DisplayLambdaBasicsOverview();

// Create the policy to use with the AWS Lambda functions and then attach
the
// policy to a new role.
var roleArn = await lambdaRoleWrapper.CreateLambdaRoleAsync(roleName,
policyDocument);

Console.WriteLine("Waiting for role to become active.");
uiWrapper.WaitABit(15, "Wait until the role is active before trying to
use it.");

// Attach the appropriate AWS Identity and Access Management (IAM) role
policy to the new role.
var success = await
lambdaRoleWrapper.AttachLambdaRolePolicyAsync(policyArn, roleName);
uiWrapper.WaitABit(10, "Allow time for the IAM policy to be attached to
the role.");

// Create the Lambda function using a zip file stored in an Amazon Simple
Storage Service
// (Amazon S3) bucket.
uiWrapper.DisplayTitle("Create Lambda Function");
Console.WriteLine($"Creating the AWS Lambda function: {functionName}.");
var lambdaArn = await lambdaWrapper.CreateLambdaFunctionAsync(
    functionName,
    bucketName,
    incrementKey,
```

```
        roleArn,
        incrementHandler);

    Console.WriteLine("Waiting for the new function to be available.");
    Console.WriteLine($"The AWS Lambda ARN is {lambdaArn}");

    // Get the Lambda function.
    Console.WriteLine($"Getting the {functionName} AWS Lambda function.");
    FunctionConfiguration config;
    do
    {
        config = await lambdaWrapper.GetFunctionAsync(functionName);
        Console.WriteLine(".");
    }
    while (config.State != State.Active);

    Console.WriteLine($"\\nThe function, {functionName} has been created.");
    Console.WriteLine($"The runtime of this Lambda function is
{config.Runtime}.");

    uiWrapper.PressEnter();

    // List the Lambda functions.
    uiWrapper.DisplayTitle("Listing all Lambda functions.");
    var functions = await lambdaWrapper.ListFunctionsAsync();
    DisplayFunctionList(functions);

    uiWrapper.DisplayTitle("Invoke increment function");
    Console.WriteLine("Now that it has been created, invoke the Lambda
increment function.");
    string? value;
    do
    {
        Console.WriteLine("Enter a value to increment: ");
        value = Console.ReadLine();
    }
    while (string.IsNullOrEmpty(value));

    string functionParameters = "{" +
        "\\\"action\\\": \\\"increment\\\", " +
        "\\\"x\\\": \"" + value + "\"" +
        "}";
    var answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
```

```
Console.WriteLine($"{value} + 1 = {answer}.");

uiWrapper.DisplayTitle("Update function");
Console.WriteLine("Now update the Lambda function code.");
await lambdaWrapper.UpdateFunctionCodeAsync(functionName, bucketName,
calculatorKey);

do
{
    config = await lambdaWrapper.GetFunctionAsync(functionName);
    Console.WriteLine(".");
}
while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

await lambdaWrapper.UpdateFunctionConfigurationAsync(
    functionName,
    calculatorHandler,
    new Dictionary<string, string> { { "LOG_LEVEL", "DEBUG" } });

do
{
    config = await lambdaWrapper.GetFunctionAsync(functionName);
    Console.WriteLine(".");
}
while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

uiWrapper.DisplayTitle("Call updated function");
Console.WriteLine("Now call the updated function...");

bool done = false;

do
{
    string? opSelected;

    Console.WriteLine("Select the operation to perform:");
    Console.WriteLine("\t1. add");
    Console.WriteLine("\t2. subtract");
    Console.WriteLine("\t3. multiply");
    Console.WriteLine("\t4. divide");
    Console.WriteLine("\t0r enter \"q\" to quit.");
    Console.WriteLine("Enter the number (1, 2, 3, 4, or q) of the
operation you want to perform: ");
    do
```

```
{
    Console.WriteLine("Your choice? ");
    opSelected = Console.ReadLine();
}
while (opSelected == string.Empty);

var operation = (opSelected) switch
{
    "1" => "add",
    "2" => "subtract",
    "3" => "multiply",
    "4" => "divide",
    "q" => "quit",
    _ => "add",
};

if (operation == "quit")
{
    done = true;
}
else
{
    // Get two numbers and an action from the user.
    value = string.Empty;
    do
    {
        Console.WriteLine("Enter the first value: ");
        value = Console.ReadLine();
    }
    while (value == string.Empty);

    string? value2;
    do
    {
        Console.WriteLine("Enter a second value: ");
        value2 = Console.ReadLine();
    }
    while (value2 == string.Empty);

    functionParameters = "{" +
        "\"action\": \"" + operation + "\", " +
        "\"x\": \"" + value + "\", " +
        "\"y\": \"" + value2 + "\" " +
        "}";
}
```



```
        answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
        Console.WriteLine($"The answer when we {operation} the two
numbers is: {answer}.");
    }

    uiWrapper.PressEnter();
} while (!done);

// Delete the function created earlier.

uiWrapper.DisplayTitle("Clean up resources");
// Detach the IAM policy from the IAM role.
Console.WriteLine("First detach the IAM policy from the role.");
success = await lambdaRoleWrapper.DetachLambdaRolePolicyAsync(policyArn,
roleName);
uiWrapper.WaitABit(15, "Let's wait for the policy to be fully detached
from the role.");

Console.WriteLine("Delete the AWS Lambda function.");
success = await lambdaWrapper.DeleteFunctionAsync(functionName);
if (success)
{
    Console.WriteLine($"The {functionName} function was deleted.");
}
else
{
    Console.WriteLine($"Could not remove the function {functionName}");
}

// Now delete the IAM role created for use with the functions
// created by the application.
Console.WriteLine("Now we can delete the role that we created.");
success = await lambdaRoleWrapper.DeleteLambdaRoleAsync(roleName);
if (success)
{
    Console.WriteLine("The role has been successfully removed.");
}
else
{
    Console.WriteLine("Couldn't delete the role.");
}
```

```
        Console.WriteLine("The Lambda Scenario is now complete.");
        uiWrapper.PressEnter();

        // Displays a formatted list of existing functions returned by the
        // LambdaMethods.ListFunctions.
        void DisplayFunctionList(List<FunctionConfiguration> functions)
        {
            functions.ForEach(functionConfig =>
            {
                Console.WriteLine($"{functionConfig.FunctionName}\t{functionConfig.Description}");
            });
        }
    }
}

namespace LambdaActions;

using Amazon.IdentityManagement;
using Amazon.IdentityManagement.Model;

public class LambdaRoleWrapper
{
    private readonly IAmazonIdentityManagementService _lambdaRoleService;

    public LambdaRoleWrapper(IAmazonIdentityManagementService lambdaRoleService)
    {
        _lambdaRoleService = lambdaRoleService;
    }

    /// <summary>
    /// Attach an AWS Identity and Access Management (IAM) role policy to the
    /// IAM role to be assumed by the AWS Lambda functions created for the
    scenario.
    /// </summary>
    /// <param name="policyArn">The Amazon Resource Name (ARN) of the IAM
    policy.</param>
    /// <param name="roleName">The name of the IAM role to attach the IAM policy
    to.</param>
    /// <returns>A Boolean value indicating the success of the action.</returns>
    public async Task<bool> AttachLambdaRolePolicyAsync(string policyArn, string
    roleName)
    {
```

```
        var response = await _lambdaRoleService.AttachRolePolicyAsync(new
AttachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role to create.</param>
    /// <param name="policyDocument">The policy document for the new IAM role.</
param>
    /// <returns>A string representing the ARN for newly created role.</returns>
    public async Task<string> CreateLambdaRoleAsync(string roleName, string
policyDocument)
    {
        var request = new CreateRoleRequest
        {
            AssumeRolePolicyDocument = policyDocument,
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.CreateRoleAsync(request);
        return response.Role.Arn;
    }

    /// <summary>
    /// Deletes an IAM role.
    /// </summary>
    /// <param name="roleName">The name of the role to delete.</param>
    /// <returns>A Boolean value indicating the success of the operation.</
returns>
    public async Task<bool> DeleteLambdaRoleAsync(string roleName)
    {
        var request = new DeleteRoleRequest
        {
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.DeleteRoleAsync(request);
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    public async Task<bool> DetachLambdaRolePolicyAsync(string policyArn, string
roleName)
```

```
    {
        var response = await _lambdaRoleService.DetachRolePolicyAsync(new
DetachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
}

namespace LambdaScenarioCommon;
public class UIWrapper
{
    public readonly string SepBar = new('-', Console.WindowWidth);

    /// <summary>
    /// Show information about the AWS Lambda Basics scenario.
    /// </summary>
    public void DisplayLambdaBasicsOverview()
    {
        Console.Clear();

        DisplayTitle("Welcome to AWS Lambda Basics");
        Console.WriteLine("This example application does the following:");
        Console.WriteLine("\t1. Creates an AWS Identity and Access Management
(IAM) role that will be assumed by the functions we create.");
        Console.WriteLine("\t2. Attaches an IAM role policy that has Lambda
permissions.");
        Console.WriteLine("\t3. Creates a Lambda function that increments the
value passed to it.");
        Console.WriteLine("\t4. Calls the increment function and passes a
value.");
        Console.WriteLine("\t5. Updates the code so that the function is a simple
calculator.");
        Console.WriteLine("\t6. Calls the calculator function with the values
entered.");
        Console.WriteLine("\t7. Deletes the Lambda function.");
        Console.WriteLine("\t7. Detaches the IAM role policy.");
        Console.WriteLine("\t8. Deletes the IAM role.");
        PressEnter();
    }

    /// <summary>
    /// Display a message and wait until the user presses enter.
    /// </summary>
    public void PressEnter()
```

```
{
    Console.WriteLine("\nPress <Enter> to continue. ");
    _ = Console.ReadLine();
    Console.WriteLine();
}

/// <summary>
/// Pad a string with spaces to center it on the console display.
/// </summary>
/// <param name="strToCenter">The string to be centered.</param>
/// <returns>The padded string.</returns>
public string CenterString(string strToCenter)
{
    var padAmount = (Console.WindowWidth - strToCenter.Length) / 2;
    var leftPad = new string(' ', padAmount);
    return $"{leftPad}{strToCenter}";
}

/// <summary>
/// Display a line of hyphens, the centered text of the title and another
/// line of hyphens.
/// </summary>
/// <param name="strTitle">The string to be displayed.</param>
public void DisplayTitle(string strTitle)
{
    Console.WriteLine(SepBar);
    Console.WriteLine(CenterString(strTitle));
    Console.WriteLine(SepBar);
}

/// <summary>
/// Display a countdown and wait for a number of seconds.
/// </summary>
/// <param name="numSeconds">The number of seconds to wait.</param>
public void WaitABit(int numSeconds, string msg)
{
    Console.WriteLine(msg);

    // Wait for the requested number of seconds.
    for (int i = numSeconds; i > 0; i--)
    {
        System.Threading.Thread.Sleep(1000);
        Console.Write($"{i}...");
    }
}
```

```
        PressEnter();
    }
}
```

Tentukan handler Lambda yang menambah angka.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace LambdaIncrement;

public class Function
{
    /// <summary>
    /// A simple function increments the integer parameter.
    /// </summary>
    /// <param name="input">A JSON string containing an action, which must be
    /// "increment" and a string representing the value to increment.</param>
    /// <param name="context">The context object passed by Lambda containing
    /// information about invocation, function, and execution environment.</
    param>
    /// <returns>A string representing the incremented value of the parameter.</
    returns>
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext
    context)
    {
        if (input["action"] == "increment")
        {
            int inputValue = Convert.ToInt32(input["x"]);
            return inputValue + 1;
        }
        else
        {
            return 0;
        }
    }
}
```

```
}  
}
```

Tentukan handler Lambda kedua yang melakukan operasi aritmatika.

```
using Amazon.Lambda.Core;  
  
// Assembly attribute to enable the Lambda function's JSON input to be converted  
// into a .NET class.  
[assembly:  
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))  
]  
  
namespace LambdaCalculator;  
  
public class Function  
{  
  
    /// <summary>  
    /// A simple function that takes two number in string format and performs  
    /// the requested arithmetic function.  
    /// </summary>  
    /// <param name="input">JSON data containing an action, and x and y values.  
    /// Valid actions include: add, subtract, multiply, and divide.</param>  
    /// <param name="context">The context object passed by Lambda containing  
    /// information about invocation, function, and execution environment.</  
    param>  
    /// <returns>A string representing the results of the calculation.</returns>  
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext  
    context)  
    {  
        var action = input["action"];  
        int x = Convert.ToInt32(input["x"]);  
        int y = Convert.ToInt32(input["y"]);  
        int result;  
        switch (action)  
        {  
            case "add":  
                result = x + y;  
                break;  
            case "subtract":  
                result = x - y;
```

```
        break;
    case "multiply":
        result = x * y;
        break;
    case "divide":
        if (y == 0)
        {
            Console.Error.WriteLine("Divide by zero error.");
            result = 0;
        }
        else
            result = x / y;
        break;
    default:
        Console.Error.WriteLine($"{action} is not a valid operation.");
        result = 0;
        break;
    }
    return result;
}
}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for .NET API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

C++

SDK untuk C++

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
#!/ Get started with functions scenario.
/*!
 \param clientConfig: AWS client configuration.
 \return bool: Successful completion.
 */
bool AwsDoc::Lambda::getStartedWithFunctionsScenario(
    const Aws::Client::ClientConfiguration &clientConfig) {

    Aws::Lambda::LambdaClient client(clientConfig);

    // 1. Create an AWS Identity and Access Management (IAM) role for Lambda
    function.
    Aws::String roleArn;
    if (!getIamRoleArn(roleArn, clientConfig)) {
        return false;
    }

    // 2. Create a Lambda function.
    int seconds = 0;
    do {
        Aws::Lambda::Model::CreateFunctionRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetDescription(LAMBDA_DESCRIPTION); // Optional.
#ifdef USE_CPP_LAMBDA_FUNCTION
        request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
        request.SetTimeout(15);
        request.SetMemorySize(128);

        // Assume the AWS Lambda function was built in Docker with same
        architecture
        // as this code.
#endif
#ifdef defined(__x86_64__)
```

```

        request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
    #elif defined(__aarch64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
    #else
    #error "Unimplemented architecture"
    #endif // defined(architecture)
    #else
        request.SetRuntime(Aws::Lambda::Model::Runtime::python3_8);
    #endif

    request.SetRole(roleArn);
    request.SetHandler(LAMBDA_HANDLER_NAME);
    request.SetPublish(true);
    Aws::Lambda::Model::FunctionCode code;
    std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                           std::ios_base::in | std::ios_base::binary);
    if (!ifstream.is_open()) {
        std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
        std::endl;
    }

    #if USE_CPP_LAMBDA_FUNCTION
        std::cerr
            << "The cpp Lambda function must be built following the
            instructions in the cpp_lambda/README.md file. "
            << std::endl;
    #endif

    #endif

        deleteIamRole(clientConfig);
        return false;
    }

    Aws::StringStream buffer;
    buffer << ifstream.rdbuf();

    code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
        buffer.str().c_str(),
                                           buffer.str().length()));

    request.SetCode(code);

    Aws::Lambda::Model::CreateFunctionOutcome outcome =
    client.CreateFunction(
        request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda function was successfully created. " <<
seconds

```

```

        << " seconds elapsed." << std::endl;
    break;
}
else if (outcome.GetError().GetErrorType() ==
        Aws::Lambda::LambdaErrors::INVALID_PARAMETER_VALUE &&
        outcome.GetError().GetMessage().find("role") >= 0) {
    if ((seconds % 5) == 0) { // Log status every 10 seconds.
        std::cout
            << "Waiting for the IAM role to become available as a
CreateFunction parameter. "
            << seconds
            << " seconds elapsed." << std::endl;

        std::cout << outcome.GetError().GetMessage() << std::endl;
    }
}
else {
    std::cerr << "Error with CreateFunction. "
        << outcome.GetError().GetMessage()
        << std::endl;
    deleteIamRole(clientConfig);
    return false;
}
++seconds;
std::this_thread::sleep_for(std::chrono::seconds(1));
} while (60 > seconds);

std::cout << "The current Lambda function increments 1 by an input." <<
std::endl;

// 3. Invoke the Lambda function.
{
    int increment = askQuestionForInt("Enter an increment integer: ");

    Aws::Lambda::Model::InvokeResult invokeResult;
    Aws::Utils::Json::JsonValue jsonPayload;
    jsonPayload.WithString("action", "increment");
    jsonPayload.WithInteger("number", increment);
    if (invokeLambdaFunction(jsonPayload, Aws::Lambda::Model::LogType::Tail,
        invokeResult, client)) {
        Aws::Utils::Json::JsonValue jsonValue(invokeResult.GetPayload());
        Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
            jsonValue.View().GetAllObjects();
        auto iter = values.find("result");

```

```
        if (iter != values.end() && iter->second.IsIntegerType()) {
            {
                std::cout << INCREMENT_RESULT_PREFIX
                    << iter->second.AsInteger() << std::endl;
            }
        }
    else {
        std::cout << "There was an error in execution. Here is the log."
            << std::endl;
        Aws::Utils::ByteBuffer buffer =
    Aws::Utils::HashingUtils::Base64Decode(
            invokeResult.GetLogResult());
        std::cout << "With log " << buffer.GetUnderlyingData() <<
    std::endl;
    }
}

std::cout
    << "The Lambda function will now be updated with new code. Press
return to continue, ";
    Aws::String answer;
    std::getline(std::cin, answer);

// 4. Update the Lambda function code.
{
    Aws::Lambda::Model::UpdateFunctionCodeRequest request;
    request.SetFunctionName(LAMBDA_NAME);
    std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
        std::ios_base::in | std::ios_base::binary);
    if (!ifstream.is_open()) {
        std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
    std::endl;
}

#ifdef USE_CPP_LAMBDA_FUNCTION
    std::cerr
        << "The cpp Lambda function must be built following the
instructions in the cpp_lambda/README.md file. "
        << std::endl;
#endif

    deleteLambdaFunction(client);
    deleteIamRole(clientConfig);
    return false;
}
```

```
Aws::StringStream buffer;
buffer << ifstream.rdbuf();
request.SetZipFile(
    Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                           buffer.str().length()));

request.SetPublish(true);

Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
client.UpdateFunctionCode(
    request);

if (outcome.IsSuccess()) {
    std::cout << "The lambda code was successfully updated." <<
std::endl;
}
else {
    std::cerr << "Error with Lambda::UpdateFunctionCode. "
    << outcome.GetError().GetMessage()
    << std::endl;
}
}

std::cout
    << "This function uses an environment variable to control the logging
level."
    << std::endl;

std::cout
    << "UpdateFunctionConfiguration will be used to set the LOG_LEVEL to
DEBUG."
    << std::endl;

seconds = 0;

// 5. Update the Lambda function configuration.
do {
    ++seconds;
    std::this_thread::sleep_for(std::chrono::seconds(1));
    Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;
    request.SetFunctionName(LAMBDA_NAME);
    Aws::Lambda::Model::Environment environment;
    environment.AddVariables("LOG_LEVEL", "DEBUG");
    request.SetEnvironment(environment);
```

```

    Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
client.UpdateFunctionConfiguration(
    request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda configuration was successfully updated."
            << std::endl;
        break;
    }

    // RESOURCE_IN_USE: function code update not completed.
    else if (outcome.GetError().GetErrorType() !=
        Aws::Lambda::LambdaErrors::RESOURCE_IN_USE) {
        if ((seconds % 10) == 0) { // Log status every 10 seconds.
            std::cout << "Lambda function update in progress . After " <<
seconds
                << " seconds elapsed." << std::endl;
        }
    }
    else {
        std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
            << outcome.GetError().GetMessage()
            << std::endl;
    }

} while (0 < seconds);

if (0 > seconds) {
    std::cerr << "Function failed to become active." << std::endl;
}
else {
    std::cout << "Updated function active after " << seconds << " seconds."
        << std::endl;
}

std::cout
    << "\n\nThe new code applies an arithmetic operator to two variables, x
an y."
    << std::endl;
std::vector<Aws::String> operators = {"plus", "minus", "times", "divided-
by"};
for (size_t i = 0; i < operators.size(); ++i) {
    std::cout << "    " << i + 1 << " " << operators[i] << std::endl;
}

```

```

// 6. Invoke the updated Lambda function.
do {
    int operatorIndex = askQuestionForIntRange("Select an operator index 1 -
4 ", 1,
                                           4);
    int x = askQuestionForInt("Enter an integer for the x value ");
    int y = askQuestionForInt("Enter an integer for the y value ");

    Aws::Utils::Json::JsonValue calculateJsonPayload;
    calculateJsonPayload.WithString("action", operators[operatorIndex - 1]);
    calculateJsonPayload.WithInteger("x", x);
    calculateJsonPayload.WithInteger("y", y);
    Aws::Lambda::Model::InvokeResult calculatedResult;
    if (invokeLambdaFunction(calculateJsonPayload,
                            Aws::Lambda::Model::LogType::Tail,
                            calculatedResult, client)) {
        Aws::Utils::Json::JsonValue jsonValue(calculatedResult.GetPayload());
        Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
            jsonValue.View().GetAllObjects();
        auto iter = values.find("result");
        if (iter != values.end() && iter->second.IsIntegerType()) {
            std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                << operators[operatorIndex - 1] << " "
                << y << " is " << iter->second.AsInteger() <<
std::endl;
        }
        else if (iter != values.end() && iter->second.IsFloatingPointType())
        {
            std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                << operators[operatorIndex - 1] << " "
                << y << " is " << iter->second.AsDouble() << std::endl;
        }
        else {
            std::cout << "There was an error in execution. Here is the log."
                << std::endl;
            Aws::Utils::ByteBuffer buffer =
Aws::Utils::HashingUtils::Base64Decode(
                calculatedResult.GetLogResult());
            std::cout << "With log " << buffer.GetUnderlyingData() <<
std::endl;
        }
    }
}

```

```
        answer = askQuestion("Would you like to try another operation? (y/n) ");
    } while (answer == "y");

    std::cout
        << "A list of the lambda functions will be retrieved. Press return to
continue, ";
    std::getline(std::cin, answer);

    // 7. List the Lambda functions.

    std::vector<Aws::String> functions;
    Aws::String marker;

    do {
        Aws::Lambda::Model::ListFunctionsRequest request;
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
            request);

        if (outcome.IsSuccess()) {
            const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
            std::cout << result.GetFunctions().size()
                << " lambda functions were retrieved." << std::endl;

            for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
                functions.push_back(functionConfiguration.GetFunctionName());
                std::cout << functions.size() << " "
                    << functionConfiguration.GetDescription() << std::endl;
                std::cout << " "
                    <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                    functionConfiguration.GetRuntime()) << ": "
                    << functionConfiguration.GetHandler()
                    << std::endl;
            }
            marker = result.GetNextMarker();
        }
        else {
            std::cerr << "Error with Lambda::ListFunctions. "
```



```
        << outcome.GetError().GetMessage()
        << std::endl;
    }
} while (!marker.empty());

// 8. Get a Lambda function.
if (!functions.empty()) {
    std::stringstream question;
    question << "Choose a function to retrieve between 1 and " <<
functions.size()
        << " ";
    int functionIndex = askQuestionForIntRange(question.str(), 1,
static_cast<int>(functions.size()));

    Aws::String functionName = functions[functionIndex - 1];

    Aws::Lambda::Model::GetFunctionRequest request;
    request.SetFunctionName(functionName);

    Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

    if (outcome.IsSuccess()) {
        std::cout << "Function retrieve.\n" <<
outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
            << std::endl;
    }
    else {
        std::cerr << "Error with Lambda::GetFunction. "
            << outcome.GetError().GetMessage()
            << std::endl;
    }
}

std::cout << "The resources will be deleted. Press return to continue, ";
std::getline(std::cin, answer);

// 9. Delete the Lambda function.
bool result = deleteLambdaFunction(client);

// 10. Delete the IAM role.
return result && deleteIamRole(clientConfig);
```

```

}

//! Routine which invokes a Lambda function and returns the result.
/*!
 \param jsonPayload: Payload for invoke function.
 \param logType: Log type setting for invoke function.
 \param invokeResult: InvokeResult object to receive the result.
 \param client: Lambda client.
 \return bool: Successful completion.
 */
bool
AwsDoc::Lambda::invokeLambdaFunction(const Aws::Utils::Json::JsonValue
&jsonPayload,
                                     Aws::Lambda::Model::LogType logType,
                                     Aws::Lambda::Model::InvokeResult
&invokeResult,
                                     const Aws::Lambda::LambdaClient &client) {
    int seconds = 0;
    bool result = false;
    /*
     * In this example, the Invoke function can be called before recently created
resources are
     * available. The Invoke function is called repeatedly until the resources
are
     * available.
     */
    do {
        Aws::Lambda::Model::InvokeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetLogType(logType);
        std::shared_ptr<Aws::IOStream> payload =
Aws::MakeShared<Aws::StringStream>(
            "FunctionTest");
        *payload << jsonPayload.View().WriteReadable();
        request.SetBody(payload);
        request.SetContentType("application/json");
        Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

        if (outcome.IsSuccess()) {
            invokeResult = std::move(outcome.GetResult());
            result = true;
            break;
        }
    }
}

```

```

        // ACCESS_DENIED: because the role is not available yet.
        // RESOURCE_CONFLICT: because the Lambda function is being created or
updated.
        else if ((outcome.GetError().GetErrorType() ==
            Aws::Lambda::LambdaErrors::ACCESS_DENIED) ||
            (outcome.GetError().GetErrorType() ==
            Aws::Lambda::LambdaErrors::RESOURCE_CONFLICT)) {
            if ((seconds % 5) == 0) { // Log status every 10 seconds.
                std::cout << "Waiting for the invoke api to be available, status
" <<
                    ((outcome.GetError().GetErrorType() ==
                    Aws::Lambda::LambdaErrors::ACCESS_DENIED ?
                    "ACCESS_DENIED" : "RESOURCE_CONFLICT")) << ". " <<
seconds
                    << " seconds elapsed." << std::endl;
            }
        }
        else {
            std::cerr << "Error with Lambda::InvokeRequest. "
                << outcome.GetError().GetMessage()
                << std::endl;
            break;
        }
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
    } while (seconds < 60);


    return result;
}

```

- Untuk API detailnya, lihat topik berikut di AWS SDK for C++ API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Go

SDKuntuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Buat skenario interaktif yang menunjukkan cara memulai fungsi Lambda.

```
// GetStartedFunctionsScenario shows you how to use AWS Lambda to perform the
// following
// actions:
//
// 1. Create an AWS Identity and Access Management (IAM) role and Lambda
//    function, then upload handler code.
// 2. Invoke the function with a single parameter and get results.
// 3. Update the function code and configure with an environment variable.
// 4. Invoke the function with new parameters and get results. Display the
//    returned execution log.
// 5. List the functions for your account, then clean up resources.
type GetStartedFunctionsScenario struct {
    sdkConfig      aws.Config
    functionWrapper actions.FunctionWrapper
    questioner     demotools.IQuestioner
    helper         IScenarioHelper
    isTestRun      bool
}

// NewGetStartedFunctionsScenario constructs a GetStartedFunctionsScenario
// instance from a configuration.
// It uses the specified config to get a Lambda client and create wrappers for
// the actions
// used in the scenario.
func NewGetStartedFunctionsScenario(sdkConfig aws.Config, questioner
    demotools.IQuestioner,
    helper IScenarioHelper) GetStartedFunctionsScenario {
    lambdaClient := lambda.NewFromConfig(sdkConfig)
    return GetStartedFunctionsScenario{
        sdkConfig:      sdkConfig,
```

```

functionWrapper: actions.FunctionWrapper{LambdaClient: lambdaClient},
questioner:      questioner,
helper:          helper,
}
}

// Run runs the interactive scenario.
func (scenario GetStartedFunctionsScenario) Run() {
defer func() {
if r := recover(); r != nil {
log.Printf("Something went wrong with the demo.\n")
}
}()

log.Println(strings.Repeat("-", 88))
log.Println("Welcome to the AWS Lambda get started with functions demo.")
log.Println(strings.Repeat("-", 88))

role := scenario.GetOrCreateRole()
funcName := scenario.CreateFunction(role)
scenario.InvokeIncrement(funcName)
scenario.UpdateFunction(funcName)
scenario.InvokeCalculator(funcName)
scenario.ListFunctions()
scenario.Cleanup(role, funcName)

log.Println(strings.Repeat("-", 88))
log.Println("Thanks for watching!")
log.Println(strings.Repeat("-", 88))
}

// GetOrCreateRole checks whether the specified role exists and returns it if it
// does.
// Otherwise, a role is created that specifies Lambda as a trusted principal.
// The AWSLambdaBasicExecutionRole managed policy is attached to the role and the
// role
// is returned.
func (scenario GetStartedFunctionsScenario) GetOrCreateRole() *iamtypes.Role {
var role *iamtypes.Role
iamClient := iam.NewFromConfig(scenario.sdkConfig)
log.Println("First, we need an IAM role that Lambda can assume.")
roleName := scenario.questioner.Ask("Enter a name for the role:",
demotools.NotEmpty{})
getOutput, err := iamClient.GetRole(context.TODO(), &iam.GetRoleInput{

```

```
RoleName: aws.String(roleName)}})
if err != nil {
    var noSuch *iamtypes.NoSuchEntityException
    if errors.As(err, &noSuch) {
        log.Printf("Role %v doesn't exist. Creating it....\n", roleName)
    } else {
        log.Panicf("Couldn't check whether role %v exists. Here's why: %v\n",
            roleName, err)
    }
} else {
    role = getOutput.Role
    log.Printf("Found role %v.\n", *role.RoleName)
}
if role == nil {
    trustPolicy := PolicyDocument{
        Version: "2012-10-17",
        Statement: []PolicyStatement{{
            Effect: "Allow",
            Principal: map[string]string{"Service": "lambda.amazonaws.com"},
            Action: []string{"sts:AssumeRole"},
        }},
    }
    policyArn := "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
    createOutput, err := iamClient.CreateRole(context.TODO(), &iam.CreateRoleInput{
        AssumeRolePolicyDocument: aws.String(trustPolicy.String()),
        RoleName: aws.String(roleName),
    })
    if err != nil {
        log.Panicf("Couldn't create role %v. Here's why: %v\n", roleName, err)
    }
    role = createOutput.Role
    _, err = iamClient.AttachRolePolicy(context.TODO(), &iam.AttachRolePolicyInput{
        PolicyArn: aws.String(policyArn),
        RoleName: aws.String(roleName),
    })
    if err != nil {
        log.Panicf("Couldn't attach a policy to role %v. Here's why: %v\n", roleName,
            err)
    }
    log.Printf("Created role %v.\n", *role.RoleName)
    log.Println("Let's give AWS a few seconds to propagate resources...")
    scenario.helper.Pause(10)
}
log.Println(strings.Repeat("-", 88))
```

```

    return role
}

// CreateFunction creates a Lambda function and uploads a handler written in
// Python.
// The code for the Python handler is packaged as a []byte in .zip format.
func (scenario GetStartedFunctionsScenario) CreateFunction(role *iamtypes.Role)
string {
    log.Println("Let's create a function that increments a number.\n" +
        "The function uses the 'lambda_handler_basic.py' script found in the\n" +
        "'handlers' directory of this project.")
    funcName := scenario.questioner.Ask("Enter a name for the Lambda function:",
        demotools.NotEmpty{})
    zipPackage := scenario.helper.CreateDeploymentPackage("lambda_handler_basic.py",
        fmt.Sprintf("%v.py", funcName))
    log.Printf("Creating function %v and waiting for it to be ready.", funcName)
    funcState := scenario.functionWrapper.CreateFunction(funcName,
        fmt.Sprintf("%v.lambda_handler", funcName),
        role.Arn, zipPackage)
    log.Printf("Your function is %v.", funcState)
    log.Println(strings.Repeat("-", 88))
    return funcName
}

// InvokeIncrement invokes a Lambda function that increments a number. The
// function
// parameters are contained in a Go struct that is used to serialize the
// parameters to
// a JSON payload that is passed to the function.
// The result payload is deserialized into a Go struct that contains an int
// value.
func (scenario GetStartedFunctionsScenario) InvokeIncrement(funcName string) {
    parameters := actions.IncrementParameters{Action: "increment"}
    log.Println("Let's invoke our function. This function increments a number.")
    parameters.Number = scenario.questioner.AskInt("Enter a number to increment:",
        demotools.NotEmpty{})
    log.Printf("Invoking %v with %v...\n", funcName, parameters.Number)
    invokeOutput := scenario.functionWrapper.Invoke(funcName, parameters, false)
    var payload actions.LambdaResultInt
    err := json.Unmarshal(invokeOutput.Payload, &payload)
    if err != nil {
        log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
            funcName, err)
    }
}

