



Panduan GuardDuty Pengguna Amazon

# Amazon GuardDuty



# Amazon GuardDuty: Panduan GuardDuty Pengguna Amazon

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 kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

---

# Table of Contents

|  |    |
|--|----|
| Apa itu GuardDuty? .....   | 1  |
| Fitur dari GuardDuty .....   | 2  |
| PCIDSSKepatuhan .....  | 5  |
| Harga di GuardDuty .....   | 5  |
| Menggunakan uji GuardDuty coba gratis 30 hari .....                            | 6  |
| Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis 12 bulan ..... | 7  |
| Mengakses GuardDuty .....  | 8  |
| Konsep dan terminologi .....   | 9  |
| Memulai .....  | 14 |
| Sebelum Anda mulai .....   | 14 |
| Langkah 1: Aktifkan Amazon GuardDuty .....                                     | 16 |
| Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar .....      | 18 |
| Langkah 3: Konfigurasi GuardDuty temuan ekspor ke bucket Amazon S3 .....       | 19 |
| Langkah 4: Siapkan GuardDuty pencarian peringatan melalui SNS .....            | 22 |
| Langkah selanjutnya .....  | 24 |
| Sumber data dasar .....  | 26 |
| AWS CloudTrail acara manajemen .....   | 26 |
| Bagaimana GuardDuty menangani peristiwa AWS CloudTrail global .....            | 27 |
| VPCLog Aliran .....  | 28 |
| Log kueri Route53 Resolver DNS .....   | 28 |
| GuardDuty fitur aktivasi .....   | 30 |
| Aktivasi fitur .....   | 30 |
| GuardDuty APIperubahan .....   | 30 |
| Fitur aktivasi dibandingkan dengan sumber data .....                           | 31 |
| Memahami cara kerja aktivasi fitur .....                                       | 31 |
| Memasukkan fitur perubahan aktivasi .....                                      | 32 |
| Pemetaan ke dataSourcesfeatures .....  | 33 |
| Perlindungan S3 .....  | 36 |
| Bagaimana GuardDuty menggunakan peristiwa data S3 .....                        | 36 |
| Fitur .....  | 37 |
| AWS CloudTrail peristiwa data untuk S3 .....                                   | 37 |
| Mengkonfigurasi Perlindungan S3 untuk akun mandiri .....                       | 38 |
| Untuk mengaktifkan atau menonaktifkan Perlindungan S3 .....                    | 38 |
| Mengkonfigurasi Perlindungan S3 di lingkungan beberapa akun .....              | 39 |

|   |     |
|---|-----|
| EKSPerlindungan .....   | 47  |
| Fitur .....   | 47  |
| EKSpemantauan log audit .....   | 47  |
| EKSPemantauan Log Audit .....   | 47  |
| Mengkonfigurasi Pemantauan Log EKS Audit untuk akun mandiri .....   | 38  |
| Mengkonfigurasi Pemantauan Log EKS Audit di lingkungan beberapa akun .....                                    | 49  |
| Pemantauan Runtime .....  | 57  |
| Cara kerjanya .....   | 58  |
| Dengan EC2 instans Amazon .....   | 59  |
| Dengan Fargate (hanya AmazonECS) .....  | 62  |
| Dengan EKS cluster Amazon .....   | 63  |
| Setelah konfigurasi Runtime Monitoring .....  | 64  |
| Uji coba gratis 30 hari .....   | 65  |
| Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS<br>Runtime Monitoring ..... | 65  |
| Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring .....                          | 66  |
| Konsep kunci - Pendekatan untuk mengelola agen GuardDuty keamanan .....                                       | 67  |
| Sumber daya Fargate (EKS khusus Amazon) - Pendekatan untuk mengelola agen<br>keamanan GuardDuty .....         | 67  |
| EKSCluster Amazon - Pendekatan untuk mengelola agen GuardDuty keamanan .....                                  | 68  |
| Mengaktifkan Runtime Monitoring .....   | 72  |
| Prasyarat .....   | 73  |
| Langkah-langkah untuk akun mandiri .....  | 85  |
| Langkah-langkah untuk lingkungan multi-akun .....   | 86  |
| Mengelola agen GuardDuty keamanan .....   | 90  |
| Mengkonfigurasi EKS Runtime Monitoring (hanya) API .....  | 207 |
| Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri .....   | 207 |
| Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun .....                                      | 214 |
| Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring .....   | 257 |
| Memeriksa EKS status konfigurasi Runtime Monitoring .....   | 258 |
| Nonaktifkan EKS Runtime Monitoring .....  | 259 |
| Menilai cakupan runtime .....   | 260 |
| Cakupan untuk EC2 instans Amazon .....  | 261 |
| Cakupan untuk ECS cluster Amazon .....  | 271 |
| Cakupan untuk EKS cluster Amazon .....  | 282 |
| Pertanyaan yang sering diajukan (FAQs) .....  | 295 |

|   |     |
|---|-----|
| Pengaturan CPU dan pemantauan memori .....                | 298 |
| Jenis acara runtime yang dikumpulkan .....                | 299 |
| Memproses acara .....                                     | 299 |
| Acara kontainer .....                                     | 301 |
| AWS Fargate (ECSHanya Amazon) peristiwa tugas .....       | 302 |
| Acara pod Kubernetes .....                                | 302 |
| DNSacara .....  | 303 |
| Buka acara .....  | 303 |
| Memuat acara modul .....                                  | 304 |
| Acara Mprotect .....                                      | 304 |
| Acara gunung .....  | 304 |
| Tautkan acara .....                                       | 304 |
| Acara Symlink .....                                       | 305 |
| Acara Dup .....   | 305 |
| Acara peta memori .....                                   | 306 |
| Acara soket .....   | 306 |
| Connect event .....                                       | 306 |
| Proses acara VM Readv .....                               | 307 |
| Proses acara VM Writev .....                              | 307 |
| Acara Ptrace .....  | 308 |
| Mengikat acara .....                                      | 308 |
| Dengarkan acara .....                                     | 309 |
| Ganti nama acara .....                                    | 309 |
| Atur UID acara .....                                      | 309 |
| Acara Chmod .....   | 310 |
| Agen hosting ECR repositori Amazon GuardDuty .....        | 310 |
| Untuk EKS agen versi 1.6.0 dan di atas .....              | 310 |
| Untuk EKS agen versi 1.5.0 dan sebelumnya .....           | 312 |
| Untuk AWS Fargate (ECSHanya Amazon) .....                 | 315 |
| GuardDuty sejarah rilis agen .....                        | 317 |
| Dampak penonaktifan .....                                 | 331 |
| Proses untuk membersihkan sumber daya agen keamanan ..... | 333 |
| Perlindungan Malware untuk EC2 .....                      | 335 |
| Fitur .....   | 338 |
| Volume Penyimpanan Blok Elastis (EBS) .....               | 338 |
| EBSVolume yang didukung .....                             | 339 |

|  |     |
|--|-----|
| Memodifikasi ID KMS kunci default .....  | 340 |
| Kustomisasi dalam Perlindungan Malware untuk EC2 .....                           | 341 |
| Pengaturan umum .....  | 341 |
| Opsi pindai dengan tag yang ditentukan pengguna .....                            | 342 |
| GuardDutyExcludedTag global .....  | 346 |
| GuardDuty-pemindaian malware yang dimulai .....                                  | 346 |
| Uji coba gratis 30 hari .....  | 348 |
| Mengkonfigurasi pemindaian GuardDuty malware yang dimulai .....                  | 348 |
| Temuan yang memanggil pemindaian GuardDuty malware yang dimulai .....            | 361 |
| Pemindaian malware sesuai permintaan .....                                       | 363 |
| Cara kerja pemindaian malware sesuai permintaan .....                            | 364 |
| Memulai .....  | 365 |
| Memantau status dan hasil pemindaian malware .....                               | 368 |
| GuardDuty akun layanan .....   | 369 |
| Perlindungan Malware untuk EC2 kuota .....                                       | 372 |
| Perlindungan Malware untuk S3 .....  | 377 |
| Harga .....  | 379 |
| Cara kerjanya .....  | 380 |
| Gambaran Umum .....  | 380 |
| IAMizin peran .....  | 380 |
| Penandaan opsional objek berdasarkan hasil pemindaian .....                      | 380 |
| Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember ..... | 381 |
| Kemampuan Perlindungan Malware untuk S3 .....                                    | 383 |
| (Opsional) Memulai dengan Perlindungan Malware hanya untuk S3 (konsol) .....     | 384 |
| Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda .....             | 385 |
| Prasyarat - Membuat atau memperbarui kebijakan peran IAM .....                   | 386 |
| Aktifkan Perlindungan Malware untuk deteksi ancaman S3 untuk bucket Anda .....   | 391 |
| Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3 .....         | 394 |
| Status sumber daya paket Perlindungan Malware .....                              | 396 |
| Memecahkan masalah rincian status paket Perlindungan Malware .....               | 396 |
| EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini .....                | 397 |
| EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada .....  | 398 |
| Bucket S3 tidak ada lagi .....   | 398 |
| Tidak dapat menempatkan objek uji .....  | 399 |
| Pemantauan dalam Perlindungan Malware untuk S3 .....                             | 400 |
| Menggunakan Amazon EventBridge .....   | 401 |

|   |     |
|---|-----|
| Menggunakan CloudWatch untuk memantau metrik status pemindaian .....                      | 410 |
| Menggunakan tag objek S3 .....  | 413 |
| Menggunakan kontrol akses berbasis tag ( ) TBAC .....                                     | 414 |
| TBACMenambahkan sumber daya bucket S3 .....   | 415 |
| Mengedit Perlindungan Malware untuk S3 untuk bucket yang dilindungi .....                 | 417 |
| Melihat penggunaan dan biaya .....  | 418 |
| Nonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi .....              | 418 |
| Dukungan fitur Amazon S3 .....  | 419 |
| Kuota dalam Perlindungan Malware untuk S3 .....   | 425 |
| RDSPerlindungan .....   | 427 |
| Database yang didukung .....  | 427 |
| Bagaimana RDS Protection menggunakan pemantauan aktivitas RDS login .....                 | 428 |
| Fitur .....   | 429 |
| RDSpemantauan aktivitas login .....   | 429 |
| Mengkonfigurasi RDS Perlindungan untuk akun mandiri .....                                 | 430 |
| Mengkonfigurasi RDS Perlindungan di lingkungan multi-akun .....                           | 430 |
| Perlindungan Lambda .....   | 438 |
| Fitur .....   | 438 |
| Pemantauan Aktivitas Jaringan Lambda .....  | 438 |
| Mengkonfigurasi Perlindungan Lambda .....   | 439 |
| Mengkonfigurasi Perlindungan Lambda untuk akun mandiri .....                              | 439 |
| Mengkonfigurasi Perlindungan Lambda di lingkungan multi-akun .....                        | 440 |
| Melindungi beban kerja AI .....   | 448 |
| Mengelola beberapa akun .....   | 449 |
| Akun administrator dan hubungan akun anggota .....  | 449 |
| Mengelola akun dengan AWS Organizations .....   | 454 |
| Pertimbangan dan rekomendasi .....  | 454 |
| Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty ..... | 456 |
| Menunjuk akun administrator yang didelegasikan GuardDuty .....                            | 458 |
| Memperbarui preferensi mengaktifkan otomatis organisasi .....                             | 459 |
| Menambahkan anggota ke organisasi .....   | 463 |
| (Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada .....                  | 465 |
| Mempertahankan organisasi Anda di dalam GuardDuty .....                                   | 466 |
| Mengubah akun GuardDuty administrator yang didelegasikan .....                            | 467 |
| Mengelola akun dengan undangan .....  | 469 |
| Menambahkan dan mengelola akun berdasarkan undangan .....                                 | 470 |

|  |     |
|--|-----|
| Mengkonsolidasikan akun GuardDuty administrator di bawah satu akun administrator yang didelegasikan GuardDuty organisasi ..... | 475 |
| Aktifkan GuardDuty di beberapa akun secara bersamaan .....   | 477 |
| Memahami temuan .....  | 480 |
| GuardDuty format temuan .....  | 480 |
| Tujuan Ancaman .....   | 482 |
| GuardDuty mesin pemindai deteksi malware .....   | 484 |
| Sampel temuan .....  | 485 |
| Menghasilkan temuan sampel melalui GuardDuty konsol atau API .....   | 485 |
| GuardDuty Temuan uji .....   | 487 |
| Pertimbangan .....   | 487 |
| GuardDuty temuan skrip tester dapat menghasilkan .....   | 488 |
| Langkah 1 - Prasyarat .....  | 490 |
| Langkah 2 - Menyebarkan sumber daya AWS .....  | 491 |
| Langkah 3 - Jalankan skrip pengujian .....   | 493 |
| Langkah 4 - Bersihkan sumber daya AWS tes .....  | 495 |
| Memecahkan masalah umum .....  | 495 |
| Tingkat keparahan untuk GuardDuty temuan .....   | 497 |
| Meninjau temuan GuardDuty .....  | 499 |
| Detail temuan .....  | 500 |
| Menemukan ikhtisar .....   | 500 |
| Sumber Daya .....  | 501 |
| RDSdatabase (DB) detail pengguna .....   | 508 |
| Detail penemuan Runtime Monitoring .....   | 508 |
| EBSdetail pemindaian volume .....  | 510 |
| Perlindungan Malware untuk EC2 menemukan detail .....  | 511 |
| Perlindungan Malware untuk detail penemuan S3 .....  | 512 |
| Tindakan .....   | 513 |
| Aktor atau Target .....  | 515 |
| Informasi tambahan .....   | 515 |
| Bukti .....  | 516 |
| Perilaku anomali .....   | 516 |
| GuardDuty menemukan agregasi .....   | 521 |
| Tipe temuan .....  | 523 |
| Tipe temuan EC2 .....  | 523 |
| Backdoor:EC2/C&CActivity.B .....   | 525 |



|   |     |
|---|-----|
| Backdoor:EC2/C&CActivity.B!DNS .....                  | 526 |
| Backdoor:EC2/DenialOfService.Dns .....                | 527 |
| Backdoor:EC2/DenialOfService.Tcp .....                | 528 |
| Backdoor:EC2/DenialOfService.Udp .....                | 528 |
| Backdoor:EC2/DenialOfService.UdpOnTcpPorts .....      | 529 |
| Backdoor:EC2/DenialOfService.UnusualProtocol .....    | 530 |
| Backdoor:EC2/Spambot .....                            | 530 |
| Behavior:EC2/NetworkPortUnusual .....                 | 531 |
| Behavior:EC2/TrafficVolumeUnusual .....               | 531 |
| CryptoCurrency:EC2/BitcoinTool.B .....                | 532 |
| CryptoCurrency:EC2/BitcoinTool.B!DNS .....            | 533 |
| DefenseEvasion:EC2/UnusualDNSResolver .....           | 533 |
| DefenseEvasion:EC2/UnusualDoHActivity .....           | 534 |
| DefenseEvasion:EC2/UnusualDoTActivity .....           | 534 |
| Impact:EC2/AbusedDomainRequest.Reputation .....       | 535 |
| Impact:EC2/BitcoinDomainRequest.Reputation .....      | 536 |
| Impact:EC2/MaliciousDomainRequest.Reputation .....    | 536 |
| Impact:EC2/PortSweep .....                            | 537 |
| Impact:EC2/SuspiciousDomainRequest.Reputation .....   | 537 |
| Impact:EC2/WinRMBruteForce .....                      | 538 |
| Recon:EC2/PortProbeEMRUnprotectedPort .....           | 539 |
| Recon:EC2/PortProbeUnprotectedPort .....              | 539 |
| Recon:EC2/Portscan .....                              | 540 |
| Trojan:EC2/BlackholeTraffic .....                     | 541 |
| Trojan:EC2/BlackholeTraffic!DNS .....                 | 542 |
| Trojan:EC2/DGADomainRequest.B .....                   | 542 |
| Trojan:EC2/DGADomainRequest.C!DNS .....               | 543 |
| Trojan:EC2/DNSDataExfiltration .....                  | 544 |
| Trojan:EC2/DriveBySourceTraffic!DNS .....             | 544 |
| Trojan:EC2/DropPoint .....                            | 545 |
| Trojan:EC2/DropPoint!DNS .....                        | 545 |
| Trojan:EC2/PhishingDomainRequest!DNS .....            | 546 |
| UnauthorizedAccess:EC2/MaliciousIPCaller.Custom ..... | 546 |
| UnauthorizedAccess:EC2/MetadataDNSRebind .....        | 547 |
| UnauthorizedAccess:EC2/RDPBruteForce .....            | 548 |
| UnauthorizedAccess:EC2/SSHBruteForce .....            | 549 |

|  |     |
|--|-----|
| UnauthorizedAccess:EC2/TorClient .....                                     | 550 |
| UnauthorizedAccess:EC2/TorRelay .....                                      | 551 |
| IAMmenemukan jenis .....   | 551 |
| CredentialAccess:IAMUser/AnomalousBehavior .....                           | 552 |
| DefenseEvasion:IAMUser/AnomalousBehavior .....                             | 553 |
| Discovery:IAMUser/AnomalousBehavior .....                                  | 554 |
| Exfiltration:IAMUser/AnomalousBehavior .....                               | 554 |
| Impact:IAMUser/AnomalousBehavior .....                                     | 555 |
| InitialAccess:IAMUser/AnomalousBehavior .....                              | 556 |
| PenTest:IAMUser/KaliLinux .....  | 557 |
| PenTest:IAMUser/ParrotLinux .....  | 557 |
| PenTest:IAMUser/PentooLinux .....  | 558 |
| Persistence:IAMUser/AnomalousBehavior .....                                | 558 |
| Policy:IAMUser/RootCredentialUsage .....                                   | 559 |
| PrivilegeEscalation:IAMUser/AnomalousBehavior .....                        | 560 |
| Recon:IAMUser/MaliciousIPCaller .....                                      | 561 |
| Recon:IAMUser/MaliciousIPCaller.Custom .....                               | 561 |
| Recon:IAMUser/TorIPCaller .....  | 562 |
| Stealth:IAMUser/CloudTrailLoggingDisabled .....                            | 562 |
| Stealth:IAMUser/PasswordPolicyChange .....                                 | 563 |
| UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B .....                     | 563 |
| UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS ..... | 564 |
| UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS ..... | 565 |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller .....                         | 567 |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom .....                  | 567 |
| UnauthorizedAccess:IAMUser/TorIPCaller .....                               | 568 |
| Tipe temuan S3 .....   | 568 |
| Discovery:S3/AnomalousBehavior .....                                       | 570 |
| Discovery:S3/MaliciousIPCaller .....                                       | 570 |
| Discovery:S3/MaliciousIPCaller.Custom .....                                | 571 |
| Discovery:S3/TorIPCaller .....   | 571 |
| Exfiltration:S3/AnomalousBehavior .....                                    | 572 |
| Exfiltration:S3/MaliciousIPCaller .....                                    | 573 |
| Impact:S3/AnomalousBehavior.Delete .....                                   | 573 |
| Impact:S3/AnomalousBehavior.Permission .....                               | 574 |
| Impact:S3/AnomalousBehavior.Write .....                                    | 575 |

|   |     |
|---|-----|
| Impact:S3/MaliciousIPCaller .....                           | 576 |
| PenTest:S3/KaliLinux .....                                  | 576 |
| PenTest:S3/ParrotLinux .....                                | 577 |
| PenTest:S3/Pentoolinux .....                                | 577 |
| Policy:S3/AccountBlockPublicAccessDisabled .....            | 578 |
| Policy:S3/BucketAnonymousAccessGranted .....                | 579 |
| Policy:S3/BucketBlockPublicAccessDisabled .....             | 579 |
| Policy:S3/BucketPublicAccessGranted .....                   | 580 |
| Stealth:S3/ServerAccessLoggingDisabled .....                | 581 |
| UnauthorizedAccess:S3/MaliciousIPCaller.Custom .....        | 581 |
| UnauthorizedAccess:S3/TorIPCaller .....                     | 582 |
| EKSjenis pencarian log audit .....                          | 582 |
| CredentialAccess:Kubernetes/MaliciousIPCaller .....         | 584 |
| CredentialAccess:Kubernetes/MaliciousIPCaller.Custom .....  | 585 |
| CredentialAccess:Kubernetes/SuccessfulAnonymousAccess ..... | 586 |
| CredentialAccess:Kubernetes/TorIPCaller .....               | 586 |
| DefenseEvasion:Kubernetes/MaliciousIPCaller .....           | 587 |
| DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom .....    | 588 |
| DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess .....   | 588 |
| DefenseEvasion:Kubernetes/TorIPCaller .....                 | 589 |
| Discovery:Kubernetes/MaliciousIPCaller .....                | 590 |
| Discovery:Kubernetes/MaliciousIPCaller.Custom .....         | 591 |
| Discovery:Kubernetes/SuccessfulAnonymousAccess .....        | 591 |
| Discovery:Kubernetes/TorIPCaller .....                      | 592 |
| Execution:Kubernetes/ExecInKubeSystemPod .....              | 593 |
| Impact:Kubernetes/MaliciousIPCaller .....                   | 593 |
| Impact:Kubernetes/MaliciousIPCaller.Custom .....            | 594 |
| Impact:Kubernetes/SuccessfulAnonymousAccess .....           | 595 |
| Impact:Kubernetes/TorIPCaller .....                         | 595 |
| Persistence:Kubernetes/ContainerWithSensitiveMount .....    | 596 |
| Persistence:Kubernetes/MaliciousIPCaller .....              | 597 |
| Persistence:Kubernetes/MaliciousIPCaller.Custom .....       | 597 |
| Persistence:Kubernetes/SuccessfulAnonymousAccess .....      | 598 |
| Persistence:Kubernetes/TorIPCaller .....                    | 599 |
| Policy:Kubernetes/AdminAccessToDefaultServiceAccount .....  | 599 |
| Policy:Kubernetes/AnonymousAccessGranted .....              | 600 |

|   |     |
|---|-----|
| Policy:Kubernetes/ExposedDashboard .....  | 601 |
| Policy:Kubernetes/KubeflowDashboardExposed .....  | 601 |
| PrivilegeEscalation:Kubernetes/PrivilegedContainer .....  | 602 |
| CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed .....                             | 602 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated .....                       | 603 |
| Execution:Kubernetes/AnomalousBehavior.ExecInPod .....  | 604 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!<br>PrivilegedContainer ..... | 605 |
| Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!<br>ContainerWithSensitiveMount ..... | 606 |
| Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed .....                                   | 607 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated .....                              | 608 |
| Discovery:Kubernetes/AnomalousBehavior.PermissionChecked .....                                  | 609 |
| Jenis penemuan Runtime Monitoring .....   | 610 |
| CryptoCurrency:Runtime/BitcoinTool.B .....  | 612 |
| Backdoor:Runtime/C&CActivity.B .....  | 613 |
| UnauthorizedAccess:Runtime/TorRelay .....   | 614 |
| UnauthorizedAccess:Runtime/TorClient .....  | 614 |
| Trojan:Runtime/BlackholeTraffic .....   | 615 |
| Trojan:Runtime/DropPoint .....  | 616 |
| CryptoCurrency:Runtime/BitcoinTool.B!DNS .....  | 616 |
| Backdoor:Runtime/C&CActivity.B!DNS .....  | 617 |
| Trojan:Runtime/BlackholeTraffic!DNS .....   | 618 |
| Trojan:Runtime/DropPoint!DNS .....  | 619 |
| Trojan:Runtime/DGADomainRequest.C!DNS .....   | 619 |
| Trojan:Runtime/DriveBySourceTraffic!DNS .....   | 620 |
| Trojan:Runtime/PhishingDomainRequest!DNS .....  | 621 |
| Impact:Runtime/AbusedDomainRequest.Reputation .....   | 621 |
| Impact:Runtime/BitcoinDomainRequest.Reputation .....  | 622 |
| Impact:Runtime/MaliciousDomainRequest.Reputation .....  | 623 |
| Impact:Runtime/SuspiciousDomainRequest.Reputation .....   | 624 |
| UnauthorizedAccess:Runtime/MetadataDNSRebind .....  | 624 |
| Execution:Runtime/NewBinaryExecuted .....   | 626 |
| PrivilegeEscalation:Runtime/DockerSocketAccessed .....  | 626 |
| PrivilegeEscalation:Runtime/RuncContainerEscape .....   | 627 |
| PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified .....                                   | 628 |

|   |     |
|---|-----|
| DefenseEvasion:Runtime/ProcessInjection.Proc .....                | 629 |
| DefenseEvasion:Runtime/ProcessInjection.Ptrace .....              | 629 |
| DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite .....  | 630 |
| Execution:Runtime/ReverseShell .....                              | 630 |
| DefenseEvasion:Runtime/FilelessExecution .....                    | 631 |
| Impact:Runtime/CryptoMinerExecuted .....                          | 632 |
| Execution:Runtime/NewLibraryLoaded .....                          | 632 |
| PrivilegeEscalation:Runtime/ContainerMountsHostDirectory .....    | 633 |
| PrivilegeEscalation:Runtime/UserfaultfdUsage .....                | 633 |
| Execution:Runtime/SuspiciousTool .....                            | 634 |
| Execution:Runtime/SuspiciousCommand .....                         | 635 |
| DefenseEvasion:Runtime/SuspiciousCommand .....                    | 636 |
| DefenseEvasion:Runtime/PtraceAntiDebugging .....                  | 636 |
| Execution:Runtime/MaliciousFileExecuted .....                     | 637 |
| Execution:Runtime/SuspiciousShellCreated .....                    | 638 |
| PrivilegeEscalation:Runtime/ElevationToRoot .....                 | 638 |
| Perlindungan Malware untuk jenis pencarian EC2 .....              | 639 |
| Execution:EC2/MaliciousFile .....                                 | 640 |
| Execution:ECS/MaliciousFile .....                                 | 641 |
| Execution:Kubernetes/MaliciousFile .....                          | 641 |
| Execution:Container/MaliciousFile .....                           | 641 |
| Execution:EC2/SuspiciousFile .....                                | 642 |
| Execution:ECS/SuspiciousFile .....                                | 643 |
| Execution:Kubernetes/SuspiciousFile .....                         | 643 |
| Execution:Container/SuspiciousFile .....                          | 644 |
| Perlindungan Malware untuk tipe pencarian S3 .....                | 645 |
| Object:S3/MaliciousFile .....                                     | 645 |
| Jenis temuan Perlindungan RDS .....                               | 646 |
| CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin .....      | 646 |
| CredentialAccess:RDS/AnomalousBehavior.FailedLogin .....          | 647 |
| CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce ..... | 648 |
| CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin .....      | 649 |
| CredentialAccess:RDS/MaliciousIPCaller.FailedLogin .....          | 650 |
| Discovery:RDS/MaliciousIPCaller .....                             | 650 |
| CredentialAccess:RDS/TorIPCaller.SuccessfulLogin .....            | 651 |
| CredentialAccess:RDS/TorIPCaller.FailedLogin .....                | 651 |

|   |     |
|---|-----|
| Discovery:RDS/TorIPCaller .....                             | 652 |
| Tipe temuan Lambda Protection .....                         | 653 |
| Backdoor:Lambda/C&CActivity.B .....                         | 653 |
| CryptoCurrency:Lambda/BitcoinTool.B .....                   | 654 |
| Trojan:Lambda/BlackholeTraffic .....                        | 655 |
| Trojan:Lambda/DropPoint .....                               | 655 |
| UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom .....    | 656 |
| UnauthorizedAccess:Lambda/TorClient .....                   | 656 |
| UnauthorizedAccess:Lambda/TorRelay .....                    | 657 |
| Tipe temuan yang sudah dihentikan .....                     | 657 |
| Exfiltration:S3/ObjectRead.Unusual .....                    | 658 |
| Impact:S3/PermissionsModification.Unusual .....             | 659 |
| Impact:S3/ObjectDelete.Unusual .....                        | 660 |
| Discovery:S3/BucketEnumeration.Unusual .....                | 660 |
| Persistence:IAMUser/NetworkPermissions .....                | 661 |
| Persistence:IAMUser/ResourcePermissions .....               | 662 |
| Persistence:IAMUser/UserPermissions .....                   | 663 |
| PrivilegeEscalation:IAMUser/AdministrativePermissions ..... | 663 |
| Recon:IAMUser/NetworkPermissions .....                      | 664 |
| Recon:IAMUser/ResourcePermissions .....                     | 665 |
| Recon:IAMUser/UserPermissions .....                         | 666 |
| ResourceConsumption:IAMUser/ComputeResources .....          | 666 |
| Stealth:IAMUser/LoggingConfigurationModified .....          | 667 |
| UnauthorizedAccess:IAMUser/ConsoleLogin .....               | 668 |
| UnauthorizedAccess:EC2/TorIPCaller .....                    | 669 |
| Backdoor:EC2/XORDDOS .....                                  | 669 |
| Behavior:IAMUser/InstanceLaunchUnusual .....                | 670 |
| CryptoCurrency:EC2/BitcoinTool.A .....                      | 670 |
| UnauthorizedAccess:IAMUser/UnusualASNCaller .....           | 670 |
| Temuan berdasarkan tipe sumber daya .....                   | 671 |
| Tabel temuan .....  | 671 |
| Mengelola GuardDuty temuan .....                            | 701 |
| Ringkasan .....   | 702 |
| Mengakses dasbor Ringkasan .....                            | 703 |
| Memahami dasbor Ringkasan .....                             | 703 |
| Memberikan umpan balik di dasbor Ringkasan .....            | 706 |

|  |     |
|--|-----|
| Memfilter temuan .....   | 707 |
| Membuat filter di GuardDuty konsol .....   | 707 |
| Atribut filter .....   | 708 |
| Aturan penekanan .....   | 715 |
| .....  | 715 |
| Kasus penggunaan umum untuk aturan penekanan dan contoh .....                                      | 716 |
| Membuat aturan penekanan .....   | 719 |
| Menghapus aturan penekanan .....   | 722 |
| .....  | 721 |
| Daftar IP terpercaya dan daftar ancaman .....  | 723 |
| Format daftar .....  | 724 |
| Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman .....                | 728 |
| Menggunakan enkripsi sisi server untuk daftar IP terpercaya dan daftar ancaman .....               | 729 |
| Menambahkan dan mengaktifkan daftar IP terpercaya atau daftar IP ancaman .....                     | 729 |
| Memperbarui daftar IP terpercaya dan daftar ancaman .....  | 732 |
| Menonaktifkan atau menghapus daftar IP terpercaya atau daftar ancaman .....                        | 733 |
| Mengekspor temuan .....  | 734 |
| Pertimbangan .....   | 735 |
| Langkah 1 - Izin diperlukan untuk mengekspor temuan .....  | 736 |
| Langkah 2 — Melampirkan kebijakan ke kunci Anda KMS .....  | 736 |
| Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3 .....  | 738 |
| Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol) .....  | 742 |
| Langkah 5 - Frekuensi untuk mengekspor temuan .....  | 743 |
| Mengotomatiskan tanggapan dengan Acara CloudWatch .....  | 744 |
| CloudWatch Frekuensi pemberitahuan acara untuk GuardDuty .....                                     | 745 |
| CloudWatch format acara untuk GuardDuty .....  | 746 |
| Membuat aturan CloudWatch Acara untuk memberi tahu Anda tentang GuardDuty temuan<br>(konsol) ..... | 747 |
| Membuat aturan dan target CloudWatch Acara untuk GuardDuty (CLI) .....                             | 753 |
| CloudWatch Acara untuk lingkungan GuardDuty multi-akun .....                                       | 755 |
| Memahami CloudWatch Log dan alasan melewatkan sumber daya .....                                    | 756 |
| Mengaudit CloudWatch Log dalam Perlindungan GuardDuty Malware untuk EC2 .....                      | 756 |
| GuardDuty Perlindungan Malware untuk retensi log EC2 .....   | 758 |
| Alasan melewatkan sumber daya .....  | 758 |
| Melaporkan positif palsu dalam Perlindungan Malware untuk EC2 .....                                | 763 |
| Pengajuan file positif palsu .....   | 763 |

|   |     |
|---|-----|
| Mengatasi temuan .....  | 765 |
| Memperbaiki instans Amazon yang berpotensi dikompromikan EC2 .....                              | 765 |
| Memulihkan bucket S3 yang berpotensi dikompromikan .....  | 767 |
| Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu .....                                | 769 |
| Memperbaiki objek S3 yang berpotensi berbahaya .....  | 769 |
| Memulihkan cluster yang berpotensi dikompromikan ECS .....                                      | 770 |
| Memulihkan kredensi yang berpotensi dikompromikan AWS .....                                     | 771 |
| Memulihkan wadah mandiri yang berpotensi dikompromikan .....                                    | 772 |
| Memediasi temuan Pemantauan Log Audit EKS .....   | 773 |
| Potensi masalah konfigurasi .....   | 774 |
| Memulihkan pengguna Kubernetes yang berpotensi dikompromikan .....                              | 774 |
| Remediasi pod Kubernetes yang berpotensi dikompromikan .....                                    | 777 |
| Memulihkan gambar kontainer yang berpotensi dikompromikan .....                                 | 779 |
| Remediasi node Kubernetes yang berpotensi dikompromikan .....                                   | 779 |
| Remediasi temuan Runtime Monitoring .....   | 780 |
| Memulihkan gambar kontainer yang dikompromikan .....  | 782 |
| Memulihkan database yang berpotensi dikompromikan .....   | 782 |
| Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil .....    | 783 |
| Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal .           | 784 |
| Memulihkan kredensyal yang berpotensi dikompromikan .....                                       | 785 |
| Batasi akses jaringan .....   | 786 |
| Memperbaiki fungsi Lambda yang berpotensi dikompromikan .....                                   | 786 |
| Memperkirakan biaya .....   | 788 |
| Memahami cara GuardDuty menghitung biaya penggunaan .....                                       | 789 |
| .....   | 789 |
| Runtime Monitoring - Bagaimana VPC flow log dari EC2 instans memengaruhi biaya penggunaan ..... | 790 |
| Bagaimana GuardDuty memperkirakan biaya penggunaan untuk CloudTrail acara .....                 | 790 |
| Meninjau statistik GuardDuty penggunaan .....   | 790 |
| Keamanan .....  | 793 |
| Perlindungan data .....   | 794 |
| Enkripsi diam .....   | 795 |
| Enkripsi bergerak .....   | 795 |
| Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan .....                         | 795 |
| Logging dengan CloudTrail .....   | 797 |



|   |     |
|---|-----|
| GuardDuty informasi di CloudTrail .....                                 | 797 |
| GuardDuty peristiwa pesawat kontrol di CloudTrail .....                 | 798 |
| GuardDuty peristiwa data di CloudTrail .....                            | 798 |
| Contoh: entri file GuardDuty log .....                                  | 799 |
| Identity and Access Management .....                                    | 802 |
| Audiens .....   | 802 |
| Mengautentikasi dengan identitas .....                                  | 803 |
| Mengelola akses menggunakan kebijakan .....                             | 807 |
| Bagaimana Amazon GuardDuty bekerja dengan IAM .....                     | 809 |
| Contoh kebijakan berbasis identitas .....                               | 816 |
| Menggunakan peran terkait layanan .....                                 | 825 |
| AWS kebijakan terkelola .....   | 846 |
| Pemecahan Masalah .....   | 855 |
| Validasi kepatuhan .....  | 857 |
| Ketahanan .....   | 859 |
| Keamanan infrastruktur .....  | 859 |
| Integrasi dengan layanan lain AWS .....                                 | 861 |
| Integrasi dengan GuardDuty AWS Security Hub .....                       | 861 |
| Integrasi GuardDuty dengan Amazon Detective .....                       | 861 |
| AWS Security Hub integrasi .....  | 861 |
| Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub ..... | 862 |
| Melihat GuardDuty temuan di AWS Security Hub .....                      | 863 |
| Mengaktifkan dan mengonfigurasi integrasi .....                         | 881 |
| Menggunakan GuardDuty kontrol di Security Hub .....                     | 881 |
| Menghentikan publikasi temuan ke Security Hub .....                     | 882 |
| Integrasi Amazon Detective .....  | 882 |
| Mengaktifkan integrasi .....  | 882 |
| Berputar ke Detektif Amazon dari sebuah temuan GuardDuty .....          | 883 |
| Menggunakan integrasi dengan lingkungan GuardDuty multi-akun .....      | 883 |
| Menangguhkan atau menonaktifkan .....                                   | 885 |
| GuardDuty pengumuman .....  | 887 |
| Format SNS pesan Amazon .....   | 893 |
| Kuota .....   | 898 |
| Pemecahan Masalah .....   | 903 |
| Masalah umum di GuardDuty .....   | 903 |

|   |         |
|---|---------|
| Saya mendapatkan kesalahan akses saat mengekspor GuardDuty temuan. Bagaimana saya bisa menyelesaikan ini? .....   | 903     |
| Perlindungan Malware untuk masalah EC2 .....  | 904     |
| Saya memulai pemindaian malware On-Demand tetapi menghasilkan kesalahan izin yang diperlukan hilang. ....   | 904     |
| Saya menerima iam:GetRole kesalahan saat bekerja dengan Perlindungan Malware untuk EC2. ....  | 904     |
| Saya adalah akun GuardDuty administrator yang perlu mengaktifkan GuardDuty pemindaian malware yang dimulai tetapi tidak menggunakan kebijakan AWS terkelola: AmazonGuardDutyFullAccess untuk mengelola. GuardDuty ..... | 904     |
| Masalah Runtime Monitoring .....  | 905     |
| AWS Step Functions Alur kerja saya gagal secara tak terduga .....   | 905     |
| Memecahkan masalah kesalahan memori .....   | 905     |
| Mengelola beberapa masalah akun .....   | 906     |
| Saya ingin mengelola banyak akun tetapi tidak memiliki izin AWS Organizations manajemen yang diperlukan. ....   | 906     |
| Masalah pemecahan masalah lainnya .....   | 906     |
| Wilayah dan titik akhir .....   | 907     |
| Ketersediaan fitur khusus wilayah .....   | 907     |
| Tindakan dan parameter lama .....   | 909     |
| Riwayat dokumen .....   | 911     |
| Pembaruan sebelumnya .....  | 975     |
| .....   | cmlxxvi |

# Apa itu Amazon GuardDuty?

Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau, menganalisis, dan memproses sumber AWS data dan log di AWS lingkungan Anda. GuardDuty Menggunakan feed intelijen ancaman, seperti daftar alamat IP berbahaya dan domain, hash file, dan model machine learning (ML) untuk mengidentifikasi aktivitas mencurigakan dan berpotensi berbahaya di lingkungan Anda. AWS Daftar berikut memberikan ikhtisar skenario ancaman potensial yang GuardDuty dapat membantu Anda mendeteksi:

- Kredensi yang dikompromikan dan diekstraksi. AWS
- Eksfiltrasi dan penghancuran data yang dapat menyebabkan peristiwa ransomware. Pola peristiwa login yang tidak biasa dalam versi mesin yang didukung dari basis data Amazon Aurora dan RDS Amazon, yang menunjukkan perilaku anomali.
- Aktivitas cryptomining yang tidak sah di instans Amazon Elastic Compute Cloud (AmazonEC2) dan beban kerja container Anda.
- Kehadiran malware di EC2 instans Amazon dan beban kerja penampung, serta file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3).
- Tingkat sistem operasi, jaringan, dan peristiwa file yang menunjukkan perilaku tidak sah pada kluster Amazon Elastic Kubernetes Service (Amazon), EKS Amazon Elastic Container Service (Amazon) - tugas, dan ECS instans AWS Fargate (Fargate) Amazon serta beban kerja container. EC2

## [Apa itu Amazon GuardDuty](#)

### Daftar Isi

- [Fitur dari GuardDuty](#)
- [PCIDSSKepatuhan](#)
- [Harga di GuardDuty](#)
- [Mengakses GuardDuty](#)

## Fitur dari GuardDuty

Berikut adalah beberapa cara utama Amazon GuardDuty dapat membantu Anda memantau, mendeteksi, dan mengelola potensi ancaman di AWS lingkungan Anda.

Terus memantau sumber data tertentu dan log peristiwa

- **Deteksi ancaman dasar** — Ketika Anda mengaktifkan GuardDuty Akun AWS, GuardDuty secara otomatis mulai menelan sumber data dasar yang terkait dengan akun itu. Sumber data ini mencakup peristiwa AWS CloudTrail manajemen, log VPC aliran (dari EC2 instans Amazon), dan DNS log. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan memproses sumber data ini untuk menghasilkan temuan keamanan terkait. Untuk informasi selengkapnya, lihat [GuardDuty sumber data dasar](#).
- **Paket GuardDuty perlindungan yang berfokus pada kasus penggunaan** — Untuk meningkatkan visibilitas deteksi ancaman ke dalam keamanan AWS lingkungan Anda, GuardDuty menawarkan paket perlindungan khusus yang dapat Anda pilih untuk diaktifkan. Paket perlindungan membantu Anda memantau log dan peristiwa dari AWS layanan lain. Sumber-sumber ini termasuk log EKS audit, aktivitas RDS login, peristiwa data Amazon S3 CloudTrail, EBS volume, Runtime Monitoring di Amazon, Amazon, EC2 dan EKS Amazon ECS -Fargate, dan log aktivitas jaringan Lambda. GuardDuty mengkonsolidasikan sumber log dan peristiwa ini di bawah istilah - [Fitur](#). Anda dapat mengaktifkan satu atau lebih paket perlindungan khusus di dukungan Wilayah AWS kapan saja. GuardDuty akan mulai memantau, memproses, dan menganalisis aktivitas berdasarkan rencana perlindungan yang Anda aktifkan. Untuk informasi selengkapnya tentang setiap rencana perlindungan dan cara kerjanya, lihat dokumen rencana perlindungan yang sesuai.

| Rencana perlindungan               | Deskripsi  |
|------------------------------------|--|
| <a href="#">Perlindungan S3</a>    | Mengidentifikasi potensi risiko keamanan seperti eksfiltrasi data dan upaya penghancuran di bucket Amazon S3 Anda.                                 |
| <a href="#">EKSPerindungan</a>     | EKSAudit Log Monitoring menganalisis log audit Kubernetes dari EKS kluster Amazon Anda untuk aktivitas yang berpotensi mencurigakan dan berbahaya. |
| <a href="#">Pemantauan Runtime</a> | Memantau dan menganalisis peristiwa tingkat sistem operasi di Amazon, Amazon, EC2 dan EKS Amazon Anda  |

| Rencana perlindungan                           | Deskripsi   |
|--|---|
|  | ECS (termasuk AWS Fargate), untuk mendeteksi potensi ancaman runtime.   |
| <a href="#">Perlindungan Malware untuk EC2</a> | Mendeteksi potensi keberadaan malware dengan memindai EBS volume Amazon yang terkait dengan EC2 instans Amazon Anda. Ada opsi untuk menggunakan fitur ini sesuai permintaan.  |
| <a href="#">Perlindungan Malware untuk S3</a>  | Mendeteksi potensi keberadaan malware di objek yang baru diunggah dalam bucket Amazon S3 Anda.  |
| <a href="#">RDSPerlindungan</a>                | Menganalisis dan membuat profil aktivitas RDS login Anda untuk potensi ancaman akses ke basis data Amazon Aurora dan Amazon RDS yang didukung.  |
| <a href="#">Perlindungan Lambda</a>            | Memantau log aktivitas jaringan Lambda, dimulai dengan log VPC aliran, untuk mendeteksi ancaman terhadap fungsi Anda AWS Lambda . Contoh ancaman potensial ini termasuk cryptomining dan berkomunikasi dengan server jahat. |

**i** Aktifkan Perlindungan Malware untuk S3 secara mandiri

GuardDuty menawarkan fleksibilitas untuk menggunakan Perlindungan Malware untuk S3 secara independen, tanpa mengaktifkan layanan Amazon GuardDuty . Untuk informasi selengkapnya tentang memulai hanya dengan Perlindungan Malware untuk S3, lihat [GuardDuty Perlindungan Malware untuk S3](#). Untuk menggunakan semua paket perlindungan lainnya, Anda harus mengaktifkan GuardDuty layanan.

## Mengelola lingkungan multi-akun

Anda dapat mengelola AWS lingkungan beberapa akun dengan menggunakan metode undangan AWS Organizations (disarankan) atau lama. Untuk informasi selengkapnya, lihat [Mengelola beberapa akun](#).

## Menghasilkan temuan keamanan untuk ancaman yang terdeteksi

Ketika GuardDuty mendeteksi potensi ancaman keamanan yang terkait dengan AWS sumber daya Anda, itu mulai menghasilkan temuan keamanan yang memberikan informasi tentang sumber daya yang berpotensi dikompromikan. Setelah Anda mengaktifkan GuardDuty di akun Anda, buat [Sampel temuan](#) untuk melihat yang terkait [Detail temuan](#). Untuk daftar lengkap temuan keamanan, lihat [Tipe temuan](#).

Dengan GuardDuty, Anda juga dapat menggunakan skrip pengujian yang menghasilkan temuan GuardDuty keamanan khusus untuk memahami cara meninjau dan menanggapi GuardDuty temuan. Untuk informasi selengkapnya, lihat [GuardDuty Temuan uji di akun khusus](#).

## Menilai dan mengelola temuan keamanan

GuardDuty menggabungkan temuan keamanan Anda di seluruh akun dan menampilkan hasil di dasbor Ringkasan di GuardDuty konsol. Anda juga dapat mengambil temuan melalui AWS Security Hub API, AWS Command Line Interface, atau AWS SDK. Dengan pandangan holistik tentang status keamanan Anda saat ini, Anda dapat mengidentifikasi tren dan potensi masalah, dan mengambil langkah-langkah perbaikan yang diperlukan. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty temuan](#).

## Integrasi dengan layanan AWS keamanan terkait

Untuk lebih membantu Anda menganalisis dan menyelidiki tren keamanan di AWS lingkungan Anda, pertimbangkan untuk menggunakan layanan AWS terkait keamanan berikut dalam kombinasi dengan GuardDuty

- **AWS Security Hub**— Layanan ini memberi Anda pandangan komprehensif tentang keadaan keamanan AWS sumber daya Anda dan membantu Anda memeriksa AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Hal ini dilakukan sebagian dengan mengonsumsi, menggabungkan, mengatur, dan memprioritaskan temuan keamanan Anda dari berbagai layanan (AWS termasuk Amazon Macie) dan produk Jaringan Mitra () yang didukung. AWS APN Security Hub membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi di AWS lingkungan Anda.

Untuk informasi tentang penggunaan GuardDuty dan Security Hub bersama-sama, lihat [Integrasi dengan GuardDuty AWS Security Hub](#). Untuk mempelajari selengkapnya tentang Security Hub, lihat [Panduan Pengguna AWS Security Hub](#).

- **Detektif Amazon** — Layanan ini membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat. Detective secara otomatis mengumpulkan data log dari sumber daya Anda. AWS Kemudian

menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien. Agregasi data Detective prebuilt, ringkasan, dan konteks membantu Anda menganalisis dan menentukan sifat dan tingkat potensi masalah keamanan.

Untuk informasi tentang penggunaan GuardDuty dan Detektif bersama-sama, lihat [Integrasi GuardDuty dengan Amazon Detective](#) Untuk mempelajari lebih lanjut tentang Detektif, lihat Panduan Pengguna [Detektif](#) Amazon.

- Amazon EventBridge — Layanan ini membantu Anda menerima notifikasi dan menanggapi temuan GuardDuty keamanan dalam waktu dekat. GuardDuty menciptakan peristiwa ketika ada perubahan dalam temuan. Anda dapat memilih seberapa sering Anda ingin menerima notifikasi dari EventBridge. Untuk informasi selengkapnya, lihat [Apa itu Amazon EventBridge](#) di Panduan EventBridge Pengguna Amazon.

## PCIDSSKepatuhan

GuardDuty mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh pedagang atau penyedia layanan, dan telah divalidasi sebagai sesuai dengan Industri Kartu Pembayaran (PCI) Standar Keamanan Data (DSS). Untuk informasi selengkapnya PCIDSS, termasuk cara meminta salinan Paket AWS PCI Kepatuhan, lihat [PCIDSSLevel 1](#).

Untuk informasi selengkapnya, lihat [Pengujian pihak ketiga baru membandingkan Amazon GuardDuty dengan sistem deteksi intrusi jaringan di Blog Keamanan.AWS](#)

## Harga di GuardDuty

AWS Tingkat Gratis membantu Anda menjelajahi dan mencoba AWS layanan secara gratis hingga batas yang ditentukan untuk setiap layanan. Ada tiga kategori — 12 bulan gratis, selalu gratis, dan uji coba gratis jangka pendek. Amazon GuardDuty termasuk dalam kategori uji coba gratis jangka pendek dan menawarkan uji coba gratis 30 hari. Ketika Anda terus menggunakan GuardDuty setelah uji coba gratis ini berakhir, Anda mulai mengeluarkan biaya berdasarkan cara Anda menggunakan layanan ini.

Pemindaian malware sesuai permintaan (di bawah Perlindungan Malware untuk EC2) dan Perlindungan Malware untuk S3 tidak termasuk dalam kategori uji coba gratis jangka pendek GuardDuty 30 hari. Perlindungan Malware untuk S3 termasuk dalam kategori gratis 12 bulan AWS Tingkat Gratis sedangkan pemindaian malware On-Demand mengikuti model pay-as-you-use biaya.

Tidak ada uji coba gratis 30 hari atau model biaya Tingkat Gratis 12 bulan dengan pemindaian malware sesuai permintaan. Untuk informasi lebih lanjut, lihat [GuardDuty harga](#).

## Menggunakan uji GuardDuty coba gratis 30 hari

Saat menggunakan GuardDuty untuk pertama kalinya Wilayah AWS, Anda Akun AWS secara otomatis terdaftar dalam uji coba gratis 30 hari di Wilayah tersebut. Beberapa paket perlindungan juga akan diaktifkan secara otomatis dan termasuk dalam uji coba gratis 30 hari. Karena GuardDuty merupakan layanan regional, ketika Anda mengaktifkannya untuk pertama kalinya di Wilayah yang berbeda, akun Anda akan mendapatkan uji coba gratis 30 hari GuardDuty dan beberapa paket perlindungan yang didukung di Wilayah tersebut.

Saat bekerja dengan beberapa akun dalam suatu GuardDuty organisasi, setiap akun mendapatkan uji coba gratis 30 hari sendiri untuk digunakan GuardDuty dan paket perlindungan.

Tabel berikut menunjukkan paket perlindungan mana yang diaktifkan secara otomatis saat Anda mengaktifkan GuardDuty untuk pertama kalinya.

| Rencana perlindungan   | Termasuk dalam uji GuardDuty coba gratis 30 hari | Memiliki uji coba gratis 30 hari sendiri <sup>1</sup> |
|--|--|---|
| <a href="#">EKSPerindungan</a>   | Ya   | Ya  |
| <a href="#">Perlindungan Lambda</a>  | Ya   | Ya  |
| <a href="#">Perlindungan Malware untuk EC2 – GuardDuty-pemindaian malware yang dimulai</a> | Ya   | Ya  |
| <a href="#">Perlindungan Malware untuk EC2 – Pemindaian malware sesuai permintaan</a>      | Tidak  | Tidak   |
| <a href="#">GuardDuty Perlindungan Malware untuk S3</a>                                    | Tidak  | Tidak   |



| Rencana perlindungan               | Termasuk dalam uji GuardDuty coba gratis 30 hari | Memiliki uji coba gratis 30 hari sendiri <sup>1</sup> |
|------------------------------------|--|---|
| <a href="#">RDSPerlindungan</a>    | Ya   | Ya  |
| <a href="#">Pemantauan Runtime</a> | Tidak  | Ya  |
| <a href="#">Perlindungan S3</a>    | Ya   | Ya  |

<sup>1</sup> Setiap paket perlindungan memiliki uji coba gratis sendiri. Misalnya, ketika Anda mengaktifkan paket perlindungan setelah uji coba gratis GuardDuty 30 hari berakhir untuk akun Anda dan rencana perlindungan baru dirilis, Anda dapat mengaktifkan paket perlindungan ini dengan uji coba gratisnya sendiri. Untuk informasi selengkapnya tentang uji coba gratis untuk paket perlindungan, lihat dokumen yang terkait dengan setiap paket perlindungan.

Lihat perkiraan biaya penggunaan selama uji coba gratis — Selama uji coba gratis 30 hari GuardDuty dan kemungkinan rencana perlindungan, GuardDuty berikan perkiraan biaya penggunaan untuk akun Anda. Jika Anda adalah akun GuardDuty administrator yang didelegasikan, Anda dapat melihat total perkiraan biaya penggunaan dan rincian tingkat akun untuk semua akun anggota yang telah diaktifkan. GuardDuty Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty](#).

Biaya penggunaan setelah uji coba gratis berakhir — Saat Anda terus menggunakan GuardDuty atau paket perlindungannya setelah uji coba gratis berakhir, Anda akan mulai mengeluarkan biaya penggunaan terkait. Untuk melihat tagihan Anda, navigasikan ke Cost Explorer di <https://console.aws.amazon.com/billing/konsol>. Untuk informasi selengkapnya tentang penagihan AWS akun, lihat [Panduan AWS Billing Pengguna](#).

## Menggunakan Perlindungan Malware untuk S3 dengan Tingkat Gratis 12 bulan

Perlindungan Malware untuk S3 menggunakan paket Tingkat Gratis yang terkait dengan Anda Akun AWS yang baru, memiliki tingkat gratis yang berkelanjutan, atau memiliki tingkat gratis 12 bulan yang kedaluwarsa. Untuk informasi selengkapnya, lihat [Harga untuk Perlindungan Malware untuk S3](#).

# Mengakses GuardDuty

Anda dapat menggunakan GuardDuty salah satu cara berikut:

## GuardDuty konsol

<https://console.aws.amazon.com/guardduty/>

Konsol adalah antarmuka berbasis browser untuk mengakses dan menggunakan GuardDuty. GuardDuty Konsol menyediakan akses ke GuardDuty akun, data, dan sumber daya Anda.

## AWS alat baris perintah

Dengan alat baris AWS perintah, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan GuardDuty tugas dan AWS tugas. Alat baris perintah berguna jika Anda ingin membangun skrip yang melakukan tugas.

Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#). Untuk melihat AWS CLI perintah yang tersedia GuardDuty, lihat [referensi CLI perintah](#).

## GuardDuty HTTPS API

Anda dapat mengakses GuardDuty dan AWS secara terprogram dengan menggunakan GuardDuty HTTPS API, yang memungkinkan Anda mengeluarkan HTTPS permintaan langsung ke layanan. Untuk informasi selengkapnya, lihat [GuardDuty API Referensi](#).

## AWS SDKs

AWS menyediakan kit pengembangan perangkat lunak (SDKs) yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Python, Ruby, .NET, iOS, Android, dan banyak lagi). SDKs menyediakan cara mudah untuk membuat akses terprogram ke GuardDuty. Untuk informasi tentang AWS SDKs, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

# Konsep dan terminologi

Saat Anda memulai dengan Amazon GuardDuty, Anda bisa mendapatkan keuntungan dari mempelajari konsep-konsep utamanya.

## Akun

Akun Amazon Web Services (AWS) standar yang berisi AWS sumber daya Anda. Anda dapat masuk AWS dengan akun Anda dan mengaktifkan GuardDuty.

Anda juga dapat mengundang akun lain untuk mengaktifkan GuardDuty dan menjadi terkait dengan AWS akun Anda di GuardDuty. Jika undangan Anda diterima, akun Anda ditetapkan sebagai akun administrator, dan GuardDuty akun yang ditambahkan menjadi akun anggota Anda. Anda kemudian dapat melihat dan mengelola GuardDuty temuan akun tersebut atas nama mereka.

Pengguna akun administrator dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan untuk akun mereka sendiri dan semua akun anggota mereka. Anda dapat memiliki hingga 10.000 akun anggota GuardDuty.

Pengguna akun anggota dapat mengonfigurasi GuardDuty serta melihat dan mengelola GuardDuty temuan di akun mereka (baik melalui konsol GuardDuty manajemen atau GuardDuty API). Pengguna akun anggota tidak dapat melihat atau mengelola temuan di akun anggota lain.

Anda tidak dapat menjadi akun GuardDuty administrator dan akun anggota secara bersamaan. Anda hanya dapat menerima satu undangan keanggotaan. Menerima undangan keanggotaan bersifat opsional.

Untuk informasi selengkapnya, lihat [Mengelola banyak akun di Amazon GuardDuty](#).

## Detektor

Amazon GuardDuty adalah layanan regional. Saat Anda mengaktifkan GuardDuty secara spesifik Wilayah AWS, Anda Akun AWS akan dikaitkan dengan ID detektor. ID alfanumerik 32 karakter ini unik untuk akun Anda di Wilayah tersebut. Misalnya, ketika Anda mengaktifkan GuardDuty akun yang sama di Wilayah yang berbeda, akun Anda akan dikaitkan dengan ID detektor yang berbeda. Format a detectorId adalah12abc34d567e8fa901bc2d34e56789f0.

Semua GuardDuty temuan, akun, dan tindakan tentang mengelola temuan dan GuardDuty layanan menggunakan ID detektor untuk menjalankan API operasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

**Note**

Di lingkungan multi-akun, semua temuan untuk akun anggota digulung ke detektor akun administrator.

Beberapa GuardDuty fungsi dikonfigurasi melalui detektor, seperti mengonfigurasi frekuensi pemberitahuan CloudWatch Acara, dan mengaktifkan atau menonaktifkan rencana perlindungan opsional untuk diproses. GuardDuty

Menggunakan Perlindungan Malware untuk S3 di dalam GuardDuty

Saat Anda mengaktifkan Perlindungan Malware untuk S3 di akun yang GuardDuty diaktifkan, Perlindungan Malware untuk tindakan S3 seperti mengaktifkan, mengedit, dan menonaktifkan sumber daya yang dilindungi tidak terkait dengan ID detektor.

Jika Anda tidak mengaktifkan GuardDuty dan memilih opsi deteksi ancaman Perlindungan Malware untuk S3, tidak ada ID detektor yang dibuat untuk akun Anda.

## Sumber data dasar

Asal atau lokasi satu set data. Untuk mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. GuardDuty menganalisis dan memproses data dari log AWS CloudTrail peristiwa, peristiwa AWS CloudTrail manajemen, peristiwa AWS CloudTrail data untuk S3, log VPC aliran, DNS log, lihat. [GuardDuty sumber data dasar](#)

## Fitur

Objek fitur yang dikonfigurasi untuk paket GuardDuty perlindungan Anda membantu mendeteksi aktivitas yang tidak sah atau tidak terduga di AWS lingkungan Anda. Setiap rencana GuardDuty perlindungan mengkonfigurasi objek fitur yang sesuai untuk menganalisis dan memproses data. Beberapa objek fitur termasuk log EKS audit, pemantauan aktivitas RDS login, log aktivitas jaringan Lambda, dan EBS volume. Untuk informasi selengkapnya, lihat [Fitur aktivasi di GuardDuty](#).

## Menemukan

Masalah keamanan potensial ditemukan oleh GuardDuty. Untuk informasi selengkapnya, lihat [Memahami GuardDuty temuan Amazon](#).

Temuan ditampilkan di GuardDuty konsol dan berisi deskripsi rinci tentang masalah keamanan. Anda juga dapat mengambil temuan yang dihasilkan dengan memanggil [GetFindings](#) dan [ListFindings](#) API operasi.

Anda juga dapat melihat GuardDuty temuan Anda melalui CloudWatch acara Amazon. GuardDuty mengirimkan temuan ke Amazon CloudWatch melalui HTTPS protokol. Untuk informasi selengkapnya, lihat [Membuat tanggapan khusus terhadap GuardDuty temuan dengan Amazon CloudWatch Events](#).

## IAM peran

Ini adalah IAM peran dengan izin yang diperlukan untuk memindai objek S3. Saat menandai objek yang dipindai diaktifkan, IAM PassRole izin membantu GuardDuty menambahkan tag ke objek yang dipindai.

## Sumber daya paket Perlindungan Malware

Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket, GuardDuty buat Perlindungan Malware untuk sumber daya EC2 paket. Sumber daya ini dikaitkan dengan Perlindungan Malware untuk ID EC2 paket, pengenal unik untuk bucket Anda yang dilindungi. Gunakan sumber daya paket Perlindungan Malware untuk melakukan API operasi pada sumber daya yang dilindungi.

## Ember yang dilindungi (sumber daya terlindungi)

Bucket Amazon S3 dianggap dilindungi saat Anda mengaktifkan Perlindungan Malware untuk S3 untuk bucket ini dan status perlindungannya berubah menjadi Aktif.

GuardDuty hanya mendukung bucket S3 sebagai sumber daya yang dilindungi.

## Status perlindungan

Status yang terkait dengan sumber daya paket Perlindungan Malware Anda. Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket, status ini menunjukkan apakah bucket sudah diatur dengan benar atau tidak.

## Awalan objek S3

Di bucket Amazon Simple Storage Service (Amazon S3), Anda dapat menggunakan awalan untuk mengatur penyimpanan Anda. Awalan adalah pengelompokan logis objek dalam ember S3. Untuk informasi selengkapnya, lihat [Mengatur dan mencantumkan objek](#) di Panduan Pengguna Amazon S3.

## Opsi pemindaian

Saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, Anda dapat menentukan EC2 instans Amazon dan volume Amazon Elastic Block Store (EBS) yang akan dipindai atau dilewati. Fitur ini memungkinkan Anda menambahkan tag yang ada yang terkait dengan EC2 instance dan EBS volume Anda ke daftar tag inklusi atau daftar tag pengecualian. Sumber daya yang terkait dengan tag yang Anda tambahkan ke daftar tag inklusi, dipindai untuk malware, dan yang ditambahkan ke daftar tag pengecualian tidak dipindai. Untuk informasi selengkapnya, lihat [Opsi pindai dengan tag yang ditentukan pengguna](#).

## Retensi snapshot

Ketika Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini menyediakan opsi untuk menyimpan snapshot EBS volume Anda di AWS akun Anda. GuardDuty menghasilkan EBS volume replika berdasarkan snapshot volume Anda EBS. Anda dapat menyimpan snapshot EBS volume Anda hanya jika Perlindungan Malware untuk EC2 pemindaian mendeteksi malware dalam volume replika EBS. Jika tidak ada malware yang terdeteksi dalam EBS volume replika, GuardDuty secara otomatis menghapus snapshot EBS volume Anda, terlepas dari pengaturan retensi snapshot. Untuk informasi selengkapnya, lihat [Retensi snapshot](#).

## Aturan penindasan

Aturan penekanan memungkinkan Anda membuat kombinasi atribut yang sangat spesifik untuk menekan temuan. Misalnya, Anda dapat menentukan aturan melalui GuardDuty filter untuk mengarsipkan otomatis hanya Recon:EC2/Portscan dari instance tersebut dalam spesifik VPC, menjalankan spesifik AMI, atau dengan tag tertentu EC2. Aturan ini akan mengakibatkan temuan pemindaian port diarsipkan secara otomatis dari instans yang memenuhi kriteria. Namun, masih memungkinkan peringatan jika GuardDuty mendeteksi instans yang melakukan aktivitas berbahaya lainnya, seperti penambangan mata uang kripto.

Aturan penindasan yang ditentukan dalam akun GuardDuty administrator berlaku untuk akun GuardDuty anggota. GuardDuty akun anggota tidak dapat mengubah aturan penindasan.

Dengan aturan penindasan, GuardDuty masih menghasilkan semua temuan. Aturan penekanan memberikan penekanan pada temuan sekaligus mempertahankan riwayat yang lengkap dan tidak berubah dari semua aktivitas.

Biasanya aturan penindasan digunakan untuk menyembunyikan temuan yang telah Anda tentukan sebagai positif palsu untuk lingkungan Anda, dan mengurangi kebisingan dari temuan bernilai rendah sehingga Anda dapat fokus pada ancaman yang lebih besar. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

## Daftar IP terpercaya

Daftar alamat IP terpercaya untuk komunikasi yang sangat aman dengan AWS lingkungan Anda. GuardDuty tidak menghasilkan temuan berdasarkan daftar IP terpercaya. Untuk informasi selengkapnya, lihat [Bekerja dengan daftar IP terpercaya dan daftar ancaman](#).

## Daftar IP ancaman

Daftar alamat IP berbahaya yang diketahui. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan daftar ancaman ini. Untuk informasi selengkapnya, lihat [Bekerja dengan daftar IP terpercaya dan daftar ancaman](#).

# Memulai dengan GuardDuty

Tutorial ini memberikan pengantar langsung ke GuardDuty Persyaratan minimum untuk mengaktifkan GuardDuty sebagai akun mandiri atau sebagai GuardDuty administrator AWS Organizations tercakup dalam Langkah 1. Langkah 2 hingga 5 mencakup menggunakan fitur tambahan yang direkomendasikan oleh GuardDuty untuk mendapatkan hasil maksimal dari temuan Anda.

## Topik

- [Sebelum Anda mulai](#)
- [Langkah 1: Aktifkan Amazon GuardDuty](#)
- [Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar](#)
- [Langkah 3: Konfigurasi GuardDuty temuan ekspor ke bucket Amazon S3](#)
- [Langkah 4: Siapkan GuardDuty pencarian peringatan melalui SNS](#)
- [Langkah selanjutnya](#)

## Sebelum Anda mulai

GuardDuty adalah layanan deteksi ancaman yang memantau [GuardDuty sumber data dasar](#) seperti log AWS CloudTrail peristiwa, peristiwa AWS CloudTrail manajemen, Amazon VPC Flow Logs, dan DNS log. GuardDuty juga menganalisis fitur yang terkait dengan jenis perlingkungannya hanya jika Anda mengaktifkannya secara terpisah. [Fitur](#) termasuk log audit Kubernetes, aktivitas RDS login, log S3, EBS volume, pemantauan Runtime, dan log aktivitas jaringan Lambda. Menggunakan sumber dan fitur data ini (jika diaktifkan), GuardDuty menghasilkan temuan keamanan untuk akun Anda.

Setelah Anda mengaktifkan GuardDuty, itu mulai memantau lingkungan Anda. Anda dapat GuardDuty menonaktifkan akun apa pun di Wilayah mana pun, kapan saja. Ini akan berhenti GuardDuty dari memproses sumber data dasar dan fitur apa pun yang diaktifkan secara terpisah.

Anda tidak perlu mengaktifkan salah satu [GuardDuty sumber data dasar](#) secara eksplisit. Amazon GuardDuty menarik aliran data independen langsung dari layanan tersebut. Untuk GuardDuty akun baru, semua jenis perlindungan yang tersedia yang didukung dalam akun Wilayah AWS diaktifkan dan disertakan dalam periode uji coba gratis 30 hari secara default. Anda dapat memilih keluar dari salah satu atau semuanya. Jika Anda adalah GuardDuty pelanggan yang sudah ada, Anda dapat memilih untuk mengaktifkan salah satu atau semua paket perlindungan yang tersedia di



Anda Wilayah AWS. Untuk informasi selengkapnya, lihat [Fitur](#) yang terkait dengan setiap jenis perlindungan GuardDuty.

Saat mengaktifkan GuardDuty, pertimbangkan item berikut:

- GuardDuty adalah layanan Regional, artinya prosedur konfigurasi apa pun yang Anda ikuti di halaman ini harus diulang di setiap Wilayah yang ingin Anda pantau GuardDuty.

Kami sangat menyarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail acara untuk AWS layanan global seperti IAM. Jika tidak GuardDuty diaktifkan di semua Wilayah yang didukung, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang. Untuk daftar lengkap Wilayah yang GuardDuty tersedia, lihat [Wilayah dan titik akhir](#).

- Setiap pengguna dengan hak administrator di AWS akun dapat mengaktifkan GuardDuty, namun, mengikuti praktik keamanan terbaik dengan hak istimewa terkecil, disarankan agar Anda membuat IAM peran, pengguna, atau grup untuk dikelola GuardDuty secara khusus. Untuk informasi tentang izin yang diperlukan untuk mengaktifkan GuardDuty lihat [Izin diperlukan untuk mengaktifkan GuardDuty](#).
- Ketika Anda mengaktifkan GuardDuty untuk pertama kalinya di salah satu Wilayah AWS, secara default, itu juga memungkinkan semua jenis perlindungan yang tersedia yang didukung di Wilayah tersebut, termasuk Perlindungan Malware untuk EC2. GuardDuty membuat peran terkait layanan untuk akun Anda yang dipanggil `AWSServiceRoleForAmazonGuardDuty` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan GuardDuty untuk mengkonsumsi dan menganalisis peristiwa secara langsung dari [GuardDuty sumber data dasar](#) untuk menghasilkan temuan keamanan. Perlindungan Malware untuk EC2 membuat peran terkait layanan lain untuk akun Anda yang dipanggil `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Peran ini mencakup izin dan kebijakan kepercayaan yang memungkinkan Perlindungan Malware untuk EC2 melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda. GuardDuty Ini memungkinkan GuardDuty untuk membuat snapshot EBS volume di akun Anda, dan berbagi snapshot itu dengan akun GuardDuty layanan. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan untuk GuardDuty](#). Untuk informasi selengkapnya tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan](#).
- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di Wilayah mana pun, AWS akun Anda secara otomatis terdaftar dalam uji coba GuardDuty gratis 30 hari untuk Wilayah tersebut.

## [Memulai: Mengaktifkan Amazon GuardDuty untuk lingkungan mandiri atau multi-akun](#)

### Langkah 1: Aktifkan Amazon GuardDuty

Langkah pertama yang harus digunakan GuardDuty adalah mengaktifkannya di akun Anda. Setelah diaktifkan, GuardDuty akan segera mulai memantau ancaman keamanan di Wilayah saat ini.

Jika Anda ingin mengelola GuardDuty temuan untuk akun lain dalam organisasi Anda sebagai GuardDuty administrator, Anda harus menambahkan akun anggota dan GuardDuty mengaktifkannya juga.

#### Note

Jika Anda ingin mengaktifkan Perlindungan GuardDuty Malware untuk S3 tanpa mengaktifkan GuardDuty, maka untuk langkah-langkahnya, lihat. [GuardDuty Perlindungan Malware untuk S3](#)

#### Standalone account environment

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>
2. Pilih opsi Amazon GuardDuty - Semua fitur.
3. Pilih Mulai.
4. Pada GuardDuty halaman Selamat Datang di, lihat persyaratan layanan. Pilih Aktifkan GuardDuty.

#### Multi-account environment

#### Important

Sebagai prasyarat untuk proses ini, Anda harus berada di organisasi yang sama dengan semua akun yang ingin Anda kelola, dan memiliki akses ke akun AWS Organizations manajemen untuk mendelegasikan administrator di dalam organisasi Anda. GuardDuty Izin tambahan mungkin diperlukan untuk mendelegasikan administrator, untuk info


selengkapnya, lihat [Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty](#).

Untuk menunjuk akun administrator yang didelegasikan GuardDuty

1. Buka AWS Organizations konsol di <https://console.aws.amazon.com/organizations/>, menggunakan akun manajemen.
2. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Apakah GuardDuty sudah diaktifkan di akun Anda?

- Jika belum GuardDuty diaktifkan, Anda dapat memilih Memulai dan kemudian menunjuk administrator yang GuardDuty didelegasikan pada halaman Selamat Datang GuardDuty di.
  - Jika GuardDuty diaktifkan, Anda dapat menunjuk administrator yang GuardDuty didelegasikan pada halaman Pengaturan.
3. Masukkan ID AWS akun dua belas digit dari akun yang ingin Anda tetapkan sebagai administrator yang GuardDuty didelegasikan untuk organisasi dan pilih Delegasi.

 Note

Jika belum GuardDuty diaktifkan, menunjuk administrator yang didelegasikan akan mengaktifkan GuardDuty akun tersebut di Wilayah Anda saat ini.


Untuk menambahkan akun anggota

Prosedur ini mencakup penambahan akun anggota ke akun administrator yang GuardDuty didelegasikan melalui AWS Organizations. Ada juga opsi untuk menambahkan anggota melalui undangan. Untuk mempelajari lebih lanjut tentang kedua metode untuk mengasosiasikan anggota GuardDuty, lihat [Mengelola banyak akun di Amazon GuardDuty](#).

1. Masuk ke akun administrator yang didelegasikan
2. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
3. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.

Tabel akun menampilkan semua akun dalam organisasi.

4. Pilih akun yang ingin Anda tambahkan sebagai anggota dengan mencentang kotak di samping ID akun. Kemudian dari menu Tindakan, pilih Tambah anggota.

 Tip

Anda dapat mengotomatiskan penambahan akun baru sebagai anggota dengan mengaktifkan fitur Aktifkan otomatis; namun, ini hanya berlaku untuk akun yang bergabung dengan organisasi Anda setelah fitur diaktifkan.

## Langkah 2: Menghasilkan temuan sampel dan menjelajahi operasi dasar

Ketika GuardDuty menemukan masalah keamanan, itu menghasilkan temuan. GuardDuty Temuan adalah kumpulan data yang berisi detail yang berkaitan dengan masalah keamanan unik itu. Detail temuan dapat digunakan untuk membantu Anda menyelidiki masalah tersebut.

GuardDuty mendukung menghasilkan temuan sampel dengan nilai placeholder, yang dapat digunakan untuk menguji GuardDuty fungsionalitas dan membiasakan diri dengan temuan sebelum perlu menanggapi masalah keamanan nyata yang ditemukan oleh GuardDuty. Ikuti panduan di bawah ini untuk menghasilkan temuan sampel untuk setiap jenis temuan yang tersedia di GuardDuty, untuk cara tambahan untuk menghasilkan temuan sampel, termasuk menghasilkan peristiwa keamanan simulasi dalam akun Anda, lihat [Sampel temuan](#).

Untuk membuat dan mengeksplorasi temuan sampel

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.
3. Di panel navigasi, pilih Ringkasan untuk melihat wawasan tentang temuan yang dihasilkan di lingkungan Anda AWS . Untuk informasi selengkapnya tentang komponen dasbor Ringkasan, lihat [Dasbor ringkasan](#).
4. Di panel navigasi, pilih Temuan. Temuan sampel ditampilkan pada halaman Temuan saat ini dengan awalan [SAMPLE].
5. Pilih temuan dari daftar untuk menampilkan detail temuan.
  - Anda dapat meninjau bidang informasi yang berbeda yang tersedia di panel detail temuan. Berbagai jenis temuan dapat memiliki bidang yang berbeda. Untuk informasi selengkapnya

tentang bidang yang tersedia di semua jenis pencarian, lihat [Detail temuan](#). Dari panel detail, Anda dapat mengambil tindakan berikut:

- Pilih ID pencarian di bagian atas panel untuk membuka JSON detail lengkap temuan tersebut. JSONFile lengkap juga dapat diunduh dari panel ini. JSON ini berisi beberapa informasi tambahan yang tidak termasuk dalam tampilan konsol dan merupakan format yang dapat dicerna oleh alat dan layanan lain.
- Lihat bagian Sumber daya yang terpengaruh. Dalam temuan nyata, informasi di sini akan membantu Anda mengidentifikasi sumber daya di akun Anda yang harus diselidiki dan akan menyertakan tautan ke sumber daya yang sesuai AWS Management Console untuk ditindaklanjuti.
- Pilih ikon kaca pembesar dengan + atau - untuk membuat filter inklusif atau eksklusif untuk detail tersebut. Untuk informasi selengkapnya tentang menemukan filter, lihat [Memfilter temuan](#).

## 6. Arsipkan semua temuan sampel Anda

- a. Pilih semua temuan dengan memilih kotak centang di bagian atas daftar.
- b. Hapus pilihan temuan apa pun yang ingin Anda simpan.
- c. Pilih menu Tindakan, lalu pilih Arsip untuk menyembunyikan temuan sampel.

### Note

Untuk melihat temuan yang diarsipkan, pilih Saat ini, lalu pilih Diarsipkan untuk beralih tampilan temuan.


## Langkah 3: Konfigurasi GuardDuty temuan ekspor ke bucket Amazon S3

GuardDuty merekomendasikan konfigurasi pengaturan untuk mengekspor temuan karena memungkinkan Anda untuk mengekspor temuan Anda ke bucket S3 untuk penyimpanan tidak terbatas di luar periode retensi 90 hari. GuardDuty ini memungkinkan Anda untuk menyimpan catatan temuan atau melacak masalah dalam AWS lingkungan Anda dari waktu ke waktu. Proses yang diuraikan di sini memandu Anda melalui pengaturan bucket S3 baru dan membuat KMS kunci baru untuk mengenkripsi temuan dari dalam konsol. Untuk informasi selengkapnya tentang hal ini,

termasuk cara menggunakan bucket atau bucket yang sudah ada di akun lain, lihat [Mengekspor temuan](#).

Untuk mengonfigurasi opsi temuan ekspor S3

1. Untuk mengenkripsi temuan, Anda memerlukan KMS kunci dengan kebijakan yang memungkinkan GuardDuty untuk menggunakan kunci tersebut untuk enkripsi. Langkah-langkah berikut akan membantu Anda membuat KMS kunci baru. Jika Anda menggunakan KMS kunci dari akun lain, Anda perlu menerapkan kebijakan kunci dengan masuk ke Akun AWS yang memiliki kunci tersebut. Wilayah KMS kunci dan bucket S3 Anda harus sama. Namun, Anda dapat menggunakan bucket dan key pair yang sama ini untuk setiap Wilayah dari tempat Anda ingin mengekspor temuan.
  - a. Buka AWS KMS konsol di <https://console.aws.amazon.com/kms>.
  - b. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
  - c. Di panel navigasi, pilih Kunci yang dikelola pelanggan.
  - d. Pilih Buat kunci.
  - e. Pilih Simetris di bawah Jenis kunci, lalu pilih Berikutnya.

 Note

Untuk langkah-langkah mendetail tentang membuat KMS kunci, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang.

- f. Berikan Alias untuk kunci Anda, lalu pilih Berikutnya.
- g. Pilih Berikutnya, dan sekali lagi pilih Berikutnya untuk menerima administrasi default dan izin penggunaan.
- h. Setelah Anda meninjau konfigurasi, pilih Selesai untuk membuat kunci.
- i. Pada halaman kunci yang dikelola Pelanggan, pilih alias kunci Anda.
- j. Di tab Kebijakan kunci, pilih Beralih ke tampilan kebijakan.
- k. Pilih Edit dan tambahkan kebijakan kunci berikut ke KMS kunci Anda, berikan GuardDuty akses ke kunci Anda. Pernyataan ini memungkinkan GuardDuty untuk hanya menggunakan kunci yang Anda tambahkan kebijakan ini. Saat mengedit kebijakan kunci, pastikan JSON sintaksnya valid. Jika Anda menambahkan pernyataan sebelum pernyataan akhir, Anda harus menambahkan koma setelah braket penutup.

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "111122223333",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
    }
  }
}
```

Ganti *Region1* dengan Wilayah KMS kunci Anda. Ganti *444455556666* dengan Akun AWS yang memiliki KMS kuncinya. Ganti *KMSKeyId* dengan ID kunci KMS kunci yang Anda pilih untuk enkripsi. Untuk mengidentifikasi semua nilai ini — Wilayah Akun AWS, dan ID kunci, lihat KMS kunci Anda. ARN Untuk menemukan kunciARN, lihat [Menemukan ID kunci dan ARN](#).

Demikian pula, ganti *111122223333* dengan Akun AWS GuardDuty akun. Ganti *Region2* dengan Wilayah GuardDuty akun. Ganti *SourceDetectorID* dengan ID detektor GuardDuty akun untuk *Region2*.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

- I. Pilih Simpan.
2. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
3. Pada panel navigasi, silakan pilih Pengaturan.
4. Di bawah opsi ekspor temuan, pilih Konfigurasi sekarang.
5. Pilih ember baru. Berikan nama unik untuk bucket S3 Anda.
6. (Opsional) Anda dapat menguji pengaturan ekspor baru Anda dengan menghasilkan temuan sampel. Pada panel navigasi, silakan pilih Pengaturan.

7. Di bawah bagian Temuan sampel, pilih Hasilkan temuan sampel. Temuan sampel baru akan muncul sebagai entri dalam ember S3 yang dibuat GuardDuty hingga lima menit.

## Langkah 4: Siapkan GuardDuty pencarian peringatan melalui SNS

GuardDuty terintegrasi dengan Amazon EventBridge, yang dapat digunakan untuk mengirim data temuan ke aplikasi dan layanan lain untuk diproses. Dengan EventBridge Anda dapat menggunakan GuardDuty temuan untuk memulai respons otomatis terhadap temuan Anda dengan menghubungkan peristiwa pencarian ke target seperti AWS Lambda fungsi, otomatisasi Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) dan banyak lagi.

Dalam contoh ini Anda akan membuat SNS topik untuk menjadi target EventBridge aturan, lalu Anda akan menggunakan EventBridge untuk membuat aturan yang menangkap data temuan dari GuardDuty. Aturan yang dihasilkan akan meneruskan detail temuan ke alamat email. Untuk mempelajari bagaimana Anda dapat mengirim temuan ke Slack atau Amazon Chime, dan juga memodifikasi jenis peringatan temuan yang dikirim, lihat. [Mengatur topik Amazon SNS dan titik akhir](#)

Untuk membuat SNS topik untuk peringatan temuan Anda

1. Buka SNS konsol Amazon di <https://console.aws.amazon.com/sns/v3/home>.
2. Di panel navigasi, pilih Pengguna.
3. Pilih Buat Topik.
4. Untuk Jenis, pilih Standar.
5. Untuk Nama, masukkan **GuardDuty**.
6. Pilih Buat Topik. Detail topik untuk topik baru Anda akan terbuka.
7. Di bagian Subscriptions (Berlangganan), pilih Create subscription (Buat langganan).
8. Untuk Protokol, pilih Email.
9. Untuk Endpoint, masukkan alamat email untuk mengirim notifikasi.
10. Pilih Buat langganan.

Setelah Anda membuat langganan, Anda harus mengonfirmasi langganan melalui email.

11. Untuk memeriksa pesan langganan, buka kotak masuk email Anda, dan di pesan berlangganan, pilih Konfirmasi langganan.



**Note**

Untuk memeriksa status konfirmasi email, buka SNS konsol dan pilih Langganan.

Untuk membuat EventBridge aturan untuk menangkap GuardDuty temuan dan memformatnya

1. Buka EventBridge konsol di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi untuk aturan.

Aturan tidak boleh memiliki nama yang sama dengan aturan lain di Wilayah yang sama dan di bus peristiwa yang sama.

5. Untuk Bus peristiwa, pilih default.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk sumber acara, pilih AWS acara.
9. Untuk pola Acara, pilih Formulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk Layanan AWS , pilih GuardDuty.
12. Untuk Jenis Acara, pilih GuardDutyMenemukan.
13. Pilih Berikutnya.
14. Untuk Jenis target, pilih Layanan AWS .
15. Untuk Pilih target, pilih SNSStopik, dan untuk Topik, pilih nama SNS topik yang Anda buat sebelumnya.
16. Di bagian Pengaturan tambahan, untuk Konfigurasi input target, pilih Transformator input.

Menambahkan transformator input memformat data JSON temuan yang dikirim dari GuardDuty ke dalam pesan yang dapat dibaca manusia.

17. Pilih Konfigurasi transformator input.
18. Di bagian Transformator input target, untuk jalur Input, tempel kode berikut:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Untuk memformat email, untuk Template, tempel kode berikut dan pastikan untuk mengganti teks berwarna merah dengan nilai yang sesuai dengan Wilayah Anda:

```
"You have a severity severity GuardDuty finding type Finding_Type in
the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Pilih Konfirmasi.
21. Pilih Berikutnya.
22. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat [EventBridge tag Amazon](#) di Panduan EventBridge Pengguna Amazon.
23. Pilih Berikutnya.
24. Tinjau detail aturan dan pilih Buat aturan.
25. (Opsional) Uji aturan baru Anda dengan menghasilkan temuan sampel dengan proses di Langkah 2. Anda akan menerima email untuk setiap temuan sampel yang dihasilkan.

## Langkah selanjutnya

Saat Anda terus menggunakan GuardDuty, Anda akan memahami jenis temuan yang relevan dengan lingkungan Anda. Setiap kali Anda menerima temuan baru, Anda dapat menemukan informasi, termasuk rekomendasi perbaikan tentang temuan itu, dengan memilih Pelajari lebih lanjut dari deskripsi temuan di panel rincian temuan, atau dengan mencari nama temuan di [Tipe temuan](#)

Fitur-fitur berikut akan membantu Anda menyetel GuardDuty sehingga dapat memberikan temuan yang paling relevan untuk AWS lingkungan Anda:

- Untuk mengurutkan temuan dengan mudah berdasarkan kriteria tertentu, seperti ID instans, ID akun, nama bucket S3, dan lainnya, Anda dapat membuat dan menyimpan filter di dalamnya GuardDuty. Untuk informasi selengkapnya, lihat [Memfilter temuan](#).
- Jika Anda menerima temuan untuk perilaku yang diharapkan di lingkungan Anda, Anda dapat secara otomatis mengarsipkan temuan berdasarkan kriteria yang Anda tentukan dengan [aturan penekanan](#).
- Untuk mencegah temuan dihasilkan dari subset tepercayaIPs, atau memiliki GuardDuty monitor IPs di luar lingkup pemantauan normalnya, Anda dapat menyiapkan [IP Tepercaya dan daftar ancaman](#).

## GuardDuty sumber data dasar

GuardDuty menggunakan sumber data dasar untuk mendeteksi komunikasi dengan domain berbahaya dan alamat IP yang diketahui, dan mengidentifikasi perilaku yang berpotensi anomali dan aktivitas yang tidak sah. Saat transit dari sumber-sumber ini ke GuardDuty, semua data log dienkripsi. GuardDuty mengekstrak berbagai bidang dari sumber log ini untuk profil dan deteksi anomali, dan kemudian membuang log ini.

Saat Anda mengaktifkan GuardDuty untuk pertama kalinya di suatu Wilayah, ada uji coba gratis 30 hari yang mencakup deteksi ancaman untuk semua sumber data dasar. Selama uji coba gratis ini, Anda dapat memantau perkiraan penggunaan bulanan yang dirinci oleh setiap sumber data dasar. Sebagai akun GuardDuty administrator yang didelegasikan, Anda dapat melihat perkiraan biaya penggunaan bulanan yang dirinci oleh setiap akun anggota milik organisasi Anda dan telah diaktifkan GuardDuty. Setelah uji coba 30 hari berakhir, Anda dapat menggunakan AWS Billing informasi tentang biaya penggunaan.

Tidak ada biaya tambahan saat GuardDuty mengakses peristiwa dan log dari sumber data dasar ini.

Setelah Anda mengaktifkan GuardDuty di Anda Akun AWS, secara otomatis mulai memantau sumber log yang dijelaskan di bagian berikut. Anda tidak perlu mengaktifkan hal lain GuardDuty untuk mulai menganalisis dan memproses sumber data ini untuk menghasilkan temuan keamanan terkait.

### Topik

- [AWS CloudTrail acara manajemen](#)
- [VPCLog Aliran](#)
- [Log kueri Route53 Resolver DNS](#)

## AWS CloudTrail acara manajemen

AWS CloudTrail memberi Anda riwayat AWS API panggilan untuk akun Anda, termasuk API panggilan yang dilakukan menggunakan AWS Management Console, alat baris perintah, dan AWS layanan tertentu. AWS SDKs CloudTrail juga membantu Anda mengidentifikasi pengguna dan akun mana yang dipanggil AWS APIs untuk layanan yang mendukung CloudTrail, alamat IP sumber dari mana panggilan dipanggil, dan waktu di mana panggilan dipanggil. Untuk informasi selengkapnya, lihat [Apa yang ada AWS CloudTrail](#) di Panduan AWS CloudTrail Pengguna.

GuardDuty Memantau peristiwa CloudTrail manajemen, juga dikenal sebagai peristiwa bidang kontrol. Peristiwa ini memberikan wawasan tentang operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda.

Berikut ini adalah contoh peristiwa CloudTrail manajemen yang GuardDuty memantau:

- Mengkonfigurasi keamanan (IAMAttachRolePolicyAPIoperasi)
- Mengkonfigurasi aturan untuk merutekan data (operasi Amazon EC2 CreateSubnetAPI)
- Menyiapkan logging (AWS CloudTrail CreateTrailAPIoperasi)

Ketika Anda mengaktifkan GuardDuty, itu mulai mengkonsumsi peristiwa CloudTrail manajemen langsung dari CloudTrail melalui aliran peristiwa independen dan duplikat dan menganalisis log CloudTrail peristiwa Anda.

GuardDuty tidak mengelola CloudTrail acara Anda atau memengaruhi CloudTrail konfigurasi yang ada. Demikian pula, CloudTrail konfigurasi Anda tidak memengaruhi cara GuardDuty mengkonsumsi dan memproses log peristiwa. Untuk mengelola akses dan retensi CloudTrail acara Anda, gunakan konsol CloudTrail layanan atau API. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#) di Panduan AWS CloudTrail Pengguna.

## Bagaimana GuardDuty menangani peristiwa AWS CloudTrail global

Untuk sebagian besar AWS layanan, CloudTrail acara dicatat di Wilayah AWS tempat mereka dibuat. Untuk layanan global seperti AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), CloudFront Amazon, dan Amazon Route 53 (Route 53), peristiwa hanya dihasilkan di Wilayah tempat kejadian tetapi memiliki signifikansi global.

Saat GuardDuty mengkonsumsi [peristiwa layanan CloudTrail Global](#) dengan nilai keamanan seperti konfigurasi jaringan atau izin pengguna, peristiwa tersebut akan mereplikasi peristiwa tersebut dan memprosesnya di setiap Wilayah yang telah Anda aktifkan. GuardDuty Perilaku ini membantu GuardDuty menjaga profil pengguna dan peran di setiap Wilayah, yang sangat penting untuk mendeteksi kejadian anomali.

Kami sangat menyarankan agar Anda mengaktifkan GuardDuty semua Wilayah AWS yang diaktifkan untuk Anda Akun AWS. Ini membantu GuardDuty menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang mungkin tidak Anda gunakan secara aktif.

## VPCLog Aliran

Fitur VPC Flow Logs Amazon VPC menangkap informasi tentang lalu lintas IP yang menuju dan dari antarmuka jaringan yang dilampirkan ke instans Amazon Elastic Compute Cloud (AmazonEC2) di lingkungan Anda. AWS

Ketika Anda mengaktifkan GuardDuty, itu segera mulai menganalisis log VPC aliran Anda dari EC2 instans Amazon dalam akun Anda. Ini mengkonsumsi peristiwa log VPC aliran langsung dari fitur VPC Flow Logs melalui aliran log aliran independen dan duplikat. Proses ini tidak memengaruhi konfigurasi log aliran apa pun yang ada.

### [Perlindungan Lambda](#)

Lambda Protection adalah peningkatan opsional untuk Amazon. GuardDuty Saat ini, Pemantauan Aktivitas Jaringan Lambda mencakup log aliran VPC Amazon dari semua fungsi Lambda untuk akun Anda, bahkan log yang tidak menggunakan jaringan. VPC Untuk melindungi fungsi Lambda Anda dari potensi ancaman keamanan, Anda perlu mengonfigurasi Perlindungan Lambda di akun Anda. GuardDuty Untuk informasi selengkapnya, lihat [Perlindungan Lambda](#).

### [GuardDuty Pemantauan Runtime](#)


Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari instance ini GuardDuty , Akun AWS Anda tidak akan membebankan biaya untuk analisis VPC log aliran dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

GuardDuty tidak mengelola log aliran Anda atau membuatnya dapat diakses di akun Anda. Untuk mengelola akses dan retensi log alur, Anda harus mengonfigurasi fitur VPC Flow Logs.

## Log kueri Route53 Resolver DNS

Jika Anda menggunakan AWS DNS resolver untuk EC2 instans Amazon Anda (setelan default), maka GuardDuty dapat mengakses dan memproses log kueri Route53 Resolver permintaan dan respons Anda melalui resolver internalDNS. AWS DNS Jika Anda menggunakan DNS resolver lain, seperti Open DNS atau GoogleDNS, atau jika Anda menyiapkan DNS resolver sendiri, maka GuardDuty tidak dapat mengakses dan memproses data dari sumber data ini.

Saat Anda mengaktifkan GuardDuty, itu segera mulai menganalisis log DNS kueri Route53 Resolver Anda dari aliran data independen. Aliran data ini terpisah dari data yang disediakan melalui fitur [pencatatan kueri Route 53 Resolver](#). Konfigurasi fitur ini tidak mempengaruhi GuardDuty analisis.

 Note

GuardDuty tidak mendukung DNS log pemantauan untuk EC2 instans Amazon yang diluncurkan AWS Outposts karena fitur pencatatan Amazon Route 53 Resolver kueri tidak tersedia di lingkungan tersebut.

## Fitur aktivasi di GuardDuty

Saat Anda mengaktifkan Amazon GuardDuty untuk pertama kalinya atau mengaktifkan jenis perlindungan di dalamnya GuardDuty, GuardDuty mulailah memproses yang sesuai [Sumber data dasar](#) di AWS lingkungan Anda. GuardDuty menggunakan sumber data ini untuk memproses aliran peristiwa, seperti log VPC aliran, DNS log, dan log AWS CloudTrail peristiwa dan manajemen. Kemudian menganalisis peristiwa ini untuk mengidentifikasi potensi ancaman keamanan dan menghasilkan temuan di akun Anda.

Selain sumber data log, GuardDuty dapat menggunakan data tambahan dari AWS layanan lain di AWS lingkungan Anda untuk memantau dan menganalisis potensi ancaman keamanan.

## Aktivasi fitur

Ketika Anda menambahkan GuardDuty perlindungan tambahan, misalnya, Perlindungan S3, Pemantauan Runtime, atau EKS Perlindungan, Anda dapat mengonfigurasi GuardDuty fitur yang sesuai dengan jenis perlindungan. Secara historis, GuardDuty perlindungan disebut `dataSources` dalam APIs. Namun, setelah Maret 2023, jenis GuardDuty perlindungan baru sekarang dikonfigurasi sebagai `features` dan tidak `dataSources`. GuardDuty masih mendukung konfigurasi jenis perlindungan yang diluncurkan sebelum Maret 2023, seperti `dataSources` melalui API, tetapi jenis perlindungan baru hanya tersedia sebagai `features`.

Jika Anda mengelola jenis GuardDuty konfigurasi dan perlindungan melalui konsol, Anda tidak terpengaruh secara langsung oleh perubahan ini dan tidak perlu mengambil tindakan apa pun. Aktivasi fitur memengaruhi perilaku APIs yang dipanggil untuk mengaktifkan GuardDuty atau melindungi jenis di dalamnya GuardDuty. Untuk informasi selengkapnya, lihat [GuardDuty API perubahan](#).

## GuardDuty API perubahan Maret 2023

Fitur perlindungan GuardDuty APIs konfigurasi yang tidak termasuk dalam daftar [GuardDuty sumber data dasar](#). Objek fitur berisi detail fitur, seperti nama fitur dan status, dan mungkin berisi konfigurasi tambahan untuk beberapa fitur. Migrasi ini memengaruhi hal-hal berikut APIs di GuardDuty API Referensi Amazon:

- [CreateDetector](#)
- [GetDetector](#)



- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

## Fitur aktivasi dibandingkan dengan sumber data

Secara historis, semua GuardDuty fitur dilewatkan melalui `dataSources` objek di API. Dari Maret 2023, GuardDuty lebih suka `features` objek daripada `dataSources` objek di API. Semua sumber data sebelumnya memiliki fitur yang sesuai, tetapi fitur yang lebih baru mungkin tidak memiliki sumber data yang sesuai.

Daftar berikut menunjukkan perbandingan antara `dataSources` dan `features` objek ketika melewati API:

- `dataSources` objek berisi objek untuk setiap jenis perlindungan dan statusnya. `features` objek adalah daftar fitur yang tersedia yang sesuai dengan setiap jenis perlindungan di dalamnya GuardDuty.


Mulai Maret 2023, aktivasi fitur akan menjadi satu-satunya cara untuk mengonfigurasi GuardDuty fitur baru di AWS lingkungan Anda.

- `dataSources` skema dalam API permintaan atau tanggapan adalah sama di setiap Wilayah AWS tempat yang GuardDuty tersedia. Namun, setiap fitur mungkin tidak tersedia di setiap Wilayah. Oleh karena itu, nama fitur yang tersedia mungkin berbeda berdasarkan Wilayah.

## Memahami cara kerja aktivasi fitur

GuardDuty APIs akan terus mengembalikan `dataSources` objek sebagaimana berlaku, dan mereka juga akan mengembalikan `features` objek yang berisi informasi yang sama dalam format yang berbeda. GuardDuty fitur yang diluncurkan sebelum Maret 2023 akan tersedia melalui `dataSources` objek dan `features` objek. GuardDuty fitur yang diluncurkan sejak Maret 2023 hanya akan tersedia melalui `features` objek. Anda tidak dapat membuat atau memperbarui

detektor, atau menjelaskan AWS Organizations penggunaan keduanya dataSources dan notasi features objek dalam API permintaan yang sama. Untuk mengaktifkan jenis GuardDuty perlindungan, Anda harus memigrasikan sumber data yang ada ke features objek dengan menggunakan yang sama APIs yang sekarang menyertakan features objek juga.

 Note

GuardDuty tidak akan menambahkan sumber data baru setelah modifikasi ini.

GuardDuty telah menghentikan penggunaan sumber data. Namun, masih mendukung [GuardDuty sumber data dasar](#). Praktik GuardDuty terbaik merekomendasikan penggunaan aktivasi fitur untuk semua jenis perlindungan yang sudah diaktifkan untuk akun Anda. Praktik terbaik juga memerlukan aktivasi fitur saat Anda mengaktifkan jenis perlindungan baru untuk akun Anda.

## Memasukkan fitur perubahan aktivasi

- Jika Anda mengelola GuardDuty konfigurasi melalui APIs, SDKs, atau AWS CloudFormation template, dan ingin mengaktifkan GuardDuty fitur baru yang potensial, Anda harus memodifikasi kode dan template Anda, masing-masing. Untuk informasi selengkapnya, lihat yang diperbarui APIs di [GuardDuty API Referensi Amazon](#).
- Untuk GuardDuty fitur yang dikonfigurasi sebelum upgrade ini, Anda dapat terus menggunakan APIs, SDKs, atau AWS CloudFormation template. Namun, kami menyarankan Anda beralih menggunakan feature objek.

Semua sumber data memiliki objek fitur yang setara. Untuk informasi selengkapnya, lihat [Pemetaan ke dataSources features](#).

- Saat ini, `additionalConfiguration` dalam features objek hanya tersedia untuk jenis perlindungan tertentu.
  - Untuk jenis perlindungan seperti itu, jika fitur Anda `AdditionalConfiguration` status disetel ke `ENABLED` tetapi konfigurasi fitur Anda tidak status disetel ke `ENABLED`, tidak GuardDuty akan mengambil tindakan apa pun dalam kasus ini.
- Berikut ini APIs akan terpengaruh oleh ini:
  - [UpdateDetector](#)
  - [UpdateMemberDetectors](#)
  - [UpdateOrganizationConfiguration](#)

## Pemetaan ke `dataSourcesfeatures`

Tabel berikut menunjukkan pemetaan jenis perlindungan, `dataSources`, dan `features`.

| GuardDuty jenis perlindungan                     | Nama sumber <sup>data*</sup>  | Nama fitur   |
|--|---|--|
| <a href="#">VPCLog Aliran</a>                    | <code>flowLogs</code> (baca saja; tidak dapat dimodifikasi)                       | <code>FLOW_LOGS</code> (baca saja; tidak dapat dimodifikasi)   |
| <a href="#">Log kueri Route53 Resolver DNS</a>   | <code>dnsLogs</code> (baca saja; tidak dapat dimodifikasi)                        | <code>DNS_LOGS</code> (baca saja; tidak dapat dimodifikasi)    |
| <a href="#">CloudTrail acara</a>                 | <code>cloudTrail</code> (baca saja; tidak dapat dimodifikasi)                     | <code>CLOUD_TRAIL</code> (baca saja; tidak dapat dimodifikasi) |
| <a href="#">S3</a>                               | <code>s3Logs</code>   | <code>S3_DATA_EVENTS</code>                                    |
| <a href="#">EKSPemantauan Log Audit</a>          | <code>kubernetes.auditlogs</code>   | <code>EKS_AUDIT_LOGS</code>                                    |
| <a href="#">Perlindungan Malware untuk EC2</a>   | <code>malwareProtection.scanEc2InstanceWithFindings.ebsVolumes</code>             | <code>EBS_MALWARE_PROTECTION</code>                            |
| <a href="#">RDSAcara login</a>                   |   | <code>RDS_LOGIN_EVENTS</code>                                  |
| EKSPemantauan Runtime                            | GuardDuty hanya menyediakan dukungan aktivasi fitur untuk jenis perlindungan ini. | <code>EKS_RUNTIME_MONITORING</code>                            |
| <a href="#">Pemantauan Runtime</a>               |   | <code>RUNTIME_MONITORING</code>                                |
| GuardDuty agen keamanan untuk EKS cluster Amazon |   | <code>EKS_RUNTIME_MONITORING.addi</code>                       |

| GuardDuty jenis perlindungan                              | Nama sumber <sup>data*</sup> | Nama fitur   |
|---|------------------------------|--|
|   |                              | tionalConfiguration.EKS_ADDON_MANAGEMENT<br><br>RUNTIME_MONITORING.<br>.additionalConfiguration.EKS_ADDON_MANAGEMENT |
| GuardDuty agen keamanan untuk cluster Amazon ECS -Fargate |                              | RUNTIME_MONITORING.<br>.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT   |
| GuardDuty agen keamanan untuk EC2 instans Amazon          |                              | RUNTIME_MONITORING.<br>.additionalConfiguration.EC2_AGENT_MANAGEMENT   |
| <a href="#">Perlindungan Lambda</a>                       |                              | LAMBDA_NETWORK_LOGS  |

\* `GetUsageStatistics` menggunakan `dataSource` namanya sendiri. Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty](#) atau [GetUsageStatistics](#).

## GuardDuty Perlindungan S3

Perlindungan S3 membantu Amazon GuardDuty memantau peristiwa AWS CloudTrail data untuk Amazon Simple Storage Service (Amazon S3) yang menyertakan API operasi tingkat objek untuk mengidentifikasi potensi risiko keamanan data dalam bucket Amazon S3 Anda.

GuardDuty memantau peristiwa AWS CloudTrail manajemen dan peristiwa data AWS CloudTrail S3 untuk mengidentifikasi potensi ancaman di sumber daya Amazon S3 Anda. Kedua sumber data memantau berbagai jenis kegiatan. Contoh peristiwa CloudTrail manajemen untuk S3 mencakup operasi yang mencantumkan atau mengonfigurasi bucket Amazon S3, `ListBuckets` seperti `DeleteBuckets`, dan `PutBucketReplication`. Contoh peristiwa CloudTrail data untuk S3 termasuk API operasi tingkat objek, seperti `GetObjectListObjects`, `DeleteObject` dan `PutObject`.

Saat Anda mengaktifkan Amazon GuardDuty untuk Akun AWS, GuardDuty mulai memantau peristiwa CloudTrail manajemen. Anda tidak perlu secara eksplisit mengaktifkan atau mengonfigurasi login peristiwa data S3 AWS CloudTrail untuk menggunakan Perlindungan S3. Anda dapat mengaktifkan fitur Perlindungan S3 (yang memantau peristiwa CloudTrail data untuk S3) untuk akun apa pun di Wilayah AWS mana pun fitur ini tersedia di Amazon GuardDuty, kapan saja. An Akun AWS yang telah diaktifkan GuardDuty, dapat mengaktifkan Perlindungan S3 untuk pertama kalinya dengan periode uji coba gratis 30 hari. Untuk Akun AWS yang memungkinkan GuardDuty untuk pertama kalinya, Perlindungan S3 sudah diaktifkan dan disertakan dalam uji coba gratis 30 hari ini. Untuk informasi selengkapnya, lihat [Memperkirakan biaya GuardDuty](#).

Kami menyarankan Anda mengaktifkan Perlindungan S3 di GuardDuty. Jika fitur ini tidak diaktifkan, tidak GuardDuty akan dapat sepenuhnya memantau bucket Amazon S3 Anda atau menghasilkan temuan untuk akses mencurigakan ke data yang disimpan di bucket S3 Anda.

## Bagaimana GuardDuty menggunakan peristiwa data S3

Saat Anda mengaktifkan peristiwa data S3 (Perlindungan S3), GuardDuty mulailah menganalisis peristiwa data S3 dari semua bucket S3 Anda, dan memantaunya untuk aktivitas berbahaya dan mencurigakan. Untuk informasi selengkapnya, lihat [AWS CloudTrail peristiwa data untuk S3](#).

Ketika pengguna yang tidak diautentikasi mengakses objek S3, itu berarti bahwa objek S3 dapat diakses publik. Oleh karena itu, GuardDuty tidak memproses permintaan tersebut. GuardDuty memproses permintaan yang dibuat ke objek S3 dengan menggunakan kredensi valid IAM (AWS Identity and Access Management) atau AWS STS (AWS Security Token Service).

** Catatan**

Setelah mengaktifkan Perlindungan S3, Amazon GuardDuty memantau peristiwa data dari bucket Amazon S3 yang berada di Wilayah yang sama tempat Anda mengaktifkan GuardDuty

Ketika GuardDuty mendeteksi potensi ancaman berdasarkan pemantauan peristiwa data S3, itu menghasilkan temuan keamanan. Untuk informasi tentang jenis temuan yang GuardDuty dapat dihasilkan untuk bucket Amazon S3, lihat. [GuardDuty Jenis temuan S3](#)

Jika Anda menonaktifkan Perlindungan S3, GuardDuty menghentikan pemantauan peristiwa data S3 dari data yang disimpan di bucket S3 Anda.

## Fitur dalam Perlindungan S3

### AWS CloudTrail peristiwa data untuk S3

Peristiwa data, juga dikenal sebagai operasi bidang data, memberikan wawasan tentang operasi sumber daya yang dilakukan pada atau di dalam sumber daya. Operasi ini sering kali merupakan aktivitas bervolume tinggi.

Berikut ini adalah contoh peristiwa CloudTrail data untuk S3 yang GuardDuty dapat memantau:

- GetObjectAPIoperasi
- PutObjectAPIoperasi
- ListObjectsAPIoperasi
- DeleteObjectAPIoperasi

Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, Perlindungan S3 diaktifkan secara default dan juga termasuk dalam periode uji coba gratis 30 hari. Namun, fitur ini bersifat opsional dan Anda dapat memilih untuk mengaktifkan atau menonaktifkannya untuk akun atau Wilayah apa pun kapan saja. Untuk informasi selengkapnya tentang mengonfigurasi Amazon S3 sebagai fitur, lihat. [Perlindungan S3](#)

## Mengkonfigurasi Perlindungan S3 untuk akun mandiri

Untuk akun yang terkait dengan AWS Organizations, proses ini dapat diotomatisasi melalui pengaturan konsol. Untuk informasi selengkapnya, lihat [Mengkonfigurasi Perlindungan S3 di lingkungan beberapa akun](#).

### Untuk mengaktifkan atau menonaktifkan Perlindungan S3

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan S3 untuk akun mandiri.

#### Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan S3.
3. Halaman Perlindungan S3 memberikan status Perlindungan S3 saat ini untuk akun Anda. Pilih Aktifkan atau Nonaktifkan untuk mengaktifkan atau menonaktifkan Perlindungan S3 kapan saja.
4. Pilih Konfirmasi untuk mengonfirmasi pilihan Anda.

#### API/CLI

1. Jalankan [updateDetector](#) dengan menggunakan ID detektor valid Anda untuk Wilayah saat ini dan meneruskan `features` objek name sebagai `S3_DATA_EVENTS` disetel ke `ENABLED` atau `DISABLED` untuk mengaktifkan atau menonaktifkan Perlindungan S3, masing-masing.

#### Note

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

2. Atau, Anda dapat menggunakan AWS Command Line Interface. Untuk mengaktifkan Perlindungan S3, jalankan perintah berikut dan pastikan untuk menggunakan ID detektor valid Anda sendiri.



```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Untuk menonaktifkan Perlindungan S3, ganti ENABLED DISABLED dengan contoh.

## Mengkonfigurasi Perlindungan S3 di lingkungan beberapa akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengonfigurasi (mengaktifkan atau menonaktifkan) Perlindungan S3 untuk akun anggota di organisasi mereka. AWS Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan Perlindungan S3 secara otomatis di semua akun, hanya akun baru, atau tidak ada akun di organisasi. Untuk informasi selengkapnya, lihat [Mengelola akun dengan AWS Organizations](#).

### Mengkonfigurasi Perlindungan S3 untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Perlindungan S3 untuk akun GuardDuty administrator yang didelegasikan.

#### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun manajemen.

2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, pilih Edit.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

## Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

## API/CLI

Jalankan [updateDetector](#) dengan menggunakan ID detektor akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini dan meneruskan features objek name sebagai S3\_DATA\_EVENTS dan status sebagai ENABLED.

Atau, Anda dapat mengkonfigurasi Perlindungan S3 dengan menggunakan AWS Command Line Interface. Jalankan perintah berikut, dan pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan ID detektor akun GuardDuty administrator yang didelegasikan untuk Wilayah saat ini.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

## Aktifkan Perlindungan S3 secara otomatis untuk semua akun anggota di organisasi

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.


Masuk menggunakan akun administrator Anda.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman Perlindungan S3

1. Di panel navigasi, pilih Perlindungan S3.

2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis mengaktifkan Perlindungan S3 untuk akun yang ada dan baru di organisasi.
3. Pilih Simpan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

### Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Perlindungan S3.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan atau nonaktifkan Perlindungan S3 secara selektif di akun anggota](#).

### API/CLI

- Untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun GuardDuty administrator detector-id yang didelegasikan, dan *111122223333*. Untuk menonaktifkan Perlindungan S3, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

```
aws guardduty update-member-detectors --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features  
'[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk semua akun anggota aktif yang ada di organisasi Anda.

### Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan S3.
3. Pada halaman Perlindungan S3, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

### API/CLI

- Untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Pastikan untuk mengganti `12abc34d567e8fa901bc2d34e56789f0` dengan

akun GuardDuty administrator detector-id yang didelegasikan, dan **111122223333**. Untuk menonaktifkan Perlindungan S3, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features ' [{"name": "S3_DATA_EVENTS", "status": "ENABLED"} ]'
```

#### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan Perlindungan S3 secara otomatis untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Perlindungan S3 untuk akun baru yang bergabung dengan organisasi Anda.

### Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan akun anggota baru di organisasi melalui konsol, menggunakan halaman Perlindungan S3 atau Akun.

Untuk mengaktifkan Perlindungan S3 secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman Perlindungan S3:
  1. Di panel navigasi, pilih Perlindungan S3.
  2. Pada halaman Perlindungan S3, pilih Edit.
  3. Pilih Konfigurasi akun secara manual.

4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan S3 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
5. Pilih Simpan.
  - Menggunakan halaman Akun:
    1. Di panel navigasi, pilih Akun.
    2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
    3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Perlindungan S3.
    4. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan milik Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Untuk menonaktifkannya, lihat [Aktifkan atau nonaktifkan Perlindungan S3 secara selektif di akun anggota](#). Tetapkan preferensi untuk mengaktifkan atau menonaktifkan paket perlindungan secara otomatis di Wilayah tersebut untuk akun baru (NEW) yang bergabung dengan organisasi, semua akun (ALL), atau tidak ada akun (NONE) di organisasi. Untuk informasi selengkapnya, lihat [autoEnableOrganizationAnggota](#). Berdasarkan preferensi Anda, Anda mungkin perlu mengganti NEW dengan ALL atau NONE.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan atau nonaktifkan Perlindungan S3 secara selektif di akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif untuk akun anggota.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom Perlindungan S3 untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif

Pilih akun yang ingin Anda konfigurasi Perlindungan S3. Anda dapat memilih beberapa akun sekaligus. Di menu dropdown Edit Protection Plans, pilih S3Pro, lalu pilih opsi yang sesuai.

### API/CLI

Untuk mengaktifkan atau menonaktifkan Perlindungan S3 secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectorsAPI](#) operasi menggunakan ID detektor Anda sendiri. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Perlindungan S3 untuk satu akun anggota. Untuk menonaktifkannya, ganti `true` dengan `false`.


Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

#### Note


Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

 Note

Jika Anda menggunakan skrip untuk mengaktifkan akun baru dan ingin menonaktifkan Perlindungan S3 di akun baru Anda, Anda dapat memodifikasi [createDetector](#) API operasi dengan `dataSources` objek opsional seperti yang dijelaskan dalam topik ini.

## Secara otomatis menonaktifkan Perlindungan S3 untuk akun baru GuardDuty

 Important

Secara default, Perlindungan S3 diaktifkan secara otomatis untuk Akun AWS bergabung GuardDuty untuk pertama kalinya.

Jika Anda adalah akun GuardDuty administrator yang mengaktifkan GuardDuty untuk pertama kalinya pada akun baru dan tidak ingin Perlindungan S3 diaktifkan secara default, Anda dapat menonaktifkannya dengan memodifikasi [createDetector](#) API operasi dengan objek opsional. Contoh berikut menggunakan AWS CLI untuk mengaktifkan GuardDuty detektor baru dengan Perlindungan S3 dinonaktifkan.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",  
"Status" : "DISABLED"}]'
```



# GuardDuty EKSPerlindungan

EKSAudit Log Monitoring membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan dalam EKS klaster dalam Amazon Elastic Kubernetes Service (Amazon). EKS EKSAudit Log Monitoring menggunakan log EKS audit untuk menangkap aktivitas kronologis dari pengguna, aplikasi yang menggunakan KubernetesAPI, dan bidang kontrol. Untuk informasi selengkapnya, lihat [EKSpemantauan log audit](#).

## Note

EKSRuntime Monitoring dikelola sebagai bagian dari Runtime Monitoring. Untuk informasi selengkapnya, lihat [GuardDuty Pemantauan Runtime](#).

## Fitur dalam EKS Perlindungan

### EKSpemantauan log audit

EKSlog audit menangkap tindakan berurutan dalam EKS klaster Amazon Anda, termasuk aktivitas dari pengguna, aplikasi yang menggunakan KubernetesAPI, dan bidang kontrol. Audit logging adalah komponen dari semua klaster Kubernetes.

Untuk informasi selengkapnya, lihat [Auditing](#) dalam dokumentasi Kubernetes.

Amazon EKS memungkinkan log EKS audit untuk dicerna sebagai Amazon CloudWatch Logs melalui fitur [EKScontrol plane logging](#). GuardDuty tidak mengelola pencatatan pesawat EKS kontrol Amazon Anda atau membuat log EKS audit dapat diakses di akun Anda jika Anda belum mengaktifkannya untuk AmazonEKS. Untuk mengelola akses dan retensi log EKS audit, Anda harus mengonfigurasi fitur pencatatan bidang EKS kontrol Amazon. Untuk informasi selengkapnya, lihat [Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan](#) Pengguna Amazon EKS.

Untuk informasi tentang mengonfigurasi Pemantauan Log EKS Audit, lihat [EKSPemantauan Log Audit](#).

### EKSPemantauan Log Audit

EKSAudit Log Monitoring membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di EKS cluster Anda dalam Amazon Elastic Kubernetes Service. Saat Anda mengaktifkan Pemantauan

Log EKS Audit, GuardDuty segera mulai memantau [EKSpemantauan log audit](#) dari EKS kluster Amazon Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan. Ini menggunakan peristiwa log audit Kubernetes langsung dari fitur logging pesawat EKS kontrol Amazon melalui aliran log audit yang independen dan duplikatif. Proses ini tidak memerlukan pengaturan tambahan atau memengaruhi konfigurasi pencatatan pesawat EKS kontrol Amazon yang ada yang mungkin Anda miliki.

Saat Anda menonaktifkan Pemantauan Log EKS Audit, GuardDuty segera hentikan pemantauan dan analisis log EKS audit untuk EKS sumber daya Amazon Anda.

EKSPemantauan Log Audit mungkin tidak tersedia di semua Wilayah AWS tempat GuardDuty yang tersedia. Untuk informasi selengkapnya, lihat [Ketersediaan fitur khusus wilayah](#).

Bagaimana periode uji coba gratis 30 hari memengaruhi akun GuardDuty

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, Pemantauan Log EKS Audit sudah termasuk dalam periode uji coba gratis 30 hari.
- GuardDuty Akun yang ada, yang telah disimpulkan oleh uji coba gratis 30 hari, dapat mengaktifkan Pemantauan Log EKS Audit untuk pertama kalinya dengan masa uji coba gratis 30 hari.

## Mengkonfigurasi Pemantauan Log EKS Audit untuk akun mandiri

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit untuk akun mandiri.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih EKS Perlindungan.
3. Di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi Pemantauan Log EKS Audit saat ini. Di bagian Pemantauan Log EKS Audit, pilih Aktifkan untuk mengaktifkan atau Nonaktifkan untuk menonaktifkan fitur Pemantauan Log EKS Audit.
4. Pilih Simpan.

## API/CLI

- Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan meneruskan nama features objek sebagai EKS\_AUDIT\_LOGS dan status sebagai ENABLED atau DISABLED.

Atau, Anda juga dapat mengaktifkan atau menonaktifkan EKS Audit Log Monitoring menjalankan AWS CLI perintah. Kode contoh berikut memungkinkan GuardDuty EKS Audit Log Monitoring. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
```

## Mengkonfigurasi Pemantauan Log EKS Audit di lingkungan beberapa akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit; fitur untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan Pemantauan Log EKS Audit secara otomatis untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat [Mengelola beberapa akun di Amazon](#). GuardDuty

### Mengkonfigurasi Pemantauan Log EKS Audit untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Pemantauan Log EKS Audit untuk akun GuardDuty administrator yang didelegasikan.

#### Console

- Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.  
Pastikan untuk menggunakan kredensi akun manajemen.
- Di panel navigasi, pilih EKS Perlindungan.

3. Di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi Pemantauan Log EKS Audit saat ini di bagian masing-masing. Untuk memperbarui konfigurasi akun GuardDuty administrator yang didelegasikan, pilih Edit di panel Pemantauan Log EKS Audit.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

## API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai EKS\_AUDIT\_LOGS dan status sebagai ENABLED atau DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Anda dapat mengaktifkan atau menonaktifkan EKS Audit Log Monitoring dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan yang valid *detector ID*.

### Note

Kode contoh berikut memungkinkan EKS Audit Log Monitoring. Pastikan untuk mengganti *12abc34d567e8fa901bc2d34e56789f0* dengan akun GuardDuty administrator yang

didelegasikan dan `detector-id` **555555555555** dengan akun GuardDuty administrator yang didelegasikan. Akun AWS

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Untuk menonaktifkan Pemantauan Log EKS Audit, ganti `ENABLED` dengan `DISABLED`.

Aktifkan otomatis Pemantauan Log EKS Audit untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log EKS Audit untuk akun anggota yang ada di organisasi Anda.

## Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman EKSPerlindungan

1. Di panel navigasi, pilih EKSPerlindungan.
2. Di bawah tab Konfigurasi, Anda dapat melihat status Pemantauan Log EKS Audit saat ini untuk akun anggota aktif di organisasi Anda.

Untuk memperbarui konfigurasi Pemantauan Log EKS Audit, pilih Edit.

3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Log EKS Audit untuk akun yang ada dan yang baru di organisasi.
4. Pilih Simpan.

**Note**

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

### Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Log EKS Audit.
4. Pilih Simpan.


Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun dan ingin menyesuaikan konfigurasi Pemantauan Log EKS Audit untuk akun tertentu di organisasi Anda, lihat [Aktifkan atau nonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun anggota](#).

### API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Log EKS Audit untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log EKS Audit untuk semua akun anggota aktif yang ada di organisasi.

## Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih EKSPerindungan.
3. Pada halaman EKSPerindungan, Anda dapat melihat status saat ini dari konfigurasi pemindaian malware GuardDuty yang dimulai. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan otomatis Pemantauan Log EKS Audit untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengkonfigurasi GuardDuty pemindaian malware yang dimulai. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi GuardDuty pemindaian malware yang dimulai secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat [Step 3 - Accept an invitation](#).

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Log EKS Audit untuk akun baru yang bergabung dengan organisasi Anda.

## Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Log EKS Audit untuk akun anggota baru di organisasi, baik menggunakan halaman Pemantauan Log EKS Audit atau Akun.

Untuk mengaktifkan Pemantauan Log EKS Audit secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman EKSPerlindungan:

1. Di panel navigasi, pilih EKSPerlindungan.
2. Pada halaman EKSPerlindungan, pilih Edit di Pemantauan Log EKS Audit.



3. Pilih Konfigurasi akun secara manual.
  4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Pemantauan Log EKS Audit akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
  5. Pilih Simpan.
- Menggunakan halaman Akun:
    1. Di panel navigasi, pilih Akun.
    2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
    3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Log EKS Audit.
    4. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun baru Anda, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan cara mengaktifkan Pemantauan Log EKS Audit untuk anggota baru yang bergabung dengan organisasi Anda. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Aktifkan atau nonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit untuk akun anggota selektif di organisasi Anda.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom Pemantauan Log EKS Audit untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit

Pilih akun yang ingin Anda konfigurasi untuk Pemantauan Log EKS Audit. Anda dapat memilih beberapa akun sekaligus. Di bawah menu tarik-turun Edit Rencana Perlindungan, pilih Pemantauan Log EKS Audit, lalu pilih opsi yang sesuai.

## API/CLI

Untuk mengaktifkan atau menonaktifkan Pemantauan Log EKS Audit secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan EKS Audit Log Monitoring untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
"ENABLED"}]'
```

# GuardDuty Pemantauan Runtime

Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda.

AWS Sumber daya yang didukung dalam Runtime Monitoring — GuardDuty awalnya merilis Runtime Monitoring untuk hanya mendukung sumber daya Amazon Elastic Kubernetes Service (Amazon EKS). Sekarang, Anda dapat menggunakan fitur Runtime Monitoring untuk menyediakan deteksi ancaman untuk sumber daya AWS Fargate Amazon Elastic Container Service (Amazon ECS) dan Amazon Elastic Compute Cloud EC2 (Amazon).

GuardDuty tidak mendukung EKS kluster Amazon yang berjalan. AWS Fargate

Dalam dokumen ini dan bagian lain yang terkait dengan Runtime Monitoring, GuardDuty menggunakan terminologi jenis sumber daya untuk merujuk ke Amazon, EKS Fargate Amazon, ECS dan sumber daya Amazon. EC2

Runtime Monitoring menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman, Anda dapat mengelola agen keamanan untuk jenis sumber daya tertentu baik secara otomatis atau manual (dengan pengecualian untuk Fargate (ECS hanya Amazon)). Mengelola agen keamanan secara otomatis berarti Anda mengizinkan GuardDuty untuk menginstal dan memperbarui agen keamanan atas nama Anda. Di sisi lain, ketika Anda mengelola agen keamanan untuk sumber daya Anda secara manual, Anda bertanggung jawab untuk menginstal dan memperbarui agen keamanan, sesuai kebutuhan.

Dengan kemampuan yang diperluas ini, GuardDuty dapat membantu Anda mengidentifikasi dan merespons potensi ancaman yang dapat menargetkan aplikasi dan data yang berjalan di beban kerja dan instance pribadi Anda. Misalnya, ancaman berpotensi dimulai dengan mengorbankan satu wadah yang menjalankan aplikasi web yang rentan. Aplikasi web ini mungkin memiliki izin akses ke wadah dan beban kerja yang mendasarinya. Dalam skenario ini, kredensial yang dikonfigurasi secara tidak benar berpotensi menyebabkan akses yang lebih luas ke akun, dan data yang tersimpan di dalamnya.

Dengan menganalisis peristiwa runtime dari setiap kontainer dan beban kerja, GuardDuty berpotensi mengidentifikasi kompromi kontainer dan AWS kredensial terkait pada fase awal, dan mendeteksi

upaya untuk meningkatkan hak istimewa, API permintaan mencurigakan, dan akses berbahaya ke data di lingkungan Anda.

## Daftar Isi

- [Cara kerjanya](#)
- [Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring](#)
- [Konsep kunci - Pendekatan untuk mengelola agen GuardDuty keamanan](#)
- [Mengaktifkan GuardDuty Runtime Monitoring](#)
- [Mengkonfigurasi EKS Runtime Monitoring \(hanya\) API](#)
- [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#)
- [Menilai cakupan runtime untuk sumber daya Anda](#)
- [Pengaturan CPU dan pemantauan memori](#)
- [Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty](#)
- [Agen hosting ECR repositori Amazon GuardDuty](#)
- [GuardDuty sejarah rilis agen](#)
- [Dampak menonaktifkan dan membersihkan sumber daya](#)

## Cara kerjanya

Untuk menggunakan Runtime Monitoring, Anda harus mengaktifkan Runtime Monitoring dan kemudian mengelola agen GuardDuty keamanan. Daftar berikut menjelaskan proses dua langkah ini:

1. Aktifkan Runtime Monitoring untuk akun Anda sehingga GuardDuty dapat menerima peristiwa runtime yang diterimanya dari EC2 instans Amazon, ECS kluster Amazon, dan beban kerja Amazon. EKS
2. Kelola GuardDuty agen untuk sumber daya individual yang ingin Anda pantau perilaku runtime. Berdasarkan jenis sumber daya, Anda dapat memilih untuk menggunakan agen GuardDuty keamanan baik secara manual atau dengan mengizinkan GuardDuty untuk mengelolanya atas nama Anda, yang disebut konfigurasi agen otomatis.

GuardDuty menggunakan [peran identitas Instance](#) yang mengautentikasi agen keamanan untuk setiap jenis sumber daya untuk mengirim peristiwa runtime terkait ke titik akhirVPC.

**Note**

GuardDuty tidak membuat acara runtime dapat diakses oleh Anda.

Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari instance ini GuardDuty , Akun AWS Anda tidak akan membebankan biaya untuk analisis VPC log aliran dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

Topik berikut menjelaskan cara mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan bekerja secara berbeda untuk setiap jenis sumber daya.

**Daftar Isi**

- [Cara kerja Runtime Monitoring dengan instans Amazon EC2](#)
- [Bagaimana Runtime Monitoring bekerja dengan Fargate \(hanya AmazonECS\)](#)
- [Cara kerja Runtime Monitoring dengan kluster Amazon EKS](#)
- [Setelah konfigurasi Runtime Monitoring](#)

## Cara kerja Runtime Monitoring dengan instans Amazon EC2

EC2Instans Amazon Anda dapat menjalankan beberapa jenis aplikasi dan beban kerja di lingkungan Anda AWS . Bila Anda mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan, GuardDuty membantu Anda mendeteksi ancaman dalam EC2 instans Amazon yang ada dan yang berpotensi baru. Fitur ini juga mendukung EC2 instans Amazon yang ECS dikelola Amazon.

Mengaktifkan Runtime Monitoring akan GuardDuty siap untuk mengkonsumsi peristiwa runtime dari proses yang sedang berjalan dan proses baru dalam instans Amazon. EC2 GuardDuty membutuhkan agen keamanan untuk mengirim peristiwa runtime dari EC2 instance Anda ke GuardDuty.

Untuk EC2 instans Amazon, agen GuardDuty keamanan beroperasi pada tingkat instans. Anda dapat memutuskan apakah Anda ingin memantau semua atau EC2 instans Amazon selektif di akun Anda. Jika Anda ingin mengelola instance selektif, agen keamanan hanya diperlukan untuk instance ini.

GuardDuty juga dapat menggunakan peristiwa runtime dari tugas baru dan tugas yang ada yang berjalan di EC2 instans Amazon dalam kluster AmazonECS.

Untuk menginstal agen GuardDuty keamanan, Runtime Monitoring menyediakan dua opsi berikut:

- [Gunakan konfigurasi agen otomatis \(disarankan\)](#), atau
- [Kelola agen keamanan secara manual](#)

## Gunakan konfigurasi agen otomatis melalui GuardDuty (disarankan)

Gunakan konfigurasi agen otomatis yang memungkinkan GuardDuty untuk menginstal agen keamanan di EC2 instans Amazon Anda atas nama Anda. GuardDuty juga mengelola pembaruan ke agen keamanan.

Secara default, GuardDuty instal agen keamanan pada semua instans di akun Anda. Jika Anda GuardDuty ingin menginstal dan mengelola agen keamanan hanya untuk EC2 instance yang dipilih, tambahkan tag penyertaan atau pengecualian ke EC2 instance Anda, sesuai kebutuhan.

Terkadang, Anda mungkin tidak ingin memantau peristiwa runtime untuk semua EC2 instans Amazon milik akun Anda. Untuk kasus ketika Anda ingin memantau peristiwa runtime untuk sejumlah instance terbatas, tambahkan tag inklusi sebagai `GuardDutyManaged: true` ke instance yang dipilih ini. Dimulai dengan ketersediaan konfigurasi agen otomatis untuk AmazonEC2, jika EC2 instans Anda memiliki tag inklusi (`GuardDutyManaged:true`), GuardDuty akan menghormati tag dan mengelola agen keamanan untuk instans yang dipilih meskipun Anda tidak secara eksplisit mengaktifkan konfigurasi agen otomatis.

Di sisi lain, jika ada sejumlah EC2 instance yang tidak ingin Anda pantau peristiwa runtime, tambahkan tag pengecualian (`GuardDutyManaged:false`) ke instance yang dipilih ini. GuardDuty akan menghormati tag pengecualian dengan tidak menginstal atau mengelola agen keamanan untuk EC2 sumber daya ini.

## Dampak

Ketika Anda menggunakan konfigurasi agen otomatis dalam suatu Akun AWS atau organisasi, Anda mengizinkan GuardDuty untuk mengambil langkah-langkah berikut atas nama Anda:

- GuardDuty membuat satu SSM asosiasi untuk semua EC2 instans Amazon Anda yang SSM dikelola dan muncul di bawah Fleet Manager di <https://console.aws.amazon.com/systems-manager/konsol>.
- Menggunakan tag penyertaan dengan konfigurasi agen otomatis dinonaktifkan — Setelah mengaktifkan Runtime Monitoring, ketika Anda tidak mengaktifkan konfigurasi agen otomatis tetapi

menambahkan tag inklusi ke EC2 instans Amazon Anda, itu berarti Anda mengizinkan GuardDuty untuk mengelola agen keamanan atas nama Anda. SSM asosiasi kemudian akan menginstal agen keamanan di setiap instance yang memiliki tag inklusi (`GuardDutyManaged:true`).

- Jika Anda mengaktifkan konfigurasi agen otomatis — SSM Asosiasi kemudian akan menginstal agen keamanan di semua EC2 instance milik akun Anda.
- Menggunakan tag pengecualian dengan konfigurasi agen otomatis — Sebelum Anda mengaktifkan konfigurasi agen otomatis, ketika Anda menambahkan tag pengecualian ke EC2 instans Amazon Anda, itu berarti Anda mengizinkan GuardDuty untuk mencegah menginstal dan mengelola agen keamanan untuk instance yang dipilih ini.

Sekarang, ketika Anda mengaktifkan konfigurasi agen otomatis, SSM asosiasi akan menginstal dan mengelola agen keamanan di semua EC2 instance kecuali yang ditandai dengan tag pengecualian.

- GuardDuty membuat VPC titik akhir di semua VPCs, termasuk bersama VPCs, selama setidaknya ada satu EC2 instance Linux yang tidak dalam status instance VPC yang dihentikan atau dimatikan. Ini termasuk yang terpusat VPC dan berbicara VPCs. GuardDuty tidak mendukung pembuatan VPC titik akhir hanya untuk yang terpusat VPC. Untuk informasi selengkapnya tentang cara VPC kerja terpusat, lihat [VPC Endpoint antarmuka](#) di AWS Whitepaper - Membangun Infrastruktur Multi Jaringan yang Dapat Diskalakan dan Aman. VPC AWS

Untuk informasi tentang status instans yang berbeda, lihat [Siklus hidup instans](#) di EC2 Panduan Pengguna Amazon.

GuardDuty juga mendukung [Menggunakan berbagi VPC dengan agen keamanan otomatis](#).

Ketika semua prasyarat dipertimbangkan untuk organisasi Anda dan Akun AWS, GuardDuty akan menggunakan yang dibagikan VPC untuk menerima acara runtime.

#### Note

Tidak ada biaya tambahan untuk penggunaan VPC endpoint.

## Kelola agen keamanan secara manual

Ada dua cara untuk mengelola agen keamanan untuk Amazon EC2 secara manual:

- Gunakan dokumen GuardDuty terkelola AWS Systems Manager untuk menginstal agen keamanan di EC2 instans Amazon Anda yang sudah SSM dikelola.

Setiap kali Anda meluncurkan EC2 instans Amazon baru, pastikan itu SSM diaktifkan.

- Gunakan skrip pengelola RPM paket (RPM) untuk menginstal agen keamanan di EC2 instans Amazon Anda, terlepas dari apakah mereka dikelola atau tidak. SSM

## Langkah selanjutnya

Untuk memulai konfigurasi Runtime Monitoring untuk memantau EC2 instans Amazon Anda, lihat. [Prasyarat untuk dukungan instans Amazon EC2](#)

## Bagaimana Runtime Monitoring bekerja dengan Fargate (hanya AmazonECS)

Saat Anda mengaktifkan Runtime Monitoring, GuardDuty menjadi siap untuk mengkonsumsi peristiwa runtime dari tugas. Tugas-tugas ini berjalan di dalam ECS kluster Amazon, yang pada gilirannya berjalan pada AWS Fargate (Fargate) instance. GuardDuty Untuk menerima acara runtime ini, Anda harus menggunakan agen keamanan khusus yang dikelola sepenuhnya.

Runtime Monitoring mendukung pengelolaan agen keamanan untuk ECS kluster Amazon Anda (AWS Fargate) hanya melalui. GuardDuty Tidak ada dukungan untuk mengelola agen keamanan secara manual di ECS cluster Amazon.

Anda dapat mengizinkan GuardDuty untuk mengelola agen GuardDuty keamanan atas nama Anda, dengan menggunakan konfigurasi agen otomatis untuk AWS akun atau organisasi. GuardDuty akan mulai menyebarkan agen keamanan ke tugas Fargate baru yang diluncurkan di cluster Amazon ECS Anda. Daftar berikut menentukan apa yang diharapkan ketika Anda mengaktifkan agen GuardDuty keamanan.

Dampak memungkinkan agen GuardDuty keamanan

GuardDuty membuat titik akhir cloud pribadi virtual (VPC)

Ketika Anda menyebarkan agen GuardDuty keamanan, GuardDuty akan membuat VPC titik akhir di mana agen keamanan mengirimkan peristiwa runtime ke. GuardDuty

### Catatan

- Bekerja dengan terpusat VPC dengan agen otomatis — Ketika Anda menggunakan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya, GuardDuty akan



membuat VPC titik akhir atas nama Anda untuk semua. VPCs Ini termasuk yang terpusat VPC dan berbicaraVPCs. GuardDuty tidak mendukung pembuatan VPC titik akhir hanya untuk yang terpusatVPC. Untuk informasi selengkapnya tentang cara VPC kerja terpusat, lihat [VPCEndpoint antarmuka](#) di AWS Whitepaper - Membangun Infrastruktur Multi Jaringan yang Dapat Diskalakan dan Aman. VPC AWS

- Tidak ada biaya tambahan untuk penggunaan VPC endpoint.

GuardDuty menambahkan wadah sespan

Untuk tugas atau layanan Fargate baru yang mulai berjalan, GuardDuty kontainer (sespan) menempel pada setiap kontainer dalam tugas Amazon Fargate. ECS Agen GuardDuty keamanan berjalan di dalam GuardDuty wadah terlampir. Ini GuardDuty membantu mengumpulkan peristiwa runtime dari setiap kontainer yang berjalan dalam tugas-tugas ini.

Saat Anda memulai tugas Fargate, jika GuardDuty container (sespan) tidak dapat diluncurkan dalam keadaan sehat, Runtime Monitoring dirancang untuk tidak mencegah tugas berjalan.

Secara default, tugas Fargate tidak dapat diubah. GuardDuty tidak akan menyebarkan sespan saat tugas sudah dalam keadaan berjalan. Jika Anda ingin memantau wadah dalam tugas yang sudah berjalan, Anda dapat menghentikan tugas dan memulainya lagi.

## Cara kerja Runtime Monitoring dengan kluster Amazon EKS

Runtime Monitoring menggunakan [EKSadd-on aws-guardduty-agent](#), juga disebut sebagai agen GuardDuty keamanan. Setelah agen GuardDuty keamanan dikerahkan di EKS cluster Anda, GuardDuty dapat menerima peristiwa runtime untuk cluster ini. EKS

GuardDuty mendukung EKS kluster Amazon yang berjalan hanya pada EC2 instans Amazon. GuardDuty tidak mendukung EKS kluster Amazon yang berjalan. AWS Fargate

Anda dapat memantau peristiwa runtime EKS klaster Amazon di level akun atau klaster. Anda dapat mengelola agen GuardDuty keamanan hanya untuk EKS kluster Amazon yang ingin Anda pantau untuk deteksi ancaman. Anda dapat mengelola agen GuardDuty keamanan baik secara manual atau dengan mengizinkan GuardDuty untuk mengelolanya atas nama Anda, dengan menggunakan konfigurasi agen Otomatis.

Ketika Anda menggunakan pendekatan konfigurasi agen otomatis GuardDuty untuk memungkinkan mengelola penyebaran agen keamanan atas nama Anda, itu akan secara otomatis membuat titik

akhir Amazon Virtual Private Cloud (AmazonVPC). Agen keamanan mengirimkan peristiwa runtime GuardDuty dengan menggunakan endpoint Amazon VPC ini.

#### Catatan

- Tidak ada biaya tambahan untuk penggunaan VPC endpoint.
- Bekerja dengan terpusat VPC dengan agen otomatis — Ketika Anda menggunakan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya, GuardDuty akan membuat VPC titik akhir atas nama Anda untuk semua. VPCs Ini termasuk yang terpusat VPC dan berbicaraVPCs. GuardDuty tidak mendukung pembuatan VPC titik akhir hanya untuk yang terpusatVPC. Untuk informasi selengkapnya tentang cara VPC kerja terpusat, lihat [VPCEndpoint antarmuka](#) di AWS Whitepaper - Membangun Infrastruktur Multi Jaringan yang Dapat Diskalakan dan Aman. VPC AWS

## Setelah konfigurasi Runtime Monitoring

### Menilai cakupan runtime

Setelah Anda mengaktifkan Runtime Monitoring dan menyebarkan agen GuardDuty keamanan, kami sarankan Anda untuk terus menilai status cakupan sumber daya tempat Anda menggunakan agen keamanan. Status cakupan bisa sehat atau tidak sehat. Status cakupan Sehat menunjukkan GuardDuty bahwa menerima peristiwa runtime dari sumber daya yang sesuai ketika ada aktivitas tingkat sistem operasi.

Ketika status cakupan menjadi Sehat untuk sumber daya, GuardDuty dapat menerima peristiwa runtime dan menganalisisnya untuk deteksi ancaman. Saat GuardDuty mendeteksi potensi ancaman keamanan dalam tugas atau aplikasi yang berjalan di beban kerja dan instance container Anda, GuardDuty buat satu atau beberapa jenis pencarian Runtime Monitoring.

Anda juga dapat mengonfigurasi Amazon EventBridge (EventBridge) untuk menerima pemberitahuan ketika status cakupan berubah dari Tidak Sehat menjadi Sehat dan sebaliknya. Untuk informasi selengkapnya, lihat [Menilai cakupan runtime untuk sumber daya Anda](#).

### Pengaturan CPU dan pemantauan memori untuk agen GuardDuty keamanan

Setelah Anda menilai bahwa status cakupan ditampilkan sebagai Sehat, Anda dapat mengevaluasi kinerja agen keamanan untuk jenis sumber daya Anda. Untuk EKS kluster Amazon

yang memiliki rilis agen keamanan v1.5 atau lebih tinggi, GuardDuty mendukung konfigurasi parameter agen keamanan (add-on). Untuk informasi selengkapnya, lihat [Pengaturan CPU dan pemantauan memori](#).

GuardDuty mendeteksi potensi ancaman

Saat GuardDuty mulai menerima peristiwa runtime untuk sumber daya Anda, ia mulai menganalisis peristiwa tersebut. Saat GuardDuty mendeteksi potensi ancaman keamanan di salah satu EC2 instans Amazon Anda, kluster Amazon, atau ECS kluster AmazonEKS, itu menghasilkan satu atau lebih. [Jenis penemuan Runtime Monitoring](#) Anda dapat mengakses detail temuan untuk melihat detail sumber daya yang terkena dampak.

## Bagaimana cara kerja uji coba gratis 30 hari di Runtime Monitoring

Masa uji coba gratis 30 hari bekerja secara berbeda untuk GuardDuty akun baru dan akun yang sudah ada yang telah mengaktifkan EKS Runtime Monitoring sebelum kemampuan Runtime Monitoring diperluas ke EC2 instans Amazon dan (hanya AWS Fargate Amazon). ECS

### Saya menggunakan masa GuardDuty percobaan atau saya tidak pernah mengaktifkan EKS Runtime Monitoring

Daftar berikut menjelaskan cara kerja periode uji coba gratis 30 hari jika Anda menggunakan periode uji coba GuardDuty 30 hari atau belum pernah mengaktifkan EKS Runtime Monitoring:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, Runtime Monitoring dan EKS Runtime Monitoring tidak akan diaktifkan secara default.

Saat Anda mengaktifkan Runtime Monitoring untuk akun atau organisasi Anda, pastikan juga mengonfigurasi agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau untuk deteksi ancaman. Misalnya, jika Anda ingin menggunakan Runtime Monitoring untuk EC2 instans Amazon Anda, maka setelah Anda mengaktifkan Runtime Monitoring, Anda juga harus mengonfigurasi agen keamanan untuk Amazon. EC2 Anda dapat memilih untuk melakukan ini baik secara manual atau otomatis melalui GuardDuty.

- Paket perlindungan Runtime Monitoring diaktifkan di tingkat akun. Periode uji coba gratis 30 hari bekerja di tingkat sumber daya. Setelah agen GuardDuty keamanan diterapkan ke jenis sumber daya tertentu, uji coba gratis 30 hari dimulai saat GuardDuty menerima peristiwa runtime pertama yang terkait dengan jenis sumber daya ini. Misalnya, Anda telah menerapkan GuardDuty agen di tingkat sumber daya (untuk EC2 instans Amazon, ECS kluster Amazon, dan EKS kluster Amazon).

Saat GuardDuty menerima acara runtime pertama untuk EC2 instans Amazon, uji coba gratis 30 hari hanya akan dimulai untuk AmazonEC2.

- Bila Anda hanya ingin mengaktifkan EKS Runtime Monitoring — Saat Anda mengaktifkan GuardDuty untuk pertama kalinya, EKS Runtime Monitoring tidak diaktifkan secara default (setelah rilis Runtime Monitoring). Anda harus mengaktifkan EKS Runtime Monitoring. Untuk menggunakannya secara optimal, pastikan Anda mengelola agen GuardDuty keamanan secara manual atau mengaktifkan konfigurasi agen otomatis sehingga GuardDuty mengelola agen atas nama Anda. Masa uji coba gratis 30 hari untuk EKS Runtime Monitoring dimulai saat GuardDuty menerima acara runtime pertamanya untuk sumber daya Amazon. EKS

## Saya mengaktifkan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring

- Untuk GuardDuty akun yang sudah ada yang mengaktifkan paket perlindungan EKS Runtime Monitoring dan menggunakan pengalaman GuardDuty konsol untuk menggunakan paket perlindungan ini — Dengan pengumuman Runtime Monitoring, pengalaman konsol Runtime Monitoring kini telah dikonsolidasikan ke dalam EKS Runtime Monitoring. Konfigurasi Anda yang ada untuk EKS Runtime Monitoring tetap sama. Anda dapat terus menggunakan CLI dukunganAPI/ untuk melakukan operasi yang terkait dengan EKS Runtime Monitoring.
- Untuk menggunakan EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring, Anda perlu mengonfigurasi Runtime Monitoring untuk akun atau organisasi Anda. Untuk menjaga konfigurasi yang sama untuk Runtime Monitoring, lihat [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#). Namun, ini tidak akan memengaruhi uji coba gratis 30 hari Anda untuk EKS sumber daya Amazon.
- Paket perlindungan Runtime Monitoring diaktifkan pada tingkat akun per Wilayah. Setelah agen GuardDuty keamanan diterapkan ke salah satu jenis sumber daya yang ditentukan (EC2 instans Amazon dan ECS klaster Amazon), uji coba gratis 30 hari dimulai saat GuardDuty menerima peristiwa runtime pertama yang terkait dengan sumber daya. Ada uji coba gratis 30 hari yang terkait dengan setiap jenis sumber daya.

Misalnya, setelah mengaktifkan Runtime Monitoring, Anda memilih untuk menerapkan GuardDuty agen hanya di EC2 instans Amazon, uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai saat GuardDuty menerima peristiwa runtime pertamanya untuk instans Amazon. EC2 Kemudian, saat Anda menerapkan GuardDuty agen untuk Fargate (khusus ECS Amazon), uji coba gratis 30 hari untuk sumber daya ini hanya akan dimulai GuardDuty saat menerima acara runtime pertamanya untuk klaster Amazon. ECS Mengingat Anda sudah mengaktifkan EKS Runtime

Monitoring untuk akun Anda, GuardDuty tidak mengatur ulang uji coba gratis 30 hari untuk sumber daya AmazonEKS.

## Konsep kunci - Pendekatan untuk mengelola agen GuardDuty keamanan

Pertimbangkan konsep kunci yang akan membantu Anda mengelola agen keamanan di EKS cluster Amazon dan kluster Amazon ECS Anda.

### Daftar Isi

- [Sumber daya Fargate \(ECSkhusus Amazon\) - Pendekatan untuk mengelola agen keamanan GuardDuty](#)
- [EKSCluster Amazon - Pendekatan untuk mengelola agen GuardDuty keamanan](#)

## Sumber daya Fargate (ECSkhusus Amazon) - Pendekatan untuk mengelola agen keamanan GuardDuty

Runtime Monitoring memberi Anda opsi untuk mendeteksi potensi ancaman keamanan pada semua ECS kluster Amazon (tingkat akun) atau kluster selektif (tingkat kluster) di akun Anda. Saat Anda mengaktifkan konfigurasi agen Otomatis untuk setiap tugas Amazon ECS Fargate yang akan dijalankan, GuardDuty akan menambahkan wadah sespan untuk setiap beban kerja kontainer dalam tugas tersebut. Agen GuardDuty keamanan akan dikerahkan ke wadah sespan ini. Beginilah cara GuardDuty mendapatkan visibilitas ke dalam perilaku runtime container di dalam tugas AmazonECS.

Runtime Monitoring mendukung pengelolaan agen keamanan untuk ECS kluster Amazon Anda (AWS Fargate) hanya melalui GuardDuty. Tidak ada dukungan untuk mengelola agen keamanan secara manual di ECS cluster Amazon.

Sebelum mengonfigurasi akun, nilai bagaimana Anda ingin mengelola agen GuardDuty keamanan dan berpotensi memantau perilaku runtime kontainer yang termasuk dalam ECS tugas Amazon. Pertimbangkan pendekatan berikut.

### Topik

- [Kelola agen GuardDuty keamanan untuk semua ECS cluster Amazon](#)
- [Kelola agen GuardDuty keamanan untuk sebagian besar ECS cluster Amazon tetapi kecualikan beberapa kluster Amazon ECS](#)

- [Kelola agen GuardDuty keamanan untuk kluster Amazon ECS selektif](#)

## Kelola agen GuardDuty keamanan untuk semua ECS cluster Amazon

Pendekatan ini akan membantu Anda mendeteksi potensi ancaman keamanan di tingkat akun. Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk semua ECS kluster Amazon milik akun Anda.

## Kelola agen GuardDuty keamanan untuk sebagian besar ECS cluster Amazon tetapi kecualikan beberapa kluster Amazon ECS

Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk sebagian besar ECS kluster Amazon di AWS lingkungan Anda, tetapi kecualikan beberapa kluster. Pendekatan ini membantu Anda memantau perilaku runtime container dalam ECS tugas Amazon Anda di tingkat kluster. Misalnya, jumlah ECS cluster Amazon milik akun Anda adalah 1000. Namun, Anda hanya ingin memantau 930 ECS cluster Amazon.

Pendekatan ini mengharuskan Anda untuk menambahkan GuardDuty tag yang telah ditentukan sebelumnya ke ECS cluster Amazon yang tidak ingin Anda pantau. Untuk informasi selengkapnya, lihat [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#).

## Kelola agen GuardDuty keamanan untuk kluster Amazon ECS selektif

Gunakan pendekatan ini saat Anda GuardDuty ingin mendeteksi potensi ancaman keamanan untuk beberapa ECS kluster Amazon. Pendekatan ini membantu Anda memantau perilaku runtime container dalam ECS tugas Amazon Anda di tingkat kluster. Misalnya, jumlah ECS cluster Amazon milik akun Anda adalah 1000. Namun, Anda ingin memantau 230 cluster saja.

Pendekatan ini mengharuskan Anda untuk menambahkan GuardDuty tag yang telah ditentukan sebelumnya ke ECS cluster Amazon yang ingin Anda pantau. Untuk informasi selengkapnya, lihat [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#).

## EKSCluster Amazon - Pendekatan untuk mengelola agen GuardDuty keamanan

GuardDuty Untuk mengkonsumsi peristiwa runtime dari EKS cluster Anda di tingkat akun atau tingkat kluster, diperlukan untuk mengelola agen GuardDuty keamanan untuk cluster yang sesuai.

## Pendekatan untuk mengelola agen GuardDuty keamanan

Sebelum 13 September 2023, Anda dapat mengonfigurasi GuardDuty untuk mengelola agen keamanan di tingkat akun. Perilaku ini menunjukkan bahwa secara default, GuardDuty akan mengelola agen keamanan pada semua EKS cluster milik. Akun AWS Sekarang, GuardDuty berikan kemampuan granular untuk membantu Anda memilih EKS cluster tempat Anda GuardDuty ingin mengelola agen keamanan.

Ketika Anda memilih untuk [Kelola agen GuardDuty keamanan secara manual](#), Anda masih dapat memilih EKS cluster yang ingin Anda pantau. Namun, untuk mengelola agen secara manual, membuat VPC titik akhir Amazon untuk Anda Akun AWS adalah prasyarat.

### Note

Terlepas dari pendekatan yang Anda gunakan untuk mengelola agen GuardDuty keamanan, EKS Runtime Monitoring selalu diaktifkan di tingkat akun.

### Topik

- [Mengelola agen keamanan melalui GuardDuty](#)
- [Kelola agen GuardDuty keamanan secara manual](#)

### Mengelola agen keamanan melalui GuardDuty

GuardDuty menyebarkan dan mengelola agen keamanan atas nama Anda. Kapan saja, Anda dapat memantau EKS cluster di akun Anda dengan menggunakan salah satu pendekatan berikut.

### Topik

- [Pantau semua EKS cluster](#)
- [Pantau semua EKS cluster dan kecualikan cluster selektif EKS](#)
- [Pantau kluster selektif EKS](#)

### Pantau semua EKS cluster

- Kapan menggunakan pendekatan ini — Gunakan pendekatan ini ketika Anda GuardDuty ingin menyebarkan dan mengelola agen keamanan untuk semua EKS cluster di akun Anda. Secara

default, juga GuardDuty akan menyebarkan agen keamanan pada EKS kluster baru yang berpotensi dibuat di akun Anda.

- Dampak menggunakan pendekatan ini:
  - GuardDuty membuat titik akhir Amazon Virtual Private Cloud (AmazonVPC) tempat agen GuardDuty keamanan mengirimkan peristiwa runtime. GuardDuty Tidak ada biaya tambahan untuk pembuatan VPC endpoint Amazon saat Anda mengelola agen keamanan melalui GuardDuty.
  - Diperlukan bahwa node pekerja Anda memiliki jalur jaringan yang valid ke `guardduty-data` VPC titik akhir aktif. GuardDuty menyebarkan agen keamanan di EKS cluster Anda. Amazon Elastic Kubernetes Service (EKSAman) akan mengoordinasikan penyebaran agen keamanan pada node dalam cluster. EKS
  - Atas dasar ketersediaan IP, GuardDuty pilih subnet untuk membuat titik akhir. VPC Jika Anda menggunakan topologi jaringan tingkat lanjut, Anda harus memvalidasi bahwa konektivitas dimungkinkan.
- Pertimbangan — Saat ini, saat Anda menggunakan opsi ini, EKS Runtime Monitoring tidak membuat shared. VPC

#### Pantau semua EKS cluster dan kecualikan cluster selektif EKS

- Kapan menggunakan pendekatan ini — Gunakan pendekatan ini ketika Anda ingin GuardDuty mengelola agen keamanan untuk semua EKS cluster di akun Anda tetapi kecualikan kluster selektif EKS. Metode ini menggunakan pendekatan berbasis tag <sup>1</sup> di mana Anda dapat menandai EKS cluster yang Anda tidak ingin menerima peristiwa runtime. Tag yang telah ditentukan harus memiliki `GuardDutyManaged - false` sebagai pasangan kunci-nilai.
- Dampak menggunakan pendekatan ini:
  - Pendekatan ini mengharuskan Anda untuk mengaktifkan manajemen otomatis GuardDuty agen hanya setelah menambahkan tag ke EKS cluster yang ingin Anda kecualikan dari pemantauan.

Oleh karena itu, dampaknya ketika Anda [Mengelola agen keamanan melalui GuardDuty](#) menerapkan pendekatan ini juga. Saat Anda menambahkan tag sebelum mengaktifkan manajemen otomatis GuardDuty agen, tidak GuardDuty akan menyebarkan atau mengelola agen keamanan untuk EKS kluster yang dikecualikan dari pemantauan.
- Pertimbangan:



- Anda harus menambahkan pasangan nilai kunci tag sebagai `GuardDutyManaged: false` untuk EKS kluster selektif sebelum mengaktifkan konfigurasi agen Otomatis jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster hingga Anda menggunakan tag.
- Anda harus mencegah tag diubah, kecuali oleh identitas tepercaya.

#### Important

Mengelola izin untuk mengubah nilai `GuardDutyManaged` tag untuk EKS kluster Anda dengan menggunakan kebijakan atau IAM kebijakan kontrol layanan. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan \(SCPs\)](#) di Panduan AWS Organizations Pengguna atau [Kontrol akses ke AWS sumber daya](#) di Panduan IAM Pengguna.

- Untuk EKS kluster yang berpotensi baru yang tidak ingin Anda pantau, pastikan untuk menambahkan pasangan `GuardDutyManaged - false` kunci-nilai pada saat membuat cluster ini EKS.
- Pendekatan ini juga akan memiliki pertimbangan yang sama seperti yang ditentukan untuk [Pantau semua EKS cluster](#).

## Pantau kluster selektif EKS

- Kapan menggunakan pendekatan ini — Gunakan pendekatan ini saat Anda GuardDuty ingin menerapkan dan mengelola pembaruan ke agen keamanan hanya untuk EKS kluster selektif di akun Anda. Metode ini menggunakan pendekatan berbasis tag <sup>1</sup> di mana Anda dapat menandai EKS cluster yang ingin Anda terima peristiwa runtime.
- Dampak menggunakan pendekatan ini:
  - Dengan menggunakan tag inklusi, secara otomatis GuardDuty akan menyebarkan dan mengelola agen keamanan hanya untuk EKS cluster selektif yang ditandai dengan `GuardDutyManaged - true` sebagai pasangan kunci-nilai.
  - Menggunakan pendekatan ini juga akan memiliki dampak yang sama seperti yang ditentukan untuk [Pantau semua EKS cluster](#).
- Pertimbangan:
  - Jika nilai `GuardDutyManaged` tag tidak disetel ke `true`, tag penyertaan tidak akan berfungsi seperti yang diharapkan dan ini dapat memengaruhi pemantauan EKS kluster Anda.
  - Untuk memastikan bahwa EKS kluster selektif Anda sedang dipantau, Anda perlu mencegah tag diubah, kecuali oleh identitas tepercaya.

**⚠ Important**

Mengelola izin untuk mengubah nilai GuardDutyManaged tag untuk EKS kluster Anda dengan menggunakan kebijakan atau IAM kebijakan kontrol layanan. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan \(SCPs\)](#) di Panduan AWS Organizations Pengguna atau [Kontrol akses ke AWS sumber daya](#) di Panduan IAM Pengguna.

- Untuk EKS kluster yang berpotensi baru yang tidak ingin Anda pantau, pastikan untuk menambahkan pasangan GuardDutyManaged - false kunci-nilai pada saat membuat cluster ini EKS.
- Pendekatan ini juga akan memiliki pertimbangan yang sama seperti yang ditentukan untuk [Pantau semua EKS cluster](#).

<sup>1</sup> Untuk informasi selengkapnya tentang menandai EKS kluster selektif, lihat [Menandai sumber daya EKS Amazon Anda](#) di Panduan Pengguna Amazon EKS.

### Kelola agen GuardDuty keamanan secara manual

- Kapan menggunakan pendekatan ini — Gunakan pendekatan ini saat Anda ingin menyebarkan dan mengelola agen GuardDuty keamanan di semua EKS cluster Anda secara manual. Pastikan EKS Runtime Monitoring diaktifkan untuk akun Anda. Agen GuardDuty keamanan mungkin tidak berfungsi seperti yang diharapkan jika Anda tidak mengaktifkan EKS Runtime Monitoring.
- Dampak menggunakan pendekatan ini — Anda perlu mengoordinasikan penyebaran perangkat lunak agen GuardDuty keamanan dalam EKS cluster Anda di semua akun dan di Wilayah AWS mana fitur ini tersedia.
- Pertimbangan — Anda harus mendukung aliran data yang aman sambil memantau dan mengatasi kesenjangan cakupan karena kluster dan beban kerja baru terus digunakan.

## Mengaktifkan GuardDuty Runtime Monitoring

Sebelum mengaktifkan Runtime Monitoring di akun Anda, pastikan bahwa jenis sumber daya yang ingin Anda pantau peristiwa runtime, mendukung persyaratan platform. Untuk informasi selengkapnya, lihat [Prasyarat](#).

Jika Anda telah menggunakan EKS Runtime Monitoring sebelum peluncuran Runtime Monitoring, Anda dapat menggunakan APIs untuk memeriksa dan memperbarui konfigurasi yang ada untuk EKS Runtime Monitoring. Anda juga dapat memigrasikan konfigurasi yang ada dari EKS Runtime Monitoring ke Runtime Monitoring. Untuk informasi selengkapnya, lihat [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

#### Note

Saat ini, dokumentasi ini menyediakan langkah-langkah untuk mengaktifkan Runtime Monitoring untuk akun dan organisasi Anda hanya berdasarkan konsol. Anda juga dapat mengaktifkan Runtime Monitoring dengan menggunakan [APIActions](#) atau [AWS CLI for GuardDuty](#).

Anda dapat mengonfigurasi Runtime Monitoring dengan menggunakan langkah-langkah dalam topik berikut.

#### Daftar Isi

- [Prasyarat untuk mengaktifkan Runtime Monitoring](#)
- [Mengaktifkan Runtime Monitoring untuk akun mandiri](#)
- [Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun](#)
- [Mengelola agen GuardDuty keamanan](#)

## Prasyarat untuk mengaktifkan Runtime Monitoring

Untuk mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan, Anda harus memenuhi prasyarat untuk setiap jenis sumber daya yang ingin Anda pantau untuk deteksi ancaman.

#### Daftar Isi

- [Prasyarat untuk dukungan instans Amazon EC2](#)
- [Prasyarat untuk dukungan \(khusus AWS Fargate Amazon\) ECS](#)
- [Prasyarat untuk dukungan cluster Amazon EKS](#)
- [Menggunakan Infrastructure as Code \(IaC\) dengan GuardDuty agen keamanan otomatis](#)

## Prasyarat untuk dukungan instans Amazon EC2

Buat EC2 instance dikelola SSM

EC2Instans Amazon yang GuardDuty ingin Anda pantau peristiwa runtime harus dikelola AWS Systems Manager (SSM). Ini terlepas dari apakah Anda menggunakan GuardDuty untuk mengelola agen keamanan secara otomatis atau mengelolanya secara manual (kecuali [Metode 2 - Dengan menggunakan Linux Package Managers](#)).

Untuk mengelola EC2 instans Amazon Anda AWS Systems Manager, lihat [Menyiapkan Systems Manager untuk EC2 instans Amazon](#) di AWS Systems Manager Panduan Pengguna.

Memvalidasi persyaratan arsitektur

Arsitektur distribusi OS Anda dapat memengaruhi perilaku agen GuardDuty keamanan. Anda harus memenuhi persyaratan berikut sebelum menggunakan Runtime Monitoring untuk EC2 instans Amazon:

- Tabel berikut menunjukkan distribusi OS yang telah diverifikasi untuk mendukung agen GuardDuty keamanan untuk EC2 instans Amazon.

| Distribusi OS   | Versi kernel                   | Dukungan kernel            | CPUarsitektur |                   |
|---|--------------------------------|----------------------------|---------------|-------------------|
|   |                                |                            | x64 () AMD64  | Graviton () ARM64 |
| <ul style="list-style-type: none"> <li>• AL2dan AL2023</li> <li>• Ubuntu 20.04 dan Ubuntu 22.04</li> <li>• Debian 11 dan Debian 12</li> </ul> | 5.4, 5.10, 5.15, 6.1, 6.5, 6.8 | eBPF, Tracepoin ts, Kprobe | Didukung      | Didukung          |

- Persyaratan tambahan - Hanya jika Anda memiliki ECS Amazon/Amazon EC2

Untuk ECS Amazon/AmazonEC2, kami menyarankan Anda menggunakan Amazon terbaru yang ECS dioptimalkan AMIs (tertanggal 29 September 2023 atau lebih baru), atau gunakan ECS agen Amazon versi v1.77.0.

## Memvalidasi kebijakan kontrol layanan organisasi Anda

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin tidak membatasi. `guardduty:SendSecurityTelemetry` Hal ini diperlukan GuardDuty untuk mendukung Runtime Monitoring di berbagai jenis sumber daya.

Jika Anda adalah akun anggota, hubungi dengan administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCPs organisasi Anda, lihat [Kebijakan kontrol layanan \(SCPs\)](#).

## Saat menggunakan konfigurasi agen otomatis

Untuk [Gunakan konfigurasi agen otomatis \(disarankan\)](#), Anda Akun AWS harus memenuhi prasyarat berikut:

- Saat menggunakan tag inklusi dengan konfigurasi agen otomatis, GuardDuty untuk membuat SSM asosiasi untuk instance baru, pastikan instans baru SSM dikelola dan ditampilkan di bawah Fleet Manager di <https://console.aws.amazon.com/systems-manager/konsol>.
- Saat menggunakan tag pengecualian dengan konfigurasi agen otomatis:
  - Tambahkan `false` tag `GuardDutyManaged`: sebelum mengonfigurasi agen GuardDuty otomatis untuk akun Anda.