```

```
log.Printf("Invoking %v with %v returned %v.\n", funcName, parameters.Number,
payload)
log.Println(strings.Repeat("-", 88))
}

// UpdateFunction updates the code for a Lambda function by uploading a simple
arithmetic
// calculator written in Python. The code for the Python handler is packaged as a
// []byte in .zip format.
// After the code is updated, the configuration is also updated with a new log
// level that instructs the handler to log additional information.
func (scenario GetStartedFunctionsScenario) UpdateFunction(funcName string) {
log.Println("Let's update the function to an arithmetic calculator.\n" +
"The function uses the 'lambda_handler_calculator.py' script found in the \n" +
"'handlers' directory of this project.")
scenario.questioner.Ask("Press Enter when you're ready.")
log.Println("Creating deployment package...")
zipPackage :=
scenario.helper.CreateDeploymentPackage("lambda_handler_calculator.py",
fmt.Sprintf("%v.py", funcName))
log.Println("...and updating the Lambda function and waiting for it to be
ready.")
funcState := scenario.functionWrapper.UpdateFunctionCode(funcName, zipPackage)
log.Printf("Updated function %v. Its current state is %v.", funcName, funcState)
log.Println("This function uses an environment variable to control logging
level.")
log.Println("Let's set it to DEBUG to get the most logging.")
scenario.functionWrapper.UpdateFunctionConfiguration(funcName,
map[string]string{"LOG_LEVEL": "DEBUG"})
log.Println(strings.Repeat("-", 88))
}

// InvokeCalculator invokes the Lambda calculator function. The parameters are
stored in a
// Go struct that is used to serialize the parameters to a JSON payload. That
payload is then passed
// to the function.
// The result payload is deserialized to a Go struct that stores the result as
either an
// int or float32, depending on the kind of operation that was specified.
func (scenario GetStartedFunctionsScenario) InvokeCalculator(funcName string) {
wantInvoke := true
choices := []string{"plus", "minus", "times", "divided-by"}
for wantInvoke {
```



```

    choice := scenario.questioner.AskChoice("Select an arithmetic operation:\n",
choices)
x := scenario.questioner.AskInt("Enter a value for x:", demotools.NotEmpty{})
y := scenario.questioner.AskInt("Enter a value for y:", demotools.NotEmpty{})
log.Printf("Invoking %v %v %v...", x, choices[choice], y)
calcParameters := actions.CalculatorParameters{
    Action: choices[choice],
    X:      x,
    Y:      y,
}
invokeOutput := scenario.functionWrapper.Invoke(funcName, calcParameters, true)
var payload any
if choice == 3 { // divide-by results in a float.
    payload = actions.LambdaResultFloat{}
} else {
    payload = actions.LambdaResultInt{}
}
err := json.Unmarshal(invokeOutput.Payload, &payload)
if err != nil {
    log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
funcName, err)
}
log.Printf("Invoking %v with %v %v %v returned %v.\n", funcName,
calcParameters.X, calcParameters.Action, calcParameters.Y, payload)
scenario.questioner.Ask("Press Enter to see the logs from the call.")
logRes, err := base64.StdEncoding.DecodeString(*invokeOutput.LogResult)
if err != nil {
    log.Panicf("Couldn't decode log result. Here's why: %v\n", err)
}
log.Println(string(logRes))
wantInvoke = scenario.questioner.AskBool("Do you want to calculate again? (y/
n)", "y")
}
log.Println(strings.Repeat("-", 88))
}

// ListFunctions lists up to the specified number of functions for your account.
func (scenario GetStartedFunctionsScenario) ListFunctions() {
    count := scenario.questioner.AskInt(
        "Let's list functions for your account. How many do you want to see?",
demotools.NotEmpty{})
    functions := scenario.functionWrapper.ListFunctions(count)
    log.Printf("Found %v functions:", len(functions))
    for _, function := range functions {

```

```
    log.Printf("\t%v", *function.FunctionName)
}
log.Println(strings.Repeat("-", 88))
}

// Cleanup removes the IAM and Lambda resources created by the example.
func (scenario GetStartedFunctionsScenario) Cleanup(role *iamtypes.Role, funcName
string) {
    if scenario.questioner.AskBool("Do you want to clean up resources created for
this example? (y/n)",
        "y") {
        iamClient := iam.NewFromConfig(scenario.sdkConfig)
        policiesOutput, err := iamClient.ListAttachedRolePolicies(context.TODO(),
            &iam.ListAttachedRolePoliciesInput{RoleName: role.RoleName})
        if err != nil {
            log.Panicf("Couldn't get policies attached to role %v. Here's why: %v\n",
                *role.RoleName, err)
        }
        for _, policy := range policiesOutput.AttachedPolicies {
            _, err = iamClient.DetachRolePolicy(context.TODO(),
                &iam.DetachRolePolicyInput{
                    PolicyArn: policy.PolicyArn, RoleName: role.RoleName,
                })
            if err != nil {
                log.Panicf("Couldn't detach policy %v from role %v. Here's why: %v\n",
                    *policy.PolicyArn, *role.RoleName, err)
            }
        }
        _, err = iamClient.DeleteRole(context.TODO(), &iam.DeleteRoleInput{RoleName:
role.RoleName})
        if err != nil {
            log.Panicf("Couldn't delete role %v. Here's why: %v\n", *role.RoleName, err)
        }
        log.Printf("Deleted role %v.\n", *role.RoleName)

        scenario.functionWrapper.DeleteFunction(funcName)
        log.Printf("Deleted function %v.\n", funcName)
    } else {
        log.Println("Okay. Don't forget to delete the resources when you're done with
them.")
    }
}
}
```

Buat struct yang membungkus tindakan Lambda individual.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
    LambdaClient *lambda.Client
}

// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(functionName string) types.State {
    var state types.State
    funcOutput, err := wrapper.LambdaClient.GetFunction(context.TODO(),
        &lambda.GetFunctionInput{
            FunctionName: aws.String(functionName),
        })
    if err != nil {
        log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
    } else {
        state = funcOutput.Configuration.State
    }
    return state
}

// CreateFunction creates a new Lambda function from code contained in the
// zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
// until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(functionName string, handlerName
    string,
    iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
    var state types.State
```

```
_, err := wrapper.LambdaClient.CreateFunction(context.TODO(),
&lambda.CreateFunctionInput{
    Code:          &types.FunctionCode{ZipFile: zipPackage.Bytes()},
    FunctionName:  aws.String(functionName),
    Role:          iamRoleArn,
    Handler:       aws.String(handlerName),
    Publish:       true,
    Runtime:       types.RuntimePython38,
})
if err != nil {
    var resConflict *types.ResourceConflictException
    if errors.As(err, &resConflict) {
        log.Printf("Function %v already exists.\n", functionName)
        state = types.StateActive
    } else {
        log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
    }
} else {
    waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
    funcOutput, err := waiter.WaitForOutput(context.TODO(),
&lambda.GetFunctionInput{
        FunctionName: aws.String(functionName)}, 1*time.Minute)
    if err != nil {
        log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
functionName, err)
    } else {
        state = funcOutput.Configuration.State
    }
}
return state
}

// UpdateFunctionCode updates the code for the Lambda function specified by
functionName.
// The existing code for the Lambda function is entirely replaced by the code in
the
// zipPackage buffer. After the update action is called, a
lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(functionName string, zipPackage
*bytes.Buffer) types.State {
    var state types.State
```

```
_, err := wrapper.LambdaClient.UpdateFunctionCode(context.TODO(),
&lambda.UpdateFunctionCodeInput{
    FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
})
if err != nil {
    log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
functionName, err)
} else {
    waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
    funcOutput, err := waiter.WaitForOutput(context.TODO(),
&lambda.GetFunctionInput{
    FunctionName: aws.String(functionName)}, 1*time.Minute)
    if err != nil {
        log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
functionName, err)
    } else {
        state = funcOutput.Configuration.State
    }
}
return state
}

// UpdateFunctionConfiguration updates a map of environment variables configured
for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(functionName string,
envVars map[string]string) {
    _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(context.TODO(),
&lambda.UpdateFunctionConfigurationInput{
    FunctionName: aws.String(functionName),
    Environment: &types.Environment{Variables: envVars},
})
    if err != nil {
        log.Panicf("Couldn't update configuration for %v. Here's why: %v",
functionName, err)
    }
}

// ListFunctions lists up to maxItems functions for the account. This function
uses a
```

```
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(maxItems int)
[]types.FunctionConfiguration {
    var functions []types.FunctionConfiguration
    paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
&lambda.ListFunctionsInput{
    MaxItems: aws.Int32(int32(maxItems)),
    })
    for paginator.HasMorePages() && len(functions) < maxItems {
        pageOutput, err := paginator.NextPage(context.TODO())
        if err != nil {
            log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
        }
        functions = append(functions, pageOutput.Functions...)
    }
    return functions
}

// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(functionName string) {
    _, err := wrapper.LambdaClient.DeleteFunction(context.TODO(),
&lambda.DeleteFunctionInput{
    FunctionName: aws.String(functionName),
    })
    if err != nil {
        log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
    }
}

// Invoke invokes the Lambda function specified by functionName, passing the
parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
tells
// Lambda to include the last few log lines in the returned result.
func (wrapper FunctionWrapper) Invoke(functionName string, parameters any, getLog
bool) *lambda.InvokeOutput {
    logType := types.LogTypeNone
    if getLog {
        logType = types.LogTypeTail
    }
}
```

```
payload, err := json.Marshal(parameters)
if err != nil {
    log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
}
invokeOutput, err := wrapper.LambdaClient.Invoke(context.TODO(),
&lambda.InvokeInput{
    FunctionName: aws.String(functionName),
    LogType:      logType,
    Payload:      payload,
})
if err != nil {
    log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
}
return invokeOutput
}

// IncrementParameters is used to serialize parameters to the increment Lambda
handler.
type IncrementParameters struct {
    Action string `json:"action"`
    Number int    `json:"number"`
}

// CalculatorParameters is used to serialize parameters to the calculator Lambda
handler.
type CalculatorParameters struct {
    Action string `json:"action"`
    X      int    `json:"x"`
    Y      int    `json:"y"`
}

// LambdaResultInt is used to deserialize an int result from a Lambda handler.
type LambdaResultInt struct {
    Result int `json:"result"`
}

// LambdaResultFloat is used to deserialize a float32 result from a Lambda
handler.
type LambdaResultFloat struct {
    Result float32 `json:"result"`
}
```

Buat struct yang mengimplementasikan fungsi untuk membantu menjalankan skenario.

```
// IScenarioHelper abstracts I/O and wait functions from a scenario so that they
// can be mocked for unit testing.
type IScenarioHelper interface {
    Pause(secs int)
    CreateDeploymentPackage(sourceFile string, destinationFile string) *bytes.Buffer
}

// ScenarioHelper lets the caller specify the path to Lambda handler functions.
type ScenarioHelper struct {
    HandlerPath string
}

// Pause waits for the specified number of seconds.
func (helper *ScenarioHelper) Pause(secs int) {
    time.Sleep(time.Duration(secs) * time.Second)
}

// CreateDeploymentPackage creates an AWS Lambda deployment package from a source
// file. The
// deployment package is stored in .zip format in a bytes.Buffer. The buffer can
// be
// used to pass a []byte to Lambda when creating the function.
// The specified destinationFile is the name to give the file when it's deployed
// to Lambda.
func (helper *ScenarioHelper) CreateDeploymentPackage(sourceFile string,
    destinationFile string) *bytes.Buffer {
    var err error
    buffer := &bytes.Buffer{}
    writer := zip.NewWriter(buffer)
    zFile, err := writer.Create(destinationFile)
    if err != nil {
        log.Panicf("Couldn't create destination archive %v. Here's why: %v\n",
            destinationFile, err)
    }
    sourceBody, err := os.ReadFile(fmt.Sprintf("%v/%v", helper.HandlerPath,
        sourceFile))
    if err != nil {
        log.Panicf("Couldn't read handler source file %v. Here's why: %v\n",
```



```
    sourceFile, err)
} else {
    _, err = zFile.Write(sourceBody)
    if err != nil {
        log.Panicf("Couldn't write handler %v to zip archive. Here's why: %v\n",
            sourceFile, err)
    }
}
err = writer.Close()
if err != nil {
    log.Panicf("Couldn't close zip writer. Here's why: %v\n", err)
}
return buffer
}
```

Tentukan handler Lambda yang menambah angka.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
    number,
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
    function
                 is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
    result = None
    action = event.get("action")
    if action == "increment":
        result = event.get("number", 0) + 1
        logger.info("Calculated result of %s", result)
    else:
```

```
        logger.error("%s is not a valid action.", action)

    response = {"result": result}
    return response
```

Tentukan handler Lambda kedua yang melakukan operasi aritmatika.

```
import logging
import os

logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}

def lambda_handler(event, context):
    """
    Accepts an action and two numbers, performs the specified action on the
    numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
    function
                   is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
    """
    # Set the log level based on a variable configured in the Lambda environment.
    logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
    logger.debug("Event: %s", event)

    action = event.get("action")
```

```
func = ACTIONS.get(action)
x = event.get("x")
y = event.get("y")
result = None
try:
    if func is not None and x is not None and y is not None:
        result = func(x, y)
        logger.info("%s %s %s is %s", x, action, y, result)
    else:
        logger.error("I can't calculate %s %s %s.", x, action, y)
except ZeroDivisionError:
    logger.warning("I can't divide %s by 0!", x)

response = {"result": result}
return response
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Go API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
/*
 * Lambda function names appear as:
 *
 * arn:aws:lambda:us-west-2:335556666777:function:HelloFunction
 *
 * To find this value, look at the function in the AWS Management Console.
 *
 * Before running this Java code example, set up your development environment,
including your credentials.
 *
 * For more information, see this documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example performs the following tasks:
 *
 * 1. Creates an AWS Lambda function.
 * 2. Gets a specific AWS Lambda function.
 * 3. Lists all Lambda functions.
 * 4. Invokes a Lambda function.
 * 5. Updates the Lambda function code and invokes it again.
 * 6. Updates a Lambda function's configuration value.
 * 7. Deletes a Lambda function.
 */

public class LambdaScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
"-");

    public static void main(String[] args) throws InterruptedException {
        final String usage = ""

            Usage:
                <functionName> <filePath> <role> <handler> <bucketName> <key>

\s

            Where:
                functionName - The name of the Lambda function.\s
                filePath - The path to the .zip or .jar where the code is
located.\s

                role - The AWS Identity and Access Management (IAM) service
role that has Lambda permissions.\s

```

```
        handler - The fully qualified method name (for example,
example.Handler::handleRequest).\s
        bucketName - The Amazon Simple Storage Service (Amazon S3)
bucket name that contains the .zip or .jar used to update the Lambda function's
code.\s
        key - The Amazon S3 key name that represents the .zip or .jar
(for example, LambdaHello-1.0-SNAPSHOT.jar).
        """;

    if (args.length != 6) {
        System.out.println(usage);
        System.exit(1);
    }

    String functionName = args[0];
    String filePath = args[1];
    String role = args[2];
    String handler = args[3];
    String bucketName = args[4];
    String key = args[5];

    Region region = Region.US_WEST_2;
    LambdaClient awsLambda = LambdaClient.builder()
        .region(region)
        .build();

    System.out.println(DASHES);
    System.out.println("Welcome to the AWS Lambda example scenario.");
    System.out.println(DASHES);

    System.out.println(DASHES);
    System.out.println("1. Create an AWS Lambda function.");
    String funArn = createLambdaFunction(awsLambda, functionName, filePath,
role, handler);
    System.out.println("The AWS Lambda ARN is " + funArn);
    System.out.println(DASHES);

    System.out.println(DASHES);
    System.out.println("2. Get the " + functionName + " AWS Lambda
function.");
    getFunction(awsLambda, functionName);
    System.out.println(DASHES);

    System.out.println(DASHES);
```

```
System.out.println("3. List all AWS Lambda functions.");
listFunctions(awsLambda);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("4. Invoke the Lambda function.");
System.out.println("*** Sleep for 1 min to get Lambda function ready.");
Thread.sleep(60000);
invokeFunction(awsLambda, functionName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("5. Update the Lambda function code and invoke it
again.");
updateFunctionCode(awsLambda, functionName, bucketName, key);
System.out.println("*** Sleep for 1 min to get Lambda function ready.");
Thread.sleep(60000);
invokeFunction(awsLambda, functionName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("6. Update a Lambda function's configuration value.");
updateFunctionConfiguration(awsLambda, functionName, handler);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("7. Delete the AWS Lambda function.");
LambdaScenario.deleteLambdaFunction(awsLambda, functionName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("The AWS Lambda scenario completed successfully");
System.out.println(DASHES);
awsLambda.close();
}

public static String createLambdaFunction(LambdaClient awsLambda,
    String functionName,
    String filePath,
    String role,
    String handler) {

    try {
        LambdaWaiter waiter = awsLambda.waiter();
```

```
InputStream is = new FileInputStream(filePath);
SdkBytes fileToUpload = SdkBytes.fromInputStream(is);

FunctionCode code = FunctionCode.builder()
    .zipFile(fileToUpload)
    .build();

CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
    .functionName(functionName)
    .description("Created by the Lambda Java API")
    .code(code)
    .handler(handler)
    .runtime(Runtime.JAVA8)
    .role(role)
    .build();

// Create a Lambda function using a waiter
CreateFunctionResponse functionResponse =
awsLambda.createFunction(functionRequest);
GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
    .functionName(functionName)
    .build();
WaiterResponse<GetFunctionResponse> waiterResponse =
waiter.waitUntilFunctionExists(getFunctionRequest);
waiterResponse.matched().response().ifPresent(System.out::println);
return functionResponse.functionArn();

} catch (LambdaException | FileNotFoundException e) {
    System.err.println(e.getMessage());
    System.exit(1);
}
return "";
}

public static void getFunction(LambdaClient awsLambda, String functionName) {
    try {
        GetFunctionRequest functionRequest = GetFunctionRequest.builder()
            .functionName(functionName)
            .build();

        GetFunctionResponse response =
awsLambda.getFunction(functionRequest);
```

```
        System.out.println("The runtime of this Lambda function is " +
response.configuration().runtime());

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void listFunctions(LambdaClient awsLambda) {
    try {
        ListFunctionsResponse functionResult = awsLambda.listFunctions();
        List<FunctionConfiguration> list = functionResult.functions();
        for (FunctionConfiguration config : list) {
            System.out.println("The function name is " +
config.functionName());
        }

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void invokeFunction(LambdaClient awsLambda, String
functionName) {

    InvokeResponse res;
    try {
        // Need a SdkBytes instance for the payload.
        JSONObject jsonObj = new JSONObject();
        jsonObj.put("inputValue", "2000");
        String json = jsonObj.toString();
        SdkBytes payload = SdkBytes.fromUtf8String(json);

        InvokeRequest request = InvokeRequest.builder()
            .functionName(functionName)
            .payload(payload)
            .build();

        res = awsLambda.invoke(request);
        String value = res.payload().asUtf8String();
        System.out.println(value);
    }
}
```



```
    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void updateFunctionCode(LambdaClient awsLambda, String
functionName, String bucketName, String key) {
    try {
        LambdaWaiter waiter = awsLambda.waiter();
        UpdateFunctionCodeRequest functionCodeRequest =
UpdateFunctionCodeRequest.builder()
            .functionName(functionName)
            .publish(true)
            .s3Bucket(bucketName)
            .s3Key(key)
            .build();

        UpdateFunctionCodeResponse response =
awsLambda.updateFunctionCode(functionCodeRequest);
        GetFunctionConfigurationRequest getFunctionConfigRequest =
GetFunctionConfigurationRequest.builder()
            .functionName(functionName)
            .build();

        WaiterResponse<GetFunctionConfigurationResponse> waiterResponse =
waiter
            .waitUntilFunctionUpdated(getFunctionConfigRequest);
        waiterResponse.matched().response().ifPresent(System.out::println);
        System.out.println("The last modified value is " +
response.lastModified());

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void updateFunctionConfiguration(LambdaClient awsLambda, String
functionName, String handler) {
    try {
        UpdateFunctionConfigurationRequest configurationRequest =
UpdateFunctionConfigurationRequest.builder()
            .functionName(functionName)
```

```
        .handler(handler)
        .runtime(Runtime.JAVA11)
        .build();

        awsLambda.updateFunctionConfiguration(configurationRequest);

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void deleteLambdaFunction(LambdaClient awsLambda, String
functionName) {
    try {
        DeleteFunctionRequest request = DeleteFunctionRequest.builder()
            .functionName(functionName)
            .build();

        awsLambda.deleteFunction(request);
        System.out.println("The " + functionName + " function was deleted");

    } catch (LambdaException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Java 2.x API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Buat peran AWS Identity and Access Management (IAM) yang memberikan izin Lambda untuk menulis ke log.

```
log(`Creating role (${NAME_ROLE_LAMBDA})...`);
const response = await createRole(NAME_ROLE_LAMBDA);

import { AttachRolePolicyCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} policyArn
 * @param {string} roleName
 */
export const attachRolePolicy = (policyArn, roleName) => {
  const command = new AttachRolePolicyCommand({
    PolicyArn: policyArn,
    RoleName: roleName,
  });

  return client.send(command);
};
```

Buat fungsi Lambda dan unggah kode handler.

```
const createFunction = async (funcName, roleArn) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);

  const command = new CreateFunctionCommand({
```

```

Code: { ZipFile: code },
FunctionName: funcName,
Role: roleArn,
Architectures: [Architecture.arm64],
Handler: "index.handler", // Required when sending a .zip file
PackageType: PackageType.Zip, // Required when sending a .zip file
Runtime: Runtime.nodejs16x, // Required when sending a .zip file
});

return client.send(command);
};

```

Panggil fungsi dengan satu parameter dan dapatkan hasil.

```

const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};

```

Perbarui kode fungsi dan konfigurasi lingkungan Lambda dengan variabel lingkungan.

```

const updateFunctionCode = async (funcName, newFunc) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
  const command = new UpdateFunctionCodeCommand({
    ZipFile: code,
    FunctionName: funcName,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });
};

```

```

    return client.send(command);
  };

  const updateFunctionConfiguration = (funcName) => {
    const client = new LambdaClient({});
    const config = readFileSync(`${dirname}../functions/config.json`).toString();
    const command = new UpdateFunctionConfigurationCommand({
      ...JSON.parse(config),
      FunctionName: funcName,
    });
    return client.send(command);
  };

```

Buat daftar fungsi untuk akun Anda.

```

const listFunctions = () => {
  const client = new LambdaClient({});
  const command = new ListFunctionsCommand({});

  return client.send(command);
};

```

Hapus IAM peran dan fungsi Lambda.

```

import { DeleteRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const deleteRole = (roleName) => {
  const command = new DeleteRoleCommand({ RoleName: roleName });
  return client.send(command);
};

/**
 * @param {string} funcName
 */

```

```
const deleteFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new DeleteFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for JavaScript API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Kotlin

SDK untuk Kotlin

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
suspend fun main(args: Array<String>) {
  val usage = """
    Usage:
      <functionName> <role> <handler> <bucketName> <updatedBucketName>
    <key>

    Where:
      functionName - The name of the AWS Lambda function.
      role - The AWS Identity and Access Management (IAM) service role that
      has AWS Lambda permissions.
      handler - The fully qualified method name (for example,
      example.Handler::handleRequest).
```

```
        bucketName - The Amazon Simple Storage Service (Amazon S3) bucket
name that contains the ZIP or JAR used for the Lambda function's code.
        updatedBucketName - The Amazon S3 bucket name that contains the .zip
or .jar used to update the Lambda function's code.
        key - The Amazon S3 key name that represents the .zip or .jar file
(for example, LambdaHello-1.0-SNAPSHOT.jar).
        """"

if (args.size != 6) {
    println(usage)
    exitProcess(1)
}

val functionName = args[0]
val role = args[1]
val handler = args[2]
val bucketName = args[3]
val updatedBucketName = args[4]
val key = args[5]

println("Creating a Lambda function named $functionName.")
val funArn = createScFunction(functionName, bucketName, key, handler, role)
println("The AWS Lambda ARN is $funArn")

// Get a specific Lambda function.
println("Getting the $functionName AWS Lambda function.")
getFunction(functionName)

// List the Lambda functions.
println("Listing all AWS Lambda functions.")
listFunctionsSc()

// Invoke the Lambda function.
println("*** Invoke the Lambda function.")
invokeFunctionSc(functionName)

// Update the AWS Lambda function code.
println("*** Update the Lambda function code.")
updateFunctionCode(functionName, updatedBucketName, key)

// println("*** Invoke the function again after updating the code.")
invokeFunctionSc(functionName)

// Update the AWS Lambda function configuration.
```

```
println("Update the run time of the function.")
updateFunctionConfiguration(functionName, handler)

// Delete the AWS Lambda function.
println("Delete the AWS Lambda function.")
delFunction(functionName)
}

suspend fun createScFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String,
): String {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }

    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java8
        }

    // Create a Lambda function using a waiter
    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitForFunctionActive {
            functionName = myFunctionName
        }
        return functionResponse.functionArn.toString()
    }
}

suspend fun getFunction(functionNameVal: String) {
    val functionRequest =
        GetFunctionRequest {
```



```
        functionName = functionNameVal
    }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val response = awsLambda.getFunction(functionRequest)
        println("The runtime of this Lambda function is
    ${response.configuration?.runtime}")
    }
}

suspend fun listFunctionsSc() {
    val request =
        ListFunctionsRequest {
            maxItems = 10
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val response = awsLambda.listFunctions(request)
        response.functions?.forEach { function ->
            println("The function name is ${function.functionName}")
        }
    }
}

suspend fun invokeFunctionSc(functionNameVal: String) {
    val json = """"{"inputValue":"1000"}""""
    val byteArray = json.trimIndent().encodeToByteArray()
    val request =
        InvokeRequest {
            functionName = functionNameVal
            payload = byteArray
            logType = LogType.Tail
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val res = awsLambda.invoke(request)
        println("The function payload is
    ${res.payload?.toString(Charsets.UTF_8)}")
    }
}

suspend fun updateFunctionCode(
    functionNameVal: String?,
    bucketName: String?,
```

```
        key: String?,
    ) {
        val functionCodeRequest =
            UpdateFunctionCodeRequest {
                functionName = functionNameVal
                publish = true
                s3Bucket = bucketName
                s3Key = key
            }

        LambdaClient { region = "us-west-2" }.use { awsLambda ->
            val response = awsLambda.updateFunctionCode(functionCodeRequest)
            awsLambda.waitUntilFunctionUpdated {
                functionName = functionNameVal
            }
            println("The last modified value is " + response.lastModified)
        }
    }
}

suspend fun updateFunctionConfiguration(
    functionNameVal: String?,
    handlerVal: String?,
) {
    val configurationRequest =
        UpdateFunctionConfigurationRequest {
            functionName = functionNameVal
            handler = handlerVal
            runtime = Runtime.Java11
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        awsLambda.updateFunctionConfiguration(configurationRequest)
    }
}

suspend fun delFunction(myFunctionName: String) {
    val request =
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

```
}  
}
```

- Untuk API detailnya, lihat topik berikut AWS SDK untuk API referensi Kotlin.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
namespace Lambda;  
  
use Aws\S3\S3Client;  
use GuzzleHttp\Psr7\Stream;  
use Iam\IAMService;  
  
class GettingStartedWithLambda  
{  
    public function run()  
    {  
        echo("\n");  
        echo("-----\n");  
        print("Welcome to the AWS Lambda getting started demo using PHP!\n");  
        echo("-----\n");  
    }  
}
```

```
$clientArgs = [
    'region' => 'us-west-2',
    'version' => 'latest',
    'profile' => 'default',
];
$uniqid = uniqid();

$iamService = new IAMService();
$s3client = new S3Client($clientArgs);
$lambdaService = new LambdaService();

echo "First, let's create a role to run our Lambda code.\n";
$roleName = "test-lambda-role-$uniqid";
$rolePolicyDocument = "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
        {
            \"Effect\": \"Allow\",
            \"Principal\": {
                \"Service\": \"lambda.amazonaws.com\"
            },
            \"Action\": \"sts:AssumeRole\"
        }
    ]
}";
$role = $iamService->createRole($roleName, $rolePolicyDocument);
echo "Created role {$role['RoleName']}. \n";

$iamService->attachRolePolicy(
    $role['RoleName'],
    "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
);
echo "Attached the AWSLambdaBasicExecutionRole to {$role['RoleName']}.
\n";

echo "\nNow let's create an S3 bucket and upload our Lambda code there.
\n";

$bucketName = "test-example-bucket-$uniqid";
$s3client->createBucket([
    'Bucket' => $bucketName,
]);
echo "Created bucket $bucketName.\n";

$functionName = "doc_example_lambda_$uniqid";
```

```
$codeBasic = __DIR__ . "/lambda_handler_basic.zip";
$handler = "lambda_handler_basic";
$file = file_get_contents($codeBasic);
$s3client->putObject([
    'Bucket' => $bucketName,
    'Key' => $functionName,
    'Body' => $file,
]);
echo "Uploaded the Lambda code.\n";

$createLambdaFunction = $lambdaService->createFunction($functionName,
$role, $bucketName, $handler);
// Wait until the function has finished being created.
do {
    $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
    } while ($getLambdaFunction['Configuration']['State'] == "Pending");
    echo "Created Lambda function {$getLambdaFunction['Configuration']
['FunctionName']}. \n";

    sleep(1);

    echo "\nOk, let's invoke that Lambda code.\n";
    $basicParams = [
        'action' => 'increment',
        'number' => 3,
    ];
    /** @var Stream $invokeFunction */
    $invokeFunction = $lambdaService->invoke($functionName, $basicParams)
['Payload'];
    $result = json_decode($invokeFunction->getContents())->result;
    echo "After invoking the Lambda code with the input of
    {$basicParams['number']} we received $result.\n";

    echo "\nSince that's working, let's update the Lambda code.\n";
    $codeCalculator = "lambda_handler_calculator.zip";
    $handlerCalculator = "lambda_handler_calculator";
    echo "First, put the new code into the S3 bucket.\n";
    $file = file_get_contents($codeCalculator);
    $s3client->putObject([
        'Bucket' => $bucketName,
        'Key' => $functionName,
        'Body' => $file,
    ]);
```

```
    echo "New code uploaded.\n";

    $lambdaService->updateFunctionCode($functionName, $bucketName,
    $functionName);
    // Wait for the Lambda code to finish updating.
    do {
        $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
    "Successful");
    echo "New Lambda code uploaded.\n";

    $environment = [
        'Variable' => ['Variables' => ['LOG_LEVEL' => 'DEBUG']],
    ];
    $lambdaService->updateFunctionConfiguration($functionName,
    $handlerCalculator, $environment);
    do {
        $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
    "Successful");
    echo "Lambda code updated with new handler and a LOG_LEVEL of DEBUG for
    more information.\n";

    echo "Invoke the new code with some new data.\n";
    $calculatorParams = [
        'action' => 'plus',
        'x' => 5,
        'y' => 4,
    ];
    $invokeFunction = $lambdaService->invoke($functionName,
    $calculatorParams, "Tail");
    $result = json_decode($invokeFunction['Payload']->getContents())->result;
    echo "Indeed, {$calculatorParams['x']} + {$calculatorParams['y']} does
    equal $result.\n";
    echo "Here's the extra debug info: ";
    echo base64_decode($invokeFunction['LogResult']) . "\n";

    echo "\nBut what happens if you try to divide by zero?\n";
    $divZeroParams = [
        'action' => 'divide',
        'x' => 5,
        'y' => 0,
```

```
];
$invokeFunction = $lambdaService->invoke($functionName, $divZeroParams,
"Tail");
$result = json_decode($invokeFunction['Payload']->getContents())->result;
echo "You get a |$result| result.\n";
echo "And an error message: ";
echo base64_decode($invokeFunction['LogResult']) . "\n";

echo "\nHere's all the Lambda functions you have in this Region:\n";
$listLambdaFunctions = $lambdaService->listFunctions(5);
$allLambdaFunctions = $listLambdaFunctions['Functions'];
$next = $listLambdaFunctions->get('NextMarker');
while ($next != false) {
    $listLambdaFunctions = $lambdaService->listFunctions(5, $next);
    $next = $listLambdaFunctions->get('NextMarker');
    $allLambdaFunctions = array_merge($allLambdaFunctions,
$listLambdaFunctions['Functions']);
}
foreach ($allLambdaFunctions as $function) {
    echo "{$function['FunctionName']}\n";
}

echo "\n\nAnd don't forget to clean up your data!\n";

$lambdaService->deleteFunction($functionName);
echo "Deleted Lambda function.\n";
$iamService->deleteRole($role['RoleName']);
echo "Deleted Role.\n";
$deleteObjects = $s3client->listObjectsV2([
    'Bucket' => $bucketName,
]);
$deleteObjects = $s3client->deleteObjects([
    'Bucket' => $bucketName,
    'Delete' => [
        'Objects' => $deleteObjects['Contents'],
    ]
]);
echo "Deleted all objects from the S3 bucket.\n";
$s3client->deleteBucket(['Bucket' => $bucketName]);
echo "Deleted the bucket.\n";
}
}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for PHP API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Tentukan handler Lambda yang menambah angka.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
    number,
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
    function
        is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
```



```
result = None
action = event.get("action")
if action == "increment":
    result = event.get("number", 0) + 1
    logger.info("Calculated result of %s", result)
else:
    logger.error("%s is not a valid action.", action)

response = {"result": result}
return response
```

Tentukan handler Lambda kedua yang melakukan operasi aritmatika.

```
import logging
import os

logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}

def lambda_handler(event, context):
    """
    Accepts an action and two numbers, performs the specified action on the
    numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
    function
                 is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
```

```
"""
# Set the log level based on a variable configured in the Lambda environment.
logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
logger.debug("Event: %s", event)

action = event.get("action")
func = ACTIONS.get(action)
x = event.get("x")
y = event.get("y")
result = None
try:
    if func is not None and x is not None and y is not None:
        result = func(x, y)
        logger.info("%s %s %s is %s", x, action, y, result)
    else:
        logger.error("I can't calculate %s %s %s.", x, action, y)
except ZeroDivisionError:
    logger.warning("I can't divide %s by 0!", x)

response = {"result": result}
return response
```

Buat fungsi yang membungkus tindakan Lambda.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource

    @staticmethod
    def create_deployment_package(source_file, destination_file):
        """
        Creates a Lambda deployment package in .zip format in an in-memory
        buffer. This
        buffer can be passed directly to Lambda when creating the function.

        :param source_file: The name of the file that contains the Lambda handler
        function.
```

```
        :param destination_file: The name to give the file when it's deployed to
Lambda.
        :return: The deployment package.
        """
        buffer = io.BytesIO()
        with zipfile.ZipFile(buffer, "w") as zipped:
            zipped.write(source_file, destination_file)
        buffer.seek(0)
        return buffer.read()

def get_iam_role(self, iam_role_name):
    """
    Get an AWS Identity and Access Management (IAM) role.

    :param iam_role_name: The name of the role to retrieve.
    :return: The IAM role.
    """
    role = None
    try:
        temp_role = self.iam_resource.Role(iam_role_name)
        temp_role.load()
        role = temp_role
        logger.info("Got IAM role %s", role.name)
    except ClientError as err:
        if err.response["Error"]["Code"] == "NoSuchEntity":
            logger.info("IAM role %s does not exist.", iam_role_name)
        else:
            logger.error(
                "Couldn't get IAM role %s. Here's why: %s: %s",
                iam_role_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
    return role

def create_iam_role_for_lambda(self, iam_role_name):
    """
    Creates an IAM role that grants the Lambda function basic permissions. If
a
    role with the specified name already exists, it is used for the demo.

    :param iam_role_name: The name of the role to create.
```

```
        :return: The role and a value that indicates whether the role is newly
        created.
        """
        role = self.get_iam_role(iam_role_name)
        if role is not None:
            return role, False

        lambda_assume_role_policy = {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {"Service": "lambda.amazonaws.com"},
                    "Action": "sts:AssumeRole",
                }
            ],
        }
        policy_arn = "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"

        try:
            role = self.iam_resource.create_role(
                RoleName=iam_role_name,
                AssumeRolePolicyDocument=json.dumps(lambda_assume_role_policy),
            )
            logger.info("Created role %s.", role.name)
            role.attach_policy(PolicyArn=policy_arn)
            logger.info("Attached basic execution policy to role %s.", role.name)
        except ClientError as error:
            if error.response["Error"]["Code"] == "EntityAlreadyExists":
                role = self.iam_resource.Role(iam_role_name)
                logger.warning("The role %s already exists. Using it.",
iam_role_name)
            else:
                logger.exception(
                    "Couldn't create role %s or attach policy %s.",
                    iam_role_name,
                    policy_arn,
                )
                raise

        return role, True

    def get_function(self, function_name):
```

```

"""
Gets data about a Lambda function.

:param function_name: The name of the function.
:return: The function data.
"""
response = None
try:
    response =
self.lambda_client.get_function(FunctionName=function_name)
except ClientError as err:
    if err.response["Error"]["Code"] == "ResourceNotFoundException":
        logger.info("Function %s does not exist.", function_name)
    else:
        logger.error(
            "Couldn't get function %s. Here's why: %s: %s",
            function_name,
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
return response

def create_function(
    self, function_name, handler_name, iam_role, deployment_package
):
    """
    Deploys a Lambda function.

    :param function_name: The name of the Lambda function.
    :param handler_name: The fully qualified name of the handler function.
    This
        must include the file name and the function name.
    :param iam_role: The IAM role to use for the function.
    :param deployment_package: The deployment package that contains the
    function
        code in .zip format.
    :return: The Amazon Resource Name (ARN) of the newly created function.
    """
    try:
        response = self.lambda_client.create_function(
            FunctionName=function_name,
            Description="AWS Lambda doc example",

```

```
        Runtime="python3.8",
        Role=iam_role.arn,
        Handler=handler_name,
        Code={"ZipFile": deployment_package},
        Publish=True,
    )
    function_arn = response["FunctionArn"]
    waiter = self.lambda_client.get_waiter("function_active_v2")
    waiter.wait(FunctionName=function_name)
    logger.info(
        "Created function '%s' with ARN: '%s'.",
        function_name,
        response["FunctionArn"],
    )
except ClientError:
    logger.error("Couldn't create function %s.", function_name)
    raise
else:
    return function_arn

def delete_function(self, function_name):
    """
    Deletes a Lambda function.

    :param function_name: The name of the function to delete.
    """
    try:
        self.lambda_client.delete_function(FunctionName=function_name)
    except ClientError:
        logger.exception("Couldn't delete function %s.", function_name)
        raise

def invoke_function(self, function_name, function_params, get_log=False):
    """
    Invokes a Lambda function.

    :param function_name: The name of the function to invoke.
    :param function_params: The parameters of the function as a dict. This
dict
                           is serialized to JSON before it is sent to
Lambda.
```

```
        :param get_log: When true, the last 4 KB of the execution log are
included in
                the response.
:return: The response from the function invocation.
"""
try:
    response = self.lambda_client.invoke(
        FunctionName=function_name,
        Payload=json.dumps(function_params),
        LogType="Tail" if get_log else "None",
    )
    logger.info("Invoked function %s.", function_name)
except ClientError:
    logger.exception("Couldn't invoke function %s.", function_name)
    raise
return response

def update_function_code(self, function_name, deployment_package):
    """
    Updates the code for a Lambda function by submitting a .zip archive that
contains
    the code for the function.

    :param function_name: The name of the function to update.
    :param deployment_package: The function code to update, packaged as bytes
in
                .zip format.
:return: Data about the update, including the status.
"""
try:
    response = self.lambda_client.update_function_code(
        FunctionName=function_name, ZipFile=deployment_package
    )
except ClientError as err:
    logger.error(
        "Couldn't update function %s. Here's why: %s: %s",
        function_name,
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
else:
    return response
```

```
def update_function_configuration(self, function_name, env_vars):
    """
    Updates the environment variables for a Lambda function.

    :param function_name: The name of the function to update.
    :param env_vars: A dict of environment variables to update.
    :return: Data about the update, including the status.
    """
    try:
        response = self.lambda_client.update_function_configuration(
            FunctionName=function_name, Environment={"Variables": env_vars}
        )
    except ClientError as err:
        logger.error(
            "Couldn't update function configuration %s. Here's why: %s: %s",
            function_name,
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
    else:
        return response

def list_functions(self):
    """
    Lists the Lambda functions for the current account.
    """
    try:
        func_paginator = self.lambda_client.get_paginator("list_functions")
        for func_page in func_paginator.paginate():
            for func in func_page["Functions"]:
                print(func["FunctionName"])
                desc = func.get("Description")
                if desc:
                    print(f"\t{desc}")
                    print(f"\t{func['Runtime']}: {func['Handler']}")
    except ClientError as err:
        logger.error(
            "Couldn't list functions. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
```



```
)
raise
```

Buat fungsi yang menjalankan skenario.

```
class UpdateFunctionWaiter(CustomWaiter):
    """A custom waiter that waits until a function is successfully updated."""

    def __init__(self, client):
        super().__init__(
            "UpdateSuccess",
            "GetFunction",
            "Configuration.LastUpdateStatus",
            {"Successful": WaitState.SUCCESS, "Failed": WaitState.FAILURE},
            client,
        )

    def wait(self, function_name):
        self._wait(FunctionName=function_name)

def run_scenario(lambda_client, iam_resource, basic_file, calculator_file,
lambda_name):
    """
    Runs the scenario.

    :param lambda_client: A Boto3 Lambda client.
    :param iam_resource: A Boto3 IAM resource.
    :param basic_file: The name of the file that contains the basic Lambda
    handler.
    :param calculator_file: The name of the file that contains the calculator
    Lambda handler.
    :param lambda_name: The name to give resources created for the scenario, such
    as the
                        IAM role and the Lambda function.
    """
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    print("-" * 88)
```

```
print("Welcome to the AWS Lambda getting started with functions demo.")
print("-" * 88)

wrapper = LambdaWrapper(lambda_client, iam_resource)

print("Checking for IAM role for Lambda...")
iam_role, should_wait = wrapper.create_iam_role_for_lambda(lambda_name)
if should_wait:
    logger.info("Giving AWS time to create resources...")
    wait(10)

print(f"Looking for function {lambda_name}...")
function = wrapper.get_function(lambda_name)
if function is None:
    print("Zipping the Python script into a deployment package...")
    deployment_package = wrapper.create_deployment_package(
        basic_file, f"{lambda_name}.py"
    )
    print(f"...and creating the {lambda_name} Lambda function.")
    wrapper.create_function(
        lambda_name, f"{lambda_name}.lambda_handler", iam_role,
        deployment_package
    )
else:
    print(f"Function {lambda_name} already exists.")
print("-" * 88)

print(f"Let's invoke {lambda_name}. This function increments a number.")
action_params = {
    "action": "increment",
    "number": q.ask("Give me a number to increment: ", q.is_int),
}
print(f"Invoking {lambda_name}...")
response = wrapper.invoke_function(lambda_name, action_params)
print(
    f"Incrementing {action_params['number']} resulted in "
    f"{json.load(response['Payload'])}"
)
print("-" * 88)

print(f"Let's update the function to an arithmetic calculator.")
q.ask("Press Enter when you're ready.")
print("Creating a new deployment package...")
deployment_package = wrapper.create_deployment_package(
```

```

calculator_file, f"{lambda_name}.py"
)
print(f"...and updating the {lambda_name} Lambda function.")
update_waiter = UpdateFunctionWaiter(lambda_client)
wrapper.update_function_code(lambda_name, deployment_package)
update_waiter.wait(lambda_name)
print(f"This function uses an environment variable to control logging
level.")
print(f"Let's set it to DEBUG to get the most logging.")
wrapper.update_function_configuration(
    lambda_name, {"LOG_LEVEL": logging.getLevelName(logging.DEBUG)}
)

actions = ["plus", "minus", "times", "divided-by"]
want_invoke = True
while want_invoke:
    print(f"Let's invoke {lambda_name}. You can invoke these actions:")
    for index, action in enumerate(actions):
        print(f"{index + 1}: {action}")
    action_params = {}
    action_index = q.ask(
        "Enter the number of the action you want to take: ",
        q.is_int,
        q.in_range(1, len(actions)),
    )
    action_params["action"] = actions[action_index - 1]
    print(f"You've chosen to invoke 'x {action_params['action']} y'.")
    action_params["x"] = q.ask("Enter a value for x: ", q.is_int)
    action_params["y"] = q.ask("Enter a value for y: ", q.is_int)
    print(f"Invoking {lambda_name}...")
    response = wrapper.invoke_function(lambda_name, action_params, True)
    print(
        f"Calculating {action_params['x']} {action_params['action']}
{action_params['y']} "
        f"resulted in {json.load(response['Payload'])}"
    )
    q.ask("Press Enter to see the logs from the call.")
    print(base64.b64decode(response["LogResult"]).decode())
    want_invoke = q.ask("That was fun. Shall we do it again? (y/n) ",
q.is_yesno)
    print("-" * 88)

    if q.ask(

```

```
        "Do you want to list all of the functions in your account? (y/n) ",
q.is_yesno
    ):
        wrapper.list_functions()
    print("-" * 88)

    if q.ask("Ready to delete the function and role? (y/n) ", q.is_yesno):
        for policy in iam_role.attached_policies.all():
            policy.detach_role(RoleName=iam_role.name)
        iam_role.delete()
        print(f"Deleted role {lambda_name}.")
        wrapper.delete_function(lambda_name)
        print(f"Deleted function {lambda_name}.")

    print("\nThanks for watching!")
    print("-" * 88)

if __name__ == "__main__":
    try:
        run_scenario(
            boto3.client("lambda"),
            boto3.resource("iam"),
            "lambda_handler_basic.py",
            "lambda_handler_calculator.py",
            "doc_example_lambda_calculator",
        )
    except Exception:
        logging.exception("Something went wrong with the demo!")
```

- Untuk API detailnya, lihat topik berikut AWS SDK untuk Referensi Python (Boto3). API
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

Siapkan IAM izin prasyarat untuk fungsi Lambda yang mampu menulis log.

```
# Get an AWS Identity and Access Management (IAM) role.
#
# @param iam_role_name: The name of the role to retrieve.
# @param action: Whether to create or destroy the IAM apparatus.
# @return: The IAM role.
def manage_iam(iam_role_name, action)
  role_policy = {
    'Version': "2012-10-17",
    'Statement': [
      {
        'Effect': "Allow",
        'Principal': {
          'Service': "lambda.amazonaws.com"
        },
        'Action': "sts:AssumeRole"
      }
    ]
  }
  case action
  when "create"
    role = $iam_client.create_role(
      role_name: iam_role_name,
      assume_role_policy_document: role_policy.to_json
    )
    $iam_client.attach_role_policy(
      {
        policy_arn: "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole",
        role_name: iam_role_name
      }
    )
  end
end
```

```

    $iam_client.wait_until(:role_exists, { role_name: iam_role_name }) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
    @logger.debug("Successfully created IAM role: #{role['role']['arn']}")
    @logger.debug("Enforcing a 10-second sleep to allow IAM role to activate
fully.")
    sleep(10)
    return role, role_policy.to_json
  when "destroy"
    $iam_client.detach_role_policy(
      {
        policy_arn: "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole",
        role_name: iam_role_name
      }
    )
    $iam_client.delete_role(
      role_name: iam_role_name
    )
    @logger.debug("Detached policy & deleted IAM role: #{iam_role_name}")
  else
    raise "Incorrect action provided. Must provide 'create' or 'destroy'"
  end
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error creating role or attaching policy:\n
#{e.message}")
end

```

Tentukan handler Lambda yang menambah angka yang disediakan sebagai parameter pemanggilan.

```

require "logger"

# A function that increments a whole number by one (1) and logs the result.
# Requires a manually-provided runtime parameter, 'number', which must be Int
#
# @param event [Hash] Parameters sent when the function is invoked
# @param context [Hash] Methods and properties that provide information
# about the invocation, function, and execution environment.
# @return incremented_number [String] The incremented number.
def lambda_handler(event:, context:)

```

```
logger = Logger.new($stdout)
log_level = ENV["LOG_LEVEL"]
logger.level = case log_level
  when "debug"
    Logger::DEBUG
  when "info"
    Logger::INFO
  else
    Logger::ERROR
  end
logger.debug("This is a debug log message.")
logger.info("This is an info log message. Code executed successfully!")
number = event["number"].to_i
incremented_number = number + 1
logger.info("You provided #{number.round} and it was incremented to
#{incremented_number.round}")
incremented_number.round.to_s
end
```

Zip fungsi Lambda Anda ke dalam paket penerapan.

```
# Creates a Lambda deployment package in .zip format.
# This zip can be passed directly as a string to Lambda when creating the
function.
#
# @param source_file: The name of the object, without suffix, for the Lambda
file and zip.
# @return: The deployment package.
def create_deployment_package(source_file)
  Dir.chdir(File.dirname(__FILE__))
  if File.exist?("lambda_function.zip")
    File.delete("lambda_function.zip")
    @logger.debug("Deleting old zip: lambda_function.zip")
  end
  Zip::File.open("lambda_function.zip", create: true) {
    |zipfile|
    zipfile.add("lambda_function.rb", "#{source_file}.rb")
  }
  @logger.debug("Zipping #{source_file}.rb into: lambda_function.zip.")
  File.read("lambda_function.zip").to_s
rescue StandardError => e
```

```
@logger.error("There was an error creating deployment package:\n\n#{e.message}")\nend
```

Buat fungsi Lambda baru.

```
# Deploys a Lambda function.\n#\n# @param function_name: The name of the Lambda function.\n# @param handler_name: The fully qualified name of the handler function. This\n#                       must include the file name and the function name.\n# @param role_arn: The IAM role to use for the function.\n# @param deployment_package: The deployment package that contains the function\n#                             code in .zip format.\n# @return: The Amazon Resource Name (ARN) of the newly created function.\ndef create_function(function_name, handler_name, role_arn, deployment_package)\n  response = @lambda_client.create_function({\n\n    role: role_arn.to_s,\n    function_name: function_name,\n    handler: handler_name,\n    runtime: "ruby2.7",\n    code: {\n      zip_file: deployment_package\n    },\n    environment: {\n      variables: {\n        "LOG_LEVEL" => "info"\n      }\n    }\n  })\n\n  @lambda_client.wait_until(:function_active_v2, { function_name:\nfunction_name}) do |w|\n    w.max_attempts = 5\n    w.delay = 5\n  end\n  response\nrescue Aws::Lambda::Errors::ServiceException => e\n  @logger.error("There was an error creating #{function_name}:\n\n#{e.message}")\nrescue Aws::Writers::Errors::WaiterFailed => e\n  @logger.error("Failed waiting for #{function_name} to activate:\n\n#{e.message}")\nend
```


Panggil fungsi Lambda Anda dengan parameter runtime opsional.

```
# Invokes a Lambda function.
# @param function_name [String] The name of the function to invoke.
# @param payload [nil] Payload containing runtime parameters.
# @return [Object] The response from the function invocation.
def invoke_function(function_name, payload = nil)
  params = { function_name: function_name}
  params[:payload] = payload unless payload.nil?
  @lambda_client.invoke(params)
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
end
```

Perbarui konfigurasi fungsi Lambda Anda untuk menyuntikkan variabel lingkungan baru.

```
# Updates the environment variables for a Lambda function.
# @param function_name: The name of the function to update.
# @param log_level: The log level of the function.
# @return: Data about the update, including the status.
def update_function_configuration(function_name, log_level)
  @lambda_client.update_function_configuration({
    function_name: function_name,
    environment: {
      variables: {
        "LOG_LEVEL" => log_level
      }
    }
  })
  @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
    w.max_attempts = 5
    w.delay = 5
  end
rescue Aws::Lambda::Errors::ServiceException => e
  @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
rescue Aws::Waiters::Errors::WaiterFailed => e
```

```
@logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
end
```

Perbarui kode fungsi Lambda Anda dengan paket penerapan berbeda yang berisi kode berbeda.

```
# Updates the code for a Lambda function by submitting a .zip archive that
contains
# the code for the function.

# @param function_name: The name of the function to update.
# @param deployment_package: The function code to update, packaged as bytes in
#                               .zip format.
# @return: Data about the update, including the status.
def update_function_code(function_name, deployment_package)
  @lambda_client.update_function_code(
    function_name: function_name,
    zip_file: deployment_package
  )
  @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
    w.max_attempts = 5
    w.delay = 5
  end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating function code for:
#{function_name}:\n #{e.message}")
    nil
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
  end
end
```

Daftar semua fungsi Lambda yang ada menggunakan paginator bawaan.

```
# Lists the Lambda functions for the current account.
def list_functions
  functions = []
  @lambda_client.list_functions.each do |response|
    response["functions"].each do |function|
```

```
        functions.append(function["function_name"])
    end
end
functions
rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
end
```

Hapus fungsi Lambda tertentu.

```
# Deletes a Lambda function.
# @param function_name: The name of the function to delete.
def delete_function(function_name)
    print "Deleting function: #{function_name}..."
    @lambda_client.delete_function(
        function_name: function_name
    )
    print "Done!".green
rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
end
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Ruby API Referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

Cargo.toml dengan dependensi yang digunakan dalam skenario ini.

```
[package]
name = "lambda-code-examples"
version = "0.1.0"
edition = "2021"

# See more keys and their definitions at https://doc.rust-lang.org/cargo/reference/manifest.html

[dependencies]
aws-config = { version = "1.0.1", features = ["behavior-version-latest"] }
aws-sdk-ec2 = { version = "1.3.0" }
aws-sdk-iam = { version = "1.3.0" }
aws-sdk-lambda = { version = "1.3.0" }
aws-sdk-s3 = { version = "1.4.0" }
aws-smithy-types = { version = "1.0.1" }
aws-types = { version = "1.0.1" }
clap = { version = "~4.4", features = ["derive"] }
tokio = { version = "1.20.1", features = ["full"] }
tracing-subscriber = { version = "0.3.15", features = ["env-filter"] }
tracing = "0.1.37"
serde_json = "1.0.94"
anyhow = "1.0.71"
uuid = { version = "1.3.3", features = ["v4"] }
lambda_runtime = "0.8.0"
serde = "1.0.164"
```

Kumpulan utilitas yang merampingkan panggilan Lambda untuk skenario ini. File ini adalah `src/ations.rs` di peti.

```

use anyhow::anyhow;
use aws_sdk_iam::operation::{create_role::CreateRoleError,
    delete_role::DeleteRoleOutput};
use aws_sdk_lambda::{
    operation::{
        delete_function::DeleteFunctionOutput, get_function::GetFunctionOutput,
        invoke::InvokeOutput, list_functions::ListFunctionsOutput,
        update_function_code::UpdateFunctionCodeOutput,
        update_function_configuration::UpdateFunctionConfigurationOutput,
    },
    primitives::ByteStream,
    types::{Environment, FunctionCode, LastUpdateStatus, State},
};
use aws_sdk_s3::{
    error::ErrorMetadata,
    operation::{delete_bucket::DeleteBucketOutput,
        delete_object::DeleteObjectOutput},
    types::CreateBucketConfiguration,
};
use aws_smithy_types::Blob;
use serde::{ser::SerializeMap, Serialize};
use std::{fmt::Display, path::PathBuf, str::FromStr, time::Duration};
use tracing::{debug, info, warn};

/* Operation describes */
#[derive(Clone, Copy, Debug, Serialize)]
pub enum Operation {
    #[serde(rename = "plus")]
    Plus,
    #[serde(rename = "minus")]
    Minus,
    #[serde(rename = "times")]
    Times,
    #[serde(rename = "divided-by")]
    DividedBy,
}

impl FromStr for Operation {
    type Err = anyhow::Error;

    fn from_str(s: &str) -> Result<Self, Self::Err> {
        match s {

```

```

        "plus" => Ok(Operation::Plus),
        "minus" => Ok(Operation::Minus),
        "times" => Ok(Operation::Times),
        "divided-by" => Ok(Operation::DividedBy),
        _ => Err(anyhow!("Unknown operation {s}")),
    }
}

impl Display for Operation {
    fn fmt(&self, f: &mut std::fmt::Formatter<'_>) -> std::fmt::Result {
        match self {
            Operation::Plus => write!(f, "plus"),
            Operation::Minus => write!(f, "minus"),
            Operation::Times => write!(f, "times"),
            Operation::DividedBy => write!(f, "divided-by"),
        }
    }
}

/**
 * InvokeArgs will be serialized as JSON and sent to the AWS Lambda handler.
 */
#[derive(Debug)]
pub enum InvokeArgs {
    Increment(i32),
    Arithmetic(Operation, i32, i32),
}

impl Serialize for InvokeArgs {
    fn serialize<S>(&self, serializer: S) -> Result<S::Ok, S::Error>
    where
        S: serde::Serializer,
    {
        match self {
            InvokeArgs::Increment(i) => serializer.serialize_i32(*i),
            InvokeArgs::Arithmetic(o, i, j) => {
                let mut map: S::SerializeMap =
                    serializer.serialize_map(Some(3))?;
                map.serialize_key(&"op".to_string())?;
                map.serialize_value(&o.to_string())?;
                map.serialize_key(&"i".to_string())?;
                map.serialize_value(&i)?;
                map.serialize_key(&"j".to_string())?;
            }
        }
    }
}

```

```

        map.serialize_value(&j)?;
        map.end()
    }
}

/** A policy document allowing Lambda to execute this function on the account's
    behalf. */
const ROLE_POLICY_DOCUMENT: &str = r#{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "Service": "lambda.amazonaws.com" },
            "Action": "sts:AssumeRole"
        }
    ]
}";

/**
 * A LambdaManager gathers all the resources necessary to run the Lambda example
 * scenario.
 * This includes instantiated aws_sdk clients and details of resource names.
 */
pub struct LambdaManager {
    iam_client: aws_sdk_iam::Client,
    lambda_client: aws_sdk_lambda::Client,
    s3_client: aws_sdk_s3::Client,
    lambda_name: String,
    role_name: String,
    bucket: String,
    own_bucket: bool,
}

// These unit type structs provide nominal typing on top of String parameters for
// LambdaManager::new
pub struct LambdaName(pub String);
pub struct RoleName(pub String);
pub struct Bucket(pub String);
pub struct OwnBucket(pub bool);

impl LambdaManager {
    pub fn new(

```

```

    iam_client: aws_sdk_iam::Client,
    lambda_client: aws_sdk_lambda::Client,
    s3_client: aws_sdk_s3::Client,
    lambda_name: LambdaName,
    role_name: RoleName,
    bucket: Bucket,
    own_bucket: OwnBucket,
) -> Self {
    Self {
        iam_client,
        lambda_client,
        s3_client,
        lambda_name: lambda_name.0,
        role_name: role_name.0,
        bucket: bucket.0,
        own_bucket: own_bucket.0,
    }
}

/**
 * Load the AWS configuration from the environment.
 * Look up lambda_name and bucket if none are given, or generate a random
name if not present in the environment.
 * If the bucket name is provided, the caller needs to have created the
bucket.
 * If the bucket name is generated, it will be created.
 */
pub async fn load_from_env(lambda_name: Option<String>, bucket:
Option<String>) -> Self {
    let sdk_config = aws_config::load_from_env().await;
    let lambda_name = LambdaName(lambda_name.unwrap_or_else(|| {
        std::env::var("LAMBDA_NAME").unwrap_or_else(|_|
"rust_lambda_example".to_string())
    }));
    let role_name = RoleName(format!("{}_role", lambda_name.0));
    let (bucket, own_bucket) =
        match bucket {
            Some(bucket) => (Bucket(bucket), false),
            None => (
                Bucket(std::env::var("LAMBDA_BUCKET").unwrap_or_else(|_| {
                    format!("rust-lambda-example-{}", uuid::Uuid::new_v4())
                })),
                true,
            ),
        }
}

```



```

    };

    let s3_client = aws_sdk_s3::Client::new(&sdk_config);

    if own_bucket {
        info!("Creating bucket for demo: {}", bucket.0);
        s3_client
            .create_bucket()
            .bucket(bucket.0.clone())
            .create_bucket_configuration(
                CreateBucketConfiguration::builder()

.location_constraint(aws_sdk_s3::types::BucketLocationConstraint::from(
                    sdk_config.region().unwrap().as_ref(),
                ))
                .build(),
            )
            .send()
            .await
            .unwrap();
    }

    Self::new(
        aws_sdk_iam::Client::new(&sdk_config),
        aws_sdk_lambda::Client::new(&sdk_config),
        s3_client,
        lambda_name,
        role_name,
        bucket,
        OwnBucket(own_bucket),
    )
}

/**
 * Upload function code from a path to a zip file.
 * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
 * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
 */
async fn prepare_function(
    &self,
    zip_file: PathBuf,
    key: Option<String>,
) -> Result<FunctionCode, anyhow::Error> {

```

```

    let body = ByteStream::from_path(zip_file).await?;

    let key = key.unwrap_or_else(|| format!("{}", self.lambda_name));

    info!("Uploading function code to s3://{}/{}", self.bucket, key);
    let _ = self
        .s3_client
        .put_object()
        .bucket(self.bucket.clone())
        .key(key.clone())
        .body(body)
        .send()
        .await?;