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

- Agar tag pengecualian berfungsi, perbarui konfigurasi instance sehingga dokumen identitas instance tersedia di layanan metadata instance (). IMDS Prosedur untuk melakukan langkah ini sudah menjadi bagian dari [Mengaktifkan Runtime Monitoring](#) akun Anda.

## CPU dan batas memori untuk GuardDuty agen

### CPU batasi

CPU Batas maksimum untuk agen GuardDuty keamanan yang terkait dengan EC2 instans Amazon adalah 10 persen dari total v CPU core. Misalnya, jika EC2 instans Anda memiliki 4 v CPU core, maka agen keamanan dapat menggunakan maksimum 40 persen dari total 400 persen yang tersedia.

## Batas memori

Dari memori yang terkait dengan EC2 instans Amazon Anda, ada memori terbatas yang dapat digunakan agen GuardDuty keamanan.

Tabel berikut menunjukkan batas memori.

| Memori EC2 instance Amazon        | Memori maksimum untuk GuardDuty agen |
|-----------------------------------|--------------------------------------|
| Kurang dari 8 GB                  | 128 MB                               |
| Kurang dari 32 GB                 | 270 MB                               |
| Lebih dari atau sama dengan 32 GB | 1 GB                                 |

### Langkah selanjutnya

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengelola agen keamanan (secara otomatis atau manual).

## Prasyarat untuk dukungan (khusus AWS Fargate Amazon) ECS

### Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari ECS kluster Amazon Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi.

### Pertimbangan awal:

AWS Fargate (Fargate) Platform untuk ECS cluster Amazon Anda harus Linux. Versi platform yang sesuai harus setidaknya 1.4.0, atau LATEST. Untuk informasi selengkapnya tentang versi platform, lihat [versi platform Linux](#) di Panduan Pengembang Layanan Amazon Elastic Container.

Versi platform Windows belum didukung.

### Platform terverifikasi

Distribusi dan CPU arsitektur OS berdampak pada dukungan yang diberikan oleh agen GuardDuty keamanan. Tabel berikut menunjukkan konfigurasi terverifikasi untuk menerapkan agen GuardDuty keamanan dan mengonfigurasi Runtime Monitoring.

| Distribusi OS | Dukungan kernel           | CPUarsitektur |                   |
|---------------|---------------------------|---------------|-------------------|
|               |                           | x64 () AMD64  | Graviton () ARM64 |
| Linux         | eBPF, Tracepoints, Kprobe | Didukung      | Didukung          |

Berikan ECR izin dan detail subnet

Sebelum mengaktifkan Runtime Monitoring, Anda harus memberikan detail berikut:

Berikan peran eksekusi tugas dengan izin

Peran eksekusi tugas mengharuskan Anda memiliki izin Amazon Elastic Container Registry (Amazon ECR) tertentu. Anda dapat menggunakan kebijakan mazonECSTask ExecutionRolePolicy terkelola [A](#) atau menambahkan izin berikut ke TaskExecutionRole kebijakan Anda:

```
...
    "ecr:GetAuthorizationToken",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage",
...

```

Untuk lebih membatasi ECR izin Amazon, Anda dapat menambahkan ECR repositori Amazon URI yang menampung agen GuardDuty keamanan untuk (hanya AWS Fargate Amazon). ECS Untuk informasi selengkapnya, lihat [Repositori untuk GuardDuty agen di \(hanya AWS Fargate Amazon ECS\)](#).

Berikan detail subnet dalam definisi tugas

Anda dapat memberikan subnet publik sebagai masukan dalam definisi tugas Anda atau membuat titik ECR VPC akhir Amazon.

- Menggunakan opsi definisi tugas - Menjalankan [CreateService](#) dan [UpdateService](#) API sdi API Referensi Layanan Amazon Elastic Container mengharuskan Anda untuk meneruskan informasi subnet. Untuk informasi selengkapnya, lihat [definisi ECS tugas Amazon](#) di Panduan Pengembang Layanan Kontainer Elastis Amazon.

- Menggunakan opsi ECR VPC titik akhir Amazon - Menyediakan jalur jaringan ke Amazon ECR - Pastikan bahwa ECR repositori Amazon URI yang menampung agen GuardDuty keamanan dapat diakses jaringan. Jika tugas Fargate Anda akan berjalan di subnet pribadi, maka Fargate akan membutuhkan jalur jaringan untuk mengunduh wadah. GuardDuty

Untuk informasi tentang mengaktifkan Fargate mengunduh penampung, lihat [Menggunakan GuardDuty gambar Amazon dengan Amazon di ECR Panduan Pengguna ECS Amazon](#) Elastic Container Registry.

## Memvalidasi kebijakan kontrol layanan organisasi Anda

Langkah ini diperlukan GuardDuty untuk mendukung Runtime Monitoring dan menilai cakupan di berbagai jenis sumber daya.

Jika Anda telah menyiapkan kebijakan kontrol layanan (SCP) untuk mengelola izin di organisasi Anda, validasi bahwa batas izin tidak membatasi `guardduty:SendSecurityTelemetry` dalam kebijakan Anda dan kebijakannya. `TaskExecutionRole`

Kebijakan berikut adalah contoh untuk mengizinkan `guardduty:SendSecurityTelemetry` kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        ...,
        ...,
        "guardduty:SendSecurityTelemetry"
      ],
      "Resource": "*"
    }
  ]
}
```

1. Gunakan langkah-langkah berikut untuk memvalidasi bahwa batas izin tidak membatasi: `guardduty:SendSecurityTelemetry`



1. Masuk ke AWS Management Console dan buka IAM konsol di <https://console.aws.amazon.com/iam/>.
  2. Di panel navigasi, di bawah Manajemen akses, pilih Peran.
  3. Pilih nama Peran untuk halaman detail.
  4. Perluas bagian batas Izin. Pastikan bahwa `guardduty:SendSecurityTelemetry` tidak ditolak atau dibatasi.
2. Gunakan langkah-langkah berikut untuk memvalidasi bahwa batas Izin untuk `TaskExecutionRole` kebijakan Anda tidak membatasi: `guardduty:SendSecurityTelemetry`
1. Masuk ke AWS Management Console dan buka IAM konsol di <https://console.aws.amazon.com/iam/>.
  2. Di panel navigasi, di bawah Manajemen akses, pilih Kebijakan.
  3. Pilih nama Kebijakan untuk halaman detail.
  4. Di bawah tab Entitas terlampir, lihat bagian Terlampir sebagai batas izin. Pastikan bahwa `guardduty:SendSecurityTelemetry` tidak ditolak atau dibatasi.

Untuk informasi tentang kebijakan dan izin, lihat [Batas izin](#) di IAMPanduan Pengguna.

Jika Anda adalah akun anggota, hubungi dengan administrator yang didelegasikan terkait. Untuk informasi tentang mengelola SCPs organisasi Anda, lihat [Kebijakan kontrol layanan \(SCPs\)](#).

### CPU dan batas memori

Dalam definisi tugas Fargate, Anda harus menentukan nilai CPU dan memori di tingkat tugas. Tabel berikut menunjukkan kombinasi yang valid dari tingkat tugas CPU dan nilai memori, dan batas memori maksimum agen GuardDuty keamanan yang sesuai untuk wadah. GuardDuty

| CPU nilai      | Nilai memori           | GuardDuty batas memori maksimum agen |
|----------------|------------------------|--------------------------------------|
| 256 (.25 vCPU) | 512 MiB, 1 GB, 2GB     | 128 MB                               |
| 512 (.5 v) CPU | 1 GB, 2 GB, 3 GB, 4 GB |                                      |
| 1024 (1 vCPU)  | 2 GB, 3 GB, 4 GB       |                                      |

| CPU nilai        | Nilai memori                                   | GuardDuty batas memori maksimum agen |
|------------------|--|--------------------------------------|
|                  | 5 GB, 6 GB, 7 GB, 8 GB                         |                                      |
| 2048 (2 vCPU)    | Antara 4 GB dan 16 GB dalam peningkatan 1 GB   |                                      |
| 4096 (4 vCPU)    | Antara 8 GB dan 20 GB dalam peningkatan 1 GB   |                                      |
| 8192 (8 v) CPU   | Antara 16 GB dan 28 GB dalam peningkatan 4 GB  | 270 MB                               |
|                  | Antara 32 GB dan 60 GB dalam peningkatan 4 GB  | 512 MB                               |
| 16384 (16 v) CPU | Antara 32 GB dan 120 GB dalam peningkatan 8 GB | 1 GB                                 |

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan kluster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan Container. Untuk informasi selengkapnya, lihat [Menyiapkan pemantauan di ECS kluster Amazon](#).

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring dan juga mengkonfigurasi agen keamanan.

## Prasyarat untuk dukungan cluster Amazon EKS

### Memvalidasi persyaratan arsitektur

Platform yang Anda gunakan dapat memengaruhi cara agen GuardDuty keamanan mendukung GuardDuty dalam menerima peristiwa runtime dari EKS cluster Anda. Anda harus memvalidasi bahwa Anda menggunakan salah satu platform terverifikasi. Jika Anda mengelola GuardDuty agen secara manual, pastikan bahwa versi Kubernetes mendukung versi GuardDuty agen yang sedang digunakan.

## Platform terverifikasi

Distribusi OS, versi kernel, dan CPU arsitektur memengaruhi dukungan yang diberikan oleh agen GuardDuty keamanan. Tabel berikut menunjukkan konfigurasi terverifikasi untuk menerapkan agen GuardDuty keamanan dan mengonfigurasi EKS Runtime Monitoring.

| Distribusi OS       | Versi kernel                      | Dukungan kernel           | CPU arsitektur |   | Versi Kubernetes yang didukung |
|---------------------|-----------------------------------|---------------------------|----------------|---|--------------------------------|
|                     |                                   |                           | x64 () AMD64   | Graviton () ARM64<br>(Graviton2 dan di atas) <sup>1</sup> |                                |
| Ubuntu AL2          | 5.4, 5.10, 5.15, 6.1 <sup>2</sup> | e BPF Titik jejak, Kprobe | Didukung       | Didukung  | v1.21 - v1.30                  |
| AL2023 <sup>3</sup> |                                   |                           |                |   |                                |
| Bottlerocket        |                                   |                           |                |   | v1.23 - v1.30                  |

- Runtime Monitoring untuk EKS kluster Amazon tidak mendukung instans Graviton generasi pertama seperti tipe instans A1.
- Saat ini, dengan versi Kernel 6.1, tidak GuardDuty dapat menghasilkan [Jenis penemuan Runtime Monitoring](#) yang terkait [DNSacara](#) dengan.
- Runtime Monitoring mendukung AL2 023 dengan rilis agen GuardDuty keamanan v1.6.0 ke atas. Untuk informasi selengkapnya, lihat [GuardDuty agen keamanan untuk EKS cluster Amazon](#).

Versi Kubernetes didukung oleh agen keamanan GuardDuty

Tabel berikut menunjukkan versi Kubernetes untuk EKS kluster Anda yang didukung oleh agen keamanan. GuardDuty

| Versi Kubernetes | Versi agen GuardDuty keamanan EKS add-on Amazon |
|------------------|---|
| 1,28 - 1,30      | v1.4.1 dan yang lebih baru                      |
| 1.27             | v1.3.0, v1.3.1                                  |
| 1.26             | v1.2.0  |
| 1,21 - 1,25      | Semua versi                                     |

Beberapa versi agen GuardDuty keamanan akan mencapai akhir dukungan standar. Untuk informasi tentang versi rilis agen, lihat [GuardDuty agen keamanan untuk EKS cluster Amazon](#).

CPU dan batas memori

Tabel berikut menunjukkan batas memori CPU dan untuk EKS add-on Amazon for GuardDuty (aws-guardduty-agent).

| Parameter | Batas minimum | Batas maksimum |
|-----------|---------------|----------------|
| CPU       | 200m          | 1000m          |
| Memori    | 257 Mi        | 1024 Mi        |

Saat Anda menggunakan EKS add-on Amazon versi 1.5.0 atau yang lebih baru, GuardDuty menyediakan kemampuan untuk mengonfigurasi skema add-on untuk nilai memori dan Anda CPU. Untuk informasi tentang rentang yang dapat dikonfigurasi, lihat [Parameter dan nilai yang dapat dikonfigurasi](#).

Setelah mengaktifkan EKS Runtime Monitoring dan menilai status cakupan EKS kluster, Anda dapat menyiapkan dan melihat metrik wawasan container. Untuk informasi selengkapnya, lihat [Pengaturan CPU dan pemantauan memori](#).

Langkah selanjutnya

Langkah selanjutnya adalah mengkonfigurasi Runtime Monitoring, dan juga mengelola agen keamanan baik secara manual maupun otomatis. GuardDuty

## Menggunakan Infrastructure as Code (IAC) dengan GuardDuty agen keamanan otomatis

Gunakan bagian ini hanya jika daftar berikut berlaku untuk kasus penggunaan Anda:

- Anda menggunakan alat Infrastructure as Code (IAC), seperti AWS Cloud Development Kit (AWS CDK) dan Terraform, untuk mengelola sumber daya Anda AWS, dan
- Anda perlu mengaktifkan konfigurasi agen GuardDuty otomatis untuk satu atau beberapa jenis sumber daya - AmazonEKS, AmazonEC2, atau Amazon ECS -Fargate.

### Ikhtisar grafik ketergantungan sumber daya IAC

Saat Anda mengaktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya, GuardDuty secara otomatis membuat VPC titik akhir dan grup keamanan yang terkait dengan VPC titik akhir ini, dan menginstal agen keamanan untuk jenis sumber daya ini. Secara default, GuardDuty akan menghapus VPC endpoint dan grup keamanan terkait hanya setelah Anda menonaktifkan Runtime Monitoring. Untuk informasi selengkapnya, lihat [Dampak menonaktifkan dan membersihkan sumber daya](#).

Ketika Anda menggunakan alat IAC, ia mempertahankan grafik ketergantungan sumber daya. Pada saat penghapusan sumber daya menggunakan alat IAC, itu hanya menghapus sumber daya yang dapat dilacak sebagai bagian dari grafik ketergantungan sumber daya. Alat IAC mungkin tidak tahu tentang sumber daya yang dibuat di luar konfigurasi yang ditentukan. Misalnya, Anda membuat VPC dengan alat IAC dan kemudian menambahkan grup keamanan ke ini VPC dengan menggunakan AWS konsol atau API operasi. Dalam grafik ketergantungan sumber daya, VPC sumber daya yang Anda buat bergantung pada grup keamanan terkait. Jika Anda menghapus VPC sumber daya ini dengan menggunakan alat IAC, maka Anda akan mendapatkan kesalahan. Cara untuk mengatasi kesalahan ini adalah dengan menghapus grup keamanan terkait secara manual atau memperbarui konfigurasi IAC untuk memasukkan sumber daya tambahan ini.

### Masalah umum - Menghapus sumber daya di IAC

Saat menggunakan konfigurasi agen GuardDuty otomatis, Anda mungkin ingin menghapus sumber daya (AmazonEKS, AmazonEC2, atau Amazon ECS -Fargate) yang Anda buat dengan menggunakan alat IAC. Namun, sumber daya ini bergantung pada VPC titik akhir yang GuardDuty dibuat. Ini mencegah alat IAC untuk menghapus sumber daya dengan sendirinya dan mengharuskan Anda untuk menonaktifkan Runtime Monitoring, yang selanjutnya menghapus titik akhir secara otomatis. VPC

Misalnya, ketika Anda mencoba menghapus VPC titik akhir yang GuardDuty dibuat atas nama Anda, Anda akan mendapatkan kesalahan yang mirip dengan contoh berikut.

## Example

### Contoh kesalahan saat menggunakan CDK

The following resource(s) failed to delete:

```
[mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subnet1SubnetEXAMPLE1]
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPLE)
HandlerErrorCode: InvalidRequest)
```

## Example

### Contoh kesalahan saat menggunakan Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE, 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE, 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

## Solusi - Mencegah masalah penghapusan sumber daya

Bagian ini membantu Anda mengelola VPC endpoint dan grup keamanan secara independen.

### GuardDuty

Untuk mendapatkan kepemilikan penuh atas sumber daya yang dikonfigurasi dengan menggunakan alat IAC, lakukan langkah-langkah berikut dalam urutan yang tercantum:

1. Buat aVPC. Untuk mengizinkan izin masuk, kaitkan GuardDuty VPC titik akhir dengan grup keamanan, ke ini. VPC
2. Aktifkan konfigurasi agen GuardDuty otomatis untuk jenis sumber daya Anda

Setelah Anda menyelesaikan langkah-langkah sebelumnya, tidak GuardDuty akan membuat VPC endpoint sendiri dan akan menggunakan kembali salah satu yang Anda buat dengan menggunakan alat IAc.

Untuk informasi tentang membuat sendiri VPC, lihat [Membuat VPC hanya](#) di Gateway VPC Transit Amazon. Untuk informasi tentang membuat VPC titik akhir, lihat bagian berikut untuk jenis sumber daya Anda:

- Untuk Amazon EC2, lihat [Membuat VPC titik akhir Amazon secara manual](#).
- Untuk Amazon EKS, lihat [Prasyarat untuk menyebarkan agen keamanan GuardDuty](#).

## Mengaktifkan Runtime Monitoring untuk akun mandiri

Gunakan langkah-langkah berikut untuk mengaktifkan Runtime Monitoring di akun Anda.

### Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan Runtime Monitoring untuk akun Anda.
4. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya Amazon ECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

## Mengaktifkan Runtime Monitoring untuk lingkungan multi-akun

Di lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Runtime Monitoring untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk jenis sumber daya milik akun anggota di organisasinya.

Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Untuk akun GuardDuty administrator yang didelegasikan

Untuk mengaktifkan Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Menggunakan Aktifkan untuk semua akun

Jika Anda ingin mengaktifkan Runtime Monitoring untuk semua akun milik organisasi, termasuk akun GuardDuty administrator yang didelegasikan, pilih Aktifkan untuk semua akun.

5. Menggunakan Konfigurasi akun secara manual

Jika Anda ingin mengaktifkan Runtime Monitoring untuk setiap akun anggota satu per satu, lalu pilih Konfigurasi akun secara manual.

- Pilih Aktifkan di bawah bagian Administrator Delegasi (akun ini).

6. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)



- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

Untuk semua akun anggota

Untuk mengaktifkan Runtime Monitoring untuk semua akun anggota di organisasi

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Pada halaman Runtime Monitoring, di bawah tab Configuration, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Aktifkan untuk semua akun.
5. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

Untuk semua akun anggota aktif yang ada

Untuk mengaktifkan Runtime Monitoring untuk akun anggota yang ada di organisasi

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.


Masuk menggunakan akun GuardDuty administrator yang didelegasikan untuk organisasi.

2. Di panel navigasi, pilih Runtime Monitoring.

3. Pada halaman Runtime Monitoring, di bawah tab Configuration, Anda dapat melihat status konfigurasi Runtime Monitoring saat ini.
4. Dalam panel Runtime Monitoring, di bawah bagian Account anggota aktif, pilih Tindakan.
5. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
6. Pilih Konfirmasi.
7. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Aktifkan otomatis Runtime Monitoring hanya untuk akun anggota baru

Untuk mengaktifkan Runtime Monitoring untuk akun anggota baru di organisasi Anda

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan akun GuardDuty administrator organisasi yang didelegasikan yang ditunjuk.

2. Di panel navigasi, pilih Runtime Monitoring
3. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.
4. Pilih Konfigurasikan akun secara manual.
5. Pilih Aktifkan secara otomatis untuk akun anggota baru.

6. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

Hanya untuk akun anggota aktif selektif

Untuk mengaktifkan Runtime Monitoring untuk akun anggota aktif individu

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau nilai di kolom Runtime Monitoring dan Manage agent secara otomatis. Nilai-nilai ini menunjukkan apakah Runtime Monitoring dan manajemen GuardDuty agen Diaktifkan atau Tidak diaktifkan untuk akun terkait.
4. Dari tabel Akun, pilih akun yang ingin Anda aktifkan Runtime Monitoring. Anda dapat memilih beberapa akun sekaligus.
5. Pilih Konfirmasi.
6. Pilih Edit paket perlindungan. Pilih tindakan yang sesuai.
7. Pilih Konfirmasi.
8. GuardDuty Untuk menerima peristiwa runtime dari satu atau beberapa jenis sumber daya — EC2 instans Amazon, ECS kluster Amazon, atau EKS kluster Amazon, gunakan opsi berikut untuk mengelola agen keamanan untuk sumber daya ini:

Untuk mengaktifkan agen GuardDuty keamanan

- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)

- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

## Mengelola agen GuardDuty keamanan

Anda dapat mengelola agen GuardDuty keamanan untuk sumber daya yang ingin Anda pantau. Jika Anda ingin memantau lebih dari satu jenis sumber daya, pastikan untuk mengelola GuardDuty agen untuk sumber daya tersebut.

### Important

Saat bekerja dengan agen GuardDuty keamanan untuk EC2 instans Amazon, Anda dapat menginstal dan menggunakan agen pada host yang mendasarinya dalam EKS kluster Amazon. Jika Anda telah menggunakan agen keamanan di EKS cluster itu, host yang sama dapat memiliki dua agen keamanan yang berjalan di dalamnya pada saat yang bersamaan. Untuk informasi tentang cara GuardDuty kerja dalam skenario ini, lihat [Menangani agen keamanan ganda](#).

Topik berikut akan membantu Anda dengan langkah selanjutnya untuk mengelola agen keamanan.

### Daftar Isi

- [Menggunakan berbagi VPC dengan agen keamanan otomatis](#)
- [Menangani agen keamanan ganda yang diinstal pada host](#)
- [Mengelola agen keamanan otomatis untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#)
- [Mengelola agen keamanan otomatis untuk Fargate \(hanya AmazonECS\)](#)
- [Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon](#)
- [Mengelola agen keamanan secara manual untuk EKS kluster Amazon](#)

## Menggunakan berbagi VPC dengan agen keamanan otomatis

Bila Anda memilih GuardDuty untuk mengelola agen keamanan secara otomatis, Runtime Monitoring mendukung penggunaan bersama VPC untuk Akun AWS yang dimiliki oleh organisasi yang sama di

AWS Organizations. Atas nama Anda, GuardDuty dapat mengatur kebijakan VPC titik akhir Amazon berdasarkan detail yang terkait dengan yang dibagikan VPC untuk organisasi Anda.

Sebelum rilis ini, GuardDuty mendukung penggunaan shared VPCs hanya ketika Anda memilih untuk mengelola agen GuardDuty keamanan secara manual.

## Daftar Isi

- [Cara kerjanya](#)
- [Prasyarat untuk menggunakan bersama VPC](#)
- [Pertanyaan yang sering diajukan \(FAQs\)](#)

## Cara kerjanya

Jika akun pemilik bersama VPC mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk salah satu sumber daya (Amazon EKS atau AWS Fargate (ECS) Amazon)), semua yang dibagikan VPCs menjadi memenuhi syarat untuk instalasi otomatis VPC titik akhir Amazon bersama dan grup keamanan terkait di akun VPC pemilik bersama. GuardDuty mengambil ID organisasi yang terkait dengan Amazon VPC bersama.

Sekarang, Akun AWS yang termasuk dalam organisasi yang sama dengan akun VPC pemilik Amazon bersama juga dapat berbagi VPC titik akhir Amazon yang sama. GuardDuty membuat berbagi VPC ketika akun VPC pemilik bersama atau akun yang berpartisipasi memerlukan VPC titik akhir Amazon. Contoh membutuhkan VPC endpoint Amazon termasuk mengaktifkan GuardDuty, Runtime Monitoring, Runtime Monitoring, EKS atau meluncurkan tugas Amazon -Fargate baru. ECS Jika akun ini mengaktifkan Pemantauan Waktu Proses dan konfigurasi agen otomatis untuk semua jenis sumber daya, GuardDuty buat VPC titik akhir Amazon dan tetapkan kebijakan titik akhir dengan ID organisasi yang sama dengan akun pemilik bersama VPC. GuardDuty menambahkan GuardDutyManaged tag dan menyetelnya `true` untuk VPC titik akhir Amazon yang GuardDuty dibuat. Jika akun VPC pemilik Amazon bersama belum mengaktifkan Runtime Monitoring atau konfigurasi agen otomatis untuk salah satu sumber daya, kebijakan VPC endpoint Amazon tidak GuardDuty akan ditetapkan. Untuk informasi tentang mengonfigurasi Runtime Monitoring dan mengelola agen keamanan secara otomatis di akun VPC pemilik bersama, lihat. [Mengaktifkan GuardDuty Runtime Monitoring](#)

Setiap akun yang menggunakan kebijakan VPC endpoint Amazon yang sama disebut sebagai AWS akun peserta Amazon VPC bersama terkait.

Contoh berikut menunjukkan kebijakan VPC titik akhir default dari akun VPC pemilik bersama dan akun peserta. Ini `aws:PrincipalOrgID` akan menampilkan ID organisasi yang terkait dengan VPC sumber daya bersama. Penggunaan kebijakan ini terbatas pada akun peserta yang ada dalam organisasi akun pemilik.

### Example

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "*",
    "Resource": "*",
    "Effect": "Allow",
    "Principal": "*"
  },
  {
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalOrgID": "o-abcdef0123"
      }
    },
    "Action": "*",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
  }
]
```

Prasyarat untuk menggunakan bersama VPC

Prasyarat untuk pengaturan awal

Lakukan langkah-langkah berikut di Akun AWS mana Anda ingin menjadi pemilik yang dibagikanVPC:

1. Membuat organisasi — Membuat organisasi dengan mengikuti langkah-langkah dalam [Membuat dan mengelola organisasi](#) dalam Panduan AWS Organizations Pengguna.

Untuk informasi tentang menambahkan atau menghapus akun anggota, lihat [Mengelola Akun AWS di organisasi Anda](#).

2. Membuat VPC sumber daya bersama — Anda dapat membuat VPC sumber daya bersama dari akun pemilik. Untuk informasi selengkapnya, lihat [Berbagi VPC dengan akun lain](#) di Panduan VPC Pengguna Amazon.

### Prasyarat khusus untuk Runtime Monitoring GuardDuty

Daftar berikut memberikan prasyarat yang khusus untuk: GuardDuty

- Akun pemilik akun bersama VPC dan akun yang berpartisipasi dapat berasal dari organisasi yang berbeda di GuardDuty. Namun, mereka harus menjadi anggota organisasi yang sama di AWS Organizations. Ini diperlukan GuardDuty untuk membuat VPC titik akhir Amazon dan grup keamanan untuk yang dibagikan VPC. Untuk informasi tentang cara VPCs kerja bersama, lihat [Berbagi VPC dengan akun lain](#) di Panduan VPC Pengguna Amazon.
- Aktifkan EKS Runtime Monitoring atau Runtime Monitoring, dan konfigurasi agen GuardDuty otomatis untuk sumber daya apa pun di akun VPC pemilik bersama dan akun peserta. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring](#).

Jika Anda telah menyelesaikan konfigurasi ini, lanjutkan dengan langkah berikutnya.

- Saat bekerja dengan tugas Amazon EKS atau Amazon ECS (AWS Fargate hanya), pastikan untuk memilih VPC sumber daya bersama yang terkait dengan akun pemilik dan pilih subnetnya.

### Pertanyaan yang sering diajukan (FAQs)

Daftar berikut menyediakan langkah-langkah pemecahan masalah untuk pertanyaan yang sering diajukan saat menggunakan VPC sumber daya bersama dengan konfigurasi agen GuardDuty otomatis di Runtime Monitoring:

Saya sudah menggunakan Runtime Monitoring (atau EKS Runtime Monitoring). Bagaimana cara mengaktifkan berbagi VPC?

Untuk informasi tentang prasyarat untuk membuat bersama, lihat. VPC [Prasyarat](#)

Ketika akun VPC pemilik bersama dan akun peserta telah memenuhi prasyarat, GuardDuty akan mencoba untuk menetapkan kebijakan endpoint Amazon VPC secara otomatis.

Jika sebelum rilis ini, Anda Akun AWS mengalami masalah cakupan tentang berbagi yang VPC tidak didukung, ikuti prasyarat. Saat jenis sumber daya Anda ECS (AWS Fargate hanya tugas Amazon EKS atau Amazon) memanggil persyaratan VPC titik akhir bersama, GuardDuty akan mencoba menyetel kebijakan titik VPC akhir yang baru.

Sebagai akun VPC pemilik bersama, saya ingin kebijakan VPC titik akhir bersama dibatasi pada subset akun peserta di organisasi saya. Bagaimana saya bisa melakukan itu?

Jika Anda memiliki `true` tagGuardDutyManaged: yang terkait dengan titik akhir, hapus. Hal ini mencegah GuardDuty untuk mencoba memodifikasi atau mengesampingkan kebijakan VPC endpoint dari shared. VPC

Untuk informasi selengkapnya, lihat [Mengontrol akses ke VPC titik akhir menggunakan kebijakan titik akhir](#).

Mengapa VPC titik akhir bersama berubah dari **aws:PrincipalAccount** ke **aws:PrincipalOrgId**? Bagaimana saya bisa mencegahnya?

Saat GuardDuty mendeteksi bahwa akun VPC dibagikan oleh beberapa akun dari organisasi yang sama AWS Organizations, GuardDuty mencoba mengubah kebijakan untuk menentukan ID organisasi.

Untuk mencegah hal ini, hapus `true` tagGuardDutyManaged: dari VPC titik akhir bersama. Hal ini mencegah GuardDuty untuk mencoba memodifikasi atau mengesampingkan kebijakan VPC endpoint dari shared. VPC

Apa yang terjadi jika akun VPC pemilik bersama atau salah satu akun peserta dinonaktifkan atau Runtime Monitoring ( GuardDuty atau Runtime Monitoring)EKS?

Saat akun VPC pemilik bersama dinonaktifkan GuardDuty atau Runtime Monitoring (atau EKS Runtime Monitoring), GuardDuty periksa apakah jenis sumber daya milik akun peserta telah menggunakan VPC titik akhir bersama atau akun peserta mana pun yang pernah mengaktifkan manajemen GuardDuty agen untuk jenis sumber daya apa pun. Jika ya, GuardDuty tidak akan menghapus VPC titik akhir dan grup keamanan.

Jika akun VPC peserta bersama menonaktifkan GuardDuty atau Runtime Monitoring (atau EKS Runtime Monitoring), maka tidak ada dampak pada akun VPC pemilik bersama dan akun pemilik tidak akan menghapus VPC sumber daya bersama maupun grup keamanan.

Bagaimana cara menghapus VPC sumber daya bersama? Apa yang akan menjadi dampaknya?

Sebagai akun VPC pemilik bersama, Anda dapat menghapus VPC sumber daya bersama meskipun sedang digunakan oleh akun Anda atau akun yang berpartisipasi dalam Runtime Monitoring. Untuk informasi tentang menghapus yang dibagikan VPC dan memahami dampaknya, lihat [To delete a VPC endpoint](#).



## Menangani agen keamanan ganda yang diinstal pada host

EC2Instans Amazon dapat mendukung berbagai jenis beban kerja. Saat Anda mengonfigurasi agen keamanan otomatis di EC2 instans Amazon, EC2 instans yang sama mungkin memiliki agen keamanan lainEKS.

### Gambaran Umum

Pertimbangkan skenario di mana Anda telah mengaktifkan Runtime Monitoring. Sekarang, Anda mengaktifkan agen otomatis untuk Amazon EKS melalui GuardDuty. Anda juga telah mengaktifkan agen otomatis untuk AmazonEC2. Mungkin saja host dasar yang sama dipasang dengan dua agen keamanan - satu untuk Amazon EKS dan yang lainnya untuk AmazonEC2. Hal ini dapat mengakibatkan dua agen keamanan berjalan di dalam host yang sama, mengumpulkan peristiwa runtime dan mengirimkannya ke GuardDuty, dan berpotensi menghasilkan temuan duplikat.

### Dampak

- Ketika ada lebih dari satu agen keamanan yang berjalan di host yang sama, akun Anda mungkin mengalami dua kali lipat jumlah CPU dan kebutuhan pemrosesan memori. Untuk informasi tentang batas CPU dan memori untuk setiap jenis sumber daya, lihat [Prasyarat](#) sumber daya tersebut.
- GuardDuty telah merancang fitur Runtime Monitoring sedemikian rupa sehingga meskipun ada tumpang tindih dua agen keamanan yang mengumpulkan peristiwa runtime dari host dasar yang sama, akun Anda hanya akan dikenakan biaya untuk satu aliran peristiwa runtime.

### Bagaimana GuardDuty menangani banyak agen

GuardDuty mendeteksi ketika dua agen keamanan berjalan pada host yang sama dan menunjuk hanya satu dari mereka untuk menjadi agen keamanan yang secara aktif mengumpulkan peristiwa runtime. Agen kedua akan mengkonsumsi sumber daya sistem minimum untuk mencegah dampak apa pun terhadap kinerja aplikasi Anda.

### GuardDuty mempertimbangkan skenario berikut:

- Ketika sebuah EC2 instance berada di bawah lingkup agen EC2 keamanan Amazon EKS dan Amazon, agen EKS keamanan mengambil prioritas. Ini hanya akan berlaku ketika Anda menggunakan agen keamanan v1.1.0 atau lebih tinggi untuk AmazonEC2. Versi agen yang lebih lama akan terus berjalan dan mengumpulkan peristiwa runtime karena versi agen yang lebih lama tidak terpengaruh oleh prioritas.

- Ketika Amazon EKS dan Amazon EC2 telah GuardDuty mengelola agen keamanan dan EC2 instans Amazon Anda juga SSM dikelola, kedua agen keamanan akan dipasang di tingkat host. Setelah agen diinstal, GuardDuty memutuskan agen keamanan mana yang akan terus berjalan. Ketika kedua agen keamanan berjalan, akhirnya hanya satu dari mereka yang akan mengumpulkan acara runtime.
- Ketika agen keamanan terkait dengan keduanya EC2 dan EKS berjalan pada saat yang sama, GuardDuty mungkin menghasilkan temuan duplikat selama periode tumpang tindih saja.

Ini bisa terjadi ketika:

- Agen keamanan untuk keduanya EC2 dan EKS dikonfigurasi melalui GuardDuty (secara otomatis), atau
- EKSSumber daya Amazon Anda memiliki agen keamanan otomatis.
- Ketika agen EKS keamanan sudah berjalan, jika Anda menyebarkan agen EC2 keamanan secara manual pada host dasar yang sama dan memenuhi semua prasyarat, GuardDuty mungkin tidak menginstal agen keamanan kedua.

## Mengelola agen keamanan otomatis untuk EC2 instans Amazon

### Note

Sebelum Anda melanjutkan, pastikan untuk mengikuti semua [Prasyarat untuk dukungan instans Amazon EC2](#).

### Migrasi dari agen EC2 manual Amazon ke agen otomatis

Bagian ini berlaku untuk Anda Akun AWS jika sebelumnya Anda mengelola agen keamanan secara manual dan sekarang ingin menggunakan konfigurasi agen GuardDuty otomatis. Jika ini tidak berlaku untuk Anda, lanjutkan dengan mengonfigurasi agen keamanan untuk akun Anda.

Ketika Anda mengaktifkan agen GuardDuty otomatis, GuardDuty mengelola agen keamanan atas nama Anda. Untuk informasi tentang langkah-langkah apa yang GuardDuty diambil, lihat [Gunakan konfigurasi agen otomatis \(disarankan\)](#).

## Pembersihan sumber daya

### Hapus SSM asosiasi

- Hapus SSM asosiasi apa pun yang mungkin telah Anda buat saat mengelola agen keamanan untuk Amazon EC2 secara manual. Untuk informasi selengkapnya, lihat [Menghapus asosiasi](#).
- Hal ini dilakukan agar GuardDuty dapat mengambil alih pengelolaan SSM tindakan apakah Anda menggunakan agen otomatis di tingkat akun atau tingkat instans (dengan menggunakan tag inklusi atau pengecualian). Untuk informasi selengkapnya tentang SSM tindakan apa yang dapat GuardDuty dilakukan, lihat [izin peran terkait layanan untuk GuardDuty](#).
- Ketika Anda menghapus SSM asosiasi yang sebelumnya dibuat untuk mengelola agen keamanan secara manual, mungkin ada periode singkat tumpang tindih ketika GuardDuty membuat SSM asosiasi untuk mengelola agen keamanan secara otomatis. Selama periode ini, Anda dapat mengalami konflik berdasarkan SSM penjadwalan. Untuk informasi selengkapnya, lihat [EC2SSMpenjadwalan Amazon](#).

### Mengelola tag inklusi dan pengecualian untuk instans Amazon EC2 Anda

- Tag penyertaan — Jika Anda tidak mengaktifkan konfigurasi agen GuardDuty otomatis tetapi menandai EC2 instans Amazon Anda dengan tag inklusi (`GuardDutyManaged:true`), GuardDuty buat SSM asosiasi yang akan menginstal dan mengelola agen keamanan pada EC2 instans yang dipilih. Ini adalah perilaku yang diharapkan yang membantu Anda mengelola agen keamanan hanya pada EC2 instans yang dipilih. Untuk informasi selengkapnya, lihat [Cara kerja Runtime Monitoring dengan instans Amazon EC2](#).

Untuk GuardDuty mencegah menginstal dan mengelola agen keamanan, hapus tag inklusi dari EC2 instance ini. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus tag](#) di Panduan EC2 Pengguna Amazon.

- Tag pengecualian — Saat Anda ingin mengaktifkan konfigurasi agen GuardDuty otomatis untuk semua EC2 instance di akun Anda, pastikan tidak ada EC2 instance yang ditandai dengan tag pengecualian (`:`). `GuardDutyManaged false`

## Mengkonfigurasi GuardDuty agen untuk akun mandiri

### Configure for all instances

Untuk mengonfigurasi Runtime Monitoring untuk semua instance di akun mandiri Anda

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Edit.
4. Di EC2 bagian ini, pilih Aktifkan.
5. Pilih Simpan.
6. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun Anda.
  - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
  - b. Buka tab Target untuk SSM asosiasi (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

### Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `true` tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.

Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.

- Buka tab Targets untuk SSM asosiasi yang akan dibuat (GuardDutyRuntimeMonitoring-do-not-delete). Tombol Tag muncul sebagai tag: GuardDutyManaged.

### Using exclusion tag in selected instances

#### Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk

AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
  - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.  
  
Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
  - b. Pilih contoh yang ingin Anda izinkan tag.
  - c. Di bawah menu Tindakan, pilih Pengaturan instans.
  - d. Pilih Izinkan tag dalam metadata contoh.
  - e. Di bawah Akses ke tag dalam metadata instance, pilih Izinkan.
  - f. Pilih Simpan.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan di tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan untuk EC2 instans Amazon](#).

Mengonfigurasi GuardDuty agen di lingkungan multi-akun

Untuk akun GuardDuty administrator yang didelegasikan

Configure for all instances

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, pilih salah satu opsi berikut untuk akun GuardDuty administrator yang didelegasikan:

- Opsi 1

Di bawah Konfigurasi agen otomatis, di EC2bagian ini, pilih Aktifkan untuk semua akun.

- Opsi 2
  - Di bawah Konfigurasi agen otomatis, di EC2bagian ini, pilih Konfigurasi akun secara manual.
  - Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.
- Pilih Simpan.

Jika Anda memilih Konfigurasi akun secara manual untuk Runtime Monitoring, lakukan langkah-langkah berikut:

- Di bawah Konfigurasi agen otomatis, di EC2bagian ini, pilih Konfigurasi akun secara manual.
- Di bawah Administrator Delegasi (akun ini), pilih Aktifkan.
- Pilih Simpan.

Terlepas dari opsi mana yang Anda pilih untuk mengaktifkan konfigurasi agen otomatis untuk akun GuardDuty administrator yang didelegasikan, Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun ini.

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Buka tab Target untuk SSM asosiasi (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai Instancelds.

### Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `true` tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.

Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.

- Buka tab Targets untuk SSM asosiasi yang akan dibuat (GuardDutyRuntimeMonitoring-do-not-delete). Tombol Tag muncul sebagai tag: GuardDutyManaged.

### Using exclusion tag in selected instances

#### Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.


Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
  - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.  
  
Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
  - b. Di bawah menu Tindakan, pilih Pengaturan instans.
  - c. Pilih Izinkan tag dalam metadata contoh.

4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan untuk EC2 instans Amazon](#).

Aktifkan otomatis untuk semua akun anggota

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring:

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis untuk Amazon EC2.
2. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat (`GuardDutyRuntimeMonitoring-do-not-delete`) akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun ini.
  - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
  - b. Buka tab Target untuk SSM asosiasi. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using inclusion tag in selected instances

Untuk mengonfigurasi GuardDuty agen untuk EC2 instans Amazon yang dipilih


1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `true` tag `GuardDutyManaged:` ke EC2 instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).



Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan pada semua EC2 sumber daya milik akun Anda.
  - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
  - b. Buka tab Target untuk SSM asosiasi (GuardDutyRuntimeMonitoring-do-not-delete). Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

Using exclusion tag in selected instances

 Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk EC2 instans Amazon yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
  - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.

Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
  - b. Di bawah menu Tindakan, pilih Pengaturan instans.

- c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan untuk EC2 instans Amazon](#).

Aktifkan otomatis hanya untuk akun anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengatur konfigurasi agen otomatis untuk EC2 sumber daya Amazon agar secara otomatis mengaktifkan akun anggota baru saat mereka bergabung dengan organisasi.

Configure for all instances

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan secara otomatis untuk akun anggota baru di bawah bagian Runtime Monitoring:

1. Di panel navigasi, pilih Runtime Monitoring.
2. Pada halaman Runtime Monitoring, pilih Edit.
3. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, konfigurasi agen otomatis untuk Amazon EC2 akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator organisasi yang didelegasikan yang dapat mengubah pilihan ini.
4. Pilih Simpan.

Ketika akun anggota baru bergabung dengan organisasi, konfigurasi ini akan diaktifkan untuk mereka secara otomatis. GuardDuty Untuk mengelola agen keamanan untuk EC2 instans Amazon yang termasuk dalam akun anggota baru ini, pastikan semua prasyarat [EC2Misalnya](#) terpenuhi.

Ketika SSM asosiasi dibuat (`GuardDutyRuntimeMonitoring-do-not-delete`), Anda dapat memverifikasi bahwa SSM asosiasi akan menginstal dan mengelola agen keamanan pada semua EC2 instance milik akun anggota baru.

- Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
- Buka tab Target untuk SSM asosiasi. Perhatikan bahwa tombol Tag muncul sebagai InstanceIds.

## Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih di akun Anda

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `true` tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk instance yang dipilih ini. Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Anda dapat memverifikasi bahwa SSM asosiasi yang GuardDuty membuat akan menginstal dan mengelola agen keamanan hanya pada EC2 sumber daya yang ditandai dengan tag inklusi.
  - a. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
  - b. Buka tab Target untuk SSM asosiasi yang akan dibuat. Tombol Tag muncul sebagai tag: GuardDutyManaged.

## Using exclusion tag in selected instances

### Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans tertentu di akun mandiri Anda

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.

2. Tambahkan `false` tagGuardDutyManaged: ke instance yang tidak GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
  - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.  
  
Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
  - b. Di bawah menu Tindakan, pilih Pengaturan instans.
  - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai runtime [Cakupan untuk EC2 instans Amazon](#).

Hanya akun anggota selektif

Configure for all instances

1. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda aktifkan konfigurasi agen Runtime Monitoring-Automated agent (Amazon). EC2 Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan Runtime Monitoring.
2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated agent (Amazon). EC2
3. Pilih Konfirmasi.


Using inclusion tag in selected instances

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `true` tagGuardDutyManaged: ke instance yang GuardDuty ingin Anda pantau dan deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).

Menambahkan tag ini akan memungkinkan GuardDuty untuk mengelola agen keamanan untuk EC2 instans Amazon yang ditandai. Anda tidak perlu secara eksplisit mengaktifkan konfigurasi agen otomatis (Runtime Monitoring - Automated agent configuration ). EC2

Using exclusion tag in selected instances

 Note

Pastikan Anda menambahkan tag pengecualian ke EC2 instans Amazon sebelum meluncurkannya. Setelah Anda mengaktifkan konfigurasi agen otomatis untuk AmazonEC2, EC2 instans apa pun yang diluncurkan tanpa tag pengecualian akan tercakup dalam konfigurasi agen GuardDuty otomatis.

Untuk mengonfigurasi agen GuardDuty keamanan untuk instans yang dipilih

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Tambahkan `false` tag `GuardDutyManaged:` ke EC2 instance yang tidak GuardDuty ingin Anda pantau atau deteksi potensi ancaman. Untuk informasi tentang menambahkan tag ini, lihat [Untuk menambahkan tag ke sumber daya individual](#).
3. Agar [tag pengecualian tersedia](#) dalam metadata instance, lakukan langkah-langkah berikut:
  - a. Di bawah tab Detail instans Anda, lihat status untuk Izinkan tag dalam metadata instance.  
  
Jika saat ini Dinonaktifkan, gunakan langkah-langkah berikut untuk mengubah status menjadi Diaktifkan. Jika tidak, lewati langkah ini.
  - b. Di bawah menu Tindakan, pilih Pengaturan instans.
  - c. Pilih Izinkan tag dalam metadata contoh.
4. Setelah Anda menambahkan tag pengecualian, lakukan langkah yang sama seperti yang ditentukan dalam tab Configure for all instance.

Anda sekarang dapat menilai [Cakupan untuk EC2 instans Amazon](#).

## Mengelola agen keamanan secara manual untuk EC2 instans Amazon

Setelah Anda mengaktifkan Runtime Monitoring, Anda harus menginstal agen GuardDuty keamanan secara manual. Dengan menginstal agen, GuardDuty akan menerima peristiwa runtime dari EC2 instans Amazon.

Untuk mengelola agen GuardDuty keamanan, Anda harus membuat VPC titik akhir Amazon dan kemudian ikuti langkah-langkah untuk menginstal agen keamanan secara manual.

### Membuat VPC titik akhir Amazon secara manual

Sebelum Anda dapat menginstal agen GuardDuty keamanan, Anda harus membuat titik akhir Amazon Virtual Private Cloud (AmazonVPC). Ini akan membantu GuardDuty menerima peristiwa runtime dari EC2 instans Amazon Anda.

#### Note

Tidak ada biaya tambahan untuk penggunaan VPC endpoint.

Untuk membuat titik VPC akhir Amazon

1. Masuk ke AWS Management Console dan buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah cloud VPC pribadi, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan **com.amazonaws.us-east-1.guardduty-data**.

Pastikan untuk mengganti *us-east-1* dengan Anda Wilayah AWS. Ini harus Wilayah yang sama dengan EC2 instans Amazon yang termasuk dalam ID AWS akun Anda.

6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat instans Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan VPC titik akhir Amazon hanya ke akun yang ditentukan. Dengan organisasi yang Condition disediakan di bawah kebijakan ini, Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan VPC endpoint Amazon ke akun tertentu IDs di organisasi Anda, lihat [Organization condition to restrict access to your endpoint](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi VPC dan VPC titik akhir. Daftar berikut menunjukkan cara berbagi VPC titik akhir dengan AWS akun IDs lain:

- Untuk menentukan beberapa akun untuk mengakses VPC titik akhir, ganti `"aws:PrincipalAccount: "111122223333"` dengan blok berikut:

```
"aws:PrincipalAccount": [
  "666666666666",
  "555555555555"
]
```

Pastikan untuk mengganti AWS akun IDs dengan akun akun IDs yang perlu mengakses VPC titik akhir.

- Untuk memungkinkan semua anggota dari organisasi mengakses VPC titik akhir, ganti `"aws:PrincipalAccount: "111122223333"` dengan baris berikut:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Pastikan untuk mengganti organisasi *o-abcdef0123* dengan ID organisasi Anda.

- Untuk membatasi akses sumber daya dengan ID organisasi, tambahkan ResourceOrgID ke kebijakan. Untuk informasi selengkapnya, lihat [aws:ResourceOrgID](#) di Panduan IAM Pengguna.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Di bawah Pengaturan tambahan, pilih Aktifkan DNS nama.
9. Di bawah Subnet, pilih subnet tempat instans Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 dalam terikat dari VPC (atau EC2 instans Amazon Anda). Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, lihat [Membuat grup keamanan](#) di EC2Panduan Pengguna Amazon.

Jika ada masalah saat membatasi izin masuk ke VPC (atau instance) Anda, berikan dukungan ke port 443 yang di-bound dari alamat IP apa pun. (0.0.0.0/0)

## Memasang agen keamanan secara manual

GuardDuty menyediakan dua metode berikut untuk menginstal agen GuardDuty keamanan di EC2 instans Amazon Anda:

- Metode 1 - Dengan menggunakan AWS Systems Manager - Metode ini mengharuskan EC2 instans Amazon Anda AWS Systems Manager dikelola.
- Metode 2 - Dengan menggunakan Linux Package Managers - Anda dapat menggunakan metode ini apakah EC2 instans Amazon Anda AWS Systems Manager dikelola atau tidak.

### Metode 1 - Dengan menggunakan AWS Systems Manager

Untuk menggunakan metode ini, pastikan EC2 instans Amazon Anda AWS Systems Manager dikelola dan kemudian instal agen.



## AWS Systems Manager EC2instans Amazon yang dikelola

Gunakan langkah-langkah berikut untuk membuat EC2 instans Amazon Anda AWS Systems Manager dikelola.

- [AWS Systems Manager](#) membantu Anda mengelola AWS aplikasi end-to-end dan sumber daya serta mengaktifkan operasi yang aman dalam skala besar.

Untuk mengelola EC2 instans Amazon Anda AWS Systems Manager, lihat [Menyiapkan Systems Manager untuk EC2 instans Amazon](#) di AWS Systems Manager Panduan Pengguna.

- Tabel berikut menunjukkan AWS Systems Manager dokumen GuardDuty terkelola baru:

| Nama dokumen  | Jenis dokumen | Tujuan  |
|---|---------------|---|
| AmazonGuardDuty-RunTimeMonitoringSsmPlugin          | Distributor   | Untuk mengemas agen GuardDuty keamanan.   |
| AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin | Perintah      | Untuk menjalankan skrip instalasi/penghapusan instalasi untuk menginstal agen keamanan. GuardDuty |

Untuk informasi selengkapnya AWS Systems Manager, lihat [Dokumen Amazon EC2 Systems Manager](#) di Panduan AWS Systems Manager Pengguna.

### Untuk Server Debian

Amazon Machine Images (AMIs) untuk Server Debian yang disediakan oleh AWS mengharuskan Anda untuk menginstal AWS Systems Manager agen (SSMagen). Anda perlu melakukan langkah tambahan untuk menginstal SSM agen agar instans SSM Amazon EC2 Debian Server Anda dikelola. Untuk informasi tentang langkah-langkah yang perlu Anda ambil, lihat [Menginstal SSM agen secara manual pada instance Server Debian](#) di AWS Systems Manager Panduan Pengguna.

Untuk menginstal GuardDuty agen untuk EC2 instans Amazon dengan menggunakan AWS Systems Manager

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Di panel navigasi, pilih Dokumen
3. Di Dimiliki oleh Amazon, pilih AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. Pilih Run Command.
5. Masukkan parameter Run Command berikut
  - Tindakan: Pilih Instal.
  - Jenis Instalasi: Pilih Instal atau Hapus Instalasi.
  - Nama: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
  - Versi: Jika ini tetap kosong, Anda akan mendapatkan versi terbaru dari agen GuardDuty keamanan. Untuk informasi lebih lanjut tentang versi rilis, [GuardDuty agen keamanan untuk EC2 instans Amazon](#).
6. Pilih EC2 instans Amazon yang ditargetkan. Anda dapat memilih satu atau beberapa EC2 instans Amazon. Untuk informasi selengkapnya, lihat [AWS Systems Manager Menjalankan perintah dari konsol](#) di Panduan AWS Systems Manager Pengguna
7. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan](#).

## Metode 2 - Dengan menggunakan Linux Package Managers

Dengan metode ini, Anda dapat menginstal agen GuardDuty keamanan dengan menjalankan RPM skrip atau skrip Debian. Berdasarkan sistem operasi, Anda dapat memilih metode yang disukai:

- Gunakan RPM skrip untuk menginstal agen keamanan pada distribusi OS AL2 atau AL2 023.
- Gunakan skrip Debian untuk menginstal agen keamanan pada distribusi OS Ubuntu atau Debian. Untuk informasi tentang distribusi Ubuntu dan Debian OS yang didukung, lihat. [Memvalidasi persyaratan arsitektur](#)

## RPM installation

### Important

Sebaiknya verifikasi RPM tanda tangan agen GuardDuty keamanan sebelum menginstalnya di mesin Anda.

#### 1. Verifikasi RPM tanda tangan agen GuardDuty keamanan

##### a. Siapkan template

Siapkan perintah dengan kunci publik yang sesuai, tanda tangan x86\_64RPM, tanda tangan arm64RPM, dan tautan akses yang sesuai ke RPM skrip yang dihosting di bucket Amazon S3. Ganti nilai Wilayah AWS, ID AWS akun, dan versi GuardDuty agen untuk mengakses RPM skrip.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/  
publickey.pem
```

- GuardDuty RPM Tanda tangan agen keamanan:

Tanda tangan dari x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/  
amazon-guardduty-agent-1.3.0.x86_64.sig
```

Tanda tangan arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/  
amazon-guardduty-agent-1.3.0.arm64.sig
```

- Akses tautan ke RPM skrip di bucket Amazon S3:

Tautan akses untuk x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/  
amazon-guardduty-agent-1.3.0.x86_64.rpm
```

## Tautan akses untuk arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.rpm
```

| Wilayah AWS    | Nama Wilayah                | AWS ID akun  |
|----------------|-----------------------------|--------------|
| eu-west-1      | Eropa (Irlandia)            | 694911143906 |
| us-east-1      | AS Timur (Virginia Utara)   | 593207742271 |
| us-west-2      | AS Barat (Oregon)           | 733349766148 |
| eu-west-3      | Eropa (Paris)               | 665651866788 |
| us-east-2      | AS Timur (Ohio)             | 307168627858 |
| eu-central-1   | Eropa (Frankfurt)           | 323658145986 |
| ap-northeast-2 | Asia Pasifik (Seoul)        | 914738172881 |
| eu-north-1     | Eropa (Stockholm)           | 591436053604 |
| ap-east-1      | Asia Pasifik (Hong Kong)    | 258348409381 |
| me-south-1     | Timur Tengah (Bahrain)      | 536382113932 |
| eu-west-2      | Eropa (London)              | 892757235363 |
| ap-northeast-1 | Asia Pasifik (Tokyo)        | 533107202818 |
| ap-southeast-1 | Asia Pasifik (Singapura)    | 174946120834 |
| ap-south-1     | Asia Pasifik (Mumbai)       | 251508486986 |
| ap-southeast-3 | Asia Pasifik (Jakarta)      | 510637619217 |
| sa-east-1      | Amerika Selatan (Sao Paulo) | 758426053663 |

|                |                             |              |
|----------------|-----------------------------|--------------|
| ap-northeast-3 | Asia Pasifik (Osaka)        | 273192626886 |
| eu-south-1     | Eropa (Milan)               | 266869475730 |
| af-south-1     | Afrika (Cape Town)          | 197869348890 |
| ap-southeast-2 | Asia Pasifik (Sydney)       | 005257825471 |
| me-central-1   | Timur Tengah (UAE)          | 000014521398 |
| us-west-1      | AS Barat (California Utara) | 684579721401 |
| ca-central-1   | Kanada (Pusat)              | 354763396469 |
| ca-west-1      | Kanada Barat (Calgary)      | 339712888787 |
| ap-south-2     | Asia Pasifik (Hyderabad)    | 950823858135 |
| eu-south-2     | Eropa (Spanyol)             | 919611009337 |
| eu-central-2   | Eropa (Zürich)              | 529164026651 |
| ap-southeast-4 | Asia Pasifik (Melbourne)    | 251357961535 |
| il-central-1   | Israel (Tel Aviv)           | 870907303882 |

b. Unduh templatnya

Dalam perintah berikut untuk mengunduh kunci publik yang sesuai, tanda tangan x86\_64RPM, tanda tangan arm64RPM, dan tautan akses yang sesuai ke RPM skrip yang dihosting di bucket Amazon S3, pastikan untuk mengganti ID akun dengan ID yang sesuai Akun AWS dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm ./amazon-guardduty-agent-1.3.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig ./amazon-guardduty-agent-1.3.0.x86_64.sig
```

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem ./publickey.pem
```

c. Impor kunci publik

Gunakan perintah berikut untuk mengimpor kunci publik ke database:

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verifikasi tanda tangan

Gunakan perintah berikut untuk memverifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.3.0.x86_64.sig amazon-guardduty-agent-1.3.0.x86_64.rpm
```

Jika verifikasi berlalu, Anda akan melihat pesan yang mirip dengan hasil di bawah ini. Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan RPM.

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Jika verifikasi gagal, itu berarti tanda tangan pada RPM telah berpotensi dirusak. Anda harus menghapus kunci publik dari database dan mencoba lagi proses verifikasi.

Contoh:

```
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:

```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba proses verifikasi lagi.

2. [Connect dengan SSH dari Linux atau macOS.](#)
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo rpm -ivh amazon-guardduty-agent-1.3.0.x86_64.rpm
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan.](#)

## Debian installation

### Important

Sebaiknya verifikasi tanda tangan agen GuardDuty keamanan Debian sebelum menginstalnya di mesin Anda.

1. Verifikasi tanda GuardDuty tangan agen keamanan Debian
  - a. Siapkan template untuk kunci publik yang sesuai, tanda tangan paket Debian amd64, tanda tangan paket Debian arm64, dan tautan akses terkait ke skrip Debian yang dihosting di bucket Amazon S3

Dalam template berikut, ganti nilai, ID AWS akun Wilayah AWS, dan versi GuardDuty agen untuk mengakses skrip paket Debian.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/  
publickey.pem
```

- GuardDuty tanda tangan agen keamanan Debian:

## Tanda tangan amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.sig
```

## Tanda tangan arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.sig
```

- Akses tautan ke skrip Debian di bucket Amazon S3:

### Tautan akses untuk amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.deb
```

### Tautan akses untuk arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.deb
```

| Wilayah AWS    | Nama Wilayah              | AWS ID akun  |
|----------------|---------------------------|--------------|
| eu-west-1      | Eropa (Irlandia)          | 694911143906 |
| us-east-1      | AS Timur (Virginia Utara) | 593207742271 |
| us-west-2      | AS Barat (Oregon)         | 733349766148 |
| eu-west-3      | Eropa (Paris)             | 665651866788 |
| us-east-2      | AS Timur (Ohio)           | 307168627858 |
| eu-central-1   | Eropa (Frankfurt)         | 323658145986 |
| ap-northeast-2 | Asia Pasifik (Seoul)      | 914738172881 |
| eu-north-1     | Eropa (Stockholm)         | 591436053604 |



|                |                             |              |
|----------------|-----------------------------|--------------|
| ap-east-1      | Asia Pasifik (Hong Kong)    | 258348409381 |
| me-south-1     | Timur Tengah (Bahrain)      | 536382113932 |
| eu-west-2      | Eropa (London)              | 892757235363 |
| ap-northeast-1 | Asia Pasifik (Tokyo)        | 533107202818 |
| ap-southeast-1 | Asia Pasifik (Singapura)    | 174946120834 |
| ap-south-1     | Asia Pasifik (Mumbai)       | 251508486986 |
| ap-southeast-3 | Asia Pasifik (Jakarta)      | 510637619217 |
| sa-east-1      | Amerika Selatan (Sao Paulo) | 758426053663 |
| ap-northeast-3 | Asia Pasifik (Osaka)        | 273192626886 |
| eu-south-1     | Eropa (Milan)               | 266869475730 |
| af-south-1     | Afrika (Cape Town)          | 197869348890 |
| ap-southeast-2 | Asia Pasifik (Sydney)       | 005257825471 |
| me-central-1   | Timur Tengah (UAE)          | 000014521398 |
| us-west-1      | AS Barat (California Utara) | 684579721401 |
| ca-central-1   | Kanada (Pusat)              | 354763396469 |
| ca-west-1      | Kanada Barat (Calgary)      | 339712888787 |
| ap-south-2     | Asia Pasifik (Hyderabad)    | 950823858135 |
| eu-south-2     | Eropa (Spanyol)             | 919611009337 |
| eu-central-2   | Eropa (Zürich)              | 529164026651 |
| ap-southeast-4 | Asia Pasifik (Melbourne)    | 251357961535 |

il-central-1

Israel (Tel Aviv)

870907303882

- b. Unduh kunci publik yang sesuai unduhan, tanda tangan amd64, tanda tangan arm64, dan tautan akses yang sesuai ke skrip Debian yang dihosting di bucket Amazon S3

Dalam perintah berikut, ganti ID akun dengan ID yang sesuai Akun AWS , dan Wilayah dengan Wilayah Anda saat ini.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.deb ./amazon-guardduty-
agent-1.3.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.sig ./amazon-guardduty-
agent-1.3.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

- c. Impor kunci publik ke database

```
gpg --import publickey.pem
```

gpg menunjukkan impor berhasil

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

- d. Verifikasi tanda tangan

```
gpg --verify amazon-guardduty-agent-1.3.0.amd64.sig amazon-guardduty-
agent-1.3.0.amd64.deb
```

Setelah verifikasi berhasil, Anda akan melihat pesan yang mirip dengan hasil berikut:

Contoh output:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
```

```
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Anda sekarang dapat melanjutkan untuk menginstal agen GuardDuty keamanan menggunakan Debian.

Namun, jika verifikasi gagal, itu berarti tanda tangan dalam paket Debian berpotensi dirusak.

Contoh:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Gunakan perintah berikut untuk menghapus kunci publik dari database:

```
gpg --delete-keys AwsGuardDuty
```

Sekarang, coba lagi proses verifikasi.

2. [Connect dengan SSH dari Linux atau macOS.](#)
3. Instal agen GuardDuty keamanan dengan menggunakan perintah berikut:

```
sudo dpkg -i amazon-guardduty-agent-1.3.0.amd64.deb
```

4. Validasi jika instalasi GuardDuty agen sehat. Untuk informasi selengkapnya tentang langkah-langkahnya, lihat [Memvalidasi status instalasi agen GuardDuty keamanan.](#)

## Kesalahan kehabisan memori

Jika Anda mengalami out-of-memory kesalahan saat menginstal atau memperbarui agen GuardDuty keamanan untuk Amazon EC2 secara manual, lihat [Memecahkan masalah kesalahan memori.](#)

## Memvalidasi status instalasi agen GuardDuty keamanan

Untuk memvalidasi jika agen GuardDuty keamanan sehat

1. [Connect dengan SSH dari Linux atau macOS.](#)
2. Jalankan perintah berikut untuk memeriksa status agen GuardDuty keamanan:

```
sudo systemctl status amazon-guardduty-agent
```

Jika Anda ingin melihat log instalasi agen keamanan, mereka tersedia di bawah `/var/log/amzn-guardduty-agent/`.

Untuk melihat log, lakukan `sudo journalctl -u amazon-guardduty-agent`.

### Memperbarui agen GuardDuty keamanan secara manual

Anda dapat memperbarui agen GuardDuty keamanan dengan menggunakan perintah Run. Anda dapat mengikuti langkah-langkah yang sama yang Anda gunakan untuk menginstal agen GuardDuty keamanan.

### Menghapus instalasi agen keamanan secara manual

Bagian ini menyediakan metode untuk menghapus instalasi agen GuardDuty keamanan dari EC2 sumber daya Amazon Anda. Jika Anda berencana lebih lanjut untuk menonaktifkan Runtime Monitoring, lihat [Dampak penonaktifan](#).

#### Metode 1 - Dengan menggunakan perintah Run

Untuk menghapus instalasi agen GuardDuty keamanan dengan menggunakan perintah Run

1. Anda dapat menghapus instalasi agen GuardDuty keamanan dengan mengikuti langkah-langkah seperti yang ditentukan dalam [AWS Systems Manager Jalankan Perintah](#) di Panduan AWS Systems Manager Pengguna. Gunakan tindakan Uninstall dalam parameter untuk menghapus instalasi agen GuardDuty keamanan.

Di bagian Target, pastikan dampaknya hanya pada EC2 instans Amazon yang ingin Anda hapus instalasi agen keamanan.

Gunakan GuardDuty dokumen dan distributor berikut:

- Nama dokumen: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
  - Distributor: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Setelah memberikan semua detail, saat Anda memilih Jalankan, agen keamanan yang disebarkan pada EC2 instans Amazon yang ditargetkan akan dihapus.

Untuk menghapus konfigurasi VPC endpoint Amazon, Anda harus menonaktifkan Runtime Monitoring dan Amazon EKS Runtime Monitoring.

## Metode 2 - Dengan menggunakan Linux Package Managers

1. [Connect dengan SSH dari Linux atau macOS.](#)
2. Perintah untuk menghapus instalasi

Perintah berikut akan menghapus instalasi agen GuardDuty keamanan dari EC2 instans Amazon yang Anda sambungkan:

- Untuk RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Untuk Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Setelah Anda menjalankan perintah, Anda juga dapat memeriksa log yang terkait dengan perintah.

## Hapus titik VPC akhir Amazon

Saat Anda ingin menonaktifkan Runtime Monitoring atau menghapus instalasi agen GuardDuty keamanan untuk akun Anda, Anda juga dapat memilih untuk menghapus VPC titik akhir Amazon yang dibuat secara manual (). [Membuat VPC titik akhir Amazon secara manual](#)

Untuk menghapus VPC titik akhir Amazon dengan menggunakan konsol

1. Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, pilih Titik akhir.
3. Pilih titik akhir yang dibuat secara manual pada saat mengaktifkan Runtime Monitoring.
4. Pilih Tindakan, Hapus VPC titik akhir.
5. Saat diminta mengonfirmasi, pilih **delete**.
6. Pilih Hapus.

Untuk menghapus VPC titik akhir Amazon dengan menggunakan AWS CLI

- [delete-vpc-endpoints](#) (AWS Command Line Interface)
- [Remove-EC2VpcEndpointCmdlet](#) (Alat untuk Windows) PowerShell

## Mengelola agen keamanan otomatis untuk Fargate (hanya AmazonECS)

Runtime Monitoring mendukung pengelolaan agen keamanan untuk ECS klaster Amazon Anda (AWS Fargate) hanya melalui GuardDuty. Tidak ada dukungan untuk mengelola agen keamanan secara manual di ECS cluster Amazon.

Untuk mengaktifkan mengelola agen keamanan untuk sumber daya ECS -Fargate Anda, ikuti langkah-langkah yang disediakan di bagian berikut.

### Daftar Isi

- [Mengkonfigurasi GuardDuty agen untuk akun mandiri](#)
- [Mengkonfigurasi GuardDuty agen untuk lingkungan multi-akun](#)

## Mengkonfigurasi GuardDuty agen untuk akun mandiri

### Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi:
  - a. Untuk mengelola konfigurasi agen otomatis untuk semua ECS klaster Amazon (tingkat akun)

Pilih Aktifkan di bagian Konfigurasi agen otomatis untuk AWS Fargate (ECS). Ketika ECS tugas Fargate Amazon baru diluncurkan, GuardDuty akan mengelola penyebaran agen keamanan.

- Pilih Simpan.

- b. Untuk mengelola konfigurasi agen Otomatis dengan mengecualikan beberapa kluster Amazon (tingkat ECS kluster)
  - i. Tambahkan tag ke ECS cluster Amazon yang ingin Anda kecualikan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. false
  - ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
    }
  ]
}
```

```

    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

- iii. Di bawah tab Konfigurasi, pilih Aktifkan di bagian Konfigurasi agen otomatis.



**Note**

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen keamanan akan digunakan di semua tugas yang diluncurkan dalam kluster Amazon yang sesuai. ECS

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

- iv. Pilih Simpan.
- c. Untuk mengelola konfigurasi agen Otomatis dengan menyertakan beberapa ECS kluster Amazon (tingkat kluster)
  - i. Tambahkan tag ke ECS cluster Amazon yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
  - ii. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",

```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
}
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
}
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {

```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
    },
    "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
    }
}
]
}

```

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container](#).
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

## Mengkonfigurasi GuardDuty agen untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola konfigurasi agen otomatis untuk ECS kluster Amazon milik akun anggota di organisasinya. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun di GuardDuty](#).

Mengaktifkan konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

Manage for all Amazon ECS clusters (account level)

Jika Anda memilih Aktifkan untuk semua akun untuk Runtime Monitoring, maka Anda memiliki opsi berikut:

- Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua ECS tugas Amazon yang diluncurkan.
- Pilih Konfigurasikan akun secara manual.

Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut:

1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis.
2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini).

Pilih Simpan.

Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container](#).
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon ini dengan pasangan nilai kunci sebagai `GuardDutyManaged - false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    }
  ]
}


```

```

    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
}

```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Aktifkan dalam konfigurasi agen otomatis.

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Pilih Simpan.

7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged - true`
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```

    },
    "Null": {
      "ecs:ResourceTag/GuardDutyManaged": false
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      }
    }
  }
}

```



```
    },  
    "Null": {  
      "aws:PrincipalTag/GuardDutyManaged": true  
    }  
  }  
]  
}
```

**Note**

Saat menggunakan tag inklusi untuk ECS kluster Amazon, Anda tidak perlu mengaktifkan GuardDuty agen melalui konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Aktifkan otomatis untuk semua akun anggota

Manage for all Amazon ECS clusters (account level)

Langkah-langkah berikut mengasumsikan bahwa Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.

1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua ECS tugas Amazon yang diluncurkan.
2. Pilih Simpan.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon ini dengan pasangan nilai kunci sebagai `GuardDutyManaged - false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```

    },
    "Null": {
      "ecs:ResourceTag/GuardDutyManaged": false
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      }
    }
  }
}


```

```
    },  
    "Null": {  
      "aws:PrincipalTag/GuardDutyManaged": true  
    }  
  }  
]  
}
```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

4. Di panel navigasi, pilih Runtime Monitoring.

5.

 Note

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Edit.

6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Simpan.

8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container](#).
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

## Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau tugas Amazon ECS Fargate selektif untuk semua akun anggota di organisasi Anda.

1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang Anda pilih pada langkah sebelumnya.
2. Pilih Simpan.
3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
```

```

        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

**Note**

Saat menggunakan tag inklusi untuk ECS kluster Amazon, Anda tidak perlu mengaktifkan manajemen otomatis GuardDuty agen secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif yang ada

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini.
2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan.
3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
4. Pilih Konfirmasi.
5. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon ini dengan pasangan nilai kunci sebagai GuardDutyManaged -. false
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
```



```
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
```

```
}
```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, di bagian Konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan.

6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota yang aktif.

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

7. Pilih Konfirmasi.
8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container](#).
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon yang ingin Anda sertakan semua tugasnya. Pasang nilai kunci harus `GuardDutyManaged - . true`

2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}"
        }
      }
    }
  ]
}
```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

#### Note

Saat menggunakan tag inklusi untuk ECS kluster Amazon, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan

Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Aktifkan otomatis konfigurasi agen otomatis untuk anggota baru

Manage for all Amazon ECS clusters (account level)

1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada.
2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru.
3. Pilih Simpan.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon ini dengan pasangan nilai kunci sebagai `GuardDutyManaged - false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {


```

```

        "aws:TagKeys": [
            "GuardDutyManaged"
        ]
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:CreateTags",
            "ecs>DeleteTags"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
]
}

```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon ECS yang diluncurkan.

Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis.

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Pilih Simpan.
7. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus `GuardDutyManaged -. true`
2. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
```



```

        "StringNotEquals": {
            "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
            "ecs:ResourceTag/GuardDutyManaged": false
        }
    },
    {
        "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
        "Effect": "Deny",
        "Action": [
            "ecs:CreateTags",
            "ecs>DeleteTags"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:CreateTags",
            "ecs>DeleteTags"
        ],
        "Resource": [
            "*"
        ]
    }
}

```

```
    ],  
    "Condition": {  
      "StringNotEquals": {  
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-  
admins/iam-admin"  
      },  
      "Null": {  
        "aws:PrincipalTag/GuardDutyManaged": true  
      }  
    }  
  }  
]  
}
```

#### Note

Saat menggunakan tag inklusi untuk ECS kluster Amazon, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

3. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container](#).
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Mengaktifkan konfigurasi agen otomatis untuk akun anggota aktif secara selektif

Manage for all Amazon ECS (account level)

1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Runtime Monitoring-Automated agent configuration (-Fargate). ECS Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.

2. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated (-Fargate). ECS
3. Pilih Konfirmasi.
4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Tambahkan tag ke ECS cluster Amazon ini dengan pasangan nilai kunci sebagai `GuardDutyManaged - false`
2. Mencegah modifikasi tag, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
```


```

        "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}]",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
    ],
    "Resource": [
        "*"
    ]
},

```

```
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
}
```

3. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
4. Di panel navigasi, pilih Runtime Monitoring.
- 5.

 Note

Selalu tambahkan tag pengecualian ke ECS kluster Amazon Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, wadah GuardDuty sespan akan dilampirkan ke semua kontainer dalam tugas Amazon yang diluncurkan. ECS

Pada halaman Akun, pilih akun yang ingin Anda aktifkan Runtime Monitoring-Automated agent configuration (-Fargate). ECS Anda dapat memilih beberapa akun. Pastikan akun yang Anda pilih pada langkah ini sudah diaktifkan dengan Runtime Monitoring.

Untuk ECS cluster Amazon yang belum dikecualikan, GuardDuty akan mengelola penyebaran agen keamanan di wadah sespan.

6. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated (-Fargate). ECS
7. Pilih Simpan.
8. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di](#) Panduan Pengembang Layanan Amazon Elastic Container.
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Pastikan Anda tidak mengaktifkan konfigurasi agen Otomatis (atau Runtime Monitoring-Automated agent configuration (ECS-Fargate)) untuk akun yang dipilih yang memiliki ECS kluster Amazon yang ingin Anda pantau.
2. Tambahkan tag ke ECS cluster Amazon yang ingin Anda sertakan semua tugasnya. Pasangan kunci-nilai harus GuardDutyManaged -. true
3. Mencegah modifikasi tag ini, kecuali oleh entitas tepercaya. Kebijakan yang disediakan dalam [Mencegah tag diubah kecuali oleh prinsip-prinsip resmi](#) dalam Panduan AWS Organizations Pengguna telah dimodifikasi agar dapat diterapkan di sini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:CreateTags",
        "ecs>DeleteTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
        },
        "Null": {
```

```

        "ecs:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:CreateTags",
      "ecs>DeleteTags"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
      },
      "Null": {

```

```
    "aws:PrincipalTag/GuardDutyManaged": true
  }
}
]
```

**Note**

Saat menggunakan tag inklusi untuk ECS kluster Amazon, Anda tidak perlu mengaktifkan konfigurasi agen otomatis secara eksplisit.

4. Ketika Anda GuardDuty ingin memantau tugas yang merupakan bagian dari layanan, itu memerlukan penerapan layanan baru setelah Anda mengaktifkan Runtime Monitoring. Jika penerapan terakhir untuk ECS layanan tertentu dimulai sebelum Anda mengaktifkan Runtime Monitoring, Anda dapat memulai ulang layanan, atau memperbarui layanan dengan menggunakan `forceNewDeployment`

Untuk langkah-langkah memperbarui layanan, lihat sumber daya berikut:

- [Memperbarui ECS layanan Amazon menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.](#)
- [UpdateService](#) di API Referensi Layanan Kontainer Elastis Amazon.
- [update-service](#) di Command Reference.AWS CLI

## Mengelola agen keamanan secara otomatis untuk EKS kluster Amazon


Mengkonfigurasi agen otomatis untuk akun mandiri

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Runtime Monitoring.
3. Di bawah tab Konfigurasi, pilih Aktifkan untuk mengaktifkan konfigurasi agen otomatis untuk akun Anda.



| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan           | Langkah-langkahnya   |
|---|--|
| Mengelola agen keamanan melalui GuardDuty<br><br>(Pantau semua EKS cluster) | <ol style="list-style-type: none"><li data-bbox="691 348 1458 527">1. Pilih Aktifkan di bagian Konfigurasi agen otomatis. GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster yang ada dan berpotensi baru di akun Anda.</li><li data-bbox="691 548 915 579">2. Pilih Simpan.</li></ol> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan                               | Langkah-langkahnya   |
|---|--|
| Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian) | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan belum digunakan di klaster ini</p> <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>false</code>.</li></ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <ol style="list-style-type: none"><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna</a> AWS Organizations. Dalam kebijakan ini, ganti detail berikut:</li></ol> <ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li><li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>.</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas terpercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre data-bbox="803 310 1507 579">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="691 600 1365 680">3. Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li data-bbox="691 701 1365 739">4. Di panel navigasi, pilih Runtime Monitoring.<div data-bbox="756 779 1507 1188"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua cluster di akun Anda. EKS</p></div></li><li data-bbox="691 1209 1446 1289">5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen.<p data-bbox="756 1331 1500 1461">Untuk EKS cluster yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.</p></li><li data-bbox="691 1482 938 1520">6. Pilih Simpan.</li></ol> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Untuk mengecualikan EKS cluster dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini</p> <ol style="list-style-type: none"><li data-bbox="691 478 1484 562">1. Tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>false</code>.<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.<br/><br/>Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster ini EKS. Ini dapat memengaruhi statistik penggunaan Anda.</li><li data-bbox="691 1129 1500 1398">2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut:<ul data-bbox="756 1444 1458 1738" style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li></ul></li></ol> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <ul style="list-style-type: none"><li data-bbox="755 306 1442 390">• Ganti <b>123456789012</b> dengan Akun AWS ID entitas tepercaya.</li></ul> <p data-bbox="786 436 1398 562">Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre data-bbox="805 625 1395 852">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="691 898 1490 1167">3. Untuk berhenti menerima peristiwa runtime dari kluster ini, Anda harus menghapus agen keamanan yang digunakan dari kluster iniEKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat<a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Pantau EKS cluster selektif menggunakan tag inklusi               | <ol style="list-style-type: none"><li>1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring.</li><li>2. Pilih Simpan.</li><li>3. Tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>.<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.<br/><br/>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</li><li>4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li></ul></li></ol> |

| Pendekatan yang disukai untuk menyebarkan agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre data-bbox="789 474 1507 751">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> |
| Kelola agen secara manual   | <ol style="list-style-type: none"> <li>1. Pastikan untuk memilih Nonaktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring.</li> <li>2. Pilih Simpan.</li> <li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</li> </ol>                                    |


## Mengkonfigurasi agen otomatis untuk lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan konfigurasi agen otomatis untuk akun anggota, dan mengelola Agen otomatis untuk EKS kluster milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

## Mengkonfigurasi konfigurasi agen otomatis untuk akun administrator yang didelegasikan GuardDuty

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Mengelola agen keamanan melalui GuardDuty</p> <p>(Pantau semua EKS cluster)</p>                     | <p>Jika Anda memilih Aktifkan untuk semua akun di bagian Runtime Monitoring, maka Anda memiliki opsi berikut:</p> <ul style="list-style-type: none"> <li>• Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua EKS cluster yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua EKS cluster yang dimiliki oleh semua akun anggota yang ada dan berpotensi baru dalam organisasi.</li> <li>• Pilih Konfigurasikan akun secara manual.</li> </ul> <p>Jika Anda memilih Konfigurasi akun secara manual di bagian Runtime Monitoring, lakukan hal berikut:</p> <ol style="list-style-type: none"> <li>1. Pilih Konfigurasi akun secara manual di bagian Konfigurasi agen otomatis.</li> <li>2. Pilih Aktifkan di bagian akun GuardDuty administrator yang didelegasikan (akun ini).</li> </ol> <p>Pilih Simpan.</p> |
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan belum digunakan di klaster ini</p> <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>.</li> </ol>  |



| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Untuk informasi selengkapnya tentang menandai EKS kluster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <ol style="list-style-type: none"><li>Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li>Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li>Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>Ganti <code>123456789012</code> dengan Akun AWS ID entitas terpercaya.</li></ul></li></ol> <p>Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li>Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li>Di panel navigasi, pilih Runtime Monitoring.</li></ol> <div data-bbox="586 1591 1507 1829"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan manajemen otomatis GuardDuty agen untuk akun Anda; jika tidak, agen GuardDuty</p></div> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p data-bbox="586 302 1507 430">keamanan akan digunakan di semua cluster di akun Anda. EKS</p> <ol style="list-style-type: none"> <li data-bbox="524 447 1453 527">5. Di bawah tab Konfigurasi, pilih Aktifkan di bagian manajemen GuardDuty agen.<br/><br/>Untuk EKS cluster yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.</li> <li data-bbox="524 726 773 758">6. Pilih Simpan.</li> </ol> <p data-bbox="524 837 1403 917">Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan telah digunakan di klaster ini</p> <ol style="list-style-type: none"> <li data-bbox="524 963 1487 1050">1. Tambahkan tag ke EKS cluster ini dengan kunci as GuardDuty Managed dan nilainya sebagai false.<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</li> <li data-bbox="524 1247 1487 1766">2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li data-bbox="586 1518 1419 1549">• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li> <li data-bbox="586 1572 1458 1604">• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li> <li data-bbox="586 1627 1419 1659">• Ganti <i>access-project</i> dengan GuardDutyManaged</li> <li data-bbox="586 1682 1373 1766">• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li> </ul> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre data-bbox="618 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="521 688 1495 961">3. Jika Anda mengaktifkan agen otomatis untuk EKS cluster ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster ini EKS. Ini dapat memengaruhi statistik penggunaan Anda.<br/><br/>Untuk berhenti menerima peristiwa runtime dari klaster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster ini EKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a></li><li data-bbox="521 1255 1495 1388">4. Jika Anda mengelola agen GuardDuty keamanan untuk EKS cluster ini secara manual, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Pantau EKS cluster selektif menggunakan tag inklusi             | <p>Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau EKS klaster selektif di akun Anda:</p> <ol style="list-style-type: none"><li>1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li><li>2. Pilih Simpan.</li><li>3. Tambahkan tag ke EKS cluster Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>.</li></ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</p> <ol style="list-style-type: none"><li>4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:</li></ol> <ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre data-bbox="618 306 1507 499">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>   |
| <p>Mengelola agen GuardDuty keamanan secara manual</p>          | <p>Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk EKS cluster Anda.</p> <ol data-bbox="521 737 1479 1083" style="list-style-type: none"> <li>1. Pastikan untuk memilih Nonaktifkan untuk akun GuardDuty administrator yang didelegasikan (akun ini) di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li> <li>2. Pilih Simpan.</li> <li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS klaster Amazon</a>.</li> </ol> |

### Aktifkan otomatis Agen otomatis untuk semua akun anggota


#### Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| <p>Mengelola agen keamanan melalui GuardDuty</p>                | <p>Topik ini adalah untuk mengaktifkan Runtime Monitoring untuk semua akun anggota dan oleh karena itu, langkah-langkah berikut mengasumsikan bahwa Anda harus memilih Aktifkan untuk semua akun di bagian Runtime Monitoring.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| (Pantau semua EKS cluster)                                      | <ol style="list-style-type: none"><li data-bbox="521 308 1507 583">1. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. GuardDuty akan menyebarkan dan mengelola agen keamanan untuk semua EKS cluster yang termasuk dalam akun akun GuardDuty administrator yang didelegasikan dan juga untuk semua EKS cluster yang dimiliki oleh semua akun anggota yang ada dan berpotensi baru dalam organisasi.</li><li data-bbox="521 604 776 638">2. Pilih Simpan.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya  |
|--|---|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS kluster dari pemantauan saat agen GuardDuty keamanan belum digunakan di kluster ini</p> <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>as GuardDutyManaged</code> dan nilainya <code>sebagai false</code>. <p>Untuk informasi selengkapnya tentang menandai EKS kluster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> </li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <ol style="list-style-type: none"><li>3. Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li>4. Di panel navigasi, pilih Runtime Monitoring.<div data-bbox="586 485 1507 800" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan Agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p></div></li><li>5. Di bawah tab Konfigurasi, pilih Edit di bagian konfigurasi Runtime Monitoring.</li><li>6. Pilih Aktifkan untuk semua akun di bagian Konfigurasi agen otomatis. Untuk EKS cluster yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.</li><li>7. Pilih Simpan.</li></ol> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan telah digunakan di klaster ini</p> <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya <code>sebagai false</code>.<p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p></li><li>2. Jika Anda mengaktifkan konfigurasi agen otomatis untuk EKS klaster ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk klaster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus</li></ol> |




| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>menerima peristiwa runtime dari cluster iniEKS. Ini dapat memengaruhi statistik penggunaan Anda.</p> <p>Untuk berhenti menerima peristiwa runtime dari klaster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster iniEKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a></p> <ol style="list-style-type: none"><li>3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan <code>GuardDutyManaged</code></li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul><p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipal Arn :</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></li><li>4. Jika Anda mengelola agen GuardDuty keamanan untuk EKS cluster ini secara manual, lihat<a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Pantau EKS cluster selektif menggunakan tag inklusi             | <p>Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau EKS klaster selektif untuk semua akun anggota di organisasi Anda:</p> <ol style="list-style-type: none"><li>1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li><li>2. Pilih Simpan.</li><li>3. Tambahkan tag ke EKS cluster Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>.</li></ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</p> <ol style="list-style-type: none"><li>4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:</li></ol> <ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> |

|   |  |
|---|--|
| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|   | <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>  |
| Mengelola agen GuardDuty keamanan secara manual                 | <p>Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk EKS cluster Anda.</p> <ol style="list-style-type: none"> <li>1. Jangan aktifkan konfigurasi apa pun di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li> <li>2. Pilih Simpan.</li> <li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS klaster Amazon</a>.</li> </ol> |

Mengaktifkan agen otomatis untuk semua akun anggota aktif yang ada

 Note


Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Untuk mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda

- GuardDuty Untuk menerima peristiwa runtime dari EKS cluster yang termasuk dalam akun anggota aktif yang ada di organisasi, Anda harus memilih pendekatan yang lebih disukai untuk mengelola agen GuardDuty keamanan untuk klaster ini EKS. Untuk informasi lebih lanjut tentang masing-masing pendekatan ini, lihat [Pendekatan untuk mengelola agen GuardDuty keamanan](#).

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan             | Langkah-langkahnya  |
|---|---|
| Mengelola agen keamanan melalui GuardDuty<br><br>(Pantau semua EKS cluster) | Untuk memantau semua EKS cluster untuk semua akun anggota aktif yang ada<br><br><ol style="list-style-type: none"><li data-bbox="691 474 1466 604">1. Pada halaman Runtime Monitoring, di bawah tab Konfigurasi, Anda dapat melihat status konfigurasi agen Otomatis saat ini.</li><li data-bbox="691 627 1451 709">2. Dalam panel konfigurasi agen otomatis, di bawah bagian Akun anggota aktif, pilih Tindakan.</li><li data-bbox="691 732 1419 814">3. Dari Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.</li><li data-bbox="691 837 980 869">4. Pilih Konfirmasi.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan                                 | Langkah-langkahnya   |
|---|--|
| Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian) | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan belum digunakan di klaster ini</p> <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>false</code>.</li></ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <ol style="list-style-type: none"><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna</a> AWS Organizations. Dalam kebijakan ini, ganti detail berikut:</li></ol> <ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li><li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>.</li><li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas terpercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre data-bbox="803 304 1507 577">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol data-bbox="690 598 1372 745" style="list-style-type: none"><li>3. Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li>4. Di panel navigasi, pilih Runtime Monitoring.</li></ol> <div data-bbox="755 777 1507 1186"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p></div> <ol data-bbox="690 1207 1453 1501" style="list-style-type: none"><li>5. Di bawah tab Konfigurasi, di panel konfigurasi agen otomatis, di bawah Akun anggota aktif, pilih Tindakan.</li><li>6. Dari Tindakan, pilih Aktifkan untuk semua akun anggota yang aktif.</li><li>7. Pilih Konfirmasi.</li></ol> <p data-bbox="690 1575 1469 1701">Untuk mengecualikan EKS cluster dari pemantauan setelah agen GuardDuty keamanan telah digunakan di cluster ini</p> <ol data-bbox="690 1743 1485 1837" style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>aws:GuardDutyManaged</code> dan nilainya sebagai <code>false</code>.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>Setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk cluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster ini EKS. Ini dapat memengaruhi statistik penggunaan Anda.</p> <p>2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna</a> AWS Organizations. Dalam kebijakan ini, ganti detail berikut:</p> <ul style="list-style-type: none"><li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li><li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>.</li><li>• Ganti <code>access-project</code> dengan GuardDuty Managed</li><li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas terpercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapa PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre data-bbox="792 300 1507 478">admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="691 499 1497 863">3. Terlepas dari bagaimana Anda mengelola agen keamanan (melalui GuardDuty atau secara manual), untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster ini EKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |




| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Pantau EKS cluster selektif menggunakan tag inklusi             | <ol style="list-style-type: none"><li>1. Pada halaman Akun, setelah Anda mengaktifkan Runtime Monitoring, jangan aktifkan Runtime Monitoring - Konfigurasi agen otomatis.</li><li>2. Tambahkan tag ke EKS cluster milik akun yang dipilih yang ingin Anda pantau. Pasangan kunci-nilai tag harus GuardDutyManaged - . true<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.<br/><br/>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</li><li>3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan eks:TagResource .</li><li>• Ganti <i>ec2:DeleteTags</i> dengan eks:UntagResource .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul></li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre data-bbox="789 474 1507 751">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> |
| Mengelola agen GuardDuty keamanan secara manual                 | <ol style="list-style-type: none"> <li>1. Pastikan Anda tidak memilih Aktifkan di bagian Konfigurasi agen otomatis. Tetap aktifkan Runtime Monitoring.</li> <li>2. Pilih Simpan.</li> <li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</li> </ol>                                  |

### Aktifkan otomatis konfigurasi agen otomatis untuk anggota baru

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan             | Langkah-langkahnya  |
|---|---|
| Mengelola agen keamanan melalui GuardDuty<br><br>(Pantau semua EKS cluster) | <ol style="list-style-type: none"> <li>1. Pada halaman Runtime Monitoring, pilih Edit untuk memperbarui konfigurasi yang ada.</li> <li>2. Di bagian Konfigurasi agen otomatis, pilih Aktifkan secara otomatis untuk akun anggota baru.</li> <li>3. Pilih Simpan.</li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya  |
|--|---|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan belum digunakan di klaster ini</p> <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>false</code>.<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li> <li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code>.</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <pre data-bbox="748 302 1507 401">admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="651 415 1490 499">3. Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li data-bbox="651 520 1325 558">4. Di panel navigasi, pilih Runtime Monitoring.</li></ol> <div data-bbox="716 600 1507 957"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p></div> <ol style="list-style-type: none"><li data-bbox="651 978 1503 1104">5. Di bawah tab Konfigurasi, pilih Aktifkan secara otomatis untuk akun anggota baru di bagian manajemen GuardDuty agen.<br/><p data-bbox="716 1150 1479 1283">Untuk EKS cluster yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.</p></li><li data-bbox="651 1304 902 1341">6. Pilih Simpan.</li></ol> <p data-bbox="651 1415 1455 1499">Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan telah digunakan di klaster ini</p> <ol style="list-style-type: none"><li data-bbox="651 1541 1498 1724">1. Terlepas dari apakah Anda mengelola agen GuardDuty keamanan melalui GuardDuty atau secara manual, tambahkan tag ke EKS cluster ini dengan kunci <code>asGuardDutyManaged</code> dan nilainya <code>sebagaifalse</code>.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Untuk informasi selengkapnya tentang menandai EKS kluster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan an konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>Jika Anda mengaktifkan agen otomatis untuk EKS kluster ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk kluster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster iniEKS. Ini dapat memengaruhi statistik penggunaan Anda.</p> <p>Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari kluster iniEKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a></p> <ol style="list-style-type: none"><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul></li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre data-bbox="748 474 1507 709">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="651 730 1507 863">3. Jika Anda mengelola agen GuardDuty keamanan untuk EKS cluster ini secara manual, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |


| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| <p>Pantau EKS cluster selektif menggunakan tag inklusi</p>      | <p>Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau EKS klaster selektif untuk akun anggota baru di organisasi Anda.</p> <ol style="list-style-type: none"> <li>1. Pastikan untuk menghapus Aktifkan secara otomatis untuk akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li> <li>2. Pilih Simpan.</li> <li>3. Tambahkan tag ke EKS cluster Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>.</li> </ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</p> <ol style="list-style-type: none"> <li>4. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code>.</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> </ul> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <ul style="list-style-type: none"><li>• Ganti <b>123456789012</b> dengan Akun AWS ID entitas tepercaya.</li></ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>  |
| Mengelola agen GuardDuty keamanan secara manual                 | <p>Terlepas dari bagaimana Anda memilih untuk mengaktifkan Runtime Monitoring, Anda dapat mengelola agen keamanan secara manual untuk EKS cluster Anda.</p> <ol style="list-style-type: none"><li>1. Pastikan kosongkan kotak centang Secara otomatis mengaktifkan akun anggota baru di bagian Konfigurasi agen otomatis. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya.</li><li>2. Pilih Simpan.</li><li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS klaster Amazon</a>.</li></ol> |



## Mengkonfigurasi agen otomatis untuk akun anggota aktif secara selektif

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Mengelola agen keamanan melalui GuardDuty</p> <p>(Pantau semua EKS cluster)</p>                     | <ol style="list-style-type: none"> <li>1. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Konfigurasi agen otomatis. Anda dapat memilih lebih dari satu akun sekaligus. Pastikan akun yang Anda pilih pada langkah ini sudah mengaktifkan EKS Runtime Monitoring.</li> <li>2. Dari paket Edit Protection pilih opsi yang sesuai untuk mengaktifkan Runtime Monitoring - Konfigurasi agen otomatis.</li> <li>3. Pilih Konfirmasi.</li> </ol>   |
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <p>Dari prosedur berikut, pilih salah satu skenario yang berlaku untuk Anda.</p> <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan belum digunakan di klaster ini</p> <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya sebagai <code>false</code>.</li> </ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <ol style="list-style-type: none"> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre data-bbox="618 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="524 688 1495 772">3. Buka GuardDuty konsol di <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li></ol> <div data-bbox="586 814 1507 1129"><p> <b>Note</b></p><p>Selalu tambahkan tag pengecualian ke EKS cluster Anda sebelum mengaktifkan konfigurasi agen otomatis untuk akun Anda; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p></div> <ol style="list-style-type: none"><li data-bbox="524 1144 1479 1276">4. Pada halaman Akun, pilih akun yang ingin Anda aktifkan Kelola agen secara otomatis. Anda dapat memilih lebih dari satu akun sekaligus.</li><li data-bbox="524 1291 1471 1430">5. Dari Edit paket perlindungan, pilih opsi yang sesuai untuk mengaktifkan konfigurasi agen Runtime Monitoring-Automated untuk akun yang dipilih.</li></ol> <p data-bbox="586 1472 1511 1598">Untuk EKS cluster yang belum dikecualikan dari pemantauan, GuardDuty akan mengelola penyebaran dan pembaruan ke agen GuardDuty keamanan.</p> <ol style="list-style-type: none"><li data-bbox="524 1619 776 1661">6. Pilih Simpan.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Untuk mengecualikan EKS klaster dari pemantauan saat agen GuardDuty keamanan telah digunakan di klaster ini</p> <ol style="list-style-type: none"><li data-bbox="526 432 1490 516">1. Tambahkan tag ke EKS cluster ini dengan kunci <code>as GuardDuty Managed</code> dan nilainya <code>sebagai false</code>.<br/><br/>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.<br/><br/>Jika sebelumnya Anda telah mengaktifkan konfigurasi agen otomatis untuk EKS klaster ini, maka setelah langkah ini, tidak GuardDuty akan memperbarui agen keamanan untuk klaster ini. Namun, agen keamanan akan tetap digunakan dan GuardDuty akan terus menerima peristiwa runtime dari cluster ini EKS. Ini dapat memengaruhi statistik penggunaan Anda.<br/><br/>Untuk berhenti menerima peristiwa runtime dari cluster ini, Anda harus menghapus agen keamanan yang digunakan dari klaster ini EKS. Untuk informasi selengkapnya tentang menghapus agen keamanan yang digunakan, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a></li><li data-bbox="526 1304 1490 1829">2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a>. Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li data-bbox="586 1577 1422 1608">• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li><li data-bbox="586 1629 1458 1661">• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li><li data-bbox="586 1682 1422 1713">• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li><li data-bbox="586 1734 1373 1829">• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li></ul></li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre data-bbox="618 474 1507 674">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li data-bbox="521 684 1451 863">3. Jika Anda mengelola agen GuardDuty keamanan untuk EKS cluster ini secara manual, Anda harus menghapusnya. Untuk informasi selengkapnya, lihat <a href="#">Dampak menonaktifkan dan membersihkan sumber daya</a>.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| <p>Pantau EKS cluster selektif menggunakan tag inklusi</p>      | <p>Terlepas dari cara Anda memilih untuk mengaktifkan Runtime Monitoring, langkah-langkah berikut akan membantu Anda memantau EKS klaster selektif yang termasuk dalam akun yang dipilih:</p> <ol style="list-style-type: none"> <li>1. Pastikan Anda tidak mengaktifkan konfigurasi agen Runtime Monitoring-Automated untuk akun terpilih yang memiliki EKS cluster yang ingin Anda pantau.</li> <li>2. Tambahkan tag ke EKS cluster Anda dengan kunci <code>asGuardDutyManaged</code> dan nilainya sebagai <code>true</code>.</li> </ol> <p>Untuk informasi selengkapnya tentang menandai EKS klaster Amazon, lihat <a href="#">Bekerja dengan tag menggunakan konsol</a> di Panduan EKS Pengguna Amazon.</p> <p>Setelah menambahkan tag, GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk EKS cluster selektif yang ingin Anda pantau.</p> <ol style="list-style-type: none"> <li>3. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <pre data-bbox="618 306 1507 499">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>  |
| Mengelola agen GuardDuty keamanan secara manual                 | <ol data-bbox="521 569 1487 905" style="list-style-type: none"> <li>1. Pertahankan konfigurasi Runtime Monitoring sama seperti yang dikonfigurasi pada langkah sebelumnya. Pastikan Anda tidak mengaktifkan Runtime Monitoring- Konfigurasi agen otomatis untuk salah satu akun yang dipilih.</li> <li>2. Pilih Konfirmasi.</li> <li>3. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</li> </ol> |

## Mengelola agen keamanan secara manual untuk EKS kluster Amazon

Bagian ini menjelaskan cara mengelola agen EKS add-on Amazon (GuardDuty agen) setelah mengaktifkan Runtime Monitoring. Untuk menggunakan Runtime Monitoring, Anda harus mengaktifkan Runtime Monitoring dan mengonfigurasi EKS add-on Amazon. `aws-guardduty-agent` Melakukan hanya satu dari dua langkah ini tidak akan membantu GuardDuty mendeteksi potensi ancaman atau menghasilkan temuan.

### Prasyarat untuk menyebarkan agen keamanan GuardDuty

Bagian ini menjelaskan prasyarat untuk menerapkan agen GuardDuty keamanan untuk cluster Anda secara manual. EKS Sebelum melanjutkan, pastikan Anda telah mengonfigurasi Runtime Monitoring untuk akun Anda. Agen GuardDuty keamanan (EKSadd-on) tidak akan berfungsi jika Anda tidak mengonfigurasi Runtime Monitoring. Untuk informasi selengkapnya, lihat [Mengaktifkan GuardDuty Runtime Monitoring](#). Setelah Anda menyelesaikan langkah-langkah berikut, lihat [Menyebarkan agen GuardDuty keamanan](#).

Pilih metode akses pilihan Anda untuk membuat VPC titik akhir Amazon.

## Console

### Buat titik VPC akhir

1. Buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Endpoints.
3. Pilih Buat Titik Akhir.
4. Pada halaman Buat titik akhir, untuk kategori Layanan, pilih Layanan titik akhir lainnya.
5. Untuk nama Layanan, masukkan **com.amazonaws.us-east-1.guardduty-data**.

Pastikan untuk mengganti *us-east-1* dengan wilayah yang benar. Ini harus Region yang sama dengan EKS cluster milik Akun AWS ID Anda.

6. Pilih Verifikasi layanan.
7. Setelah nama layanan berhasil diverifikasi, pilih VPC tempat klaster Anda berada. Tambahkan kebijakan berikut untuk membatasi penggunaan VPC titik akhir hanya ke akun tertentu. Dengan organisasi yang Condition disediakan di bawah kebijakan ini, Anda dapat memperbarui kebijakan berikut untuk membatasi akses ke titik akhir Anda. Untuk memberikan dukungan VPC endpoint ke akun tertentu IDs di organisasi Anda, lihat [Organization condition to restrict access to your endpoint](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

```
]
}
```

ID `aws:PrincipalAccount` akun harus cocok dengan akun yang berisi VPC dan VPC titik akhir. Daftar berikut menunjukkan cara berbagi VPC titik akhir dengan yang lain Akun AWS IDs:

Kondisi organisasi untuk membatasi akses ke titik akhir Anda

- Untuk menentukan beberapa akun untuk mengakses VPC titik akhir, ganti `"aws:PrincipalAccount": "111122223333"` dengan yang berikut ini:

```
"aws:PrincipalAccount": [
    "666666666666",
    "555555555555"
]
```

- Untuk memungkinkan semua anggota dari organisasi mengakses VPC titik akhir, ganti `"aws:PrincipalAccount": "111122223333"` dengan yang berikut ini:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Untuk membatasi akses sumber daya ke ID organisasi, tambahkan `ResourceOrgID` ke kebijakan.

Untuk informasi selengkapnya, lihat [ResourceOrgID](#).

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Di bawah Pengaturan tambahan, pilih Aktifkan DNS nama.
9. Di bawah Subnet, pilih subnet tempat kluster Anda berada.
10. Di bawah Grup keamanan, pilih grup keamanan yang mengaktifkan port 443 dalam terikat dari VPC (atau EKS kluster Anda). Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, [Buat grup keamanan](#).

Jika ada masalah saat membatasi izin masuk ke VPC (atau kluster) Anda, berikan dukungan ke port 443 yang di-bound dari alamat IP apa pun (). `0.0.0.0/0`



## API/CLI

- Memohon. [CreateVpcEndpoint](#)
- Gunakan nilai berikut untuk parameter:
  - Untuk nama Layanan, masukkan `com.amazonaws.us-east-1.guardduty-data`.

Pastikan untuk mengganti `us-east-1` dengan wilayah yang benar. Ini harus Region yang sama dengan EKS cluster milik Akun AWS ID Anda.

- Untuk [DNSOptions](#), aktifkan DNS opsi pribadi dengan menyetelnya ke `true`.
- Untuk AWS Command Line Interface, lihat [create-vpc-endpoint](#).

## Konfigurasi parameter agen GuardDuty keamanan (add-on) untuk Amazon EKS

Anda dapat mengonfigurasi parameter spesifik agen GuardDuty keamanan Anda untuk Amazon EKS. Dukungan ini tersedia untuk agen GuardDuty keamanan versi 1.5.0 dan di atasnya. Untuk informasi tentang versi add-on terbaru, lihat [GuardDuty agen keamanan untuk EKS cluster Amazon](#).

## Mengapa saya harus memperbarui skema konfigurasi agen keamanan

Skema konfigurasi untuk agen GuardDuty keamanan sama di semua kontainer dalam EKS kluster Amazon Anda. Jika nilai default tidak sejajar dengan beban kerja dan ukuran instans terkait, pertimbangkan untuk mengonfigurasi CPU pengaturan, pengaturan memori, dan pengaturan. `PriorityClass` `dnsPolicy` Terlepas dari bagaimana Anda mengelola GuardDuty agen untuk EKS kluster Amazon Anda, Anda dapat mengonfigurasi atau memperbarui konfigurasi parameter ini yang ada.

## Perilaku konfigurasi agen otomatis dengan parameter yang dikonfigurasi

Saat GuardDuty mengelola agen keamanan (EKS add-on) atas nama Anda, itu memperbarui add-on, sesuai kebutuhan. GuardDuty akan mengatur nilai parameter yang dapat dikonfigurasi ke nilai default. Namun, Anda masih dapat memperbarui parameter ke nilai yang diinginkan. Jika ini mengarah ke konflik, opsi default untuk `resolveConflicts` adalah `None`.

## Parameter dan nilai yang dapat dikonfigurasi

Untuk informasi tentang langkah-langkah untuk mengkonfigurasi parameter add-on, lihat:

- [Menyebarkan agen GuardDuty keamanan](#) atau

- [Memperbarui agen keamanan secara manual](#)

Tabel berikut menyediakan rentang dan nilai yang dapat Anda gunakan untuk menerapkan EKS add-on Amazon secara manual atau memperbarui pengaturan add-on yang ada.

#### CPU pengaturan

| Parameter  | Nilai default | Rentang yang dapat dikonfigurasi          |
|------------|---------------|---|
| Permintaan | 200m          | Antara 200m dan 10000m, keduanya inklusif |
| Batas      | 1000m         |   |

#### Pengaturan memori

| Parameter  | Nilai default | Rentang yang dapat dikonfigurasi            |
|------------|---------------|---|
| Permintaan | 256Mi         | Antara 256Mi dan 20000Mi, keduanya inklusif |
| Batas      | 1024Mi        |   |

#### PriorityClass pengaturan

Saat GuardDuty membuat EKS add-on Amazon untuk Anda, yang ditetapkan `PriorityClass` adalah `aws-guardduty-agent.priorityclass`. Ini berarti bahwa tidak ada tindakan yang akan diambil berdasarkan prioritas pod agen. Anda dapat mengonfigurasi parameter add-on ini dengan memilih salah satu `PriorityClass` opsi berikut:

| Dapat dikonfigurasi <b>PriorityClass</b>       | Nilai <b>preemptio nPolicy</b> | <b>preemptio nPolicy</b> deskripsi | Nilai pod |
|--|--------------------------------|------------------------------------|-----------|
| <code>aws-guardduty-agent.priorityclass</code> | Never                          | Tidak ada tindakan                 | 1000000   |

| Dapat dikonfigurasi <b>PriorityClass</b>            | Nilai <b>preemptio nPolicy</b>    | <b>preemptio nPolicy</b> deskripsi   | Nilai pod  |
|---|-----------------------------------|--|------------|
| <code>aws-guardduty-agent.priorityclass-high</code> | <code>PreemptLowerPriority</code> | Menetapkan nilai ini akan mendahului sebuah pod yang berjalan dengan nilai prioritas lebih rendah dari nilai pod agen. | 100000000  |
| <code>system-cluster-critical</code> <sup>1</sup>   | <code>PreemptLowerPriority</code> |  | 2000000000 |
| <code>system-node-critical</code> <sup>1</sup>      | <code>PreemptLowerPriority</code> |  | 2000001000 |

<sup>1</sup> Kubernetes menyediakan dua `PriorityClass` opsi ini — dan `system-cluster-critical` dan `system-node-critical`. Untuk informasi selengkapnya, lihat [PriorityClass](#) di dokumentasi Kubernetes.

## dnsPolicy pengaturan

Pilih salah satu opsi DNS kebijakan berikut yang didukung Kubernetes. Ketika tidak ada konfigurasi yang `ClusterFirst` ditentukan, digunakan sebagai nilai default.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Untuk informasi tentang kebijakan ini, lihat [DNSKebijakan Pod](#) di dokumentasi Kubernetes.

## Menyebarkan agen GuardDuty keamanan

Bagian ini menjelaskan bagaimana Anda dapat menggunakan agen GuardDuty keamanan untuk pertama kalinya untuk EKS kluster tertentu. Sebelum Anda melanjutkan dengan bagian ini, pastikan Anda telah menyiapkan prasyarat dan mengaktifkan Runtime Monitoring untuk akun Anda. Agen

GuardDuty keamanan (EKSadd-on) tidak akan berfungsi jika Anda tidak mengaktifkan Runtime Monitoring.

Pilih metode akses pilihan Anda untuk menggunakan agen GuardDuty keamanan untuk pertama kalinya.

## Console

1. Buka EKS konsol Amazon di <https://console.aws.amazon.com/eks/rumah#/cluster>.
2. Pilih nama Cluster Anda.
3. Pilih tab Add-ons.
4. Pilih Get more add-ons
5. Pada halaman Pilih add-on, pilih Amazon GuardDuty Runtime Monitoring.
6. Pada halaman Konfigurasi pengaturan add-on yang dipilih, gunakan pengaturan default. Jika Status EKS add-on Anda Memerlukan aktivasi, pilih Aktifkan GuardDuty. Tindakan ini akan membuka GuardDuty konsol untuk mengonfigurasi Runtime Monitoring untuk akun Anda.
7. Setelah mengonfigurasi Runtime Monitoring untuk akun Anda, beralih kembali ke EKS konsol Amazon. Status EKS add-on Anda seharusnya telah berubah menjadi Siap untuk menginstal.
8. (Opsional) Menyediakan EKS skema konfigurasi add-on

Untuk Versi add-on, jika Anda memilih v1.5.0 dan yang lebih baru, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihat [Konfigurasikan EKS parameter add-on](#).

- a. Perluas Pengaturan konfigurasi opsional untuk melihat parameter yang dapat dikonfigurasi serta nilai serta format yang diharapkan.
  - b. Atur parameternya. Nilai-nilai harus dalam kisaran yang disediakan di [Konfigurasikan EKS parameter add-on](#).
  - c. Pilih Simpan perubahan untuk membuat add-on berdasarkan konfigurasi lanjutan.
  - d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat [resolveConflicts](#) di EKS API Referensi Amazon.
9. Pilih Berikutnya.
  10. Pada halaman Tinjau dan buat, verifikasi semua detail, dan pilih Buat.
  11. Arahkan kembali ke detail cluster dan pilih tab Resources.

12. Anda dapat melihat pod baru dengan awalan `aws-guardduty-agent`.

## API/CLI

Anda dapat mengonfigurasi agen EKS add-on Amazon (`aws-guardduty-agent`) menggunakan salah satu opsi berikut:

- Jalankan [CreateAddon](#) untuk akun Anda.

### Note

Untuk `addonVersion`, jika Anda memilih `v1.5.0` dan yang lebih baru, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi selengkapnya, lihat [Konfigurasi EKS parameter add-on](#).

Gunakan nilai berikut untuk parameter permintaan:

- Untuk `addonName`, masukkan `aws-guardduty-agent`.

Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on `v1.5.0` dan yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-values 'file://example.json'
```

## Example Contoh.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
```

```
"memory": "2048Mi"
}
}
}
```

- Untuk informasi tentang didukung `addonVersion` , Lihat [Versi Kubernetes didukung oleh agen keamanan GuardDuty](#) .
- Atau, Anda dapat menggunakan AWS CLI. Untuk informasi selengkapnya, lihat [create-addon](#).

## Memperbarui agen keamanan secara manual

Ketika Anda mengelola agen GuardDuty keamanan secara manual, Anda bertanggung jawab untuk memperbaruinya untuk akun Anda. Untuk pemberitahuan tentang versi agen baru, Anda dapat berlangganan RSS feed ke [GuardDuty sejarah rilis agen](#).

Anda dapat memperbarui agen keamanan ke versi terbaru untuk mendapatkan manfaat dari dukungan dan peningkatan yang ditambahkan. Jika versi agen Anda saat ini mencapai akhir dukungan standar, maka untuk terus menggunakan Runtime Monitoring (atau EKS Runtime Monitoring), Anda harus memperbarui versi agen Anda saat ini. Untuk informasi tentang versi rilis, lihat [GuardDuty agen keamanan untuk EKS cluster Amazon](#).

## Prasyarat

Sebelum Anda memperbarui versi agen keamanan, pastikan bahwa versi agen yang Anda rencanakan untuk digunakan sekarang, kompatibel dengan versi Kubernetes Anda. Untuk informasi selengkapnya, lihat [Versi Kubernetes didukung oleh agen keamanan GuardDuty](#) .

## Console

1. Buka EKS konsol Amazon di <https://console.aws.amazon.com/eks/umah#/cluster>.
2. Pilih nama Cluster Anda.
3. Pilih Add-on.
4. Di bawah Add-on, pilih GuardDutyRuntime Monitoring.
5. Pilih Edit untuk memperbarui detail agen.
6. Pada halaman Configure GuardDuty Runtime Monitoring, perbarui detailnya.

## 7. (Opsional) Memperbarui parameter konfigurasi add-on

Jika versi EKS add-on Anda 1.5.0 atau lebih tinggi, Anda juga dapat memperbarui pengaturan konfigurasi add-on.

- a. Perluas pengaturan konfigurasi opsional untuk melihat skema konfigurasi.
- b. Perbarui nilai parameter berdasarkan rentang yang disediakan di [Konfigurasi EKS parameter add-on](#).
- c. Pilih Simpan perubahan untuk memulai pembaruan.
- d. Untuk metode Resolusi konflik, opsi yang Anda pilih akan digunakan untuk menyelesaikan konflik saat Anda memperbarui nilai parameter ke nilai non-default. Untuk informasi selengkapnya tentang opsi yang tercantum, lihat [resolveConflicts](#) di EKS API Referensi Amazon.

### API/CLI

Untuk memperbarui agen GuardDuty keamanan untuk EKS kluster Amazon Anda, lihat [Memperbarui add-on](#).

#### Note

Untuk `add-on-version`, jika Anda memilih v1.5.0 dan yang lebih baru, Runtime Monitoring mendukung konfigurasi parameter spesifik agen. GuardDuty Untuk informasi tentang rentang parameter, lihat [Konfigurasi EKS parameter add-on](#).

Anda dapat menggunakan AWS CLI contoh berikut saat menggunakan nilai yang dapat dikonfigurasi yang didukung untuk versi add-on v1.5.0 dan yang lebih baru. Pastikan untuk mengganti nilai placeholder yang disorot dengan warna merah dan yang terkait `Example.json` dengan nilai yang dikonfigurasi.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-values 'file://example.json'
```

### Example Contoh.json

```
{
```

```
"priorityClassName": "aws-guardduty-agent.priorityclass-high",
"dnsPolicy": "Default",
"resources": {
  "requests": {
    "cpu": "237m",
    "memory": "512Mi"
  },
  "limits": {
    "cpu": "2000m",
    "memory": "2048Mi"
  }
}
}
```

Jika versi EKS add-on Amazon Anda 1.5.0 atau lebih tinggi, dan Anda telah mengonfigurasi skema add-on, Anda dapat memverifikasi apakah nilai muncul dengan benar untuk kluster Anda atau tidak. Untuk informasi selengkapnya, lihat [Memverifikasi pembaruan skema konfigurasi](#).

### Memverifikasi pembaruan skema konfigurasi

Setelah Anda mengonfigurasi parameter, lakukan langkah-langkah berikut untuk memverifikasi bahwa skema konfigurasi telah diperbarui:

1. Buka EKS konsol Amazon di <https://console.aws.amazon.com/eks/rumah#/cluster>.
2. Pada panel navigasi, silakan pilih Kluster.
3. Pada halaman Clusters, pilih nama Cluster yang ingin Anda verifikasi pembaruannya.
4. Pilih tab Sumber Daya.
5. Dari panel Jenis sumber daya, di bawah Beban kerja, pilih. DaemonSets
6. Pilih aws-guardduty-agent.
7. Pada aws-guardduty-agent halaman, pilih Tampilan mentah untuk melihat respons yang tidak diformat. JSON Verifikasi bahwa parameter yang dapat dikonfigurasi menampilkan nilai yang Anda berikan.

Setelah Anda memverifikasi, beralih ke GuardDuty konsol. Pilih yang sesuai Wilayah AWS dan lihat status cakupan untuk EKS kluster Amazon Anda. Untuk informasi selengkapnya, lihat [Cakupan untuk EKS cluster Amazon](#).



## Mengkonfigurasi EKS Runtime Monitoring (hanya) API

Sebelum mengonfigurasi EKS Runtime Monitoring di akun Anda, pastikan Anda menggunakan salah satu platform terverifikasi yang mendukung versi Kubernetes yang saat ini digunakan. Untuk lebih lanjut, lihat [Memvalidasi persyaratan arsitektur](#).

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan [Memeriksa EKS status konfigurasi Runtime Monitoring](#) dan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk [Nonaktifkan EKS Runtime Monitoring](#). Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk Runtime Monitoring. EKS

## Mengkonfigurasi EKS Runtime Monitoring untuk akun mandiri

Untuk akun yang terkait dengan [AWS Organizations](#), lihat [Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun](#).

Pilih metode akses pilihan Anda untuk mengaktifkan EKS Runtime Monitoring untuk akun Anda.


### API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan   | Langkah-langkahnya  |
|---|---|
| Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster) | <ol style="list-style-type: none"> <li>Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.<br/><br/>Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>ENABLED</code>.</li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <ol style="list-style-type: none"><li>2. Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <code>ListDetectors</code> API. <code>detectorId</code></li></ol> <p>Contoh berikut memungkinkan keduanya <code>EKS_RUNTIME_MONITORING</code> dan <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya  |
|--|---|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged - false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>3.</p> <div data-bbox="743 304 1507 709" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS klaster Anda sebelum menyetel STATUS dari EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> </div> <p>Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <pre>aws guardduty update-detector --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "<i>ENABLED</i>", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "<i>ENABLED</i>"}] ]'</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Pantau EKS cluster selektif (menggunakan tag inklusi)           | <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged - . true Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul><p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></li></ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

3. Jalankan [updateDetector](#) API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai `ENABLED`.

Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as `DISABLED`.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan `- pair. GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'
```

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Mengelola agen keamanan secara manual                           | <p>1. Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.</p> <p>Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> sebagai <code>DISABLED</code>.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan <code>EKS_RUNTIME_MONITORING</code> dan menonaktifkan <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'</pre> <p>2. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</p> |

## Mengkonfigurasi EKS Runtime Monitoring untuk lingkungan multi-akun

Di lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan EKS Runtime Monitoring untuk akun anggota, dan



mengelola manajemen GuardDuty agen untuk EKS klaster milik akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun](#).

Mengkonfigurasi EKS Runtime Monitoring untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk EKS klaster milik akun administrator yang didelegasikan GuardDuty .

## API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan          | Langkah-langkahnya   |
|--|--|
| <p>Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster)</p> | <p>Jalankan <a href="#">updateDetectorAPI</a> dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.</p> <p>Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>ENABLED</code>.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectorsAPI</a>.<br/><code>detectorId</code></p> |


Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

Contoh berikut memungkinkan keduanya EKS\_RUNTIME\_MONITORING dan EKS\_ADDON\_MANAGEMENT :

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'
```

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>3.</p> <div data-bbox="743 304 1507 714" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS klaster Anda sebelum menyetel STATUS dari EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> </div> <p>Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre>aws guardduty update-detector --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " <i>ENABLED</i>", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " <i>ENABLED</i>"}] ]'</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Pantau EKS cluster selektif (menggunakan tag inklusi)           | <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged -. true Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul><p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></li></ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

3. Jalankan [updateDetector](#) API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama `features` objek sebagai `EKS_RUNTIME_MONITORING` dan status sebagai `ENABLED`.

Tetapkan status untuk `EKS_ADDON_MANAGEMENT` as `DISABLED`.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan `- pair. GuardDutyManaged true`

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Contoh berikut memungkinkan `EKS_RUNTIME_MONITORING` dan menonaktifkan `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'
```

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Mengelola agen keamanan secara manual                           | <p>1. Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama <code>features</code> objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.</p> <p>Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> sebagai <code>DISABLED</code>.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan <code>EKS_RUNTIME_MONITORING</code> dan menonaktifkan <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> <p>2. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</p> |

Aktifkan EKS Runtime Monitoring secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan EKS Runtime Monitoring untuk semua akun anggota. Ini termasuk akun GuardDuty administrator yang didelegasikan, akun anggota yang ada,



dan akun baru yang bergabung dengan organisasi. Pilih pendekatan yang Anda inginkan untuk mengelola agen GuardDuty keamanan untuk EKS kluster yang termasuk dalam akun anggota ini.


## API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan          | Langkah-langkahnya   |
|--|--|
| <p>Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster)</p> | <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="558 1556 1507 1829">aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya


 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li data-bbox="558 373 1507 598"> <p>Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed <code>.false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</p> </li> <li data-bbox="558 619 1507 1585"> <p>Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:</p> <ul style="list-style-type: none"> <li data-bbox="621 892 1458 924">• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li> <li data-bbox="621 945 1490 976">• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code>.</li> <li data-bbox="621 997 1458 1029">• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li data-bbox="621 1050 1409 1144">• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code>:</p> <pre data-bbox="672 1375 1409 1564">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="558 1606 1507 1837"> <p><b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS kluster Anda sebelum menyetel STATUS dari <code>EKS_RUNTIME_MONITORING</code> ke <code>ENABLED</code>; jika tidak, agen</p> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p data-bbox="621 346 1507 478">GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> <p data-bbox="621 548 1412 724">Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai EKS_RUNTIME_MONITORING dan status sebagai ENABLED.</p> <p data-bbox="621 772 1328 850">Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED.</p> <p data-bbox="621 898 1463 1031">GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p data-bbox="621 1079 1474 1304">Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p data-bbox="621 1352 1401 1430">Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="621 1478 1507 1730">aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <div data-bbox="621 352 1507 569"><p> <b>Note</b></p><p>Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p></div> <p data-bbox="621 642 1479 863">Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| <p>Pantau EKS cluster selektif (menggunakan tag inklusi)</p>    | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed <code>- . true</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya , gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna.AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Jalankan <a href="#">updateDetectorAPI</a> dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.</li> </ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

## Langkah-langkahnya

Tetapkan status untuk EKS\_ADDON\_MANAGEMENT asDISABLED.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan - pair. GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

Contoh berikut memungkinkan EKS\_RUNTIME\_MONITORING dan menonaktifkan EKS\_ADDON\_MANAGEMENT :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Mengelola agen keamanan secara manual                           | <p>akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> <ol style="list-style-type: none"> <li> <p>Jalankan <a href="#">updateDetector</a> API dengan menggunakan ID detektor regional Anda sendiri dan meneruskan nama features objek sebagai <code>EKS_RUNTIME_MONITORING</code> dan status sebagai <code>ENABLED</code>.</p> <p>Tetapkan status untuk <code>EKS_ADDON_MANAGEMENT</code> as <code>DISABLED</code>.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan <code>EKS_RUNTIME_MONITORING</code> dan menonaktifkan <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] } ]'</pre> </li> <li> <p>Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</p> </li> </ol> |

Mengkonfigurasi EKS Runtime Monitoring untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan EKS Runtime Monitoring dan mengelola agen GuardDuty keamanan untuk akun anggota aktif yang ada di organisasi Anda.




## API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan          | Langkah-langkahnya   |
|--|--|
| <p>Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster)</p> | <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="558 1430 1507 1701">aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya


 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li data-bbox="558 373 1507 600"> <p>Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed <code>.false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</p> </li> <li data-bbox="558 621 1507 1591"> <p>Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:</p> <ul style="list-style-type: none"> <li data-bbox="623 890 1458 926">• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li> <li data-bbox="623 947 1490 982">• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code>.</li> <li data-bbox="623 1003 1458 1039">• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li data-bbox="623 1060 1409 1144">• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya, gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p> <pre data-bbox="672 1381 1409 1570">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="558 1612 1507 1837"> <p><b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS kluster Anda sebelum menyetel STATUS dari EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen</p> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p data-bbox="623 352 1507 478">GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> <p data-bbox="623 548 1477 722">Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p data-bbox="623 772 1325 852">Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p data-bbox="623 900 1463 1031">GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p data-bbox="623 1079 1474 1304">Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p data-bbox="623 1352 1401 1432">Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="623 1486 1507 1736">aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <div data-bbox="621 352 1507 569"><p> <b>Note</b></p><p>Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p></div> <p data-bbox="621 640 1479 865">Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| <p>Pantau EKS cluster selektif (menggunakan tag inklusi)</p>    | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangan kunci-nilai adalah GuardDuty Managed <code>- . true</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas terpercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code>.</li> <li>• Ganti <code>ec2&gt;DeleteTags</code> dengan <code>eks:UntagResource</code>.</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas terpercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas terpercaya, gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectorsAPI</a> operasi menggunakan akun Anda sendiri <code>detector ID</code>.</li> </ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

## Langkah-langkahnya

Tetapkan status untuk EKS\_ADDON\_MANAGEMENT asDISABLED.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan - pair. GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

Contoh berikut memungkinkan EKS\_RUNTIME\_MONITORING dan menonaktifkan EKS\_ADDON\_MANAGEMENT :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "DISABLED"}] ]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p>  |
| <p>Mengelola agen keamanan secara manual</p>                    | <ol style="list-style-type: none"> <li> <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectorsAPI</a> operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectorsAPI</a>. <code>detectorId</code></p> <p>Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> </li> <li> <p>Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS kluster Amazon</a>.</p> </li> </ol> |



## Aktifkan EKS Runtime Monitoring secara otomatis untuk anggota baru

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan EKS Runtime Monitoring secara otomatis dan memilih pendekatan untuk cara mengelola agen GuardDuty keamanan untuk akun baru yang bergabung dengan organisasi Anda.

### API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan          | Langkah-langkahnya   |
|--|--|
| <p>Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster)</p> | <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan <a href="#">UpdateOrganizationConfiguration</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan


Langkah-langkahnya

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectorsAPI`.  
`detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'
```

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged</code> - <code>false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p>3.</p> <div data-bbox="743 304 1507 709" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS kluster Anda sebelum menyetel STATUS dari EKS_RUNTIME_MONITORING ke ENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> </div> <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan <a href="#">UpdateOrganizationConfiguration</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT as ENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <pre data-bbox="748 520 1507 842">aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'</pre> <p>Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Pantau EKS cluster selektif (menggunakan tag inklusi)           | <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged -. true Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2&gt;DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul><p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></li></ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan akun Anda sendiri *detector ID*.

Tetapkan status untuk EKS\_ADDON\_MANAGEMENT asDISABLED.

GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan - pair. GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

Contoh berikut memungkinkan EKS\_RUNTIME\_MONITORING dan menonaktifkan EKS\_ADDON\_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu
```

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <pre data-bbox="743 296 1507 401">ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'</pre> <p data-bbox="743 436 1507 730">Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> |



| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Mengelola agen keamanan secara manual                           | <p>1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun baru Anda, jalankan <a href="#">UpdateOrganizationConfiguration</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT untuk satu akun. Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p> <p>Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <pre data-bbox="747 1428 1507 1753">aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'</pre> <p>Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya a.</p> <ol style="list-style-type: none"> <li>2. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS klaster Amazon</a>.</li> </ol> |

Aktifkan EKS Runtime Monitoring untuk akun anggota aktif individu

#### API/CLI

Berdasarkan [Pendekatan untuk mengelola agen GuardDuty keamanan](#), Anda dapat memilih pendekatan yang disukai dan mengikuti langkah-langkah seperti yang disebutkan dalam tabel berikut.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan          | Langkah-langkahnya  |
|--|---|
| <p>Kelola agen keamanan melalui GuardDuty (Pantau semua EKS cluster)</p> | <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon di akun Anda.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri.</p> |


Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

Contoh berikut memungkinkan keduanya `EKS_RUNTIME_MONITORING` dan `EKS_ADDON_MANAGEMENT` :


```
aws guardduty update-member-detectors --  
detector-id 12abc34d567e8fa901bc2d34e56  
789f0 --account-ids 111122223333 --feature  
s '[{"Name" : "EKS_RUNTIME_MONITORING",  
"Status" : "ENABLED", "AdditionalConfigu  
ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",  
"Status" : "ENABLED"}]} ]'
```


 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan  | Langkah-langkahnya   |
|--|--|
| <p>Pantau semua EKS cluster tetapi kecualikan beberapa di antaranya (menggunakan tag pengecualian)</p> | <ol style="list-style-type: none"> <li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah <code>GuardDutyManaged - false</code> Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li> <li>2. Untuk mencegah modifikasi tag, kecualikan oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut: <ul style="list-style-type: none"> <li>• Ganti <code>ec2:CreateTags</code> dengan <code>eks:TagResource</code> .</li> <li>• Ganti <code>ec2:DeleteTags</code> dengan <code>eks:UntagResource</code> .</li> <li>• Ganti <code>access-project</code> dengan <code>GuardDutyManaged</code></li> <li>• Ganti <code>123456789012</code> dengan Akun AWS ID entitas tepercaya.</li> </ul> <p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapa <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <p>3.</p> <div data-bbox="743 304 1507 709" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> <b>Note</b></p> <p>Selalu tambahkan tag pengecualian ke EKS klaster Anda sebelum menyetel STATUS dari EKS_RUNTIME_MONITORING keENABLED; jika tidak, agen GuardDuty keamanan akan digunakan di semua EKS cluster di akun Anda.</p> </div> <p>Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asENABLED.</p> <p>GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang belum dikecualikan dari pemantauan.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan keduanya EKS_RUNTIME_MONITORING dan EKS_ADDON_MANAGEMENT :</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
|   | <pre data-bbox="748 306 1507 621">aws guardduty update-member-detectors --<br/>detector-id 12abc34d567e8fa901bc2d34e56<br/>789f0 --account-ids 111122223333 --feature<br/>s '[{"Name" : "EKS_RUNTIME_MONITORING",<br/>"Status" : "ENABLED", "AdditionalConfigu<br/>ration" : [{"Name" : "EKS_ADDON_MANAGEM<br/>ENT", "Status" : " ENABLED"}] ]'</pre> <div data-bbox="743 657 1507 877"><p> <b>Note</b></p><p>Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p></div> <p data-bbox="743 947 1487 1220">Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.</p> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
| Pantau EKS cluster selektif (menggunakan tag inklusi)           | <ol style="list-style-type: none"><li>1. Tambahkan tag ke EKS cluster yang ingin Anda kecualikan agar tidak dipantau. Pasangkan kunci-nilai adalah GuardDutyManaged -. true Untuk informasi selengkapnya tentang menambahkan tag, lihat <a href="#">Bekerja dengan tag menggunakan CLI, API, atau eksctl di Panduan Pengguna Amazon EKS</a>.</li><li>2. Untuk mencegah modifikasi tag, kecuali oleh entitas tepercaya, gunakan kebijakan yang disediakan dalam <a href="#">Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal resmi dalam Panduan Pengguna AWS Organizations</a> Dalam kebijakan ini, ganti detail berikut:<ul style="list-style-type: none"><li>• Ganti <i>ec2:CreateTags</i> dengan <code>eks:TagResource</code> .</li><li>• Ganti <i>ec2:DeleteTags</i> dengan <code>eks:UntagResource</code> .</li><li>• Ganti <i>access-project</i> dengan GuardDuty Managed</li><li>• Ganti <i>123456789012</i> dengan Akun AWS ID entitas tepercaya.</li></ul><p>Jika Anda memiliki lebih dari satu entitas tepercaya , gunakan contoh berikut untuk menambahkan beberapaPrincipalArn :</p><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></li></ol> |

Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan

Langkah-langkahnya

3. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.

Tetapkan status untuk EKS\_ADDON\_MANAGEMENT asDISABLED.


GuardDuty akan mengelola penyebaran dan pembaruan ke agen keamanan untuk semua EKS cluster Amazon yang telah ditandai dengan - pair. GuardDutyManaged true

Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. detectorId

Contoh berikut memungkinkan EKS\_RUNTIME\_MONITORING dan menonaktifkan EKS\_ADDON\_MANAGEMENT :

```
aws guardduty update-member-detectors --
detector-id 12abc34d567e8fa901bc2d34e56
789f0 --account-ids 111122223333 --feature
s '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "ENABLED", "AdditionalConfigu
ration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " DISABLED"}] ]'
```



| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya   |
|---|--|
|   | <p data-bbox="776 338 894 373"> <b>Note</b></p> <p data-bbox="824 396 1438 478">Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.</p> <p data-bbox="743 590 1487 863">Ketika kode telah berhasil dijalankan, daftar <code>UnprocessedAccounts</code> akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya</p> <ol style="list-style-type: none"><li data-bbox="743 835 773 863">a.</li></ol> |

| Pendekatan yang disukai untuk mengelola agen GuardDuty keamanan | Langkah-langkahnya  |
|---|---|
| Mengelola agen keamanan secara manual                           | <ol style="list-style-type: none"> <li data-bbox="678 321 1513 1470"> <p>1. Untuk mengaktifkan EKS Runtime Monitoring secara selektif untuk akun anggota Anda, jalankan <a href="#">updateMemberDetectors</a> API operasi menggunakan akun Anda sendiri <i>detector ID</i>.</p> <p>Tetapkan status untuk EKS_ADDON_MANAGEMENT asDISABLED.</p> <p>Atau, Anda dapat menggunakan AWS CLI perintah dengan menggunakan ID detektor regional Anda sendiri. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <a href="https://console.aws.amazon.com/guardduty/konsol">https://console.aws.amazon.com/guardduty/konsol</a>, atau jalankan <a href="#">ListDetectors</a> API. <code>detectorId</code></p> <p>Contoh berikut memungkinkan EKS_RUNTIME_MONITORING dan menonaktifkan EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="747 1161 1507 1476">aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 5555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> </li> <li data-bbox="678 1491 1513 1627"> <p>2. Untuk mengelola agen keamanan, lihat <a href="#">Mengelola agen keamanan secara manual untuk EKS klaster Amazon</a>.</p> </li> </ol> |

# Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring

Dengan peluncuran GuardDuty Runtime Monitoring, cakupan deteksi ancaman telah diperluas ke ECS wadah Amazon dan EC2 instans Amazon. EKS Pengalaman Runtime Monitoring kini telah dikonsolidasikan ke dalam Runtime Monitoring. Anda dapat mengaktifkan Runtime Monitoring dan mengelola agen GuardDuty keamanan individual untuk setiap jenis sumber daya (EC2 instans Amazon, ECS klaster Amazon, dan EKS klaster Amazon) yang ingin Anda pantau perilaku runtime.

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan [Memeriksa EKS status konfigurasi Runtime Monitoring](#) dan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk [Nonaktifkan EKS Runtime Monitoring](#). Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk Runtime Monitoring. EKS

Untuk bermigrasi dari EKS Runtime Monitoring ke Runtime Monitoring

1. GuardDuty Konsol mendukung EKS Runtime Monitoring sebagai bagian dari Runtime Monitoring.

Anda dapat mulai menggunakan Runtime Monitoring oleh [Memeriksa EKS status konfigurasi Runtime Monitoring](#) organisasi dan akun Anda.

Pastikan untuk tidak menonaktifkan EKS Runtime Monitoring sebelum mengaktifkan Runtime Monitoring. Jika Anda menonaktifkan EKS Runtime Monitoring, manajemen EKS add-on Amazon juga akan dinonaktifkan. Lanjutkan dengan langkah-langkah berikut dalam urutan yang tercantum.

2. Pastikan Anda memenuhi semua [Prasyarat untuk mengaktifkan Runtime Monitoring](#).

3. Aktifkan Runtime Monitoring dengan mereplikasi pengaturan konfigurasi organisasi yang sama untuk Runtime Monitoring seperti yang Anda miliki untuk EKS Runtime Monitoring. Untuk informasi selengkapnya, lihat [Mengaktifkan Runtime Monitoring](#).

- Jika Anda memiliki akun mandiri, Anda harus mengaktifkan Runtime Monitoring.

Jika agen GuardDuty keamanan Anda sudah digunakan, pengaturan yang sesuai direplikasi secara otomatis dan Anda tidak perlu mengonfigurasi pengaturan lagi.

- Jika Anda memiliki organisasi dengan pengaturan auto-enablement, pastikan untuk mereplikasi pengaturan auto-enablement yang sama untuk Runtime Monitoring.

- Jika Anda memiliki organisasi dengan pengaturan yang dikonfigurasi untuk akun anggota aktif yang ada secara individual, pastikan untuk mengaktifkan Runtime Monitoring dan mengonfigurasi agen GuardDuty keamanan untuk anggota ini secara individual.
4. Setelah Anda memastikan bahwa pengaturan Runtime Monitoring dan agen GuardDuty keamanan sudah benar, [nonaktifkan EKS Runtime Monitoring](#) dengan menggunakan perintah API atau perintah. AWS CLI
  5. (Opsional) jika Anda ingin membersihkan sumber daya apa pun yang terkait dengan agen GuardDuty keamanan, lihat [Dampak menonaktifkan dan membersihkan sumber daya](#).

Jika Anda ingin terus menggunakan EKS Runtime Monitoring tanpa mengaktifkan Runtime Monitoring, lihat. [Mengkonfigurasi EKS Runtime Monitoring \(hanya\) API](#)

## Memeriksa EKS status konfigurasi Runtime Monitoring

Gunakan AWS CLI perintah berikut APIs atau untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada.

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada di akun Anda

- Jalankan [GetDetector](#) untuk memeriksa status konfigurasi akun Anda sendiri.
- Atau, Anda dapat menjalankan perintah berikut dengan menggunakan AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Pastikan untuk mengganti ID detektor Wilayah Anda Akun AWS dan saat ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Untuk memeriksa status konfigurasi EKS Runtime Monitoring yang ada untuk organisasi Anda (hanya sebagai akun GuardDuty administrator yang didelegasikan)

- Jalankan [DescribeOrganizationConfiguration](#) untuk memeriksa status konfigurasi organisasi Anda.

Atau, Anda dapat menjalankan perintah berikut menggunakan AWS CLI:

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Pastikan untuk mengganti ID detektor dengan ID detektor akun GuardDuty administrator yang didelegasikan dan Wilayah dengan Wilayah Anda saat ini. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

## Menonaktifkan EKS Runtime Monitoring setelah bermigrasi ke Runtime Monitoring

Setelah Anda memastikan bahwa pengaturan yang ada untuk akun atau organisasi Anda telah direplikasi ke Runtime Monitoring, Anda dapat menonaktifkan EKS Runtime Monitoring.

Untuk menonaktifkan EKS Runtime Monitoring

- Untuk menonaktifkan EKS Runtime Monitoring di akun Anda sendiri

Jalankan [UpdateDetector](#) API dengan regional Anda sendiri *detector-id*.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan daerah Anda sendiri *detector-id*.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Untuk menonaktifkan EKS Runtime Monitoring untuk akun anggota di organisasi Anda

Jalankan [UpdateMemberDetectors](#) API dengan regional *detector-id* dari akun GuardDuty administrator organisasi yang didelegasikan.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan regional *detector-id* dari akun GuardDuty administrator yang didelegasikan dari organisasi dan *111122223333* dengan Akun AWS ID akun anggota yang ingin Anda nonaktifkan fitur ini.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "DISABLED"}]'
```

- Untuk memperbarui pengaturan EKS Runtime Monitoring, aktifkan otomatis untuk organisasi Anda

Lakukan langkah berikut hanya jika Anda telah mengonfigurasi pengaturan pengaktifan otomatis EKS Runtime Monitoring ke akun anggota baru (NEW) atau semua (ALL) di organisasi. Jika Anda sudah mengonfigurasinya sebagai NONE, maka Anda dapat melewati langkah ini.

#### Note

Menyetel konfigurasi aktifkan otomatis EKS Runtime Monitoring NONE berarti bahwa EKS Runtime Monitoring tidak akan diaktifkan secara otomatis untuk akun anggota yang ada atau ketika akun anggota baru bergabung dengan organisasi Anda.

Jalankan [UpdateOrganizationConfigurationAPI](#) dengan regional *detector-id* dari akun GuardDuty administrator organisasi yang didelegasikan.

Atau, Anda dapat menggunakan AWS CLI perintah berikut. Ganti *12abc34d567e8fa901bc2d34e56789f0* dengan regional *detector-id* dari akun GuardDuty administrator organisasi yang didelegasikan. Ganti *EXISTING\_VALUE* dengan konfigurasi Anda saat ini untuk mengaktifkan otomatis GuardDuty.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
--features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

## Menilai cakupan runtime untuk sumber daya Anda

Setelah Anda mengaktifkan Runtime Monitoring dan agen GuardDuty keamanan disebarkan ke sumber daya Anda, GuardDuty berikan statistik cakupan untuk jenis sumber daya yang sesuai dan status cakupan individual untuk sumber daya milik akun Anda. Status cakupan ditentukan dengan memastikan bahwa Anda telah mengaktifkan Runtime Monitoring, VPC titik akhir Amazon Anda telah dibuat, dan agen GuardDuty keamanan untuk sumber daya terkait telah digunakan. Status cakupan Sehat menunjukkan bahwa ketika ada peristiwa runtime yang terkait dengan sumber daya

Anda, GuardDuty dapat menerima peristiwa runtime tersebut melalui VPC titik akhir Amazon, dan memantau perilakunya. Jika ada masalah pada saat mengonfigurasi Runtime Monitoring, membuat VPC endpoint Amazon, atau menerapkan agen GuardDuty keamanan, status cakupan akan muncul sebagai Tidak Sehat. Jika status cakupan tidak sehat, tidak GuardDuty akan dapat menerima atau memantau perilaku runtime dari sumber daya yang sesuai, atau menghasilkan temuan Runtime Monitoring.

Topik berikut akan membantu Anda meninjau statistik cakupan, mengonfigurasi EventBridge pemberitahuan, dan memecahkan masalah cakupan untuk jenis sumber daya tertentu.

## Daftar Isi

- [Cakupan untuk EC2 instans Amazon](#)
- [Cakupan untuk ECS cluster Amazon](#)
- [Cakupan untuk EKS cluster Amazon](#)
- [Pertanyaan yang sering diajukan \(FAQs\)](#)

## Cakupan untuk EC2 instans Amazon

Untuk EC2 sumber daya Amazon, cakupan runtime dievaluasi pada tingkat instans. EC2Instans Amazon Anda dapat menjalankan beberapa jenis aplikasi dan beban kerja antara lain di lingkungan Anda. AWS Fitur ini juga mendukung EC2 instans Amazon yang ECS dikelola Amazon dan jika Anda memiliki ECS klaster Amazon yang berjalan di EC2 instans Amazon, masalah cakupan pada tingkat instans akan muncul di bawah cakupan EC2 runtime Amazon.

### Topik

- [Meninjau statistik cakupan](#)
- [Mengkonfigurasi pemberitahuan perubahan status cakupan](#)
- [Memecahkan masalah cakupan](#)

## Meninjau statistik cakupan

Statistik cakupan untuk EC2 instans Amazon yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase EC2 contoh sehat di semua EC2 instance yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

(Contoh Sehat/Semua contoh) \* 100

Jika Anda juga telah menerapkan agen GuardDuty keamanan untuk ECS kluster Amazon Anda, maka masalah cakupan tingkat instans apa pun yang terkait dengan ECS kluster Amazon yang berjalan di EC2 instans Amazon akan muncul sebagai masalah cakupan runtime EC2 instans Amazon.

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

## Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime EC2 instance, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap EC2 instans Amazon yang tersedia di tabel daftar Instans.
  - Anda dapat memfilter tabel daftar Instance dengan kolom berikut:
    - ID Akun
    - Jenis manajemen agen
    - Versi agen
    - Status cakupan
    - ID Instance
    - Cluster ARN
- Jika salah satu EC2 instans Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah menyertakan informasi tambahan tentang alasan status Tidak Sehat.

## API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan ini API.
  - Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`



- AGENT\_VERSION
- MANAGEMENT\_TYPE
- INSTANCE\_ID
- CLUSTER\_ARN
- Ketika `filter-criteria` termasuk RESOURCE\_TYPE sebagai EC2, Runtime Monitoring tidak mendukung penggunaan ISSUE sebagai AttributeName. Jika Anda menggunakannya, API respons akan menghasilkan `InvalidInputException`.

Anda dapat mengubah contoh AttributeName `sort-criteria` dengan opsi berikut:

- ACCOUNT\_ID
- COVERAGE\_STATUS
- INSTANCE\_ID
- UPDATED\_AT
- Anda dapat mengubah `max-results` (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}]} ]' --max-results 5
```

- Jalankan `GetCoverageStatistics` API untuk mengambil statistik agregat cakupan berdasarkan `statisticsType`
- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
  - COUNT\_BY\_COVERAGE\_STATUS— Merupakan statistik cakupan untuk EKS cluster yang dikumpulkan berdasarkan status cakupan.
  - COUNT\_BY\_RESOURCE\_TYPE— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
  - Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
    - ACCOUNT\_ID
    - RESOURCE\_TYPE

- COVERAGE\_STATUS
  - AGENT\_VERSION
  - MANAGEMENT\_TYPE
  - INSTANCE\_ID
  - CLUSTER\_ARN
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Jika status cakupan EC2 instans Anda tidak sehat, lihat [Memecahkan masalah cakupan](#).

## Mengkonfigurasi pemberitahuan perubahan status cakupan

Status cakupan EC2 instans Amazon Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggung jawaban berubah, kami sarankan Anda untuk memantau status pertanggung jawaban secara berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di [EventBridge bus](#) untuk akun Anda.

### Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan EC2 instans Amazon Anda berubah dari Healthy keUnhealthy, detail-type seharusnya *GuardDuty Runtime Protection Unhealthy*. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy keHealthy, ganti nilai dengan detail-type *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EC2",
      "ec2InstanceDetails": {
        "instanceId": "",
        "instanceType": "",
        "clusterArn": "",
        "agentDetails": {
          "version": ""
        },
        "managementType": ""
      }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

## Memecahkan masalah cakupan

Jika status cakupan EC2 instans Amazon Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Jika EC2 instans Anda dikaitkan dengan EKS klaster dan agen keamanan untuk EKS diinstal baik secara manual atau melalui konfigurasi agen otomatis, maka untuk memecahkan masalah cakupan, lihat [Cakupan untuk EKS cluster Amazon](#)

Tabel berikut mencantumkan jenis masalah dan langkah pemecahan masalah yang sesuai.

| Jenis masalah            | Pesan masalah              | Langkah pemecahan masalah   |
|--------------------------|----------------------------|---|
| Tidak Ada Pelaporan Agen | Menunggu SSM pemberitahuan | <p>Menerima SSM pemberitahuan mungkin memakan waktu beberapa menit.</p> <p>Pastikan EC2 instans Amazon SSM dikelola. Untuk informasi selengkapnya, lihat langkah-langkah di bawah Metode 1 - Dengan menggunakan AWS Systems Manager di <a href="#">Memasang agen keamanan secara manual</a>.</p>  |
|                          | (Kosong dengan sengaja)    | <p>Jika Anda mengelola agen GuardDuty keamanan secara manual, pastikan Anda mengikuti langkah-langkah di bawah ini <a href="#">Mengelola agen keamanan secara manual untuk EC2 instans Amazon</a>.</p> <p>Jika Anda telah mengaktifkan konfigurasi agen otomatis:</p> <ul style="list-style-type: none"> <li>• EC2Instance Anda SSM dikelola.</li> <li>• Lihat status agen keamanan Anda secara berkala. Untuk informasi selengkapnya, lihat <a href="#">Memvalidasi status instalasi agen GuardDuty keamanan</a>.</li> </ul> <p>Validasi bahwa VPC titik akhir untuk EC2 instans Amazon Anda dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat <a href="#">Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?</a>.</p> <p>Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin <code>guardduty:SendSecurityTelemetry</code> Untuk informasi selengkapnya, lihat <a href="#">Memvalidasi kebijakan kontrol layanan organisasi Anda</a>.</p> |
|                          | Agen terputus              | <ul style="list-style-type: none"> <li>• Lihat status agen keamanan Anda. Untuk informasi selengkapnya, lihat <a href="#">Memvalidasi status instalasi agen GuardDuty keamanan</a>.</li> <li>• Lihat log agen keamanan untuk mengidentifikasi akar penyebab potensial. Log memberikan kesalahan</li> </ul>  |
|                          |                            |   |

| Jenis masalah                 | Pesan masalah                                  | Langkah pemecahan masalah   |
|-------------------------------|--|---|
|                               |  | <p>terperinci yang dapat Anda gunakan untuk memecahkan masalah sendiri. File log tersedia di bawah <code>/var/log/amzn-guardduty-agent/</code> .</p> <p>Lakukansudo <code>journalctl -u amazon-guardduty-agent</code> .</p>   |
| SSMPenciptaan Asosiasi Gagal  | GuardDuty SSMasosiasi sudah ada di akun Anda   | <ol style="list-style-type: none"> <li>1. Hapus asosiasi yang ada secara manual. Untuk informasi selengkapnya, lihat <a href="#">Menghapus asosiasi</a> di Panduan AWS Systems Manager Pengguna.</li> <li>2. Setelah Anda menghapus asosiasi, nonaktifkan lalu aktifkan kembali konfigurasi agen GuardDuty otomatis untuk AmazonEC2.</li> </ol>   |
|                               | Akun Anda memiliki terlalu banyak SSM asosiasi | <p>Pilih salah satu dari dua opsi berikut:</p> <ul style="list-style-type: none"> <li>• Hapus SSM asosiasi yang tidak digunakan. Untuk informasi selengkapnya, lihat <a href="#">Menghapus asosiasi</a> di Panduan AWS Systems Manager Pengguna.</li> <li>• Periksa apakah akun Anda memenuhi syarat untuk kenaikan kuota. Untuk informasi selengkapnya, lihat <a href="#">kuota Layanan Systems Manager</a> di bagian. Referensi Umum AWS</li> </ul> |
| SSMPembaruan Asosiasi Gagal   | GuardDuty SSMasosiasi tidak ada di akun Anda   | GuardDuty SSMasosiasi tidak ada di akun Anda. Nonaktifkan dan kemudian aktifkan kembali Runtime Monitoring.   |
| SSMPenghapusan Asosiasi Gagal | GuardDuty SSMasosiasi tidak ada di akun Anda   | SSMASosiasi tidak ada di akun Anda. Jika SSM asosiasi dihapus dengan sengaja, maka tidak diperlukan tindakan.   |

| Jenis masalah                       | Pesan masalah   | Langkah pemecahan masalah  |
|-------------------------------------|---|--|
| SSMEksekusi Asosiasi Instance Gagal | Persyaratan arsitektur atau prasyarat lainnya tidak terpenuhi.              | <p>Untuk informasi tentang distribusi sistem operasi terverifikasi, lihat <a href="#">Prasyarat untuk dukungan instans Amazon EC2</a>.</p> <p>Jika Anda masih mengalami masalah ini, langkah-langkah berikut akan membantu Anda mengidentifikasi dan berpotensi menyelesaikan masalah:</p> <ol style="list-style-type: none"> <li>1. Buka AWS Systems Manager konsol di <a href="https://console.aws.amazon.com/systems-manager/">https://console.aws.amazon.com/systems-manager/</a>.</li> <li>2. Di panel navigasi, di bawah Manajemen node, pilih Manajer Negara.</li> <li>3. Filter berdasarkan properti Nama Dokumen dan masukkan AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.</li> <li>4. Pilih ID asosiasi yang sesuai dan lihat riwayat Eksekusinya.</li> <li>5. Menggunakan riwayat eksekusi, melihat kegagalan, mengidentifikasi akar penyebab potensial, dan mencoba untuk menyelesaikannya.</li> </ol> |
| VPCPembuatan Endpoint Gagal         | VPCpembuatan titik akhir tidak didukung untuk dibagikan VPC<br><i>vpcId</i> | Runtime Monitoring mendukung penggunaan shared VPC dalam suatu organisasi. Untuk informasi selengkapnya, lihat <a href="#">Menggunakan berbagi VPC dengan agen keamanan otomatis</a> .   |

| Jenis masalah | Pesan masalah  | Langkah pemecahan masalah  |
|---------------|--|--|
|               | <p>Hanya saat menggunakan dibagikan VPC dengan konfigurasi agen otomatis</p> <p>ID akun pemilik <b>111122223333</b> untuk dibagikan VPC <b>vpcId</b> tidak mengaktifkan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya</p> | <p>Akun VPC pemilik bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS (AWS Fargate)). Untuk informasi selengkapnya, lihat <a href="#">Prasyarat khusus untuk Runtime Monitoring GuardDuty</a>.</p> |

| Jenis masalah                                 | Pesan masalah   | Langkah pemecahan masalah   |
|---|---|---|
|   | <p>Mengaktifkan privat DNS membutuhkan keduanya <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC atribut yang disetel ke <code>true</code> <i>vpcId</i> (Layanan: Ec2, Kode Status: 400, ID Permintaan: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i> ).</p> | <p>Pastikan bahwa VPC atribut berikut diatur ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> . Untuk informasi selengkapnya, lihat <a href="#">DNS atribut di VPC</a>.</p> <p>Jika Anda menggunakan VPC Konsol Amazon di <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> untuk membuat AmazonVPC, pastikan untuk memilih Aktifkan DNS nama host dan Aktifkan DNS resolusi. Untuk informasi selengkapnya, lihat <a href="#">opsi VPC konfigurasi</a>.</p>   |
| <p>Penghapusan VPC Endpoint Bersama Gagal</p> | <p>Penghapusan VPC endpoint bersama tidak diizinkan untuk ID akun <i>111122223333</i> , dibagikan VPC <i>vpcId</i>, ID akun pemilik <i>555555555555</i> .</p>   | <p>Langkah-langkah potensial:</p> <ul style="list-style-type: none"> <li>• Menonaktifkan status Runtime Monitoring akun VPC peserta bersama tidak memengaruhi kebijakan VPC titik akhir bersama dan grup keamanan yang ada di akun pemilik.</li> </ul> <p>Untuk menghapus grup VPC endpoint dan keamanan bersama, Anda harus menonaktifkan Runtime Monitoring atau status konfigurasi agen otomatis di akun VPC pemilik bersama.</p> <ul style="list-style-type: none"> <li>• Akun VPC peserta bersama tidak dapat menghapus VPC titik akhir bersama dan grup keamanan yang dihosting di akun VPC pemilik bersama.</li> </ul> |



| Jenis masalah         | Pesan masalah           | Langkah pemecahan masalah   |
|-----------------------|-------------------------|---|
| Agen tidak melaporkan | (Kosong dengan sengaja) | <p>Jenis masalah telah mencapai akhir dukungan. Jika Anda terus mengalami masalah ini dan belum melakukannya, aktifkan agen GuardDuty otomatis untuk AmazonEC2.</p> <p>Jika masalah masih berlanjut, pertimbangkan untuk menonaktifkan Runtime Monitoring selama beberapa menit dan kemudian aktifkan lagi.</p> |

## Cakupan untuk ECS cluster Amazon

Cakupan runtime untuk ECS klaster Amazon mencakup tugas yang sedang berjalan dan instans ECS penampung AWS Fargate (Fargate) Amazon. <sup>1</sup>

Untuk ECS klaster Amazon yang berjalan di Fargate, cakupan runtime dinilai pada tingkat tugas. Cakupan runtime ECS cluster mencakup tugas-tugas Fargate yang sudah mulai berjalan setelah Anda mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk Fargate (hanya). ECS Secara default, tugas Fargate tidak dapat diubah. GuardDuty tidak akan dapat menginstal agen keamanan untuk memantau kontainer pada tugas yang sudah berjalan. Untuk memasukkan tugas Fargate seperti itu, Anda harus berhenti dan memulai tugas lagi. Pastikan untuk memeriksa apakah layanan terkait didukung.

Untuk informasi tentang ECS wadah Amazon, lihat [Pembuatan kapasitas](#).

### Daftar Isi

- [Meninjau statistik cakupan](#)
- [Mengkonfigurasi pemberitahuan perubahan status cakupan](#)
- [Memecahkan masalah cakupan](#)

## Meninjau statistik cakupan

Statistik cakupan untuk ECS sumber daya Amazon yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase ECS klaster Amazon yang sehat di semua ECS cluster Amazon yang dipilih. Wilayah AWS Ini termasuk cakupan untuk ECS cluster Amazon yang terkait dengan instance Fargate dan AmazonEC2. Persamaan berikut mewakili ini sebagai:

(Cluster sehat/Semua cluster) \* 100

## Pertimbangan

- Statistik cakupan untuk ECS klaster mencakup status cakupan tugas Fargate atau instance ECS kontainer yang terkait dengan cluster tersebut. ECS Status cakupan tugas Fargate mencakup tugas yang sedang berjalan atau baru saja selesai berjalan.
- Di tab cakupan runtime ECS cluster, bidang yang dicakup instance Container menunjukkan status cakupan instance container yang terkait dengan cluster Amazon Anda. ECS

Jika ECS klaster Amazon Anda hanya berisi tugas Fargate, hitungannya muncul sebagai 0/0.

- Jika ECS klaster Amazon Anda dikaitkan dengan EC2 instans Amazon yang tidak memiliki agen keamanan, ECS klaster Amazon juga akan memiliki status cakupan Tidak Sehat.

Untuk mengidentifikasi dan memecahkan masalah cakupan untuk EC2 instans Amazon terkait, lihat instans [Memecahkan masalah cakupan](#) AmazonEC2.

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

## Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan Runtime.
- Di bawah tab cakupan runtime ECS cluster, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan setiap ECS klaster Amazon yang tersedia di tabel daftar Cluster.
  - Anda dapat memfilter tabel daftar Cluster dengan kolom berikut:
    - ID Akun
    - Nama Cluster
    - Jenis manajemen agen
    - Status cakupan
- Jika salah satu ECS klaster Amazon Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah menyertakan informasi tambahan tentang alasan status Tidak Sehat.

Jika ECS klaster Amazon dikaitkan dengan EC2 instans Amazon, navigasikan ke tab cakupan runtime EC2 instans dan filter menurut bidang nama Cluster untuk melihat Masalah terkait.

## API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor valid Anda sendiri, Wilayah saat ini, dan titik akhir layanan. Anda dapat memfilter dan mengurutkan daftar instance menggunakan ini API.
- Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
- Anda dapat mengubah contoh `AttributeName` `sort-criteria` dengan opsi berikut:
  - `ACCOUNT_ID`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ECS_CLUSTER_NAME`
  - `UPDATED_AT`

Bidang akan diperbarui hanya ketika tugas baru dibuat di ECS klaster Amazon terkait atau ada perubahan dalam status cakupan yang sesuai.

- Anda dapat mengubah `max-results` (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}}] }' --max-results 5
```

- Jalankan [GetCoverageStatistics](#) API untuk mengambil statistik agregat cakupan berdasarkan `statisticsType`

- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
  - `COUNT_BY_COVERAGE_STATUS`— Merupakan statistik cakupan untuk ECS cluster yang dikumpulkan berdasarkan status cakupan.
  - `COUNT_BY_RESOURCE_TYPE`— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
- Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
  - `INSTANCE_ID`
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectorsAPI`. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Untuk informasi selengkapnya tentang masalah cakupan, lihat [Memecahkan masalah cakupan](#).

## Mengkonfigurasi pemberitahuan perubahan status cakupan

Status cakupan ECS klaster Amazon Anda mungkin tampak tidak sehat. Untuk mengetahui kapan status pertanggung jawaban berubah, kami sarankan Anda untuk memantau status pertanggung jawaban secara berkala, dan memecahkan masalah jika status menjadi tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk menerima pemberitahuan saat status cakupan berubah dari Tidak Sehat menjadi Sehat atau lainnya. Secara default, GuardDuty publikasikan ini di [EventBridge bus](#) untuk akun Anda.

### Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi

selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan ECS kluster Amazon Anda berubah dari Healthy keUnhealthy, detail-type seharusnya *GuardDuty Runtime Protection Unhealthy*. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy keHealthy, ganti nilai dengan detail-type *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "ECS",
      "ecsClusterDetails": {
        "clusterName": "",
        "fargateDetails": {
          "issues": [],
          "managementType": ""
        },
        "containerInstanceDetails": {
          "coveredContainerInstances": int,
          "compatibleContainerInstances": int
        }
      }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

}

## Memecahkan masalah cakupan

Jika status cakupan ECS klaster Amazon Anda tidak sehat, Anda dapat melihat alasannya di bawah kolom Masalah.