    Ok(FunctionCode::builder()
        .s3_bucket(self.bucket.clone())
        .s3_key(key)
        .build())
}

/**
 * Create a function, uploading from a zip file.
 */
pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
anyhow::Error> {
    let code = self.prepare_function(zip_file, None).await?;

    let key = code.s3_key().unwrap().to_string();

    let role = self.create_role().await.map_err(|e| anyhow!(e))?;

    info!("Created iam role, waiting 15s for it to become active");
    tokio::time::sleep(Duration::from_secs(15)).await;

    info!("Creating lambda function {}", self.lambda_name);
    let _ = self
        .lambda_client
        .create_function()
        .function_name(self.lambda_name.clone())
        .code(code)
        .role(role.arn())
        .runtime(aws_sdk_lambda::types::Runtime::ProvidedAl2)
        .handler("_unused")
        .send()

```

```
        .await
        .map_err(anyhow::Error::from)?;

self.wait_for_function_ready().await?;

self.lambda_client
    .publish_version()
    .function_name(self.lambda_name.clone())
    .send()
    .await?;

Ok(key)
}

/**
 * Create an IAM execution role for the managed Lambda function.
 * If the role already exists, use that instead.
 */
async fn create_role(&self) -> Result<aws_sdk_iam::types::Role,
CreateRoleError> {
    info!("Creating execution role for function");
    let get_role = self
        .iam_client
        .get_role()
        .role_name(self.role_name.clone())
        .send()
        .await;
    if let Ok(get_role) = get_role {
        if let Some(role) = get_role.role {
            return Ok(role);
        }
    }

    let create_role = self
        .iam_client
        .create_role()
        .role_name(self.role_name.clone())
        .assume_role_policy_document(ROLE_POLICY_DOCUMENT)
        .send()
        .await;

    match create_role {
        Ok(create_role) => match create_role.role {
            Some(role) => Ok(role),
```

```

        None => Err(CreateRoleError::generic(
            ErrorMetadata::builder()
                .message("CreateRole returned empty success")
                .build(),
        )),
    },
    Err(err) => Err(err.into_service_error()),
}

}

/**
 * Poll `is_function_ready` with a 1-second delay. It returns when the
 * function is ready or when there's an error checking the function's state.
 */
pub async fn wait_for_function_ready(&self) -> Result<(), anyhow::Error> {
    info!("Waiting for function");
    while !self.is_function_ready(None).await? {
        info!("Function is not ready, sleeping 1s");
        tokio::time::sleep(Duration::from_secs(1)).await;
    }
    Ok(())
}

/**
 * Check if a Lambda function is ready to be invoked.
 * A Lambda function is ready for this scenario when its state is active and
 * its LastUpdateStatus is Successful.
 * Additionally, if a sha256 is provided, the function must have that as its
 * current code hash.
 * Any missing properties or failed requests will be reported as an Err.
 */
async fn is_function_ready(
    &self,
    expected_code_sha256: Option<&str>,
) -> Result<bool, anyhow::Error> {
    match self.get_function().await {
        Ok(func) => {
            if let Some(config) = func.configuration() {
                if let Some(state) = config.state() {
                    info!(?state, "Checking if function is active");
                    if !matches!(state, State::Active) {
                        return Ok(false);
                    }
                }
            }
        }
    }
}

```

```

        match config.last_update_status() {
            Some(last_update_status) => {
                info!(?last_update_status, "Checking if function is
ready");

                match last_update_status {
                    LastUpdateStatus::Successful => {
                        // continue
                    }
                    LastUpdateStatus::Failed |
LastUpdateStatus::InProgress => {
                        return Ok(false);
                    }
                    unknown => {
                        warn!(
                            status_variant = unknown.as_str(),
                            "LastUpdateStatus unknown"
                        );
                        return Err(anyhow!(
                            "Unknown LastUpdateStatus, fn config is
{config:?}"
                        ));
                    }
                }
            }
            None => {
                warn!("Missing last update status");
                return Ok(false);
            }
        };
        if expected_code_sha256.is_none() {
            return Ok(true);
        }
        if let Some(code_sha256) = config.code_sha256() {
            return Ok(code_sha256 ==
expected_code_sha256.unwrap_or_default());
        }
    }
    Err(e) => {
        warn!(?e, "Could not get function while waiting");
    }
}
Ok(false)
}

```

```
/** Get the Lambda function with this Manager's name. */
pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
    info!("Getting lambda function");
    self.lambda_client
        .get_function()
        .function_name(self.lambda_name.clone())
        .send()
        .await
        .map_err(anyhow::Error::from)
}

/** List all Lambda functions in the current Region. */
pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
    info!("Listing lambda functions");
    self.lambda_client
        .list_functions()
        .send()
        .await
        .map_err(anyhow::Error::from)
}

/** Invoke the lambda function using calculator InvokeArgs. */
pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
anyhow::Error> {
    info!(?args, "Invoking {}", self.lambda_name);
    let payload = serde_json::to_string(&args)?;
    debug!(?payload, "Sending payload");
    self.lambda_client
        .invoke()
        .function_name(self.lambda_name.clone())
        .payload(Blob::new(payload))
        .send()
        .await
        .map_err(anyhow::Error::from)
}

/** Given a Path to a zip file, update the function's code and wait for the
update to finish. */
pub async fn update_function_code(
    &self,
    zip_file: PathBuf,
```

```

    key: String,
) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
    let function_code = self.prepare_function(zip_file, Some(key)).await?;

    info!("Updating code for {}", self.lambda_name);
    let update = self
        .lambda_client
        .update_function_code()
        .function_name(self.lambda_name.clone())
        .s3_bucket(self.bucket.clone())
        .s3_key(function_code.s3_key().unwrap().to_string())
        .send()
        .await
        .map_err(anyhow::Error::from)?;

    self.wait_for_function_ready().await?;

    Ok(update)
}

/** Update the environment for a function. */
pub async fn update_function_configuration(
    &self,
    environment: Environment,
) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
    info!(
        ?environment,
        "Updating environment for {}", self.lambda_name
    );
    let updated = self
        .lambda_client
        .update_function_configuration()
        .function_name(self.lambda_name.clone())
        .environment(environment)
        .send()
        .await
        .map_err(anyhow::Error::from)?;

    self.wait_for_function_ready().await?;

    Ok(updated)
}

```

```
/** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
pub async fn delete_function(
    &self,
    location: Option<String>,
) -> (
    Result<DeleteFunctionOutput, anyhow::Error>,
    Result<DeleteRoleOutput, anyhow::Error>,
    Option<Result<DeleteObjectOutput, anyhow::Error>>,
) {
    info!("Deleting lambda function {}", self.lambda_name);
    let delete_function = self
        .lambda_client
        .delete_function()
        .function_name(self.lambda_name.clone())
        .send()
        .await
        .map_err(anyhow::Error::from);

    info!("Deleting iam role {}", self.role_name);
    let delete_role = self
        .iam_client
        .delete_role()
        .role_name(self.role_name.clone())
        .send()
        .await
        .map_err(anyhow::Error::from);

    let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
        if let Some(location) = location {
            info!("Deleting object {location}");
            Some(
                self.s3_client
                    .delete_object()
                    .bucket(self.bucket.clone())
                    .key(location)
                    .send()
                    .await
                    .map_err(anyhow::Error::from),
            )
        } else {
            info!(?location, "Skipping delete object");
            None
        };
};
```



```

        (delete_function, delete_role, delete_object)
    }

pub async fn cleanup(
    &self,
    location: Option<String>,
) -> (
    (
        Result<DeleteFunctionOutput, anyhow::Error>,
        Result<DeleteRoleOutput, anyhow::Error>,
        Option<Result<DeleteObjectOutput, anyhow::Error>>,
    ),
    Option<Result<DeleteBucketOutput, anyhow::Error>>,
) {
    let delete_function = self.delete_function(location).await;

    let delete_bucket = if self.own_bucket {
        info!("Deleting bucket {}", self.bucket);
        if delete_function.2.is_none() ||
delete_function.2.as_ref().unwrap().is_ok() {
            Some(
                self.s3_client
                    .delete_bucket()
                    .bucket(self.bucket.clone())
                    .send()
                    .await
                    .map_err(anyhow::Error::from),
            )
        } else {
            None
        }
    } else {
        info!("No bucket to clean up");
        None
    };

    (delete_function, delete_bucket)
}

/**
 * Testing occurs primarily as an integration test running the `scenario` bin
 successfully.

```

```

* Each action relies deeply on the internal workings and state of Amazon Simple
Storage Service (Amazon S3), Lambda, and IAM working together.
* It is therefore infeasible to mock the clients to test the individual actions.
*/
#[cfg(test)]
mod test {
    use super::{InvokeArgs, Operation};
    use serde_json::json;

    /** Make sure that the JSON output of serializing InvokeArgs is what's
    expected by the calculator. */
    #[test]
    fn test_serialize() {
        assert_eq!(json!(InvokeArgs::Increment(5)), 5);
        assert_eq!(
            json!(InvokeArgs::Arithmetic(Operation::Plus, 5, 7)).to_string(),
            r#"{"op":"plus","i":5,"j":7}"#.to_string(),
        );
    }
}

```

Biner untuk menjalankan skenario dari depan ke ujung, menggunakan flag baris perintah untuk mengontrol beberapa perilaku. File ini adalah `src/bin/scenario.rs` di peti.

```

/*
## Service actions

Service actions wrap the SDK call, taking a client and any specific parameters
necessary for the call.

* CreateFunction
* GetFunction
* ListFunctions
* Invoke
* UpdateFunctionCode
* UpdateFunctionConfiguration
* DeleteFunction

## Scenario

```

A scenario runs at a command prompt and prints output to the user on the result of each service action. A scenario can run in one of two ways: straight through, printing out progress as it goes, or as an interactive question/answer script.

Getting started with functions

Use an SDK to manage AWS Lambda functions: create a function, invoke it, update its code, invoke it again, view its output and logs, and delete it.

This scenario uses two Lambda handlers:

Note: Handlers don't use AWS SDK API calls.

The increment handler is straightforward:

1. It accepts a number, increments it, and returns the new value.
2. It performs simple logging of the result.

The arithmetic handler is more complex:

1. It accepts a set of actions ['plus', 'minus', 'times', 'divided-by'] and two numbers, and returns the result of the calculation.
2. It uses an environment variable to control log level (such as DEBUG, INFO, WARNING, ERROR).

It logs a few things at different levels, such as:

- * DEBUG: Full event data.
- * INFO: The calculation result.
- * WARN~ING~: When a divide by zero error occurs.
- * This will be the typical `RUST_LOG` variable.

The steps of the scenario are:

1. Create an AWS Identity and Access Management (IAM) role that meets the following requirements:
 - * Has an `assume_role` policy that grants 'lambda.amazonaws.com' the 'sts:AssumeRole' action.
 - * Attaches the 'arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole' managed role.
 - * You must wait for ~10 seconds after the role is created before you can use it!
2. Create a function (CreateFunction) for the increment handler by packaging it as a zip and doing one of the following:
 - * Adding it with CreateFunction Code.ZipFile.
 - * --or--

- * Uploading it to Amazon Simple Storage Service (Amazon S3) and adding it with CreateFunction Code.S3Bucket/S3Key.
 - * `_Note`: Zipping the file does not have to be done in code._
 - * If you have a waiter, use it to wait until the function is active. Otherwise, call GetFunction until State is Active.
3. Invoke the function with a number and print the result.
 4. Update the function (UpdateFunctionCode) to the arithmetic handler by packaging it as a zip and doing one of the following:
 - * Adding it with UpdateFunctionCode ZipFile.
 - * `--or--`
 - * Uploading it to Amazon S3 and adding it with UpdateFunctionCode S3Bucket/S3Key.
 5. Call GetFunction until Configuration.LastUpdateStatus is 'Successful' (or 'Failed').
 6. Update the environment variable by calling UpdateFunctionConfiguration and pass it a log level, such as:
 - * `Environment={'Variables': {'RUST_LOG': 'TRACE'}}`
 7. Invoke the function with an action from the list and a couple of values. Include LogType='Tail' to get logs in the result. Print the result of the calculation and the log.
 8. [Optional] Invoke the function to provoke a divide-by-zero error and show the log result.
 9. List all functions for the account, using pagination (ListFunctions).
 10. Delete the function (DeleteFunction).
 11. Delete the role.

Each step should use the function created in Service Actions to abstract calling the SDK.

```
*/

use aws_sdk_lambda::{operation::invoke::InvokeOutput, types::Environment};
use clap::Parser;
use std::{collections::HashMap, path::PathBuf};
use tracing::{debug, info, warn};
use tracing_subscriber::EnvFilter;

use lambda_code_examples::actions::{
    InvokeArgs::{Arithmetic, Increment},
    LambdaManager, Operation,
};

#[derive(Debug, Parser)]
pub struct Opt {
    /// The AWS Region.
```

```
#[structopt(short, long)]
pub region: Option<String>,

// The bucket to use for the FunctionCode.
#[structopt(short, long)]
pub bucket: Option<String>,

// The name of the Lambda function.
#[structopt(short, long)]
pub lambda_name: Option<String>,

// The number to increment.
#[structopt(short, long, default_value = "12")]
pub inc: i32,

// The left operand.
#[structopt(long, default_value = "19")]
pub num_a: i32,

// The right operand.
#[structopt(long, default_value = "23")]
pub num_b: i32,

// The arithmetic operation.
#[structopt(short, long, default_value = "plus")]
pub operation: Operation,

#[structopt(long)]
pub cleanup: Option<bool>,

#[structopt(long)]
pub no_cleanup: Option<bool>,
}

fn code_path(lambda: &str) -> PathBuf {
    PathBuf::from(format!("../target/lambda/{lambda}/bootstrap.zip"))
}

fn log_invoke_output(invoker: &InvokeOutput, message: &str) {
    if let Some(payload) = invoker.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
        info!("Could not extract payload")
    }
}
```

```
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}

async fn main_block(
    opt: &Opt,
    manager: &LambdaManager,
    code_location: String,
) -> Result<(), anyhow::Error> {
    let invoke = manager.invoke(Increment(opt.inc)).await?;
    log_invoke_output(&invoke, "Invoked function configured as increment");

    let update_code = manager
        .update_function_code(code_path("arithmetic"), code_location.clone())
        .await?;

    let code_sha256 = update_code.code_sha256().unwrap_or("Unknown SHA");
    info!(?code_sha256, "Updated function code with arithmetic.zip");

    let arithmetic_args = Arithmetic(opt.operation, opt.num_a, opt.num_b);
    let invoke = manager.invoke(arithmetic_args).await?;
    log_invoke_output(&invoke, "Invoked function configured as arithmetic");

    let update = manager
        .update_function_configuration(
            Environment::builder()
                .set_variables(Some(HashMap::from([
                    "RUST_LOG".to_string(),
                    "trace".to_string(),
                ])))
                .build(),
        )
        .await?;
    let updated_environment = update.environment();
    info!(?updated_environment, "Updated function configuration");

    let invoke = manager
        .invoke(Arithmetic(opt.operation, opt.num_a, opt.num_b))
        .await?;
    log_invoke_output(
```

```
        &invoke,
        "Invoked function configured as arithmetic with increased logging",
    );

    let invoke = manager
        .invoke(Arithmetic(Operation::DividedBy, opt.num_a, 0))
        .await?;
    log_invoke_output(
        &invoke,
        "Invoked function configured as arithmetic with divide by zero",
    );

    Ok::<(), anyhow::Error>(( ))
}

#[tokio::main]
async fn main() {
    tracing_subscriber::fmt()
        .without_time()
        .with_file(true)
        .with_line_number(true)
        .with_env_filter(EnvFilter::from_default_env())
        .init();

    let opt = Opt::parse();
    let manager = LambdaManager::load_from_env(opt.lambda_name.clone(),
opt.bucket.clone()).await;

    let key = match manager.create_function(code_path("increment")).await {
        Ok(init) => {
            info!(?init, "Created function, initially with increment.zip");
            let run_block = main_block(&opt, &manager, init.clone()).await;
            info!(?run_block, "Finished running example, cleaning up");
            Some(init)
        }
        Err(err) => {
            warn!(?err, "Error happened when initializing function");
            None
        }
    };

    if Some(false) == opt.cleanup || Some(true) == opt.no_cleanup {
        info!("Skipping cleanup")
    } else {
```

```

    let delete = manager.cleanup(key).await;
    info!(?delete, "Deleted function & cleaned up resources");
  }
}

```

- Untuk API detailnya, lihat topik berikut AWS SDK untuk API referensi Rust.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

SAP ABAP

SDK untuk SAP ABAP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturannya dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

TRY.
  "Create an AWS Identity and Access Management (IAM) role that grants AWS
  Lambda permission to write to logs."
  DATA(lv_policy_document) = `{` &&
    ` "Version": "2012-10-17", ` &&
    ` "Statement": [ ` &&
      `{ ` &&
        ` "Effect": "Allow", ` &&
        ` "Action": [ ` &&
          ` "sts:AssumeRole" ` &&
        ` ], ` &&
      ` "Principal": { ` &&

```



```

        "Service": [ ` &&
            "lambda.amazonaws.com" ` &&
        ] ` &&
    } ` &&
} ` &&
] ` &&
} ` .

TRY.
    DATA(lo_create_role_output) = lo_iam->createrole(
        iv_rolename = iv_role_name
        iv_assumerolepolicydocument = lv_policy_document
        iv_description = 'Grant lambda permission to write to logs'
    ).
    MESSAGE 'IAM role created.' TYPE 'I'.
    WAIT UP TO 10 SECONDS.          " Make sure that the IAM role is
ready for use. "
    CATCH /aws1/cx_iamentityalrddyexex.
        MESSAGE 'IAM role already exists.' TYPE 'E'.
    CATCH /aws1/cx_iaminvalidinputex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_iammalformedplydocex.
        MESSAGE 'Policy document in the request is malformed.' TYPE 'E'.
ENDTRY.

TRY.
    lo_iam->attachrolepolicy(
        iv_rolename = iv_role_name
        iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole'
    ).
    MESSAGE 'Attached policy to the IAM role.' TYPE 'I'.
    CATCH /aws1/cx_iaminvalidinputex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_iamnosuchentityex.
        MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
    CATCH /aws1/cx_iamplynnotattachableex.
        MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
    CATCH /aws1/cx_iamunmodableentityex.
        MESSAGE 'Service that depends on the service-linked role is not
modifiable.' TYPE 'E'.
ENDTRY.

" Create a Lambda function and upload handler code. "

```

```

" Lambda function performs 'increment' action on a number. "
TRY.
    lo_lmd->createfunction(
        iv_functionname = iv_function_name
        iv_runtime = `python3.9`
        iv_role = lo_create_role_output->get_role( )->get_arn( )
        iv_handler = iv_handler
        io_code = io_initial_zip_file
        iv_description = 'AWS Lambda code example'
    ).
    MESSAGE 'Lambda function created.' TYPE 'I'.
CATCH /aws1/cx_lmdcodestorageexcdex.
    MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
CATCH /aws1/cx_lmdinvparamvalueex.
    MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
CATCH /aws1/cx_lmdresourcenotfoundex.
    MESSAGE 'The requested resource does not exist.' TYPE 'E'.
ENDTRY.

" Verify the function is in Active state "
WHILE lo_lmd->getfunction( iv_functionname = iv_function_name )-
>get_configuration( )->ask_state( ) <> 'Active'.
    IF sy-index = 10.
        EXIT.                " Maximum 10 seconds. "
    ENDIF.
    WAIT UP TO 1 SECONDS.
ENDWHILE.

"Invoke the function with a single parameter and get results."
TRY.
    DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
        `{` &&
        ` "action": "increment",` &&
        ` "number": 10` &&
        `}`
    ).
    DATA(lo_initial_invoke_output) = lo_lmd->invoke(
        iv_functionname = iv_function_name
        iv_payload = lv_json
    ).
    ov_initial_invoke_payload = lo_initial_invoke_output->get_payload( ).
    " ov_initial_invoke_payload is returned for testing purposes. "
    DATA(lo_writer_json) = cl_sxml_string_writer=>create( type =
if_sxml=>co_xt_json ).

```

```

        CALL TRANSFORMATION id SOURCE XML ov_initial_invoke_payload RESULT
XML lo_writer_json.
        DATA(lv_result) = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
        MESSAGE 'Lambda function invoked.' TYPE 'I'.
    CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_lmdinvrequestcontex.
        MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
    CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
    CATCH /aws1/cx_lmdunsuppmediatyp00.
        MESSAGE 'Invoke request body does not have JSON as its content type.'
TYPE 'E'.
    ENDRY.

    " Update the function code and configure its Lambda environment with an
environment variable. "
    " Lambda function is updated to perform 'decrement' action also. "
    TRY.
        lo_lmd->updatefunctioncode(
            iv_functionname = iv_function_name
            iv_zipfile = io_updated_zip_file
        ).
        WAIT UP TO 10 SECONDS.          " Make sure that the update is
completed. "
        MESSAGE 'Lambda function code updated.' TYPE 'I'.
    CATCH /aws1/cx_lmdcodestorageexcex.
        MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
    CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
    ENDRY.

    TRY.
        DATA lt_variables TYPE /aws1/
cl_lmdenvironmentvaria00=>tt_environmentvariables.
        DATA ls_variable LIKE LINE OF lt_variables.
        ls_variable-key = 'LOG_LEVEL'.
        ls_variable-value = NEW /aws1/cl_lmdenvironmentvaria00( iv_value =
'info' ).
        INSERT ls_variable INTO TABLE lt_variables.

```

```

        lo_lmd->updatefunctionconfiguration(
            iv_functionname = iv_function_name
            io_environment = NEW /aws1/cl_lmdenvironment( it_variables =
lt_variables )
        ).
        WAIT UP TO 10 SECONDS.           " Make sure that the update is
completed. "
        MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
        CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
        CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in
progress.' TYPE 'E'.
        CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        "Invoke the function with new parameters and get results. Display the
execution log that's returned from the invocation."
        TRY.
            lv_json = /aws1/cl_rt_util=>string_to_xstring(
                `{` &&
                `"action": "decrement",` &&
                `"number": 10` &&
                `}`
            ).
            DATA(lo_updated_invoke_output) = lo_lmd->invoke(
                iv_functionname = iv_function_name
                iv_payload = lv_json
            ).
            ov_updated_invoke_payload = lo_updated_invoke_output->get_payload( ).
            " ov_updated_invoke_payload is returned for testing purposes. "
            lo_writer_json = cl_sxml_string_writer=>create( type =
if_sxml=>co_xt_json ).
            CALL TRANSFORMATION id SOURCE XML ov_updated_invoke_payload RESULT
XML lo_writer_json.
            lv_result = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
            MESSAGE 'Lambda function invoked.' TYPE 'I'.
            CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
            CATCH /aws1/cx_lmdinvrequestcontex.
            MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
            CATCH /aws1/cx_lmdresourcenotfoundex.

```

```
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
    CATCH /aws1/cx_lmdunsuppedmediatyp00.
        MESSAGE 'Invoke request body does not have JSON as its content type.'
TYPE 'E'.
    ENDRY.

" List the functions for your account. "
TRY.
    DATA(lo_list_output) = lo_lmd->listfunctions( ).
    DATA(lt_functions) = lo_list_output->get_functions( ).
    MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
    CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    ENDRY.

" Delete the Lambda function. "
TRY.
    lo_lmd->deletefunction( iv_functionname = iv_function_name ).
    MESSAGE 'Lambda function deleted.' TYPE 'I'.
    CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
    ENDRY.

" Detach role policy. "
TRY.
    lo_iam->detachrolepolicy(
        iv_rolename = iv_role_name
        iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole'
    ).
    MESSAGE 'Detached policy from the IAM role.' TYPE 'I'.
    CATCH /aws1/cx_iaminvalidinputex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
    CATCH /aws1/cx_iamnosuchentityex.
        MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
    CATCH /aws1/cx_iamplynotattachableex.
        MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
    CATCH /aws1/cx_iamunmodableentityex.
        MESSAGE 'Service that depends on the service-linked role is not
modifiable.' TYPE 'E'.
    ENDRY.
```

```
" Delete the IAM role. "  
TRY.  
    lo_iam->deleterole( iv_rolename = iv_role_name ).  
    MESSAGE 'IAM role deleted.' TYPE 'I'.  
CATCH /aws1/cx_iamnosuchentityex.  
    MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.  
CATCH /aws1/cx_iamunmodableentityex.  
    MESSAGE 'Service that depends on the service-linked role is not  
modifiable.' TYPE 'E'.  
ENDTRY.  
  
CATCH /aws1/cx_rt_service_generic INTO lo_exception.  
    DATA(lv_error) = lo_exception->get_longtext( ).  
    MESSAGE lv_error TYPE 'E'.  
ENDTRY.
```

- Untuk API detailnya, lihat topik berikut AWS SDK untuk SAP ABAP API referensi.
 - [CreateFunction](#)
 - [DeleteFunction](#)
 - [GetFunction](#)
 - [Memohon](#)
 - [ListFunctions](#)
 - [UpdateFunctionCode](#)
 - [UpdateFunctionConfiguration](#)

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Menginvokasi fungsi Lambda dari browser

Contoh kode berikut menunjukkan cara memanggil AWS Lambda fungsi dari browser.

JavaScript

SDK untuk JavaScript (v2)

Anda dapat membuat aplikasi berbasis browser yang menggunakan AWS Lambda fungsi untuk memperbarui tabel Amazon DynamoDB dengan pilihan pengguna.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- Lambda

SDK untuk JavaScript (v3)

Anda dapat membuat aplikasi berbasis browser yang menggunakan AWS Lambda fungsi untuk memperbarui tabel Amazon DynamoDB dengan pilihan pengguna. Aplikasi ini menggunakan AWS SDK for JavaScript v3.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- Lambda

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Transformasi data untuk aplikasi Anda dengan S3 Object Lambda

Contoh kode berikut menunjukkan cara mengubah data untuk aplikasi Anda dengan S3 Object Lambda.

.NET

AWS SDK for .NET

Menunjukkan cara menambahkan kode kustom ke GET permintaan S3 standar untuk memodifikasi objek yang diminta diambil dari S3 sehingga objek sesuai dengan kebutuhan klien atau aplikasi yang meminta.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- Lambda
- Amazon S3

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Gunakan API Gateway untuk menjalankan fungsi Lambda

Contoh kode berikut menunjukkan cara membuat AWS Lambda fungsi yang dipanggil oleh Amazon API Gateway.

Java

SDK untuk Java 2.x

Menunjukkan cara membuat AWS Lambda fungsi dengan menggunakan runtime Lambda Java. API Contoh ini memanggil AWS layanan yang berbeda untuk melakukan kasus penggunaan tertentu. Contoh ini menunjukkan cara membuat fungsi Lambda yang dipanggil oleh API Amazon Gateway yang memindai tabel Amazon DynamoDB untuk peringatan kerja dan menggunakan Amazon Simple SNS Notification Service (Amazon) untuk mengirim pesan teks kepada karyawan Anda yang memberi selamat kepada mereka pada tanggal ulang tahun satu tahun mereka.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB
- Lambda
- Amazon SNS

JavaScript

SDK untuk JavaScript (v3)

Menunjukkan cara membuat AWS Lambda fungsi dengan menggunakan runtime Lambda JavaScript . API Contoh ini memanggil AWS layanan yang berbeda untuk melakukan kasus penggunaan tertentu. Contoh ini menunjukkan cara membuat fungsi Lambda yang dipanggil oleh API Amazon Gateway yang memindai tabel Amazon DynamoDB untuk peringatan kerja dan menggunakan Amazon Simple SNS Notification Service (Amazon) untuk mengirim pesan teks kepada karyawan Anda yang memberi selamat kepada mereka pada tanggal ulang tahun satu tahun mereka.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Contoh ini juga tersedia di [panduan developer v3 AWS SDK for JavaScript](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- DynamoDB
- Lambda
- Amazon SNS

Python

SDK untuk Python (Boto3)

Contoh ini menunjukkan cara membuat dan menggunakan Amazon API Gateway REST API yang menargetkan suatu AWS Lambda fungsi. Handler Lambda menunjukkan cara merutekan berdasarkan HTTP metode; cara mendapatkan data dari string kueri, header, dan badan; dan cara mengembalikan respons. JSON

- Menyebarkan fungsi Lambda.
- Buat API Gateway RESTAPI.
- Buat REST sumber daya yang menargetkan fungsi Lambda.
- Berikan izin untuk membiarkan API Gateway menjalankan fungsi Lambda.
- Gunakan paket Permintaan untuk mengirim permintaan ke file RESTAPI.
- Bersihkan semua sumber daya yang dibuat selama demo.

Contoh ini paling baik dilihat di GitHub. Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- APIGerbang
- Lambda

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Menggunakan Step Functions untuk menginvokasi fungsi Lambda

Contoh kode berikut menunjukkan cara membuat mesin AWS Step Functions status yang memanggil AWS Lambda fungsi secara berurutan.

Java

SDK untuk Java 2.x

Menunjukkan cara membuat alur kerja AWS tanpa server dengan menggunakan AWS Step Functions dan AWS SDK for Java 2.x. Setiap langkah alur kerja diimplementasikan menggunakan AWS Lambda fungsi.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- Lambda
- Amazon SES

- Step Functions

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Menggunakan peristiwa terjadwal untuk menginvokasi fungsi Lambda

Contoh kode berikut menunjukkan cara membuat AWS Lambda fungsi yang dipanggil oleh acara EventBridge terjadwal Amazon.

Java

SDK untuk Java 2.x

Menunjukkan cara membuat acara EventBridge terjadwal Amazon yang memanggil AWS Lambda fungsi. Konfigurasi EventBridge untuk menggunakan ekspresi cron untuk menjadwalkan saat fungsi Lambda dipanggil. Dalam contoh ini, Anda membuat fungsi Lambda dengan menggunakan runtime Lambda Java. API Contoh ini memanggil AWS layanan yang berbeda untuk melakukan kasus penggunaan tertentu. Contoh ini menunjukkan cara membuat aplikasi yang mengirimkan pesan teks seluler kepada karyawan Anda berisi ucapan selamat pada hari jadi setahun kerja mereka.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

JavaScript

SDK untuk JavaScript (v3)

Menunjukkan cara membuat acara EventBridge terjadwal Amazon yang memanggil AWS Lambda fungsi. Konfigurasi EventBridge untuk menggunakan ekspresi cron untuk

menjadwalkan saat fungsi Lambda dipanggil. Dalam contoh ini, Anda membuat fungsi Lambda dengan menggunakan runtime Lambda. JavaScript API Contoh ini memanggil AWS layanan yang berbeda untuk melakukan kasus penggunaan tertentu. Contoh ini menunjukkan cara membuat aplikasi yang mengirimkan pesan teks seluler kepada karyawan Anda berisi ucapan selamat pada hari jadi setahun kerja mereka.

Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Contoh ini juga tersedia di [panduan developer v3 AWS SDK for JavaScript](#).

Layanan yang digunakan dalam contoh ini

- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

Python

SDK untuk Python (Boto3)

Contoh ini menunjukkan cara mendaftarkan AWS Lambda fungsi sebagai target EventBridge acara Amazon terjadwal. Penangan Lambda menulis pesan ramah dan data peristiwa lengkap ke Amazon CloudWatch Logs untuk pengambilan nanti.