Tabel berikut menyediakan langkah-langkah pemecahan masalah yang disarankan untuk masalah Fargate (khusus ECS Amazon). Untuk informasi tentang masalah cakupan EC2 instans Amazon, lihat [Memecahkan masalah cakupan EC2 instans Amazon](#).

| Jenis masalah         | Informasi tambahan   | Langkah pemecahan masalah yang disarankan   |
|-----------------------|--|---|
| Agen tidak melaporkan | Agen tidak melaporkan tugas di TaskDefinition - ' <i>TASK_DEFINITION</i> ' | Validasi bahwa VPC titik akhir untuk tugas ECS klaster Amazon Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat <a href="#">Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?</a> .<br><br>Jika organisasi Anda memiliki kebijakan kontrol layanan (SCP), validasi bahwa batas izin tidak membatasi izin. <code>guardduty:SendSecurityTelemetry</code> Untuk informasi selengkapnya, lihat <a href="#">Memvalidasi kebijakan kontrol layanan organisasi Anda</a> . |
|                       | <i>VPC_ISSUE</i> ; for task in TaskDefinition - ' <i>TASK_DEFINITION</i> ' | Lihat detail VPC masalah di informasi tambahan.   |
| Agen keluar           | ExitCode: EXIT_CODE untuk tugas di   | Lihat detail masalah di informasi tambahan.   |

| Jenis masalah | Informasi tambahan   | Langkah pemecahan masalah yang disarankan |
|---------------|--|---|
|               | <p>TaskDefinition -<br/>'<i>TASK_DEFINITION</i>'</p> <p>Alasan: <i>REASON</i><br/>untuk tugas-tugas di<br/>TaskDefinition -<br/>'<i>TASK_DEFINITION</i>'</p> <p>ExitCode: EXIT_CODE<br/>dengan alasan:<br/>'<i>EXIT_CODE</i>' untuk<br/>tugas-tugas di<br/>TaskDefinition -<br/>'<i>TASK_DEFINITION</i>'</p> |   |

| Jenis masalah | Informasi tambahan  | Langkah pemecahan masalah yang disarankan  |
|---------------|---|--|
|               | <p>Agen keluar:<br/>Alasan:CannotPullContainerError :<br/>tarik manifes gambar<br/>telah dicoba lagi...</p> | <p>Peran eksekusi tugas harus memiliki izin Amazon Elastic Container Registry (Amazon ECR) berikut:</p> <pre data-bbox="935 443 1507 837">...<br/>    "ecr:GetAuthorizationToken",<br/>    "ecr:BatchCheckLayerAvailability",<br/>    "ecr:GetDownloadUrlForLayer",<br/>    "ecr:BatchGetImage",<br/>...</pre> <p>Untuk informasi selengkapnya, lihat <a href="#">Berikan ECR izin dan detail subnet</a>.</p> <p>Setelah Anda menambahkan ECR izin Amazon, Anda harus memulai ulang tugas.</p> <p>Jika masalah berlanjut, lihat <a href="#">AWS Step Functions Alur kerja saya gagal secara tak terduga</a>.</p> |



| Jenis masalah                | Informasi tambahan  | Langkah pemecahan masalah yang disarankan   |
|------------------------------|---|---|
| VPC Pembuatan Endpoint Gagal | <p>Mengaktifkan privat DNS membutuhkan keduanya <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC atribut yang disetel ke <code>true</code> <code>vpcId</code> (Layanan: ECS, Kode Status: 400, ID Permintaan: <code>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</code> ).</p> | <p>Pastikan bahwa VPC atribut berikut diatur ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> . Untuk informasi selengkapnya, lihat <a href="#">DNS atribut di VPC</a>.</p> <p>Jika Anda menggunakan VPC Konsol Amazon di <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> untuk membuat Amazon VPC , pastikan untuk memilih Aktifkan DNS nama host dan Aktifkan DNS resolusi. Untuk informasi selengkapnya, lihat <a href="#">opsi VPC konfigurasi</a>.</p> |
| Agen tidak disediakan        | <p>Pemanggilan yang tidak didukung oleh <code>SERVICE</code> untuk tugas di TaskDefinition - <code>'TASK_DEFINITION'</code> .</p>   | <p>Tugas ini dipanggil oleh a <code>SERVICE</code> yang tidak didukung.</p>   |
|                              | <p>CPU arsitektur yang tidak didukung <code>'TYPE'</code> untuk tugas di TaskDefinition - <code>'TASK_DEFINITION'</code> .</p>  | <p>Tugas ini berjalan pada CPU arsitektur yang tidak didukung. Untuk informasi tentang CPU arsitektur yang didukung, lihat <a href="#">Memvalidasi persyaratan arsitektur</a>.</p>  |
|                              | <p>TaskExecutionRole hilang dari TaskDefinition - <code>'TASK_DEFINITION'</code> .</p>  | <p>Peran eksekusi ECS tugas tidak ada. Untuk informasi tentang menyediakan peran eksekusi tugas dan izin yang diperlukan, lihat <a href="#">Berikan ECR izin dan detail subnet</a>.</p>   |

| Jenis masalah | Informasi tambahan  | Langkah pemecahan masalah yang disarankan   |
|---------------|---|---|
|               | <p>Konfigurasi jaringan <code>'CONFIGURATION_DETAILS'</code> tidak ada untuk tugas di <code>TaskDefinition - 'TASK_DEFINITION'</code></p> | <p>Masalah konfigurasi jaringan mungkin muncul karena VPC konfigurasi yang hilang, atau subnet yang hilang atau kosong.</p> <p>Validasi bahwa konfigurasi jaringan Anda benar. Untuk informasi selengkapnya, lihat <a href="#">Berikan ECR izin dan detail subnet</a>.</p> <p>Untuk informasi selengkapnya, lihat <a href="#">parameter definisi ECS tugas Amazon</a> di Panduan Pengembang Layanan Kontainer Elastis Amazon.</p> |

| Jenis masalah | Informasi tambahan   | Langkah pemecahan masalah yang disarankan  |
|---------------|--|--|
| Lainnya       | <p>Masalah tak dikenal, untuk tugas di TaskDefinition - <code>'TASK_DEFINITION'</code></p> | <p>Gunakan pertanyaan-pertanyaan berikut untuk mengidentifikasi akar penyebab masalah:</p> <ul style="list-style-type: none"> <li>• Apakah tugas dimulai sebelum Anda mengaktifkan Runtime Monitoring?</li> </ul> <p>Di AmazonECS, tugasnya tidak dapat diubah. Untuk menilai perilaku runtime dari tugas Fargate yang sedang berjalan, pastikan Runtime Monitoring sudah diaktifkan, lalu restart tugas GuardDuty untuk menambahkan sespan container.</p> <ul style="list-style-type: none"> <li>• Apakah tugas ini bagian dari penerapan layanan yang dimulai sebelum Anda mengaktifkan Runtime Monitoring?</li> </ul> <p>Jika ya, Anda dapat memulai ulang layanan atau memperbarui layanan <code>forceNewDeployment</code> dengan menggunakan langkah-langkah dalam <a href="#">Memperbarui layanan</a>.</p> <p>Anda juga dapat menggunakan <a href="#">UpdateService</a> atau <a href="#">AWS CLI</a>.</p> <ul style="list-style-type: none"> <li>• Apakah tugas diluncurkan setelah mengecualikan ECS cluster dari Runtime Monitoring?</li> </ul> <p>Saat Anda mengubah GuardDuty tag yang telah ditentukan sebelumnya dari <code>GuardDutyManaged - true</code> menjadi <code>GuardDutyManaged</code></p> |

| Jenis masalah | Informasi tambahan | Langkah pemecahan masalah yang disarankan  |
|---------------|--------------------|--|
|               |                    | <p>-false, tidak GuardDuty akan menerima peristiwa runtime untuk cluster. ECS</p> <ul style="list-style-type: none"> <li>• Apakah layanan Anda berisi tugas yang memiliki format lama taskArn?</li> </ul> <p>GuardDuty Runtime Monitoring tidak mendukung cakupan untuk tugas yang memiliki format lama. taskArn</p> <p>Untuk informasi tentang Nama Sumber Daya Amazon (ARNs) untuk ECS sumber daya Amazon, lihat <a href="#">Nama Sumber Daya Amazon (ARNs) dan IDs.</a></p> |

## Cakupan untuk EKS cluster Amazon

Setelah Anda mengaktifkan Runtime Monitoring dan menginstal agen GuardDuty keamanan (add-on) EKS baik secara manual atau melalui konfigurasi agen otomatis, Anda dapat mulai menilai cakupan untuk cluster Anda. EKS

### Daftar Isi

- [Meninjau statistik cakupan](#)
- [Mengkonfigurasi pemberitahuan perubahan status cakupan](#)
- [Memecahkan masalah cakupan EKS](#)

### Meninjau statistik cakupan

Statistik cakupan untuk EKS cluster yang terkait dengan akun Anda sendiri atau akun anggota Anda adalah persentase EKS cluster sehat di semua EKS cluster yang dipilih. Wilayah AWS Persamaan berikut mewakili ini sebagai:

$(\text{Cluster sehat/Semua cluster}) * 100$

Pilih salah satu metode akses untuk meninjau statistik cakupan akun Anda.

## Console

- Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Di panel navigasi, pilih Runtime Monitoring.
- Pilih tab cakupan runtime EKS cluster.
- Di bawah tab cakupan runtime EKS cluster, Anda dapat melihat statistik cakupan yang dikumpulkan berdasarkan status cakupan yang tersedia di tabel daftar Clusters.
  - Anda dapat memfilter tabel daftar Clusters dengan kolom berikut:
    - Nama cluster
    - ID Akun
    - Jenis manajemen agen
    - Status cakupan
    - Versi pengaya
  - Jika salah satu EKS klaster Anda memiliki status Cakupan sebagai Tidak Sehat, kolom Masalah dapat mencakup informasi tambahan tentang alasan status Tidak Sehat.

## API/CLI

- Jalankan [ListCoverage](#) API dengan ID detektor, Wilayah, dan titik akhir layanan Anda yang valid. Anda dapat memfilter dan mengurutkan daftar cluster menggunakan ini API.
- Anda dapat mengubah contoh `filter-criteria` dengan salah satu opsi berikut untuk `CriterionKey`:
  - `ACCOUNT_ID`
  - `CLUSTER_NAME`
  - `RESOURCE_TYPE`
  - `COVERAGE_STATUS`
  - `ADDON_VERSION`
  - `MANAGEMENT_TYPE`
- Anda dapat mengubah contoh `AttributeName sort-criteria` dengan opsi berikut:

- CLUSTER\_NAME
- COVERAGE\_STATUS
- ISSUE
- ADDON\_VERSION
- UPDATED\_AT
- Anda dapat mengubah *max-results* (hingga 50).
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}]} ]' --max-results 5
```

- Jalankan [GetCoverageStatistics](#) API untuk mengambil statistik agregat cakupan berdasarkan `statisticsType`
- Anda dapat mengubah contoh `statisticsType` ke salah satu opsi berikut:
  - COUNT\_BY\_COVERAGE\_STATUS— Merupakan statistik cakupan untuk EKS cluster yang dikumpulkan berdasarkan status cakupan.
  - COUNT\_BY\_RESOURCE\_TYPE— Statistik cakupan dikumpulkan berdasarkan jenis AWS sumber daya dalam daftar.
- Anda dapat mengubah contoh `filter-criteria` dalam perintah. Anda dapat menggunakan opsi berikut untuk `CriterionKey`:
  - ACCOUNT\_ID
  - CLUSTER\_NAME
  - RESOURCE\_TYPE
  - COVERAGE\_STATUS
  - ADDON\_VERSION
  - MANAGEMENT\_TYPE
- Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}]}'
```

Jika status cakupan EKS klaster Anda tidak sehat, lihat [Memecahkan masalah cakupan EKS](#).

## Mengkonfigurasi pemberitahuan perubahan status cakupan

Status cakupan EKS klaster di akun Anda mungkin muncul sebagai Tidak Sehat. Untuk mendeteksi kapan status pertanggung jawaban menjadi tidak sehat, kami sarankan Anda memantau status pertanggung jawaban secara berkala dan memecahkan masalah, jika statusnya tidak sehat. Atau, Anda dapat membuat EventBridge aturan Amazon untuk memberi tahu Anda ketika status cakupan berubah dari salah satu Unhealthy ke Healthy atau sebaliknya. Secara default, GuardDuty publikasikan ini di [EventBridgebus](#) untuk akun Anda.

### Skema pemberitahuan sampel

Dalam EventBridge aturan, Anda dapat menggunakan contoh peristiwa dan pola peristiwa yang telah ditentukan sebelumnya untuk menerima pemberitahuan status cakupan. Untuk informasi selengkapnya tentang membuat EventBridge aturan, lihat [Membuat aturan](#) di Panduan EventBridge Pengguna Amazon.

Selain itu, Anda dapat membuat pola acara khusus dengan menggunakan skema pemberitahuan contoh berikut. Pastikan untuk mengganti nilai untuk akun Anda. Untuk mendapatkan pemberitahuan saat status cakupan EKS klaster Amazon Anda berubah dari Healthy ke Unhealthy, detail-type seharusnya *GuardDuty Runtime Protection Unhealthy*. Untuk mendapatkan pemberitahuan ketika status cakupan berubah dari Unhealthy ke Healthy, ganti nilai dengan detail-type *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Akun AWS ID",
  "time": "event timestamp (string)",
  "region": "Wilayah AWS",
```

```
"resources": [
  ],
"detail": {
  "schemaVersion": "1.0",
  "resourceAccountId": "string",
  "currentStatus": "string",
  "previousStatus": "string",
  "resourceDetails": {
    "resourceType": "EKS",
    "eksClusterDetails": {
      "clusterName": "string",
      "availableNodes": "string",
      "desiredNodes": "string",
      "addonVersion": "string"
    }
  },
  "issue": "string",
  "lastUpdatedAt": "timestamp"
}
}
```

## Memecahkan masalah cakupan EKS

Jika status cakupan untuk EKS klaster Anda `Unhealthy`, Anda dapat melihat kesalahan terkait baik di bawah kolom Masalah di GuardDuty konsol, atau dengan menggunakan tipe [CoverageResourceData](#).

Saat bekerja dengan tag inklusi atau pengecualian untuk memantau EKS klaster Anda secara selektif, mungkin perlu beberapa waktu bagi tag untuk disinkronkan. Ini dapat memengaruhi status cakupan EKS klaster terkait. Anda dapat mencoba menghapus dan menambahkan tag yang sesuai (penyertaan atau pengecualian) lagi. Untuk informasi selengkapnya, lihat [Menandai EKS sumber daya Amazon Anda](#) di Panduan EKS Pengguna Amazon.

Struktur masalah cakupan adalah `Issue type:Extra information`. Biasanya, masalah akan memiliki informasi Tambahan opsional yang mungkin mencakup pengecualian atau deskripsi sisi klien tertentu tentang masalah tersebut. Berdasarkan informasi tambahan, tabel berikut memberikan langkah-langkah yang disarankan untuk memecahkan masalah cakupan untuk cluster Anda EKS.



| Jenis masalah (awalan)  | Informasi tambahan   | Langkah pemecahan masalah yang disarankan   |
|---|--|---|
| Pembuatan Addon Gagal   | <p>Addon <code>aws-guard-duty-agent</code> tidak kompatibel dengan versi cluster saat ini <code>ClusterName</code> .</p> <p>Addon ditentukan tidak didukung.</p> | <p>Pastikan Anda menggunakan salah satu versi Kubernetes yang mendukung penerapan add-on. <code>aws-guard-duty-agent</code> EKS Untuk informasi selengkapnya, lihat <a href="#">Versi Kubernetes didukung oleh agen keamanan GuardDuty</a> .</p> <p>Untuk informasi tentang memperbarui versi Kubernetes Anda, lihat <a href="#">Memperbarui versi Kubernetes EKS klaster Amazon</a>.</p> |
| <p>Pembuatan Addon Gagal</p> <p>Pembaruan Addon Gagal</p> <p>Addon Status Tidak Sehat</p> | <p>EKS Masalah addon</p> <p>-AddonIssueCode :</p> <p>AddonIssueMessage</p>   | <p>Untuk informasi tentang langkah-langkah yang disarankan untuk kode masalah add-on tertentu, lihat <a href="#">Troubleshooting steps for Addon creation/ updatation error with Addon issue code</a>.</p> <p>Untuk daftar kode masalah addon yang mungkin Anda alami dalam masalah ini, lihat <a href="#">AddonIssue</a>.</p>  |

| Jenis masalah (awalan)       | Informasi tambahan  | Langkah pemecahan masalah yang disarankan   |
|------------------------------|---|---|
| VPC Pembuatan Endpoint Gagal | <p>VPC pembuatan titik akhir tidak didukung untuk dibagikan VPC <i>vpcId</i></p> <p>Hanya saat menggunakan an dibagikan VPC dengan konfigurasi agen otomatis</p> <p>ID akun pemilik <i>111122223333</i> untuk dibagikan VPC <i>vpcId</i> tidak mengaktifkan Runtime Monitoring, konfigurasi agen otomatis, atau keduanya.</p> | <p>Runtime Monitoring sekarang mendukung penggunaan shared VPC dalam suatu organisasi. Pastikan akun Anda memenuhi semua prasyarat. Untuk informasi selengkapnya, lihat <a href="#">Prasyarat untuk menggunakan bersama VPC</a>.</p> <p>Akun VPC pemilik bersama harus mengaktifkan Runtime Monitoring dan konfigurasi agen otomatis untuk setidaknya satu jenis sumber daya (Amazon EKS atau Amazon ECS (AWS Fargate)). Untuk informasi selengkapnya, lihat <a href="#">Prasyarat khusus untuk Runtime Monitoring GuardDuty</a>.</p> |

| Jenis masalah (awalan) | Informasi tambahan  | Langkah pemecahan masalah yang disarankan  |
|------------------------|---|--|
|                        | <p>Mengaktifkan privat DNS membutuhkan keduanya <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> VPC atribut yang disetel ke <code>true</code> <i>vpcId</i> (Layanan: Ec2, Kode Status: 400, ID Permintaan: <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i> ).</p> | <p>Pastikan bahwa VPC atribut berikut diatur ke <code>true</code> — <code>enableDnsSupport</code> dan <code>enableDnsHostnames</code> . Untuk informasi selengkapnya, lihat <a href="#">DNSatribut di VPC</a>.</p> <p>Jika Anda menggunakan VPC Konsol Amazon di <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> untuk membuat AmazonVPC, pastikan untuk memilih Aktifkan DNS nama host dan Aktifkan DNS resolusi. Untuk informasi selengkapnya, lihat <a href="#">opsi VPC konfigurasi</a>.</p> |

| Jenis masalah (awalan)                 | Informasi tambahan  | Langkah pemecahan masalah yang disarankan   |
|--|---|---|
| Penghapusan VPC Endpoint Bersama Gagal | Penghapusan VPC endpoint bersama tidak diizinkan untuk ID akun <b>111122223333</b> , dibagikan VPC <i>vpcId</i> , ID akun pemilik <b>555555555555</b> . | <p>Langkah-langkah potensial:</p> <ul style="list-style-type: none"><li>• Menonaktifkan status Runtime Monitoring akun VPC peserta bersama tidak memengaruhi kebijakan VPC titik akhir bersama dan grup keamanan yang ada di akun pemilik.</li></ul> <p>Untuk menghapus grup VPC endpoint dan keamanan bersama, Anda harus menonaktifkan Runtime Monitoring atau status konfigurasi agen otomatis di akun VPC pemilik bersama.</p> <ul style="list-style-type: none"><li>• Akun VPC peserta bersama tidak dapat menghapus VPC titik akhir bersama dan grup keamanan yang dihosting di akun VPC pemilik bersama.</li></ul> |

| Jenis masalah (awalan)                                 | Informasi tambahan  | Langkah pemecahan masalah yang disarankan  |
|--|---|--|
| EKSCluster lokal                                       | EKSSaddons tidak didukung pada cluster pos lokal.           | Tidak bisa ditindaklanjuti.<br><br>Untuk informasi selengkapnya, lihat <a href="#">Amazon EKS di AWS pos terdepan</a> .  |
| EKSIzin pengaktifan Runtime Monitoring tidak diberikan | (mungkin atau mungkin tidak menampilkan informasi tambahan) | <ol style="list-style-type: none"><li>1. Jika informasi tambahan tersedia untuk masalah ini, perbaiki akar penyebabnya dan ikuti langkah berikutnya.</li><li>2. Alihkan EKS Runtime Monitoring untuk memmatikannya lalu nyalakan kembali. Pastikan bahwa GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.</li></ol> |

| Jenis masalah (awalan)   | Informasi tambahan  | Langkah pemecahan masalah yang disarankan  |
|--|---|--|
| EKSRuntime Monitoring pemberdayaan penyediaan sumber daya sedang berlangsung | (mungkin atau mungkin tidak menampilkan informasi tambahan) | Tidak bisa ditindaklanjuti.<br><br>Setelah Anda mengaktifkan EKS Runtime Monitoring, status cakupan mungkin tetap ada <code>UnHealthy</code> hingga langkah penyediaan sumber daya selesai. Status cakupan dipantau dan diperbarui secara berkala. |
| Lainnya (masalah lainnya)  | Kesalahan karena kegagalan otorisasi                        | Alihkan EKS Runtime Monitoring untuk mematikannya lalu nyalakan kembali. Pastikan bahwa GuardDuty agen juga dikerahkan, baik secara otomatis melalui GuardDuty atau manual.  |

| Kesalahan pembuatan atau pembaruan addon   | Langkah pemecahan masalah  |
|--|--|
| EKSMasalah Addon - <code>InsufficientNumber OfReplicas</code> : Add-on tidak sehat karena tidak memiliki jumlah replika yang diinginkan. | <ul style="list-style-type: none"> <li>Dengan menggunakan pesan masalah, Anda dapat mengidentifikasi dan memperbaiki akar masalahnya. Anda bisa mulai dengan mendeskripsikan cluster Anda. Misalnya, gunakan <code>kubectl describe pods</code> untuk</li> </ul> |

| Kesalahan pembuatan atau pembaruan addon  | Langkah pemecahan masalah   |
|---|---|
| <p>EKSMasalah Addon -AdmissionRequestDenied : webhook penerimaan "validate.kyverno.svc-fail" menolak permintaan: kebijakan DaemonSet/amazon-guarddduty/aws-guarddduty-agent untuk pelanggaran sumber daya:: restrict-image-registries:autogen-validate-registries ...</p> | <p>mengidentifikasi akar penyebab kegagalan pod.</p> <p>Setelah Anda memperbaiki akar penyebabnya, coba lagi langkahnya (pembuatan atau pembaruan add-on).</p> <ul style="list-style-type: none"> <li>• Jika masalah berlanjut, validasi bahwa VPC titik akhir untuk EKS klaster Amazon Anda telah dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat <a href="#">Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?</a>.</li> </ul> <ol style="list-style-type: none"> <li>1. EKSCluster Amazon atau administrator keamanan harus meninjau kebijakan keamanan yang memblokir pembaruan Addon.</li> <li>2. Anda harus menonaktifkan controller (webhook) atau meminta controller menerima permintaan dari AmazonEKS.</li> </ol> |
| <p>EKSMasalah Addon -ConfigurationConflict : Konflik ditemukan saat mencoba menerapkan. Tidak akan berlanjut karena menyelesaikan mode konflik. Conflicts: DaemonSet.apps aws-guarddduty-agent - .spec.template.spec.containers[name="aws-guarddduty-agent"].image</p>    | <p>Saat membuat atau memperbarui Addon, berikan bendera OVERWRITE konflik penyelesaian. Ini berpotensi menimpa setiap perubahan yang telah dibuat langsung ke sumber daya terkait di Kubernetes dengan menggunakan Kubernetes. API</p> <p>Anda dapat <a href="#">menghapus Addon</a> terlebih dahulu dan kemudian menginstal ulang.</p>   |

## Kesalahan pembuatan atau pembaruan addon

EKS Masalah Addon - AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope

## Langkah pemecahan masalah

Anda harus menambahkan izin yang hilang ke eks:addon-cluster-admin ClusterRoleBinding manual. Tambahkan yang berikut ini yam1 ke eks:addon-cluster-admin :

```
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: eks:addon-cluster-admin
subjects:
- kind: User
  name: eks:addon-manager
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cluster-admin
  apiGroup: rbac.authorization.k8s.io
---
```

Anda sekarang dapat menerapkan ini yam1 ke EKS cluster Amazon Anda dengan menggunakan perintah berikut:

```
kubectl apply -f eks-addon-cluster-admin.yam1
```



| Kesalahan pembuatan atau pembaruan addon  | Langkah pemecahan masalah  |
|---|--|
| <p>EKS<br/>Masalah Addon - AccessDenied:<br/>admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label</p> | <p>Anda harus menonaktifkan pengontrol atau meminta pengontrol menerima permintaan dari EKS cluster Amazon.</p> <p>Sebelum membuat atau memperbarui add-on, Anda juga dapat membuat GuardDuty namespace dan memberi label sebagai <code>owner</code></p> |

## Pertanyaan yang sering diajukan (FAQs)

### Daftar Isi

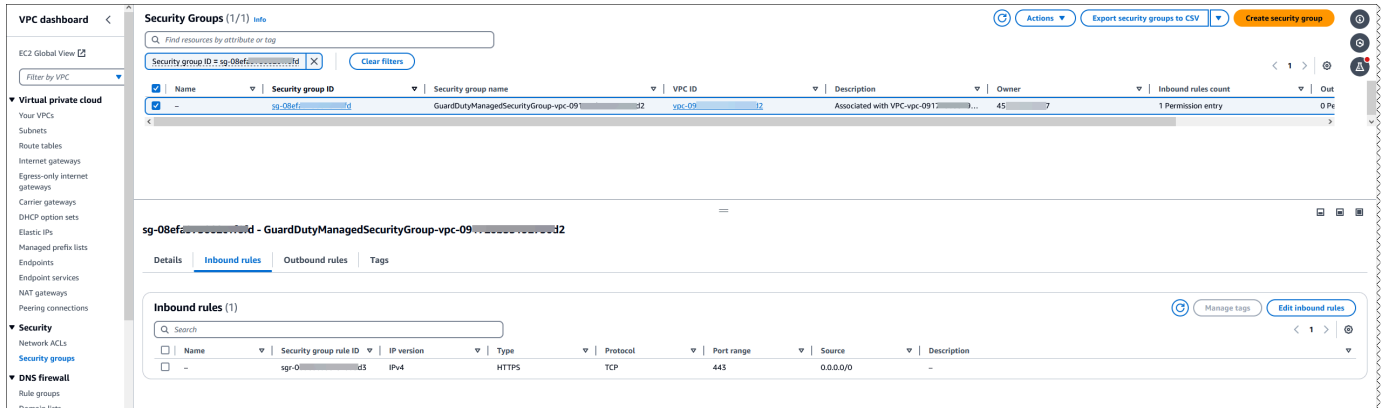
- [Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?](#)
- [Mengapa status cakupan untuk sumber daya saya Unhealthy?](#)
- [Siapa yang dapat melihat status cakupan runtime untuk sumber daya milik saya? Akun AWS](#)
- [Bagaimana saya bisa memvalidasi jika agen GuardDuty keamanan berjalan pada tugas Fargate?](#)
- [Lebih banyak pertanyaan pemecahan masalah](#)

### Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?

Gunakan langkah-langkah berikut untuk memvalidasi bahwa konfigurasi VPC titik akhir untuk jenis sumber daya Anda diatur dengan benar di akun VPC pemilik:

1. Masuk ke AWS Management Console dan buka VPC konsol Amazon di <https://console.aws.amazon.com/vpc/>.
2. Di panel navigasi, di bawah Virtual private cloud, pilih Endpoints.
3. Dalam tabel Endpoints, pilih baris yang memiliki nama Service mirip dengan `com.amazonaws.us-east-1.guardduty-data`. Region (`us-east-1`) mungkin berbeda untuk titik akhir Anda.
4. Panel untuk detail titik akhir akan muncul. Di bawah tab Grup Keamanan, pilih tautan ID Grup terkait untuk detail selengkapnya.

5. Dalam tabel Grup Keamanan, pilih baris dengan ID grup Keamanan terkait untuk melihat detailnya.
6. Di bawah tab Aturan masuk, pastikan bahwa ada kebijakan masuk dengan rentang Port sebagai 443 dan Sumber sebagai 0.0.0.0/0. Aturan masuk mengontrol lalu lintas masuk yang diizinkan untuk mencapai instance. Gambar berikut menunjukkan aturan masuk untuk grup keamanan yang terkait dengan yang VPC digunakan oleh agen GuardDuty keamanan.



Jika Anda belum memiliki grup keamanan yang mengaktifkan port 443 dalam terikat, [Buat grup keamanan](#) di EC2Panduan Pengguna Amazon.

Jika ada masalah saat membatasi izin masuk ke VPC (atau cluster) Anda, berikan dukungan ke port 443 yang di-bound dari alamat IP apa pun (0.0.0.0/0).

## Mengapa status cakupan untuk sumber daya saya **Unhealthy**?

Jika Anda baru saja menggunakan agen GuardDuty keamanan (baik melalui konfigurasi agen otomatis atau secara manual) atau mengikuti langkah-langkah yang disarankan untuk memecahkan masalah cakupan, mungkin perlu beberapa menit agar status cakupan menjadi sehat. Anda dapat memeriksa status cakupan secara berkala atau mengonfigurasi Amazon EventBridge (EventBridge) untuk menerima pemberitahuan saat status cakupan berubah.

Selain itu, Anda juga dapat memvalidasi bahwa konfigurasi VPC titik akhir untuk sumber daya Anda sudah benar. Untuk informasi selengkapnya, lihat [Bagaimana cara memvalidasi bahwa konfigurasi VPC titik akhir sudah benar?](#).

## Siapa yang dapat melihat status cakupan runtime untuk sumber daya milik saya? Akun AWS

Sebagai akun anggota atau akun mandiri, Anda dapat melihat statistik cakupan sumber daya yang terkait dengan akun Anda sendiri. Sebagai akun GuardDuty administrator organisasi yang didelegasikan, Anda dapat melihat statistik cakupan untuk sumber daya yang terkait dengan akun Anda dan akun anggota milik organisasi Anda.

## Bagaimana saya bisa memvalidasi jika agen GuardDuty keamanan berjalan pada tugas Fargate?

Agen GuardDuty keamanan berjalan sebagai wadah sespan untuk tugas Fargate.

Pilih metode yang disukai untuk memvalidasi jika wadah sespan ditampilkan saat tugas sedang berjalan.

### Amazon ECS console

1. Buka konsol di <https://console.aws.amazon.com/ecs/v2>.
2. Pada panel navigasi, silakan pilih Klaster.
3. Pada halaman Clusters, pilih nama cluster terkait untuk detail selengkapnya.
4. Pilih tab Tugas.
5. Pilih tautan tugas terkait untuk melihat detail tugas.
6. Pada halaman detail tugas, tabel Kontainer menyertakan detail sespan. ID runtime Container akan memiliki awalan ID Tugas Anda.

### CLI

Jalankan `describe-tasks` dan cari wadah dengan nama yang disetel ke `aws-gd-agent` dan `lastStatusset` ke `RUNNING`.

Contoh berikut menunjukkan output untuk cluster default untuk tugas `aws:ecs:us-east-1:123456789012:task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE`

### Output

Wadah bernama `aws-gd-agent` ada di `RUNNING` negara bagian.

```
"containers": [
```

```
{
  "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/4df26bb4-
f057-467b-a079-96167EXAMPLE",
  "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/0b69d5c0-
d655-4695-98cd-5d2d5EXAMPLE",
  "lastStatus": "RUNNING",
  "healthStatus": "UNKNOWN",
  "memory": "1 GB",
  "name": "aws-gd-agent"
}
```

Untuk informasi selengkapnya, lihat [mendeskripsikan tugas](#).

## Lebih banyak pertanyaan pemecahan masalah

Untuk pertanyaan pemecahan masalah lainnya terkait tugas Fargate Anda, lihat [Pemecahan Masalah Pemantauan Waktu Proses di Panduan Pengembang Layanan Amazon Elastic FAQs](#) Container.

## Pengaturan CPU dan pemantauan memori

Setelah mengaktifkan Runtime Monitoring dan menilai bahwa status cakupan kluster Anda Sehat, Anda dapat menyiapkan dan melihat metrik wawasan.

Topik berikut dapat membantu Anda mengevaluasi kinerja agen yang diterapkan terhadap batas memori CPU dan GuardDuty agen.

### Menyiapkan pemantauan di ECS kluster Amazon

Langkah-langkah berikut dari Panduan CloudWatch Pengguna Amazon dapat membantu Anda mengevaluasi kinerja agen yang diterapkan terhadap batas CPU dan memori GuardDuty agen:

1. [Menyiapkan Wawasan Kontainer di Amazon ECS untuk metrik tingkat kluster dan layanan](#)
2. [Metrik ECS Wawasan Kontainer Amazon](#)

### Menyiapkan pemantauan di EKS kluster Amazon

Setelah agen GuardDuty keamanan diterapkan dan Anda menilai bahwa status cakupan kluster Anda Sehat, Anda dapat mengatur dan melihat metrik wawasan Container.

## Mengevaluasi kinerja agen keamanan

1. [Menyiapkan Wawasan Kontainer di Amazon EKS dan Kubernetes di Panduan Pengguna Amazon CloudWatch](#)
2. [Metrik Amazon EKS dan Kubernetes Container Insights di Panduan Pengguna Amazon CloudWatch](#)

## Kelola kinerja dengan agen keamanan v1.5.0 ke atas

Dengan agen keamanan [v1.5.0 dan](#) yang lebih baru, ketika wawasan menunjukkan bahwa GuardDuty agen terkait mencapai batas yang ditetapkan, Anda dapat mengonfigurasi parameter tertentu. Untuk informasi selengkapnya, lihat [Konfigurasi EKS parameter add-on](#).

## Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty

Agan GuardDuty keamanan mengumpulkan jenis peristiwa berikut dan mengirimkannya ke GuardDuty backend untuk deteksi dan analisis ancaman. GuardDuty tidak membuat acara ini dapat diakses oleh Anda. Jika GuardDuty mendeteksi potensi ancaman dan menghasilkan temuan Runtime Monitoring, Anda dapat melihat detail temuan yang sesuai. Untuk informasi selengkapnya tentang cara GuardDuty menggunakan jenis acara yang dikumpulkan, lihat [Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan](#).

## Memproses acara

| Nama bidang   | Deskripsi  |
|---------------|--|
| Nama proses   | Nama proses yang diamati.  |
| Jalur Proses  | Jalur absolut dari proses yang dapat dieksekusi.                                       |
| ID Proses     | ID yang ditetapkan untuk proses oleh sistem operasi.                                   |
| Namespace PID | ID proses proses dalam namespace sekunder selain PID namespace tingkat PID host. Untuk |

| Nama bidang                           | Deskripsi   |
|---------------------------------------|---|
|                                       | proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.                                |
| Memproses ID Pengguna                 | ID unik pengguna yang mengeksekusi proses.  |
| Proses UUID                           | ID unik yang ditetapkan untuk proses oleh GuardDuty.  |
| Proses GID                            | ID proses dari grup proses.   |
| Proses EGID                           | ID grup yang efektif dari grup proses.  |
| Proses EUID                           | ID pengguna yang efektif dari proses tersebut.  |
| Nama Pengguna Proses                  | Nama pengguna yang mengeksekusi proses.   |
| Waktu Mulai Proses                    | Waktu ketika proses itu dibuat. Bidang ini dalam format string UTC tanggal (2023-03-22T19:37:20.168Z ). |
| Proses yang Dapat Dieksekusi -256 SHA | SHA256Hash dari proses yang dapat dieksekusi.   |
| Jalur Skrip Proses                    | Path dari file script yang dieksekusi.  |
| Variabel Lingkungan Proses            | Variabel lingkungan tersedia untuk proses. Hanya LD_PRELOAD dan LD_LIBRARY_PATH dikumpulkan.            |
| Proses Direktori Kerja Sekarang (PWD) | Presentasikan direktori kerja proses.   |
| Proses orang tua                      | Rincian proses proses induk. Proses induk adalah proses yang menciptakan proses yang diamati.           |

| Nama bidang  | Deskripsi   |
|--|---|
| <p>Argumen Baris Perintah</p> <p>Saat ini, bidang ini terbatas pada versi agen tertentu yang sesuai dengan jenis sumber daya:</p> <ul style="list-style-type: none"> <li>• Fargate (ECShanya Amazon) dengan agen GuardDuty keamanan v1.0.0 ke atas.</li> <li>• EC2Instans Amazon dengan agen GuardDuty keamanan v1.0.0 dan yang lebih baru.</li> <li>• EKSCluster Amazon dengan agen keamanan v1.4.0 dan di atasnya.</li> </ul> <p>Untuk informasi selengkapnya, lihat <a href="#">GuardDuty sejarah rilis agen</a>.</p> | <p>Argumen baris perintah disediakan pada saat eksekusi proses. Bidang ini mungkin berisi data pelanggan yang sensitif.</p> |

## Acara kontainer

| Nama bidang           | Deskripsi   |
|-----------------------|---|
| Nama Kontainer        | <p>Nama wadahnya.</p> <p>Bila tersedia, bidang ini menampilkan nilai <code>labelio.kubernetes.container.name</code> .</p> |
| Kontainer UID         | ID unik dari kontainer yang ditetapkan oleh runtime kontainer.  |
| Runtime Kontainer     | Runtime kontainer (seperti <code>docker</code> atau <code>containerd</code> ) digunakan untuk menjalankan kontainer.      |
| ID Gambar Kontainer   | ID dari gambar kontainer.   |
| Nama Gambar Kontainer | Nama gambar kontainer.  |

## AWS Fargate (ECSHanya Amazon) peristiwa tugas

| Nama bidang                         | Deskripsi   |
|-------------------------------------|---|
| Nama Sumber Daya Tugas Amazon (ARN) | ARN Tugas.  |
| Nama Klaster                        | Nama ECS cluster Amazon.  |
| Nama Keluarga                       | Nama keluarga definisi tugas. familyIni digunakan sebagai nama untuk definisi tugas yang digunakan untuk meluncurkan tugas.                             |
| Nama Layanan                        | Nama ECS layanan Amazon, jika tugas diluncurkan sebagai bagian dari layanan.  |
| Jenis Peluncuran                    | Infrastruktur tempat tugas Anda berjalan. Untuk Runtime Monitoring dengan tipe sumber daya asECSCluster , jenis peluncuran bisa berupa EC2 atauFARGATE. |
| CPU                                 | Jumlah CPU unit yang digunakan oleh tugas seperti yang dinyatakan dalam definisi tugas.   |

## Acara pod Kubernetes

| Nama bidang             | Deskripsi   |
|-------------------------|---|
| ID Pod                  | ID dari pod Kubernetes.   |
| Nama pod                | Nama pod Kubernetes.  |
| Ruang Nama Pod          | Nama namespace Kubernetes tempat beban kerja Kubernetes berada. |
| Nama Cluster Kubernetes | Nama cluster Kubernetes.  |



## DNSacara

| Nama bidang                  | Deskripsi   |
|------------------------------|---|
| Jenis Soket                  | Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.  |
| Alamat Keluarga              | Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4. |
| ID Arah                      | ID dari arah koneksi.   |
| Nomor Protokol               | Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.  |
| DNSIP Titik Akhir Jarak Jauh | IP jarak jauh dari koneksi.   |
| DNSPort Endpoint Jarak Jauh  | Nomor port koneksi.   |
| DNSIP Titik Akhir Lokal      | IP lokal dari koneksi.  |
| DNSPelabuhan Endpoint Lokal  | Nomor port koneksi.   |
| DNSMuatan                    | Payload DNS paket yang berisi DNS pertanyaan dan tanggapan .  |

## Buka acara

| Nama bidang | Deskripsi   |
|-------------|---|
| Filepath    | Jalur file yang dibuka dalam acara ini.                                     |
| Bendera     | Menjelaskan mode akses file, seperti read-only, write-only, dan read-write. |

## Memuat acara modul

| Nama bidang | Deskripsi                          |
|-------------|------------------------------------|
| Nama Modul  | Nama modul dimuat ke dalam kernel. |

## Acara Mprotect

| Nama bidang    | Deskripsi   |
|----------------|---|
| Rentang Alamat | Rentang alamat tempat perlindungan aksesnya dimodifikasi.         |
| Wilayah Memori | Menentukan Wilayah ruang alamat proses seperti tumpukan dan heap. |
| Bendera        | Merupakan opsi yang mengontrol perilaku acara ini.                |

## Acara gunung

| Nama bidang       | Deskripsi  |
|-------------------|--|
| Target Gunung     | Jalur tempat sumber mount dipasang.                |
| Sumber Gunung     | Jalur pada host yang dipasang di target mount.     |
| Jenis Sistem File | Merupakan jenis yang dipasangfileSystem.           |
| Bendera           | Merupakan opsi yang mengontrol perilaku acara ini. |

## Tautkan acara

| Nama bidang  | Deskripsi                      |
|--------------|--------------------------------|
| Jalur Tautan | Jalur tempat hard link dibuat. |

| Nama bidang  | Deskripsi                              |
|--------------|--|
| Jalur Target | Jalur file di mana hard link menunjuk. |

## Acara Symlink

| Nama bidang  | Deskripsi                                    |
|--------------|--|
| Jalur Tautan | Jalur tempat tautan simbolis dibuat.         |
| Jalur Target | Jalur file di mana tautan simbolik menunjuk. |

## Acara Dup

| Nama bidang                     | Deskripsi   |
|---------------------------------|---|
| Deskriptor File Lama            | Deskriptor file yang mewakili objek file terbuka.   |
| Deskriptor File Baru            | Deskriptor file baru yang merupakan duplikat dari deskriptor file lama. Baik deskriptor file lama dan baru mewakili objek file terbuka yang sama. |
| IP Titik Akhir Jarak Jauh Dup   | Alamat IP jarak jauh dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.   |
| Port Titik Akhir Jarak Jauh Dup | Port jarak jauh dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.        |
| IP Titik Akhir Lokal Dup        | Alamat IP lokal dari soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.        |
| Pelabuhan Titik Akhir Lokal Dup | Port lokal soket jaringan diwakili oleh deskriptor file lama. Hanya berlaku ketika deskriptor file lama mewakili soket jaringan.                  |

## Acara peta memori

| Nama bidang | Deskripsi                           |
|-------------|-------------------------------------|
| Filepath    | Jalur file tempat memori dipetakan. |

## Acara soket

| Nama bidang     | Deskripsi  |
|-----------------|--|
| Keluarga alamat | Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol versi IP 4.                                       |
| Jenis Soket     | Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.   |
| Nomor protokol  | Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat AF_INET hanya memiliki protokol IP. |

## Connect event

| Nama bidang     | Deskripsi  |
|-----------------|--|
| Keluarga alamat | Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4.  |
| Jenis Soket     | Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.   |
| Nomor Protokol  | Menentukan protokol tertentu dalam keluarga alamat. Biasanya ada protokol tunggal dalam keluarga alamat. Misalnya, keluarga alamat AF_INET hanya memiliki protokol IP. |

| Nama bidang               | Deskripsi  |
|---------------------------|--|
| Filepath                  | Jalur file soket jika keluarga alamat adalahAF_UNIX. |
| IP Titik Akhir Jarak Jauh | IP jarak jauh dari koneksi.                          |
| Port Endpoint Jarak Jauh  | Nomor port koneksi.                                  |
| IP Titik Akhir Lokal      | IP lokal dari koneksi.                               |
| Pelabuhan Endpoint Lokal  | Nomor port koneksi.                                  |

## Proses acara VM Readv

| Nama bidang                        | Deskripsi   |
|------------------------------------|---|
| Bendera                            | Merupakan opsi yang mengontrol perilaku acara ini.    |
| Target PID                         | ID proses dari proses dari mana memori sedang dibaca. |
| Proses Target UUID                 | ID unik dari proses target.                           |
| Target Jalur yang Dapat Dieksekusi | Jalur absolut dari file eksekusi proses target.       |

## Proses acara VM Writev

| Nama bidang                        | Deskripsi   |
|------------------------------------|---|
| Bendera                            | Merupakan opsi yang mengontrol perilaku acara ini.  |
| Target PID                         | ID proses dari proses dimana memori sedang ditulis. |
| Proses Target UUID                 | ID unik dari proses target.                         |
| Target Jalur yang Dapat Dieksekusi | Jalur absolut dari file eksekusi proses target.     |

## Acara Ptrace

| Nama bidang                        | Deskripsi  |
|------------------------------------|--|
| Target PID                         | ID proses dari proses target.                      |
| Proses Target UUID                 | ID unik dari proses target.                        |
| Target Jalur yang Dapat Dieksekusi | Jalur absolut dari file eksekusi proses target.    |
| Bendera                            | Merupakan opsi yang mengontrol perilaku acara ini. |

## Mengikat acara

| Nama bidang            | Deskripsi   |
|------------------------|---|
| Alamat Keluarga        | Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4. |
| Jenis soket            | Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.  |
| Nomor protokol         | Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.  |
| IP titik akhir lokal   | IP lokal dari koneksi.  |
| Port titik akhir lokal | Nomor port koneksi.   |

## Dengarkan acara

| Nama bidang            | Deskripsi   |
|------------------------|---|
| Alamat Keluarga        | Merupakan protokol komunikasi yang terkait dengan alamat. Misalnya, keluarga alamat AF_INET digunakan untuk protokol IP v4. |
| Jenis soket            | Jenis soket untuk menunjukkan semantik komunikasi. Misalnya, SOCK_RAW.  |
| Nomor protokol         | Nomor protokol layer 4 seperti 17 untuk UDP dan 6 untuk TCP.  |
| IP titik akhir lokal   | IP lokal dari koneksi.  |
| Port titik akhir lokal | Nomor port koneksi.   |

## Ganti nama acara

| Nama bidang | Deskripsi                              |
|-------------|--|
| Filepath    | Path tempat file yang diganti namanya. |
| Target      | Jalur baru file.                       |

## Atur UID acara

| Nama bidang | Deskripsi   |
|-------------|---|
| Baru EUID   | ID pengguna baru yang efektif dari proses tersebut. |
| Baru UID    | ID pengguna baru dari proses tersebut.              |

## Acara Chmod

| Nama bidang | Deskripsi                                      |
|-------------|--|
| Filepath    | Path dari file yang memanggil acara ini.       |
| Filemode    | Izin akses yang diperbarui untuk file terkait. |

## Agen hosting ECR repositori Amazon GuardDuty

Bagian berikut mencantumkan repositori Amazon Elastic Container Registry (AmazonECR) tempat GuardDuty menghosting agen keamanan yang akan digunakan di cluster Amazon dan EKS Amazon Anda. ECS

### Daftar Isi

- [Repositori untuk EKS agen versi 1.6.0 atau lebih tinggi](#)
- [Repositori untuk EKS agen versi 1.5.0 dan sebelumnya](#)
- [Repositori untuk GuardDuty agen di \(hanya AWS Fargate AmazonECS\)](#)

## Repositori untuk EKS agen versi 1.6.0 atau lebih tinggi

Tabel berikut menunjukkan ECR repositori Amazon yang menghosting versi agen EKS add-on Amazon (`aws-guardduty-agent`) 1.6.0 dan yang lebih baru, untuk masing-masing. Wilayah AWS

| Wilayah AWS                 | ECRRepositori Amazon URI                                   |
|-----------------------------|--|
| AS Barat<br>(Oregon)        | <code>602401143452.dkr.ecr.us-west-2.amazonaws.com</code>  |
| Eropa (Paris)               | <code>602401143452.dkr.ecr.eu-west-3.amazonaws.com</code>  |
| Asia Pasifik<br>(Mumbai)    | <code>602401143452.dkr.ecr.ap-south-1.amazonaws.com</code> |
| Asia Pasifik<br>(Hyderabad) | <code>900889452093.dkr.ecr.ap-south-2.amazonaws.com</code> |



| Wilayah AWS                 | ECRRepositori Amazon URI                          |
|-----------------------------|---|
| Kanada (Pusat)              | 602401143452.dkr.ecr.ca-central-1.amazonaws.com   |
| Kanada Barat (Calgary)      | 761377655185.dkr.ecr.ca-west-1.amazonaws.com      |
| Timur Tengah (UAE)          | 759879836304.dkr.ecr.me-central-1.amazonaws.com   |
| Eropa (London)              | 602401143452.dkr.ecr.eu-west-2.amazonaws.com      |
| AS Barat (California Utara) | 602401143452.dkr.ecr.us-west-1.amazonaws.com      |
| AS Timur (N. Virginia)      | 602401143452.dkr.ecr.us-east-1.amazonaws.com      |
| AS Timur (Ohio)             | 602401143452.dkr.ecr.us-east-2.amazonaws.com      |
| Eropa (Irlandia)            | 602401143452.dkr.ecr.eu-west-1.amazonaws.com      |
| Amerika Selatan (Sao Paulo) | 602401143452.dkr.ecr.sa-east-1.amazonaws.com      |
| Eropa (Stockholm)           | 602401143452.dkr.ecr.eu-north-1.amazonaws.com     |
| Eropa (Frankfurt)           | 602401143452.dkr.ecr.eu-central-1.amazonaws.com   |
| Eropa (Zürich)              | 900612956339.dkr.ecr.eu-central-2.amazonaws.com   |
| Asia Pasifik (Singapura)    | 602401143452.dkr.ecr.ap-southeast-1.amazonaws.com |
| Asia Pasifik (Sydney)       | 602401143452.dkr.ecr.ap-southeast-2.amazonaws.com |
| Asia Pasifik (Jakarta)      | 296578399912.dkr.ecr.ap-southeast-3.amazonaws.com |

| Wilayah AWS                                   | ECRRepositori Amazon URI                          |
|---|---|
| Asia Pasifik (Tokyo)                          | 602401143452.dkr.ecr.ap-northeast-1.amazonaws.com |
| Asia Pasifik (Seoul)                          | 602401143452.dkr.ecr.ap-northeast-2.amazonaws.com |
| Asia Pasifik (Osaka)                          | 602401143452.dkr.ecr.ap-northeast-3.amazonaws.com |
| Asia Pasifik (Hong Kong)                      | 800184023465.dkr.ecr.ap-east-1.amazonaws.com      |
| Middle East (Bahrain) (Middle East (Bahrain)) | 759879836304.dkr.ecr.me-south-1.amazonaws.com     |
| Eropa (Milan)                                 | 590381155156.dkr.ecr.eu-south-1.amazonaws.com     |
| Eropa (Spanyol)                               | 455263428931.dkr.ecr.eu-south-2.amazonaws.com     |
| Afrika (Cape Town)                            | 877085696533.dkr.ecr.af-south-1.amazonaws.com     |
| Asia Pasifik (Melbourne)                      | 491585149902.dkr.ecr.ap-southeast-4.amazonaws.com |
| Israel (Tel Aviv)                             | 066635153087.dkr.ecr.il-central-1.amazonaws.com   |

## Repositori untuk EKS agen versi 1.5.0 dan sebelumnya

Tabel berikut menunjukkan ECR repositori Amazon yang menghosting versi agen EKS add-on Amazon (aws-guardduty-agent) 1.5.0 dan yang lebih lama, untuk masing-masing Wilayah AWS

| Wilayah AWS                    | ECRRepositori Amazon URI                        |
|--------------------------------|---|
| AS Barat<br>(Oregon)           | 039403964562.dkr.ecr.us-west-2.amazonaws.com    |
| Eropa (Paris)                  | 113643092156.dkr.ecr.eu-west-3.amazonaws.com    |
| Asia Pasifik<br>(Mumbai)       | 610108029387.dkr.ecr.ap-south-1.amazonaws.com   |
| Asia Pasifik<br>(Hyderabad)    | 618745550137.dkr.ecr.ap-south-2.amazonaws.com   |
| Kanada (Pusat)                 | 001188825231.dkr.ecr.ca-central-1.amazonaws.com |
| Timur Tengah<br>(UAE)          | 601769779514.dkr.ecr.me-central-1.amazonaws.com |
| Eropa (London)                 | 109118265657.dkr.ecr.eu-west-2.amazonaws.com    |
| AS Barat<br>(California Utara) | 373421517865.dkr.ecr.us-west-1.amazonaws.com    |
| AS Timur (N.<br>Virginia)      | 031903291036.dkr.ecr.us-east-1.amazonaws.com    |
| AS Timur (Ohio)                | 591382732059.dkr.ecr.us-east-2.amazonaws.com    |
| Eropa (Irlandia)               | 673884943994.dkr.ecr.eu-west-1.amazonaws.com    |
| Amerika Selatan<br>(Sao Paulo) | 941219317354.dkr.ecr.sa-east-1.amazonaws.com    |
| Eropa (Stockhol<br>m)          | 366771026645.dkr.ecr.eu-north-1.amazonaws.com   |
| Eropa (Frankfurt)              | 409493279830.dkr.ecr.eu-central-1.amazonaws.com |
| Eropa (Zürich)                 | 718440343717.dkr.ecr.eu-central-2.amazonaws.com |

| Wilayah AWS                                   | ECRRepositori Amazon URI                          |
|---|---|
| Asia Pasifik (Singapura)                      | 584580519942.dkr.ecr.ap-southeast-1.amazonaws.com |
| Asia Pasifik (Sydney)                         | 011662287384.dkr.ecr.ap-southeast-2.amazonaws.com |
| Asia Pasifik (Jakarta)                        | 617474730032.dkr.ecr.ap-southeast-3.amazonaws.com |
| Asia Pasifik (Tokyo)                          | 781592569369.dkr.ecr.ap-northeast-1.amazonaws.com |
| Asia Pasifik (Seoul)                          | 732248494576.dkr.ecr.ap-northeast-2.amazonaws.com |
| Asia Pasifik (Osaka)                          | 810724417379.dkr.ecr.ap-northeast-3.amazonaws.com |
| Asia Pasifik (Hong Kong)                      | 790429075973.dkr.ecr.ap-east-1.amazonaws.com      |
| Middle East (Bahrain) (Middle East (Bahrain)) | 541829937850.dkr.ecr.me-south-1.amazonaws.com     |
| Eropa (Milan)                                 | 528450769569.dkr.ecr.eu-south-1.amazonaws.com     |
| Eropa (Spanyol)                               | 531047660167.dkr.ecr.eu-south-2.amazonaws.com     |
| Afrika (Cape Town)                            | 379032919888.dkr.ecr.af-south-1.amazonaws.com     |
| Asia Pasifik (Melbourne)                      | 750462861327.dkr.ecr.ap-southeast-4.amazonaws.com |
| Israel (Tel Aviv)                             | 292660727137.dkr.ecr.il-central-1.amazonaws.com   |

## Repositori untuk GuardDuty agen di (hanya AWS Fargate AmazonECS)

Tabel berikut menunjukkan ECR repositori Amazon yang menghosting GuardDuty agen untuk (ECShanya AWS Fargate Amazon) untuk masing-masing. Wilayah AWS

| Wilayah AWS                    | ECRRepositori Amazon URI  |
|--------------------------------|---|
| AS Barat<br>(Oregon)           | 733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate    |
| Eropa (Paris)                  | 665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate    |
| Asia Pasifik<br>(Mumbai)       | 251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate   |
| Asia Pasifik<br>(Hyderabad)    | 950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate   |
| Kanada (Pusat)                 | 354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate |
| Timur Tengah<br>(UAE)          | 000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate |
| Eropa (London)                 | 892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate    |
| AS Barat<br>(California Utara) | 684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate    |
| AS Timur (N.<br>Virginia)      | 593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate    |
| AS Timur (Ohio)                | 307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate    |
| Eropa (Irlandia)               | 694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate    |

| Wilayah AWS                                   | ECRRepositori Amazon URI  |
|---|---|
| Amerika Selatan (Sao Paulo)                   | 758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate      |
| Eropa (Stockholm)                             | 591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Eropa (Frankfurt)                             | 323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate   |
| Eropa (Zürich)                                | 529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate   |
| Asia Pasifik (Singapura)                      | 174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Sydney)                         | 005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Jakarta)                        | 510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Tokyo)                          | 533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Seoul)                          | 914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Osaka)                          | 273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate |
| Asia Pasifik (Hong Kong)                      | 258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate      |
| Middle East (Bahrain) (Middle East (Bahrain)) | 536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate     |

| Wilayah AWS              | ECRRepositori Amazon URI  |
|--------------------------|---|
| Eropa (Milan)            | 266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Eropa (Spanyol)          | 919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate     |
| Afrika (Cape Town)       | 197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Asia Pasifik (Melbourne) | 251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate |
| Israel (Tel Aviv)        | 870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate   |

## GuardDuty sejarah rilis agen

Bagian berikut menyediakan versi rilis untuk GuardDuty agen yang akan digunakan di EC2 instans Amazon, kluster Amazon, dan ECS kluster Amazon EKS

### GuardDuty agen keamanan untuk EC2 instans Amazon

| Versi agen | Catatan rilis  | Tanggal ketersediaan |
|------------|--|----------------------|
| v1.3.0     | <p>Penyetelan dan penyempurnaan kinerja umum</p> <p>Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan <a href="#">Jenis penemuan Runtime Monitoring</a>.</p> | Agustus 19, 2024     |
| v1.2.0     | Mendukung distribusi OS Ubuntu 20.04, Ubuntu 22.04, Debian 11, dan Debian 12   | Juni 13, 2024        |

| Versi agen | Catatan rilis  | Tanggal ketersediaan |
|------------|--|----------------------|
|            | Mendukung kernel 6.5 dan 6.8<br><br>Penyetelan dan penyempurnaan kinerja umum  |                      |
| v1.1.0     | Mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk instans Amazon EC2<br><br>Mendukung sinyal dan temuan keamanan baru yang dirilis dengan pengumuman ketersediaan umum Runtime Monitoring untuk instance EC2<br><br>Penyetelan dan penyempurnaan kinerja umum | Maret 26, 2024       |
| v1.0.2     | Mendukung Amazon terbaru ECSAMIs.  | Februari 2, 2024     |
| v1.0.1     | Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon yang ECS AMIs diluncurkan setelah 31 Januari 2024.<br><br>Penyetelan dan penyempurnaan kinerja umum  | 23 Januari 2024      |



| Versi agen | Catatan rilis   | Tanggal ketersediaan |
|------------|---|----------------------|
| v1.0.0     | <p>Rilis awal RPM instalasi</p> <p>Versi agen yang dirilis sebelum v1.0.2 tidak kompatibel dengan Amazon yang ECS AMIs diluncurkan setelah 31 Januari 2024.</p> | 26 November 2023     |

## RPM S3 bucket example script

Kunci publik, tanda tangan x86\_64RPM, tanda tangan arm64RPM, dan tautan akses terkait ke RPM skrip yang dihosting di bucket Amazon S3 dapat dibentuk dari templat berikut. Ganti nilai Wilayah AWS, ID AWS akun, dan versi GuardDuty agen untuk mengakses RPM skrip. Template berikut menyertakan versi agen terbaru untuk EC2 instans Amazon.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem
```

- GuardDuty RPM Tanda tangan agen keamanan:

Tanda tangan dari x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig
```

Tanda tangan arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- Akses tautan ke RPM skrip di bucket Amazon S3:

Tautan akses untuk x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm
```

## Tautan akses untuk arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.rpm
```

## Debian S3 bucket example script

Kunci publik, tanda tangan dengan arm64, dan tautan akses yang sesuai ke skrip yang dihosting di bucket Amazon S3 dapat dibentuk dari templat berikut. Ganti nilai Wilayah AWS, ID AWS akun, dan versi GuardDuty agen untuk mengakses skrip. Template berikut menyertakan versi agen terbaru untuk EC2 instans Amazon.

- Kunci publik:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/publickey.pem
```

- GuardDuty Tanda tangan agen keamanan:

### Tanda tangan amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.sig
```

### Tanda tangan arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- Akses tautan ke skrip di bucket Amazon S3:

### Tautan akses untuk amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.deb
```

### Tautan akses untuk arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.deb
```

| Wilayah AWS    | Nama Wilayah                | AWS ID akun  |
|----------------|-----------------------------|--------------|
| eu-west-1      | Eropa (Irlandia)            | 694911143906 |
| us-east-1      | AS Timur (Virginia Utara)   | 593207742271 |
| us-east-2      | AS Timur (Ohio)             | 733349766148 |
| eu-west-3      | Eropa (Paris)               | 665651866788 |
| us-east-2      | AS Timur (Ohio)             | 307168627858 |
| eu-central-1   | Eropa (Frankfurt)           | 323658145986 |
| ap-northeast-2 | Asia Pasifik (Seoul)        | 914738172881 |
| eu-north-1     | Eropa (Stockholm)           | 591436053604 |
| ap-east-1      | Asia Pasifik (Hong Kong)    | 258348409381 |
| me-south-1     | Timur Tengah (Bahrain)      | 536382113932 |
| eu-west-2      | Eropa (London)              | 892757235363 |
| ap-northeast-1 | Asia Pasifik (Tokyo)        | 533107202818 |
| ap-southeast-1 | Asia Pasifik (Singapura)    | 174946120834 |
| ap-south-1     | Asia Pasifik (Mumbai)       | 251508486986 |
| ap-southeast-3 | Asia Pasifik (Jakarta)      | 510637619217 |
| sa-east-1      | Amerika Selatan (Sao Paulo) | 758426053663 |
| ap-northeast-3 | Asia Pasifik (Osaka)        | 273192626886 |
| eu-south-1     | Eropa (Milan)               | 266869475730 |
| af-south-1     | Afrika (Cape Town)          | 197869348890 |
| ap-southeast-2 | Asia Pasifik (Sydney)       | 005257825471 |

|                |                             |              |
|----------------|-----------------------------|--------------|
| me-central-1   | Timur Tengah (UAE)          | 000014521398 |
| us-west-1      | AS Barat (California Utara) | 684579721401 |
| ca-central-1   | Kanada (Pusat)              | 354763396469 |
| ap-south-2     | Asia Pasifik (Hyderabad)    | 950823858135 |
| eu-south-2     | Eropa (Spanyol)             | 919611009337 |
| eu-central-2   | Eropa (Zürich)              | 529164026651 |
| ap-southeast-4 | Asia Pasifik (Melbourne)    | 251357961535 |
| il-central-1   | Israel (Tel Aviv)           | 870907303882 |

## GuardDuty agen keamanan untuk AWS Fargate (ECShanya Amazon)

Tabel berikut menunjukkan riwayat versi rilis untuk agen GuardDuty keamanan untuk Fargate (ECShanya Amazon).

| Versi agen | Gambar kontainer   | Catatan rilis   | Tanggal ketersediaan |
|------------|--|---|----------------------|
| v1.3.0     | x86_64 (): AMD64 sha256: f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831<br><br>Graviton () ARM64: sha256: ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1 | Penyetelan dan peningkatan kinerja umum.<br><br>Termasuk dukungan untuk menangkap sinyal keamanan tambahan untuk masa depan GuardDuty <a href="#">Jenis penemuan Runtime Monitoring</a> . | Agustus 9, 2024      |

| Versi agen | Gambar kontainer  | Catatan rilis   | Tanggal ketersediaan |
|------------|---|---|----------------------|
| v1.2.0     | <p>x86_64 (): AMD64 sha256:1d<br/>bad20ac2dc66d52d00<br/>bb28dde4281fe0d3c5<br/>f261b1649b247c2369<br/>d9e26b93</p> <p>Graviton () ARM64: sha256:91<br/>930f8446f5f95b93b8<br/>ccb18773992affa401<br/>eb3f42da89d68077a5<br/>6bafa6cd</p> | Penyetelan dan peningkatan kinerja umum.  | 31 Mei 2024          |
| v1.1.0     | <p>x86_64 (): AMD64 sha256:83<br/>ce3cf2ef85a349ed17<br/>97a8cf30a008ac5d8c<br/>9f673f2835823957e9<br/>dcf71657</p> <p>Graviton () ARM64: sha256:0d<br/>4b61648d7bdeab8ab8<br/>d94684f805498927c7<br/>d437d318204dcccfe8<br/>c9383dc7</p> | <p>Mendukung sinyal dan temuan keamanan baru.</p> <p>Penyetelan dan peningkatan kinerja umum.</p> | 01 Mei 2024          |

| Versi agen | Gambar kontainer   | Catatan rilis   | Tanggal ketersediaan |
|------------|--|---|----------------------|
| v1.0.1     | x86_64 (): AMD64 sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68<br><br>Graviton () ARM64: sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7 | Penyetelan dan peningkatan kinerja umum.                                | Januari 26, 2024     |
| v1.0.0     | x86_64 (): AMD64 sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017<br><br>Graviton () ARM64: sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984 | Rilis awal agen GuardDuty keamanan untuk AWS Fargate (ECShanya Amazon). | 26 November 2023     |

## GuardDuty agen keamanan untuk EKS cluster Amazon

Tabel berikut menunjukkan riwayat versi rilis [GuardDuty agen EKS add-on Amazon](#).

| Versi agen | Gambar kontainer                    | Catatan rilis  | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|-------------------------------------|----------------|----------------------|--|
| v1.7.0     | x86_64 (): AMD64 sha256:f3a2a8806e6 | Penyetelan dan | Agustus 17, 2024     | –  |

| Versi agen | Gambar kontainer  | Catatan rilis   | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|---|---|----------------------|--|
|            | <p>c2a7fd63a91cccf6f7<br/>dffcd7e68554a423d6<br/>10cea8c7e8f2185ec</p> <p>Graviton () ARM64:<br/>sha256:b1a6db35a07<br/>2c0de3c695e5e909a0<br/>3e6c4e1fdbbe47ecfae<br/>b2784435cf67ebe0a</p>  | <p>peningkat<br/>an kinerja<br/>umum.</p> <p>Termasuk<br/>dukungan<br/>untuk<br/>menangkap<br/>sinyal<br/>keamanan<br/>tambahan<br/>untuk masa<br/>depan <a href="#">Jenis<br/>penemuan<br/>Runtime<br/>Monitoring.</a></p> |                      |  |
| v1.6.1     | <p>x86_64 (): AMD64<br/>sha256:30650708a66<br/>01f6d6b9046f54b30f<br/>5fd65af296b1e40b8c<br/>24426b9bdb07c3ab1</p> <p>Graviton () ARM64:<br/>sha256:5f637c42ffb<br/>306b20f776d9d83e1e<br/>0b4be40ce245be44af<br/>cf43a8902b4d71019</p> | <p>Penyetela<br/>n dan<br/>peningkat<br/>an kinerja<br/>umum.</p>   | 14 Mei 2024          | –  |

| Versi agen | Gambar kontainer  | Catatan rilis   | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|---|---|----------------------|--|
| v1.6.0     | <p>x86_64 (): AMD64<br/>sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010</p> <p>Graviton () ARM64:<br/>sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650</p> | <ul style="list-style-type: none"> <li>• Mendukung konfigurasi agen GuardDuty otomatis EKS EC2 untuk/sumber daya.</li> <li>• Mendukung sinyal dan temuan keamanan baru. Untuk informasi selengkapnya, silakan lihat <a href="#">Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty dan Jenis penemuan Runtime Monitoring</a>.</li> <li>• Penyetelan dan</li> </ul> | April 29, 2024       | –  |



| Versi agen | Gambar kontainer  | Catatan rilis  | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|---|--|----------------------|--|
|            |   | peningkat an kinerja umum.   |                      |  |
| v1.5.0     | <p>x86_64 (): AMD64<br/>sha256 : e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d</p> <p>Graviton () ARM64:<br/>sha256 : afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6</p> | <ul style="list-style-type: none"> <li>• Penyetelan dan peningkatan kinerja umum.</li> <li>• Peningkatan keamanan termasuk jenis acara baru di bawah. <a href="#">Jenis acara runtime yang dikumpulkan</a></li> <li>• Peningkatan kinerja seputar CPU penggunaan.</li> </ul> | 07 Maret 2024        | –  |

| Versi agen | Gambar kontainer   | Catatan rilis   | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|--|---|----------------------|--|
| v1.4.1     | <p>x86_64 (): AMD64<br/>sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c</p> <p>Graviton () ARM64:<br/>sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dff<br/>e0792c9e6d0778b40</p> | Penyetelan dan peningkatan kinerja umum.  | Januari 16, 2024     | –  |
| v1.4.0     | <p>x86_64 (): AMD64<br/>sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f</p> <p>Graviton () ARM64:<br/>sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aeb67f8e</p>       | <p>Manifest mount point mendukung pengumpulan data yang lebih baik</p> <p>AppArmor konfigurasi dalam manifes</p> <p>Kumpulkan argumen baris perintah</p> <p>Penyetelan dan penyempurnaan kinerja umum</p> | 21 Desember 2023     | –  |

| Versi agen | Gambar kontainer   | Catatan rilis   | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|--|---|----------------------|--|
| v1.3.1     | <p>x86_64 (): AMD64<br/>sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29</p> <p>Graviton () ARM64:<br/>sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd</p>  | Patch dan pembaruan keamanan penting.   | 23 Oktober 2023      | –  |
| v1.3.0     | <p>x86_64 (): AMD64<br/>sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbb69530bfbfd46c694</p> <p>Graviton () ARM64:<br/>sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb</p> | <p>Mendukung platform Ubuntu</p> <p>Mendukung Kubernetes versi 1.28</p> <p>Peningkatan kinerja umum dan peningkatan stabilitas.</p> | Oktober 05, 2023     | –  |

| Versi agen | Gambar kontainer  | Catatan rilis   | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|---|---|----------------------|--|
| v1.2.0     | <p>x86_64 (): AMD64<br/>sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3</p> <p>Graviton () ARM64:<br/>sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa</p> | <p>Selain instance AMD64 berbasis, v1.2.0 sekarang juga mendukung instance ARM64 berbasis. Menambahk an dan memverifikasi dukungan untuk Bottlerocket</p> <p>Mendukung Kubernetes versi 1.27</p> <p>Peningkat an kinerja umum dan peningkatan stabilitas.</p> | Juni 16, 2023        | –  |

| Versi agen | Gambar kontainer  | Catatan rilis  | Tanggal ketersediaan | Akhir dari dukungan standar <sup>1</sup> |
|------------|---|--|----------------------|--|
| v1.1.0     | sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c | Selain itu <a href="#">Versi Kubernetes didukung oleh agen keamanan GuardDuty</a> , rilis agen ini juga mendukung Kubernetes versi 1.26.<br><br>Peningkatan kinerja umum dan peningkatan stabilitas. | 2 Mei 2023           | 14 Mei 2024                              |
| v1.0.0     | sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e | Rilis awal agen EKS add-on Amazon.   | 30 Maret 2023        | 14 Mei 2024                              |

<sup>1</sup> Untuk informasi tentang memperbarui versi agen Anda saat ini yang mendekati akhir dukungan standar, lihat [Memperbarui agen keamanan secara manual](#).

## Dampak menonaktifkan dan membersihkan sumber daya

Bagian ini berlaku untuk Anda Akun AWS jika Anda memilih untuk menonaktifkan Runtime Monitoring, atau hanya konfigurasi agen GuardDuty otomatis untuk jenis sumber daya.

## Menonaktifkan konfigurasi agen GuardDuty otomatis

GuardDuty tidak menghapus agen keamanan yang digunakan pada sumber daya Anda. Namun, GuardDuty akan berhenti mengelola pembaruan ke agen keamanan.

GuardDuty terus menerima peristiwa runtime dari jenis sumber daya Anda. Untuk mencegah dampak pada statistik penggunaan Anda, pastikan untuk menghapus agen GuardDuty keamanan dari sumber daya Anda.

Apakah Akun AWS menggunakan VPC titik akhir bersama atau tidak, GuardDuty tidak menghapus titik VPC akhir. Jika diperlukan, Anda harus menghapus VPC titik akhir secara manual.

## Menonaktifkan Runtime Monitoring dan Runtime Monitoring EKS

Bagian ini berlaku untuk Anda dalam skenario berikut:

- Anda tidak pernah mengaktifkan EKS Runtime Monitoring secara terpisah dan sekarang Anda menonaktifkan Runtime Monitoring.
- Anda menonaktifkan Runtime Monitoring dan Runtime Monitoring EKS. Jika Anda tidak yakin tentang status konfigurasi EKS Runtime Monitoring, lihat [Memeriksa EKS status konfigurasi Runtime Monitoring](#)

**i** Menonaktifkan Runtime Monitoring tanpa menonaktifkan Runtime Monitoring EKS  
Dalam skenario ini, di beberapa titik waktu, Anda mengaktifkan EKS Runtime Monitoring, dan yang lebih baru, juga mengaktifkan Runtime Monitoring tanpa EKS menonaktifkan Runtime Monitoring.  
Sekarang, ketika Anda menonaktifkan Runtime Monitoring, Anda juga perlu menonaktifkan EKS Runtime Monitoring; jika tidak, Anda akan terus mengeluarkan biaya penggunaan untuk Runtime Monitoring EKS.

Jika skenario yang tercantum sebelumnya berlaku untuk Anda, maka GuardDuty akan mengambil tindakan berikut di akun Anda:

- GuardDuty menghapus VPC yang memiliki `true` tagGuardDutyManaged:. Ini adalah VPC yang GuardDuty telah dibuat untuk mengelola agen keamanan otomatis.
- GuardDuty menghapus grup keamanan yang ditandai sebagaiGuardDutyManaged:. `true`

- Untuk berbagi VPC yang telah digunakan oleh setidaknya satu akun peserta, GuardDuty tidak menghapus VPC titik akhir maupun grup keamanan yang terkait dengan sumber daya bersamaVPC.
- Untuk sumber EKS daya Amazon, GuardDuty hapus agen keamanan. Ini independen dari apakah dikelola secara manual atau melalui GuardDuty.

Untuk ECS sumber daya Amazon, karena ECS tugas tidak dapat diubah, tidak GuardDuty dapat menghapus instalasi agen keamanan dari sumber daya tersebut. Ini tidak tergantung pada bagaimana Anda mengelola agen keamanan — secara manual atau otomatis melalui GuardDuty. Setelah Anda menonaktifkan Runtime Monitoring, tidak GuardDuty akan melampirkan wadah sespan saat ECS tugas baru mulai berjalan. Untuk informasi tentang bekerja dengan Fargate- ECS tugas, lihat. [Bagaimana Runtime Monitoring bekerja dengan Fargate \(hanya AmazonECS\)](#)

Untuk EC2 sumber daya Amazon, GuardDuty hapus instalasi agen keamanan dari semua EC2 instans Amazon yang dikelola Systems Manager (SSM) hanya jika memenuhi ketentuan berikut:

- Sumber daya Anda tidak ditandai denganGuardDutyManaged: tag false pengecualian.
- GuardDuty harus memiliki izin untuk mengakses tag dalam metadata instance. Untuk EC2 sumber daya ini, Access to tag dalam metadata instance disetel ke Allow.

Ketika Anda berhenti mengelola agen keamanan secara manual

Terlepas dari pendekatan mana yang Anda gunakan untuk menyebarkan dan mengelola agen GuardDuty keamanan, untuk berhenti memantau peristiwa runtime di sumber daya Anda, Anda harus menghapus agen GuardDuty keamanan. Jika Anda ingin berhenti memantau peristiwa runtime dari jenis sumber daya di akun, Anda juga dapat menghapus titik VPC akhir Amazon.

## Proses untuk membersihkan sumber daya agen keamanan

Untuk menghapus titik VPC akhir Amazon

- Tanpa berbagi VPC - Saat Anda tidak lagi ingin memantau sumber daya di akun, pertimbangkan untuk menghapus titik VPC akhir Amazon.
- Dengan berbagi VPC — Saat akun VPC pemilik bersama menghapus VPC sumber daya bersama yang masih digunakan, status cakupan Runtime Monitoring (dan bila berlaku, EKS Runtime Monitoring) untuk sumber daya di akun VPC pemilik bersama Anda dan akun

yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi tentang status cakupan, lihat [Menilai cakupan runtime untuk sumber daya Anda](#).

Untuk informasi selengkapnya, lihat [Menghapus titik akhir antarmuka](#).

Untuk menghapus grup keamanan

- Tanpa berbagi VPC - Jika Anda tidak lagi ingin memantau jenis sumber daya di akun, pertimbangkan untuk menghapus grup keamanan yang terkait dengan AmazonVPC.
- Dengan berbagi VPC — Saat akun VPC pemilik bersama menghapus grup keamanan, akun peserta apa pun yang saat ini menggunakan grup keamanan yang terkait dengan yang dibagikanVPC, status cakupan Pemantauan Waktu Jalan untuk sumber daya di akun VPC pemilik bersama Anda dan akun yang berpartisipasi mungkin menjadi tidak sehat. Untuk informasi selengkapnya, lihat [Menilai cakupan runtime untuk sumber daya Anda](#).

Untuk informasi selengkapnya, lihat [Menghapus grup keamanan](#).

Untuk menghapus agen GuardDuty keamanan dari EKS kluster

Untuk menghapus agen keamanan dari EKS kluster yang tidak ingin Anda pantau lagi, lihat [Menghapus add-on](#).

Menghapus agen EKS add-on tidak menghapus amazon-guardduty namespace dari cluster. EKS Untuk menghapus amazon-guardduty namespace, lihat [Menghapus namespace](#).

Untuk menghapus **amazon-guardduty** namespace (cluster) EKS

Menonaktifkan konfigurasi agen otomatis tidak secara otomatis menghapus amazon-guardduty namespace dari kluster Anda. EKS Untuk menghapus amazon-guardduty namespace, lihat [Menghapus namespace](#).



## GuardDuty Perlindungan Malware untuk EC2

Perlindungan Malware for EC2 membantu Anda mendeteksi potensi keberadaan malware dengan memindai [volume Amazon Elastic Block Store \(AmazonEBS\)](#) yang dilampirkan ke instans Amazon Elastic Compute Cloud (AmazonEC2) dan beban kerja kontainer. Perlindungan Malware untuk EC2 menyediakan opsi pemindaian di mana Anda dapat memutuskan apakah Anda ingin menyertakan atau mengecualikan EC2 instans Amazon tertentu dan beban kerja kontainer pada saat pemindaian. Ini juga menyediakan opsi untuk menyimpan snapshot EBS volume Amazon yang dilampirkan ke EC2 instans Amazon atau beban kerja penampung, di akun Anda. GuardDuty Cuplikan disimpan hanya ketika malware ditemukan dan Perlindungan Malware untuk EC2 temuan dihasilkan.

Perlindungan Malware for EC2 adalah peningkatan opsional untuk GuardDuty, dan dirancang sedemikian rupa sehingga tidak akan memengaruhi kinerja sumber daya Anda. Untuk informasi tentang cara EC2 kerja Perlindungan Malware di dalamnya GuardDuty, lihat [Fitur dalam Perlindungan Malware untuk EC2](#). Untuk informasi tentang ketersediaan Perlindungan Malware untuk EC2 di berbagai jenis Wilayah AWS, lihat [Wilayah dan titik akhir](#).

### Catatan

GuardDuty Perlindungan Malware untuk EC2 tidak mendukung Fargate dengan Amazon atau EKS Amazon. ECS

Perlindungan Malware for EC2 menawarkan dua jenis pemindaian untuk mendeteksi aktivitas yang berpotensi berbahaya di EC2 instans Amazon dan beban kerja kontainer Anda — pemindaian malware yang GuardDuty dimulai dan pemindaian malware sesuai permintaan. Tabel berikut menunjukkan perbandingan antara kedua jenis pemindaian.

| Faktor                         | GuardDuty-pemindaian malware yang dimulai  | Pemindaian malware sesuai permintaan   |
|--------------------------------|--|--|
| Bagaimana pemindaian dipanggil | Setelah Anda mengaktifkan GuardDuty pemindaian malware yang dimulai, setiap kali GuardDuty menghasilkan temuan yang menunjukkan potensi keberadaan malware | Anda dapat memulai pemindaian malware On-Demand dengan memberikan Amazon Resource Name (ARN) yang terkait dengan EC2 instans Amazon atau |

| Faktor                                     | GuardDuty-pemindaian malware yang dimulai  | Pemindaian malware sesuai permintaan  |
|--|--|---|
|  | <p>di EC2 instans Amazon atau beban kerja kontainer, GuardDuty secara otomatis memulai pemindaian malware tanpa agen pada EBS volume Amazon yang dilampirkan ke sumber daya yang berpotensi terkena dampak. Untuk informasi selengkapnya, lihat <a href="#">GuardDuty-pemindaian malware yang dimulai</a>.</p> | <p>beban kerja container Anda. Anda dapat memulai pemindaian malware On-Demand bahkan ketika tidak ada GuardDuty temuan yang dihasilkan untuk sumber daya Anda. Untuk informasi selengkapnya, lihat <a href="#">Pemindaian malware sesuai permintaan</a>.</p> |
| Konfigurasi diperlukan                     | <p>Untuk menggunakan GuardDuty pemindaian malware yang dimulai, Anda harus mengaktifkannya untuk akun Anda. Untuk informasi selengkapnya, lihat <a href="#">Mengkonfigurasi pemindaian GuardDuty malware yang dimulai</a>.</p>   | <p>Akun Anda harus GuardDuty diaktifkan. Untuk menggunakan pemindaian malware On-Demand, tidak ada konfigurasi yang diperlukan di tingkat fitur.</p>  |
| Tunggu waktu untuk memulai pemindaian baru | <p>Setiap kali GuardDuty menghasilkan salah satu <a href="#">Temuan yang memanggil pemindaian GuardDuty malware yang dimulai</a>, pemindaian malware dimulai secara otomatis hanya sekali setiap 24 jam.</p>   | <p>Anda dapat memulai pemindaian malware On-Demand pada sumber daya yang sama kapan saja setelah 1 jam dari waktu mulai pemindaian sebelumnya.</p>  |

| Faktor                                       | GuardDuty-pemindaian malware yang dimulai  | Pemindaian malware sesuai permintaan  |
|--|--|---|
| Ketersediaan periode uji coba gratis 30 hari | <p>Saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai untuk pertama kalinya di akun Anda, Anda dapat menggunakan periode uji coba gratis 30 hari*.</p> <p>Untuk informasi selengkapnya tentang GuardDuty pemindaian malware yang dimulai, lihat. <a href="#">Uji coba gratis 30 hari</a></p>                   | Tidak ada periode uji coba gratis* dengan pemindaian malware sesuai permintaan untuk GuardDuty akun baru atau yang sudah ada.   |
| Opsi pemindaian                              | Setelah Anda mengonfigurasi GuardDuty pemindaian malware yang dimulai, Perlindungan Malware untuk EC2 juga membantu Anda memilih sumber daya mana yang akan dipindai atau dilewati. Perlindungan Malware for tidak EC2 akan memulai pemindaian otomatis pada sumber daya yang Anda pilih untuk dikecualikan dari pemindaian. | Pemindaian malware sesuai permintaan mendukung tag global —GuardDuty Excluded . <a href="#">Opsi pindai dengan tag yang ditentukan pengguna</a> tidak berlaku untuk pemindaian malware On-Demand karena Anda menyediakan sumber daya ARN secara manual. |

\* Anda akan dikenakan biaya penggunaan untuk membuat snapshot EBS volume dan mempertahankan snapshot. Untuk informasi selengkapnya tentang mengonfigurasi akun Anda untuk menyimpan snapshot, lihat. [Retensi snapshot](#)

# Fitur dalam Perlindungan Malware untuk EC2

## Volume Penyimpanan Blok Elastis (EBS)

Bagian ini menjelaskan cara Perlindungan Malware untuk EC2, termasuk pemindaian malware yang GuardDuty dimulai dan pemindaian malware sesuai permintaan, memindai volume Amazon yang terkait dengan instans EBS Amazon dan beban kerja EC2 kontainer Anda. Sebelum melanjutkan, pertimbangkan penyesuaian berikut:

- Opsi pemindaian — Perlindungan Malware untuk EC2 menawarkan kemampuan untuk menentukan tag untuk menyertakan atau mengecualikan EC2 instans Amazon dan EBS volume Amazon dari proses pemindaian. Hanya GuardDuty pemindaian malware yang dimulai yang mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Baik GuardDuty pemindaian malware yang dimulai dan pemindaian malware sesuai permintaan mendukung tag global. GuardDutyExcluded Untuk informasi selengkapnya, lihat [Opsi pindai dengan tag yang ditentukan pengguna](#).
- Retensi snapshot — Perlindungan Malware untuk EC2 menyediakan opsi untuk menyimpan snapshot EBS volume Amazon Anda di akun Anda AWS . Secara default, opsi ini dimatikan. Anda dapat memilih penyimpanan snapshot untuk pemindaian malware GuardDuty yang dimulai dan sesuai permintaan. Untuk informasi selengkapnya, lihat [Retensi snapshot](#).

Saat GuardDuty menghasilkan temuan yang menunjukkan potensi keberadaan malware di EC2 instans Amazon atau beban kerja kontainer dan Anda telah mengaktifkan jenis pemindaian yang GuardDuty dimulai dalam Perlindungan Malware untuk EC2, pemindaian malware yang GuardDuty dimulai dapat dipanggil berdasarkan opsi pemindaian Anda.

Untuk memulai pemindaian malware On-Demand pada EBS volume Amazon yang terkait dengan EC2 instans Amazon, berikan Amazon Resource Name (ARN) dari instans Amazon EC2.

Sebagai tanggapan terhadap pemindaian malware On-Demand atau pemindaian malware yang GuardDuty dimulai secara otomatis, GuardDuty membuat snapshot dari EBS volume relevan yang dilampirkan ke sumber daya yang berpotensi terkena dampak, dan membagikannya dengan [GuardDuty akun layanan](#). Dari snapshot ini, GuardDuty buat EBS volume replika terenkripsi di akun layanan.

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Setelah pemindaian selesai, GuardDuty hapus volume replika terenkripsi dan snapshot EBS volume Anda. EBS Jika malware ditemukan dan Anda telah mengaktifkan pengaturan retensi snapshot, snapshot EBS volume Anda tidak akan dihapus dan secara otomatis disimpan di akun Anda. AWS Ketika tidak ada malware yang ditemukan, snapshot EBS volume Anda tidak akan dipertahankan, terlepas dari pengaturan retensi snapshot. Secara default, pengaturan retensi snapshot dimatikan. Untuk informasi tentang biaya snapshot dan retensinya, lihat [EBSharga Amazon](#).

GuardDuty akan mempertahankan setiap EBS volume replika di akun layanan hingga 55 jam. Jika ada pemadaman layanan, atau kegagalan dengan EBS volume replika dan pemindaian malware, GuardDuty akan mempertahankan EBS volume seperti itu selama tidak lebih dari tujuh hari. Periode retensi volume yang diperpanjang adalah untuk melakukan triase dan mengatasi pemadaman atau kegagalan. GuardDuty Perlindungan Malware for EC2 akan menghapus EBS volume replika dari akun layanan setelah pemadaman atau kegagalan ditangani, atau setelah periode retensi yang diperpanjang berakhir.

## EBSVolume Amazon yang didukung untuk pemindaian malware

Di semua Wilayah AWS tempat GuardDuty mendukung fitur Perlindungan Malware untuk EC2 fitur, Anda dapat memindai EBS volume Amazon yang tidak dienkripsi atau dienkripsi. Anda dapat memiliki EBS volume Amazon yang dienkripsi dengan salah satu [Kunci yang dikelola AWS](#) atau kunci yang [dikelola pelanggan](#). Saat ini, beberapa Wilayah AWS mendukung kedua cara untuk mengenkripsi EBS volume Amazon Anda, sementara yang lain hanya mendukung kunci yang dikelola pelanggan.

Untuk informasi selengkapnya di mana kemampuan ini belum didukung, lihat [China Regions](#)

Daftar berikut menjelaskan kunci yang GuardDuty menggunakan apakah EBS volume Amazon Anda dienkripsi atau tidak:

- EBSVolume Amazon yang tidak dienkripsi atau dienkripsi Kunci yang dikelola AWS- GuardDuty menggunakan kuncinya sendiri untuk mengenkripsi replika volume Amazon. EBS

Jika akun Anda termasuk dalam akun Wilayah AWS yang tidak mendukung pemindaian EBS volume Amazon yang dienkripsi dengan [default Kunci yang dikelola AWS untuk EBS](#), lihat [Memodifikasi ID AWS KMS kunci default dari volume Amazon EBS](#)

- EBSVolume Amazon yang dienkripsi dengan kunci yang dikelola pelanggan — GuardDuty menggunakan kunci yang sama untuk mengenkripsi volume replika. EBS

Perlindungan Malware untuk EC2 tidak mendukung pemindaian EC2 instans Amazon dengan `productCode asmarketplace`. Jika pemindaian malware dimulai untuk EC2 instance Amazon seperti itu, pemindaian akan dilewati. Untuk informasi selengkapnya, lihat `UNSUPPORTED_PRODUCT_CODE_TYPE` di [Alasan melewati sumber daya selama pemindaian malware](#).

## Memodifikasi ID AWS KMS kunci default dari volume Amazon EBS

Secara default, memanggil enkripsi [CreateVolume](#) API with yang disetel ke `true` dan tidak menentukan ID KMS kunci, membuat EBS volume Amazon yang dienkripsi dengan kunci [default AWS KMS](#) untuk enkripsi. EBS Namun, ketika kunci enkripsi tidak disediakan secara eksplisit, Anda dapat memodifikasi kunci default dengan memanggil [ModifyEbsDefaultKmsKeyId](#) API atau dengan menggunakan perintah yang sesuai. AWS CLI

Untuk mengubah ID kunci EBS default, tambahkan izin yang diperlukan berikut ke IAM kebijakan Anda —`ec2:modifyEbsDefaultKmsKeyId`. EBS Volume Amazon yang baru dibuat yang Anda pilih untuk dienkripsi tetapi tidak menentukan ID KMS kunci terkait, akan menggunakan ID kunci default. Gunakan salah satu metode berikut untuk memperbarui ID kunci EBS default:

Untuk mengubah ID KMS kunci default dari EBS volume Amazon

Lakukan salah satu hal berikut ini:

- Menggunakan API — Anda dapat menggunakan [ModifyEbsDefaultKmsKeyId](#) API. Untuk informasi tentang cara melihat status enkripsi volume, lihat [Membuat EBS volume Amazon](#).
- Menggunakan AWS CLI perintah - Contoh berikut memodifikasi ID KMS kunci default yang akan mengenkripsi EBS volume Amazon jika Anda tidak memberikan ID KMS kunci. Pastikan untuk mengganti Region dengan ID kunci KM Anda. Wilayah AWS

```
aws ec2 modify-efs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

Perintah di atas akan menghasilkan output yang mirip dengan output berikut:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Untuk informasi selengkapnya, lihat [modify-efs-default-kms-key-id](#).