- Menyebarkan fungsi Lambda.
- Membuat acara EventBridge terjadwal dan menjadikan fungsi Lambda sebagai target.
- Memberikan izin untuk membiarkan EventBridge menjalankan fungsi Lambda.
- Mencetak data terbaru dari CloudWatch Log untuk menampilkan hasil pemanggilan terjadwal.
- Membersihkan semua sumber daya yang dibuat selama demo.

Contoh ini paling baik dilihat di [GitHub](#). Untuk kode sumber lengkap dan instruksi tentang cara mengatur dan menjalankan, lihat contoh lengkapnya di [GitHub](#).

Layanan yang digunakan dalam contoh ini

- CloudWatch Log
- EventBridge

- Lambda

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Menulis data aktivitas kustom dengan fungsi Lambda setelah otentikasi pengguna Amazon Cognito menggunakan AWS SDK

Contoh kode berikut menunjukkan cara menulis data aktivitas kustom dengan fungsi Lambda setelah autentikasi pengguna Amazon Cognito.

- Gunakan fungsi administrator untuk menambahkan pengguna ke kumpulan pengguna.
- Konfigurasi kumpulan pengguna untuk memanggil fungsi Lambda untuk `PostAuthentication` pemicunya.
- Masuk pengguna baru ke Amazon Cognito.
- Fungsi Lambda menulis informasi kustom ke CloudWatch Log dan ke tabel DynamoDB.
- Dapatkan dan tampilkan data kustom dari tabel DynamoDB, lalu bersihkan sumber daya.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara pengaturan dan menjalankannya di [Repositori Contoh Kode AWS](#).

Jalankan skenario interaktif di penggugah/prompt perintah.

```
// ActivityLog separates the steps of this scenario into individual functions so
// that
// they are simpler to read and understand.
type ActivityLog struct {
    helper      IScenarioHelper
    questioner demotools.IQuestioner
```

```

resources    Resources
cognitoActor *actions.CognitoActions
}

// NewActivityLog constructs a new activity log runner.
func NewActivityLog(sdkConfig aws.Config, questioner demotools.IQuestioner,
helper IScenarioHelper) ActivityLog {
scenario := ActivityLog{
helper:      helper,
questioner:  questioner,
resources:   Resources{},
cognitoActor: &actions.CognitoActions{CognitoClient:
cognitoidentityprovider.NewFromConfig(sdkConfig)},
}
scenario.resources.init(scenario.cognitoActor, questioner)
return scenario
}

// AddUserToPool selects a user from the known users table and uses administrator
credentials to add the user to the user pool.
func (runner *ActivityLog) AddUserToPool(userPoolId string, tableName string)
(string, string) {
log.Println("To facilitate this example, let's add a user to the user pool using
administrator privileges.")
users, err := runner.helper.GetKnownUsers(tableName)
if err != nil {
panic(err)
}
user := users.Users[0]
log.Printf("Adding known user %v to the user pool.\n", user.UserName)
err = runner.cognitoActor.AdminCreateUser(userPoolId, user.UserName,
user.UserEmail)
if err != nil {
panic(err)
}
pwSet := false
password := runner.questioner.AskPassword("\nEnter a password that has at least
eight characters, uppercase, lowercase, numbers and symbols.\n"+
"(the password will not display as you type):", 8)
for !pwSet {
log.Printf("\nSetting password for user '%v'.\n", user.UserName)
err = runner.cognitoActor.AdminSetUserPassword(userPoolId, user.UserName,
password)
if err != nil {

```

```
var invalidPassword *types.InvalidPasswordException
if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("\nEnter another password:", 8)
} else {
    panic(err)
}
} else {
    pwSet = true
}
}

log.Println(strings.Repeat("-", 88))

return user.UserName, password
}

// AddActivityLogTrigger adds a Lambda handler as an invocation target for the
// PostAuthentication trigger.
func (runner *ActivityLog) AddActivityLogTrigger(userPoolId string,
activityLogArn string) {
log.Println("Let's add a Lambda function to handle the PostAuthentication
trigger from Cognito.\n" +
"This trigger happens after a user is authenticated, and lets your function
take action, such as logging\n" +
"the outcome.")
err := runner.cognitoActor.UpdateTriggers(
userPoolId,
actions.TriggerInfo{Trigger: actions.PostAuthentication, HandlerArn:
aws.String(activityLogArn)})
if err != nil {
panic(err)
}
runner.resources.triggers = append(runner.resources.triggers,
actions.PostAuthentication)
log.Printf("Lambda function %v added to user pool %v to handle
PostAuthentication Cognito trigger.\n",
activityLogArn, userPoolId)

log.Println(strings.Repeat("-", 88))
}

// SignInUser signs in as the specified user.
func (runner *ActivityLog) SignInUser(clientId string, userName string, password
string) {
```

```
log.Printf("Now we'll sign in user %v and check the results in the logs and the
DynamoDB table.", userName)
runner.questioner.Ask("Press Enter when you're ready.")
authResult, err := runner.cognitoActor.SignIn(clientId, userName, password)
if err != nil {
    panic(err)
}
log.Println("Sign in successful.",
    "The PostAuthentication Lambda handler writes custom information to CloudWatch
Logs.")

runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
*authResult.AccessToken)
}

// GetKnownUserLastLogin gets the login info for a user from the Amazon DynamoDB
table and displays it.
func (runner *ActivityLog) GetKnownUserLastLogin(tableName string, userName
string) {
log.Println("The PostAuthentication handler also writes login data to the
DynamoDB table.")
runner.questioner.Ask("Press Enter when you're ready to continue.")
users, err := runner.helper.GetKnownUsers(tableName)
if err != nil {
    panic(err)
}
for _, user := range users.Users {
    if user.UserName == userName {
        log.Println("The last login info for the user in the known users table is:")
        log.Printf("\t%+v", *user.LastLogin)
    }
}
log.Println(strings.Repeat("-", 88))
}

// Run runs the scenario.
func (runner *ActivityLog) Run(stackName string) {
defer func() {
    if r := recover(); r != nil {
        log.Println("Something went wrong with the demo.")
        runner.resources.Cleanup()
    }
}()
}
```



```

log.Println(strings.Repeat("-", 88))
log.Printf("Welcome\n")

log.Println(strings.Repeat("-", 88))

stackOutputs, err := runner.helper.GetStackOutputs(stackName)
if err != nil {
    panic(err)
}
runner.resources.userPoolId = stackOutputs["UserPoolId"]
runner.helper.PopulateUserTable(stackOutputs["TableName"])
userName, password := runner.AddUserToPool(stackOutputs["UserPoolId"],
stackOutputs["TableName"])

runner.AddActivityLogTrigger(stackOutputs["UserPoolId"],
stackOutputs["ActivityLogFunctionArn"])
runner.SignInUser(stackOutputs["UserPoolClientId"], userName, password)
runner.helper.ListRecentLogEvents(stackOutputs["ActivityLogFunction"])
runner.GetKnownUserLastLogin(stackOutputs["TableName"], userName)

runner.resources.Cleanup()

log.Println(strings.Repeat("-", 88))
log.Println("Thanks for watching!")
log.Println(strings.Repeat("-", 88))
}

```

Tangani PostAuthentication pelatuk dengan fungsi Lambda.

```

const TABLE_NAME = "TABLE_NAME"

// LoginInfo defines structured login data that can be marshalled to a DynamoDB
// format.
type LoginInfo struct {
    UserPoolId string `dynamodbav:"UserPoolId"`
    ClientId   string `dynamodbav:"ClientId"`
    Time      string `dynamodbav:"Time"`
}

```

```
// UserInfo defines structured user data that can be marshalled to a DynamoDB
format.
type UserInfo struct {
    UserName string    `dynamodbav:"UserName"`
    UserEmail string    `dynamodbav:"UserEmail"`
    LastLogin LoginInfo `dynamodbav:"LastLogin"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
    userEmail, err := attributevalue.Marshal(user.UserEmail)
    if err != nil {
        panic(err)
    }
    return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
    dynamoClient *dynamodb.Client
}

// HandleRequest handles the PostAuthentication event by writing custom data to
the logs and
// to an Amazon DynamoDB table.
func (h *handler) HandleRequest(ctx context.Context,
    event events.CognitoEventUserPoolsPostAuthentication)
(events.CognitoEventUserPoolsPostAuthentication, error) {
    log.Printf("Received post authentication trigger from %v for user '%v'",
    event.TriggerSource, event.UserName)
    tableName := os.Getenv(TABLE_NAME)
    user := UserInfo{
        UserName: event.UserName,
        UserEmail: event.Request.UserAttributes["email"],
        LastLogin: LoginInfo{
            UserPoolId: event.UserPoolID,
            ClientId:   event CallerContext.ClientID,
            Time:       time.Now().Format(time.UnixDate),
        },
    }
    // Write to CloudWatch Logs.
    fmt.Printf("#%v", user)

    // Also write to an external system. This examples uses DynamoDB to demonstrate.
    userMap, err := attributevalue.MarshalMap(user)
```

```

if err != nil {
    log.Printf("Couldn't marshal to DynamoDB map. Here's why: %v\n", err)
} else if len(userMap) == 0 {
    log.Printf("User info marshaled to an empty map.")
} else {
    _, err := h.dynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
        Item:      userMap,
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't write to DynamoDB. Here's why: %v\n", err)
    } else {
        log.Printf("Wrote user info to DynamoDB table %v.\n", tableName)
    }
}

return event, nil
}

func main() {
    sdkConfig, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        log.Panicln(err)
    }
    h := handler{
        dynamoClient: dynamodb.NewFromConfig(sdkConfig),
    }
    lambda.Start(h.HandleRequest)
}

```

Buat struct yang melakukan tugas-tugas umum.

```

// IScenarioHelper defines common functions used by the workflows in this
// example.
type IScenarioHelper interface {
    Pause(secs int)
    GetStackOutputs(stackName string) (actions.StackOutputs, error)
    PopulateUserTable(tableName string)
    GetKnownUsers(tableName string) (actions.UserList, error)
    AddKnownUser(tableName string, user actions.User)
}

```

```
ListRecentLogEvents(functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
// example.
type ScenarioHelper struct {
    questioner demotools.IQuestioner
    dynamoActor *actions.DynamoActions
    cfnActor     *actions.CloudFormationActions
    cwlActor     *actions.CloudWatchLogsActions
    isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
ScenarioHelper {
    scenario := ScenarioHelper{
        questioner: questioner,
        dynamoActor: &actions.DynamoActions{DynamoClient:
            dynamodb.NewFromConfig(sdkConfig)},
        cfnActor:     &actions.CloudFormationActions{CfnClient:
            cloudformation.NewFromConfig(sdkConfig)},
        cwlActor:     &actions.CloudWatchLogsActions{CwlClient:
            cloudwatchlogs.NewFromConfig(sdkConfig)},
    }
    return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
    if !helper.isTestRun {
        time.Sleep(time.Duration(secs) * time.Second)
    }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
// structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
(actions.StackOutputs, error) {
    return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
```

```
log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
this example.\n", tableName)
err := helper.dynamoActor.PopulateTable(tableName)
if err != nil {
    panic(err)
}
}

// GetKnownUsers gets the users from the known users table in a structured
format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
error) {
    knownUsers, err := helper.dynamoActor.Scan(tableName)
    if err != nil {
        log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
tableName, err)
    }
    return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
    log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
table...\n",
        user.UserName, user.UserEmail)
    err := helper.dynamoActor.AddUser(tableName, user)
    if err != nil {
        panic(err)
    }
}

// ListRecentLogEvents gets the most recent log stream and events for the
specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
    log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
    helper.Pause(10)
    log.Println("Okay, let's check the logs to find what's happened recently with
your Lambda function.")
    logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
    if err != nil {
        panic(err)
    }
    log.Printf("Getting some recent events from log stream %v\n",
*logStream.LogStreamName)
```

```
events, err := helper.cwlActor.GetLogEvents(functionName,
*logStream.LogStreamName, 10)
if err != nil {
    panic(err)
}
for _, event := range events {
    log.Printf("\t%v", *event.Message)
}
log.Println(strings.Repeat("-", 88))
}
```

Buat struct yang membungkus tindakan Amazon Cognito.

```
type CognitoActions struct {
    CognitoClient *cognitoidentityprovider.Client
}

// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
trigger.
type Trigger int

const (
    PreSignUp Trigger = iota
    UserMigration
    PostAuthentication
)

type TriggerInfo struct {
    Trigger    Trigger
    HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
triggers ...TriggerInfo) error {
```

```
output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
&cognitoidentityprovider.DescribeUserPoolInput{
    UserPoolId: aws.String(userPoolId),
})
if err != nil {
    log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
userPoolId, err)
    return err
}
lambdaConfig := output.UserPool.LambdaConfig
for _, trigger := range triggers {
    switch trigger.Trigger {
    case PreSignUp:
        lambdaConfig.PreSignUp = trigger.HandlerArn
    case UserMigration:
        lambdaConfig.UserMigration = trigger.HandlerArn
    case PostAuthentication:
        lambdaConfig.PostAuthentication = trigger.HandlerArn
    }
}
_, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
&cognitoidentityprovider.UpdateUserPoolInput{
    UserPoolId:    aws.String(userPoolId),
    LambdaConfig: lambdaConfig,
})
if err != nil {
    log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
}
return err
}

// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(clientId string, userName string, password
string, userEmail string) (bool, error) {
    confirmed := false
    output, err := actor.CognitoClient.SignUp(context.TODO(),
&cognitoidentityprovider.SignUpInput{
        ClientId: aws.String(clientId),
        Password: aws.String(password),
        Username: aws.String(userName),
        UserAttributes: []types.AttributeType{
            {Name: aws.String("email"), Value: aws.String(userEmail)},
```

```
    },
  })
  if err != nil {
    var invalidPassword *types.InvalidPasswordException
    if errors.As(err, &invalidPassword) {
      log.Println(*invalidPassword.Message)
    } else {
      log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
    }
  } else {
    confirmed = output.UserConfirmed
  }
  return confirmed, err
}

// SignIn signs in a user to Amazon Cognito using a username and password
// authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
string) (*types.AuthenticationResultType, error) {
  var authResult *types.AuthenticationResultType
  output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
&cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:      "USER_PASSWORD_AUTH",
  ClientId:      aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
})
  if err != nil {
    var resetRequired *types.PasswordResetRequiredException
    if errors.As(err, &resetRequired) {
      log.Println(*resetRequired.Message)
    } else {
      log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
    }
  } else {
    authResult = output.AuthenticationResult
  }
  return authResult, err
}
```



```
// ForgotPassword starts a password recovery flow for a user. This flow typically
// sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
(*types.CodeDeliveryDetailsType, error) {
    output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
&cognitoidentityprovider.ForgotPasswordInput{
    ClientId: aws.String(clientId),
    Username: aws.String(userName),
})
    if err != nil {
        log.Printf("Couldn't start password reset for user '%v'. Here's why: %v\n",
userName, err)
    }
    return output.CodeDeliveryDetails, err
}

// ConfirmForgotPassword confirms a user with a confirmation code and a new
// password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
userName string, password string) error {
    _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
&cognitoidentityprovider.ConfirmForgotPasswordInput{
    ClientId:      aws.String(clientId),
    ConfirmationCode: aws.String(code),
    Password:      aws.String(password),
    Username:      aws.String(userName),
})
    if err != nil {
        var invalidPassword *types.InvalidPasswordException
        if errors.As(err, &invalidPassword) {
            log.Println(*invalidPassword.Message)
        } else {
            log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
        }
    }
    return err
}

// DeleteUser removes a user from the user pool.
```

```
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
    _, err := actor.CognitoClient.DeleteUser(context.TODO(),
        &cognitoidentityprovider.DeleteUserInput{
            AccessToken: aws.String(userAccessToken),
        })
    if err != nil {
        log.Printf("Couldn't delete user. Here's why: %v\n", err)
    }
    return err
}

// AdminCreateUser uses administrator credentials to add a user to a user pool.
// This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
    userEmail string) error {
    _, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
        &cognitoidentityprovider.AdminCreateUserInput{
            UserPoolId:      aws.String(userPoolId),
            Username:      aws.String(userName),
            MessageAction: types.MessageActionTypeSuppress,
            UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
                aws.String(userEmail)}}},
        })
    if err != nil {
        var userExists *types.UsernameExistsException
        if errors.As(err, &userExists) {
            log.Printf("User %v already exists in the user pool.", userName)
            err = nil
        } else {
            log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
        }
    }
    return err
}

// AdminSetUserPassword uses administrator credentials to set a password for a
// user without requiring a
// temporary password.
```

```

func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
string, password string) error {
_, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
&cognitoidentityprovider.AdminSetUserPasswordInput{
Password:  aws.String(password),
UserPoolId: aws.String(userPoolId),
Username:  aws.String(userName),
Permanent: true,
})
if err != nil {
var invalidPassword *types.InvalidPasswordException
if errors.As(err, &invalidPassword) {
log.Println(*invalidPassword.Message)
} else {
log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
err)
}
}
return err
}

```

Buat struct yang membungkus tindakan DynamoDB.

```

// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
actions
// used in the examples.
type DynamoActions struct {
DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
UserName string
UserEmail string
LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
UserPoolId string

```

```
    ClientId  string
    Time      string
}

// userList defines a list of users.
type userList struct {
    Users []User
}

// UserNameList returns the usernames contained in a userList as a list of
strings.
func (users *UserList) UserNameList() []string {
    names := make([]string, len(users.Users))
    for i := 0; i < len(users.Users); i++ {
        names[i] = users.Users[i].UserName
    }
    return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
    var err error
    var item map[string]types.AttributeValue
    var writeReqs []types.WriteRequest
    for i := 1; i < 4; i++ {
        item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), userEmail: fmt.Sprintf("test_email_%v@example.com", i)})
        if err != nil {
            log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
err)
            return err
        }
        writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
&types.PutRequest{Item: item}})
    }
    _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
&dynamodb.BatchWriteItemInput{
    RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
})
    if err != nil {
        log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
tableName, err)
    }
    return err
}
```

```

}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
    var userList UserList
    output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName, err)
    } else {
        err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
        if err != nil {
            log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
        }
    }
    return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
    userItem, err := attributevalue.MarshalMap(user)
    if err != nil {
        log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
    }
    _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
        Item:      userItem,
        TableName: aws.String(tableName),
    })
    if err != nil {
        log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
    }
    return err
}

```

Buat struct yang membungkus tindakan CloudWatch Log.

```

type CloudWatchLogsActions struct {
    CwlClient *cloudwatchlogs.Client
}

```

```
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
(types.LogStream, error) {
    var logStream types.LogStream
    logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
    output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
    &cloudwatchlogs.DescribeLogStreamsInput{
        Descending:    aws.Bool(true),
        Limit:          aws.Int32(1),
        LogGroupName:  aws.String(logGroupName),
        OrderBy:       types.OrderByLastEventTime,
    })
    if err != nil {
        log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
        logGroupName, err)
    } else {
        logStream = output.LogStreams[0]
    }
    return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
logStreamName string, eventCount int32) (
[]types.OutputLogEvent, error) {
    var events []types.OutputLogEvent
    logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
    output, err := actor.CwlClient.GetLogEvents(context.TODO(),
    &cloudwatchlogs.GetLogEventsInput{
        LogStreamName: aws.String(logStreamName),
        Limit:          aws.Int32(eventCount),
        LogGroupName:  aws.String(logGroupName),
    })
    if err != nil {
        log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
        logStreamName, err)
    } else {
        events = output.Events
    }
    return events, err
}
```

Buat struct yang membungkus tindakan AWS CloudFormation .

```
// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
    CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
// structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
    output, err := actor.CfnClient.DescribeStacks(context.TODO(),
        &cloudformation.DescribeStacksInput{
            StackName: aws.String(stackName),
        })
    if err != nil || len(output.Stacks) == 0 {
        log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
            stackName, err)
    }
    stackOutputs := StackOutputs{}
    for _, out := range output.Stacks[0].Outputs {
        stackOutputs[*out.OutputKey] = *out.OutputValue
    }
    return stackOutputs
}
```

Pembersihan sumber daya

```
// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
    userPoolId      string
    userAccessTokens []string
    triggers        []actions.Trigger
}
```

```

cognitoActor *actions.CognitoActions
questioner demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
demotools.IQuestioner) {
resources.userAccessTokens = []string{}
resources.triggers = []actions.Trigger{}
resources.cognitoActor = cognitoActor
resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
defer func() {
if r := recover(); r != nil {
log.Printf("Something went wrong during cleanup.\n%v\n", r)
log.Println("Use the AWS Management Console to remove any remaining resources
\n" +
"that were created for this scenario.")
}
}()

wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
resources that were created "+
"during this demo (y/n)?", "y")
if wantDelete {
for _, accessToken := range resources.userAccessTokens {
err := resources.cognitoActor.DeleteUser(accessToken)
if err != nil {
log.Println("Couldn't delete user during cleanup.")
panic(err)
}
log.Println("Deleted user.")
}
triggerList := make([]actions.TriggerInfo, len(resources.triggers))
for i := 0; i < len(resources.triggers); i++ {
triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
HandlerArn: nil}
}
err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,
triggerList...)
if err != nil {
log.Println("Couldn't update Cognito triggers during cleanup.")
}
}

```



```
    panic(err)
  }
  log.Println("Removed Cognito triggers from user pool.")
} else {
  log.Println("Be sure to remove resources when you're done with them to avoid
unexpected charges!")
}
}
```

- Untuk API detailnya, lihat topik berikut di AWS SDK for Go API Referensi.
 - [AdminCreateUser](#)
 - [AdminSetUserPassword](#)
 - [DeleteUser](#)
 - [InitiateAuth](#)
 - [UpdateUserPool](#)

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Contoh tanpa server untuk penggunaan Lambda AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan Lambda dengan AWS SDKs

Contoh

- [Menghubungkan ke RDS database Amazon dalam fungsi Lambda](#)
- [Memanggil fungsi Lambda dari pemicu Kinesis](#)
- [Memanggil fungsi Lambda dari pemicu DynamoDB](#)
- [Memanggil fungsi Lambda dari pemicu Amazon DocumentDB](#)
- [Memanggil fungsi Lambda dari pemicu Amazon MSK](#)
- [Menginvokasi fungsi Lambda dari pemicu Amazon S3](#)
- [Memanggil fungsi Lambda dari pemicu Amazon SNS](#)
- [Memanggil fungsi Lambda dari pemicu Amazon SQS](#)
- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Kinesis](#)

- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu DynamoDB](#)
- [Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Amazon SQS](#)

Menghubungkan ke RDS database Amazon dalam fungsi Lambda

Contoh kode berikut menunjukkan bagaimana menerapkan fungsi Lambda yang terhubung ke database. RDS Fungsi membuat permintaan database sederhana dan mengembalikan hasilnya.

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Go.

```
/*
Golang v2 code here.
*/

package main

import (
    "context"
    "database/sql"
    "encoding/json"
    "fmt"
    "os"

    "github.com/aws/aws-lambda-go/lambda"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
    _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
    Name string `json:"name"`
```

```
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {

    var dbName string = os.Getenv("DatabaseName")
    var dbUser string = os.Getenv("DatabaseUser")
    var dbHost string = os.Getenv("DBHost") // Add hostname without https
    var dbPort int = os.Getenv("Port")      // Add port number
    var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
    var region string = os.Getenv("AWS_REGION")

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
        context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
        panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authenticationToken, dbEndpoint, dbName,
    )

    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    defer db.Close()

    var sum int
    err = db.QueryRow("SELECT ?? AS sum", 3, 2).Scan(&sum)
    if err != nil {
        panic(err)
    }
    s := fmt.Sprint(sum)
    message := fmt.Sprintf("The selected sum is: %s", s)

    messageBytes, err := json.Marshal(message)
    if err != nil {
        return nil, err
    }
}
```

```
}

messageString := string(messageBytes)
return map[string]interface{}{
    "statusCode": 200,
    "headers":    map[string]string{"Content-Type": "application/json"},
    "body":      messageString,
}, nil
}

func main() {
    lambda.Start(HandleRequest)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rdsdata.RdsDataClient;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementRequest;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.rdsdata.model.Field;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
```

```
public class RdsLambdaHandler implements
RequestHandler<APIGatewayProxyRequestEvent, APIGatewayProxyResponseEvent> {

    @Override
    public APIGatewayProxyResponseEvent handleRequest(APIGatewayProxyRequestEvent
event, Context context) {
        APIGatewayProxyResponseEvent response = new
APIGatewayProxyResponseEvent();

        try {
            // Obtain auth token
            String token = createAuthToken();

            // Define connection configuration
            String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true",
                System.getenv("ProxyHostName"),
                System.getenv("Port"),
                System.getenv("DBName"));

            // Establish a connection to the database
            try (Connection connection =
DriverManager.getConnection(connectionString, System.getenv("DBUserName"),
token);
                PreparedStatement statement =
connection.prepareStatement("SELECT ? + ? AS sum")) {

                statement.setInt(1, 3);
                statement.setInt(2, 2);

                try (ResultSet resultSet = statement.executeQuery()) {
                    if (resultSet.next()) {
                        int sum = resultSet.getInt("sum");
                        response.setStatusCode(200);
                        response.setBody("The selected sum is: " + sum);
                    }
                }
            }
        } catch (Exception e) {
            response.setStatusCode(500);
            response.setBody("Error: " + e.getMessage());
        }
    }
}
```

```
        return response;
    }

    private String createAuthToken() {
        // Create RDS Data Service client
        RdsDataClient rdsDataClient = RdsDataClient.builder()
            .region(Region.of(System.getenv("AWS_REGION")))
            .credentialsProvider(DefaultCredentialsProvider.create())
            .build();

        // Define authentication request
        ExecuteStatementRequest request = ExecuteStatementRequest.builder()
            .resourceArn(System.getenv("ProxyHostName"))
            .secretArn(System.getenv("DBUserName"))
            .database(System.getenv("DBName"))
            .sql("SELECT 'RDS IAM Authentication'")
            .build();

        // Execute request and obtain authentication token
        ExecuteStatementResponse response =
            rdsDataClient.executeStatement(request);
        Field tokenField = response.records().get(0).get(0);

        return tokenField.stringValue();
    }
}
```

JavaScript

SDKuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan [contoh lengkapnya](#) dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
/*
Node.js code here.
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;
}
```

```
}

export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
};
```

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan TypeScript

```
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

// RDS settings
// Using '!' (non-null assertion operator) to tell the TypeScript compiler that
// the DB settings are not null or undefined,
const proxy_host_name = process.env.PROXY_HOST_NAME!
const port = parseInt(process.env.PORT!)
const db_name = process.env.DB_NAME!
const db_user_name = process.env.DB_USER_NAME!
const aws_region = process.env.AWS_REGION!

async function createAuthToken(): Promise<string> {

  // Create RDS Signer object
  const signer = new Signer({
    hostname: proxy_host_name,
    port: port,
    region: aws_region,
    username: db_user_name
  });

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}
```



```
}

async function dbOps(): Promise<mysql.QueryResult | undefined> {
  try {
    // Obtain auth token
    const token = await createAuthToken();
    const conn = await mysql.createConnection({
      host: proxy_host_name,
      user: db_user_name,
      password: token,
      database: db_name,
      ssl: 'Amazon RDS' // Ensure you have the CA bundle for SSL connection
    });
    const [rows, fields] = await conn.execute('SELECT ? + ? AS sum', [3, 2]);
    console.log('result:', rows);
    return rows;
  }
  catch (err) {
    console.log(err);
  }
}


export const lambdaHandler = async (event: any): Promise<{ statusCode: number;
body: string }> => {
  // Execute database flow
  const result = await dbOps();

  // Return error if result is undefined
  if (result == undefined)
    return {
      statusCode: 500,
      body: JSON.stringify(`Error with connection to DB host`)
    }

  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify(`The selected sum is: ${result[0].sum}`)
  };
};
```

PHP

SDK untuk PHP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan PHP

```
<?php
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;
use Aws\Rds\AuthTokenGenerator;
use Aws\Credentials\CredentialProvider;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    private function getAuthToken(): string {
        // Define connection authentication parameters
        $dbConnection = [
            'hostname' => getenv('DB_HOSTNAME'),
            'port' => getenv('DB_PORT'),
            'username' => getenv('DB_USERNAME'),
            'region' => getenv('AWS_REGION'),
        ];
    }
}
```

```
// Create RDS AuthTokenGenerator object
$generator = new
AuthTokenGenerator(CredentialProvider::defaultProvider());

// Request authorization token from RDS, specifying the username
return $generator->createToken(
    $dbConnection['hostname'] . ':' . $dbConnection['port'],
    $dbConnection['region'],
    $dbConnection['username']
);
}

private function getQueryResults() {
    // Obtain auth token
    $token = $this->getAuthToken();

    // Define connection configuration
    $connectionConfig = [
        'host' => getenv('DB_HOSTNAME'),
        'user' => getenv('DB_USERNAME'),
        'password' => $token,
        'database' => getenv('DB_NAME'),
    ];

    // Create the connection to the DB
    $conn = new PDO(
        "mysql:host={$connectionConfig['host']};dbname={$connectionConfig['database']}",
        $connectionConfig['user'],
        $connectionConfig['password'],
        [
            PDO::MYSQL_ATTR_SSL_CA => '/path/to/rds-ca-2019-root.pem',
            PDO::MYSQL_ATTR_SSL_VERIFY_SERVER_CERT => true,
        ]
    );

    // Obtain the result of the query
    $stmt = $conn->prepare('SELECT ?+? AS sum');
    $stmt->execute([3, 2]);

    return $stmt->fetch(PDO::FETCH_ASSOC);
}
```

```
/**
 * @param mixed $event
 * @param Context $context
 * @return array
 */
public function handle(mixed $event, Context $context): array
{
    $this->logger->info("Processing query");

    // Execute database flow
    $result = $this->getQueryResults();

    return [
        'sum' => $result['sum']
    ];
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Python.

```
import json
import os
import boto3
import pymysql

# RDS settings
proxy_host_name = os.environ['PROXY_HOST_NAME']
port = int(os.environ['PORT'])
db_name = os.environ['DB_NAME']
```

```
db_user_name = os.environ['DB_USER_NAME']
aws_region = os.environ['AWS_REGION']

# Fetch RDS Auth Token
def get_auth_token():
    client = boto3.client('rds')
    token = client.generate_db_auth_token(
        DBHostname=proxy_host_name,
        Port=port
        DBUsername=db_user_name
        Region=aws_region
    )
    return token

def lambda_handler(event, context):
    token = get_auth_token()
    try:
        connection = pymysql.connect(
            host=proxy_host_name,
            user=db_user_name,
            password=token,
            db=db_name,
            port=port,
            ssl={'ca': 'Amazon RDS'} # Ensure you have the CA bundle for SSL
        )

        with connection.cursor() as cursor:
            cursor.execute('SELECT %s + %s AS sum', (3, 2))
            result = cursor.fetchone()

        return result

    except Exception as e:
        return (f"Error: {str(e)}") # Return an error message if an exception
    occurs
```