# Kustomisasi dalam Perlindungan Malware untuk EC2

Bagian ini menjelaskan bagaimana Anda dapat menyesuaikan opsi pemindaian untuk EC2 instans Amazon atau beban kerja kontainer saat pemindaian malware dipanggil, baik dimulai sesuai permintaan atau melalui GuardDuty

## Pengaturan umum

### Retensi snapshot

GuardDuty memberi Anda opsi untuk menyimpan snapshot EBS volume Anda di AWS akun Anda. Secara default, pengaturan retensi snapshot dimatikan. Snapshot hanya akan dipertahankan jika pengaturan ini diaktifkan sebelum pemindaian dimulai.

Saat pemindaian dimulai, GuardDuty hasilkan EBS volume replika berdasarkan snapshot volume Anda. EBS Setelah pemindaian selesai dan pengaturan retensi snapshot di akun Anda sudah diaktifkan, snapshot EBS volume Anda akan dipertahankan hanya ketika malware ditemukan dan dihasilkan. [Perlindungan Malware untuk jenis pencarian EC2](#) Apakah Anda telah mengaktifkan pengaturan retensi snapshot atau tidak, ketika tidak ada malware yang terdeteksi, GuardDuty secara otomatis menghapus snapshot volume Anda. EBS

### Biaya penggunaan snapshot

Selama pemindaian malware, seperti GuardDuty membuat snapshot EBS volume Amazon Anda, ada biaya penggunaan yang terkait dengan langkah ini. Jika Anda mengaktifkan pengaturan penyimpanan snapshot untuk akun Anda, ketika malware ditemukan dan snapshot dipertahankan, Anda akan dikenakan biaya penggunaan untuk hal yang sama. Untuk informasi tentang biaya snapshot dan retensinya, lihat [EBSharga Amazon](#).

Pilih metode akses pilihan Anda untuk mengaktifkan pengaturan retensi snapshot.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Pilih Pengaturan umum di bagian bawah konsol. Untuk mempertahankan snapshot, aktifkan retensi Snapshots.

## API/CLI

1. Jalankan [UpdateMalwareScanSettings](#) untuk memperbarui konfigurasi saat ini untuk pengaturan retensi snapshot.
2. Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk menyimpan snapshot secara otomatis saat Perlindungan GuardDuty Malware untuk EC2 menghasilkan temuan.

Pastikan untuk mengganti *detector-id* dengan valid Anda sendiri `detectorId`.

3. Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

4. Jika Anda ingin mematikan retensi snapshot, ganti `RETENTION_WITH_FINDING` dengan `NO_RETENTION`.

## Opsi pindai dengan tag yang ditentukan pengguna

Dengan menggunakan GuardDuty pemindaian malware yang dimulai, Anda juga dapat menentukan tag untuk menyertakan atau mengecualikan EC2 instans Amazon dan EBS volume Amazon dari proses pemindaian dan deteksi ancaman. Anda dapat menyesuaikan setiap GuardDuty pemindaian malware yang dimulai dengan mengedit tag di daftar tag penyertaan atau pengecualian. Setiap daftar dapat mencakup hingga 50 tag.

Jika Anda belum memiliki tag yang ditentukan pengguna yang terkait dengan EC2 sumber daya Anda, lihat [Menandai sumber EC2 daya Amazon](#) Anda di Panduan EC2 Pengguna Amazon atau [Menandai EC2 sumber daya Amazon](#) Anda di Panduan EC2 Pengguna Amazon.

### Note

Pemindaian malware sesuai permintaan tidak mendukung opsi pemindaian dengan tag yang ditentukan pengguna. Ini mendukung [GuardDutyExcludedTag global](#).



## Untuk mengecualikan EC2 instance dari pemindaian malware

Jika Anda ingin mengecualikan EC2 instans Amazon atau EBS volume Amazon selama proses pemindaian, Anda dapat mengatur `GuardDutyExcluded` tag `true` untuk EC2 instans Amazon atau EBS volume Amazon apa pun, dan GuardDuty tidak akan memindainya. Untuk informasi selengkapnya tentang `GuardDutyExcluded` tag, lihat [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#). Anda juga dapat menambahkan tag EC2 instans Amazon ke daftar pengecualian. Jika Anda menambahkan beberapa tag ke daftar tag pengecualian, EC2 instans Amazon apa pun yang berisi setidaknya satu tag ini akan dikecualikan dari proses pemindaian malware.

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan EC2 instans Amazon, ke daftar pengecualian.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian tag Inklusi/Pengecualian. Pilih Tambahkan tag.
4. Pilih tag Pengecualian dan kemudian pilih untuk Konfirmasi.
5. Tentukan tag **Key** dan **Value** pasangkan yang ingin Anda kecualikan. Ini opsional untuk menyediakan **Value**. Setelah Anda menambahkan semua tag, pilih Simpan.

#### Important

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon atau [Pembatasan Tag](#) di Panduan EC2 Pengguna Amazon.

Jika nilai untuk kunci tidak disediakan dan EC2 instance ditandai dengan kunci yang ditentukan, EC2 instance ini akan dikecualikan dari proses pemindaian pemindaian malware GuardDuty yang dimulai, terlepas dari nilai yang ditetapkan tag.

## API/CLI

- Perbarui pengaturan pemindaian malware dengan mengecualikan EC2 instance atau beban kerja kontainer dari proses pemindaian.

Perintah AWS CLI contoh berikut menambahkan tag baru ke daftar tag pengecualian. Pastikan untuk mengganti contoh *detector-id* dengan valid Anda sendiri `detectorId`.

MapEquals adalah daftar Key Value /pasangan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

### Important

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon atau [Pembatasan Tag](#) di Panduan EC2 Pengguna Amazon.

## Untuk memasukkan EC2 instance dalam pemindaian malware

Jika Anda ingin memindai EC2 instance, tambahkan tagnya ke daftar inklusi. Saat Anda menambahkan tag ke daftar tag inklusi, EC2 instance yang tidak berisi tag yang ditambahkan akan dilewati dari pemindaian malware. Jika Anda menambahkan beberapa tag ke daftar tag inklusi, EC2 instance yang berisi setidaknya satu dari tag tersebut disertakan dalam pemindaian malware. Terkadang, sebuah EC2 instance dapat dilewati selama proses pemindaian. Untuk informasi selengkapnya, lihat [Alasan melewatkan sumber daya selama pemindaian malware](#).

Pilih metode akses pilihan Anda untuk menambahkan tag yang terkait dengan EC2 instance, ke daftar inklusi.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. Perluas bagian tag Inklusi/Pengecualian. Pilih Tambahkan tag.
4. Pilih tag Inklusi dan kemudian pilih Konfirmasi.
5. Pilih Tambahkan tag inklusi baru dan tentukan tag **Key** dan **Value** pasangan yang ingin Anda sertakan. Ini opsional untuk menyediakan **Value**.

Setelah Anda menambahkan semua tag inklusi, pilih Simpan.

Jika nilai untuk kunci tidak diberikan, sebuah EC2 instance ditandai dengan kunci yang ditentukan, EC2 instance akan disertakan dalam proses Perlindungan Malware untuk EC2 pemindaian, terlepas dari nilai yang ditetapkan tag.

## API/CLI

- Perbarui pengaturan pemindaian malware untuk menyertakan EC2 instance atau beban kerja kontainer dalam proses pemindaian.

AWS CLI Contoh perintah berikut menambahkan tag baru ke daftar tag inklusi. Pastikan Anda mengganti contoh *detector-id* dengan valid Anda sendiri `detectorId`. Ganti contoh *TestKey* and *TestValue* dengan Key dan Value pasangan tag yang terkait dengan EC2 sumber daya Anda.

`MapEquals` adalah daftar Key Value /pasangan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Include": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

**⚠ Important**

Kunci dan nilai tag peka huruf besar dan kecil. Untuk informasi selengkapnya, lihat [Pembatasan tag](#) di Panduan EC2 Pengguna Amazon atau [Pembatasan Tag](#) di Panduan EC2 Pengguna Amazon.

**ℹ Note**

Mungkin diperlukan waktu hingga 5 menit GuardDuty untuk mendeteksi tag baru.

Kapan saja, Anda dapat memilih tag Inklusi atau tag Pengecualian tetapi tidak keduanya. Jika Anda ingin beralih di antara tag, pilih tag itu dari menu tarik-turun saat Anda menambahkan tag baru, dan Konfirmasikan pilihan Anda. Tindakan ini menghapus semua tag Anda saat ini.

## GuardDutyExcludedTag global

Secara default, snapshot EBS volume Anda dibuat dengan GuardDutyScanId tag. Jangan hapus tag ini karena hal itu akan GuardDuty mencegah mengakses snapshot. Kedua jenis pemindaian dalam Perlindungan Malware untuk EC2 tidak memindai EC2 instans Amazon atau EBS volume Amazon yang memiliki GuardDutyExcluded tag yang disetel ke true. Jika Perlindungan Malware untuk EC2 pemindaian pada sumber daya tersebut, ID pemindaian akan dihasilkan tetapi pemindaian akan dilewati dengan EXCLUDED\_BY\_SCAN\_SETTINGS alasan. Untuk informasi selengkapnya, lihat [Alasan melewatkan sumber daya selama pemindaian malware](#).

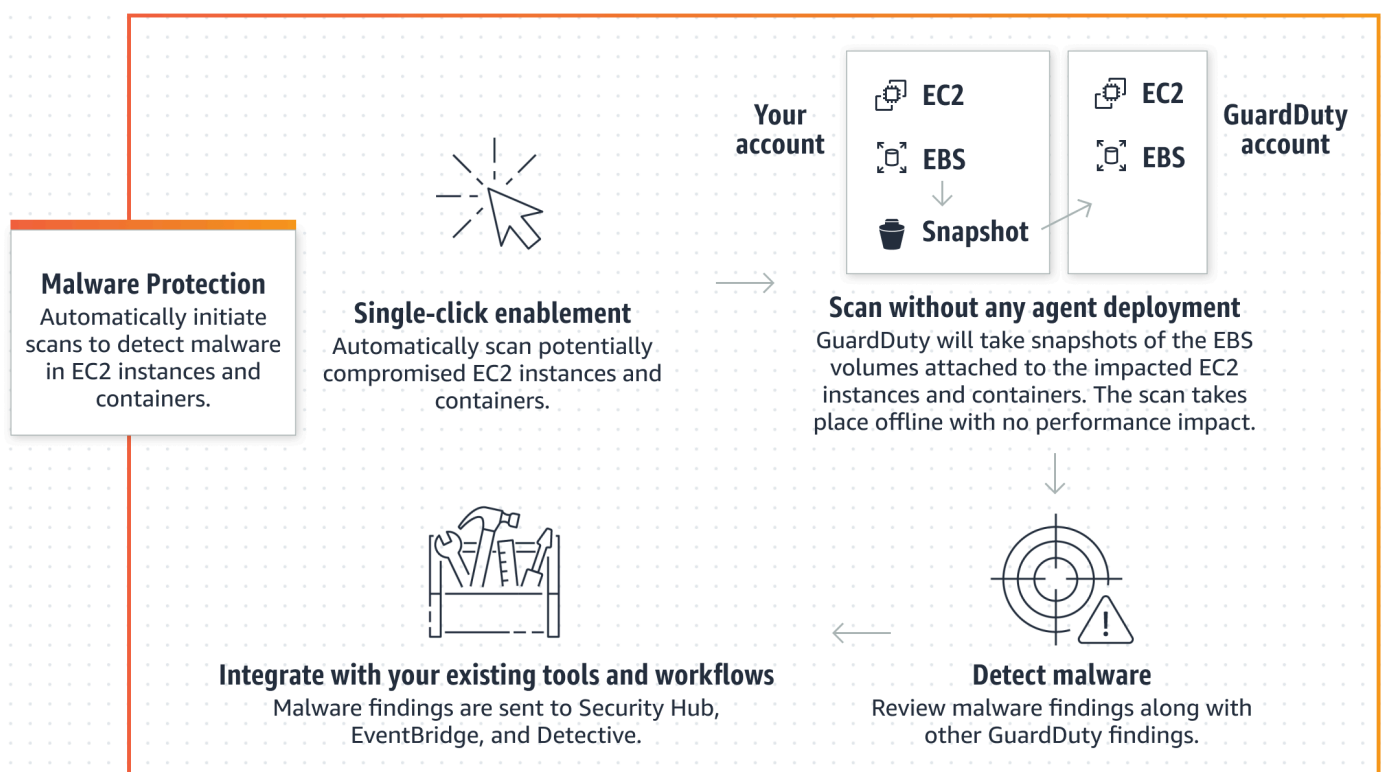
## GuardDuty-pemindaian malware yang dimulai

Dengan GuardDuty pemindaian malware yang dimulai diaktifkan, setiap kali GuardDuty mendeteksi aktivitas berbahaya yang menunjukkan potensi keberadaan malware di EC2 instans Amazon atau beban kerja container dan GuardDuty menghasilkan [Temuan yang memanggil pemindaian GuardDuty malware yang dimulai](#), GuardDuty secara otomatis memulai pemindaian tanpa agen pada volume Amazon Elastic Block Store (Amazon) yang dilampirkan ke instans EBS EC2 Amazon yang berpotensi terkena dampak atau beban kerja kontainer untuk mendeteksi keberadaan malware. Dengan opsi pemindaian, Anda dapat menambahkan tag inklusi yang terkait dengan sumber daya yang ingin Anda pindai atau menambahkan tag pengecualian yang terkait dengan sumber daya yang ingin Anda lewati dari proses pemindaian. Inisiasi pemindaian otomatis akan

selalu mempertimbangkan opsi pemindaian Anda. Anda juga dapat memilih untuk mengaktifkan pengaturan retensi snapshot untuk mempertahankan snapshot EBS volume Anda hanya jika Perlindungan Malware untuk EC2 mendeteksi keberadaan malware. Untuk informasi selengkapnya, lihat [Kustomisasi dalam Perlindungan Malware untuk EC2](#).

Untuk setiap EC2 instans Amazon dan beban kerja kontainer yang GuardDuty menghasilkan temuan, pemindaian malware GuardDuty yang dimulai secara otomatis akan dipanggil setiap 24 jam sekali. Untuk informasi tentang bagaimana EBS volume Amazon yang dilampirkan ke EC2 instans Amazon atau beban kerja penampung dipindai, lihat. [Fitur dalam Perlindungan Malware untuk EC2](#)

Gambar berikut menjelaskan cara kerja pemindaian malware GuardDuty yang dimulai.



Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Ketika malware ditemukan, GuardDuty hasilkan [Perlindungan Malware untuk jenis pencarian EC2](#). Jika GuardDuty tidak menghasilkan temuan yang menunjukkan malware pada sumber daya yang sama, tidak ada GuardDuty pemindaian malware yang dimulai yang akan dipanggil. Anda juga dapat memulai pemindaian malware On-Demand pada sumber daya yang sama. Untuk informasi selengkapnya, lihat [Pemindaian malware sesuai permintaan](#).

## Uji coba gratis 30 hari

Anda dapat memilih untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk perangkat Akun AWS yang didukung Wilayah AWS kapan saja. Jika Anda memiliki organisasi, setiap akun anggota memiliki uji coba gratis 30 hari sendiri.

Untuk memahami cara kerja uji coba gratis 30 hari, pertimbangkan skenario berikut:

- Saat Anda mengaktifkan GuardDuty untuk pertama kalinya ( GuardDuty akun baru), GuardDuty pemindaian malware yang dimulai juga akan diaktifkan dan disertakan dalam uji coba gratis 30 hari yang terkait dengan layanan. GuardDuty
- GuardDuty Akun yang ada dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk pertama kalinya dengan uji coba gratis 30 hari. Saat Anda mengaktifkan fitur ini di Wilayah yang berbeda untuk pertama kalinya, Anda akan mendapatkan uji coba gratis 30 hari di Wilayah tersebut.
- Jika Anda memiliki GuardDuty akun yang telah menggunakan Perlindungan Malware EC2 sebelum pemindaian malware sesuai permintaan diumumkan dan GuardDuty akun ini sudah menggunakan model harga untuk itu Wilayah AWS, Anda dapat terus menggunakan GuardDuty pemindaian malware yang dimulai.

### Note

Bahkan jika Anda berada pada periode uji coba gratis 30 hari, biaya penggunaan standar untuk membuat snapshot EBS volume Amazon dan retensi mereka berlaku. Untuk informasi selengkapnya, lihat [EBSharga Amazon](#).

Untuk informasi tentang mengaktifkan pemindaian malware GuardDuty yang dimulai, lihat.

[Mengkonfigurasi pemindaian GuardDuty malware yang dimulai](#)

## Mengkonfigurasi pemindaian GuardDuty malware yang dimulai

### Mengkonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun mandiri

Untuk akun yang terkait AWS Organizations, Anda dapat mengotomatiskan proses ini melalui pengaturan konsol, seperti yang dijelaskan di bagian berikutnya.

Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai

Pilih metode akses pilihan Anda untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun mandiri.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
3. EC2Panel Perlindungan Malware untuk mencantumkan status pemindaian malware GuardDuty yang dimulai saat ini untuk akun Anda. Anda dapat mengaktifkan atau menonaktifkannya kapan saja dengan memilih Aktifkan atau Nonaktifkan masing-masing.
4. Pilih Simpan.

## API/CLI

- Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan `dataSources` objek dengan `EbsVolumes` set ke `true` atau `false`.

Anda juga dapat mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai menggunakan alat baris AWS perintah dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan valid Anda sendiri *detector ID*.

### Note

Kode contoh berikut memungkinkan GuardDuty pemindaian malware yang dimulai. Untuk menonaktifkannya, ganti `true` dengan `false`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]
```

## Mengonfigurasi GuardDuty pemindaian malware yang dimulai di lingkungan beberapa akun

Di lingkungan multi-akun, hanya akun GuardDuty administrator yang dapat mengonfigurasi pemindaian GuardDuty malware yang dimulai. GuardDuty Akun administrator dapat mengaktifkan atau menonaktifkan penggunaan GuardDuty pemindaian malware yang dimulai untuk akun anggota mereka. Setelah akun administrator mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun anggota, akun anggota akan mengikuti pengaturan akun administrator dan tidak dapat mengubah pengaturan ini melalui konsol. GuardDuty Akun administrator yang mengelola akun anggota mereka dengan AWS Organizations dukungan dapat memilih untuk mengaktifkan pemindaian malware GuardDuty yang dimulai secara otomatis pada semua akun yang ada dan yang baru di organisasi. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty akun dengan AWS Organizations](#).

Membangun akses tepercaya untuk mengaktifkan GuardDuty pemindaian malware yang dimulai

Jika akun administrator GuardDuty yang didelegasikan tidak sama dengan akun manajemen di organisasi Anda, akun manajemen harus mengaktifkan pemindaian malware GuardDuty yang dimulai untuk organisasi mereka. Dengan cara ini, akun administrator yang didelegasikan dapat membuat akun anggota [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) di yang dikelola. AWS Organizations

### Note

Sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan, lihat [Pertimbangan dan rekomendasi](#)

Pilih metode akses pilihan Anda untuk mengizinkan akun GuardDuty administrator yang didelegasikan mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota di organisasi.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan akun manajemen untuk AWS Organizations organisasi Anda.

2. a. Jika Anda belum menetapkan akun GuardDuty administrator yang didelegasikan, maka:



Pada halaman Pengaturan, di bawah akun GuardDuty administrator yang didelegasikan, masukkan 12 digit **account ID** yang ingin Anda tetapkan untuk mengelola GuardDuty kebijakan di organisasi Anda. Pilih Delegasikan.

- b. i. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang berbeda dari akun manajemen, maka:

Pada halaman Pengaturan, di bawah Administrator Delegasi, aktifkan pengaturan Izin. Tindakan ini akan memungkinkan akun GuardDuty administrator yang didelegasikan untuk melampirkan izin yang relevan ke akun anggota dan mengaktifkan GuardDuty pemindaian malware yang dimulai di akun anggota ini.

- ii. Jika Anda telah menetapkan akun GuardDuty administrator yang didelegasikan yang sama dengan akun manajemen, maka Anda dapat langsung mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota. Untuk informasi selengkapnya, lihat [Aktifkan GuardDuty pemindaian malware yang dimulai secara otomatis untuk semua akun anggota](#).

 Tip

Jika akun GuardDuty administrator yang didelegasikan berbeda dari akun manajemen Anda, Anda harus memberikan izin ke akun GuardDuty administrator yang didelegasikan untuk memungkinkan mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota.

3. Jika Anda ingin mengizinkan akun GuardDuty administrator yang didelegasikan untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota di Wilayah lain, ubah Wilayah AWS, dan ulangi langkah-langkah di atas.

## API/CLI

1. Menggunakan kredensi akun manajemen Anda, jalankan perintah berikut:

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Opsional) untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun manajemen yang bukan akun administrator yang didelegasikan, akun manajemen pertama-

tama akan membuat secara [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) eksplisit di akun mereka, dan kemudian mengaktifkan GuardDuty pemindaian malware yang dimulai dari akun administrator yang didelegasikan, mirip dengan akun anggota lainnya.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. Anda telah menetapkan akun GuardDuty administrator yang didelegasikan dalam yang dipilih Wilayah AWS saat ini. Jika Anda telah menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan di satu wilayah, akun tersebut harus merupakan akun GuardDuty administrator yang didelegasikan di semua wilayah lain. Ulangi langkah di atas untuk semua Wilayah lainnya.

Mengkonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk akun administrator yang didelegasikan GuardDuty .

Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun manajemen.

2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di samping GuardDuty pemindaian malware yang dimulai.
4. Lakukan salah satu hal berikut ini:

Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

## Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

## API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek name sebagai `EBS_MALWARE_PROTECTION` dan status sebagai `ENABLED` atau `DISABLED`.

Anda dapat mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan yang valid *detector ID*.

### Note

Kode contoh berikut memungkinkan GuardDuty pemindaian malware yang dimulai. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 5555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Aktifkan GuardDuty pemindaian malware yang dimulai secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur pemindaian malware GuardDuty yang dimulai untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

## Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan Perlindungan Malware untuk EC2 halaman


1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
2. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di bagian GuardDuty pemindaian malware yang dimulai.
3. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada dan baru di organisasi.
4. Pilih Simpan.

### Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah GuardDuty pemindaian malware yang dimulai.
4. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit di bagian GuardDuty pemindaian malware yang dimulai.
5. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada dan baru di organisasi.
6. Pilih Simpan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

### Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah GuardDuty pemindaian malware yang dimulai.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan atau nonaktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota](#).

### API/CLI

- Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan operasi menggunakan milik Anda sendiri [updateMemberDetectors](#) API *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkan akun anggota, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada di organisasi.

Untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk semua akun anggota aktif yang ada

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
3. Pada Perlindungan Malware for EC2, Anda dapat melihat status saat ini dari konfigurasi pemindaian malware GuardDuty yang dimulai. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Simpan.

Aktifkan GuardDuty pemindaian malware yang dimulai secara otomatis untuk akun anggota baru

Akun anggota yang baru ditambahkan harus Aktifkan GuardDuty sebelum memilih mengkonfigurasi GuardDuty pemindaian malware yang dimulai. Akun anggota yang dikelola oleh undangan dapat mengonfigurasi GuardDuty pemindaian malware yang dimulai secara manual untuk akun mereka. Untuk informasi selengkapnya, lihat [Step 3 - Accept an invitation](#).

Pilih metode akses pilihan Anda untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun baru yang bergabung dengan organisasi Anda.

## Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota baru di organisasi, baik menggunakan halaman Perlindungan Malware untuk EC2 atau Akun.

Untuk mengaktifkan pemindaian malware GuardDuty yang dimulai secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan Perlindungan Malware untuk EC2 halaman:

1. Di panel navigasi, pilih Perlindungan Malware untuk EC2.
2. Pada EC2 halaman Perlindungan Malware untuk, pilih Edit dalam GuardDuty pemindaian malware yang dimulai.
3. Pilih Konfigurasi akun secara manual.
4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, GuardDuty pemindaian malware yang dimulai akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
5. Pilih Simpan.

- Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah GuardDuty pemindaian malware yang dimulai.
4. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota baru, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkannya, lihat [Aktifkan atau nonaktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota](#).

Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan atau nonaktifkan pemindaian malware GuardDuty yang dimulai secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengonfigurasi GuardDuty pemindaian malware yang dimulai untuk akun anggota secara selektif.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Akun.
3. Pada halaman Akun, tinjau kolom pemindaian malware yang GuardDuty dimulai untuk mengetahui status akun anggota Anda.
4. Pilih akun yang ingin Anda konfigurasi GuardDuty pemindaian malware yang dimulai. Anda dapat memilih beberapa akun sekaligus.
5. Dari menu Edit paket perlindungan, pilih opsi yang sesuai untuk GuardDuty pemindaian malware yang dimulai.

## API/CLI


Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan operasi menggunakan milik Anda sendiri `updateMemberDetectors` API *detector ID*.



Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
"Status": "ENABLED"}]'
```

 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai secara selektif untuk akun anggota Anda, jalankan `updateMemberDetectors` API operasi menggunakan milik Anda sendiri *detector ID*. Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan GuardDuty pemindaian malware yang dimulai untuk satu akun anggota. Untuk menonaktifkannya, ganti `true` dengan `false`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan `ListDetectors` API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

 Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar UnprocessedAccounts akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan GuardDuty pemindaian malware yang dimulai untuk akun yang ada di Organisasi yang dikelola melalui undangan

Perlindungan GuardDuty Malware untuk peran EC2 terkait layanan (SLR) harus dibuat di akun anggota. Akun administrator tidak dapat mengaktifkan fitur pemindaian malware GuardDuty yang dimulai di akun anggota yang tidak dikelola oleh AWS Organizations

Saat ini, Anda dapat melakukan langkah-langkah berikut melalui GuardDuty konsol di <https://console.aws.amazon.com/guardduty/> untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota yang ada.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun administrator Anda.

2. Di panel navigasi, pilih Akun.
3. Pilih akun anggota yang ingin Anda aktifkan pemindaian malware GuardDuty yang dimulai. Anda dapat memilih beberapa akun sekaligus.
4. Pilih Tindakan.
5. Pilih anggota Disassociate.
6. Di akun anggota Anda, pilih Perlindungan Malware di bawah Paket Perlindungan di panel navigasi.
7. Pilih Aktifkan GuardDuty pemindaian malware yang dimulai. GuardDuty akan membuat akun SLR untuk anggota. Untuk informasi lebih lanjut tentang SLR, lihat [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#).
8. Di akun administrator Anda, pilih Akun di panel navigasi.
9. Pilih akun anggota yang perlu ditambahkan kembali ke organisasi.
10. Pilih Tindakan dan kemudian, pilih Tambah anggota.

## API/CLI

1. Gunakan akun administrator untuk berjalan [DisassociateMembers](#) API di akun anggota yang ingin mengaktifkan GuardDuty pemindaian malware yang dimulai.
2. Gunakan akun anggota Anda untuk memanggil [UpdateDetector](#) untuk mengaktifkan pemindaian GuardDuty malware yang dimulai.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Gunakan akun administrator untuk menjalankan [CreateMembers](#) API untuk menambahkan anggota kembali ke organisasi.

## Temuan yang memanggil pemindaian GuardDuty malware yang dimulai

Pemindaian malware GuardDuty yang dimulai akan dipanggil saat GuardDuty mendeteksi perilaku mencurigakan yang menunjukkan malware pada instans Amazon EC2 atau beban kerja kontainer.

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)

- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)(Hanya keluar)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)(Hanya keluar)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)(Hanya keluar)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)

- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

## Pemindaian malware sesuai permintaan

Pemindaian malware sesuai permintaan membantu Anda mendeteksi keberadaan malware di volume Amazon Elastic Block Store (AmazonEBS) yang dilampirkan ke EC2 instans Amazon Anda. Tanpa konfigurasi yang diperlukan, Anda dapat memulai pemindaian malware sesuai permintaan dengan memberikan Amazon Resource Name (ARN) dari EC2 instans Amazon yang ingin dipindai. Anda dapat memulai pemindaian malware sesuai permintaan baik melalui GuardDuty konsol atau API. Sebelum memulai pemindaian malware sesuai permintaan, Anda dapat mengatur pengaturan pilihan [Retensi snapshot](#) Anda. Skenario berikut dapat membantu Anda mengidentifikasi kapan harus menggunakan jenis pemindaian malware On-Demand dengan GuardDuty:

- Anda ingin mendeteksi keberadaan malware di EC2 instans Amazon Anda tanpa mengaktifkan pemindaian malware GuardDuty yang dimulai.
- Anda telah mengaktifkan GuardDuty pemindaian malware yang dimulai dan pemindaian dipanggil secara otomatis. Setelah mengikuti perbaikan yang disarankan untuk jenis Perlindungan Malware yang dihasilkan untuk EC2 menemukan, jika Anda ingin memulai pemindaian pada sumber daya yang sama, Anda dapat memulai pemindaian malware sesuai permintaan setelah 1 jam berlalu dari waktu mulai pemindaian sebelumnya.

Pemindaian malware sesuai permintaan tidak mengharuskan 24 jam berlalu sejak pemindaian malware sebelumnya dimulai. Seharusnya satu jam berlalu sebelum memulai pemindaian malware

On-Demand pada sumber daya yang sama. Untuk menghindari duplikasi pemindaian malware pada EC2 contoh yang sama, lihat [Memindai ulang instance Amazon EC2 yang sama](#).

#### Note

Pemindaian malware sesuai permintaan tidak termasuk dalam periode uji coba gratis 30 hari dengan. GuardDuty Biaya penggunaan berlaku untuk total EBS volume Amazon yang dipindai untuk setiap pemindaian malware. Untuk informasi selengkapnya, lihat [GuardDuty harga Amazon](#). Untuk informasi tentang biaya pembuatan snapshot EBS volume Amazon dan retensinya, lihat [EBS harga Amazon](#).

## Cara kerja pemindaian malware sesuai permintaan

Dengan pemindaian malware sesuai permintaan, Anda dapat memulai permintaan pemindaian malware untuk EC2 instans Amazon Anda bahkan saat sedang digunakan. Setelah Anda memulai pemindaian malware On-Demand, GuardDuty buat snapshot dari EBS volume Amazon yang dilampirkan ke instans Amazon EC2 yang Amazon Resource Name (ARN) disediakan untuk pemindaian. Selanjutnya, GuardDuty bagikan foto-foto ini dengan [GuardDuty akun layanan](#). GuardDuty membuat EBS volume replika terenkripsi dari snapshot tersebut di akun layanan. GuardDuty Untuk informasi selengkapnya tentang bagaimana EBS volume Amazon dipindai, lihat [Volume Penyimpanan Blok Elastis \(EBS\)](#).

#### Note

GuardDuty membuat snapshot dari data yang telah ditulis ke EBS volume Amazon pada point-in-time saat Anda memulai pemindaian malware On-Demand.

Jika malware ditemukan dan Anda telah mengaktifkan pengaturan retensi snapshot, snapshot EBS volume Anda secara otomatis disimpan di Anda. Akun AWS Pemindaian malware sesuai permintaan menghasilkan [Perlindungan Malware untuk jenis pencarian EC2](#). Jika malware tidak ditemukan, maka terlepas dari pengaturan retensi snapshot, snapshot EBS volume Anda akan dihapus.

Secara default, snapshot EBS volume Anda dibuat dengan GuardDutyScanId tag. Jangan hapus tag ini karena hal itu akan GuardDuty mencegah mengakses snapshot. Kedua jenis pemindaian dalam Perlindungan Malware untuk EC2 tidak memindai EC2 instans Amazon atau EBS volume

Amazon yang memiliki `GuardDutyExcluded` tag yang disetel ke `true`. Jika Perlindungan Malware untuk EC2 pemindaian pada sumber daya tersebut, ID pemindaian akan dihasilkan tetapi pemindaian akan dilewati dengan `EXCLUDED_BY_SCAN_SETTINGS` alasan. Untuk informasi selengkapnya, lihat [Alasan melewatkan sumber daya selama pemindaian malware](#).

## AWS Organizations kebijakan kontrol layanan - Akses ditolak

Menggunakan [kebijakan kontrol Layanan \(SCPs\)](#) di AWS Organizations, akun GuardDuty administrator yang didelegasikan dapat membatasi izin dan menolak tindakan seperti memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon yang dimiliki oleh akun Anda.

Sebagai akun GuardDuty anggota, saat Anda memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon Anda, Anda mungkin menerima kesalahan. Anda dapat terhubung dengan akun manajemen untuk memahami mengapa akun SCP anggota disiapkan. Untuk informasi selengkapnya, lihat [SCPefek pada izin](#).

## Memulai dengan pemindaian malware On-Demand

Sebagai akun GuardDuty administrator, Anda dapat memulai pemindaian malware sesuai permintaan atas nama akun anggota aktif Anda yang memiliki prasyarat berikut di akun mereka. Akun mandiri dan akun anggota aktif juga GuardDuty dapat memulai pemindaian malware sesuai permintaan untuk instance Amazon mereka sendiri. EC2

### Prasyarat

- GuardDuty harus diaktifkan di Wilayah AWS tempat Anda ingin memulai pemindaian malware sesuai permintaan.
- Pastikan bahwa [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) itu melekat pada IAM pengguna atau IAM peran. Anda akan memerlukan kunci akses dan kunci rahasia yang terkait dengan IAM pengguna atau IAM peran.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda memiliki opsi untuk memulai pemindaian malware sesuai permintaan atas nama akun anggota yang aktif.
- Jika Anda adalah akun anggota yang tidak memilikinya [izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#), maka memulai pemindaian malware sesuai permintaan untuk EC2 instance Amazon milik akun Anda, akan secara otomatis membuat untuk Perlindungan Malware SLR untuk. EC2

**⚠ Important**

Pastikan tidak ada yang menghapus [SLRizin untuk Perlindungan Malware EC2](#) ketika pemindaian malware, baik GuardDuty yang dimulai atau sesuai permintaan, masih berlangsung. Melakukannya akan mencegah pemindaian selesai dengan sukses dan memberikan hasil pemindaian yang pasti.

Sebelum Anda memulai pemindaian malware sesuai permintaan, pastikan tidak ada pemindaian yang dimulai pada sumber daya yang sama dalam 1 jam terakhir; jika tidak, itu akan di-de-ditipu. Untuk informasi selengkapnya, lihat [Memindai ulang sumber daya yang sama](#).

## Memulai pemindaian malware sesuai permintaan

Pilih metode akses pilihan Anda untuk memulai pemindaian malware sesuai permintaan.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Mulai pemindaian menggunakan salah satu opsi berikut:
  - a. Menggunakan Perlindungan Malware untuk EC2 halaman:
    - i. Di panel navigasi, di bawah Paket perlindungan, pilih Perlindungan Malware untuk EC2.
    - ii. Pada EC2 halaman Perlindungan Malware untuk, berikan EC2 contoh Amazon ARN <sup>1</sup> yang ingin Anda lakukan pemindaian.
  - b. Menggunakan halaman Pemindaian Malware:
    - i. Di panel navigasi, pilih Pemindaian Malware.
    - ii. Pilih Mulai pemindaian sesuai permintaan dan berikan EC2 instans Amazon ARN <sup>1</sup> yang ingin Anda lakukan pemindaian.
    - iii. Jika ini adalah pemindaian ulang, pilih ID EC2 instans Amazon di halaman Pemindaian Malware.

Perluas dropdown Mulai pemindaian sesuai permintaan dan pilih Pindai ulang instance yang dipilih.



3. Setelah Anda berhasil memulai pemindaian menggunakan salah satu metode, ID pemindaian akan dihasilkan. Anda dapat menggunakan ID pemindaian ini untuk melacak kemajuan pemindaian. Untuk informasi selengkapnya, lihat [Memantau status dan hasil pemindaian malware](#).

## API/CLI

Invoke [StartMalwareScan](#) yang menerima EC2 instans Amazon <sup>1</sup> yang ingin Anda lakukan pemindaian malware sesuai permintaan. `resourceArn`

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Setelah Anda berhasil memulai pemindaian, `StartMalwareScan` mengembalikan `scanId`. [DescribeMalwareScans](#) memanggil memantau kemajuan pemindaian yang dimulai.

<sup>1</sup> Untuk informasi tentang format EC2 instans Amazon Anda ARN, lihat [Nama Sumber Daya Amazon \(ARN\)](#). Untuk EC2 instans Amazon, Anda dapat menggunakan ARN format contoh berikut dengan mengganti nilai untuk partisi, Wilayah, Akun AWS ID, dan ID EC2 instans Amazon. Untuk informasi tentang panjang ID instans Anda, lihat [Sumber daya IDs](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

## Memindai ulang instance Amazon EC2 yang sama

Baik pemindaian GuardDuty dimulai atau sesuai permintaan, Anda dapat memulai pemindaian malware sesuai permintaan baru pada EC2 instance yang sama setelah 1 jam dari waktu mulai pemindaian malware sebelumnya. Jika pemindaian malware baru dimulai dalam waktu 1 jam sejak inisiasi pemindaian malware sebelumnya, permintaan Anda akan menghasilkan kesalahan berikut, dan tidak ada ID pemindaian yang akan dihasilkan untuk permintaan ini.

A scan was initiated on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.

Untuk informasi tentang cara memulai pemindaian baru pada sumber daya yang sama, lihat [Memulai pemindaian malware sesuai permintaan](#).

Untuk melacak status pemindaian malware, lihat [Memantau status pemindaian dan hasil dalam Perlindungan GuardDuty Malware untuk EC2](#).

# Memantau status pemindaian dan hasil dalam Perlindungan GuardDuty Malware untuk EC2

Anda dapat memantau status pemindaian setiap Perlindungan GuardDuty Malware untuk EC2 pemindaian. Nilai yang mungkin untuk Status pemindaian adalah `CompletedRunning`, `Skipped`, dan `Failed`.

Setelah pemindaian selesai, hasil Pemindaian diisi untuk pemindaian yang memiliki Status sebagai `Completed`. Nilai yang mungkin untuk hasil Scan adalah `Clean` dan `Infected`. Menggunakan jenis Pindai, Anda dapat mengidentifikasi apakah pemindaian malware itu GuardDuty `initiated` atau `on demand`.

Hasil pemindaian untuk setiap pemindaian malware memiliki periode retensi 90 hari. Pilih metode akses pilihan Anda untuk melacak status pemindaian malware Anda.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Pemindaian malware.
3. Anda dapat memfilter pemindaian malware dengan Properti berikut yang tersedia dalam kriteria filter.
  - Pindai ID
  - ID Akun
  - EC2contoh ARN
  - Jenis pemindaian
  - Status pemindaian

Untuk informasi tentang properti yang digunakan untuk kriteria filter, lihat [Detail temuan](#).

## API/CLI

- Setelah pemindaian malware memiliki hasil pemindaian, Anda dapat memfilter pemindaian malware berdasarkan `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, dan `SCAN_START_TIME`.

Kriteria GUARDDUTY\_FINDING\_ID filter SCAN\_TYPE tersedia saat GuardDuty dimulai. Untuk informasi tentang kriteria filter apa pun, lihat [Detail temuan](#).

- Anda dapat mengubah contoh *filter-criteria* dalam perintah di bawah ini. Saat ini, Anda dapat memfilter berdasarkan satu CriterionKey per satu. Pilihan untuk CriterionKey adalah EC2\_INSTANCE\_ARN, SCAN\_ID, ACCOUNT\_ID, SCAN\_TYPE, GUARDDUTY\_FINDING\_ID, SCAN\_STATUS, dan SCAN\_START\_TIME.

Jika Anda menggunakan yang sama CriterionKey seperti di bawah ini, pastikan untuk mengganti contoh EqualsValue dengan yang valid Anda sendiri AWS *scan-id*.

Ganti contoh detector-id dengan valid Anda sendiri *detector-id*. Anda dapat mengubah *max-results* (hingga 50) dan *sort-criteria*. AttributeName itu wajib dan harus scanStartTime.

```
aws guardduty describe-malware-scans --detector-id 60b8777933648562554d637e0e4bb3b2 --max-results 1 --sort-criteria '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "SCAN_ID", "FilterCondition": {"EqualsValue": "123456789012"}}] }'
```

- Respons dari perintah ini menampilkan maksimal satu hasil dengan rincian tentang sumber daya yang terpengaruh dan temuan malware (jikaInfected).

## GuardDuty akun layanan oleh Wilayah AWS

Saat snapshot dibuat dan dibagikan dengan akun GuardDuty layanan, acara baru akan dibuat di CloudTrail log Anda. Acara ini menentukan yang sesuai snapshotId dan userId (akun GuardDuty layanan untuk itu Wilayah AWS). Untuk informasi selengkapnya, lihat [Fitur dalam Perlindungan Malware untuk EC2](#).

Contoh berikut adalah cuplikan dari CloudTrail peristiwa yang menunjukkan badan permintaan untuk permintaan: ModifySnapshotAttribute

```
"requestParameters": {
  "snapshotId": "snap-1234567890abcdef0",
  "createVolumePermission": {
    "add": {
      "items": [
        {
```

```

        "userId": "111122223333"
      }
    ]
  },
  "attributeType": "CREATE_VOLUME_PERMISSION"
}

```

Tabel berikut menunjukkan akun GuardDuty layanan untuk setiap Wilayah. `userId` ini adalah akun GuardDuty layanan dan tergantung pada Wilayah yang dipilih.

| Wilayah AWS                 | Kode Wilayah   | GuardDuty ID akun layanan ( <b>userId</b> ) |
|-----------------------------|----------------|---|
| AS Timur (Virginia Utara)   | us-east-1      | 652050842985                                |
| AS Timur (Ohio)             | us-east-2      | 178123968615                                |
| AS Barat (California Utara) | us-west-1      | 669213148797                                |
| AS Barat (Oregon)           | us-west-2      | 447226417196                                |
| Asia Pasifik (Mumbai)       | ap-south-1     | 913179291432                                |
| Asia Pasifik (Osaka)        | ap-northeast-3 | 089661699081                                |
| Asia Pasifik (Seoul)        | ap-northeast-2 | 039163547507                                |
| Asia Pasifik (Tokyo)        | ap-northeast-1 | 874749492622                                |
| Asia Pasifik (Singapura)    | ap-southeast-1 | 247460962669                                |
| Asia Pasifik (Sydney)       | ap-southeast-2 | 124839743349                                |
| Kanada (Pusat)              | ca-central-1   | 175877067165                                |
| Kanada Barat (Calgary)      | ca-west-1      | 894794104037                                |
| Europa (Frankfurt)          | eu-central-1   | 002294850712                                |
| Europa (Irlandia)           | eu-west-1      | 283769539786                                |

| Wilayah AWS                              | Kode Wilayah   | GuardDuty ID akun layanan ( <b>userId</b> ) |
|--|----------------|---|
| Eropa (London)                           | eu-west-2      | 310125036783                                |
| Eropa (Paris)                            | eu-west-3      | 866607715269                                |
| Eropa (Stockholm)                        | eu-north-1     | 693780578038                                |
| Tiongkok (Beijing)                       | cn-north-1     | 448721096076                                |
| Tiongkok (Ningxia)                       | cn-northwest-1 | 480864352451                                |
| Amerika Selatan (Sao Paulo)              | sa-east-1      | 546914126324                                |
| Asia Pasifik (Hyderabad) (Keikutsertaan) | ap-south-2     | 682251015962                                |
| Asia Pasifik (Melbourne) (Keikutsertaan) | ap-southeast-4 | 353488359550                                |
| Eropa (Spanyol) (Opt-in)                 | eu-south-2     | 936182149045                                |
| Eropa (Zurich) (Opt-in)                  | eu-central-2   | 867642063380                                |
| Israel (Tel Aviv) (Keikutsertaan)        | il-central-1   | 619233833001                                |
| Eropa (Milan) (Opt-in)                   | eu-south-1     | 977238331021                                |
| Asia Pasifik (Hong Kong) (Keikutsertaan) | ap-east-1      | 249472122084                                |
| Timur Tengah (Bahrain) (Opt-in)          | me-south-1     | 404001805210                                |
| Afrika (Cape Town) (Keikutsertaan)       | af-south-1     | 957664736811                                |
| Asia Pasifik (Jakarta) (Keikutsertaan)   | ap-southeast-3 | 452118225523                                |

| Wilayah AWS                    | Kode Wilayah | GuardDuty ID akun layanan ( <b>userId</b> ) |
|--------------------------------|--------------|---|
| Timur Tengah (UAE)<br>(Opt-in) | me-central-1 | 828603743433                                |

## Perlindungan Malware untuk EC2 kuota

Perlindungan Malware untuk EC2 memiliki ketersediaan default berikut dari beragam sumber daya yang digunakan fitur tersebut.

| Cakupan  | Bawaan | Komentar   |
|--|--------|--|
| Ekstraksi dan analisis data dalam file terkompresi atau diarsipkan | 5      | Jumlah maksimum level bersarang yang diizinkan dalam file yang diarsipkan.   |
| Jumlah file dalam file yang diarsipkan                             | 1000   | Jumlah maksimum file yang dapat dipindai dalam arsip. Hitungan ini adalah jumlah dari jumlah file yang diekstrak dari arsip dan jumlah file yang diekstrak dari semua arsip bersarang.   |
| Jumlah Ancaman   | 32     | Jumlah maksimum ancaman yang dapat Anda lihat di panel temuan. GuardDuty Perlindungan Malware untuk EC2 mungkin telah mendeteksi lebih banyak nama ancaman. Jika jumlah nama ancaman yang terdeteksi lebih tinggi dari nilai default, Anda dapat melihat JSON detailnya dengan memilih ID Menemukan di |

| Cakupan                                 | Bawaan | Komentar   |
|---|--------|--|
|   |        | bawah nama temuan di panel detail GuardDuty konsol.  |
| Jumlah file per ancaman yang terdeteksi | 5      | Jumlah maksimum file yang diidentifikasi per ancaman yang terdeteksi. Misalnya, jika GuardDuty mendeteksi 10 file yang terkait dengan ancaman tunggal, ancaman akan menampilkan maksimal 5 file.   |
| EBSvolume per pemindaian per instance   | 11     | Jumlah maksimum EBS volume yang GuardDuty dapat memindai per EC2 instance. Jika ada lebih dari 11 EBS volume yang perlu dipindai, Perlindungan GuardDuty Malware untuk EC2 mengurutkan <code>deviceName</code> berdasarkan abjad, dan memilih 11 volume pertama. EBS |

| Cakupan                         | Bawaan   | Komentar  |
|---------------------------------|--|---|
| Ukuran volume EBS               | 2048 GB  | Terkait dengan EC2 instans Amazon dan beban kerja kontainer, Perlindungan GuardDuty Malware for EC2 dapat memindai setiap EBS volume Amazon yang berukuran hingga 2048 GB. Kuota ini berlaku untuk masing-masing Wilayah AWS tempat dukungan untuk Perlindungan Malware EC2 tersedia. |
| Jenis sistem file yang didukung | GuardDuty Perlindungan Malware untuk EC2 dapat memindai jenis sistem file berikut: <ul data-bbox="592 1050 1023 1606" style="list-style-type: none"><li>• Sistem File Teknologi Baru (NTFS)</li><li>• Sistem File X (XFS)</li><li>• Sistem File kedua diperpanjang (ext2)</li><li>• Sistem File diperpanjang keempat (ext4)</li><li>• Tabel Alokasi File (FAT) Sistem File</li><li>• Tabel Alokasi File Virtual (VFAT) Sistem File</li></ul> | N/A.  |



| Cakupan  | Bawaan | Komentar  |
|--|--------|---|
| Pindai tag opsi  | 50     | Jumlah maksimum tag sumber daya yang dapat Anda tambahkan untuk menyesuaikan pengaturan opsi pemindaian malware Anda. Untuk informasi selengkapnya, lihat <a href="#">Opsii pindai dengan tag yang ditentukan pengguna</a> .  |
| Menemukan periode retensi                                    | 90     | Jumlah hari maksimum yang GuardDuty mempertahankan temuan. Untuk informasi terbaru, lihat <a href="#">GuardDuty Kuota Amazon</a> .  |
| Periode retensi pemindaian malware                           | 90     | Jumlah hari maksimum Perlindungan GuardDuty Malware untuk EC2 mempertahankan riwayat pemindaian. Untuk informasi selengkapnya tentang melihat pemindaian malware terbaru, lihat <a href="#">Memantau status pemindaian dan hasil dalam Perlindungan GuardDuty Malware untuk EC2</a> . |
| Transaksi per detik (TPS) untuk pemindaian malware On-Demand | 1      | Jumlah permintaan pemindaian malware On-Demand yang dapat dimulai per detik di setiap Wilayah.  |

| Cakupan  | Bawaan | Komentar   |
|--|--------|--|
| Batas burst untuk pemindaian malware On-Demand | 1      | Jumlah permintaan pemindaian malware On-Demand bersamaan yang dapat dimulai per detik di setiap Wilayah. |

# GuardDuty Perlindungan Malware untuk S3

Perlindungan Malware untuk S3 membantu Anda mendeteksi potensi keberadaan malware dengan memindai objek yang baru diunggah ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda. Ketika objek S3 atau versi baru dari objek S3 yang ada diunggah ke bucket yang Anda pilih, GuardDuty secara otomatis memulai pemindaian malware.

## [Perlindungan Malware untuk S3 - Ikhtisar dan Demo](#)

Dua pendekatan untuk mengaktifkan Perlindungan Malware untuk S3

Anda dapat mengaktifkan Perlindungan Malware untuk S3 ketika Anda Akun AWS mengaktifkan GuardDuty layanan dan Anda menggunakan Perlindungan Malware untuk S3 sebagai bagian dari keseluruhan GuardDuty pengalaman, atau ketika Anda ingin menggunakan fitur Perlindungan Malware untuk S3 dengan sendirinya tanpa mengaktifkan layanan. GuardDuty Saat Anda mengaktifkan Perlindungan Malware untuk S3 dengan sendirinya, GuardDuty dokumentasi merujuknya sebagai menggunakan Perlindungan Malware untuk S3 sebagai fitur independen.

Pertimbangan untuk menggunakan Perlindungan Malware untuk S3 secara independen

- GuardDuty temuan keamanan — Detector ID adalah pengenalan unik yang dikaitkan dengan akun Anda di Wilayah. Ketika Anda mengaktifkan GuardDuty di satu atau beberapa Wilayah dalam akun, ID detektor akan dibuat secara otomatis untuk akun ini di setiap Wilayah tempat Anda mengaktifkan GuardDuty. Untuk informasi selengkapnya, lihat Detektor dalam [Konsep dan terminologi](#) dokumen.

Saat Anda mengaktifkan Perlindungan Malware untuk S3 secara independen di akun, akun tersebut tidak akan memiliki ID detektor terkait. Ini memengaruhi GuardDuty fitur apa yang mungkin tersedia untuk Anda. Misalnya, ketika pemindaian malware S3 mendeteksi keberadaan malware, tidak ada GuardDuty temuan yang akan dihasilkan di Anda Akun AWS karena semua GuardDuty temuan terkait dengan ID detektor.

- Memeriksa apakah objek yang dipindai berbahaya — Secara default, GuardDuty mempublikasikan hasil pemindaian malware ke bus EventBridge acara Amazon default Anda dan namespace Amazon CloudWatch . Saat Anda mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket, objek S3 yang dipindai mendapatkan tag yang menyebutkan hasil pemindaian. Untuk informasi lebih lanjut tentang penandaan, lihat [Penandaan opsional objek berdasarkan hasil pemindaian](#).

## Pertimbangan umum untuk mengaktifkan Perlindungan Malware untuk S3

Pertimbangan umum berikut berlaku apakah Anda menggunakan Perlindungan Malware untuk S3 secara independen atau sebagai bagian dari GuardDuty pengalaman:

- Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik akun Anda sendiri. Sebagai akun GuardDuty administrator yang didelegasikan, Anda tidak dapat mengaktifkan fitur ini di bucket Amazon S3 milik akun anggota.
- Anda dapat mengaktifkan fitur ini di bucket S3 milik Wilayah yang sama yang saat ini dipilih di GuardDuty konsol. GuardDuty tidak mendukung mengaktifkan fitur ini di bucket S3 lintas wilayah.
- Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima EventBridge notifikasi Amazon setiap kali ada perubahan pada bucket S3 yang dikonfigurasi oleh salah satu akun anggota organisasi Anda untuk fitur ini. [Status sumber daya paket Perlindungan Malware](#)

## Konten

- [Harga untuk Perlindungan Malware untuk S3](#)
- [Bagaimana cara kerja Perlindungan Malware untuk S3?](#)
- [Kemampuan Perlindungan Malware untuk S3](#)
- [\(Opsional\) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen \(hanya konsol\)](#)
- [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#)
- [Status sumber daya paket Perlindungan Malware](#)
- [Memecahkan masalah rincian status paket Perlindungan Malware](#)
- [Pemantauan dalam Perlindungan Malware untuk S3](#)
- [Menggunakan kontrol akses berbasis tag \(TBAC\) dengan Perlindungan Malware untuk S3](#)
- [Mengedit Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#)
- [Melihat penggunaan dan biaya untuk Perlindungan Malware untuk S3](#)
- [Nonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#)
- [Dukungan fitur Amazon S3](#)
- [Kuota dalam Perlindungan Malware untuk S3](#)

# Harga untuk Perlindungan Malware untuk S3

## Paket Tingkat Gratis (biaya pemindaian)

Masing-masing Akun AWS mendapat Tingkat Gratis 12 bulan yang mencakup penggunaan hingga batas tertentu per bulan untuk setiap Wilayah. Jika penggunaan Anda melampaui batas yang ditentukan, Anda akan mulai mengeluarkan biaya penggunaan untuk batas yang terlampaui. Untuk informasi tentang batas yang ditentukan dan contoh harga, lihat [harga paket GuardDuty perlindungan](#).

- Semua yang Akun AWS ada memenuhi syarat untuk menggunakan Tingkat Gratis 12 bulan untuk fitur ini yang dimulai dari 11 Juni 2024 dan berakhir pada 11 Juni 2025. Tingkat Gratis 12 bulan yang diperpanjang ini untuk akun Anda berlaku untuk menggunakan Perlindungan Malware untuk S3, dan tidak ada fitur lain AWS layanan GuardDuty atau lainnya.

Jika yang sudah ada Akun AWS mulai menggunakan Perlindungan Malware untuk S3 setelah 11 Juni 2025 atau setelah Tingkat Gratis 12 bulan akun berakhir, maka Anda akan mulai mengeluarkan biaya penggunaan terkait.

- Jika Anda memiliki Tingkat Gratis baru Akun AWS dan 12 bulan Anda dimulai setelah ketersediaan umum (11 Juni 2024) Perlindungan Malware untuk S3, maka periode Tingkat Gratis 12 bulan Anda untuk fitur ini akan sama dengan periode Tingkat Gratis 12 bulan untuk akun Anda.

Untuk informasi tentang biaya penggunaan setelah mengaktifkan Perlindungan Malware untuk S3, lihat [Melihat penggunaan dan biaya untuk Perlindungan Malware untuk S3](#)

## Biaya penggunaan Penandaan Objek S3

Saat Anda mengaktifkan Perlindungan Malware untuk S3, itu opsional untuk mengaktifkan penandaan untuk objek S3 yang dipindai. Ketika Anda memilih untuk mengaktifkan S3 Object Tagging, ada biaya penggunaan terkait. Untuk informasi selengkapnya tentang biaya, lihat [tab Manajemen & wawasan](#) di halaman harga Amazon S3.

Biaya penggunaan Penandaan Objek S3 tidak termasuk dalam paket Tingkat Gratis.

## Amazon S3 APIs - GET dan biaya penggunaan PUT

Anda akan dikenakan biaya penggunaan saat GuardDuty menjalankan Amazon APIs S3 berdasarkan IAM peran. Misalnya, setelah mengasumsikan IAM peran, GuardDuty jalankan PutObject API to add the test object ke bucket yang Anda pilih. Ini membantu GuardDuty menilai status fitur yang diaktifkan.

Untuk informasi tentang harga API panggilan S3 di Anda Wilayah AWS, lihat [Permintaan & pengambilan data di bawah tab Penyimpanan & permintaan](#) di halaman harga Amazon S3.

## Bagaimana cara kerja Perlindungan Malware untuk S3?

Bagian ini menjelaskan komponen Perlindungan Malware untuk S3 dan cara kerjanya setelah Anda mengaktifkannya untuk bucket S3.

### Gambaran Umum

Anda dapat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik Anda sendiri. Akun AWS GuardDuty memberi Anda fleksibilitas untuk mengaktifkan fitur ini untuk seluruh bucket Anda, atau membatasi cakupan pemindaian malware ke [awalan objek](#) tertentu tempat GuardDuty memindai setiap objek yang diunggah yang dimulai dengan salah satu awalan yang dipilih. Anda dapat menambahkan hingga 5 awalan. Saat Anda mengaktifkan fitur untuk bucket S3, bucket tersebut disebut bucket yang dilindungi.

### IAM izin peran

Perlindungan Malware untuk S3 menggunakan IAM peran yang memungkinkan GuardDuty untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini termasuk diberi tahu tentang objek yang baru diunggah di bucket yang dipilih, memindai objek tersebut, dan secara opsional menambahkan tag ke objek yang dipindai. Ini adalah prasyarat untuk mengonfigurasi bucket S3 Anda dengan fitur ini.

Anda memiliki opsi untuk memperbarui IAM peran yang ada, atau membuat peran baru untuk tujuan ini. Saat mengaktifkan Perlindungan Malware untuk S3 untuk lebih dari satu bucket, Anda dapat memperbarui IAM peran yang ada untuk menyertakan nama bucket lainnya, sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).

### Penandaan opsional objek berdasarkan hasil pemindaian

Pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, ada langkah opsional untuk mengaktifkan penandaan objek S3 yang dipindai. IAM Peran tersebut sudah menyertakan izin untuk menambahkan tag ke objek Anda setelah pemindaian. Namun, GuardDuty akan menambahkan tag hanya ketika Anda mengaktifkan opsi ini pada saat setup.

Anda harus mengaktifkan opsi ini sebelum objek diunggah. Setelah pemindaian berakhir, GuardDuty menambahkan tag yang telah ditentukan ke objek S3 yang dipindai dengan pasangan key:value berikut:

GuardDutyMalwareScanStatus:*Potential scan result*

Nilai tag hasil pemindaian potensial

meliputi `NO_THREATS_FOUND`, `THREATS_FOUND`, `UNSUPPORTED`, `ACCESS_DENIED`, dan `FAILED`.

Untuk informasi selengkapnya tentang nilai-nilai ini, lihat [S3 object potential scan result values](#).

Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian objek S3. Anda dapat menggunakan tag ini lebih lanjut untuk menambahkan kebijakan sumber daya S3 kontrol akses berbasis tag (TBAC) sehingga Anda dapat mengambil tindakan pada objek yang berpotensi berbahaya. Untuk informasi selengkapnya, lihat [TBAC Menambahkan sumber daya bucket S3](#).

Kami menyarankan Anda untuk mengaktifkan penandaan pada saat mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda. Jika Anda mengaktifkan penandaan setelah objek diunggah dan berpotensi pemindaian dimulai, tidak GuardDuty akan dapat menambahkan tag ke objek yang dipindai. Untuk informasi tentang biaya Penandaan Objek S3 terkait, lihat [Harga untuk Perlindungan Malware untuk S3](#)

## Proses setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember

Setelah Anda mengaktifkan Perlindungan Malware untuk S3, sumber daya paket Perlindungan Malware akan dibuat secara eksklusif untuk bucket S3 yang dipilih. Sumber daya ini dikaitkan dengan ID paket Perlindungan Malware, pengenal unik untuk sumber daya Anda yang dilindungi. Dengan menggunakan salah satu IAM izin, GuardDuty kemudian membuat dan mengelola aturan EventBridge terkelola dengan nama. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

## Bagaimana GuardDuty menangani data Anda - pagar pembatas untuk perlindungan data

Perlindungan Malware untuk S3 mendengarkan notifikasi Amazon EventBridge . Saat objek diunggah ke bucket yang dipilih atau salah satu awalan, GuardDuty unduh objek tersebut dari bucket S3 dengan menggunakan lalu membaca, mendekripsi, [AWS PrivateLink](#) dan memindainya di lingkungan terisolasi di Wilayah yang sama. Lingkungan pemindaian berjalan di cloud pribadi virtual yang terkunci (VPC) tanpa akses internet. VPC ini dilampirkan ke grup aturan DNS Firewall yang memungkinkan komunikasi hanya ke domain allowlisted yang dimiliki. AWS Selama pemindaian, simpan GuardDuty sementara objek S3 yang diunduh dalam lingkungan pemindaian yang dienkripsi dengan kunci [AWS Key Management Service \(AWS KMS\)](#).

Untuk informasi tentang metodologi deteksi GuardDuty malware dan mesin pemindaian yang digunakannya, lihat [GuardDuty mesin pemindai deteksi malware](#).

Setelah pemindaian malware selesai, GuardDuty proses metadata pemindaian dengan status pemindaian dan kemudian menghapus salinan objek yang diunduh.

GuardDuty membersihkan lingkungan pemindaian setiap kali sebelum pemindaian baru dimulai. GuardDuty menggunakan otorisasi kontingen untuk akses operator ke lingkungan pemindaian, dan setiap permintaan akses ditinjau, disetujui, dan diaudit.

## Meninjau hasil pemindaian objek S3

GuardDuty menerbitkan peristiwa hasil pemindaian objek S3 ke bus acara EventBridge default Amazon. GuardDuty juga mengirimkan metrik pemindaian seperti jumlah objek yang dipindai dan byte yang dipindai ke Amazon CloudWatch. Jika Anda mengaktifkan penandaan, maka GuardDuty akan menambahkan tag yang telah ditentukan GuardDutyMalwareScanStatus dan hasil pemindaian potensial sebagai nilai tag.

Untuk informasi selengkapnya, lihat [Pemantauan dalam Perlindungan Malware untuk S3](#).

## Meninjau temuan yang dihasilkan

Meninjau temuan tergantung pada apakah Anda menggunakan Perlindungan Malware untuk S3 dengan atau tidak. GuardDuty Pertimbangkan skenario berikut:

Menggunakan Perlindungan Malware untuk S3 ketika Anda mengaktifkan GuardDuty layanan (ID detektor)

Jika pemindaian malware mendeteksi file yang berpotensi berbahaya di objek S3, GuardDuty akan menghasilkan temuan terkait. Anda dapat melihat detail temuan dan menggunakan langkah-langkah yang disarankan untuk berpotensi memulihkan temuan tersebut. Berdasarkan [frekuensi temuan Ekspor](#) Anda, temuan yang dihasilkan akan diekspor ke bucket S3 dan bus EventBridge acara.

Menggunakan Perlindungan Malware untuk S3 sebagai fitur independen (tidak ada ID detektor)

GuardDuty tidak akan dapat menghasilkan temuan karena tidak ada ID detektor terkait. Untuk mengetahui status pemindaian malware objek S3, Anda dapat melihat hasil pemindaian yang GuardDuty secara otomatis dipublikasikan ke bus acara default Anda. Anda juga dapat melihat CloudWatch metrik untuk menilai jumlah objek dan byte yang GuardDuty mencoba memindai. Anda dapat mengatur CloudWatch alarm untuk mendapatkan pemberitahuan tentang hasil



pemindaian. Jika Anda telah mengaktifkan S3 Object Tagging, Anda juga dapat melihat status pemindaian malware dengan memeriksa objek S3 untuk kunci `GuardDutyMalwareScanStatus` tag dan nilai tag hasil pemindaian.

## Kemampuan Perlindungan Malware untuk S3

Daftar berikut memberikan ikhtisar tentang apa yang dapat Anda harapkan atau lakukan setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda:

- Pilih apa yang akan dipindai — Pindai file saat diunggah ke semua atau awalan tertentu (hingga 5) yang terkait dengan bucket S3 pilihan Anda.
- Pemindaian otomatis pada objek yang diunggah — Setelah Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember, secara otomatis GuardDuty akan memulai pemindaian untuk mendeteksi potensi malware di objek yang baru diunggah.
- Aktifkan melalui konsol, dengan menggunakan API/AWS CLI, atau AWS CloudFormation — Pilih metode yang disukai untuk mengaktifkan Perlindungan Malware untuk S3.

Anda dapat mengaktifkan Perlindungan Malware untuk S3 dengan menggunakan platform Infrastructure as code (IaC) seperti Terraform. Untuk informasi lebih lanjut, lihat [Sumber Daya: `aws\_guarddduty\_malware\_protection\_plan`](#).

- Format file yang didukung, Perlindungan Malware untuk kuota S3, dan fitur Amazon S3 - Perlindungan Malware untuk S3 mendukung semua format file yang dapat Anda unggah ke bucket S3. Jika file yang diunggah dilindungi kata sandi, maka GuardDuty akan melewatkan pemindaian file. Untuk informasi tentang kuota yang terkait dengan ukuran objek, tingkat kedalaman arsip maksimum, dan detail lainnya, lihat [Kuota dalam Perlindungan Malware untuk S3](#).

Untuk informasi tentang apakah fitur Amazon S3 didukung atau tidak, lihat [Dukungan fitur Amazon S3](#)

- Mendukung penandaan objek S3 yang dipindai - Ketika Anda mengaktifkan [Penandaan opsional objek berdasarkan hasil pemindaian](#), maka setelah setiap pemindaian malware, GuardDuty akan menambahkan tag yang menunjukkan status pemindaian. Anda dapat menggunakan tag ini untuk mengatur kontrol akses berbasis tag (TBAC) untuk objek S3. Misalnya, Anda dapat membatasi akses ke objek S3 yang diindikasikan sebagai berbahaya dan memiliki nilai tag sebagai `THREATS_FOUND`
- EventBridge Pemberitahuan Amazon — GuardDuty mengirimkan peristiwa ke Amazon EventBridge saat status sumber daya paket Perlindungan Malware berubah, atau pemindaian

malware objek S3 selesai. Peristiwa ini dikirim ke bus acara default. Anda dapat menggunakan EventBridge dan peristiwa ini untuk menulis aturan yang mengambil tindakan, seperti memantau kapan peristiwa ini terjadi. Untuk informasi selengkapnya, lihat [Pemantauan EventBridge dengan Amazon](#).

- CloudWatch metrik — Lihat CloudWatch metrik untuk mengaktifkan alarm pada status pemindaian malware tertentu. Untuk informasi selengkapnya, lihat [Memantau metrik status pemindaian dengan menggunakan Amazon CloudWatch](#).

## (Opsional) Memulai Perlindungan GuardDuty Malware untuk S3 secara independen (hanya konsol)

Gunakan langkah opsional ini ketika Anda ingin memulai dengan Perlindungan Malware untuk opsi deteksi ancaman S3 terlepas dari GuardDuty status di Akun AWS. Jika Anda telah mengaktifkan GuardDuty di akun Anda, maka Anda dapat melewati langkah ini dan melanjutkan dengan [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#).

Langkah-langkah untuk memulai dengan Perlindungan Malware untuk deteksi ancaman S3 saja

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pilih Perlindungan GuardDuty Malware hanya untuk S3. Ini membantu Anda mendeteksi apakah file yang baru diunggah di bucket Amazon Simple Storage Service (Amazon S3) berpotensi mengandung malware.

# Try threat detection with GuardDuty

Amazon GuardDuty - all features

Experience threat detection capabilities in your AWS environment.

**GuardDuty Malware Protection for S3 only**

Detect malicious file upload to your Amazon S3 buckets. You don't need to enable Amazon GuardDuty.

**Get started**

3. Pilih Mulai. Anda sekarang dapat melanjutkan dengan langkah-langkah di bawah [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#).

## Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda

Bagian ini mencakup langkah-langkah untuk menambahkan prasyarat dan mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 milik akun Anda sendiri. Langkah-langkah di bagian berikut tetap sama apakah Anda memulai dengan Perlindungan Malware untuk S3 secara independen atau mengaktifkannya sebagai bagian dari GuardDuty layanan.

Gunakan langkah-langkah berikut setiap kali Anda ingin menambahkan deteksi ancaman ini ke bucket S3.

1. [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#)
2. [Aktifkan Perlindungan Malware untuk S3 untuk bucket Anda](#)

## Prasyarat - Membuat atau memperbarui kebijakan peran IAM

Agar Perlindungan Malware untuk S3 dapat memindai dan (opsional) menambahkan tag ke objek S3 Anda, Anda harus membuat dan melampirkan IAM peran yang mencakup izin yang diperlukan berikut untuk:

- Izinkan EventBridge tindakan Amazon membuat dan mengelola aturan EventBridge terkelola sehingga Perlindungan Malware untuk S3 dapat mendengarkan pemberitahuan objek S3 Anda.

Untuk informasi selengkapnya, lihat [Aturan EventBridge terkelola Amazon](#) di Panduan EventBridge Pengguna Amazon.

- Izinkan Amazon S3 dan EventBridge tindakan mengirim pemberitahuan ke semua peristiwa di bucket EventBridge ini

Untuk informasi selengkapnya, lihat [Mengaktifkan Amazon EventBridge](#) di Panduan Pengguna Amazon S3.

- Izinkan tindakan Amazon S3 mengakses objek S3 yang diunggah dan menambahkan tag yang telah ditentukanGuardDutyMalwareScanStatus, ke objek S3 yang dipindai. Saat menggunakan awalan objek, tambahkan `s3:prefix` kondisi pada awalan yang ditargetkan saja. Ini GuardDuty mencegah mengakses semua objek S3 di bucket Anda.
- Izinkan tindakan KMS utama untuk mengakses objek sebelum memindai dan meletakkan objek uji pada ember dengan KMS enkripsi DSSE - KMS dan SSE - yang didukung.

### Note

Langkah ini diperlukan setiap kali Anda mengaktifkan Perlindungan Malware untuk S3 untuk ember di akun Anda. Jika sudah memiliki IAM peran yang ada, Anda dapat memperbarui kebijakannya untuk menyertakan detail sumber daya bucket S3 lainnya. [Menambahkan izin IAM kebijakan](#) Topik ini memberikan contoh tentang cara melakukan ini.

Gunakan kebijakan berikut untuk membuat atau memperbarui IAM peran.

Kebijakan

- [Menambahkan izin IAM kebijakan](#)
- [Menambahkan kebijakan hubungan Trust](#)

## Menambahkan izin IAM kebijakan

Anda dapat memilih untuk memperbarui kebijakan sebaris IAM peran yang ada, atau membuat IAM peran baru. Untuk selengkapnya tentang langkah-langkahnya, lihat [Membuat IAM peran](#) atau [Memodifikasi kebijakan izin peran](#) di IAMPanduan Pengguna.

Tambahkan templat izin berikut ke IAM peran pilihan Anda. Ganti nilai placeholder berikut dengan nilai yang sesuai yang terkait dengan akun Anda:

- Untuk *amzn-s3-demo-bucket*, ganti dengan nama bucket Amazon S3 Anda.

Untuk menggunakan IAM peran yang sama untuk lebih dari satu sumber daya bucket S3, perbarui kebijakan yang ada seperti yang ditampilkan dalam contoh berikut:

```
...
...
"Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"
],
...
...
```

Pastikan untuk menambahkan koma (,) sebelum menambahkan yang baru ARN terkait dengan bucket S3. Lakukan ini di mana pun Anda merujuk ke bucket S3 Resource di template kebijakan.

- Untuk *111122223333*, ganti dengan Akun AWS ID Anda.
- Untuk *us-east-1*, ganti dengan Anda Wilayah AWS.
- Untuk *APKAEIBAERJR2EXAMPLE*, ganti dengan ID kunci yang dikelola pelanggan Anda. Jika bucket Anda dienkrpsi menggunakan AWS KMS key, ganti nilai placeholder dengan\*, seperti yang ditunjukkan pada contoh berikut:

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

## IAM Templat Kebijakan Peran

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
    "Effect": "Allow",
    "Action": [
      "events:PutRule",
      "events>DeleteRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
      "StringLike": {
        "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
    "Effect": "Allow",
    "Action": [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ]
  },
  {
    "Sid": "AllowPostScanTag",
    "Effect": "Allow",
    "Action": [
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:PutObjectVersionTagging",
      "s3:GetObjectVersionTagging"
    ]
  }
}

```

```

    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "AllowEnableS3EventBridgeEvents",
    "Effect": "Allow",
    "Action": [
      "s3:PutBucketNotification",
      "s3:GetBucketNotification"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "AllowPutValidationObject",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
    ]
  },
  {
    "Sid": "AllowCheckBucketOwnership",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "AllowMalwareScan",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
  },

```

```

    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "AllowDecryptForMalwareScan",
    "Effect": "Allow",
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com"
      }
    }
  }
]
}

```

## Menambahkan kebijakan hubungan Trust

Lampirkan kebijakan kepercayaan berikut ke IAM peran Anda. Untuk selengkapnya tentang langkah-langkah, lihat [Memodifikasi kebijakan kepercayaan peran](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```



## Aktifkan Perlindungan Malware untuk S3 untuk bucket Anda

Bagian ini memberikan langkah-langkah terperinci tentang cara mengaktifkan Perlindungan Malware untuk S3 untuk bucket yang dipilih di akun Anda sendiri.

Langkah-langkah untuk mengaktifkan Perlindungan Malware untuk S3 untuk ember

- [Masukkan detail bucket S3](#)
- [Aktifkan penandaan untuk objek yang dipindai](#)
- [Izin](#)
- [\(Opsional\) Tandai ID paket Perlindungan Malware](#)

### Masukkan detail bucket S3

Gunakan langkah-langkah berikut untuk memberikan detail bucket Amazon S3:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan Perlindungan Malware untuk S3.
3. Di panel navigasi, pilih Perlindungan Malware untuk S3.
4. Di bagian Protected Bucket, pilih Aktifkan untuk mengaktifkan Perlindungan Malware untuk S3 untuk bucket S3 milik Anda. Akun AWS
5. Di bawah Masukkan detail bucket S3, masukkan nama bucket Amazon S3. Atau, pilih Browse S3 untuk memilih bucket S3.

Bucket S3 dan Akun AWS tempat Anda mengaktifkan Perlindungan Malware untuk S3 harus sama. Wilayah AWS Misalnya, jika akun Anda milik us-east-1 Wilayah, maka Wilayah bucket Amazon S3 Anda juga harus us-east-1

6. Di bawah Awalan, Anda dapat memilih All the objects in the S3 bucket atau Objects yang dimulai dengan awalan tertentu.
  - Pilih Semua objek di bucket S3 bila Anda mau GuardDuty dapat memindai semua objek yang baru diunggah di bucket yang dipilih.
  - Pilih Objek yang dimulai dengan awalan tertentu saat Anda ingin memindai objek yang baru diunggah milik awalan tertentu. Opsi ini membantu Anda memfokuskan ruang lingkup pemindaian malware pada awalan objek yang dipilih saja. Untuk informasi selengkapnya

tentang penggunaan awalan, lihat [Mengatur objek di konsol Amazon S3 menggunakan folder](#) di Panduan Pengguna Amazon S3.

Pilih Tambahkan awalan dan masukkan awalan. Anda dapat menambahkan hingga lima awalan.

## Aktifkan penandaan untuk objek yang dipindai

Ini adalah langkah opsional. Saat Anda mengaktifkan opsi penandaan sebelum objek diunggah ke bucket Anda, maka setelah menyelesaikan pemindaian, GuardDuty akan menambahkan tag yang telah ditentukan dengan kunci sebagai `GuardDutyMalwareScanStatus` dan nilai sebagai hasil pemindaian. Untuk menggunakan Perlindungan Malware untuk S3 secara optimal, kami sarankan untuk mengaktifkan opsi untuk menambahkan tag ke objek S3 setelah pemindaian berakhir. Biaya Penandaan Objek S3 standar berlaku. Untuk informasi selengkapnya, lihat [Harga untuk Perlindungan Malware untuk S3](#).

Mengapa Anda harus mengaktifkan penandaan?

- Mengaktifkan penandaan adalah salah satu cara untuk mengetahui tentang hasil pemindaian malware. Untuk informasi tentang hasil pemindaian malware S3, lihat [Pemantauan dalam Perlindungan Malware untuk S3](#).
- Siapkan kebijakan kontrol akses (TBAC) berbasis tag pada bucket S3 Anda yang berisi objek yang berpotensi berbahaya. Untuk informasi tentang pertimbangan dan cara menerapkan kontrol akses berbasis tag (TBAC), lihat [Menggunakan kontrol akses berbasis tag \(TBAC\) dengan Perlindungan Malware untuk S3](#)

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat [Mengkategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.

Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Pemantauan EventBridge dengan Amazon](#).

- Jika IAM peran yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, bahkan dengan penandaan diaktifkan untuk bucket Anda yang dilindungi, tidak GuardDuty akan dapat

menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi selengkapnya tentang izin IAM peran yang diperlukan untuk penandaan, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).

GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Pemantauan EventBridge dengan Amazon](#).

Untuk memilih opsi di bawah Tag objek yang dipindai

- Saat Anda ingin GuardDuty menambahkan tag ke objek S3 yang dipindai, pilih objek Tag.
- Bila Anda tidak ingin menambahkan tag GuardDuty ke objek S3 yang dipindai, pilih Jangan beri tag objek.

## Izin

Gunakan langkah-langkah berikut untuk memilih IAM peran yang memiliki izin yang diperlukan untuk melakukan tindakan pemindaian malware atas nama Anda. Tindakan ini mungkin termasuk memindai objek S3 yang baru diunggah dan (opsional) menambahkan tag ke objek tersebut.

Untuk memilih nama IAM peran

1. Jika Anda telah melakukan langkah-langkah di bawah ini [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#), maka lakukan hal berikut:
  - Di bagian Izin, untuk nama IAM peran, pilih nama IAM peran yang menyertakan izin yang diperlukan.
2. Jika Anda belum melakukan langkah-langkah di bawah ini [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#), maka lakukan hal berikut:
  - a. Pilih Lihat izin.
  - b. Di bawah Detail izin, pilih tab Kebijakan. Ini menunjukkan template IAM izin yang diperlukan.  
  
Salin templat ini dan kemudian pilih Tutup di akhir jendela Detail izin.
  - c. Pilih Lampirkan kebijakan yang membuka IAM konsol di tab baru. Anda dapat memilih untuk membuat IAM peran baru atau memperbarui IAM peran yang ada dengan izin dari templat yang disalin.

Template ini menyertakan nilai placeholder yang harus Anda ganti dengan nilai yang sesuai yang terkait dengan bucket dan Akun AWS

- d. Kembali ke tab browser dengan GuardDuty konsol. Pilih Lihat izin lagi.
- e. Di bawah Detail izin, pilih tab Hubungan kepercayaan. Ini menunjukkan templat kebijakan hubungan kepercayaan untuk IAM peran Anda.

Salin templat ini dan kemudian pilih Tutup di akhir jendela Detail izin.

- f. Buka tab browser yang IAM konsol terbuka. Untuk IAM peran pilihan Anda, tambahkan kebijakan hubungan kepercayaan ini.
3. Untuk menambahkan tag ke ID paket Perlindungan Malware yang dibuat untuk sumber daya yang dilindungi ini, lanjutkan ke bagian berikutnya; jika tidak, pilih Aktifkan di akhir halaman ini untuk menambahkan bucket S3 sebagai sumber daya yang dilindungi.

### (Opsional) Tandai ID paket Perlindungan Malware

Ini adalah langkah opsional yang membantu Anda menambahkan tag ke sumber daya paket Perlindungan Malware yang akan dibuat untuk sumber daya bucket S3 Anda.

Setiap tag memiliki dua bagian: Kunci tag dan nilai tag opsional. Untuk informasi selengkapnya tentang penandaan dan manfaatnya, lihat [Menandai sumber daya AWS](#).

Untuk menambahkan tag ke sumber daya paket Perlindungan Malware

1. Masukkan Kunci dan Nilai opsional untuk tag. Baik kunci tag dan nilai tag peka huruf besar/kecil. Untuk informasi tentang nama kunci tag dan nilai tag, lihat [Batas dan persyaratan penamaan tag](#).
2. Untuk menambahkan lebih banyak tag ke sumber daya paket Perlindungan Malware Anda, pilih Tambahkan tag baru dan ulangi langkah sebelumnya. Anda dapat menambahkan hingga 50 tanda ke setiap sumber daya .
3. Pilih Aktifkan.

### Langkah-langkah setelah mengaktifkan Perlindungan Malware untuk S3

Setelah mengaktifkan Perlindungan Malware untuk S3 untuk bucket (atau awalan objek tertentu), lakukan langkah-langkah berikut dalam urutan yang tercantum:

1. Tambahkan kebijakan sumber daya kontrol akses (TBAC) berbasis tag — Saat Anda mengaktifkan penandaan, sebelum objek diunggah ke bucket yang dipilih, pastikan untuk menambahkan TBAC kebijakan ke sumber daya bucket S3 Anda. Untuk informasi selengkapnya, lihat [TBACMenambahkan sumber daya bucket S3](#).
2. Pantau status paket Perlindungan Malware — Pantau kolom Status untuk setiap bucket yang dilindungi. Untuk informasi tentang status potensial dan apa artinya, lihat [Status sumber daya paket Perlindungan Malware](#).
3. Unggah objek:
  1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
  2. Unggah file ke bucket S3 atau awalan objek yang Anda aktifkan fitur ini. Untuk langkah-langkah mengunggah file, lihat [Mengunggah objek ke bucket Anda](#) di Panduan Pengguna Amazon S3.
4. Memantau status pemindaian objek S3 — Langkah ini mencakup informasi tentang cara memeriksa status pemindaian malware objek S3.

| Diaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3  | Perlindungan Malware yang Diaktifkan hanya untuk S3   |
|--|---|
| <ul style="list-style-type: none"> <li>• Ketika GuardDuty diaktifkan, itu dapat menghasilkan <a href="#">Perlindungan Malware untuk tipe pencarian S3</a> untuk menunjukkan keberadaan malware di objek S3 yang dipindai.</li> <li>• Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi di bawah <a href="#">Pemantauan dalam Perlindungan Malware untuk S3</a>. Ini termasuk menggunakan Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.</li> </ul> | <p>Anda berpotensi dapat memeriksa hasil pemindaian objek S3 dengan menggunakan satu atau beberapa opsi di bawah <a href="#">Pemantauan dalam Perlindungan Malware untuk S3</a>. Ini termasuk menggunakan Amazon EventBridge, CloudWatch metrik untuk paket Perlindungan Malware, dan menandai objek yang dipindai.</p> |

## Status sumber daya paket Perlindungan Malware

Bagian ini menjelaskan berbagai nilai status perlindungan yang terkait dengan sumber daya paket Perlindungan Malware Anda.

| Status                    | Deskripsi   |
|---------------------------|---|
| Aktif                     | Bucket S3 Anda telah berhasil dikonfigurasi dengan Perlindungan Malware untuk S3.   |
| Peringatan <sup>*</sup> - | Perlindungan Malware untuk S3 dirancang agar tidak terpengaruh saat peringatan muncul. Ketika GuardDuty melihat objek S3 baru, itu akan memulai pemindaian malware. Setelah berhasil memulai pemindaian, nilai kolom Status mungkin memerlukan beberapa menit untuk berubah menjadi Aktif. Anda akan menerima EventBridge pemberitahuan setelah pembaruan nilai kolom Status. |
| Kesalahan <sup>*</sup> -  | Ember Anda tidak terlindungi. Tak satu pun dari pemindaian malware yang terkait dengan bucket S3 ini akan selesai. Mungkin ada satu atau lebih akar penyebab potensial.   |

<sup>\*</sup> Untuk informasi tentang potensi masalah dan langkah-langkah terkait untuk menyelesaikannya, lihat [Memecahkan masalah rincian status paket Perlindungan Malware](#).

## Memecahkan masalah rincian status paket Perlindungan Malware

Untuk bucket yang dilindungi, GuardDuty menampilkan Status berdasarkan peringkat. Misalnya, jika bucket yang dilindungi memiliki masalah di kategori Kesalahan dan Peringatan, pertama-tama GuardDuty akan menampilkan masalah yang terkait dengan status Kesalahan.

Daftar berikut mencakup kesalahan dan peringatan untuk status paket Perlindungan Malware.

### Kesalahan

- [EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini](#)
- [EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada](#)
- [Bucket S3 tidak ada lagi](#)

## Peringatan

[Tidak dapat menempatkan objek uji](#)

## EventBridge pemberitahuan dinonaktifkan untuk bucket S3 ini

Kode alasan status terkait adalah `EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

### Detail status

GuardDuty menggunakan EventBridge untuk menerima pemberitahuan saat objek baru diunggah ke bucket S3 ini. Izin ini tidak ada dalam IAM peran Anda.

### Langkah-langkah untuk memecahkan masalah

Opsi 1: Tambahkan pernyataan izin berikut ke IAM peran Anda:

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda.

Opsi 2: Aktifkan EventBridge notifikasi dengan menggunakan konsol Amazon S3

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Pada halaman Bucket, di bawah tab Bucket tujuan umum, pilih nama bucket yang terkait dengan kesalahan ini.
3. Pada halaman bucket ini, pilih tab Properties.
4. Di bawah EventBridge bagian Amazon, pilih Edit.
5. Di EventBridge halaman Edit Amazon, untuk Kirim pemberitahuan ke Amazon EventBridge untuk semua acara di bucket ini, pilih Aktif.

## 6. Pilih Simpan perubahan.

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

## EventBridge aturan terkelola untuk menerima peristiwa bucket S3 tidak ada

Kode alasan status terkait adalah `EVENTBRIDGE_MANAGED_RULE_DISABLED`.

### Detail status

EventBridge Izin aturan terkelola untuk mengelola pengaturan EventBridge aturan tidak ada.

Langkah-langkah untuk memecahkan masalah

Tambahkan pernyataan izin berikut ke IAM peran Anda:

```
{
  "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
  "Effect": "Allow",
  "Action": [
    "events:PutRule",
    "events>DeleteRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource": [
    "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
  ],
  "Condition": {
    "StringEquals": {
      "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
    }
  }
}
```

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

## Bucket S3 tidak ada lagi

Kode alasan status terkait adalah `PROTECTED_RESOURCE_DELETED`.



## Detail status

Bucket S3 ini telah dihapus dari akun Anda dan tidak ada lagi.

### Langkah untuk memecahkan masalah

Jika menghapus bucket S3 tidak disengaja, maka Anda dapat membuat bucket baru dengan menggunakan konsol Amazon S3.

Setelah berhasil membuat bucket, aktifkan Perlindungan Malware untuk S3 dengan mengikuti langkah-langkah di bawah [Mengonfigurasi Perlindungan Malware untuk S3 untuk bucket Anda](#) halaman.

## Tidak dapat menempatkan objek uji

Kode alasan status terkait adalah `INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

### Note

Izin untuk menambahkan objek uji adalah opsional. Kehilangan izin ini dalam IAM peran Anda tidak mencegah Perlindungan Malware untuk S3 untuk memulai pemindaian malware pada objek yang baru diunggah. Setelah pemindaian berhasil dimulai, mungkin diperlukan beberapa menit agar Status paket Perlindungan Malware berubah dari Peringatan menjadi Aktif.

Jika IAM peran sudah menyertakan izin ini, maka peringatan ini menunjukkan kebijakan bucket Amazon S3 terbatas yang tidak mengizinkan peran menyertakan izin IAM ini.

## Detail status

Untuk memvalidasi penyiapan bucket yang dipilih, GuardDuty letakkan objek uji di bucket Anda.

### Langkah-langkah untuk memecahkan masalah

Anda dapat memilih untuk memperbarui IAM peran untuk menyertakan izin yang hilang. Untuk IAM peran yang dipilih, tambahkan izin berikut sehingga GuardDuty dapat menempatkan objek uji ke sumber daya yang dipilih:

```
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
```

```
"Action": [
  "s3:PutObject"
],
"Resource": [
  "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
]
}
```

Ganti *amzn-s3-demo-bucket* dengan nama bucket Amazon S3 Anda. Untuk informasi tentang izin IAM peran, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).

Mungkin perlu beberapa menit agar nilai kolom Status berubah menjadi Aktif.

## Pemantauan dalam Perlindungan Malware untuk S3

Saat menggunakan Perlindungan Malware untuk S3 dengan ID GuardDuty detektor, jika objek Amazon S3 Anda berpotensi berbahaya GuardDuty, akan dihasilkan. [Perlindungan Malware untuk tipe pencarian S3](#) Menggunakan GuardDuty konsol dan APIs, Anda dapat melihat temuan yang dihasilkan. Untuk informasi tentang memahami jenis temuan ini, lihat [Detail temuan](#).

Saat menggunakan Perlindungan Malware untuk S3 tanpa mengaktifkan GuardDuty (tanpa ID detektor), bahkan ketika objek Amazon S3 yang dipindai berpotensi berbahaya, tidak GuardDuty dapat menghasilkan temuan apa pun.

Daftar berikut memberikan potensi nilai status hasil pemindaian objek S3:

- NO\_THREATS\_FOUND— GuardDuty mendeteksi tidak ada ancaman potensial yang terkait dengan objek yang dipindai.
- THREATS\_FOUND— GuardDuty mendeteksi potensi ancaman yang terkait dengan objek yang dipindai.
- UNSUPPORTED— Ada beberapa alasan mengapa Perlindungan Malware untuk S3 akan melewati pemindaian. Alasan potensial termasuk file yang dilindungi kata sandi, Perlindungan Malware untuk kuota S3, dan fitur Amazon S3 tertentu. Untuk informasi selengkapnya, lihat [Kemampuan Perlindungan Malware untuk S3](#).
- ACCESS\_DENIED— tidak GuardDuty dapat mengakses objek ini untuk pemindaian. Periksa izin IAM peran yang terkait dengan bucket ini. Untuk informasi selengkapnya, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).

- **FAILED**— tidak GuardDuty dapat melakukan pemindaian malware pada objek ini karena kesalahan internal.

Daftar berikut memberikan nilai status pemindaian objek S3 potensial dan pemetaannya ke hasil pemindaian objek S3:

- **Selesai** — Pemindaian berhasil diselesaikan dan menunjukkan apakah objek S3 memiliki malware. Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa `THREATS_FOUND` atau `NO_THREATS_FOUND`.
- **Dilewati** — GuardDuty melewatkan pemindaian malware saat detail objek S3 tidak selaras dengan [Kuota dalam Perlindungan Malware untuk S3](#), atau GuardDuty tidak memiliki akses ke objek S3 yang diunggah di bucket yang dipilih.

Dalam hal ini, potensi nilai hasil pemindaian objek S3 dapat berupa `UNSUPPORTED` atau `ACCESS_DENIED`.

- **Gagal** — Mirip dengan nilai hasil pemindaian objek S3 `FAILED`, status pemindaian GuardDuty ini berarti tidak dapat melakukan pemindaian malware pada objek S3 karena kesalahan internal.

## Topik

- [Pemantauan EventBridge dengan Amazon](#)
- [Memantau metrik status pemindaian dengan menggunakan Amazon CloudWatch](#)
- [Pemantauan dengan tag objek S3](#)

## Pemantauan EventBridge dengan Amazon

Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi *software-as-a S-Service* (SaaS), dan AWS layanan serta rute data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

Sebagai akun pemilik bucket S3 yang dilindungi dengan Perlindungan Malware untuk S3, GuardDuty menerbitkan EventBridge notifikasi ke bus acara default dalam skenario berikut:

- Perubahan status sumber daya paket Perlindungan Malware untuk setiap bucket Anda yang dilindungi. Untuk informasi tentang berbagai status, lihat [Status sumber daya paket Perlindungan Malware](#).
- Ada kegagalan peristiwa tag karena alasan berikut:
  - IAMPeran Anda tidak memiliki izin untuk menandai objek.  
[Menambahkan izin IAM kebijakan](#)Template termasuk izin GuardDuty untuk menandai objek.
  - Sumber daya bucket atau objek yang ditentukan dalam IAM peran tidak ada lagi.
  - Objek S3 terkait telah mencapai batas tag maksimum. Untuk informasi selengkapnya tentang batas tag, lihat [Mengkategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.
- Hasil pemindaian objek S3 akan dipublikasikan ke bus EventBridge acara default Anda.

## Siapkan EventBridge aturan

Anda dapat mengatur EventBridge aturan di akun Anda untuk mengirim status sumber daya, peristiwa kegagalan tag pasca-pemindaian, atau hasil pemindaian objek S3 ke yang lain. AWS layanan Sebagai akun GuardDuty administrator yang didelegasikan, Anda akan menerima pemberitahuan status sumber daya paket Perlindungan Malware ketika ada perubahan status.

EventBridge Harga standar akan berlaku. Untuk informasi selengkapnya, lihat [EventBridge harga Amazon](#).

Semua nilai yang muncul di *red* adalah placeholder misalnya. Nilai-nilai ini akan berubah berdasarkan nilai di akun Anda, dan apakah malware terdeteksi atau tidak.

## Status sumber daya paket Perlindungan Malware

Anda dapat membuat pola EventBridge acara berdasarkan skenario berikut:

### **detail-type**Nilai potensial

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

## Pola acara

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guardduty"]
}
```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Active**:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status Active",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ACTIVE"
  }
}
```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Warning**:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status warning",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
```

```

    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "WARNING",
    "statusReasons": [
      {
        "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
      }
    ]
  }
}

```

Contoh skema pemberitahuan untuk **GuardDuty Malware Protection Resource Status Error**:

```

{
  "version": "0",
  "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
  "detail-type": "GuardDuty Malware Protection Resource Status Error",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "ERROR",
    "statusReasons": [
      {
        "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
      }
    ]
  }
}

```

Berdasarkan alasan di balik resourceStatusERROR, statusReasons nilainya akan terisi.

Untuk informasi tentang langkah-langkah pemecahan masalah untuk peringatan dan kesalahan berikut, lihat. [Memecahkan masalah rincian status paket Perlindungan Malware](#)

Hasil pemindaian objek S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Contoh skema pemberitahuan untuk **NO\_THREATS\_FOUND**:

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "NO_THREATS_FOUND",
      "threats": null
    }
  }
}
```

Contoh skema pemberitahuan untuk **THREATS\_FOUND**:

```
{
```

```

"version": "0",
"id": "72c7d362-737a-6dce-fc78-9e27a0171419",
"detail-type": "GuardDuty Malware Protection Object Scan Result",
"source": "aws.guardduty",
"account": "111122223333",
"time": "2024-02-28T01:01:01Z",
"region": "us-east-1",
"resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "COMPLETED",
  "resourceType": "S3_OBJECT",
  "s3objectDetails": {
    "bucketName": "amzn-s3-demo-bucket",
    "objectKey": "APKAEIBAERJR2EXAMPLE",
    "eTag": "ASIAI44QH8DHBEXAMPLE",
    "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
  },
  "scanResultDetails": {
    "scanResultStatus": "THREATS_FOUND",
    "threats": [
      {
        "name": "EICAR-Test-File (not a virus)"
      }
    ]
  }
}
}

```

Skema pemberitahuan sampel untuk status hasil pemindaian **UNSUPPORTED** (Dilewati):

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {

```



```

    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "UNSUPPORTED",
      "threats": null
    }
  }
}

```

Skema pemberitahuan sampel untuk status hasil pemindaian **ACCESS\_DENIED** (Dilewati):

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "ACCESS_DENIED",
      "threats": null
    }
  }
}

```

```
}

```

Skema pemberitahuan sampel untuk status **FAILED** hasil pemindaian:

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "FAILED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
    },
    "scanResultDetails": {
      "scanResultStatus": "FAILED",
      "threats": null
    }
  }
}
```

Peristiwa kegagalan tag pasca-pemindaian

Pola acara:

```
{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty"
}
```

Contoh skema pemberitahuan untuk **ACCESS\_DENIED**:

```
{

```

```

"version": "0",
"id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
"detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
"source": "aws.guardduty",
"account": "111122223333",
"time": "2024-06-10T16:16:08Z",
"region": "us-east-1",
"resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
"detail": {
  "schemaVersion": "1.0",
  "eventTime": "2024-06-10T16:16:08Z",
  "s3objectDetails": {
    "bucketName": "amzn-s3-demo-bucket",
    "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
    "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
    "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
  },
  "postScanActions": [{
    "actionType": "TAGGING",
    "status": "FAILED",
    "failureReason": "ACCESS_DENIED"
  }]
}
}

```

Contoh skema pemberitahuan untuk **MAX\_TAG\_LIMIT\_EXCEEDED**:

```

{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",

```

```
    "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
    "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
    "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
  },
  "postScanActions": [{
    "actionType": "TAGGING",
    "status": "FAILED",
    "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
  }]
}
```

Untuk memecahkan masalah alasan kegagalan ini, lihat [Memecahkan masalah kegagalan tag pasca-pemindaian objek S3](#)

## Memantau metrik status pemindaian dengan menggunakan Amazon CloudWatch

Anda dapat memantau GuardDuty penggunaan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan selama 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang bagaimana kinerja Perlindungan Malware untuk S3. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

CloudWatch Metrik untuk Perlindungan Malware untuk S3 tersedia di tingkat sumber daya. Anda dapat menanyakan metrik ini untuk setiap sumber daya yang dilindungi secara terpisah. Metrik dilaporkan di `AWS/GuardDuty/MalwareProtection` namespace. Anda dapat mengatur alarm pada sumber daya tertentu untuk memantau postur keamanan.

### Metrik status pemindaian malware

#### Metrik

CompletedScanCount

#### Deskripsi


Jumlah pemindaian malware objek S3 yang diselesaikan dalam jangka waktu tertentu.

Dimensi yang Valid:

---

|                                 |  |
|---------------------------------|--|
|                                 | <ul style="list-style-type: none"><li>• Malware Protection Plan Id</li></ul>               |
|                                 | Resource Name  |
|                                 | Unit: Jumlah   |
| FailedScanCount                 | Jumlah pemindaian malware objek S3 yang diselesaikan dalam jangka waktu tertentu.          |
|                                 | Dimensi yang Valid:  |
|                                 | <ul style="list-style-type: none"><li>• Malware Protection Plan Id</li></ul>               |
|                                 | Resource Name  |
|                                 | Unit: Jumlah   |
| SkippedScanCount                | Jumlah pemindaian malware objek S3 yang dilewati dalam jangka waktu tertentu.              |
|                                 | Dimensi yang Valid:  |
|                                 | <ul style="list-style-type: none"><li>• Malware Protection Plan Id</li></ul>               |
|                                 | Resource Name  |
|                                 | Skipped Reason   |
|                                 | Nilai potensial  |
|                                 | <ul style="list-style-type: none"><li>• UnSupported</li><li>• MissingPermissions</li></ul> |
|                                 | Unit: Jumlah   |
| Metrik hasil pemindaian malware |  |

|                    |   |
|--------------------|---|
| InfectedScanCount  | <p>Jumlah pemindaian malware objek S3 yang mendeteksi objek yang berpotensi berbahaya dalam jangka waktu tertentu.</p> <p>Dimensi yang Valid:</p> <ul style="list-style-type: none"> <li>• Malware Protection Plan Id</li> </ul> <p style="padding-left: 40px;">Resource Name</p> <p>Unit: Jumlah</p> |
| CompletedScanBytes | <p>Jumlah byte objek S3 yang dipindai dalam kerangka waktu tertentu.</p> <p>Dimensi yang Valid:</p> <ul style="list-style-type: none"> <li>• Malware Protection Plan Id</li> </ul> <p style="padding-left: 40px;">Resource Name</p> <p>Unit: Jumlah</p>   |

 Note

Secara default, statistik dalam CloudWatch metrik adalahAVG.

Dimensi berikut didukung untuk metrik Perlindungan Malware untuk S3.

| Dimensi                    | Deskripsi  |
|----------------------------|--|
| Malware Protection Plan Id | Pengidentifikasi unik yang terkait dengan sumber daya paket Perlindungan Malware yang GuardDuty dibuat untuk sumber daya Anda yang dilindungi. |

|                |  |
|----------------|--|
| Resource Name  | Nama sumber daya yang dilindungi.  |
| Skipped Reason | Alasan mengapa pemindaian malware objek S3 dilewati.                                       |
|                | Nilai potensial  |
|                | <ul style="list-style-type: none"><li>• Unsupported</li><li>• MissingPermissions</li></ul> |

Untuk informasi tentang mengakses dan menanyakan metrik ini, lihat Menggunakan metrik [Amazon CloudWatch di Panduan Pengguna](#) Amazon. CloudWatch

Untuk informasi tentang mengatur alarm, lihat [Menggunakan CloudWatch alarm Amazon](#) di CloudWatch Panduan Pengguna Amazon.

## Pemantauan dengan tag objek S3

Gunakan opsi aktifkan penandaan sehingga GuardDuty dapat menambahkan tag ke objek Amazon S3 Anda setelah menyelesaikan pemindaian malware.

Pertimbangan untuk mengaktifkan penandaan

- Ada biaya penggunaan terkait saat GuardDuty menandai objek S3 Anda. Untuk informasi selengkapnya, lihat [Harga untuk Perlindungan Malware untuk S3](#).
- Anda harus menyimpan izin penandaan yang diperlukan untuk IAM peran pilihan yang terkait dengan bucket ini; jika tidak, tidak GuardDuty dapat menambahkan tag ke objek yang dipindai. IAMPeran tersebut sudah menyertakan izin untuk menambahkan tag ke objek S3 yang dipindai. Untuk informasi selengkapnya, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).
- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat [Menggunakan kontrol akses berbasis tag \(\) TBAC](#).

Setelah Anda mengaktifkan penandaan untuk bucket S3 atau awalan tertentu, objek apa pun yang baru diunggah yang dipindai, akan memiliki tag terkait dalam format pasangan nilai kunci berikut:

GuardDutyMalwareScanStatus:*Scan-Status*

Untuk informasi tentang nilai tag potensial, lihat [Menggunakan kontrol akses berbasis tag \(\) TBAC](#).

## Memecahkan masalah kegagalan tag pasca-pemindaian objek S3 di Perlindungan Malware untuk S3

Bagian ini hanya berlaku untuk Anda jika Anda [Aktifkan penandaan untuk objek yang dipindai](#) berada dalam ember yang dilindungi.

Saat GuardDuty mencoba menambahkan tag ke objek S3 yang dipindai, tindakan penandaan dapat mengakibatkan kegagalan. Alasan potensial mengapa hal ini dapat terjadi pada ember Anda adalah ACCESS\_DENIED dan MAX\_TAG\_LIMIT\_EXCEEDED. Gunakan topik berikut untuk memahami alasan potensial untuk alasan kegagalan tag pasca-pemindaian ini dan selesaikan masalahnya.

### ACCESS\_DENIED

Daftar berikut memberikan alasan potensial yang dapat menyebabkan masalah ini:

- IAM Peran yang digunakan untuk bucket S3 yang dilindungi ini tidak memiliki AllowPostScanTag izin. Verifikasi bahwa IAM peran terkait menggunakan kebijakan bucket ini. Untuk informasi selengkapnya, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).
- Kebijakan bucket S3 yang dilindungi tidak memungkinkan GuardDuty untuk menambahkan tag ke objek ini.
- Objek S3 yang dipindai tidak ada lagi.

### MAX\_TAG\_LIMIT\_EXCEEDED

Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek S3. Untuk informasi selengkapnya, lihat Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda di bawah. [Aktifkan penandaan untuk objek yang dipindai](#)

## Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3

Saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Anda, Anda dapat memilih untuk mengaktifkan penandaan. Setelah mencoba memindai objek S3 yang baru diunggah di bucket yang dipilih, GuardDuty tambahkan tag ke objek yang dipindai untuk memberikan status pemindaian malware. Ada biaya penggunaan langsung yang terkait saat Anda mengaktifkan penandaan. Untuk informasi selengkapnya, lihat [Harga untuk Perlindungan Malware untuk S3](#).



GuardDuty menggunakan tag yang telah ditentukan dengan kunci sebagai `GuardDutyMalwareScanStatus` dan nilai sebagai salah satu status pemindaian malware. Untuk informasi tentang nilai-nilai ini, lihat [S3 object potential scan result values](#).

Pertimbangan GuardDuty untuk menambahkan tag ke objek S3 Anda:

- Secara default, Anda dapat mengaitkan hingga 10 tag dengan objek. Untuk informasi selengkapnya, lihat [Mengkategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Amazon S3.

Jika semua 10 tag sudah digunakan, tidak GuardDuty dapat menambahkan tag yang telah ditentukan ke objek yang dipindai. GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Pemantauan EventBridge dengan Amazon](#).

- Jika IAM peran yang dipilih tidak menyertakan izin GuardDuty untuk menandai objek S3, bahkan dengan penandaan diaktifkan untuk bucket Anda yang dilindungi, tidak GuardDuty akan dapat menambahkan tag ke objek S3 yang dipindai ini. Untuk informasi selengkapnya tentang izin IAM peran yang diperlukan untuk penandaan, lihat [Prasyarat - Membuat atau memperbarui kebijakan peran IAM](#).

GuardDuty juga menerbitkan hasil pemindaian ke bus EventBridge acara default Anda. Untuk informasi selengkapnya, lihat [Pemantauan EventBridge dengan Amazon](#).

## TBACMenambahkan sumber daya bucket S3

Anda dapat menggunakan kebijakan sumber daya bucket S3 untuk mengelola kontrol akses berbasis tag (TBAC) untuk objek S3 Anda. Anda dapat memberikan akses ke pengguna tertentu untuk mengakses dan membaca objek S3. Jika Anda memiliki organisasi yang dibuat dengan menggunakan AWS Organizations, Anda harus menegaskan bahwa tidak ada yang dapat memodifikasi tag yang ditambahkan oleh GuardDuty. Untuk informasi selengkapnya, lihat [Mencegah tag diubah kecuali oleh prinsipal resmi di Panduan Pengguna AWS Organizations](#). Contoh yang digunakan dalam topik terkait menyebutkan `ec2`. Saat Anda menggunakan contoh ini, ganti `ec2` dengan `s3`.

Daftar berikut menjelaskan apa yang dapat Anda lakukan dengan menggunakan TBAC:

- Cegah semua pengguna kecuali Perlindungan Malware untuk prinsipal layanan S3 membaca objek S3 yang belum ditandai dengan pasangan nilai kunci tag berikut:

### GuardDutyMalwareScanStatus:*Potential key value*

- Izinkan hanya GuardDuty untuk menambahkan kunci tag GuardDutyMalwareScanStatus dengan nilai sebagai hasil pemindaian, ke objek S3 yang dipindai. Templat kebijakan berikut dapat mengizinkan pengguna tertentu yang memiliki akses, untuk berpotensi mengganti pasangan nilai kunci tag.

Contoh kebijakan sumber daya bucket S3:

Ganti *IAM-role-name* dengan IAM peran yang Anda gunakan untuk mengonfigurasi Perlindungan Malware untuk S3 di bucket Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NoReadExceptForClean",
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": [
          "arn:aws:iam::555555555555:root",
          "arn:aws:iam::555555555555:role/IAM-role-name",
          "arn:aws:iam::555555555555:assumed-role/IAM-role-name/GuardDutyMalwareProtection"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
            "NO_THREATS_FOUND"
        }
      }
    }
  ],
  {
```

```
    "Sid": "OnlyGuardDutyCanTag",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:iam::555555555555:root",
        "arn:aws:iam::555555555555:role/IAM-role-name",
        "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
      ]
    },
    "Action": "s3:PutObjectTagging",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  }
]
```

Untuk informasi selengkapnya tentang menandai sumber daya S3 Anda, kebijakan [Penandaan dan kontrol akses](#).

## Mengedit Perlindungan Malware untuk S3 untuk bucket yang dilindungi

Gunakan langkah-langkah berikut untuk mengedit penyiapan bucket S3 Anda yang dilindungi:

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.
3. Di dalam bucket Protected, pilih bucket yang ingin Anda edit konfigurasi yang ada.
4. Pilih Edit.
5. Perbarui konfigurasi dan pengaturan yang ada untuk bucket Anda dan konfirmasi perubahannya. Untuk informasi tentang deskripsi dan langkah-langkah untuk setiap bagian, lihat [Aktifkan Perlindungan Malware untuk S3 untuk bucket Anda](#).

Pantau kolom Status untuk bucket yang dilindungi ini. Jika muncul sebagai Peringatan atau Kesalahan, lihat [Memecahkan masalah rincian status paket Perlindungan Malware](#).

## Melihat penggunaan dan biaya untuk Perlindungan Malware untuk S3

Akun Anda mulai mengeluarkan biaya penggunaan saat Anda menggunakan Perlindungan Malware untuk S3 di luar batas spesifik di bawah paket Tingkat Gratis atau paket Tingkat Gratis 12 bulan akun Anda berakhir. Untuk informasi tentang paket Tingkat Gratis, lihat [Harga untuk Perlindungan Malware untuk S3](#).

Untuk melihat biaya penggunaan, navigasikan ke Cost Explorer di konsol <https://console.aws.amazon.com/billing/>. Untuk informasi tentang Akun AWS penagihan, lihat [Panduan AWS Billing Pengguna](#).

## Nonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi

Saat Anda menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi, GuardDuty menghapus ID paket Perlindungan Malware yang terkait dengan bucket tersebut. GuardDuty tidak akan lagi memulai pemindaian malware ketika objek baru diunggah ke bucket ini atau salah satu awalan objek yang dipilih.

Jika Anda telah mengaktifkan GuardDuty dan sekarang ingin menangguhkan atau menonaktifkan GuardDuty, lihat [Menangguhkan atau menonaktifkan GuardDuty](#). Karena tidak ada konsep ID detektor dalam Perlindungan Malware untuk S3, menonaktifkan atau menangguhkan GuardDuty tidak memengaruhi status bucket yang dilindungi di akun Anda. Anda dapat terus menggunakan fitur Perlindungan Malware untuk S3 secara independen dengan harga standar terkait. Untuk informasi selengkapnya, lihat [Melihat penggunaan dan biaya untuk Perlindungan Malware untuk S3](#). Untuk berhenti menggunakan Perlindungan Malware untuk S3, Anda harus menonaktifkannya untuk semua ember yang dilindungi di akun Anda. Jika Anda ingin terus menggunakan GuardDuty dan menonaktifkan hanya Perlindungan Malware untuk S3 untuk bucket, langkah-langkah berikut tidak akan memengaruhi konfigurasi GuardDuty layanan dan paket perlindungan lain yang mungkin telah Anda aktifkan.

Untuk menonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Perlindungan Malware untuk S3.

3. Di dalam bucket Protected, pilih bucket yang ingin Anda nonaktifkan Perlindungan Malware untuk S3.

Anda hanya dapat memilih satu ember yang dilindungi sekaligus. Untuk menonaktifkan Perlindungan Malware untuk S3 selama lebih dari satu bucket, ikuti langkah-langkah ini lagi untuk bucket S3 lainnya.

4. Pilih Disable (Nonaktifkan).
5. Pilih Nonaktifkan untuk mengonfirmasi pilihan.

## Dukungan fitur Amazon S3

Tabel berikut menentukan apakah Perlindungan Malware untuk S3 mendukung fitur Amazon S3 yang terdaftar atau tidak.

| Apakah dukungan tersedia? | Deskripsi  |
|---------------------------|--|
| Ya                        | Objek S3 dapat diambil tanpa memulihkan secara asinkron. |

| Apakah dukungan tersedia? | Deskripsi   |
|---------------------------|---|
|                           |   |
| Bersyarat                 | <ul style="list-style-type: none"><li>• Dukungan Intelligent Tiering tersedia untuk objek S3 di tingkatan Akses Instans Sering, Jarang, dan Arsip.</li><li>• Tingkat opt-in Archive dan Deep Archive tidak didukung.</li><li>• Intelligent Tiering selalu membuat objek baru di tingkat Frequent Access. Oleh karena itu, pemindaian objek saat membuat didukung.</li><li>• Fitur tiering Cerdas Masa Depan mungkin memulai objek di Arsip. Karena itu, ini tidak didukung.</li></ul> |

| Apakah dukungan tersedia? | Deskripsi   |
|---------------------------|---|
| Tidak                     | GuardDuty hanya mendukung bucket tujuan umum untuk Perlindungan Malware untuk S3. |
| Tidak                     | Objek S3 harus dipulihkan sebelum dapat diakses.                                  |

| Apakah dukungan tersedia? | Deskripsi  |
|---------------------------|--|
| Tidak                     | Perlindungan Malware untuk S3 tidak didukung di Outposts.  |
| Ya                        | Semua objek S3 yang diunggah dipindai untuk malware. Jika Anda mengunggah objek dengan file versi v1 dan segera mengunggah versi lain yang diganti dengan v2, maka GuardDuty akan memindai file objek versi v1 dan v2. Namun, waktu mulai pemindaian mungkin tidak dalam urutan yang sama. |
| Ya                        | Jika bucket tujuan adalah sumber daya yang dilindungi, maka GuardDuty akan memindai semua objek S3 direplikasi ke awalan yang dilindungi dan dipantau.   |
| Tidak                     | Anda tidak dapat menentukan aturan replikasi berdasarkan tag hasil pemindaian. Amazon S3 tidak mendukung replikasi untuk tag, kecuali saat dibuat.   |



| Apakah dukungan tersedia? | Deskripsi  |
|---------------------------|--|
| Ya                        | <p>GuardDuty mendukung pemindaian malware untuk objek S3 yang dienkripsi dengan kunci yang dikelola dan dikelola pelanggan. Pastikan bahwa IAM peran tersebut mencakup izin untuk menggunakan kunci. Untuk informasi selengkapnya, lihat <a href="#">Menambahkan izin IAM kebijakan</a>.</p> |

| Apakah dukungan tersedia? | Deskripsi   |
|---------------------------|---|
| Tidak                     | Perlindungan Malware untuk S3 tidak mendukung pemindaian objek S3 yang dienkripsi dengan kunci yang tidak dapat diakses.  |
| Tidak                     | Saat objek S3 Anda dienkripsi menggunakan Klien Enkripsi Amazon S3, objek Anda tidak akan terekspos ke pihak ketiga mana pun, termasuk AWS. Untuk informasi selengkapnya tentang alasan ini tidak didukung, lihat <a href="#">Melindungi data dengan menggunakan enkripsi sisi klien</a> di Panduan Pengguna Amazon S3. |
| Ya                        | Objek S3 terkunci dikunci berdasarkan WORM - Tulis Sekali Baca Banyak. Perlindungan Malware untuk S3 dapat mengakses dan memindai objek.  |
| Ya                        | Perlindungan Malware untuk S3 dapat memindai bucket yang diatur dengan Requester Pays. Pemohon akan membayar panggilan S3. Untuk informasi selengkapnya, lihat <a href="#">Menggunakan bucket Requester Pays untuk transfer penyimpanan dan penggunaan</a> di Panduan Pengguna Amazon S3.                               |

| Apakah dukungan tersedia? | Deskripsi  |
|---------------------------|--|
| Ya                        | Anda dapat menentukan kebijakan siklus hidup berdasarkan tag hasil pemindaian. Misalnya, hapus objek berbahaya secara otomatis. Untuk informasi selengkapnya tentang konfigurasi lifecycle, lihat <a href="#">Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Amazon S3</a> .  |
| Ya                        | Anda dapat menentukan kebijakan sumber daya bucket berdasarkan tag hasil pemindaian objek S3. Misalnya, mencegah akses ke objek S3 yang belum dipindai, atau ancaman yang GuardDuty terdeteksi. Untuk informasi selengkapnya, lihat <a href="#">Menggunakan kontrol akses berbasis tag (TBAC) dengan Perlindungan Malware untuk S3</a> . |

## Kuota dalam Perlindungan Malware untuk S3

Bagian ini menyediakan kuota default, sering disebut sebagai batas. Kecuali ditentukan, setiap kuota adalah Region-specific. Untuk melihat kuota default khusus untuk menggunakan GuardDuty layanan dasar (atau inti), lihat. [GuardDuty Kuota Amazon](#)

Tabel berikut menjelaskan beberapa kuota yang akan berlaku untuk Anda Akun AWS.

| AWS nilai kuota default | Apakah itu dapat disesuaikan? | Deskripsi  |
|-------------------------|-------------------------------|--|
| 5 GB                    | Tidak                         | Ukuran objek S3 maksimum yang GuardDuty akan mencoba memindai malware. |
| 5 GB                    | Tidak                         | Jumlah maksimum data (dalam GB) yang GuardDuty dapat mengekstrak       |

| AWS nilai kuota default | Apakah itu dapat disesuaikan? | Deskripsi   |
|-------------------------|-------------------------------|---|
|                         |                               | dan menganalisis dari file arsip. Bahkan jika file arsip berisi lebih dari 5 GB, maka GuardDuty akan melewatkan konten di luar nilai ini.   |
| 1.000                   | Tidak                         | Jumlah maksimum file yang GuardDuty dapat mengekstrak dan menganalisis dalam file arsip. Jika file berisi lebih dari 1.000 file, maka GuardDuty harus melewati file yang diarsipkan.                              |
| 5                       | Tidak                         | Tingkat maksimum arsip bersarang yang GuardDuty dapat mengekstrak. Jika arsip menyertakan file yang bersarang di luar nilai ini, maka GuardDuty akan melewati file bersarang tersebut.                            |
| 25                      | Tidak                         | Jumlah maksimum bucket S3 yang dapat Anda aktifkan Perlindungan Malware untuk S3. Batas kuota ini adalah per akun di setiap Wilayah.  |
| 25                      | Di tingkat Wilayah            | Jumlah maksimum operasi pesawat kontrol yang dapat dimulai per detik di setiap Wilayah. API Operasi termasuk membuat, membaca, memperbarui, dan menghapus sumber daya. Nilai kuota ini berlaku di tingkat Region. |

## GuardDuty RDSPerlindungan

RDSPerlindungan di Amazon GuardDuty menganalisis dan memprofilkan aktivitas RDS login untuk potensi ancaman akses ke database Amazon Aurora Anda (Amazon Aurora My SQL - Compatible Edition dan Aurora Postgre -Compatible Edition) dan Amazon untuk SQL Postgre. RDS SQL Fitur ini memungkinkan Anda mengidentifikasi perilaku login yang berpotensi mencurigakan. RDSPerlindungan tidak memerlukan infrastruktur tambahan; itu dirancang agar tidak mempengaruhi kinerja instance database Anda.

Ketika RDS Protection mendeteksi upaya login yang berpotensi mencurigakan atau anomali yang menunjukkan ancaman terhadap database Anda, GuardDuty buat temuan baru dengan detail tentang database yang berpotensi dikompromikan.

Anda dapat mengaktifkan atau menonaktifkan fitur RDS Perlindungan untuk akun apa pun di Wilayah AWS mana pun fitur ini tersedia di Amazon GuardDuty, kapan saja. GuardDuty Akun yang ada dapat mengaktifkan RDS Perlindungan dengan masa uji coba 30 hari. Untuk GuardDuty akun baru, RDS Perlindungan sudah diaktifkan dan termasuk dalam periode uji coba gratis 30 hari. Untuk informasi selengkapnya, lihat [Memperkirakan biaya](#).

### Note

Ketika fitur RDS Perlindungan tidak diaktifkan, GuardDuty tidak mengumpulkan aktivitas RDS login Anda, atau mendeteksi perilaku login anomali atau mencurigakan.

Untuk informasi tentang Wilayah AWS tempat yang GuardDuty belum mendukung RDS Perlindungan, lihat [Ketersediaan fitur khusus wilayah](#).

## Basis data Amazon Aurora dan Amazon yang didukung RDS

Tabel berikut menunjukkan versi RDS database Aurora dan Amazon yang didukung.

| Amazon Aurora dan mesin Amazon RDS DB | Versi mesin yang didukung   |
|---------------------------------------|---|
| Aurora Saya SQL                       | <ul style="list-style-type: none"><li>• 2.10.2 atau yang lebih baru</li><li>• 3.02.1 atau yang lebih baru</li></ul> |

| Amazon Aurora dan mesin Amazon RDS DB | Versi mesin yang didukung  |
|---------------------------------------|--|
| Aurora Postgre SQL                    | <ul style="list-style-type: none"><li>• 10.17 atau yang lebih baru</li><li>• 11.12 atau yang lebih baru</li><li>• 12.7 atau yang lebih baru</li><li>• 13.3 atau yang lebih baru</li><li>• 14.3 atau yang lebih baru</li><li>• 15.2 atau yang lebih baru</li><li>• 16.1 atau yang lebih baru</li></ul>                                |
| RDSuntuk Postgre SQL                  | <ul style="list-style-type: none"><li>• 14.5 atau yang lebih baru</li><li>• 13.8 atau yang lebih baru</li><li>• 12.12 atau lebih baru</li><li>• 11.17 atau lebih baru</li><li>• 10.22 atau yang lebih baru</li><li>• <a href="#">RDSuntuk Postgre versi 15 SQL</a></li><li>• <a href="#">RDSuntuk Postgre versi 16 SQL</a></li></ul> |

## Bagaimana RDS Protection menggunakan pemantauan aktivitas RDS login

RDS Perlindungan di Amazon GuardDuty membantu Anda melindungi Amazon Aurora (Aurora) yang didukung dan RDS untuk database SQL Postgre di akun Anda. Setelah Anda mengaktifkan fitur RDS Perlindungan, GuardDuty segera mulai memantau aktivitas RDS login dari database Aurora dan Amazon RDS di akun Anda. GuardDuty terus memantau dan memprofilkan aktivitas RDS login untuk aktivitas mencurigakan, misalnya, akses tidak sah ke database Aurora di akun Anda, dari aktor eksternal yang sebelumnya tidak terlihat. Saat Anda mengaktifkan RDS Perlindungan untuk pertama kalinya atau Anda memiliki instance database yang baru dibuat, periode pembelajaran diperlukan untuk mendasarkan perilaku normal. Untuk alasan ini, instance database yang baru diaktifkan atau yang baru dibuat mungkin tidak memiliki temuan login anomali terkait hingga dua minggu. Untuk informasi selengkapnya, lihat [RDS pemantauan aktivitas login](#).

Ketika RDS Protection mendeteksi potensi ancaman, seperti pola yang tidak biasa dalam serangkaian upaya login yang berhasil, gagal, atau tidak lengkap, GuardDuty menghasilkan temuan

baru dengan detail tentang instance database yang berpotensi dikompromikan. Untuk informasi selengkapnya, lihat [Jenis temuan Perlindungan RDS](#). Jika Anda menonaktifkan RDS Perlindungan, GuardDuty segera berhenti memantau aktivitas RDS login dan tidak dapat mendeteksi potensi ancaman apa pun terhadap instance basis data yang didukung.

#### Note

GuardDuty tidak mengelola aktivitas Anda [Database yang didukung](#) atau RDS login, atau membuat aktivitas RDS login tersedia untuk Anda.

## Fitur dalam RDS Perlindungan

### RDS pemantauan aktivitas login

RDS aktivitas login menangkap upaya login yang berhasil dan gagal yang dilakukan ke [Basis data Amazon Aurora dan Amazon yang didukung RDS](#) AWS lingkungan Anda. Untuk membantu Anda melindungi database Anda, GuardDuty RDS Protection terus memantau aktivitas login untuk upaya login yang berpotensi mencurigakan. Misalnya, musuh dapat mencoba untuk memaksa akses ke database Amazon Aurora dengan menebak kata sandi database.

Ketika Anda mengaktifkan fitur RDS Perlindungan, GuardDuty secara otomatis mulai memantau aktivitas RDS login untuk database Anda langsung dari layanan Aurora dan AmazonRDS. Jika ada indikasi perilaku login anomali, GuardDuty buat temuan dengan detail tentang database yang berpotensi dikompromikan. Saat Anda mengaktifkan RDS Perlindungan untuk pertama kalinya atau Anda memiliki instance database yang baru dibuat, periode pembelajaran diperlukan untuk mendasarkan perilaku normal. Untuk alasan ini, instance database yang baru diaktifkan atau yang baru dibuat mungkin tidak memiliki temuan login anomali terkait hingga dua minggu.

Fitur RDS Perlindungan tidak memerlukan penyiapan tambahan apa pun; fitur ini tidak memengaruhi database Amazon Aurora atau konfigurasi Amazon RDS yang ada. GuardDuty tidak mengelola basis data atau aktivitas RDS login yang didukung, atau membuat aktivitas RDS login tersedia untuk Anda.

Jika Anda memilih untuk mengaktifkan secara otomatis fitur RDS Perlindungan untuk akun anggota baru saat mereka bergabung dengan organisasi Anda, tindakan ini secara otomatis memungkinkan GuardDuty untuk akun anggota baru tersebut. Untuk informasi selengkapnya tentang mengonfigurasi pemantauan aktivitas RDS login sebagai fitur, lihat [GuardDuty RDS Perlindungan](#).

# Mengkonfigurasi RDS Perlindungan untuk akun mandiri

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih RDSPerlindungan.
3. Halaman RDSPerlindungan menunjukkan status saat ini untuk akun Anda. Anda dapat mengaktifkan atau menonaktifkan fitur kapan saja dengan memilih Aktifkan atau Nonaktifkan. Konfirmasikan pilihan Anda.

## API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek name sebagai `RDS_LOGIN_EVENTS` dan status sebagai `ENABLED` atau `DISABLED`.

Anda juga dapat mengaktifkan atau menonaktifkan RDS Perlindungan dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan valid Anda sendiri *detector ID*.

### Note

Kode contoh berikut memungkinkan RDS Perlindungan. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

# Mengkonfigurasi RDS Perlindungan di lingkungan multi-akun

Dalam lingkungan beberapa akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan fitur RDS Perlindungan untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka.



Akun GuardDuty administrator yang didelegasikan mengelola akun anggota mereka menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan ini dapat memilih untuk mengaktifkan pemantauan aktivitas RDS login secara otomatis untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan beberapa akun, lihat [Mengelola beberapa akun di Amazon](#). GuardDuty

## Mengkonfigurasi RDS Perlindungan untuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses pilihan Anda untuk mengonfigurasi Pemantauan Aktivitas RDS Login untuk akun GuardDuty administrator yang didelegasikan.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensial akun manajemen.

2. Di panel navigasi, pilih RDSPerlindungan.
3. Pada halaman RDSPerlindungan, pilih Edit.
4. Lakukan salah satu hal berikut ini:

#### Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

#### Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

## API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek name sebagai `RDS_LOGIN_EVENTS` dan status sebagai `ENABLED` atau `DISABLED`.

Anda dapat mengaktifkan atau menonaktifkan RDS Perlindungan dengan menjalankan AWS CLI perintah berikut. Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan yang valid *detector ID*.

### Note

Kode contoh berikut memungkinkan RDS Perlindungan. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

## Aktifkan otomatis RDS Perlindungan untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur RDS Perlindungan untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman RDS Perlindungan

1. Di panel navigasi, pilih RDS Perlindungan.
2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan RDS Perlindungan untuk akun yang ada dan baru di organisasi.

### 3. Pilih Simpan.

#### Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

#### Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Aktivitas RDS Masuk.
4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan atau nonaktifkan RDS Perlindungan untuk akun anggota secara selektif](#).

#### API/CLI

- Untuk mengaktifkan atau menonaktifkan RDS Perlindungan secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan RDS Perlindungan untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

**Note**

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan RDS Perlindungan untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan RDS Perlindungan untuk semua akun anggota aktif yang ada di organisasi Anda.

### Console

Untuk mengonfigurasi RDS Perlindungan untuk semua akun anggota aktif yang ada

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih RDSPerlindungan.
3. Pada halaman RDSPerlindungan, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

### API/CLI

- Untuk mengaktifkan atau menonaktifkan RDS Perlindungan secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectors](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan RDS Perlindungan untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan otomatis RDS Perlindungan untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan aktivitas RDS login untuk akun baru yang bergabung dengan organisasi Anda.

### Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan akun anggota baru di organisasi melalui konsol, baik menggunakan halaman RDSPerlindungan atau Akun.

Untuk mengaktifkan RDS Perlindungan secara otomatis untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman RDSPerlindungan:

1. Di panel navigasi, pilih RDSPerlindungan.
2. Pada halaman RDSPerlindungan, pilih Edit.
3. Pilih Konfigurasi akun secara manual.
4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, RDS Perlindungan akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.

5. Pilih Simpan.
- Menggunakan halaman Akun:
    1. Di panel navigasi, pilih Akun.
    2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
    3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Aktivitas RDS Masuk.
    4. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan RDS Perlindungan secara selektif untuk akun anggota Anda, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan RDS Perlindungan untuk satu akun anggota. Untuk menonaktifkannya, lihat [Aktifkan atau nonaktifkan RDS Perlindungan untuk akun anggota secara selektif](#). Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `autoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan atau nonaktifkan RDS Perlindungan untuk akun anggota secara selektif

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan pemantauan aktivitas RDS login untuk akun anggota secara selektif.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Pada halaman Akun, tinjau kolom aktivitas RDS login untuk status akun anggota Anda.

3. Untuk mengaktifkan atau menonaktifkan aktivitas RDS login secara selektif

Pilih akun yang ingin Anda konfigurasi RDS Perlindungan. Anda dapat memilih beberapa akun sekaligus. Di menu tarik-turun Edit Rencana Perlindungan, pilih Aktivitas RDS Login, lalu pilih opsi yang sesuai.

## API/CLI

Untuk mengaktifkan atau menonaktifkan RDS Perlindungan secara selektif untuk akun anggota Anda, jalankan [updateMemberDetectorsAPI](#) operasi menggunakan akun Anda sendiri *detector ID*.

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan RDS Perlindungan untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
"ENABLED"}]'
```

### Note

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

# GuardDuty Perlindungan Lambda

Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan saat suatu [AWS Lambda](#) fungsi dipanggil di lingkungan Anda. AWS Saat Anda mengaktifkan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda, dimulai dari [VPCLog Aliran](#) semua fungsi Lambda untuk akun, termasuk log yang tidak menggunakan VPC jaringan, dan dihasilkan saat fungsi Lambda dipanggil. Jika GuardDuty mengidentifikasi lalu lintas jaringan mencurigakan yang menunjukkan adanya potongan kode yang berpotensi berbahaya dalam fungsi Lambda Anda, GuardDuty akan menghasilkan temuan.

## Note

Pemantauan Aktivitas Jaringan Lambda tidak menyertakan log untuk fungsi [Lambda @Edge](#).

Anda dapat mengonfigurasi Perlindungan Lambda untuk akun apa pun atau tersedia Wilayah AWS, kapan saja. Secara default, GuardDuty akun yang ada dapat mengaktifkan Perlindungan Lambda dengan masa uji coba 30 hari. Untuk GuardDuty akun baru, Perlindungan Lambda sudah diaktifkan dan termasuk dalam periode uji coba 30 hari. Untuk informasi tentang statistik penggunaan, lihat [Memperkirakan biaya](#).

GuardDuty memantau log aktivitas jaringan yang dihasilkan dengan menjalankan fungsi Lambda. Saat ini, Pemantauan Aktivitas Jaringan Lambda mencakup log aliran VPC Amazon dari semua fungsi Lambda untuk akun Anda, termasuk log yang tidak VPC menggunakan jaringan, dan dapat berubah, termasuk ekspansi ke aktivitas jaringan lain DNS seperti data kueri yang dihasilkan dengan menjalankan fungsi Lambda. Ekspansi ke bentuk lain dari pemantauan aktivitas jaringan akan meningkatkan volume data yang GuardDuty akan diproses untuk Perlindungan Lambda. Ini akan berdampak langsung pada biaya penggunaan Perlindungan Lambda. Setiap kali GuardDuty mulai memantau log aktivitas jaringan tambahan, itu akan memberikan pemberitahuan ke akun yang telah mengaktifkan Perlindungan Lambda, setidaknya 30 hari sebelum rilis.

## Fitur dalam Perlindungan Lambda

### Pemantauan Aktivitas Jaringan Lambda

Saat Anda mengaktifkan Perlindungan Lambda, memantau log aktivitas jaringan GuardDuty Lambda yang dihasilkan saat fungsi Lambda yang terkait dengan akun Anda dipanggil. Ini membantu Anda



mendeteksi potensi ancaman keamanan terhadap fungsi Lambda. GuardDuty memantau log VPC aliran dari semua fungsi Lambda Anda, termasuk yang tidak menggunakan VPC jaringan. Untuk fungsi Lambda yang dikonfigurasi untuk menggunakan VPC jaringan, Anda tidak perlu mengaktifkan log VPC aliran untuk antarmuka jaringan elastis (ENI) yang dibuat oleh Lambda untuk. GuardDuty GuardDuty hanya mengenakan biaya untuk jumlah data log aktivitas jaringan Lambda yang diproses (dalam GB) untuk menghasilkan temuan. GuardDuty mengoptimalkan biaya dengan menerapkan filter pintar dan menganalisis subset log aktivitas jaringan Lambda yang relevan dengan deteksi ancaman. Untuk informasi tentang harga, lihat [GuardDuty harga Amazon](#).

GuardDuty tidak mengelola log aktivitas jaringan Lambda Anda (termasuk VPC dan log VPC non-aliran) atau membuatnya dapat diakses di akun Anda.

## Mengkonfigurasi Perlindungan Lambda

### Mengkonfigurasi Perlindungan Lambda untuk akun mandiri

Untuk akun yang terkait AWS Organizations, Anda dapat mengotomatiskan proses ini melalui GuardDuty konsol atau API instruksi, seperti yang dijelaskan di bagian berikutnya.

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Perlindungan Lambda untuk akun mandiri.


#### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.
3. Halaman Perlindungan Lambda menunjukkan status akun Anda saat ini. Anda dapat mengaktifkan atau menonaktifkan fitur kapan saja dengan memilih Aktifkan atau Nonaktifkan.
4. Pilih Simpan.

#### API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan features objek name sebagai LAMBDA\_NETWORK\_LOGS dan status sebagai ENABLED atau DISABLED.

Anda juga dapat mengaktifkan atau menonaktifkan Lambda Network Activity Monitoring dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan valid Anda sendiri *detector ID*.

 Note

Kode contoh berikut memungkinkan Lambda Network Activity Monitoring. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). `detectorId`

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

## Mengkonfigurasi Perlindungan Lambda di lingkungan multi-akun

Dalam lingkungan multi-akun, hanya akun GuardDuty administrator yang didelegasikan yang memiliki opsi untuk mengaktifkan atau menonaktifkan Perlindungan Lambda untuk akun anggota di organisasi mereka. Akun GuardDuty anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Akun GuardDuty administrator yang didelegasikan mengelola akun anggota menggunakan AWS Organizations. Akun GuardDuty administrator yang didelegasikan dapat memilih untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk semua akun baru saat mereka bergabung dengan organisasi. Untuk informasi selengkapnya tentang lingkungan multi-akun, lihat [Mengelola beberapa akun di Amazon GuardDuty](#).

Mengkonfigurasi Perlindungan Lambda untuk GuardDuty akun administrator yang didelegasikan

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun administrator yang didelegasikan GuardDuty .

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.  
Pastikan untuk menggunakan kredensi akun manajemen.
2. Di panel navigasi, di bawah Pengaturan, pilih Perlindungan Lambda.

3. Pada halaman Perlindungan Lambda, pilih Edit.
4. Lakukan salah satu hal berikut ini:

#### Menggunakan Aktifkan untuk semua akun

- Pilih Aktifkan untuk semua akun. Ini akan memungkinkan rencana perlindungan untuk semua GuardDuty akun aktif di AWS organisasi Anda, termasuk akun baru yang bergabung dengan organisasi.
- Pilih Simpan.

#### Menggunakan Konfigurasi akun secara manual

- Untuk mengaktifkan paket perlindungan hanya untuk akun akun GuardDuty administrator yang didelegasikan, pilih Konfigurasi akun secara manual.
- Pilih Aktifkan di bawah bagian akun GuardDuty administrator yang didelegasikan (akun ini).
- Pilih Simpan.

## API/CLI

Jalankan [updateDetector](#) API operasi menggunakan ID detektor regional Anda sendiri dan meneruskan `features` objek name sebagai `LAMBDA_NETWORK_LOGS` dan status sebagai `ENABLED` atau `DISABLED`.

Anda dapat mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda dengan menjalankan perintah berikut AWS CLI . Pastikan untuk menggunakan akun GuardDuty administrator yang didelegasikan yang valid *detector ID*.

### Note

Kode contoh berikut memungkinkan Lambda Network Activity Monitoring. Untuk menonaktifkannya, ganti `ENABLED` dengan `DISABLED`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-detector --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 555555555555 --features '[{"Name":  
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Aktifkan Pemantauan Aktivitas Jaringan Lambda secara otomatis untuk semua akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan fitur Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota. Ini termasuk akun anggota yang ada dan akun baru yang bergabung dengan organisasi.

## Console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

Menggunakan halaman Perlindungan Lambda

1. Di panel navigasi, pilih Perlindungan Lambda.
2. Pilih Aktifkan untuk semua akun. Tindakan ini secara otomatis memungkinkan Pemantauan Aktivitas Jaringan Lambda untuk akun yang ada dan baru di organisasi.
3. Pilih Simpan.

### Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi akun anggota.

Menggunakan halaman Akun

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis sebelum Tambahkan akun berdasarkan undangan.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk semua akun di bawah Pemantauan Aktivitas Jaringan Lambda.

**Note**

Secara default, tindakan ini secara otomatis mengaktifkan opsi Aktifkan otomatis GuardDuty untuk akun anggota baru.

#### 4. Pilih Simpan.

Jika Anda tidak dapat menggunakan opsi Aktifkan untuk semua akun, lihat [Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota](#).

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, panggil operasi menggunakan [updateMemberDetectors](#) API akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Untuk menonaktifkan akun anggota, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada di organisasi.

## Console

Untuk mengonfigurasi Pemantauan Aktivitas Jaringan Lambda untuk semua akun anggota aktif yang ada

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Masuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Perlindungan Lambda.
3. Pada halaman Perlindungan Lambda, Anda dapat melihat status konfigurasi saat ini. Di bawah bagian Akun anggota aktif, pilih Tindakan.
4. Dari menu tarik-turun Tindakan, pilih Aktifkan untuk semua akun anggota aktif yang ada.
5. Pilih Konfirmasi.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota Anda, panggil operasi menggunakan [updateMemberDetectors](#) API akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Untuk menonaktifkan akun anggota, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

## Aktifkan Pemantauan Aktivitas Jaringan Lambda secara otomatis untuk akun anggota baru

Pilih metode akses pilihan Anda untuk mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun baru yang bergabung dengan organisasi Anda.

### Console

Akun GuardDuty administrator yang didelegasikan dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru di organisasi, menggunakan halaman Perlindungan Lambda atau Akun.

Untuk mengaktifkan secara otomatis Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Lakukan salah satu hal berikut ini:

- Menggunakan halaman Perlindungan Lambda:

1. Di panel navigasi, pilih Perlindungan Lambda.
2. Pada halaman Perlindungan Lambda, pilih Edit.
3. Pilih Konfigurasi akun secara manual.
4. Pilih Aktifkan secara otomatis untuk akun anggota baru. Langkah ini memastikan bahwa setiap kali akun baru bergabung dengan organisasi Anda, Perlindungan Lambda akan diaktifkan secara otomatis untuk akun mereka. Hanya akun GuardDuty administrator yang didelegasikan organisasi yang dapat mengubah konfigurasi ini.
5. Pilih Simpan.

- Menggunakan halaman Akun:

1. Di panel navigasi, pilih Akun.
2. Pada halaman Akun, pilih Preferensi Aktifkan otomatis.
3. Di jendela Kelola preferensi aktifkan otomatis, pilih Aktifkan untuk akun baru di bawah Pemantauan Aktivitas Jaringan Lambda.
4. Pilih Simpan.

## API/CLI

- Untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda untuk akun anggota baru, jalankan [UpdateOrganizationConfiguration](#) API operasi menggunakan akun Anda sendiri *detector ID*.
- Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Untuk menonaktifkannya, lihat [Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota](#). Jika Anda tidak ingin mengaktifkannya untuk semua akun baru yang bergabung dengan organisasi, setel `AutoEnable` ke `NONE`.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

- Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

Aktifkan atau nonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota

Pilih metode akses pilihan Anda untuk mengaktifkan atau menonaktifkan Pemantauan Aktivitas Jaringan Lambda secara selektif untuk akun anggota.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, di bagian Pengaturan, pilih Akun.

Pada halaman Akun, tinjau kolom Pemantauan Aktivitas Jaringan Lambda. Ini menunjukkan apakah Pemantauan Aktivitas Jaringan Lambda diaktifkan atau tidak.

3. Pilih akun yang ingin Anda konfigurasi Perlindungan Lambda. Anda dapat memilih beberapa akun sekaligus.



4. Dari menu tarik-turun Edit Rencana Perlindungan, pilih Pemantauan Aktivitas Jaringan Lambda, lalu pilih tindakan yang sesuai.

## API/CLI

Memohon [updateMemberDetectors](#) API menggunakan milik Anda sendiri *detector ID*.

Contoh berikut menunjukkan bagaimana Anda dapat mengaktifkan Pemantauan Aktivitas Jaringan Lambda untuk satu akun anggota. Untuk menonaktifkannya, ganti ENABLED dengan DISABLED.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
"ENABLED"}]'
```

Anda juga dapat melewati daftar akun yang IDs dipisahkan oleh spasi.

Ketika kode telah berhasil dijalankan, daftar `UnprocessedAccounts` akan kembali kosong. Jika ada masalah dalam mengubah pengaturan detektor untuk suatu akun, ID akun tersebut akan dicantumkan bersama dengan ringkasan masalahnya.

# Melindungi beban kerja AI dengan GuardDuty

[Deteksi ancaman GuardDuty dasar](#) Amazon dan Perlindungan [Lambda](#) membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang dibangun dengan lebih baik. AWS

[Deteksi GuardDuty ancaman dasar memantau peristiwa AWS CloudTrail manajemen untuk mendeteksi aktivitas mencurigakan dan berbahaya dalam beban kerja AI generatif yang dibuat dengan menggunakan layanan AWS , termasuk Amazon Bedrock dan Amazon SageMaker](#)

Misalnya, GuardDuty dapat mengidentifikasi kegiatan seperti:

- Penghapusan pagar keamanan Amazon Bedrock yang tidak biasa
- Perubahan sumber data pelatihan model yang berpotensi menyebabkan serangan keracunan data
- Pemanggilan model Amazon Bedrock yang mencurigakan
- Contoh buku catatan yang tidak biasa atau pelatihan penciptaan lapangan kerja di SageMaker
- Kredensi Amazon Elastic Compute Cloud yang diekstraksi yang mungkin telah digunakan untuk menelepon di APIs Amazon Bedrock, Amazon, atau beban kerja AI yang dikelola sendiri pada instans SageMaker, cluster, atau tugas. EC2 EKS ECS

GuardDuty Lambda Protection dapat membantu mendeteksi potensi ancaman terkait agen Amazon Bedrock. Ini mungkin termasuk aktivitas jaringan yang mencurigakan seperti cryptomining, dan berkomunikasi dengan server perintah dan kontrol berbahaya yang dapat disebabkan oleh serangan rantai pasokan atau dorongan kompleks.

Video berikut menunjukkan bagaimana temuan terkait akan terlihat.

Video berikut menunjukkan bagaimana temuan terkait akan terlihat. [Menggunakan Amazon GuardDuty untuk memantau dan mengamankan beban kerja AI Anda AWS](#)

# Mengelola banyak akun di Amazon GuardDuty

Ketika AWS lingkungan Anda memiliki beberapa akun, Anda dapat mengelolanya dengan menunjuk satu Akun AWS sebagai akun administrator. Anda kemudian dapat mengaitkan beberapa Akun AWS dengan akun administrator ini sebagai akun anggotanya. Dengan konfigurasi ini, akun GuardDuty administrator yang ditunjuk dapat menilai dan memantau keamanan keseluruhan organisasi Anda. Akun administrator juga dapat melakukan tugas manajemen akun, seperti meninjau semua temuan yang dihasilkan dan mengonfigurasi rencana perlindungan di dalamnya. GuardDuty

Dalam GuardDuty, organisasi terdiri dari akun GuardDuty administrator yang didelegasikan dan satu atau lebih akun anggota terkait. Anda dapat mengaitkan akun dengan dua cara — dengan mengintegrasikan dengan AWS Organizations, atau dengan menggunakan metode lama untuk mengirim dan menerima undangan keanggotaan di konsol. GuardDuty GuardDuty merekomendasikan agar Anda berintegrasi dengan AWS Organizations.

AWS Organizations adalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa secara terpusat. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan dan terintegrasi dengan beberapa AWS layanan, termasuk Macie, AWS Security Hub, dan Amazon. GuardDuty Untuk informasi selengkapnya, lihat [Panduan Pengguna AWS Organizations](#).

## Daftar Isi

- [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#)
- [Mengelola GuardDuty akun dengan AWS Organizations](#)
- [Mengelola GuardDuty akun dengan undangan](#)

## Memahami hubungan antara akun GuardDuty administrator dan akun anggota

Saat Anda menggunakan GuardDuty di lingkungan beberapa akun, akun administrator dapat mengelola aspek-aspek tertentu GuardDuty atas nama akun anggota. Akun administrator dapat melakukan fungsi utama berikut:

- Menambahkan dan menghapus akun anggota terkait. Proses di mana akun administrator dapat melakukan ini berbeda berdasarkan cara Anda mengelola akun — melalui organisasi atau dengan undangan.
- Akun GuardDuty administrator yang didelegasikan mengaktifkan akun GuardDuty manajemen

Jika akun AWS Organizations manajemen pernah dinonaktifkan GuardDuty, akun GuardDuty administrator yang didelegasikan dapat diaktifkan GuardDuty di akun manajemen. Namun, diperlukan bahwa akun manajemen harus belum secara eksplisit menghapus. [Izin peran terkait layanan untuk GuardDuty](#)

- Mengelola status GuardDuty dalam akun anggota terkait, termasuk mengaktifkan dan menanggihkan GuardDuty.

#### Note

Akun administrator yang didelegasikan dikelola dengan mengaktifkan AWS Organizations secara otomatis GuardDuty di akun yang ditambahkan sebagai anggota.

- Sesuaikan temuan dalam GuardDuty jaringan melalui pembuatan dan pengelolaan aturan penindasan, daftar IP terpercaya, dan daftar ancaman. Dalam lingkungan multi-akun, konfigurasi fitur ini hanya tersedia untuk akun administrator yang GuardDuty didelegasikan. Akun anggota tidak dapat memperbarui konfigurasi ini.

Tabel berikut merinci hubungan antara akun GuardDuty administrator dan akun anggota.

Dalam tabel ini:

- Self — Akun dapat melakukan tindakan yang terdaftar hanya untuk akun mereka sendiri.
- Apa saja — Akun dapat melakukan tindakan yang tercantum untuk akun terkait apa pun.
- Semua — Akun dapat melakukan tindakan yang tercantum dan berlaku untuk semua akun terkait. Biasanya, akun yang mengambil tindakan ini adalah akun GuardDuty administrator yang ditunjuk

Sel tabel dengan tanda hubung (-) menunjukkan bahwa akun tidak dapat melakukan tindakan yang tercantum.

|      |                           |                 |
|------|---------------------------|-----------------|
| Aksi | Melalui AWS Organizations | Dengan undangan |
|------|---------------------------|-----------------|

|  | Akun GuardDuty administrator yang didelegasikan | Akun anggota terkait | Akun GuardDuty administrator yang didelegasikan | Akun anggota terkait |
|--|---|----------------------|---|----------------------|
| Aktifkan GuardDuty   | Setiap  | –                    | Mandiri   | Mandiri              |
| Aktifkan GuardDuty secara otomatis untuk seluruh organisasi (ALL,NEW,NONE) | Semua   | –                    | –   | –                    |
| Lihat semua akun anggota Organizations terlepas dari GuardDuty statusnya   | Setiap  | –                    | –   | –                    |
| Membuat temuan sampel  | Mandiri   | Mandiri              | Mandiri   | Mandiri              |
| Lihat semua GuardDuty temuan   | Setiap  | Mandiri              | Setiap  | Mandiri              |
| GuardDuty Temuan arsip   | Setiap  | –                    | Setiap  | –                    |
| Menerapkan aturan penekanan  | Semua   | –                    | Semua   | –                    |

|  |       |   |       |              |
|--|-------|---|-------|--------------|
| Buat daftar IP tepercaya atau daftar ancaman   | Semua | – | Semua | –            |
| Perbarui daftar IP tepercaya atau daftar ancaman   | Semua | – | Semua | –            |
| Hapus daftar IP tepercaya atau daftar ancaman  | Semua | – | Semua | –            |
| Atur frekuensi EventBridge notifikasi  | Semua | – | Semua | Diri Sendiri |
| Mengatur lokasi Amazon S3 untuk mengekspor temuan  | Semua | – | Semua | Diri Sendiri |
| Aktifkan satu atau lebih rencana perlindungan opsional untuk seluruh organisasi (ALL,NEW,NONE) | Semua | – | –     | –            |
| Ini tidak termasuk Perlindungan Malware untuk S3.  |       |   |       |              |

|  |             |                   |             |         |
|--|-------------|-------------------|-------------|---------|
| Aktifkan paket GuardDuty perlindungan apa pun untuk akun individu                    | Setiap      | –                 | Setiap      | –       |
| Ini tidak termasuk Perlindungan Malware untuk EC2 dan Perlindungan Malware untuk S3. |             |                   |             |         |
| Perlindungan Malware untuk EC2   | Setiap      | –                 | Mandiri     | Mandiri |
| Perlindungan Malware untuk S3  | –           | Mandiri           | –           | Mandiri |
| Putuskan hubungan akun anggota   | Setiap      | –                 | Setiap      | –       |
| Putuskan hubungan dari akun administrator  | –           | Diri <sup>+</sup> | –           | Mandiri |
| Menghapus akun anggota yang tidak terkait  | Setiap      | –                 | Setiap      | –       |
| Menangguhkan GuardDuty   | * Apa saja* | –                 | * Apa saja* | –       |

|                          |             |   |             |   |
|--------------------------|-------------|---|-------------|---|
| Nonaktifkan<br>GuardDuty | * Apa saja* | – | * Apa saja* | – |
|--------------------------|-------------|---|-------------|---|

<sup>+</sup> Menunjukkan bahwa akun dapat mengambil tindakan ini hanya jika akun GuardDuty administrator yang didelegasikan belum menyiapkan preferensi aktifkan otomatis ke ALL anggota organisasi.

\* Menunjukkan bahwa akun GuardDuty administrator yang didelegasikan tidak dapat menonaktifkan GuardDuty di akun anggota secara langsung. Akun GuardDuty administrator yang didelegasikan harus terlebih dahulu memisahkan akun anggota, dan kemudian menghapusnya. Setelah ini, setiap akun anggota dapat menonaktifkan GuardDuty di akun mereka sendiri. Untuk informasi selengkapnya tentang melakukan tugas-tugas ini di organisasi Anda, lihat [Mempertahankan organisasi Anda di dalam GuardDuty](#).

## Mengelola GuardDuty akun dengan AWS Organizations

Dalam suatu AWS organisasi, akun manajemen dapat menunjuk akun apa pun dalam organisasi ini sebagai akun GuardDuty administrator yang didelegasikan. Untuk akun administrator ini, GuardDuty akan diaktifkan secara otomatis hanya di saat ini Wilayah AWS. Secara default, akun administrator dapat mengaktifkan dan mengelola GuardDuty semua akun anggota di organisasi dalam Wilayah tersebut. Akun administrator dapat melihat dan menambahkan anggota ke AWS organisasi ini.

Bagian berikut akan memandu Anda melalui berbagai tugas yang dapat Anda lakukan sebagai akun GuardDuty administrator yang didelegasikan.

### Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations

Pertimbangan dan rekomendasi berikut dapat membantu Anda memahami cara operasi akun GuardDuty administrator yang didelegasikan: GuardDuty

Akun GuardDuty administrator yang didelegasikan dapat mengelola maksimal 50.000 anggota.

Ada batas 50.000 akun anggota per akun GuardDuty administrator yang didelegasikan. Ini termasuk akun anggota yang ditambahkan melalui AWS Organizations atau mereka yang menerima undangan akun GuardDuty administrator untuk bergabung dengan organisasi mereka. Namun, mungkin ada lebih dari 50.000 akun di AWS organisasi Anda.



Jika Anda melebihi batas 50.000 akun anggota, Anda akan menerima pemberitahuan dari CloudWatch, AWS Health Dashboard, dan email ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.

Akun GuardDuty administrator yang didelegasikan adalah Regional.

Tidak seperti AWS Organizations, GuardDuty adalah layanan Regional. Akun GuardDuty administrator yang didelegasikan dan akun anggotanya harus ditambahkan AWS Organizations di setiap Wilayah yang diinginkan tempat Anda telah GuardDuty mengaktifkan. Jika akun manajemen organisasi menunjuk akun GuardDuty administrator yang didelegasikan hanya di AS Timur (Virginia N.), maka akun GuardDuty administrator yang didelegasikan hanya akan mengelola akun anggota yang ditambahkan ke organisasi di Wilayah tersebut. Untuk informasi selengkapnya tentang paritas fitur di Wilayah GuardDuty yang tersedia, lihat [Wilayah dan titik akhir](#).

Kasus khusus untuk Wilayah keikutsertaan

- Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan. [ListMembersAPI](#)
- Saat bekerja dengan konfigurasi GuardDuty aktifkan otomatis yang disetel keNEW, pastikan urutan berikut terpenuhi:
  1. Akun anggota ikut serta ke Wilayah keikutsertaan.
  2. Tambahkan akun anggota ke organisasi Anda di AWS Organizations.

Jika Anda mengubah urutan langkah-langkah ini, pengaturan GuardDuty aktifkan otomatis dengan tidak **NEW** akan berfungsi di Wilayah keikutsertaan tertentu karena akun anggota tidak lagi baru bagi organisasi. GuardDuty menyediakan dua solusi alternatif:

- Setel konfigurasi GuardDuty aktifkan otomatis keALL, yang mencakup akun anggota baru dan yang sudah ada. Dalam hal ini, urutan langkah-langkah ini tidak relevan.
- Jika akun anggota sudah menjadi bagian dari organisasi Anda, kelola GuardDuty konfigurasi untuk akun ini secara individual di Wilayah keikutsertaan tertentu dengan menggunakan GuardDuty konsol atau akun. API

Diperlukan agar AWS organisasi memiliki akun GuardDuty administrator yang didelegasikan yang sama di semua akun. Wilayah AWS

Anda harus menetapkan satu akun anggota sebagai akun GuardDuty administrator yang didelegasikan di semua Wilayah AWS tempat GuardDuty diaktifkan. Misalnya, jika Anda menunjuk akun anggota **111122223333** in *Europe (Ireland)*, Anda tidak dapat menunjuk akun anggota lain **555555555555** in *Canada (Central)*. Anda harus menggunakan akun yang sama dengan akun GuardDuty administrator yang didelegasikan di semua Wilayah lainnya.

Anda dapat menunjuk akun GuardDuty administrator yang didelegasikan baru kapan saja. Untuk informasi selengkapnya tentang menghapus akun GuardDuty administrator terdelegasi yang ada, lihat [Mengubah akun GuardDuty administrator yang didelegasikan](#).

Tidak disarankan untuk menetapkan akun manajemen organisasi Anda sebagai akun GuardDuty administrator yang didelegasikan.

Akun manajemen organisasi Anda dapat berupa akun GuardDuty administrator yang didelegasikan. Namun, praktik terbaik AWS keamanan mengikuti prinsip hak istimewa paling sedikit dan tidak merekomendasikan konfigurasi ini.

Mengubah akun GuardDuty administrator yang didelegasikan tidak menonaktifkan GuardDuty akun anggota.

Jika Anda menghapus akun GuardDuty administrator yang didelegasikan, GuardDuty hapus semua akun anggota yang terkait dengan akun GuardDuty administrator yang didelegasikan ini. GuardDuty masih tetap diaktifkan untuk semua akun anggota ini.

## Izin yang diperlukan untuk menunjuk akun administrator yang didelegasikan GuardDuty

Untuk mulai menggunakan Amazon GuardDuty dengan AWS Organizations, akun AWS Organizations manajemen untuk organisasi menetapkan akun sebagai akun GuardDuty administrator yang didelegasikan. Ini memungkinkan GuardDuty sebagai layanan tepercaya di AWS Organizations. Ini juga memungkinkan GuardDuty akun GuardDuty administrator yang didelegasikan dan juga memungkinkan akun administrator yang didelegasikan untuk mengaktifkan dan mengelola GuardDuty akun lain di organisasi di Wilayah saat ini. Untuk informasi tentang cara izin ini diberikan, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

Sebagai akun AWS Organizations manajemen, sebelum Anda menetapkan akun GuardDuty administrator yang didelegasikan untuk organisasi Anda, verifikasi bahwa Anda dapat melakukan

GuardDuty tindakan berikut: `guardduty:EnableOrganizationAdminAccount` Tindakan ini memungkinkan Anda untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda dengan menggunakan GuardDuty Anda juga harus memastikan bahwa Anda diizinkan untuk melakukan AWS Organizations tindakan yang membantu Anda mengambil informasi tentang organisasi Anda.

Untuk memberikan izin ini, sertakan pernyataan berikut dalam kebijakan AWS Identity and Access Management (IAM) untuk akun Anda:

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}
```

Jika Anda ingin menetapkan akun AWS Organizations manajemen Anda sebagai akun GuardDuty administrator yang didelegasikan, akun Anda juga akan memerlukan IAM tindakan: `CreateServiceLinkedRole` Tindakan ini memungkinkan Anda untuk menginisialisasi GuardDuty untuk akun manajemen. Namun, tinjau [Pertimbangan dan rekomendasi untuk digunakan dengan GuardDuty AWS Organizations](#) sebelum Anda melanjutkan untuk menambahkan izin.