Ruby

SDK Kuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Ruby.

```
# Ruby code here.

require 'aws-sdk-rds'
require 'json'
require 'mysql2'

def lambda_handler(event:, context:)
  endpoint = ENV['DBEndpoint'] # Add the endpoint without https"
  port = ENV['Port']           # 3306
  user = ENV['DBUser']
  region = ENV['DBRegion']     # 'us-east-1'
  db_name = ENV['DBName']

  credentials = Aws::Credentials.new(
    ENV['AWS_ACCESS_KEY_ID'],
    ENV['AWS_SECRET_ACCESS_KEY'],
    ENV['AWS_SESSION_TOKEN']
  )
  rds_client = Aws::RDS::AuthTokenGenerator.new(
    region: region,
    credentials: credentials
  )

  token = rds_client.auth_token(
    endpoint: endpoint+ ':' + port,
    user_name: user,
    region: region
  )

  begin
    conn = Mysql2::Client.new(
```

```

    host: endpoint,
    username: user,
    password: token,
    port: port,
    database: db_name,
    sslca: '/var/task/global-bundle.pem',
    sslverify: true,
    enableCleartextPlugin: true
  )
  a = 3
  b = 2
  result = conn.query("SELECT #{a} + #{b} AS sum").first['sum']
  puts result
  conn.close
  {
    statusCode: 200,
    body: result.to_json
  }
rescue => e
  puts "Database connection failed due to #{e}"
end
end

```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menghubungkan ke RDS database Amazon dalam fungsi Lambda menggunakan Rust.

```

use aws_config::BehaviorVersion;
use aws_credential_types::provider::ProvideCredentials;
use aws_sigv4::{
    http_request::{sign, SignableBody, SignableRequest, SigningSettings},
    sign::v4,
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

```

```
use serde_json::{json, Value};
use sqlx::postgres::PgConnectOptions;
use std::env;
use std::time::{Duration, SystemTime};

const RDS_CERTS: &[u8] = include_bytes!("global-bundle.pem");

async fn generate_rds_iam_token(
    db_hostname: &str,
    port: u16,
    db_username: &str,
) -> Result<String, Error> {
    let config = aws_config::load_defaults(BehaviorVersion::v2024_03_28()).await;

    let credentials = config
        .credentials_provider()
        .expect("no credentials provider found")
        .provide_credentials()
        .await
        .expect("unable to load credentials");
    let identity = credentials.into();
    let region = config.region().unwrap().to_string();

    let mut signing_settings = SigningSettings::default();
    signing_settings.expires_in = Some(Duration::from_secs(900));
    signing_settings.signature_location =
aws_sigv4::http_request::SignatureLocation::QueryParams;

    let signing_params = v4::SigningParams::builder()
        .identity(&identity)
        .region(&region)
        .name("rds-db")
        .time(SystemTime::now())
        .settings(signing_settings)
        .build()?;

    let url = format!(
        "https://{db_hostname}:{port}/?Action=connect&DBUser={db_user}",
        db_hostname = db_hostname,
        port = port,
        db_user = db_username
    );

    let signable_request =
```



```

        SignableRequest::new("GET", &url, std::iter::empty(),
SignableBody::Bytes(&[]))
            .expect("signable request");

        let (signing_instructions, _signature) =
            sign(signable_request, &signing_params.into())?.into_parts();

        let mut url = url::Url::parse(&url).unwrap();
        for (name, value) in signing_instructions.params() {
            url.query_pairs_mut().append_pair(name, &value);
        }

        let response = url.to_string().split_off("https://".len());

        Ok(response)
    }

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(handler)).await
}

async fn handler(_event: LambdaEvent<Value>) -> Result<Value, Error> {
    let db_host = env::var("DB_HOSTNAME").expect("DB_HOSTNAME must be set");
    let db_port = env::var("DB_PORT")
        .expect("DB_PORT must be set")
        .parse:::<u16>()
        .expect("PORT must be a valid number");
    let db_name = env::var("DB_NAME").expect("DB_NAME must be set");
    let db_user_name = env::var("DB_USERNAME").expect("DB_USERNAME must be set");

    let token = generate_rds_iam_token(&db_host, db_port, &db_user_name).await?;

    let opts = PgConnectOptions::new()
        .host(&db_host)
        .port(db_port)
        .username(&db_user_name)
        .password(&token)
        .database(&db_name)
        .ssl_root_cert_from_pem(RDS_CERTS.to_vec())
        .ssl_mode(sqlx::postgres::PgSslMode::Require);

    let pool = sqlx::postgres::PgPoolOptions::new()
        .connect_with(opts)

```

```
        .await?;

    let result: i32 = sqlx::query_scalar("SELECT $1 + $2")
        .bind(3)
        .bind(2)
        .fetch_one(&pool)
        .await?;

    println!("Result: {:?}", result);

    Ok(json!({
        "statusCode": 200,
        "content-type": "text/plain",
        "body": format!("The selected sum is: {result}")
    })))
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu Kinesis

Contoh kode berikut menunjukkan bagaimana menerapkan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima catatan dari aliran Kinesis. Fungsi mengambil payload Kinesis, mendekode dari Base64, dan mencatat konten rekaman.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace KinesisIntegrationSampleCode;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
{record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
records.");
    }
}
```

```
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "log"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
    if len(kinesisEvent.Records) == 0 {
        log.Printf("empty Kinesis event received")
        return nil
    }
}
```

```

for _, record := range kinesisEvent.Records {
    log.Printf("processed Kinesis event with EventId: %v", record.EventID)
    recordDataBytes := record.Kinesis.Data
    recordDataText := string(recordDataBytes)
    log.Printf("record data: %v", recordDataText)
    // TODO: Do interesting work based on the new data
}
log.Printf("successfully processed %v records", len(kinesisEvent.Records))
return nil
}

func main() {
    lambda.Start(handler)
}

```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan Java.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {

```

```
        logger.log("Empty Kinesis Event received");
        return null;
    }
    for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
        try {
            logger.log("Processed Event with EventID: "+record.getEventID());
            String data = new String(record.getKinesis().getData().array());
            logger.log("Data:"+ data);
            // TODO: Do interesting work based on the new data
        }
        catch (Exception ex) {
            logger.log("An error occurred:"+ex.getMessage());
            throw ex;
        }
    }
    logger.log("Successfully processed:"+event.getRecords().size()+"
records");
    return null;
}
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan menggunakan Lambda. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    for (const record of event.Records) {
        try {
            console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
            const recordData = await getRecordDataAsync(record.kinesis);
```

```
    console.log(`Record Data: ${recordData}`);
    // TODO: Do interesting work based on the new data
  } catch (err) {
    console.error(`An error occurred ${err}`);
    throw err;
  }
}
console.log(`Successfully processed ${event.Records.length} records.`);
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Mengonsumsi acara Kinesis dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
```

```

    logger.info(`Record Data: ${recordData}`);
    // TODO: Do interesting work based on the new data
  } catch (err) {
    logger.error(`An error occurred ${err}`);
    throw err;
  }
  logger.info(`Successfully processed ${event.Records.length} records.`);
}
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}

```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan menggunakan Lambda. PHP

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
use Bref\Logger\StderrLogger;

```



```
require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleKinesis(KinesisEvent $event, Context $context): void
    {
        $this->logger->info("Processing records");
        $records = $event->getRecords();
        foreach ($records as $record) {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
            marked as failed
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Kinesis dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
  puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
  here.
  return data
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Kinesis dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
{
    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    event.payload.records.iter().for_each(|record| {
        tracing::info!("EventId:
{}", record.event_id.as_deref().unwrap_or_default());

        let record_data = std::str::from_utf8(&record.kinesis.data);

        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
}
```

```
        // disabling time is handy because CloudWatch will add the ingestion
time.
        .without_time()
        .init();

        run(service_fn(function_handler)).await
    }
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu DynamoDB

Contoh kode berikut menunjukkan bagaimana menerapkan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima catatan dari aliran DynamoDB. Fungsi mengambil payload DynamoDB dan mencatat isi catatan.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara DynamoDB dengan Lambda menggunakan .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSer...
```

```
namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext
context)
    {
        context.Logger.LogInformation($"Beginning to process
{dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }

        context.Logger.LogInformation("Stream processing complete.");
    }
}
```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
```

```

"github.com/aws/aws-lambda-go/lambda"
"github.com/aws/aws-lambda-go/events"
"fmt"
)

func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,
error) {
    if len(event.Records) == 0 {
        return nil, fmt.Errorf("received empty event")
    }

    for _, record := range event.Records {
        LogDynamoDBRecord(record)
    }

    message := fmt.Sprintf("Records processed: %d", len(event.Records))
    return &message, nil
}

func main() {
    lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
    fmt.Println(record.EventID)
    fmt.Println(record.EventName)
    fmt.Printf("%+v\n", record.Change)
}

```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;
```

```
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
    com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
    GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
        GSON.toJson(record.getDynamodb()));
    }
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
```



```
console.log(JSON.stringify(event, null, 2));
event.Records.forEach(record => {
  logDynamoDBRecord(record);
});

const logDynamoDBRecord = (record) => {
  console.log(record.eventID);
  console.log(record.eventName);
  console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

Mengonsumsi acara DynamoDB dengan Lambda menggunakan TypeScript

```
export const handler = async (event, context) => {
  console.log(JSON.stringify(event, null, 2));
  event.Records.forEach(record => {
    logDynamoDBRecord(record);
  });
}

const logDynamoDBRecord = (record) => {
  console.log(record.eventID);
  console.log(record.eventName);
  console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan PHP

```
<?php
```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\DynamoDb\DynamoDbHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends DynamoDbHandler
{
    private StderrLogger $logger;

    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
    {
        $this->logger->info("Processing DynamoDb table items");
        $records = $event->getRecords();

        foreach ($records as $record) {
            $eventName = $record->getEventName();
            $keys = $record->getKeys();
            $old = $record->getOldImage();
            $new = $record->getNewImage();

            $this->logger->info("Event Name:". $eventName. "\n");
            $this->logger->info("Keys:". json_encode($keys). "\n");
            $this->logger->info("Old Image:". json_encode($old). "\n");
            $this->logger->info("New Image:". json_encode($new));

            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
            marked as failed
        }
    }
}
```

```
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords items");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Python.

```
import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara DynamoDB dengan Lambda menggunakan Ruby.

```
def lambda_handler(event:, context:)
  return 'received empty event' if event['Records'].empty?

  event['Records'].each do |record|
    log_dynamodb_record(record)
  end

  "Records processed: #{event['Records'].length}"
end

def log_dynamodb_record(record)
  puts record['eventID']
  puts record['eventName']
  puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
end
```

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara DynamoDB dengan Lambda menggunakan Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
};

// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
    ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_dynamo_dbrecord(record);
    }

    tracing::info!("Dynamo db records processed");

    // Prepare the response
    Ok(())
}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())
}
```

```
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu Amazon DocumentDB

Contoh kode berikut menunjukkan cara menerapkan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima catatan dari aliran perubahan DocumentDB. Fungsi mengambil payload DocumentDB dan mencatat isi catatan.

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Go.

```
package main
```

```
import (
    "context"
    "encoding/json"
    "fmt"

    "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
    Events []Record `json:"events"`
}

type Record struct {
    Event struct {
        OperationType string `json:"operationType"`
        NS             struct {
            DB   string `json:"db"`
            Coll string `json:"coll"`
        } `json:"ns"`
        FullDocument interface{} `json:"fullDocument"`
    } `json:"event"`
}

func main() {
    lambda.Start(handler)
}

func handler(ctx context.Context, event Event) (string, error) {
    fmt.Println("Loading function")
    for _, record := range event.Events {
        logDocumentDBEvent(record)
    }

    return "OK", nil
}

func logDocumentDBEvent(record Record) {
    fmt.Printf("Operation type: %s\n", record.Event.OperationType)
    fmt.Printf("db: %s\n", record.Event.NS.DB)
    fmt.Printf("collection: %s\n", record.Event.NS.Coll)
    docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", " ")
    fmt.Printf("Full document: %s\n", string(docBytes))
}
```

JavaScript

SDK Kuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara Amazon DocumentDB dengan menggunakan Lambda. JavaScript

```
console.log('Loading function');
exports.handler = async (event, context) => {
  event.events.forEach(record => {
    logDocumentDBEvent(record);
  });
  return 'OK';
};

const logDocumentDBEvent = (record) => {
  console.log('Operation type: ' + record.event.operationType);
  console.log('db: ' + record.event.ns.db);
  console.log('collection: ' + record.event.ns.coll);
  console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
    2));
};
```

Mengkonsumsi acara Amazon DocumentDB dengan Lambda menggunakan TypeScript

```
import { DocumentDBEventRecord, DocumentDBEventSubscriptionContext } from 'aws-lambda';

console.log('Loading function');

export const handler = async (
  event: DocumentDBEventSubscriptionContext,
```



```

context: any
): Promise<string> => {
  event.events.forEach((record: DocumentDBEventRecord) => {
    logDocumentDBEvent(record);
  });
  return 'OK';
};

const logDocumentDBEvent = (record: DocumentDBEventRecord): void => {
  console.log('Operation type: ' + record.event.operationType);
  console.log('db: ' + record.event.ns.db);
  console.log('collection: ' + record.event.ns.coll);
  console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
  2));
};

```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan menggunakan Lambda. PHP

```

<?php

require __DIR__.'./vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Handler;

class DocumentDBEventHandler implements Handler
{
  public function handle($event, Context $context): string
  {

    $events = $event['events'] ?? [];

```

```

    foreach ($events as $record) {
        $this->logDocumentDBEvent($record['event']);
    }
    return 'OK';
}

private function logDocumentDBEvent($event): void
{
    // Extract information from the event record

    $operationType = $event['operationType'] ?? 'Unknown';
    $db = $event['ns']['db'] ?? 'Unknown';
    $collection = $event['ns']['coll'] ?? 'Unknown';
    $fullDocument = $event['fullDocument'] ?? [];

    // Log the event details

    echo "Operation type: $operationType\n";
    echo "Database: $db\n";
    echo "Collection: $collection\n";
    echo "Full document: " . json_encode($fullDocument, JSON_PRETTY_PRINT) .
"\n";
}
}
return new DocumentDBEventHandler();

```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Python.

```

import json

def lambda_handler(event, context):
    for record in event.get('events', []):

```

```

        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})

    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
    print("Full document:", json.dumps(full_document, indent=2))

```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Ruby.

```

require 'json'

def lambda_handler(event:, context:)
    event['events'].each do |record|
        log_document_db_event(record)
    end
    'OK'
end

def log_document_db_event(record)
    event_data = record['event'] || {}
    operation_type = event_data['operationType'] || 'Unknown'
    db = event_data.dig('ns', 'db') || 'Unknown'
    collection = event_data.dig('ns', 'coll') || 'Unknown'
    full_document = event_data['fullDocument'] || {}

```

```
puts "Operation type: #{operation_type}"
puts "db: #{db}"
puts "collection: #{collection}"
puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara Amazon DocumentDB dengan Lambda menggunakan Rust.

```
use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::documentdb::{DocumentDbEvent, DocumentDbInnerEvent},
};

// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
    ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<DocumentDbEvent>) -> Result<(),
    Error> {

    tracing::info!("Event Source ARN: {:?}", event.payload.event_source_arn);
    tracing::info!("Event Source: {:?}", event.payload.event_source);

    let records = &event.payload.events;
```

```
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_document_db_event(record);
    }

    tracing::info!("Document db records processed");

    // Prepare the response
    Ok(())
}

fn log_document_db_event(record: &DocumentDbInnerEvent)-> Result<(), Error>{
    tracing::info!("Change Event: {:?}", record.event);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu Amazon MSK

Contoh kode berikut menunjukkan cara mengimplementasikan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima catatan dari klaster AmazonMSK. Fungsi mengambil MSK payload dan mencatat isi catatan.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan menggunakan Lambda. NET.

```
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KafkaEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace MSKLambda;

public class Function
{
    /// <param name="input">The event for the Lambda function handler to
    process.</param>
    /// <param name="context">The ILambdaContext that provides methods for
    logging and describing the Lambda environment.</param>
    /// <returns></returns>
    public void FunctionHandler(KafkaEvent evnt, ILambdaContext context)
    {
```

```
    foreach (var record in evnt.Records)
    {
        Console.WriteLine("Key:" + record.Key);
        foreach (var eventRecord in record.Value)
        {
            var valueBytes = eventRecord.Value.ToArray();
            var valueText = Encoding.UTF8.GetString(valueBytes);

            Console.WriteLine("Message:" + valueText);
        }
    }
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan Lambda menggunakan Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent;
import com.amazonaws.services.lambda.runtime.events.KafkaEvent.KafkaEventRecord;

import java.util.Base64;
import java.util.Map;

public class Example implements RequestHandler<KafkaEvent, Void> {

    @Override
    public Void handleRequest(KafkaEvent event, Context context) {
```

```
    for (Map.Entry<String, java.util.List<KafkaEventRecord>> entry :
event.getRecords().entrySet()) {
        String key = entry.getKey();
        System.out.println("Key: " + key);

        for (KafkaEventRecord record : entry.getValue()) {
            System.out.println("Record: " + record);

            byte[] value = Base64.getDecoder().decode(record.getValue());
            String message = new String(value);
            System.out.println("Message: " + message);
        }
    }

    return null;
}
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan menggunakan Lambda. JavaScript

```
exports.handler = async (event) => {
    // Iterate through keys
    for (let key in event.records) {
        console.log('Key: ', key)
        // Iterate through records
        event.records[key].map((record) => {
            console.log('Record: ', record)
            // Decode base64
            const msg = Buffer.from(record.value, 'base64').toString()
            console.log('Message:', msg)
        })
    }
}
```



```
    })  
  }  
}
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan Lambda menggunakan Python.

```
import base64  
  
def lambda_handler(event, context):  
    # Iterate through keys  
    for key in event['records']:  
        print('Key:', key)  
        # Iterate through records  
        for record in event['records'][key]:  
            print('Record:', record)  
            # Decode base64  
            msg = base64.b64decode(record['value']).decode('utf-8')  
            print('Message:', msg)
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi MSK acara Amazon dengan Lambda menggunakan Ruby.

```
require 'base64'

def lambda_handler(event:, context:)
  # Iterate through keys
  event['records'].each do |key, records|
    puts "Key: #{key}"

    # Iterate through records
    records.each do |record|
      puts "Record: #{record}"

      # Decode base64
      msg = Base64.decode64(record['value'])
      puts "Message: #{msg}"
    end
  end
end
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Menginvokasi fungsi Lambda dari pemicu Amazon S3

Contoh kode berikut menunjukkan cara mengimplementasikan fungsi Lambda yang menerima peristiwa yang dipicu dengan mengunggah objek ke bucket S3. Fungsi ini mengambil nama bucket S3 dan kunci objek dari parameter event dan memanggil Amazon API S3 untuk mengambil dan mencatat jenis konten objek.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi acara S3 dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace S3Integration
{
    public class Function
    {
        private static AmazonS3Client _s3Client;
        public Function() : this(null)
        {
        }

        internal Function(AmazonS3Client s3Client)
        {
            _s3Client = s3Client ?? new AmazonS3Client();
        }

        public async Task<string> Handler(S3Event evt, ILambdaContext context)
        {
            try
            {
                if (evt.Records.Count <= 0)
                {
                    context.Logger.LogLine("Empty S3 Event received");
                    return string.Empty;
                }

                var bucket = evt.Records[0].S3.Bucket.Name;
                var key = HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

                context.Logger.LogLine($"Request is for {bucket} and {key}");
            }
        }
    }
}
```

```
        var objectResult = await _s3Client.GetObjectAsync(bucket, key);

        context.Logger.LogLine($"Returning {objectResult.Key}");

        return objectResult.Key;
    }
    catch (Exception e)
    {
        context.Logger.LogLine($"Error processing request -
{e.Message}");

        return string.Empty;
    }
}
}
```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "log"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
)
```

```
)

func handler(ctx context.Context, s3Event events.S3Event) error {
    sdkConfig, err := config.LoadDefaultConfig(ctx)
    if err != nil {
        log.Printf("failed to load default config: %s", err)
        return err
    }
    s3Client := s3.NewFromConfig(sdkConfig)

    for _, record := range s3Event.Records {
        bucket := record.S3.Bucket.Name
        key := record.S3.Object.URLDecodedKey
        headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
            Bucket: &bucket,
            Key:     &key,
        })
        if err != nil {
            log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
            return err
        }
        log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
            *headOutput.ContentType)
    }

    return nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
    com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNotifi

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger = LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
            S3EventNotificationRecord record = s3event.getRecords().get(0);
            String srcBucket = record.getS3().getBucket().getName();
            String srcKey = record.getS3().getObject().getUrlDecodedKey();

            S3Client s3Client = S3Client.builder().build();
            HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
srcKey);

            logger.info("Successfully retrieved " + srcBucket + "/" + srcKey + " of
type " + headObject.contentType());

            return "Ok";
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String bucket,
String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
```

```
        .bucket(bucket)
        .key(key)
        .build();
    return s3Client.headObject(headObjectRequest);
}
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan menggunakan JavaScript Lambda.

```
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

export const handler = async (event, context) => {

    // Get the object from the event and show its content type
    const bucket = event.Records[0].s3.bucket.name;
    const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g,
    ' '));

    try {
        const { ContentType } = await client.send(new HeadObjectCommand({
            Bucket: bucket,
            Key: key,
        }));

        console.log('CONTENT TYPE:', ContentType);
        return ContentType;

    } catch (err) {
        console.log(err);
    }
}
```

```
    const message = `Error getting object ${key} from bucket ${bucket}. Make
    sure they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

Mengonsumsi acara S3 dengan menggunakan TypeScript Lambda.


```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> => {
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, '
  '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make sure
    they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```


PHP

SDKuntuk PHP

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan menggunakan PHP Lambda.

```
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());

            try {
```

```
        $fileSize = urldecode($record->getObject()->getSize());
        echo "File Size: " . $fileSize . "\n";
        // TODO: Implement your custom processing logic here
    } catch (Exception $e) {
        echo $e->getMessage() . "\n";
        echo 'Error getting object ' . $key . ' from bucket ' .
$bucket . '. Make sure they exist and your bucket is in the same region as this
function.' . "\n";
        throw $e;
    }
}
}
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')

def lambda_handler(event, context):
```

```

#print("Received event: " + json.dumps(event, indent=2))

# Get the object from the event and show its content type
bucket = event['Records'][0]['s3']['bucket']['name']
key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'],
encoding='utf-8')
try:
    response = s3.get_object(Bucket=bucket, Key=key)
    print("CONTENT TYPE: " + response['ContentType'])
    return response['ContentType']
except Exception as e:
    print(e)
    print('Error getting object {} from bucket {}. Make sure they exist and
your bucket is in the same region as this function.'.format(key, bucket))
    raise e

```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi acara S3 dengan Lambda menggunakan Ruby.

```

require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'

def lambda_handler(event:, context:)
  s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
  # puts "Received event: #{JSON.dump(event)}"

  # Get the object from the event and show its content type
  bucket = event['Records'][0]['s3']['bucket']['name']

```

```
key = URI.decode_www_form_component(event['Records'][0]['s3']['object']['key'],
Encoding::UTF_8)
begin
  response = s3.get_object(bucket: bucket, key: key)
  puts "CONTENT TYPE: #{response.content_type}"
  return response.content_type
rescue StandardError => e
  puts e.message
  puts "Error getting object #{key} from bucket #{bucket}. Make sure they exist
and your bucket is in the same region as this function."
  raise e
end
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Menggunakan peristiwa S3 dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Main function
#[tokio::main]
async fn main() -> Result<(), Error> {
  tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();
```

```
// Initialize the AWS SDK for Rust
let config = aws_config::load_from_env().await;
let s3_client = Client::new(&config);

let res = run(service_fn(|request: LambdaEvent<S3Event>| {
    function_handler(&s3_client, request)
})).await;

res
}

async fn function_handler(
    s3_client: &Client,
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request from
SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket = evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket
name to exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object key to
exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;

    match s3_get_object_result {
        Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
contains a 'body' property of type ByteStream"),
        Err(_) => tracing::info!("Failure with S3 Get Object request")
    }

    Ok(())
}
```

```
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu Amazon SNS

Contoh kode berikut menunjukkan cara menerapkan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima pesan dari suatu SNS topik. Fungsi mengambil pesan dari parameter peristiwa dan mencatat konten setiap pesan.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace SnsIntegration;

public class Function
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
```


```
    foreach (var record in evnt.Records)
    {
        await ProcessRecordAsync(record, context);
    }
    context.Logger.LogInformation("done");
}

private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
ILambdaContext context)
{
    try
    {
        context.Logger.LogInformation($"Processed record
{record.Sns.Message}");

        // TODO: Do interesting work based on the new message
        await Task.CompletedTask;
    }
    catch (Exception e)
    {
        //You can use Dead Letter Queue to handle failures. By configuring a
Lambda DLQ.
        context.Logger.LogError($"An error occurred");
        throw;
    }
}
}
```

Go

SDKuntuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
package main

import (
    "context"
    "fmt"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
    for _, record := range snsEvent.Records {
        processMessage(record)
    }
    fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
    message := record.SNS.Message
    fmt.Printf("Processed message: %s\n", message)
    // TODO: Process your record here
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```



```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;

import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }

    public void processRecord(SNSRecord record) {
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }
}
```

JavaScript

SDKuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi SNS acara dengan menggunakan Lambda. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record) {
  try {
    const message = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Mengkonsumsi SNS acara dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";

export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
```

```
    ): Promise<void> => {
      for (const record of event.Records) {
        await processMessageAsync(record);
      }
      console.info("done");
    };

    async function processMessageAsync(record: SNSEventRecord): Promise<any> {
      try {
        const message: string = JSON.stringify(record.Sns.Message);
        console.log(`Processed message ${message}`);
        await Promise.resolve(1); //Placeholder for actual async work
      } catch (err) {
        console.error("An error occurred");
        throw err;
      }
    }
  }
}
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan menggunakan Lambda. PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
PHP functions runtime for AWS Lambda.
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
```

```
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-lambda-custom-runtime-for-php-a-practical-example/  
*/  
  
// Additional composer packages may be required when using Bref or any other PHP  
// functions runtime.  
// require __DIR__ . '/vendor/autoload.php';  
  
use Bref\Context\Context;  
use Bref\Event\Sns\SnsEvent;  
use Bref\Event\Sns\SnsHandler;  
  
class Handler extends SnsHandler  
{  
    public function handleSns(SnsEvent $event, Context $context): void  
    {  
        foreach ($event->getRecords() as $record) {  
            $message = $record->getMessage();  
  
            // TODO: Implement your custom processing logic here  
            // Any exception thrown will be logged and the invocation will be  
            marked as failed  
  
            echo "Processed Message: $message" . PHP_EOL;  
        }  
    }  
}  
  
return new Handler();
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
    event['Records'].map { |record| process_message(record) }
end

def process_message(record)
    message = record['Sns']['Message']
    puts("Processing message: #{message}")
rescue StandardError => e
    puts("Error processing message: #{e}")
```

```
    raise
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SNS acara dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
// aws_lambda_events = { version = "0.10.0", default-features = false, features
//   = ["sns"] }
// lambda_runtime = "0.8.1"
// tokio = { version = "1", features = ["macros"] }
// tracing = { version = "0.1", features = ["log"] }
// tracing-subscriber = { version = "0.3", default-features = false, features =
//   ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for record in event.payload.records {
        process_record(&record)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);
}
```

```
// Implement your record handling code here.

Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Memanggil fungsi Lambda dari pemicu Amazon SQS

Contoh kode berikut menunjukkan cara menerapkan fungsi Lambda yang menerima peristiwa yang dipicu dengan menerima pesan dari antrian SQS. Fungsi mengambil pesan dari parameter peristiwa dan mencatat konten setiap pesan.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS acara dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
        ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
            //Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```


Go

SDK untuk Go V2

 Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS secara langsung dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
    for _, record := range event.Records {
        err := processMessage(record)
        if err != nil {
            return err
        }
    }
    fmt.Println("done")
    return nil
}

func processMessage(record events.SQSMessage) error {
    fmt.Printf("Processed message %s\n", record.Body)
    // TODO: Do interesting work based on the new message
    return nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS secara langsung dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
            throw e;
        }
    }
}
```

```
}  
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS acara dengan menggunakan Lambda. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
exports.handler = async (event, context) => {  
  for (const message of event.Records) {  
    await processMessageAsync(message);  
  }  
  console.info("done");  
};  
  
async function processMessageAsync(message) {  
  try {  
    console.log(`Processed message ${message.body}`);  
    // TODO: Do interesting work based on the new message  
    await Promise.resolve(1); //Placeholder for actual async work  
  } catch (err) {  
    console.error("An error occurred");  
    throw err;  
  }  
}
```

Mengonsumsi SQS acara dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.  
// SPDX-License-Identifier: Apache-2.0  
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";
```

```
export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDKuntuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengkonsumsi SQS acara dengan menggunakan Lambda. PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
```

```
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS acara dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS acara dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
    event['Records'].each do |message|
        process_message(message)
    end
    puts "done"
end

def process_message(message)
    begin
        puts "Processed message #{message['body']}"
        # TODO: Do interesting work based on the new message
    end
end
```

```
rescue StandardError => err
  puts "An error occurred"
  raise err
end
end
```

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Mengonsumsi SQS acara dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
    event.payload.records.iter().for_each(|record| {
        // process the record
        tracing::info!("Message body: {}",
            record.body.as_deref().unwrap_or_default())
    });

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
        time.
        .without_time()
}
```

```
        .init();

        run(service_fn(function_handler)).await
    }
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Kinesis

Contoh kode berikut menunjukkan cara mengimplementasikan respons batch sebagian untuk fungsi Lambda yang menerima peristiwa dari aliran Kinesis. Fungsi melaporkan kegagalan item batch dalam respons, memberi sinyal ke Lambda untuk mencoba lagi pesan tersebut nanti.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan [contoh lengkapnya](#) dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan penggunaan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))
]
```



```
namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
        ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return new StreamsEventResponse();
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
{record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                /* Since we are working with streams, we can return the failed
item immediately.
                Lambda will immediately begin to retry processing from this
failed item onwards. */
                return new StreamsEventResponse
                {
                    BatchItemFailures = new
List<StreamsEventResponse.BatchItemFailure>
                {
                    new StreamsEventResponse.BatchItemFailure
{ ItemIdentifier = record.Kinesis.SequenceNumber }
                }
                };
            }
        }
    }
}
```

```

    }
    Logger.LogInformation($"Successfully processed {evnt.Records.Count}
records.");
    return new StreamsEventResponse();
}

private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
ILambdaContext context)
{
    byte[] bytes = record.Data.ToArray();
    string data = Encoding.UTF8.GetString(bytes);
    await Task.CompletedTask; //Placeholder for actual async work
    return data;
}
}

public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}
}

```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Go.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

```

```
import (
    "context"
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
    (map[string]interface{}, error) {
    batchItemFailures := []map[string]interface{}{}

    for _, record := range kinesisEvent.Records {
        curRecordSequenceNumber := ""

        // Process your record
        if /* Your record processing condition here */ {
            curRecordSequenceNumber = record.Kinesis.SequenceNumber
        }

        // Add a condition to check if the record processing failed
        if curRecordSequenceNumber != "" {
            batchItemFailures = append(batchItemFailures, map[string]interface{}{
                "itemIdentifier": curRecordSequenceNumber})
        }
    }

    kinesisBatchResponse := map[string]interface{}{
        "batchItemFailures": batchItemFailures,
    }
    return kinesisBatchResponse, nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDKuntuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
ArrayList<>();
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
```

```

        /* Since we are working with streams, we can return the failed
        item immediately.
           Lambda will immediately begin to retry processing from this
        failed item onwards. */
        batchItemFailures.add(new
StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
        return new StreamsEventResponse(batchItemFailures);
    }
}

return new StreamsEventResponse(batchItemFailures);
}
}

```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Javascript.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
      immediately.
         Lambda will immediately begin to retry processing from this failed
      item onwards. */
    }
  }
}

```

```

    return {
      batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
    };
  }
}
console.log(`Successfully processed ${event.Records.length} records.`);
return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}

```

Melaporkan kegagalan item batch Kinesis dengan penggunaan Lambda. TypeScript

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
    }
  }
}

```

```

    logger.info(`Record Data: ${recordData}`);
    // TODO: Do interesting work based on the new data
  } catch (err) {
    logger.error(`An error occurred ${err}`);
    /* Since we are working with streams, we can return the failed item
    immediately.
           Lambda will immediately begin to retry processing from this failed
    item onwards. */
    return {
      batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
    };
  }
}
logger.info(`Successfully processed ${event.Records.length} records.`);
return { batchItemFailures: [] };
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}

```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan penggunaan Lambda. PHP

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

```

```
# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $kinesisEvent = new KinesisEvent($event);
        $this->logger->info("Processing records");
        $records = $kinesisEvent->getRecords();

        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
```



```

        fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
        $failedRecords
    );

    return [
        'batchItemFailures' => $failures
    ];
}
}

$logger = new StderrLogger();
return new Handler($logger);

```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Python.

```

# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures": [{"itemIdentifier":
curRecordSequenceNumber}]}

    return {"batchItemFailures": []}

```

Ruby

SDK untuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
      # immediately.
      # Lambda will immediately begin to retry processing from this failed item
      # onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end
```

```
def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
  sleep(1)
  data
end
```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch Kinesis dengan Lambda menggunakan Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
    Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",

```

```
        record.event_id.as_deref().unwrap_or_default()
    );

    let record_processing_result = process_record(record);

    if record_processing_result.is_err() {
        response.batch_item_failures.push(KinesisBatchItemFailure {
            item_identifier: record.kinesis.sequence_number.clone(),
        });
        /* Since we are working with streams, we can return the failed item
immediately.
        Lambda will immediately begin to retry processing from this failed
item onwards. */
        return Ok(response);
    }

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());

    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
```

```
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
time.
        .without_time()
        .init();

run(service_fn(function_handler)).await
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu DynamoDB

Contoh kode berikut menunjukkan cara mengimplementasikan respons batch sebagian untuk fungsi Lambda yang menerima peristiwa dari aliran DynamoDB. Fungsi melaporkan kegagalan item batch dalam respons, memberi sinyal ke Lambda untuk mencoba lagi pesan tersebut nanti.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
into a .NET class.
[assembly:
    LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
        ILambdaContext context)
    {
        context.Logger.LogInformation($"Beginning to process
        {dynamoEvent.Records.Count} records...");
        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
        List<StreamsEventResponse.BatchItemFailure>();
        StreamsEventResponse streamsEventResponse = new StreamsEventResponse();

        foreach (var record in dynamoEvent.Records)
        {
            try
            {
                var sequenceNumber = record.Dynamodb.SequenceNumber;
                context.Logger.LogInformation(sequenceNumber);
            }
            catch (Exception ex)
            {
                context.Logger.LogError(ex.Message);
                batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
                { ItemIdentifier = record.Dynamodb.SequenceNumber });
            }
        }

        if (batchItemFailures.Count > 0)
        {
            streamsEventResponse.BatchItemFailures = batchItemFailures;
        }

        context.Logger.LogInformation("Stream processing complete.");
        return streamsEventResponse;
    }
}
```

```
}
```

Go

SDK untuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
    "context"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

type BatchItemFailure struct {
    ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
    BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
(*BatchResult, error) {
    var batchItemFailures []BatchItemFailure
    curRecordSequenceNumber := ""

    for _, record := range event.Records {
        // Process your record
        curRecordSequenceNumber = record.Change.SequenceNumber
    }
}
```

```
if curRecordSequenceNumber != "" {
    batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
curRecordSequenceNumber})
}

batchResult := BatchResult{
    BatchItemFailures: batchItemFailures,
}

return &batchResult, nil
}

func main() {
    lambda.Start(HandleRequest)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;
```



```
public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
    Serializable> {

    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
    context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
        ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
        input.getRecords()) {
            try {
                //Process your record
                StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
                curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
                item immediately.
                Lambda will immediately begin to retry processing from this
                failed item onwards. */
                batchItemFailures.add(new
                StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

        return new StreamsEventResponse();
    }
}
```

JavaScript

SDK Kuntuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. JavaScript

```
export const handler = async (event) => {
  const records = event.Records;
  let curRecordSequenceNumber = "";

  for (const record of records) {
    try {
      // Process your record
      curRecordSequenceNumber = record.dynamodb.SequenceNumber;
    } catch (e) {
      // Return failed record's sequence number
      return { batchItemFailures: [{ itemIdentifier:
curRecordSequenceNumber }] };
    }
  }

  return { batchItemFailures: [] };
};
```

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. TypeScript

```
import {
  DynamoDBBatchResponse,
  DynamoDBBatchItemFailure,
  DynamoDBStreamEvent,
} from "aws-lambda";

export const handler = async (
  event: DynamoDBStreamEvent
): Promise<DynamoDBBatchResponse> => {
```

```
const batchItemFailures: DynamoDBBatchItemFailure[] = [];  
let curRecordSequenceNumber;  
  
for (const record of event.Records) {  
  curRecordSequenceNumber = record.dynamodb?.SequenceNumber;  
  
  if (curRecordSequenceNumber) {  
    batchItemFailures.push({  
      itemIdentifier: curRecordSequenceNumber,  
    });  
  }  
}  
  
return { batchItemFailures: batchItemFailures };  
};
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan penggunaan Lambda. PHP

```
<?php  
  
# using bref/bref and bref/logger for simplicity  
  
use Bref\Context\Context;  
use Bref\Event\DynamoDb\DynamoDbEvent;  
use Bref\Event\Handler as StdHandler;  
use Bref\Logger\StderrLogger;  
  
require __DIR__ . '/vendor/autoload.php';  
  
class Handler implements StdHandler  
{
```

```
private StderrLogger $logger;
public function __construct(StderrLogger $logger)
{
    $this->logger = $logger;
}

/**
 * @throws JsonException
 * @throws \Bref\Event\InvalidLambdaEvent
 */
public function handle(mixed $event, Context $context): array
{
    $dynamoDbEvent = new DynamoDbEvent($event);
    $this->logger->info("Processing records");

    $records = $dynamoDbEvent->getRecords();
    $failedRecords = [];
    foreach ($records as $record) {
        try {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data
        } catch (Exception $e) {
            $this->logger->error($e->getMessage());
            // failed processing the record
            $failedRecords[] = $record->getSequenceNumber();
        }
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords records");

    // change format for the response
    $failures = array_map(
        fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
        $failedRecords
    );

    return [
        'batchItemFailures' => $failures
    ];
}

$logger = new StderrLogger();
```

```
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Ruby.

```
def lambda_handler(event:, context:)
  records = event["Records"]
  cur_record_sequence_number = ""

  records.each do |record|
    begin
      # Process your record
      cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
      rescue StandardError => e
      # Return failed record's sequence number
      return {"batchItemFailures" => [{"itemIdentifier" =>
cur_record_sequence_number}]}
    end
  end

  {"batchItemFailures" => []}
end
```

Rust

SDKuntuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item batch DynamoDB dengan Lambda menggunakan Rust.

```
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;

    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("").to_string(),
            });
            return Ok(response);
        }

        // Process your record here...
```

```
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
            immediately.
            Lambda will immediately begin to retry processing from this failed
            item onwards. */
            return Ok(response);
        }
    }

    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
        time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Melaporkan kegagalan item batch untuk fungsi Lambda dengan pemicu Amazon SQS

Contoh kode berikut menunjukkan cara mengimplementasikan respons batch sebagian untuk fungsi Lambda yang menerima peristiwa dari antrian SQS. Fungsi melaporkan kegagalan item batch dalam respons, memberi sinyal ke Lambda untuk mencoba lagi pesan tersebut nanti.

.NET

AWS SDK for .NET

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
// into a .NET class.
[assembly: LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer))]
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
        ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
        List<SQSBatchResponse.BatchItemFailure>();
        foreach(var message in evnt.Records)
        {
            try
            {
```

```

        //process your message
        await ProcessMessageAsync(message, context);
    }
    catch (System.Exception)
    {
        //Add failed message identifier to the batchItemFailures list
        batchItemFailures.Add(new
SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
    }
    }
    return new SQSBatchResponse(batchItemFailures);
}

private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
ILambdaContext context)
{
    if (String.IsNullOrEmpty(message.Body))
    {
        throw new Exception("No Body in SQS Message.");
    }
    context.Logger.LogInformation($"Processed message {message.Body}");
    // TODO: Do interesting work based on the new message
    await Task.CompletedTask;
}
}

```

Go

SDKuntuk Go V2

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Go.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

```

```
import (
    "context"
    "encoding/json"
    "fmt"
    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, sqsEvent events.SQSEvent)
    (map[string]interface{}, error) {
    batchItemFailures := []map[string]interface{}{}

    for _, message := range sqsEvent.Records {

        if /* Your message processing condition here */ {
            batchItemFailures = append(batchItemFailures, map[string]interface{}{
                "itemIdentifier": message.MessageId})
        }
    }

    sqsBatchResponse := map[string]interface{}{
        "batchItemFailures": batchItemFailures,
    }
    return sqsBatchResponse, nil
}

func main() {
    lambda.Start(handler)
}
```

Java

SDK untuk Java 2.x

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;

import java.util.ArrayList;
import java.util.List;

public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,
SQSBatchResponse> {
    @Override
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context) {

        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
ArrayList<SQSBatchResponse.BatchItemFailure>();
        String messageId = "";
        for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
            try {
                //process your message
                messageId = message.getMessageId();
            } catch (Exception e) {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.add(new
SQSBatchResponse.BatchItemFailure(messageId));
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }
}
```

JavaScript

SDK untuk JavaScript (v3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. JavaScript

```
// Node.js 20.x Lambda runtime, AWS SDK for Javascript V3
export const handler = async (event, context) => {
  const batchItemFailures = [];
  for (const record of event.Records) {
    try {
      await processMessageAsync(record, context);
    } catch (error) {
      batchItemFailures.push({ itemIdentifier: record.messageId });
    }
  }
  return { batchItemFailures };
};

async function processMessageAsync(record, context) {
  if (record.body && record.body.includes("error")) {
    throw new Error("There is an error in the SQS Message.");
  }
  console.log(`Processed message: ${record.body}`);
}
```

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure, SQSRecord }
  from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
  Promise<SQSBatchResponse> => {
  const batchItemFailures: SQSBatchItemFailure[] = [];

  for (const record of event.Records) {
    try {
      await processMessageAsync(record);
    } catch (error) {
      batchItemFailures.push({ itemIdentifier: record.messageId });
    }
  }

  return {batchItemFailures: batchItemFailures};
};
```

```
async function processMessageAsync(record: SQSRecord): Promise<void> {
    if (record.body && record.body.includes("error")) {
        throw new Error('There is an error in the SQS Message.');
```

PHP

SDK untuk PHP

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan menggunakan Lambda. PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
```

```
* @throws \Bref\Event\InvalidLambdaEvent
*/
public function handleSqs(SqsEvent $event, Context $context): void
{
    $this->logger->info("Processing SQS records");
    $records = $event->getRecords();

    foreach ($records as $record) {
        try {
            // Assuming the SQS message is in JSON format
            $message = json_decode($record->getBody(), true);
            $this->logger->info(json_encode($message));
            // TODO: Implement your custom processing logic here
        } catch (Exception $e) {
            $this->logger->error($e->getMessage());
            // failed processing the record
            $this->markAsFailed($record);
        }
    }
    $totalRecords = count($records);
    $this->logger->info("Successfully processed $totalRecords SQS records");
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
```

```
def lambda_handler(event, context):
    if event:
        batch_item_failures = []
        sqs_batch_response = {}

        for record in event["Records"]:
            try:
                # process message
            except Exception as e:
                batch_item_failures.append({"itemIdentifier":
record['messageId']})

        sqs_batch_response["batchItemFailures"] = batch_item_failures
        return sqs_batch_response
```

Ruby

SDKuntuk Ruby

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
    if event
        batch_item_failures = []
        sqs_batch_response = {}

        event["Records"].each do |record|
            begin
                # process message
            rescue StandardError => e
                batch_item_failures << {"itemIdentifier" => record['messageId']}
```



```

        end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
end
end

```

Rust

SDK untuk Rust

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di repositori [contoh Nirserver](#).

Melaporkan kegagalan item SQS batch dengan Lambda menggunakan Rust.

```

// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}

async fn function_handler(event: LambdaEvent<SqsEvent>) ->
Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }
}

```

```
    }  
  }  
  
  Ok(SqsBatchResponse {  
    batch_item_failures,  
  })  
}  
  
#[tokio::main]  
async fn main() -> Result<(), Error> {  
  run(service_fn(function_handler)).await  
}
```

Untuk daftar lengkap panduan AWS SDK pengembang dan contoh kode, lihat [Menggunakan Lambda dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang SDK versi sebelumnya.

Kuota Lambda

Important

Baru Akun AWS telah mengurangi kuota konkurensi dan memori. AWS meningkatkan kuota ini secara otomatis berdasarkan penggunaan Anda.

Komputasi dan penyimpanan

Lambda menetapkan kuota untuk jumlah sumber daya komputasi dan penyimpanan yang dapat Anda gunakan untuk menjalankan dan menyimpan fungsi. Kuota untuk eksekusi dan penyimpanan bersamaan berlaku per Wilayah AWS. Kuota antarmuka jaringan elastis (ENI) berlaku per virtual private cloud (VPC), terlepas dari Wilayah. Kuota berikut dapat ditingkatkan dari nilai default mereka. Untuk informasi selengkapnya, lihat [Meminta peningkatan kuota](#) dalam Panduan Pengguna Service Quotas.

| Sumber Daya | Kuota default | Dapat ditingkatkan hingga |
|---|--|---------------------------|
| Eksekusi bersamaan | 1.000 | Puluhan ribu |
| Penyimpanan untuk fungsi yang diunggah (arsip file .zip) dan lapisan. Setiap versi fungsi dan versi lapisan mengonsumsi penyimpanan. Untuk praktik terbaik dalam mengelola penyimpanan kode, lihat Memantau penyimpanan kode Lambda di Tanah Tanpa Server. | 75 GB | Terabyte |
| Penyimpanan untuk fungsi yang ditentukan sebagai gambar kontainer. Gambar-gambar ini disimpan di AmazonECR. | Lihat kuota ECR layanan Amazon . | |
| Antarmuka jaringan elastis per cloud pribadi virtual () VPC | 500 | Ribuan |

| Sumber Daya | Kuota default | Dapat ditingkatkan hingga |
|--|---------------|---------------------------|
| <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p>Note</p> <p>Kuota ini dibagi dengan layanan lain, seperti Amazon Elastic File System (AmazonEFS). Lihat VPCkuota Amazon.</p> </div> | | |

Untuk detail tentang konkurensi dan bagaimana Lambda menskalakan konkurensi fungsi Anda sehubungan dengan lalu lintas, lihat [Memahami penskalaan fungsi Lambda](#).

Konfigurasi fungsi, penyebaran, dan eksekusi

Kuota berikut berlaku untuk konfigurasi fungsi, penyebaran, dan eksekusi. Kecuali seperti yang disebutkan, mereka tidak dapat diubah.

| | |
|---|--|
| <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p>Note</p> <p>Dokumentasi Lambda, pesan log, dan konsol menggunakan singkatan MB (bukan MiB) untuk merujuk ke 1.024 KB.</p> </div> | |
|---|--|


| Sumber Daya | Kuota |
|---------------------------------------|--|
| Fungsi alokasi memori | <p>128 MB hingga 10.240 MB, dengan peningkatan 1 MB.</p> <p>Catatan: Lambda mengalokasikan CPU daya secara proporsional dengan jumlah memori yang dikonfigurasi. Anda dapat menambah atau mengurangi memori dan CPU daya yang dialokasikan ke fungsi</p> |

| Sumber Daya | Kuota |
|--|--|
| | Anda menggunakan pengaturan Memori (MB). Pada 1.769 MB, suatu fungsi memiliki setara dengan satu v. CPU |
| Fungsi waktu habis | 900 detik (15 menit) |
| Fungsi variabel lingkungan | 4 KB, untuk semua variabel lingkungan yang terkait dengan fungsi, secara agregat |
| Fungsi kebijakan berbasis sumber daya | 20 KB |
| Fungsi lapisan | lima lapisan |
| Batas penskalaan konkurensi fungsi | Untuk setiap fungsi, 1.000 lingkungan eksekusi setiap 10 detik |
| Muatan invokasi (permintaan dan respons) | <p>6 MB masing-masing untuk permintaan dan tanggapan (sinkron)</p> <p>20 MB untuk setiap respons yang dialirkan (Sinkron. Ukuran payload untuk respons yang dialirkan dapat ditingkatkan dari nilai default. Kontak AWS Support untuk menanyakan lebih lanjut.)</p> <p>256 KB (asinkron)</p> <p>1 MB untuk total ukuran gabungan baris permintaan dan nilai header</p> |

| Sumber Daya | Kuota |
|---|---|
| Bandwidth untuk tanggapan yang dialirkan | <p>Uncapped untuk 6 MB pertama dari respons fungsi Anda</p> <p>Untuk tanggapan yang lebih besar dari 6 MB, 2 MBps untuk sisa respons</p> |
| Ukuran paket deployment (arsip file .zip) | <p>50 MB (dalam zip, untuk unggahan langsung)</p> <p>250 MB (membuka ritsleting)</p> <p>Kuota ini berlaku untuk semua file yang Anda unggah, termasuk layer dan runtime kustom.</p> <p>3 MB (editor konsol)</p> |
| Ukuran pengaturan gambar kontainer | 16 KB |
| Ukuran paket kode gambar kontainer | 10 GB (ukuran gambar maksimum yang tidak terkompresi, termasuk semua lapisan) |
| Peristiwa pengujian (editor konsol) | 10 |
| /tmp penyimpanan direktori | Antara 512 MB dan 10.240 MB, dengan peningkatan 1-MB |
| Deskriptor file | 1,024 |
| Proses eksekusi/utas | 1,024 |

Permintaan Lambda API

Kuota berikut dikaitkan dengan permintaan API Lambda.

| Sumber Daya | Kuota |
|--|---|
| Permintaan pemanggilan per fungsi per Wilayah (sinkron) | Setiap instance lingkungan eksekusi Anda dapat melayani hingga 10 permintaan per detik. Dengan kata lain, total batas pemanggilan adalah 10 kali batas konkurensi Anda. Lihat Memahami penskalaan fungsi Lambda . |
| Permintaan pemanggilan per fungsi per Wilayah (asinkron) | Setiap instance lingkungan eksekusi Anda dapat melayani jumlah permintaan yang tidak terbatas. Dengan kata lain, batas pemanggilan total hanya didasarkan pada konkurensi yang tersedia untuk fungsi Anda. Lihat Memahami penskalaan fungsi Lambda . |
| Permintaan invokasi per versi fungsi atau alias (permintaan per detik) | 10 x dialokasikan konkurensi tersedia |
| | <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E1F5FE;"> <p> Note</p> <p>Kuota ini hanya berlaku untuk fungsi yang menggunakan konkurensi terprovisi.</p> </div> |
| GetFunction API permintaan | 100 permintaan per detik. Tidak dapat ditingkatkan. |
| GetPolicy API permintaan | 15 permintaan per detik. Tidak dapat ditingkatkan. |
| Sisa API permintaan bidang kontrol (tidak termasuk pemanggilan,, GetFunction dan permintaan) GetPolicy | 15 permintaan per detik di semua APIs (bukan 15 permintaan per detik per API). Tidak dapat ditingkatkan. |

Layanan lainnya

Kuota untuk layanan lain, seperti AWS Identity and Access Management (IAM), Amazon CloudFront (Lambda @Edge), dan Amazon Virtual Private Cloud (VPCAmazon), dapat memengaruhi fungsi Lambda Anda. Untuk informasi lebih lanjut, lihat [AWS layanan kuota](#) di Referensi Umum Amazon Web Services, dan [Memanggil Lambda dengan acara dari layanan lain AWS](#).

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada Panduan Developer AWS Lambda sejak Mei 2018. Untuk pemberitahuan tentang pembaruan dokumentasi ini, berlangganan [RSSfeed](#).

| Perubahan | Deskripsi | Tanggal |
|---|--|------------------|
| Support untuk SnapStart di Wilayah baru | Lambda sekarang SnapStart tersedia di Wilayah berikut: Eropa (Spanyol), Eropa (Zurich), Asia Pasifik (Melbourne), Asia Pasifik (Hyderabad), dan Timur Tengah (). UAE | Januari 12, 2024 |
| AWS pembaruan kebijakan terkelola | Service Quotas memperbarui kebijakan AWS terkelola yang ada (AWSLambdaVPCLambdaAccessExecutionRole). | Januari 5, 2024 |
| Waktu proses Python 3.12 | Lambda sekarang mendukung Python 3.12 sebagai runtime terkelola dan image dasar container. Untuk informasi selengkapnya, lihat Python 3.12 runtime sekarang tersedia AWS Lambda di Blog Compute. AWS | 14 Desember 2023 |
| Waktu proses Java 21 | Lambda sekarang mendukung Java 21 sebagai runtime terkelola dan image basis container (). java21 | 16 November 2023 |
| Node.js 20.x runtime | Lambda sekarang mendukung Node.js 20 sebagai runtime | 14 November 2023 |

terkelola dan image basis container (. nodejs20.x) Untuk informasi selengkapnya, lihat [runtime Node.js 20.x sekarang tersedia AWS Lambda di Blog AWS Compute](#).

[runtime disediakan.al2023](#)

Lambda sekarang mendukung Amazon Linux 2023 sebagai runtime terkelola dan image basis container. Untuk informasi selengkapnya, lihat [Memperkenalkan runtime Amazon Linux 2023 untuk AWS Lambda](#) di AWS Compute Blog.

9 November 2023

[IPv6dukungan untuk subnet dual-stack](#)

Lambda sekarang mendukung IPv6 lalu lintas keluar ke subnet dual-stack. Untuk informasi selengkapnya, lihat [IPv6dukungan](#).

12 Oktober 2023

[Menguji fungsi dan aplikasi tanpa server](#)

Pelajari tentang teknik untuk men-debug dan mengotomasi pengujian fungsi tanpa server di cloud. Sekarang ada bagian pengujian dan sumber daya yang disertakan dalam bagian bahasa Python dan TypeScript. Untuk detailnya, lihat [Menguji fungsi dan aplikasi tanpa server](#).

Juni 16, 2023

| | | |
|---|--|-----------------|
| Runtime Ruby 3.2 | Lambda sekarang mendukung runtime baru untuk Ruby 3.2. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Ruby . | Juni 7, 2023 |
| Streaming respons | Lambda sekarang mendukung respons streaming dari fungsi. Untuk informasi selengkapnya, lihat Mengonfigurasi fungsi Lambda untuk mengalirkan respons. | 6 April 2023 |
| Metrik pemanggilan asinkron | Lambda merilis metrik pemanggilan asinkron. Untuk informasi selengkapnya, lihat Metrik pemanggilan asinkron . | 9 Februari 2023 |
| Kontrol versi runtime | Lambda merilis versi runtime baru yang mencakup pembaruan keamanan, perbaikan bug, dan fitur baru. Anda sekarang dapat mengontrol kapan fungsi Anda diperbarui ke versi runtime baru. Untuk informasi selengkapnya, lihat pembaruan runtime Lambda . | 23 Januari 2023 |

| | | |
|---|--|------------------|
| Lambda SnapStart | Gunakan Lambda SnapStart untuk mengurangi waktu startup untuk fungsi Java tanpa menyediakan sumber daya tambahan atau menerapkan pengoptimalan kinerja yang kompleks. Untuk informasi selengkapnya, lihat Meningkatkan kinerja startup dengan Lambda SnapStart . | 28 November 2022 |
| Node.js 18 runtime | Lambda sekarang mendukung runtime baru untuk Node.js 18. Node.js 18 menggunakan Amazon Linux 2. Untuk detailnya, lihat Membangun fungsi Lambda dengan Node.js . | 18 November 2022 |
| lambda: kunci SourceFunctionArn kondisi | Untuk AWS sumber daya, tombol lambda:SourceFunctionArn kondisi memfilter akses ke sumber daya oleh ARN fungsi Lambda. Untuk detailnya, lihat Bekerja dengan kredensial lingkungan eksekusi Lambda . | 1 Juli 2022 |
| Node.js 16 runtime | Lambda sekarang mendukung runtime baru untuk Node.js 16. Node.js 16 menggunakan Amazon Linux 2. Untuk detailnya, lihat Membangun fungsi Lambda dengan Node.js . | Mei 11, 2022 |

| | | |
|--|--|-------------------|
| Fungsi Lambda URLs | Lambda sekarang mendukung fungsiURLs, yang merupakan titik akhir khusus HTTP (S) untuk fungsi Lambda. Untuk detailnya, lihat Fungsi Lambda. URLs | April 6, 2022 |
| Acara pengujian bersama di AWS Lambda konsol | Lambda sekarang mendukung berbagi acara pengujian dengan pengguna lain dalam hal yang sama. Akun AWS Untuk detailnya, lihat Menguji fungsi Lambda di konsol. | 16 Maret 2022 |
| PrincipalOrgId dalam kebijakan berbasis sumber daya | Lambda sekarang mendukung pemberian izin ke organisasi di. AWS Organizations Untuk detailnya, lihat Menggunakan kebijakan berbasis sumber daya untuk. AWS Lambda | 11 Maret 2022 |
| .NET6 runtime | Lambda sekarang mendukung runtime baru untuk. NET6. Untuk detailnya, lihat Runtime Lambda. | Februari 23, 2022 |
| Pemfilteran peristiwa untuk sumber peristiwa Kinesis, DynamoDB, dan Amazon SQS | Lambda sekarang mendukung pemfilteran peristiwa untuk Kinesis, DynamoDB, dan sumber peristiwa Amazon. SQS Untuk detailnya, lihat Pemfilteran acara Lambda. | 24 November 2021 |

| | | |
|---|---|-------------------|
| m TLS otentikasi untuk Amazon MSK dan sumber acara Apache Kafka yang dikelola sendiri | Lambda sekarang mendukung TLS otentikasi m untuk Amazon MSK dan sumber acara Apache Kafka yang dikelola sendiri. Untuk detailnya, lihat Menggunakan Lambda dengan Amazon MSK . | November 19, 2021 |
| Lambda di Graviton2 | Lambda sekarang mendukung Graviton2 untuk fungsi menggunakan arsitektur arm64. Untuk detailnya, lihat Arsitektur set instruksi Lambda . | 29 September 2021 |
| Waktu proses Python 3.9 | Lambda sekarang mendukung runtime baru untuk Python 3.9. Untuk detailnya, lihat Runtime Lambda . | 16 Agustus 2021 |
| Versi runtime baru untuk Node.js, Python, dan Java | Versi runtime baru tersedia untuk Node.js, Python, dan Java. Untuk detailnya, lihat Runtime Lambda . | 21 Juli 2021 |
| Support untuk RabbitMQ sebagai sumber acara di Lambda | Lambda sekarang mendukung Amazon MQ untuk RabbitMQ sebagai sumber acara. Amazon MQ adalah layanan broker pesan terkelola untuk Apache ActiveMQ dan RabbitMQ yang memudahkan penyiapan dan pengoperasian broker pesan di cloud. Untuk detailnya, lihat Menggunakan Lambda dengan Amazon MQ . | 7 Juli 2021 |

[SASL/PLAINotentikasi untuk Kafka yang dikelola sendiri di Lambda](#)

SASL/sekarang PLAIN merupakan mekanisme otentikasi yang didukung untuk sumber acara Kafka yang dikelola sendiri di Lambda Pelanggan yang sudah menggunakan SASL/PLAIN pada cluster Kafka yang dikelola sendiri sekarang dapat dengan mudah menggunakan Lambda untuk membangun aplikasi konsumen tanpa harus mengubah cara mereka mengautentikasi. Untuk detailnya, lihat [Menggunakan Lambda dengan Apache Kafka yang dikelola sendiri](#).

29 Juni 2021

[Ekstensi Lambda API](#)

Ketersediaan umum untuk ekstensi Lambda. Gunakan ekstensi untuk menambah fungsi Lambda Anda. Anda dapat menggunakan ekstensi yang disediakan oleh Partner Lambda, atau Anda dapat membuat ekstensi Lambda Anda sendiri. Untuk detailnya, lihat [Ekstensi Lambda](#). API

24 Mei 2021

[Pengalaman konsol Lambda baru](#)

Konsol Lambda telah didesain ulang untuk meningkatkan performa dan konsistensi.

2 Maret 2021

[Node.js 14 runtime](#)

Lambda kini mendukung runtime Node.js 14. Node.js 14 menggunakan Amazon Linux 2. Untuk detailnya, lihat [Membangun fungsi Lambda dengan Node.js.](#)

27 Januari 2021

[Gambar kontainer Lambda](#)

Lambda sekarang mendukung fungsi yang didefinisikan sebagai gambar kontainer . Anda dapat menggabungkan fleksibilitas peralatan kontainer dengan ketangkasan dan kesederhanaan operasional Lambda untuk membangun aplikasi. Untuk detail selengkapnya, lihat [Menggunakan gambar kontainer dengan Lambda.](#)

1 Desember 2020

[Penandatanganan kode untuk fungsi Lambda](#)

Lambda kini mendukung penandatanganan kode. Administrator dapat mengonfigurasi fungsi Lambda untuk hanya menerima kode yang ditandatangani pada deployment. Lambda memeriksa tanda tangan untuk memastikan kode tidak diubah atau disusupi. Selain itu, Lambda memastikan kode sudah ditandatangani oleh developer tepercaya sebelum menerima deployment. Untuk detailnya, lihat [Mengonfigurasi penandatanganan kode untuk Lambda](#).

23 November 2020

[Pratinjau: Log Runtime Lambda API](#)

Lambda sekarang mendukung Runtime Logs. API Ekstensi Lambda dapat menggunakan Log API untuk berlangganan aliran log di lingkungan eksekusi. Untuk detailnya, lihat [Log Runtime Lambda](#). API

12 November 2020

[Sumber acara baru untuk Amazon MQ](#)

Lambda kini mendukung Amazon MQ sebagai sumber peristiwa. Gunakan fungsi Lambda untuk memproses catatan dari broker pesan Amazon MQ Anda. Untuk detailnya, lihat [Menggunakan Lambda dengan Amazon MQ](#).

5 November 2020

[Pratinjau: Ekstensi Lambda API](#)

Gunakan ekstensi Lambda untuk menambah fungsi Lambda Anda. Anda dapat menggunakan ekstensi yang disediakan oleh Lambda Partners, atau Anda dapat membuat ekstensi Lambda Anda sendiri. Untuk detailnya, lihat [Ekstensi Lambda](#). API

8 Oktober 2020

[Support untuk Java 8 dan runtime kustom di AL2](#)

Lambda kini mendukung Java 8 dan runtime kustom di Amazon Linux 2. Untuk detailnya, lihat [Runtime Lambda](#).

12 Agustus 2020

[Sumber acara baru untuk Amazon Managed Streaming for Apache Kafka](#)

Lambda sekarang mendukung Amazon MSK sebagai sumber acara. Gunakan fungsi Lambda dengan Amazon MSK untuk memproses catatan dalam topik Kafka. Untuk detailnya, lihat [Menggunakan Lambda dengan Amazon MSK](#).

11 Agustus 2020

[IAM tombol kondisi untuk VPC pengaturan Amazon](#)

Anda sekarang dapat menggunakan tombol kondisi khusus Lambda untuk VPC pengaturan. Misalnya, Anda dapat mengharuskan semua fungsi di organisasi Anda terhubung ke file VPC. Anda juga dapat menentukan subnet dan grup keamanan yang dapat dan tidak dapat digunakan oleh pengguna fungsi. Untuk detailnya, lihat [Mengonfigurasi VPC IAM fungsi](#).

10 Agustus 2020

[Pengaturan konkurensi untuk konsumen aliran HTTP Kinesis /2](#)

Anda sekarang dapat menggunakan pengaturan konkurensi berikut untuk konsumen Kinesis dengan peningkatan fan-out HTTP (/2 stream) ParallelizationFactor:,,, dan. MaximumRetryAttempts MaximumRecordAgeInSeconds DestinationConfig BisectBatchOnFunctionError Untuk detailnya, lihat [Menggunakan AWS Lambda dengan Amazon Kinesis](#).

7 Juli 2020

[Jendela Batch untuk konsumen aliran Kinesis HTTP /2](#)

Anda sekarang dapat mengkonfigurasi jendela batch (MaximumBatchingWindowInSeconds) untuk HTTP /2 stream. Lambda membaca catatan dari pengaliran hingga memenuhi batch, atau hingga rentang waktu batch kedaluwarsa. Untuk detailnya, lihat [Menggunakan AWS Lambda dengan Amazon Kinesis](#).

18 Juni 2020

[Support untuk sistem EFS file Amazon](#)

Anda sekarang dapat menghubungkan sistem EFS file Amazon ke fungsi Lambda Anda untuk akses file jaringan bersama. Untuk detailnya, lihat [Mengonfigurasi akses sistem file untuk fungsi Lambda](#).

16 Juni 2020

[AWS CDK contoh aplikasi di konsol Lambda](#)

Konsol Lambda sekarang menyertakan contoh aplikasi yang menggunakan for. AWS Cloud Development Kit (AWS CDK) TypeScript AWS CDK Ini adalah kerangka kerja yang memungkinkan Anda untuk menentukan sumber daya aplikasi Anda di TypeScript, Python, Java, atau .NET.

1 Juni 2020

[Support untuk .NETRuntime Core 3.1.0 di AWS Lambda](#)

AWS Lambda sekarang mendukung .NET Waktu proses Core 3.1.0. Untuk detailnya, lihat [.NETInti CLI](#).

31 Maret 2020

[Support untuk API Gateway HTTP APIs](#)

Dokumentasi yang diperbarui dan diperluas untuk menggunakan Lambda dengan API Gateway, termasuk dukungan untuk HTTP APIs. Menambahkan contoh aplikasi yang membuat API dan fungsi dengan AWS CloudFormation. Untuk detailnya, lihat [Menggunakan Lambda dengan Amazon API Gateway](#).

Selasa, 23 Maret 2020

[Ruby 2.7](#)

Runtime baru tersedia untuk Ruby 2.7, ruby2.7, yang merupakan runtime Ruby pertama yang menggunakan Amazon Linux 2. Untuk detailnya, lihat [Membangun fungsi Lambda dengan Ruby](#).

19 Februari 2020

[Metrik konkurensi](#)

Lambda kini melaporkan metrik ConcurrentExecutions untuk semua fungsi, alias, dan versi. Anda bisa melihat grafik untuk metrik ini pada halaman pemantauan untuk fungsi Anda. Sebelumnya, ConcurrentExecutions hanya dilaporkan pada tingkat akun dan untuk fungsi yang menggunakan konkurensi yang telah ditentukan. Untuk detailnya, lihat [Metrik fungsi AWS Lambda](#).

18 Februari 2020

[Perbarui ke status fungsi](#)

Status fungsi kini diterapkan untuk semua fungsi secara default. Saat Anda menghubungkan fungsi ke aVPC, Lambda membuat antarmuka jaringan elastis bersama. Hal ini memungkinkan peningkatan skala fungsi Anda tanpa membuat antarmuka jaringan tambahan. Selama proses ini, Anda tidak dapat melakukan operasi tambahan pada fungsi, termasuk memperbaiki konfigurasinya dan menerbitkan versi. Dalam beberapa kasus, invokasi juga terdampak. Detail tentang status fungsi saat ini tersedia dari LambdaAPI.

Pembaruan ini dirilis secara bertahap. Untuk detailnya, lihat [Lambda yang diperbarui menyatakan siklus hidup untuk VPC jaringan](#) di Blog Komputasi. AWS Untuk informasi selengkapnya tentang status, lihat [status fungsi AWS Lambda](#).

24 Januari 2020

[Pembaruan untuk API output konfigurasi fungsi](#)

Menambahkan kode alasan ke [StateReasonCode](#)(InvalidSubnet, InvalidSecurityGroup) dan LastUpdateStatusReasonCode (SubnetOutOfIPAddresses, InvalidSubnet, InvalidSecurityGroup) untuk fungsi yang terhubung ke fileVPC. Untuk informasi selengkapnya tentang status, lihat [status fungsi AWS Lambda](#).

20 Januari 2020

[Konkurensi yang disediakan](#)

Anda dapat mengalokasikan konkurensi terprovisi untuk versi fungsi, atau alias. Konkurensi terprovisi memungkinkan fungsi menskalakan tanpa fluktuasi di latensi. Untuk detailnya, lihat [Mengelola konkurensi untuk fungsi Lambda](#).

3 Desember 2019

[Buat proxy basis data](#)

Anda dapat menggunakan konsol Lambda untuk membuat proxy basis data untuk fungsi Lambda. Proksi basis data memungkinkan fungsi mencapai tingkat konkurensi tinggi tanpa membuang koneksi basis data. Untuk detailnya, lihat [Mengonfigurasi akses basis data untuk fungsi Lambda](#).

3 Desember 2019

[Dukungan persentil untuk metrik durasi](#)

Anda dapat memfilter metrik durasi berdasarkan persentil . Untuk detailnya, lihat [Metrik AWS Lambda](#).

26 November 2019

[Peningkatan konkurensi untuk sumber acara streaming](#)

Opsi baru untuk pemetaan sumber peristiwa [DynamoDB stream](#) dan [Kinesis stream](#) memungkinkan Anda memproses lebih dari satu batch sekaligus dari setiap serpihan. Saat Anda meningkatkan jumlah batch bersamaan per serpihan, konkurensi fungsi Anda dapat mencapai 10 kali jumlah serpihan di pengaliran Anda. Untuk detailnya, lihat [Pemetaan sumber peristiwa Lambda](#).

25 November 2019

Status fungsi

Saat Anda membuat atau memperbarui fungsi, fungsi memasuki status tertunda sewaktu Lambda menyediakan sumber daya untuk mendukungnya. Jika Anda menghubungkan fungsi Anda ke VPC, Lambda dapat langsung membuat shared elastic network interface, alih-alih membuat antarmuka jaringan saat fungsi Anda dipanggil. Ini menghasilkan kinerja yang lebih baik untuk fungsi VPC yang terhubung, tetapi mungkin memerlukan pembaruan untuk otomatisasi Anda. Untuk detailnya, lihat [status fungsi AWS Lambda](#).

25 November 2019

Opsi penanganan kesalahan untuk pemanggilan asinkron

Opsi konfigurasi baru sudah tersedia untuk invokasi asinkron. Anda dapat mengonfigurasi Lambda untuk membatasi percobaan ulang dan mengatur periode peristiwa maksimum. Untuk detailnya, lihat [Mengonfigurasi penanganan kesalahan untuk invokasi asinkron](#).

25 November 2019

[Penanganan kesalahan untuk sumber acara streaming](#)

Opsi konfigurasi baru tersedia untuk pemetaan sumber peristiwa yang membaca dari pengaliran. Anda dapat mengonfigurasi pemetaan sumber peristiwa [DynamoDB stream](#) dan [Kinesis stream](#) untuk membatasi percobaan ulang dan menetapkan periode catatan maksimum. Jika terjadi kesalahan, Anda dapat mengonfigurasi pemetaan sumber peristiwa untuk membagikan batch sebelum mencoba kembali, dan untuk mengirim catatan invokasi bagi batch yang gagal pada antrean atau topik. Untuk detailnya, lihat [Pemetaan sumber peristiwa Lambda](#).

25 November 2019

[Tujuan untuk pemanggilan asinkron](#)

Anda dapat mengonfigurasi Lambda untuk mengirim rekaman invokasi asinkron ke layanan lain. Catatan invokasi berisi detail tentang peristiwa, konteks, dan respons fungsi. Anda dapat mengirim catatan pemanggilan ke SQS antrian, topik, fungsi LambdaSNS, atau bus acara. EventBridge Untuk detailnya, lihat [Mengonfigurasi tujuan untuk invokasi asinkron](#).

25 November 2019

| | | |
|--|--|------------------|
| Runtime baru untuk Node.js, Python, dan Java | Runtime baru tersedia untuk Node.js 12, Python 3.8, dan Java 11. Untuk detailnya, lihat Runtime Lambda . | 18 November 2019 |
| FIFOdukungan antrian untuk sumber SQS acara Amazon | Anda sekarang dapat membuat pemetaan sumber peristiwa yang dibaca dari antrean first-in, first-out (FIFO). Sebelumnya, hanya antrean standar yang didukung. Untuk detailnya, lihat Menggunakan Lambda dengan Amazon. SQS . | 18 November 2019 |
| Buat aplikasi di konsol Lambda | Pembuatan aplikasi di konsol Lambda sekarang tersedia secara umum. Untuk petunjuk, lihat Mengelola aplikasi di konsol Lambda . | 31 Oktober 2019 |

[Buat aplikasi di konsol Lambda \(beta\)](#)

Anda dapat membuat aplikasi Lambda yang dengan alur pengiriman berkelanjutan terpadu di konsol Lambda. Konsol menyediakan aplikasi sampel yang dapat Anda gunakan sebagai titik awal untuk proyek Anda. Pilih antara AWS CodeCommit dan GitHub untuk kontrol sumber. Setiap kali Anda melakukan perubahan pada repositori Anda, alur yang disertakan membangun dan men-deploy secara otomatis. Untuk petunjuk, lihat [Mengelola aplikasi di konsol Lambda](#).

3 Oktober 2019

[Peningkatan kinerja untuk fungsi VPC -connected](#)

Lambda sekarang menggunakan jenis baru elastic network interface yang dibagikan oleh semua fungsi dalam subnet virtual private cloud (VPC). Saat Anda menghubungkan fungsi keVPC, Lambda membuat antarmuka jaringan untuk setiap kombinasi grup keamanan dan subnet yang Anda pilih. Ketika antarmuka jaringan bersama tersedia, fungsi tidak perlu lagi membuat antarmuka jaringan tambahan saat jaringan menaikkan skala. Hal ini sangat meningkatkan waktu startup. Untuk detailnya, lihat [Mengonfigurasi fungsi Lambda untuk mengakses sumber daya](#) di file. VPC

Selasa, 03 September 2019

[Pengaturan batch streaming](#)

Sekarang Anda dapat mengonfigurasi jendela batch untuk sumber peristiwa pemetaan [Amazon DynamoDB](#) dan [Amazon Kinesis](#). Konfigurasikan jendela batch hingga lima menit untuk buffer catatan yang baru hingga batch penuh tersedia. Ini mengurangi i berapa kali fungsi Anda diaktifkan saat pengaliran kurang aktif.

Selasa, 29 Agustus 2019

[CloudWatch Integrasi Wawasan Log](#)

Halaman pemantauan di konsol Lambda sekarang menyertakan laporan dari Amazon CloudWatch Logs Insights.

Selasa, 18 Juni 2019

[Amazon Linux 2018.03](#)

Lingkungan eksekusi Lambda sedang diperbarui untuk menggunakan Amazon Linux 2018.03. Untuk detailnya, lihat [Lingkungan eksekusi](#).

21 Mei 2019

[Node.js 10](#)

Runtime baru tersedia untuk Node.js 10, nodejs10.x. Runtime ini menggunakan Node.js 10.15 dan akan diperbarui dengan keluaran poin terbaru Node.js 10 secara berkala. Node.js 10 juga merupakan Runtime pertama yang menggunakan Amazon Linux 2. Untuk detailnya, lihat [Membangun fungsi Lambda dengan Node.js](#).

Selasa, 13 Mei 2019

[GetLayerVersionByArn API](#)

Gunakan [GetLayerVersionByArnAPI](#) untuk mengunduh informasi versi lapisan dengan versi ARN sebagai input. Dibandingkan dengan `GetLayerVersion`, `GetLayerVersionByArn` memungkinkan Anda menggunakan ARN secara langsung alih-alih menguraikannya untuk mendapatkan nama lapisan dan nomor versi.

Selasa, 25 April 2019

| | | |
|--|--|--------------------------|
| Ruby | AWS Lambda sekarang mendukung Ruby 2.5 dengan runtime baru. Untuk detailnya, lihat Membangun fungsi Lambda dengan Ruby . | Selasa, 29 Nopember 2018 |
| Lapisan | Dengan layer Lambda, Anda dapat mengemas dan menyebarkan pustaka, Runtime khusus, dan ketergantungan lain secara terpisah dari kode fungsi Anda. Bagikan lapisan Anda dengan akun lain atau seluruh dunia. Untuk detailnya, lihat layer Lambda . | 29 November 2018 |
| Runtime kustom | Bangun runtime khusus untuk menjalankan fungsi Lambda pada bahasa pemrograman yang Anda sukai. Untuk detailnya, lihat Runtime Lambda khusus . | 29 November 2018 |
| Pemicu Application Load Balancer | Elastic Load Balancing kini mendukung fungsi Lambda sebagai target untuk Application Load Balancer. Untuk detailnya, lihat Menggunakan Lambda Application Load Balancer . | 29 November 2018 |

[Gunakan Kinesis HTTP /2 stream consumer sebagai pemicu](#)

Anda dapat menggunakan Kinesis HTTP /2 data stream konsumen untuk mengirim acara ke. AWS Lambda Konsumen streaming telah mendedikasikan throughput baca dari setiap pecahan dalam aliran data Anda dan menggunakan HTTP /2 untuk meminimalkan latensi. Untuk detailnya, lihat [Menggunakan Lambda dengan Kinesis](#).

19 November 2018

[Python 3.7](#)

AWS Lambda sekarang mendukung Python 3.7 dengan runtime baru. Untuk informasi selengkapnya, lihat [Membangun fungsi Lambda dengan Python](#).

Selasa, 19 Nopember 2018

[Peningkatan batas muatan untuk pemanggilan fungsi asinkron](#)

Ukuran muatan maksimum untuk pemanggilan asinkron meningkat dari 128 KB menjadi 256 KB, yang cocok dengan ukuran pesan maksimum dari pemicu Amazon. SNS Untuk detailnya, lihat [Kuota Lambda](#).

16 November 2018

[AWS GovCloud Wilayah \(AS-Timur\)](#)

AWS Lambda sekarang tersedia di Wilayah AWS GovCloud (AS-Timur).

12 November 2018

[Memindahkan AWS SAM topik ke Panduan Pengembang terpisah](#)

Sejumlah topik difokuskan pada pembuatan aplikasi tanpa server menggunakan AWS Serverless Application Model (AWS SAM). Topik-topik ini telah dipindahkan ke [panduan AWS Serverless Application Model pengembangan](#).

25 Oktober 2018

[Lihat aplikasi Lambda di konsol](#)

Anda dapat melihat status aplikasi Lambda Anda di halaman [Aplikasi](#) di konsol Lambda. Halaman ini menunjukkan status AWS CloudFormation tumpukan. Ini mencakup tautan ke halaman tempat Anda dapat melihat informasi selengkapnya tentang sumber daya dalam tumpukan. Anda juga dapat melihat metrik agregat untuk aplikasi dan membuat dasbor pemantauan kustom.

11 Oktober 2018

[Batas batas waktu eksekusi fungsi](#)

Untuk memungkinkan fungsi yang berlangsung lama, waktu habis eksekusi maksimum yang dapat dikonfigurasi akan meningkat dari 5 menit menjadi 15 menit. Untuk detailnya, lihat [batas Lambda](#).

10 Oktober 2018

| | | |
|--|---|-------------------|
| Support untuk bahasa PowerShell Inti di AWS Lambda | AWS Lambda sekarang mendukung bahasa PowerShell Inti. Untuk informasi selengkapnya, lihat Model pemrograman untuk membuat fungsi Lambda di PowerShell . | 11 September 2018 |
| Support untuk .NETRuntime Core 2.1.0 di AWS Lambda | AWS Lambda sekarang mendukung .NETRuntime Core 2.1.0. Untuk informasi lebih lanjut, lihat .NETInti CLI . | 9 Juli 2018 |
| Pembaruan sekarang tersedia RSS | Anda sekarang dapat berlangganan RSS feed untuk mengikuti rilis untuk panduan ini. | 5 Juli 2018 |
| Support untuk Amazon SQS sebagai sumber acara | AWS Lambda sekarang mendukung Amazon Simple Queue Service (AmazonSQS) sebagai sumber acara. Untuk informasi lebih lanjut, lihat Memanggil fungsi Lambda . | 28 Juni 2018 |
| Wilayah China (Ningxia) | AWS Lambda sekarang tersedia di Wilayah China (Ningxia). Untuk informasi selengkapnya tentang Wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di Referensi Umum AWS | 28 Juni 2018 |

Pembaruan sebelumnya

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan Developer AWS Lambda sebelum Juni 2018.

| Perubahan | Deskripsi | Tanggal |
|--|---|--------------------------|
| Dukungan runtime untuk Node.js 8.10 | AWS Lambda sekarang mendukung Node.js runtime versi 8.10. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Node.js . | Selasa, 02 April 2018 |
| Revisi fungsi dan alias IDs | AWS Lambda sekarang mendukung revisi IDs pada versi fungsi dan alias Anda. Anda dapat menggunakan ini IDs untuk melacak dan menerapkan pembaruan bersyarat saat memperbarui versi fungsi atau sumber daya alias Anda. | 25 Januari 2018 |
| Dukungan runtime untuk Go dan .NET2.0 | AWS Lambda telah menambahkan dukungan runtime untuk Go dan .NET2.0. Untuk informasi selengkapnya, silakan lihat Membangun fungsi Lambda dengan Go dan Membangun fungsi Lambda dengan C# . | Selasa, 15 Januari 2018 |
| Desain Ulang Konsol | AWS Lambda telah memperkenalkan konsol Lambda baru untuk menyederhanakan pengalaman Anda dan menambahkan Editor Kode Cloud9 untuk meningkatkan kemampuan Anda men-debug dan merevisi kode fungsi Anda. | 30 November 2017 |
| Mengatur Batas Konkurensi pada Fungsi Individu | AWS Lambda sekarang mendukung pengaturan batas konkurensi pada fungsi individu. Untuk informasi selengkapnya, lihat Mengkonfigurasi konkurensi cadangan untuk suatu fungsi . | 30 November 2017 |
| Pergeseran Lalu Lintas dengan Alias | AWS Lambda sekarang mendukung pergeseran lalu lintas dengan alias. Untuk informasi selengkapnya, lihat Buat penerapan bergulir untuk fungsi Lambda . | Selasa, 28 Nopember 2017 |
| Deployment Kode Gradual | AWS Lambda sekarang mendukung penerapan versi baru fungsi Lambda Anda dengan aman dengan memanfaatkan Penyebaran Kode. Untuk informasi selengkapnya, lihat Deployment kode gradual . | 28 November 2017 |

| Perubahan | Deskripsi | Tanggal |
|--------------------------------------|--|-------------------------|
| Wilayah Tiongkok (Beijing) | AWS Lambda sekarang tersedia di Wilayah China (Beijing). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | 9 November 2017 |
| Memperkenalkan SAM Lokal | AWS Lambda memperkenalkan SAM Local (sekarang dikenal sebagai SAMCLI), AWS CLI alat yang menyediakan lingkungan bagi Anda untuk mengembangkan, menguji, dan menganalisis aplikasi tanpa server Anda secara lokal sebelum mengunggahnya ke runtime Lambda. Untuk informasi selengkapnya, lihat Menguji dan men-debug aplikasi nirserver . | Selasa, 11 Agustus 2017 |
| Wilayah Kanada (Pusat) | AWS Lambda sekarang tersedia di Wilayah Kanada (Tengah). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | Selasa, 22 Juni 2017 |
| Wilayah Amerika Selatan (São Paulo) | AWS Lambda sekarang tersedia di Wilayah Amerika Selatan (São Paulo). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | 6 Juni 2017 |
| AWS Lambda dukungan untuk AWS X-Ray. | Lambda memperkenalkan dukungan untuk X-Ray, yang memungkinkan Anda mendeteksi, menganalisis, dan mengoptimalkan masalah performa dengan aplikasi Lambda Anda. Untuk informasi selengkapnya, lihat Visualisasikan pemanggilan fungsi Lambda menggunakan AWS X-Ray . | Selasa, 19 April 2017 |
| Wilayah Asia Pasifik (Mumbai) | AWS Lambda sekarang tersedia di Wilayah Asia Pasifik (Mumbai). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | 28 Maret 2017 |

| Perubahan | Deskripsi | Tanggal |
|---|---|-----------------------|
| AWS Lambda sekarang mendukung Node.js runtime v6.10 | AWS Lambda menambahkan dukungan untuk Node.js runtime v6.10. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Node.js . | Selasa, 22 Maret 2017 |
| Wilayah Eropa (London) | AWS Lambda sekarang tersedia di Wilayah Eropa (London). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di Referensi Umum AWS | 1 Februari 2017 |
| AWS Lambda dukungan untuk. NETruntime, Lambda @Edge (Pratinjau), Antrian Surat Mati dan penerapan otomatis aplikasi tanpa server. | AWS Lambda menambahkan dukungan untuk C#. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan C# . Lambda @Edge memungkinkan Anda menjalankan fungsi Lambda di lokasi AWS Edge sebagai respons terhadap peristiwa. CloudFront Untuk informasi selengkapnya, lihat Menggunakan AWS Lambda dengan CloudFront Lambda @Edge . | 3 Desember 2016 |
| AWS Lambda menambahkan Amazon Lex sebagai sumber acara yang didukung. | Dengan menggunakan Lambda dan Amazon Lex, Anda dapat dengan cepat membangun bot obrolan untuk berbagai layanan seperti Slack dan Facebook. | 30 November 2016 |
| Wilayah AS Barat (California Utara) | AWS Lambda sekarang tersedia di Wilayah AS Barat (California Utara). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di Referensi Umum AWS | 21 November 2016 |

| Perubahan | Deskripsi | Tanggal |
|--|--|--------------------------|
| Memperkenalkan AWS SAM untuk membuat dan menerapkan aplikasi berbasis Lambda dan menggunakan variabel lingkungan untuk pengaturan konfigurasi fungsi Lambda. | <p>AWS SAM: Anda sekarang dapat menggunakan AWS SAM untuk mendefinisikan sintaks untuk mengekspresikan sumber daya dalam aplikasi tanpa server. Untuk menerapkan aplikasi Anda, cukup tentukan sumber daya yang Anda butuhkan sebagai bagian dari aplikasi Anda, bersama dengan kebijakan izin terkait dalam file AWS CloudFormation templat (ditulis dalam salah satu JSON atau YAML), kemas artefak penerapan Anda, dan gunakan templat.</p> <p>Variabel lingkungan: Anda dapat menggunakan variabel lingkungan untuk menentukan pengaturan konfigurasi untuk fungsi Lambda Anda di luar kode fungsi Anda. Untuk informasi selengkapnya, lihat Gunakan variabel lingkungan Lambda untuk mengonfigurasi nilai dalam kode.</p> | Selasa, 18 Nopember 2016 |
| Wilayah Asia Pasifik (Seoul) | AWS Lambda sekarang tersedia di Wilayah Asia Pasifik (Seoul). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | 29 Agustus 2016 |
| Wilayah Asia Pacific (Sydney) | Lambda kini tersedia di Wilayah Asia Pacific (Sydney). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | Selasa, 23 Juni 2016 |
| Pembaruan untuk konsol Lambda | Konsol Lambda telah diperbarui untuk menyederhanakan proses pembuatan peran. | 23 Juni 2016 |
| AWS Lambda sekarang mendukung Node.js runtime v4.3 | AWS Lambda menambahkan dukungan untuk Node.js runtime v4.3. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Node.js . | Selasa, 07 April 2016 |

| Perubahan | Deskripsi | Tanggal |
|----------------------------------|---|------------------|
| Wilayah Eropa (Frankfurt) | Lambda kini tersedia di Wilayah Europe (Frankfurt). Untuk informasi selengkapnya tentang wilayah dan titik akhir Lambda, lihat Wilayah dan titik akhir di. Referensi Umum AWS | 14 Maret 2016 |
| VPCdukungan | Anda sekarang dapat mengonfigurasi fungsi Lambda untuk mengakses sumber daya di VPC Untuk informasi selengkapnya, lihat Memberikan fungsi Lambda akses ke sumber daya di Amazon VPC . | 11 Februari 2016 |
| Runtime Lambda sudah diperbarui. | Lingkungan eksekusi sudah diperbarui. | 4 November 2015 |

| Perubahan | Deskripsi | Tanggal |
|---|--|-----------------------|
| Dukungan versioning, Python untuk mengembangkan kode untuk fungsi Lambda, peristiwa terjadwal, dan peningkatan waktu eksekusi | <p>Sekarang Anda dapat mengembangkan kode fungsi Lambda menggunakan Python. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Python.</p> <p>Versioning: Anda dapat mempertahankan satu atau beberapa versi fungsi Lambda Anda. Versioning versi memungkinkan Anda mengontrol versi fungsi Lambda mana yang dijalankan di lingkungan yang berbeda (misalnya, pengembangan, pengujian, atau produksi). Untuk informasi selengkapnya, lihat Kelola versi fungsi Lambda.</p> <p>Peristiwa terjadwal: Anda juga dapat menyiapkan Lambda untuk mengambil kode Anda secara rutin dan terjadwal menggunakan konsol Lambda. Anda dapat menentukan nilai tetap (jumlah jam, hari, atau minggu) atau Anda dapat menentukan persamaan cron. Untuk informasi selengkapnya, lihat Memanggil fungsi Lambda sesuai jadwal.</p> <p>Peningkatan dalam waktu eksekusi: Sekarang Anda dapat menyiapkan fungsi Lambda Anda untuk berjalan hingga lima menit yang memungkinkan fungsi berjalan lebih lama seperti data volume besar yang masuk dan pekerjaan pemrosesan.</p> | 08 Oktober 2015 |
| Dukungan untuk DynamoDB Streams | DynamoDB Streams kini tersedia secara umum dan Anda dapat menggunakannya di semua wilayah tempat DynamoDB tersedia. Anda dapat mengaktifkan DynamoDB Streams untuk tabel Anda dan menggunakan fungsi Lambda sebagai pemicu untuk tabel. Pemicu adalah tindakan khusus yang Anda ambil dalam menanggapi pembaruan yang dibuat pada tabel DynamoDB. Untuk panduan contoh, lihat Tutorial: Menggunakan AWS Lambda dengan aliran Amazon DynamoDB . | 14 Juli 2015 |

| Perubahan | Deskripsi | Tanggal |
|--|--|--------------|
| Lambda sekarang mendukung pemanggilan fungsi Lambda dengan klien yang kompatibel. REST | <p>Hingga saat ini, untuk menjalankan fungsi Lambda Anda dari web, seluler, atau aplikasi IoT, Anda memerlukan AWS SDKs (misalnya AWS SDK, untuk Java AWS SDK, untuk Android, atau AWS SDK untuk iOS). Sekarang, Lambda mendukung pemanggilan fungsi Lambda dengan klien yang REST kompatibel melalui penyesuaian yang dapat API Anda buat menggunakan Amazon Gateway. API Anda dapat mengirim permintaan ke titik akhir fungsi Lambda Anda. URL Anda dapat mengonfigurasi keamanan pada titik akhir untuk memungkinkan akses terbuka, leverage AWS Identity and Access Management (IAM) untuk mengotorisasi akses, atau menggunakan API kunci untuk mengukur akses ke fungsi Lambda Anda oleh orang lain.</p> <p>Untuk contoh latihan Memulai, lihat Memanggil fungsi Lambda menggunakan titik akhir Amazon Gateway API.</p> <p>Untuk informasi selengkapnya tentang Amazon API Gateway, lihat https://aws.amazon.com/api-gateway/.</p> | 09 Juli 2015 |
| Konsol Lambda kini menyediakan cetak biru untuk membuat fungsi Lambda dan mengujinya dengan mudah. | <p>Konsol Lambda menyediakan serangkaian cetak biru. Setiap cetak biru menyediakan konfigurasi sumber peristiwa sampel dan kode sampel untuk fungsi Lambda Anda yang dapat Anda gunakan untuk membuat aplikasi berbasis Lambda dengan mudah. Semua latihan Lambda Memulai sekarang menggunakan cetak biru. Untuk informasi selengkapnya, lihat ???.</p> | 09 Juli 2015 |
| Lambda sekarang mendukung Java untuk membuat fungsi Lambda Anda. | <p>Sekarang Anda dapat menulis kode Lambda di Java. Untuk informasi selengkapnya, lihat Membangun fungsi Lambda dengan Java.</p> | 15 Juni 2015 |

| Perubahan | Deskripsi | Tanggal |
|--|--|------------------|
| Lambda kini mendukung penentuan objek Amazon S3 sebagai fungsi .zip saat membuat atau memperbarui fungsi Lambda. | Anda dapat mengunggah paket deployment fungsi Lambda (file .zip) ke bucket Amazon S3 di wilayah yang sama tempat Anda ingin membuat fungsi Lambda. Kemudian, Anda dapat menentukan nama bucket dan nama kunci objek saat Anda membuat atau memperbarui fungsi Lambda. | 28 Mei 2015 |
| Lambda sekarang tersedia secara umum dengan dukungan tambahan untuk backend seluler | <p>Lambda saat ini secara umum tersedia untuk pengguna n produksi. Rilis ini juga memperkenalkan fitur baru yang mempermudah pembuatan backend seluler, tablet, dan Internet of Things (IoT) menggunakan Lambda yang menskalakan secara otomatis tanpa menyediakan atau mengelola infrastruktur. Lambda sekarang mendukung peristiwa waktu nyata (sinkron) dan peristiwa asinkron. Fitur tambahan termasuk konfigurasi dan manajemen sumber peristiwa yang lebih mudah. Model izin dan model pemrograman telah disederhanakan dengan pengenalan kebijakan sumber daya untuk fungsi Lambda Anda.</p> <p>Dokumentasi telah diperbarui dengan cara yang sesuai. Untuk informasi lebih lanjut, lihat topik berikut:</p> <p>???</p> <p>AWS Lambda</p> | 9 April 2015 |
| Rilis pratinjau | Rilis pratinjau dari Panduan Developer AWS Lambda . | 13 November 2014 |

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.