Untuk melanjutkan penunjukan akun manajemen sebagai akun GuardDuty administrator yang didelegasikan, tambahkan pernyataan berikut ke IAM kebijakan dan ganti `111122223333` dengan Akun AWS ID akun manajemen organisasi Anda:

```
{
  "Sid": "PermissionsToEnableGuardDuty"
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ]
}
```

```
],
  "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "guardduty.amazonaws.com"
    }
  }
}
```

## Menunjuk akun administrator yang didelegasikan GuardDuty

Pilih metode akses yang disukai untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk organisasi Anda. Hanya akun manajemen yang dapat melakukan langkah ini.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensi akun manajemen untuk organisasi Anda AWS Organizations .

2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin menunjuk akun administrator yang didelegasikan GuardDuty untuk organisasi Anda.
3. Lakukan salah satu hal berikut, tergantung pada apakah GuardDuty diaktifkan untuk akun manajemen Anda di Wilayah saat ini:
  - Jika GuardDuty diaktifkan, pilih Amazon GuardDuty - semua fitur dan pilih Memulai. Tindakan ini akan membawa Anda ke GuardDuty halaman Selamat Datang di.
  - Jika GuardDuty diaktifkan, pilih Pengaturan di panel navigasi.
4. Di bawah Administrator yang didelegasikan, masukkan Akun AWS ID 12 digit akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan untuk organisasi.

Pastikan GuardDuty untuk mengaktifkan akun GuardDuty administrator delegasi yang baru ditunjuk, jika tidak maka tidak akan dapat mengambil tindakan apa pun.

5. Pilih Delegasikan.
6. (Disarankan) Ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan GuardDuty

## API/CLI

1. Jalankan [enableOrganizationAdminAccount](#) menggunakan kredensi Akun AWS akun manajemen organisasi.
  - Atau, Anda dapat menggunakan AWS Command Line Interface untuk melakukan ini. AWS CLI Perintah berikut menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah Anda saat ini saja. Jalankan AWS CLI perintah berikut dan pastikan untuk mengganti `111111111111` dengan Akun AWS ID akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator yang didelegasikan:

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Untuk menunjuk akun GuardDuty administrator yang didelegasikan untuk Wilayah lain, tentukan Wilayah dalam perintah. AWS CLI Contoh berikut menunjukkan cara mengaktifkan akun GuardDuty administrator yang didelegasikan di AS Barat (Oregon). Pastikan untuk mengganti `us-west-2` dengan Wilayah yang ingin Anda tetapkan akun GuardDuty administrator yang didelegasikan.

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Untuk informasi tentang Wilayah AWS tempat GuardDuty tersedia, lihat [Wilayah dan titik akhir](#).

Jika tidak GuardDuty diaktifkan untuk akun GuardDuty administrator yang didelegasikan, akun tersebut tidak akan dapat mengambil tindakan apa pun. Jika belum dilakukan, pastikan GuardDuty untuk mengaktifkan akun GuardDuty administrator delegasi yang baru ditunjuk.

2. (Disarankan) ulangi langkah-langkah sebelumnya untuk menunjuk akun GuardDuty administrator yang didelegasikan di setiap Wilayah AWS tempat yang telah Anda aktifkan GuardDuty

## Memperbarui preferensi mengaktifkan otomatis organisasi

Fitur mengaktifkan otomatis organisasi di GuardDuty membantu Anda mengatur status paket perlindungan yang sama GuardDuty untuk akun ALL yang ada atau NEW anggota di organisasi Anda, dalam satu langkah. Demikian pula, Anda juga dapat menentukan kapan Anda tidak ingin mengambil

tindakan apa pun pada akun anggota, dengan memilih NEW. Langkah-langkah berikut menjelaskan pengaturan ini dan juga menunjukkan kapan Anda ingin menggunakan pengaturan tertentu.

Pilih metode akses yang disukai untuk memperbarui preferensi aktifkan otomatis untuk organisasi.

## Console

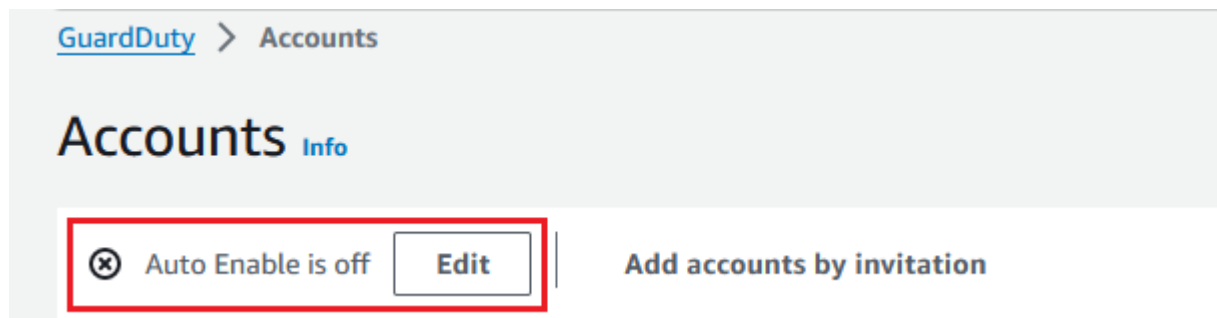
1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan GuardDuty kredensial akun administrator.

2. Di panel navigasi, pilih Akun.

Halaman Akun menyediakan opsi konfigurasi ke akun GuardDuty administrator untuk Aktifkan otomatis GuardDuty dan paket perlindungan opsional atas nama akun anggota milik organisasi.

3. Untuk memperbarui pengaturan aktifkan otomatis yang ada, pilih Edit.



Dukungan ini tersedia untuk dikonfigurasi GuardDuty dan semua paket perlindungan opsional yang didukung di Anda Wilayah AWS. Anda dapat memilih salah satu opsi konfigurasi berikut untuk GuardDuty atas nama akun anggota Anda:


- Aktifkan untuk semua akun (**ALL**) — Pilih untuk mengaktifkan opsi yang sesuai untuk semua akun dalam suatu organisasi. Ini termasuk akun baru yang bergabung dengan organisasi dan akun yang mungkin telah ditangguhkan atau dihapus dari organisasi. Ini juga termasuk akun GuardDuty administrator yang didelegasikan.

### Note

Diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

- Aktifkan otomatis untuk akun baru (**NEW**) — Pilih untuk mengaktifkan GuardDuty atau paket perlindungan opsional hanya untuk akun anggota baru secara otomatis saat mereka bergabung dengan organisasi Anda.
- Jangan aktifkan (**NONE**) — Pilih untuk mencegah mengaktifkan opsi yang sesuai untuk akun baru di organisasi Anda. Dalam hal ini, akun GuardDuty administrator akan mengelola setiap akun secara individual.

Saat Anda memperbarui pengaturan aktifkan otomatis dari ALL atau NEW ke NONE, tindakan ini tidak menonaktifkan opsi terkait untuk akun Anda yang ada. Konfigurasi ini akan berlaku untuk akun baru yang bergabung dengan organisasi. Setelah Anda memperbarui pengaturan aktifkan otomatis, tidak ada akun baru yang akan memiliki opsi yang sesuai sebagaimana diaktifkan.

 Note

Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan [ListMembersAPI](#)

4. Pilih Simpan perubahan.
5. (Opsional) jika Anda ingin menggunakan preferensi yang sama di setiap Wilayah, perbarui preferensi Anda di setiap Wilayah yang didukung secara terpisah.

Beberapa paket perlindungan opsional mungkin tidak tersedia di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).


## API/CLI

1. Jalankan [UpdateOrganizationConfiguration](#) dengan menggunakan kredensial akun GuardDuty administrator yang didelegasikan, untuk secara otomatis mengonfigurasi GuardDuty dan rencana perlindungan opsional di Wilayah tersebut untuk organisasi Anda. [Untuk informasi tentang berbagai konfigurasi auto-enable, lihat autoEnableOrganization Anggota.](#)

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/>konsol, atau jalankan [ListDetectors](#)API. `detectorId`

Untuk mengatur preferensi aktifkan otomatis untuk salah satu paket perlindungan opsional yang didukung di Wilayah Anda, ikuti langkah-langkah yang disediakan di bagian dokumentasi terkait dari setiap paket perlindungan.

2. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan [describeOrganizationConfiguration](#). Pastikan untuk menentukan ID detektor dari akun GuardDuty administrator yang didelegasikan.

 Note

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota.

1. Atau, jalankan AWS CLI perintah berikut untuk mengatur preferensi agar mengaktifkan atau menonaktifkan secara otomatis GuardDuty di Region untuk akun baru (NEW) yang bergabung dengan organisasi, semua akun (ALL), atau tidak ada akun (NONE) di organisasi. Untuk informasi selengkapnya, lihat [autoEnableOrganizationAnggota](#). Berdasarkan preferensi Anda, Anda mungkin perlu mengganti NEW dengan ALL atau NONE. Jika Anda mengonfigurasi paket perlindungan dengan ALL, paket perlindungan juga akan diaktifkan untuk akun GuardDuty administrator yang didelegasikan. Pastikan untuk menentukan ID detektor akun GuardDuty administrator yang didelegasikan yang mengelola konfigurasi organisasi.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/>konsol, atau jalankan [ListDetectors](#)API. `detectorId`


```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. Anda dapat memvalidasi preferensi untuk organisasi Anda di Wilayah saat ini. Jalankan AWS CLI perintah berikut dengan menggunakan ID detektor dari akun GuardDuty administrator yang didelegasikan.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```



(Disarankan) ulangi langkah sebelumnya di setiap Wilayah dengan menggunakan ID detektor akun GuardDuty administrator yang didelegasikan.

 Note

Ketika akun GuardDuty administrator yang didelegasikan memilih keluar dari Wilayah keikutsertaan, meskipun organisasi Anda memiliki konfigurasi GuardDuty aktifkan otomatis yang disetel ke akun anggota baru saja (NEW) atau semua akun anggota (ALL), GuardDuty tidak dapat diaktifkan untuk akun anggota mana pun di organisasi yang saat ini telah dinonaktifkan. GuardDuty Untuk informasi tentang konfigurasi akun anggota Anda, buka Akun di panel navigasi [GuardDuty konsol](#) atau gunakan [ListMembersAPI](#)

## Menambahkan anggota ke organisasi

Pilih metode akses yang disukai untuk menambahkan anggota ke organisasi Anda.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.

Tabel akun menampilkan semua akun yang ditambahkan melalui Organizations (AWS Organizations) atau By Invitation. Jika akun anggota tidak terkait dengan akun GuardDuty administrator organisasi, Status akun anggota ini bukan anggota.

3. Pilih satu atau beberapa akun IDs yang ingin Anda tambahkan sebagai anggota. Akun ini IDs harus memiliki Type as Via Organizations.

Akun yang ditambahkan melalui undangan bukan bagian dari organisasi Anda. Anda dapat mengelola akun tersebut secara individual. Untuk informasi selengkapnya, lihat [Mengelola akun dengan undangan](#).

4. Pilih dropdown Tindakan dan kemudian pilih Tambah anggota. Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku. Berdasarkan pengaturan di [Memperbarui preferensi mengaktifkan otomatis organisasi](#), GuardDuty konfigurasi akun ini dapat berubah.

5. Anda dapat memilih panah bawah kolom Status untuk mengurutkan akun berdasarkan status Bukan anggota dan kemudian memilih setiap akun yang belum GuardDuty diaktifkan di Wilayah saat ini.

Jika tidak ada akun yang tercantum dalam tabel akun yang telah ditambahkan sebagai anggota, Anda dapat mengaktifkan GuardDuty di Wilayah saat ini untuk semua akun organisasi. Pilih Aktifkan di spanduk di bagian atas halaman. Tindakan ini secara otomatis mengaktifkan GuardDuty konfigurasi Auto-enable sehingga GuardDuty diaktifkan untuk setiap akun baru yang bergabung dengan organisasi.

6. Pilih Konfirmasi untuk menambahkan akun sebagai anggota. Tindakan ini juga memungkinkan GuardDuty untuk semua akun yang dipilih. Status akun akan berubah menjadi Diaktifkan.
7. (Disarankan) Ulangi langkah-langkah ini di masing-masing Wilayah AWS. Ini memastikan bahwa akun GuardDuty administrator yang didelegasikan dapat mengelola temuan dan konfigurasi lain untuk akun anggota di semua Wilayah yang telah GuardDuty Anda aktifkan.

Fitur auto-enable memungkinkan GuardDuty untuk semua anggota masa depan organisasi Anda. Ini memungkinkan akun GuardDuty administrator yang didelegasikan untuk mengelola anggota baru yang dibuat di dalam atau ditambahkan ke organisasi. Ketika jumlah akun anggota mencapai batas 50.000, fitur Auto-enable secara otomatis dimatikan. Jika Anda menghapus akun anggota dan jumlah total anggota berkurang menjadi kurang dari 50.000, fitur Auto-enable akan diaktifkan kembali.

## API/CLI

- Jalankan [CreateMembers](#) dengan menggunakan kredensi akun GuardDuty administrator yang didelegasikan yang ditunjuk pada langkah sebelumnya.

Anda harus menentukan ID detektor regional dari akun GuardDuty administrator yang didelegasikan dan detail akun (Akun AWS ID dan alamat email yang sesuai) dari akun yang ingin Anda tambahkan sebagai GuardDuty anggota. Anda dapat membuat satu atau lebih anggota dengan API operasi ini.

Ketika Anda menjalankan `CreateMembers` di organisasi Anda, preferensi mengaktifkan otomatis untuk anggota baru akan berlaku saat akun anggota baru bergabung dengan organisasi Anda. Ketika Anda menjalankan `CreateMembers` dengan akun anggota yang ada,

konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Jalankan [ListAccounts](#) di AWS Organizations API Referensi, untuk melihat semua akun di AWS organisasi.

**⚠ Important**

Ketika Anda menambahkan akun sebagai GuardDuty anggota, itu akan secara otomatis GuardDuty diaktifkan di Wilayah itu. Ada pengecualian untuk akun manajemen organisasi. Sebelum akun manajemen ditambahkan sebagai GuardDuty anggota, itu harus GuardDuty diaktifkan.

- Atau, Anda dapat menggunakan AWS Command Line Interface. Jalankan AWS CLI perintah berikut dan pastikan untuk menggunakan ID detektor valid Anda sendiri, Akun AWS ID, dan alamat email yang terkait dengan ID akun.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Anda dapat melihat daftar semua anggota organisasi dengan menjalankan AWS CLI perintah berikut:

```
aws organizations list-accounts
```

Setelah Anda menambahkan akun ini sebagai anggota, GuardDuty konfigurasi auto-enable akan berlaku.

## (Opsional) Aktifkan paket perlindungan untuk akun anggota yang ada

Prosedur berikut mencakup langkah-langkah untuk mengaktifkan rencana perlindungan untuk akun anggota yang ada dengan menggunakan halaman Akun. Untuk langkah-langkah untuk melakukan ini

dengan menggunakan API atau AWS CLI, lihat dokumen yang terkait dengan rencana perlindungan tertentu.

Anda dapat mengaktifkan paket perlindungan untuk masing-masing akun melalui halaman Akun.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Gunakan kredensi akun GuardDuty administrator yang didelegasikan.

2. Di panel navigasi, pilih Akun.
3. Pilih satu atau beberapa akun yang ingin Anda konfigurasi paket perlindungannya. Ulangi langkah-langkah berikut untuk setiap paket perlindungan yang ingin Anda konfigurasi:
  - a. Pilih Edit Paket Perlindungan.
  - b. Dari daftar rencana perlindungan, pilih satu paket perlindungan yang ingin Anda konfigurasi.
  - c. Pilih salah satu tindakan yang ingin Anda lakukan untuk paket perlindungan ini, lalu pilih Konfirmasi.
  - d. Untuk akun yang dipilih, kolom yang sesuai dengan paket perlindungan yang dikonfigurasi akan menampilkan konfigurasi yang diperbarui sebagai Diaktifkan atau Tidak diaktifkan.

## Mempertahankan organisasi Anda di dalam GuardDuty

Sebagai akun GuardDuty administrator yang didelegasikan, Anda bertanggung jawab untuk menjaga konfigurasi GuardDuty dan rencana perlindungan opsionalnya untuk semua akun di organisasi Anda di setiap yang didukung Wilayah AWS. Bagian berikut memberikan opsi tentang mempertahankan status konfigurasi GuardDuty atau salah satu rencana perlindungan opsionalnya:

Untuk mempertahankan status konfigurasi seluruh organisasi Anda di setiap Wilayah

- Setel preferensi aktifkan otomatis untuk seluruh organisasi dengan menggunakan GuardDuty konsol — Anda dapat mengaktifkan GuardDuty secara otomatis untuk semua (ALL) anggota dalam organisasi atau anggota baru (NEW) yang bergabung dengan organisasi, atau memilih untuk tidak mengaktifkan secara otomatis salah satu anggota dalam organisasi. NONE

Anda juga dapat mengonfigurasi pengaturan yang sama atau berbeda untuk salah satu paket perlindungan di dalamnya GuardDuty.

Mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota di organisasi.

- Perbarui preferensi aktifkan otomatis dengan menggunakan API — Jalankan [UpdateOrganizationConfiguration](#) untuk mengonfigurasi secara otomatis GuardDuty dan rencana perlindungan opsionalnya untuk organisasi. Ketika Anda menjalankan [CreateMembers](#) untuk menambahkan akun anggota baru di organisasi Anda, pengaturan yang dikonfigurasi akan berlaku secara otomatis. Ketika Anda menjalankan [CreateMembers](#) dengan akun anggota yang ada, konfigurasi organisasi juga akan berlaku untuk anggota yang ada. Ini mungkin mengubah konfigurasi akun anggota yang ada saat ini.

Untuk melihat semua akun di organisasi Anda, jalankan [ListAccounts](#) di AWS Organizations API Referensi.

Untuk mempertahankan status konfigurasi untuk akun anggota secara individual di setiap Wilayah

- Untuk melihat semua akun di organisasi Anda, jalankan [ListAccounts](#) di AWS Organizations API Referensi.
- Jika Anda ingin akun anggota selektif memiliki status konfigurasi yang berbeda, jalankan [UpdateMemberDetectors](#) untuk setiap akun anggota satu per satu.

Anda dapat menggunakan GuardDuty konsol untuk melakukan tugas yang sama dengan menavigasi ke halaman Akun di GuardDuty konsol.

Untuk informasi tentang mengaktifkan paket perlindungan untuk masing-masing akun dengan menggunakan konsol atau API, lihat halaman konfigurasi untuk paket perlindungan terkait.

## Mengubah akun GuardDuty administrator yang didelegasikan

Anda dapat mengubah akun GuardDuty administrator yang didelegasikan untuk organisasi Anda di setiap Wilayah dan kemudian mendelegasikan administrator baru di setiap Wilayah. Untuk menjaga postur keamanan akun anggota organisasi Anda di Wilayah, Anda harus memiliki akun GuardDuty administrator yang didelegasikan di Wilayah tersebut.

## Menghapus akun GuardDuty administrator yang didelegasikan yang ada

Langkah 1 - Untuk menghapus akun GuardDuty administrator yang didelegasikan yang ada di setiap Wilayah

1. Sebagai akun GuardDuty administrator yang didelegasikan, cantumkan semua akun anggota yang terkait dengan akun administrator Anda. Jalankan [ListMembers](#) dengan `onlyAssociated=false`.
2. Jika preferensi aktifkan otomatis untuk GuardDuty atau salah satu paket perlindungan opsional disetel ke ALL, jalankan [UpdateOrganizationConfiguration](#) untuk memperbarui konfigurasi organisasi ke salah satu NEW atau NONE. Tindakan ini akan mencegah kesalahan saat Anda memisahkan semua akun anggota di langkah berikutnya.
3. Jalankan [DisassociateMembers](#) untuk memisahkan semua akun anggota yang terkait dengan akun administrator.
4. Jalankan [DeleteMembers](#) untuk menghapus asosiasi antara akun administrator dan akun anggota.
5. Sebagai akun manajemen organisasi, jalankan [DisableOrganizationAdminAccount](#) untuk menghapus akun GuardDuty administrator yang didelegasikan yang ada.
6. Ulangi langkah-langkah ini di setiap Wilayah AWS tempat Anda memiliki akun GuardDuty administrator yang didelegasikan ini.

Langkah 2 - Untuk membatalkan pendaftaran akun GuardDuty administrator yang didelegasikan yang ada di AWS Organizations (Tindakan global satu kali)

- Jalankan [DeregisterDelegatedAdministrator](#) di AWS Organizations API Referensi, untuk membatalkan pendaftaran akun GuardDuty administrator yang didelegasikan yang ada di AWS Organizations

Atau, Anda dapat menjalankan AWS CLI perintah berikut:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --  
service-principal guardduty.amazonaws.com
```

Pastikan untuk mengganti **111122223333** dengan akun GuardDuty administrator yang didelegasikan yang ada.

Setelah Anda membatalkan pendaftaran akun GuardDuty administrator lama yang didelegasikan, Anda dapat menambahkannya sebagai akun anggota ke akun administrator yang didelegasikan GuardDuty baru.

## Menunjuk akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah

1. Tentukan akun GuardDuty administrator baru yang didelegasikan di setiap Wilayah dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API. AWS CLI Untuk informasi selengkapnya, lihat [Menunjuk akun administrator yang didelegasikan GuardDuty](#).
2. Jalankan [DescribeOrganizationConfiguration](#) untuk melihat konfigurasi aktifkan otomatis saat ini untuk organisasi Anda.

### Important

Sebelum menambahkan anggota ke akun GuardDuty administrator yang didelegasikan baru, Anda harus memverifikasi konfigurasi aktifkan otomatis untuk organisasi Anda. Konfigurasi ini khusus untuk akun GuardDuty administrator yang didelegasikan baru dan Wilayah yang dipilih, dan tidak terkait AWS Organizations dengan. Saat Anda menambahkan akun anggota organisasi (baru atau yang sudah ada) di bawah akun GuardDuty administrator yang didelegasikan baru, konfigurasi aktifkan otomatis akun GuardDuty administrator yang didelegasikan akan berlaku pada saat mengaktifkan GuardDuty atau salah satu paket perlindungan opsionalnya.

Ubah konfigurasi organisasi untuk akun GuardDuty administrator yang didelegasikan baru dengan menggunakan metode akses pilihan Anda - GuardDuty konsol, atau API atau AWS CLI. Untuk informasi selengkapnya, lihat [Memperbarui preferensi mengaktifkan otomatis organisasi](#).

## Mengelola GuardDuty akun dengan undangan

Untuk mengelola akun di luar organisasi, Anda dapat menggunakan metode undangan lawas. Jika Anda menggunakan metode ini, akun Anda ditetapkan sebagai akun administrator saat akun lain menerima undangan Anda untuk menjadi akun anggota.

Jika akun Anda bukan akun administrator, Anda dapat menerima undangan dari akun lain. Jika Anda menerima, akun Anda menjadi akun anggota. AWS Akun tidak dapat berupa akun GuardDuty administrator dan akun anggota secara bersamaan.

Ketika Anda menerima undangan dari satu akun, Anda tidak dapat menerima undangan dari akun lain. Untuk menerima undangan dari akun lain, Anda harus terlebih dahulu memisahkan akun Anda dari akun administrator yang ada. Atau, akun administrator juga dapat memisahkan dan menghapus akun Anda dari organisasi mereka.

Akun yang terkait dengan undangan memiliki account-to-member hubungan administrator keseluruhan yang sama dengan akun yang terkait dengan AWS Organizations, seperti yang dijelaskan dalam [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#). Namun, pengguna akun administrator undangan tidak dapat mengaktifkan GuardDuty atas nama akun anggota terkait atau melihat akun non-anggota lainnya dalam AWS Organizations organisasi mereka.

#### Important

Transfer data lintas-regional dapat terjadi ketika GuardDuty membuat akun anggota menggunakan metode ini. Untuk memverifikasi alamat email akun anggota, GuardDuty gunakan layanan verifikasi email yang hanya beroperasi di Wilayah AS Timur (Virginia N.).

## Menambahkan dan mengelola akun berdasarkan undangan

Pilih salah satu metode akses untuk menambah dan mengundang akun untuk menjadi akun GuardDuty anggota sebagai akun GuardDuty administrator.

### Console

#### Langkah 1 - Tambahkan akun

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Akun.
3. Pilih Tambahkan akun berdasarkan undangan di panel atas.
4. Pada halaman Tambahkan akun anggota, di bawah Masukkan detail akun, masukkan Akun AWS ID dan alamat email yang terkait dengan akun yang ingin Anda tambahkan.



5. Untuk menambahkan baris lain untuk memasukkan detail akun satu per satu, pilih **Tambahkan akun lain**. Anda juga dapat memilih **Unggah file.csv** dengan detail akun untuk menambahkan akun secara massal.

**⚠ Important**

Baris pertama file csv Anda harus berisi header, seperti yang digambarkan dalam contoh berikut —. `Account ID,Email` Setiap baris berikutnya harus berisi satu Akun AWS ID yang valid dan alamat email yang terkait. Format baris valid jika hanya berisi satu Akun AWS ID dan alamat email terkait dipisahkan oleh koma.

```
Account ID,Email
```

```
55555555555, user@example.com
```

6. Setelah Anda menambahkan semua detail akun, pilih **Berikutnya**. Anda dapat melihat akun yang baru ditambahkan di tabel **Akun**. Status akun ini akan menjadi **Undangan tidak terkirim**. Untuk informasi tentang mengirim undangan ke satu atau beberapa akun tambahan, lihat [Step 2 - Invite an account](#).

## Langkah 2 - Undang akun

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih **Akun**.
3. Pilih satu atau beberapa akun yang ingin Anda undang ke Amazon GuardDuty.
4. Pilih menu tarik-turun **Tindakan** dan kemudian pilih **Undang**.
5. Di kotak GuardDuty dialog **Undangan ke**, masukkan pesan undangan (opsional).

Jika akun yang diundang tidak memiliki akses ke email, pilih kotak centang **Juga kirim pemberitahuan email ke pengguna root pada undangan Akun AWS** dan buat peringatan di undangan. **AWS Health Dashboard**

6. Pilih **Kirim undangan**. Jika undangan memiliki akses ke alamat email yang ditentukan, mereka dapat melihat undangan dengan membuka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>
7. Saat undangan menerima undangan, nilai di kolom **Status** berubah menjadi **Diundang**. Untuk informasi tentang menerima undangan, lihat [Step 3 - Accept an invitation](#).

## Langkah 3 - Terima undangan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

### Important

Anda harus mengaktifkan GuardDuty sebelum dapat melihat atau menerima undangan keanggotaan.

2. Lakukan hal berikut hanya jika Anda GuardDuty belum mengaktifkan; jika tidak, Anda dapat melewati langkah ini dan melanjutkan dengan langkah berikutnya.

Jika Anda belum mengaktifkan GuardDuty, pilih Memulai di GuardDuty halaman Amazon.

Pada GuardDuty halaman Selamat Datang di, pilih Aktifkan GuardDuty.

3. Setelah mengaktifkan GuardDuty akun Anda, gunakan langkah-langkah berikut untuk menerima undangan keanggotaan:
  - a. Pada panel navigasi, silakan pilih Pengaturan.
  - b. Pilih Akun .
  - c. Pada Akun, pastikan untuk memverifikasi pemilik akun tempat Anda menerima undangan. Aktifkan Terima untuk menerima undangan keanggotaan.
4. Setelah Anda menerima undangan, akun Anda menjadi akun GuardDuty anggota. Akun yang pemiliknya mengirim undangan menjadi akun GuardDuty administrator. Akun administrator akan tahu bahwa Anda telah menerima undangan. Tabel Akun di GuardDuty akun mereka akan diperbarui. Nilai di kolom Status yang sesuai dengan ID akun anggota Anda akan berubah menjadi Diaktifkan. Pemilik akun administrator sekarang dapat melihat GuardDuty dan mengelola serta konfigurasi paket perlindungan atas nama akun Anda. Akun administrator juga dapat melihat dan mengelola GuardDuty temuan yang dihasilkan untuk akun anggota Anda.

## API/CLI

Anda dapat menunjuk akun GuardDuty administrator, dan membuat atau menambahkan akun GuardDuty anggota dengan undangan melalui API operasi. Jalankan GuardDuty API operasi berikut untuk menunjuk akun administrator dan akun anggota di GuardDuty.

Selesaikan prosedur berikut menggunakan kredensial Akun AWS yang ingin Anda tetapkan sebagai akun administrator. GuardDuty

Membuat atau menambahkan akun anggota

1. Jalankan [CreateMembers](#) API operasi menggunakan kredensial AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

Anda harus menentukan ID detektor AWS akun saat ini dan ID akun serta alamat email dari akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat membuat satu atau lebih anggota dengan API operasi ini.


Anda juga dapat menggunakan Alat Baris AWS Perintah untuk menunjuk akun administrator dengan menjalankan CLI perintah berikut. Pastikan untuk menggunakan ID pendeteksi, ID akun, dan email Anda sendiri yang valid.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Jalankan [InviteMembers](#) dengan menggunakan kredensial AWS akun yang telah GuardDuty diaktifkan. Ini adalah akun yang Anda inginkan menjadi akun GuardDuty akun administrator.

Anda harus menentukan ID detektor AWS akun saat ini dan akun IDs akun yang ingin Anda jadikan GuardDuty anggota. Anda dapat mengundang satu atau lebih anggota dengan API operasi ini.

 Note

Anda juga dapat menentukan pesan undangan opsional dengan menggunakan parameter `message` permintaan.

Anda juga dapat menggunakan AWS Command Line Interface untuk menunjuk akun anggota dengan menjalankan perintah berikut. Pastikan untuk menggunakan ID detektor Anda sendiri yang valid dan akun yang valid IDs untuk akun yang ingin Anda undang.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

## Menerima undangan

Selesaikan prosedur berikut menggunakan kredensial dari setiap AWS akun yang ingin Anda tetapkan sebagai GuardDuty akun anggota.

1. Jalankan [CreateDetector](#) API operasi untuk setiap AWS akun yang diundang untuk menjadi akun GuardDuty anggota dan Anda ingin menerima undangan.

Anda harus menentukan apakah sumber daya detektor akan diaktifkan menggunakan GuardDuty layanan. Detektor harus dibuat dan diaktifkan GuardDuty agar dapat beroperasi. Anda harus mengaktifkan terlebih dahulu GuardDuty sebelum menerima undangan.

Anda juga dapat melakukan ini dengan menggunakan AWS Command Line Tools menggunakan CLI perintah berikut.

```
aws guardduty create-detector --enable
```

2. Jalankan [AcceptAdministratorInvitation](#) API operasi untuk setiap AWS akun yang ingin Anda terima undangan keanggotaan, menggunakan kredensi akun tersebut.

Anda harus menentukan ID detektor AWS akun ini untuk akun anggota, ID akun administrator yang mengirim undangan, dan ID undangan undangan yang Anda terima. Anda dapat menemukan ID akun administrator di email undangan atau dengan menggunakan [ListInvitations](#) operasi API.

Anda juga dapat menerima undangan menggunakan AWS Command Line Tools dengan menjalankan CLI perintah berikut. Pastikan Anda menggunakan ID detektor, ID akun administrator, dan ID undangan yang valid.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
--administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

## Mengkonsolidasikan akun GuardDuty administrator di bawah satu akun administrator yang didelegasikan GuardDuty organisasi

GuardDuty merekomendasikan penggunaan asosiasi melalui AWS Organizations untuk mengelola akun anggota di bawah akun GuardDuty administrator yang didelegasikan. Anda dapat menggunakan contoh proses yang diuraikan di bawah ini untuk mengkonsolidasikan akun administrator dan anggota yang terkait dengan undangan di organisasi di bawah satu akun administrator yang GuardDuty didelegasikan GuardDuty .

### Note

Akun yang sudah dikelola oleh akun GuardDuty administrator yang didelegasikan, atau akun anggota aktif yang dikaitkan dengan akun administrator yang didelegasikan tidak dapat ditambahkan ke akun GuardDuty administrator yang didelegasikan lainnya GuardDuty . Setiap organisasi hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan per Wilayah, dan setiap akun anggota hanya dapat memiliki satu akun GuardDuty administrator yang didelegasikan.

Pilih salah satu metode akses untuk mengkonsolidasikan akun GuardDuty administrator di bawah satu akun administrator yang didelegasikan GuardDuty .

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun manajemen organisasi.

2. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat [Mengundang Akun AWS untuk bergabung dengan organisasi Anda](#).

3. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan. Putuskan hubungan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.

Langkah-langkah berikut akan membantu Anda memisahkan akun anggota dari akun administrator yang sudah ada sebelumnya:

- a. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
  - b. Untuk masuk, gunakan kredensi akun administrator yang sudah ada sebelumnya.
  - c. Di panel navigasi, pilih Akun.
  - d. Pada halaman Akun, pilih satu atau beberapa akun yang ingin Anda pisahkan dari akun administrator.
  - e. Pilih Actions dan kemudian pilih Disassociate account.
  - f. Pilih Konfirmasi untuk menyelesaikan langkah.
4. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Untuk masuk, gunakan kredensial akun manajemen.

5. Pada panel navigasi, silakan pilih Pengaturan. Pada halaman Pengaturan, tentukan akun GuardDuty administrator yang didelegasikan untuk organisasi.
6. Masuk ke akun GuardDuty administrator yang didelegasikan yang ditunjuk.
7. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat [Mengelola GuardDuty akun dengan AWS Organizations](#).

## API/CLI

1. Semua akun yang ingin Anda kelola GuardDuty harus menjadi bagian dari organisasi Anda. Untuk informasi tentang menambahkan akun ke organisasi Anda, lihat [Mengundang Akun AWS untuk bergabung dengan organisasi Anda](#).
2. Pastikan semua akun anggota dikaitkan dengan akun yang ingin Anda tetapkan sebagai akun GuardDuty administrator tunggal yang didelegasikan.
  - a. Jalankan [DisassociateMembers](#) untuk memisahkan akun anggota yang masih terkait dengan akun administrator yang sudah ada sebelumnya.
  - b. Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut dan mengganti `777777777777` dengan ID detektor akun administrator

yang sudah ada sebelumnya tempat Anda ingin memisahkan akun anggota. Ganti **666666666666** dengan Akun AWS ID akun anggota yang ingin Anda pisahkan.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. Jalankan [EnableOrganizationAdminAccount](#) untuk mendelegasikan akun GuardDuty administrator Akun AWS sebagai delegasi.

Atau, Anda dapat menggunakan AWS Command Line Interface untuk menjalankan perintah berikut untuk mendelegasikan akun GuardDuty administrator yang didelegasikan:

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Tambahkan anggota dari organisasi. Untuk informasi selengkapnya, lihat [Create or add member member accounts using API](#).

#### Important

Untuk memaksimalkan efektivitas GuardDuty, layanan regional, kami sarankan Anda menunjuk akun GuardDuty administrator yang didelegasikan dan menambahkan semua akun anggota Anda di setiap Wilayah.

## Aktifkan GuardDuty di beberapa akun secara bersamaan

Gunakan metode berikut untuk mengaktifkan GuardDuty di beberapa akun secara bersamaan.

Gunakan skrip Python untuk mengaktifkan GuardDuty di beberapa akun secara bersamaan

[Anda dapat mengotomatiskan pengaktifan atau penonaktifan GuardDuty pada beberapa akun menggunakan skrip dari repositori sampel di skrip multiaccount Amazon. GuardDuty](#) Gunakan proses di bagian ini GuardDuty untuk mengaktifkan daftar akun anggota yang menggunakan AmazonEC2. Untuk informasi tentang menggunakan skrip nonaktifkan atau menyiapkan skrip secara lokal, lihat petunjuk di tautan bersama.

`enableguardduty.py` Skrip memungkinkan GuardDuty, mengirim undangan dari akun administrator, dan menerima undangan di semua akun anggota. Hasilnya adalah akun GuardDuty

akun administrator yang berisi semua temuan keamanan untuk semua akun anggota. Karena GuardDuty diisolasi berdasarkan Wilayah, temuan untuk setiap akun anggota digulung ke Wilayah yang sesuai di akun administrator. Misalnya, Wilayah us-east-1 di akun administrator GuardDuty Anda berisi temuan keamanan untuk semua temuan us-east-1 dari semua akun anggota terkait.

Skrip ini memiliki ketergantungan pada IAM peran bersama dengan kebijakan terkelola — [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#). Kebijakan ini memberikan akses kepada entitas GuardDuty dan harus ada di akun administrator dan di setiap akun yang ingin Anda aktifkan GuardDuty.

Proses berikut memungkinkan GuardDuty di semua Wilayah yang tersedia secara default. Anda dapat mengaktifkan GuardDuty di Wilayah tertentu hanya dengan menggunakan --enabled\_regions argumen opsional dan menyediakan daftar Wilayah yang dipisahkan koma. Anda juga dapat secara opsional menyesuaikan pesan undangan yang dikirim ke akun anggota dengan membuka enableguardduty.py dan mengedit string gd\_invite\_message.

1. Buat IAM peran di akun GuardDuty administrator dan lampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) kebijakan untuk mengaktifkan GuardDuty.
2. Buat IAM peran di setiap akun anggota yang ingin dikelola oleh akun GuardDuty administrator Anda. Peran ini harus memiliki nama yang sama dengan peran yang dibuat pada langkah 1, peran ini harus mengizinkan akun administrator sebagai entitas tepercaya, dan peran ini harus memiliki kebijakan AmazonGuardDutyFullAccess terkelola yang sama yang dijelaskan sebelumnya.
3. Luncurkan instans Amazon Linux baru dengan peran terlampir yang memiliki hubungan kepercayaan berikut yang memungkinkan instans untuk mengambil peran layanan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Masuk ke instans baru dan jalankan perintah berikut untuk mengaturnya.



```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Buat CSV file yang berisi daftar akun IDs dan email akun anggota yang Anda tambahkan peran di langkah 2. Akun harus muncul satu per baris, dan ID akun dan alamat email harus dipisahkan dengan koma, seperti pada contoh berikut.

```
111122223333,guardduty-member@organization.com
```

#### Note

CSVFile harus berada di lokasi yang sama dengan `enableguardduty.py` skrip Anda. Anda dapat menyalin CSV file yang ada dari Amazon S3 ke direktori Anda saat ini dengan metode berikut.

```
aws s3 cp s3://my-bucket/my_key_name example.csv
```

6. Jalankan skrip Python. Pastikan untuk memberikan ID akun GuardDuty administrator Anda, nama peran yang dibuat pada langkah pertama, dan nama CSV file Anda sebagai argumen.

```
python enableguardduty.py --master_account 444455556666 --assume_role
roleName accountID.csv
```

# Memahami GuardDuty temuan Amazon

GuardDuty Temuan mewakili masalah keamanan potensial yang terdeteksi dalam jaringan Anda. GuardDuty menghasilkan temuan setiap kali mendeteksi aktivitas tak terduga dan berpotensi berbahaya di AWS lingkungan Anda.

Anda dapat melihat dan mengelola GuardDuty temuan Anda di halaman Temuan di GuardDuty konsol atau dengan menggunakan AWS CLI atau API operasi. Untuk gambaran umum tentang cara mengelola temuan, lihat [Mengelola GuardDuty temuan Amazon](#).

Topik:

## [GuardDuty format temuan](#)

Memahami format GuardDuty menemukan jenis dan tujuan ancaman yang berbeda dilacak oleh GuardDuty.

## [Sampel temuan](#)

Cobalah menghasilkan temuan sampel untuk menguji dan memahami GuardDuty temuan dan detail terkait. Temuan ini ditandai dengan awalan [SAMPLE].

## [GuardDuty Temuan uji di akun khusus](#)

Jalankan `guardduty-tester` skrip dalam non-produksi khusus Akun AWS untuk menghasilkan GuardDuty temuan yang dipilih di AWS lingkungan Anda.

## [Detail temuan](#)

Pelajari detail yang terkait dengan GuardDuty temuan yang dihasilkan di akun Anda.

## [Tipe temuan](#)

Lihat dan cari semua GuardDuty temuan yang tersedia berdasarkan jenis. Setiap entri tipe temuan mencakup penjelasan tentang temuan tersebut serta tips dan saran perbaikan.

# GuardDuty format temuan

Saat GuardDuty mendeteksi perilaku yang mencurigakan atau tidak terduga di AWS lingkungan Anda, hal ini menghasilkan temuan. Temuan adalah notifikasi yang berisi detail tentang potensi masalah

keamanan yang GuardDuty ditemukan. [Detail temuan](#) mencakup informasi tentang apa yang terjadi, sumber daya AWS mana yang terlibat dalam aktivitas mencurigakan, kapan aktivitas ini terjadi, dan informasi lainnya.

Salah satu bagian informasi yang paling berguna dalam detail temuan adalah jenis temuan. Tujuan dari jenis temuan adalah untuk memberikan deskripsi ringkas namun dapat dibaca tentang potensi masalah keamanan. Misalnya, jenisPortProbeUnprotectedPort temuan GuardDuty Recon:EC2/ dengan cepat menginformasikan bahwa di suatu tempat diAWS lingkungan Anda, instans EC2 memiliki port yang tidak terlindungi yang kemungkinan sedang diperiksa oleh penyerang.

GuardDuty menggunakan format berikut untuk penamaan berbagai jenis temuan yang dihasilkannya:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName. DetectionMechanism! Artifact

Setiap bagian dari format ini mewakili aspek dari jenis temuan. Aspek-aspek ini memiliki penjelasan sebagai berikut:

- ThreatPurpose- menjelaskan tujuan utama dari ancaman, jenis serangan atau tahap potensi serangan. Lihat bagian berikut untuk daftar lengkap dari tujuan GuardDuty ancaman.
- ResourceTypeAffected- menjelaskan jenisAWS sumber daya mana yang diidentifikasi dalam temuan ini sebagai potensi target musuh. Saat ini, GuardDuty dapat menghasilkan temuan untuk sumber daya EC2, S3, IAM, dan EKS.
- ThreatFamilyName- menjelaskan ancaman secara keseluruhan atau potensi aktivitas berbahaya GuardDuty yang mendeteksi. Misalnya, nilai NetworkPortUnusualmenunjukkan bahwa instans EC2 yang diidentifikasi dalam GuardDuty temuan tidak memiliki riwayat komunikasi sebelumnya pada port jarak jauh tertentu yang juga diidentifikasi dalam temuan.
- DetectionMechanism- menjelaskan metode yang digunakan untuk GuardDuty mendeteksi temuan. Hal ini dapat digunakan untuk menunjukkan variasi pada jenis temuan umum atau temuan yang GuardDuty menggunakan mekanisme tertentu untuk mendeteksi. Misalnya, DenialOfServiceBackdoor:EC2/.Tcp menunjukkan bahwa denial of service (DoS) terdeteksi melalui TCP. Varian UDP adalah DenialOfServiceBackdoor:EC2/.Udp.

Nilai .Custom menunjukkan bahwa GuardDuty mendeteksi temuan berdasarkan daftar ancaman kustom Anda, sementara .Reputation menunjukkan bahwa GuardDuty mendeteksi temuan menggunakan model skor reputasi domain.

- Artifact - menjelaskan sumber daya tertentu yang dimiliki oleh alat yang digunakan dalam aktivitas berbahaya. Misalnya, DNS dalam jenis Cryptocurrencytemuan:EC2/.BBitcoinTool! DNS menunjukkan bahwa instans EC2 berkomunikasi dengan domain terkait Bitcoin yang dikenal.

## Tujuan Ancaman

Dalam tujuan GuardDuty ancaman menjelaskan tujuan utama dari ancaman, jenis serangan, atau tahap potensi serangan. Misalnya, beberapa tujuan ancaman, seperti Backdoor, menunjukkan jenis serangan. Namun, beberapa tujuan ancaman, seperti Impact sejajar dengan [taktik MITRE ATT&CK](#). Taktik MITRE ATT&CK menunjukkan fase yang berbeda dalam siklus serangan musuh. Dalam rilis saat ini GuardDuty, ThreatPurpose dapat memiliki nilai berikut:

### Backdoor

Nilai ini menunjukkan bahwa musuh telah menyusupi sumber daya AWS dan mengubah sumber daya tersebut sehingga dapat menghubungi server asal perintah dan kontrol (C&C) guna menerima petunjuk lebih lanjut untuk aktivitas berbahaya.

### Perilaku

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang berbeda dari garis dasar yang ditetapkan untuk AWS sumber daya yang terlibat.

### CredentialAccess

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi pola aktivitas yang dapat digunakan oleh musuh untuk mencuri kredensi, seperti ID atau kata sandi akun, dari lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#)

### Mata Uang Kripto

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa AWS sumber daya di lingkungan Anda adalah menghosting perangkat lunak yang terkait dengan mata uang kripto (misalnya, Bitcoin).

### DefenseEvasion

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan oleh musuh untuk menghindari deteksi ketika menyusupi lingkungan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#)

### Penemuan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan oleh musuh untuk memperluas pengetahuan mereka tentang sistem dan jaringan internal Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

## Eksekusi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi bahwa musuh mungkin mencoba menjalankan kode berbahaya untuk menjelajahi jaringan atau mencuri data. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

## Ekfiltrasi

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan oleh musuh ketika mencoba untuk mencuri data dari jaringan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

## Dampak

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang menunjukkan bahwa musuh mencoba untuk memanipulasi, mengganggu, atau menghancurkan sistem dan data Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

## InitialAccess

Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

## Terpentest

Terkadang pemilikAWS sumber daya atau perwakilan resmi mereka sengaja menjalankan tes terhadapAWS aplikasi untuk menemukan kerentanan, seperti membuka grup keamanan atau kunci akses yang terlalu permisif. Uji penetrasi ini dilakukan dalam upaya untuk mengidentifikasi dan mengunci sumber daya yang rentan sebelum ditemukan oleh musuh. Namun, beberapa alat yang digunakan oleh penguji penetrasi resmi tersedia secara bebas dan oleh karena itu dapat digunakan oleh pengguna yang tidak sah atau musuh untuk menjalankan uji probing. Meski tidak GuardDuty dapat mengidentifikasi tujuan sebenarnya di balik aktivitas tersebut, nilai Pentest menunjukkan bahwa hal GuardDuty ini mendeteksi aktivitas tersebut, bahwa hal ini mirip dengan aktivitas yang dihasilkan oleh alat uji penetrasi yang dikenal, dan bahwa hal ini dapat menunjukkan probing berbahaya terhadap jaringan Anda.

## Kegigihan

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan oleh musuh untuk mencoba dan mempertahankan akses ke sistem Anda bahkan jika rute akses awal mereka terputus. Misalnya, ini dapat termasuk membuat pengguna IAM baru setelah mendapatkan akses menggunakan kredensial pengguna yang ada. Ketika kredensial pengguna yang ada dihapus, musuh akan mempertahankan akses pada pengguna baru yang

tidak terdeteksi sebagai bagian dari peristiwa asli. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

### Kebijakan

Nilai ini menunjukkan Akun AWS bahwa Anda menunjukkan perilaku yang bertentangan dengan praktik keamanan terbaik yang direkomendasikan.

### PrivilegeEscalation

Nilai ini menginformasikan bahwa prinsipal yang terlibat dalam lingkungan AWS Anda menunjukkan perilaku yang mungkin digunakan musuh untuk mendapatkan izin dengan tingkat yang lebih tinggi ke jaringan Anda. Tujuan ancaman ini didasarkan pada [taktik MITRE ATT&CK](#).

### Pengintaian

Nilai ini menunjukkan bahwa GuardDuty telah mendeteksi aktivitas atau pola aktivitas yang dapat digunakan oleh musuh ketika melakukan pengintaian terhadap jaringan Anda untuk menentukan bagaimana mereka dapat memperluas akses mereka atau memanfaatkan sumber daya Anda. Misalnya, aktivitas ini dapat mencakup pelingkupan kerentanan di lingkungan AWS Anda dengan memeriksa port, membuat daftar pengguna, tabel basis data, dan sebagainya.

### Stealth

Nilai ini menunjukkan bahwa musuh secara aktif mencoba menyembunyikan tindakan mereka. Misalnya, mereka mungkin menggunakan server proksi anonim, sehingga sangat sulit untuk mengukur sifat sebenarnya dari aktivitas tersebut.

### Trojan

Nilai ini menunjukkan bahwa serangan menggunakan program Trojan yang diam-diam melakukan aktivitas berbahaya. Terkadang perangkat lunak ini mengambil tampilan program yang sah. Terkadang pengguna secara tidak sengaja menjalankan perangkat lunak ini. Lain kali perangkat lunak ini mungkin berjalan secara otomatis dengan memanfaatkan kerentanan.

### UnauthorizedAccess

Nilai ini menunjukkan GuardDuty bahwa mendeteksi aktivitas yang mencurigakan atau pola aktivitas yang mencurigakan oleh individu yang tidak sah.

## GuardDuty mesin pemindai deteksi malware

Amazon GuardDuty memiliki mesin pemindaian yang dibangun dan dikelola secara internal dan [vendor pihak ketiga](#). Keduanya menggunakan indikator kompromi (IoCs) yang bersumber dari

berbagai feed internal yang memiliki visibilitas di berbagai jenis malware yang mungkin ditargetkan. AWS GuardDuty juga memiliki definisi deteksi yang didasarkan pada YARA aturan yang ditambahkan oleh teknisi keamanan kami, dan deteksi berdasarkan model heuristik dan pembelajaran mesin (ML). Deteksi berbasis tanda tangan tidak hanya mencakup pencocokan byte tetapi juga potongan kode yang berpotensi kompleks, dan pemindai dapat mengurai konten dan membuat keputusan.

Mesin pemindai malware tidak melakukan analisis perilaku langsung, di mana peledakan malware memantau sampel saat dijalankan dalam sistem nyata. GuardDuty Solusinya terutama deteksi berbasis file. Untuk mendeteksi malware tanpa file, GuardDuty berikan solusi berbasis agen, seperti untuk Amazon, Amazon, EKS EC2 dan [Pemantauan Runtime](#) Amazon (termasuk). ECS AWS Fargate

Tanpa batasan pada format file yang GuardDuty memindai malware, mesin pemindai yang digunakannya dapat mendeteksi berbagai jenis malware, seperti cryptominers, ransomware, dan webshell. Mesin GuardDuty pemindaian yang dikelola sepenuhnya terus memperbarui daftar tanda tangan malware setiap 15 menit.

Mesin pemindai adalah bagian dari sistem intelijen GuardDuty ancaman yang menggunakan komponen peledakan malware internal. Ini menghasilkan intelijen ancaman baru dengan mengumpulkan malware dan sampel jinak secara independen dari berbagai sumber. File hash tipe IoC dari sistem intelijen ancaman selanjutnya dimasukkan ke mesin pemindaian malware untuk mendeteksi malware berdasarkan hash file buruk yang diketahui.

## Menghasilkan temuan sampel di GuardDuty

Anda dapat menghasilkan sampel temuan dengan Amazon GuardDuty untuk membantu Anda memvisualisasikan dan memahami berbagai jenis temuan yang GuardDuty dapat dihasilkan. Saat Anda menghasilkan temuan sampel, GuardDuty isi daftar temuan Anda saat ini dengan satu temuan sampel untuk setiap jenis temuan yang didukung.

Sampel yang dibuat adalah perkiraan yang diisi dengan nilai placeholder. Sampel ini mungkin terlihat berbeda dari temuan nyata untuk lingkungan Anda, tetapi Anda dapat menggunakannya untuk menguji berbagai konfigurasi GuardDuty, seperti EventBridge acara atau filter Anda. Untuk daftar nilai yang tersedia untuk menemukan jenis, lihat [Tipe temuan](#) tabel.

## Menghasilkan temuan sampel melalui GuardDuty konsol atau API

Pilih metode akses pilihan Anda untuk menghasilkan temuan sampel.

**Note**

Metode konsol membuat salah satu tipe temuan. Temuan sampel tunggal hanya dapat dihasilkan melalui API.

## Console

Gunakan prosedur berikut untuk membuat sampel temuan. Proses ini menghasilkan satu sampel temuan untuk setiap jenis GuardDuty temuan.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di halaman Pengaturan, di bawah Sampel temuan, pilih Buat sampel temuan.
4. Di panel navigasi, pilih Temuan. Temuan sampel ditampilkan pada halaman Temuan saat ini dengan awalan [SAMPLE].

## API/CLI

Anda dapat menghasilkan satu sampel temuan yang cocok dengan salah satu jenis GuardDuty temuan melalui [CreateSampleFindings](#) API, nilai yang tersedia untuk menemukan jenis tercantum dalam [Tipe temuan](#) tabel.

Ini berguna untuk pengujian aturan CloudWatch Acara atau otomatisasi berdasarkan temuan. Contoh berikut menunjukkan cara menghasilkan temuan sampel tunggal dari `Backdoor:EC2/DenialOfService.Tcp` jenis menggunakan AWS CLI.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

Judul temuan sampel yang dihasilkan melalui metode ini selalu dimulai dengan [SAMPLE] di konsol. Temuan sampel memiliki nilai "sample": true di additionalInfo bagian JSON rincian temuan.



Untuk menghasilkan beberapa temuan umum berdasarkan aktivitas simulasi di tempat yang berdedikasi dan terisolasi di Akun AWS lingkungan Anda, lihat [GuardDuty Temuan uji di akun khusus](#).

## GuardDuty Temuan uji di akun khusus

Gunakan dokumen ini untuk menjalankan skrip pengujian yang menghasilkan GuardDuty temuan Akun AWS yang Anda gunakan secara khusus untuk tujuan ini. Anda dapat melakukan langkah-langkah ini ketika Anda ingin memahami dan mempelajari tentang jenis GuardDuty temuan tertentu. Pengalaman ini berbeda dengan menghasilkan [Sampel temuan](#). Untuk informasi lebih lanjut tentang pengalaman pengujian GuardDuty temuan, lihat [Pertimbangan](#).

### Daftar Isi

- [Pertimbangan](#)
- [GuardDuty temuan skrip tester dapat menghasilkan](#)
- [Langkah 1 - Prasyarat](#)
- [Langkah 2 - Menyebarkan sumber daya AWS](#)
- [Langkah 3 - Jalankan skrip pengujian](#)
- [Langkah 4 - Bersihkan sumber daya AWS tes](#)
- [Memecahkan masalah umum](#)

## Pertimbangan

Sebelum Anda melanjutkan, pertimbangkan pertimbangan berikut:

- GuardDuty merekomendasikan penerapan skrip pengujian di non-produksi khusus Akun AWS atau lingkungan yang terisolasi. Dengan menjalankan skrip tester, GuardDuty akan menyebarkan AWS sumber daya tertentu di akun ini. Ini juga akan membantu Anda mengidentifikasi temuan simulasi ini.
- Skrip tester menghasilkan lebih dari 100 GuardDuty temuan dengan kombinasi AWS sumber daya yang berbeda. Saat ini, ini tidak termasuk semua. [Tipe temuan](#) Untuk daftar jenis pencarian yang dapat Anda hasilkan dengan skrip pengujian ini, lihat [GuardDuty temuan skrip tester dapat menghasilkan](#).
- Skrip tester memvalidasi status GuardDuty konfigurasi di akun khusus Anda. Jika akun ini tidak GuardDuty diaktifkan, skrip akan meminta Anda untuk mengaktifkannya saat Anda

melakukan [Langkah 3 - Jalankan skrip pengujian](#). Skrip pengujian akan meminta izin Anda untuk mengaktifkan rencana perlindungan tertentu yang diperlukan untuk menghasilkan temuan.

Mengaktifkan GuardDuty untuk pertama kalinya

Ketika GuardDuty diaktifkan di akun khusus Anda untuk pertama kalinya di Wilayah tertentu, akun Anda akan secara otomatis terdaftar dalam uji coba gratis 30 hari.

GuardDuty menawarkan paket perlindungan opsional. Pada saat memungkinkan GuardDuty, paket perlindungan tertentu juga diaktifkan dan termasuk dalam uji coba gratis GuardDuty 30 hari. Untuk informasi selengkapnya, lihat [Menggunakan uji GuardDuty coba gratis 30 hari](#).

GuardDuty sudah diaktifkan di akun Anda sebelum menjalankan skrip pengujian

Ketika sudah GuardDuty diaktifkan, maka berdasarkan parameter, skrip tester akan memeriksa status konfigurasi rencana perlindungan tertentu dan pengaturan tingkat akun lainnya yang diperlukan untuk menghasilkan temuan.

Dengan menjalankan skrip pengujian ini, paket perlindungan tertentu mungkin diaktifkan untuk pertama kalinya di akun khusus Anda di Wilayah. Ini akan memulai uji coba gratis 30 hari untuk rencana perlindungan itu. Untuk informasi tentang uji coba gratis yang terkait dengan setiap paket perlindungan, lihat [Menggunakan uji GuardDuty coba gratis 30 hari](#).

- Setelah skrip pengujian selesai, akun khusus Anda akan mengembalikan ke konfigurasi dan pengaturan paket perlindungan aslinya.

## GuardDuty temuan skrip tester dapat menghasilkan

Saat ini, skrip pengujian menghasilkan jenis temuan berikut yang terkait dengan Amazon, AmazonEKS, EC2 Amazon S3,, dan log IAM audit: EKS

- [Backdoor:EC2/C&CAActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [PenTest:IAMUser/KaliLinux](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)

- [Discovery:S3/TorIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

## Langkah 1 - Prasyarat

Untuk mempersiapkan lingkungan pengujian Anda, Anda memerlukan item berikut:

- Git — Instal alat baris perintah git berdasarkan sistem operasi yang Anda gunakan. Ini diperlukan untuk mengkloning [amazon-guardduty-testerrepository](#).
- AWS Command Line Interface— Alat open source yang memungkinkan Anda berinteraksi AWS layanan dengan menggunakan perintah di shell baris perintah Anda. Untuk informasi selengkapnya, lihat [Memulai AWS CLI](#) di Panduan AWS Command Line Interface Pengguna.
- AWS Systems Manager— Untuk memulai sesi Session Manager dengan node terkelola Anda dengan menggunakan AWS CLI Anda harus menginstal plugin Session Manager di mesin lokal Anda. Untuk informasi selengkapnya, lihat [Plugin Install Session Manager AWS CLI](#) di Panduan AWS Systems Manager Pengguna.
- Node Package Manager (NPM) - Instal NPM untuk menginstal semua dependensi.
- Docker — Anda harus menginstal Docker. Untuk petunjuk penginstalan, lihat [situs web Docker](#).

Untuk memverifikasi bahwa Docker telah diinstal, jalankan perintah berikut dan konfirmasikan ada output yang mirip dengan output berikut:

```
$ docker --version
Docker version 19.03.1
```

- Berlangganan gambar [Kali Linux](#) di AWS Marketplace.

## Langkah 2 - Menyebarkan sumber daya AWS

Bagian ini menyediakan daftar konsep kunci dan langkah-langkah untuk menyebarkan AWS sumber daya tertentu di akun khusus Anda.

### Konsep

Daftar berikut menyediakan konsep kunci yang terkait dengan perintah yang membantu Anda menyebarkan sumber daya:

- AWS Cloud Development Kit (AWS CDK)— CDK adalah kerangka pengembangan perangkat lunak open-source untuk mendefinisikan infrastruktur cloud dalam kode dan menyediakannya melalui AWS CloudFormation. CDK mendukung beberapa bahasa pemrograman untuk mendefinisikan komponen cloud yang dapat digunakan kembali yang dikenal sebagai konstruksi. Anda dapat menyusun ini bersama-sama ke tumpukan dan aplikasi. Kemudian, Anda dapat menerapkan CDK aplikasi Anda AWS CloudFormation untuk menyediakan atau memperbarui sumber daya Anda. Untuk informasi lebih lanjut, lihat [Apa itu AWS CDK?](#) di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.

- Bootstrapping — Ini adalah proses mempersiapkan AWS lingkungan Anda untuk digunakan dengan AWS CDK. Sebelum Anda menyebarkan CDK tumpukan ke lingkungan, AWS lingkungan harus di-bootstrap terlebih dahulu. Proses penyediaan AWS sumber daya tertentu di lingkungan Anda yang digunakan oleh AWS CDK adalah bagian dari langkah-langkah yang akan Anda lakukan di bagian berikutnya - [Langkah-langkah untuk menyebarkan sumber daya AWS](#)

Untuk informasi selengkapnya tentang cara kerja bootstrap, lihat [Bootstrapping di Panduan Pengembang](#). AWS Cloud Development Kit (AWS CDK)

## Langkah-langkah untuk menyebarkan sumber daya AWS

Lakukan langkah-langkah berikut untuk mulai menerapkan sumber daya:

1. Siapkan akun AWS CLI default dan Wilayah kecuali variabel Wilayah akun khusus diatur secara manual dalam `bin/cdk-gd-tester.ts` file. Untuk informasi selengkapnya, lihat [Lingkungan](#) di Panduan AWS Cloud Development Kit (AWS CDK) Pengembang.
2. Jalankan perintah berikut untuk menyebarkan sumber daya:

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

Perintah terakhir (`cdk deploy`) membuat AWS CloudFormation tumpukan atas nama Anda. Nama tumpukan ini adalah `GuardDutyTesterStack`.

Sebagai bagian dari skrip ini, GuardDuty buat sumber daya baru untuk menghasilkan GuardDuty temuan di akun Anda. Ini juga menambahkan pasangan kunci tag berikut: nilai ke instance AmazonEC2:

`CreatedBy:GuardDuty Test Script`

EC2Instans Amazon juga menyertakan EC2 instance yang meng-host EKS node dan ECS cluster.

### Tipe instans

GuardDuty membuat `t3.micro` untuk semua sumber daya dengan pengecualian untuk grup EKS node Amazon. Karena EKS membutuhkan setidaknya 2 core, EKS node

memiliki tipe `t3.medium` instance. Untuk informasi selengkapnya tentang jenis instans, lihat [Ukuran yang tersedia](#) di Panduan Jenis EC2 Instans Amazon.

## Langkah 3 - Jalankan skrip pengujian

Ini adalah proses dua langkah di mana Anda pertama-tama perlu memulai sesi dengan driver uji dan kemudian, jalankan skrip untuk menghasilkan GuardDuty temuan dengan kombinasi sumber daya tertentu.

### Bagian A - Mulai sesi dengan driver tes

1. Setelah resource Anda di-deploy, simpan kode Region ke variabel di sesi terminal Anda saat ini. Gunakan perintah berikut dan ganti `us-east-1` dengan kode Wilayah tempat Anda menerapkan sumber daya:

```
$ REGION=us-east-1
```

2. Skrip tester hanya tersedia melalui AWS Systems Manager (SSM). Untuk memulai shell interaktif pada instance host tester, kueri host InstanceId.
3. Gunakan perintah berikut untuk memulai sesi Anda untuk skrip tester:

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

### Bagian B - Menghasilkan temuan

Skrip tester adalah program berbasis Python yang secara dinamis membangun skrip bash untuk menghasilkan temuan berdasarkan masukan Anda. Anda memiliki fleksibilitas untuk menghasilkan temuan berdasarkan satu atau lebih jenis AWS sumber daya, rencana GuardDuty perlindungan, [Tujuan Ancaman](#) (taktik) [Sumber data dasar](#), atau [the section called "GuardDuty temuan skrip tester dapat menghasilkan"](#).

Gunakan contoh perintah berikut sebagai referensi, dan jalankan satu atau beberapa perintah untuk menghasilkan temuan yang ingin Anda jelajahi:

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Untuk informasi lebih lanjut tentang parameter yang valid, Anda dapat menjalankan perintah bantuan berikut:

```
python3 guardduty_tester.py --help
```

## Bagian C - Tinjau temuan yang dihasilkan

Pilih metode yang disukai untuk melihat temuan yang dihasilkan di akun Anda.

### GuardDuty console

1. Masuk ke AWS Management Console dan buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Temuan.
3. Dari tabel temuan, pilih temuan yang ingin Anda lihat detailnya. Ini akan membuka panel detail temuan. Untuk informasi, lihat [Memahami GuardDuty temuan Amazon](#).
4. Jika Anda ingin memfilter temuan ini, gunakan kunci dan nilai tag sumber daya. Misalnya, untuk memfilter temuan yang dihasilkan untuk EC2 instans Amazon, gunakan CreatedBy: GuardDuty Test Script tag key:value pair untuk kunci tag Instance dan kunci tag Instance.

### API

- Jalankan [ListFindings](#) untuk melihat temuan untuk ID detektor tertentu. Anda dapat menentukan parameter untuk memfilter temuan.



Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

## AWS CLI

- Jalankan AWS CLI perintah berikut untuk melihat temuan yang dihasilkan dan mengganti `us-east-1` and `12abc34d567e8fa901bc2d34EXAMPLE` dengan nilai yang sesuai:

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Untuk informasi selengkapnya tentang parameter yang dapat Anda gunakan untuk memfilter temuan, lihat [daftar-temuan](#) di Referensi AWS CLI Perintah.

## Langkah 4 - Bersihkan sumber daya AWS tes

Pengaturan tingkat akun dan pembaruan status konfigurasi lainnya yang dibuat selama [Langkah 3 - Jalankan skrip pengujian](#) kembali ke keadaan semula saat skrip pengujian selesai.

Setelah Anda menjalankan skrip tester, Anda dapat memilih untuk membersihkan sumber daya AWS pengujian. Anda dapat memilih untuk melakukan ini dengan menggunakan salah satu metode berikut:

- Jalankan perintah berikut:

```
cdk destroy
```

- Hapus AWS CloudFormation tumpukan dengan nama `GuardDutyTesterStack`. Untuk selengkapnya tentang langkah-langkah, lihat [Menghapus tumpukan di AWS CloudFormation konsol](#).

## Memecahkan masalah umum

GuardDuty telah mengidentifikasi masalah umum dan merekomendasikan langkah-langkah pemecahan masalah:

- **Cloud assembly schema version mismatch**— Perbarui AWS CDK CLI ke versi yang kompatibel dengan versi perakitan cloud yang diperlukan, atau ke versi terbaru yang tersedia. Untuk informasi selengkapnya, lihat [AWS CDK CLI kompatibilitas](#).
- **Docker permission denied**— Tambahkan pengguna akun khusus ke pengguna buruh pelabuhan sehingga akun khusus dapat menjalankan perintah. Untuk informasi selengkapnya tentang langkah-langkah, lihat [Akses Docker ditolak](#).
- **Your requested instance type is not supported in your requested Availability Zone**— Beberapa zona Availability tidak mendukung jenis instans tertentu. Untuk mengidentifikasi zona ketersediaan mana yang mendukung jenis instans pilihan Anda dan mencoba kembali untuk menerapkan AWS sumber daya, lakukan langkah-langkah berikut:
  1. Pilih metode yang disukai untuk menentukan zona Ketersediaan mana yang mendukung jenis instans Anda:

#### Console

Untuk mengidentifikasi Availability zone yang mendukung tipe instans pilihan

1. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Dengan menggunakan pemilih AWS Region di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin meluncurkan instance.
3. Di panel navigasi, di bawah Instance, pilih Jenis Instance.
4. Dari tabel tipe Instance, pilih jenis instance yang disukai.
5. Di bawah Jaringan, lihat Wilayah yang tercantum di bawah Availability zone.

Berdasarkan informasi ini, Anda mungkin perlu memilih Wilayah baru tempat Anda dapat menyebarkan sumber daya.

#### AWS CLI

Jalankan perintah berikut untuk melihat daftar Availability zone. Pastikan untuk menentukan jenis instans pilihan Anda dan Wilayah (*us-east-1*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

Untuk informasi selengkapnya tentang perintah ini, lihat [describe-instance-type-offerings](#) di Referensi AWS CLI Perintah.

Saat menjalankan perintah ini, jika Anda menerima kesalahan, pastikan Anda menggunakan versi terbaru AWS CLI. Untuk informasi selengkapnya, lihat [Pemecahan Masalah](#) di AWS Command Line Interface Panduan Pengguna.

2. Coba gunakan sumber AWS daya lagi dan tentukan zona Ketersediaan yang mendukung jenis instans pilihan Anda.

Untuk mencoba kembali menyebarkan sumber daya AWS

1. Siapkan Region default dalam `bin/cdk-gd-tester.ts` file.
2. Untuk menentukan zona ketersediaan, buka `amazon-guardduty-tester/lib/common/network/vpc.ts` file.
3. Dalam file ini, ganti `maxAzs: 2`, dengan `availabilityZones: ['us-east-1a', 'us-east-1c']`, tempat Anda harus menentukan zona Ketersediaan untuk jenis instans Anda.
4. Lanjutkan dengan langkah-langkah yang tersisa di bawah [Langkah-langkah untuk menyebarkan sumber daya AWS](#).

## Tingkat keparahan untuk GuardDuty temuan

Setiap GuardDuty temuan memiliki tingkat keparahan dan nilai yang ditetapkan yang mencerminkan potensi risiko temuan tersebut terhadap jaringan Anda sebagaimana ditentukan oleh teknisi keamanan kami. Nilai tingkat keparahan dapat jatuh di mana saja dalam kisaran 1,0 hingga 8,9, dengan nilai yang lebih tinggi menunjukkan risiko keamanan yang lebih besar. Untuk membantu Anda menentukan respons terhadap masalah keamanan potensial yang disorot oleh temuan, GuardDuty uraikan rentang ini menjadi tingkat keparahan Tinggi, Sedang, dan Rendah.

### Note

Nilai 0 dan antara 9.0 dan 10.0 dicadangkan untuk penggunaan masa depan.

Berikut ini adalah tingkat keparahan dan nilai yang ditentukan saat ini untuk GuardDuty temuan serta rekomendasi umum untuk masing-masing:

| Tingkat kepelikan | Rentang nilai |
|-------------------|---------------|
|-------------------|---------------|

|        |           |
|--------|-----------|
| Tinggi | 7.0 - 8.9 |
|--------|-----------|

Tingkat keparahan yang tinggi menunjukkan bahwa sumber daya yang dimaksud (EC2 contoh atau sekumpulan kredensial masuk IAM pengguna) dikompromikan dan secara aktif digunakan untuk tujuan yang tidak sah.

Kami merekomendasikan agar Anda memprioritaskan masalah keamanan temuan dengan tingkat kepelikan Tinggi dan segera mengambil langkah-langkah perbaikan untuk mencegah penggunaan yang tidak sah lainnya atas sumber daya Anda. Misalnya, bersihkan EC2 instance Anda atau hentikan, atau putar IAM kredensialnya. Lihat [Langkah-langkah Perbaikan](#) untuk detail selengkapnya.

|        |           |
|--------|-----------|
| Sedang | 4.0 - 6,9 |
|--------|-----------|

Tingkat kepelikan Sedang menunjukkan aktivitas mencurigakan yang menyimpang dari perilaku normal yang diamati dan, tergantung kasus penggunaan Anda, mungkin mengindikasikan penyusupan sumber daya.

Kami merekomendasikan agar Anda segera menyelidiki sumber daya yang bersangkutan. Langkah-langkah perbaikan akan bervariasi menurut keluarga sumber daya dan temuan, tetapi secara umum, Anda harus mengonfirmasi bahwa aktivitas tersebut sah dan konsisten dengan kasus penggunaan Anda. Jika Anda tidak dapat mengidentifikasi penyebabnya, atau mengonfirmasi aktivitas tersebut sebagai aktivitas yang sah, Anda harus mempertimbangkan bahwa sumber daya mungkin telah disusupi dan melakukan [Langkah-langkah Perbaikan](#) untuk mengamankan sumber daya.

Berikut adalah beberapa hal yang perlu dipertimbangkan ketika meninjau temuan tingkat Sedang:

- Periksa apakah pengguna yang berwenang telah menginstal perangkat lunak baru yang mengubah perilaku sumber daya (misalnya, mengizinkan lalu lintas yang lebih tinggi dari biasanya, atau mengaktifkan komunikasi pada port baru).
- Periksa apakah pengguna yang berwenang mengubah pengaturan panel kontrol, misalnya, mengubah pengaturan grup keamanan.
- Jalankan pemindaian anti-virus pada sumber daya yang bersangkutan untuk mendeteksi perangkat lunak yang tidak sah.

| Tingkat kepelikan   | Rentang nilai |
|---|---------------|
| <ul style="list-style-type: none"><li>Verifikasi izin yang dilampirkan ke IAM peran, pengguna, grup, atau kumpulan kredensial yang terlibat. Ini mungkin harus diubah atau diputar.</li></ul> |               |
| Rendah  | 1.0 - 3.9     |

Tingkat kepelikan rendah menunjukkan upaya aktivitas mencurigakan yang tidak membahayakan jaringan Anda, misalnya, pemindaian port atau upaya penyusupan yang gagal.

Tidak ada tindakan yang disarankan segera dilakukan, tetapi ada baiknya untuk mencatat informasi ini karena mungkin mengindikasikan bahwa seseorang sedang mencari titik lemah di jaringan Anda.

## Meninjau temuan GuardDuty

Gunakan prosedur berikut untuk meninjau dan memahami GuardDuty temuan Anda.

- Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Pilih Temuan lalu pilih temuan tertentu untuk melihat detailnya.

Detail untuk setiap temuan akan berbeda tergantung tipe temuan, sumber daya yang bersangkutan, dan sifat dari aktivitas tersebut. Untuk informasi selengkapnya tentang bidang temuan yang tersedia, lihat [Detail temuan](#).

- (Opsional) Jika Anda ingin mengarsipkan temuan, pilih dari daftar temuan Anda, lalu pilih menu Tindakan. Kemudian pilih Arsip.

Temuan yang diarsipkan dapat dilihat dengan memilih Diarsipkan dari menu tarik-turun Saat ini.

Saat ini GuardDuty pengguna dari akun GuardDuty anggota tidak dapat mengarsipkan temuan.

### Important

Jika Anda mengarsipkan temuan secara manual melalui prosedur di atas, semua kejadian berikutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) akan ditambahkan ke daftar temuan Anda saat ini. Untuk tidak pernah melihat temuan ini

dalam daftar saat ini, Anda dapat mengarsipkannya secara otomatis. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

- (Opsional) Untuk mengunduh temuan, pilih dari daftar temuan Anda, lalu pilih menu Tindakan. Kemudian pilih Ekspor. Saat Anda Mengekspor temuan, Anda dapat melihat JSON dokumen lengkapnya.

#### Note

Dalam beberapa kasus GuardDuty, menyadari bahwa temuan tertentu adalah positif palsu setelah dihasilkan. GuardDuty menyediakan bidang Keyakinan dalam temuanJSON, dan menetapkan nilainya ke nol. Dengan cara ini GuardDuty memungkinkan Anda tahu bahwa Anda dapat dengan aman mengabaikan temuan tersebut.

## Detail temuan

Di GuardDuty konsol Amazon, Anda dapat melihat detail pencarian di bagian ringkasan pencarian. Detail menemukan bervariasi berdasarkan jenis temuan.


Ada dua detail utama yang menentukan jenis informasi apa yang tersedia untuk temuan apa pun. Yang pertama adalah jenis sumber daya, yang dapat berupa InstanceAccessKey,S3Bucket,S3Object,Kubernetes cluster,ECS cluster,Container,RDSDBInstance, atauLambda. Detail kedua yang menentukan informasi temuan adalah Peran Sumber Daya. Peran sumber daya dapat Target untuk kunci akses, artinya sumber daya adalah target aktivitas yang mencurigakan. Untuk temuan tipe instans, peran sumber daya juga dapat menjadi Actor, yang berarti bahwa sumber daya Anda adalah aktor yang melakukan aktivitas mencurigakan. Topik ini menjelaskan beberapa detail umum yang tersedia untuk temuan.

## Menemukan ikhtisar

Bagian Ikhtisar temuan berisi fitur pengenalan paling dasar dari temuan, termasuk informasi berikut:

- ID Akun — ID AWS akun tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.

- **Hitung** — Jumlah kali GuardDuty telah mengumpulkan aktivitas yang cocok dengan pola ini dengan ID temuan ini.
- **Dibuat pada** — Waktu dan tanggal ketika temuan ini pertama kali dibuat. Jika nilai ini berbeda dari Diperbarui pada, ini menunjukkan bahwa aktivitas tersebut telah terjadi beberapa kali dan merupakan masalah yang sedang berlangsung.

 Note

Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara JSON ekspor dan CLI output menampilkan stempel waktu masuk. UTC

- **Finding ID** — Pengidentifikasi unik untuk jenis temuan ini dan kumpulan parameter. Kejadian baru dari aktivitas yang cocok dengan pola ini akan digabungkan ke ID yang sama.
- **Tipe temuan** – String berformat yang mewakili tipe aktivitas yang memicu temuan. Untuk informasi selengkapnya, lihat [GuardDuty format temuan](#).
- **Wilayah** — AWS Wilayah di mana temuan itu dihasilkan. Untuk informasi selengkapnya tentang Wilayah yang didukung, lihat [Wilayah dan titik akhir](#)
- **ID Sumber Daya** — ID AWS sumber daya tempat aktivitas berlangsung yang mendorong GuardDuty untuk menghasilkan temuan ini.
- **ID Pindai** — Berlaku untuk temuan saat Perlindungan GuardDuty Malware untuk EC2 diaktifkan, ini adalah pengenalan pemindaian malware yang berjalan pada EBS volume yang dilampirkan pada EC2 instans atau beban kerja kontainer yang berpotensi dikompromikan. Untuk informasi selengkapnya, lihat [Perlindungan Malware untuk EC2 menemukan detail](#).
- **Keparahan** — Tingkat keparahan yang ditetapkan temuan baik Tinggi, Sedang, atau Rendah. Untuk informasi selengkapnya, lihat [Tingkat keparahan untuk GuardDuty temuan](#).
- **Diperbarui di** — Terakhir kali temuan ini diperbarui dengan aktivitas baru yang cocok dengan pola yang mendorong GuardDuty untuk menghasilkan temuan ini.

## Sumber Daya

Sumber daya yang terpengaruh memberikan rincian tentang AWS sumber daya yang ditargetkan oleh aktivitas inisiasi. Informasi yang tersedia bervariasi berdasarkan tipe sumber daya dan tipe tindakan.

Peran sumber daya — Peran AWS sumber daya yang memulai temuan. Nilai ini bisa TARGET atau ACTOR, dan mewakili apakah sumber daya Anda adalah target aktivitas mencurigakan atau aktor yang melakukan aktivitas mencurigakan.

Jenis sumber daya — Jenis sumber daya yang terpengaruh. Jika beberapa sumber daya terlibat, temuan dapat mencakup beberapa jenis sumber daya. Jenis sumber daya adalah Instance, S3Bucket AccessKey, S3Object, Container, KubernetesCluster ECSCluster, dan Lambda. RDSDBInstance Tergantung tipe sumber dayanya, detail temuan yang berbeda tersedia. Pilih tab opsi sumber daya untuk mempelajari detail yang tersedia untuk sumber daya tersebut.

## Instance

Detail contoh:

### Note

Beberapa detail instance mungkin hilang jika instance telah dihentikan atau jika API pemanggilan yang mendasarinya berasal dari EC2 instance di Wilayah lain saat melakukan panggilan Lintas wilayah. API

- ID Instance — ID dari EC2 instance yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Jenis Instance — Jenis EC2 instance yang terlibat dalam temuan.
- Waktu Peluncuran - Waktu dan tanggal peluncuran instans.
- Outpost ARN — Nama Sumber Daya Amazon (ARN) dari. AWS Outposts Hanya berlaku untuk AWS Outposts instance. Untuk informasi selengkapnya, lihat [Apa itu AWS Outposts?](#)
- Nama Grup Keamanan – Nama Grup Keamanan yang melekat pada instans yang terlibat.
- ID Grup Keamanan – ID grup keamanan yang melekat pada instans yang terlibat.
- Status instans – Status instans yang ditargetkan saat ini.
- Availability Zone – Availability Zone AWS Region tempat instans yang terlibat berada.
- ID Image – ID dari Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.
- Deskripsi Image – Deskripsi ID Amazon Machine Image yang digunakan untuk membangun instans yang terlibat dalam aktivitas.



- Tanda – Daftar tanda yang melekat pada sumber daya ini, tercantum dalam format `key:value`.

## AccessKey

### Akses Detail Kunci:

- ID kunci akses — ID kunci akses pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Principal ID — ID utama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Jenis pengguna — Jenis pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan. Untuk informasi lebih lanjut, lihat [CloudTrail userIdentity elemen](#).
- Nama pengguna — Nama pengguna yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

## S3Bucket

### Detail ember Amazon S3:

- Nama – Nama bucket yang terlibat dalam temuan.
- ARN— Ember yang terlibat dalam temuan. ARN
- Pemilik – ID pengguna resmi dari pengguna yang memiliki bucket yang terlibat dalam temuan. Untuk informasi selengkapnya tentang pengguna kanonik, IDs lihat pengenalan [AWS akun](#).
- Tipe – Tipe temuan bucket, dapat berupa Tujuan atau Sumber.
- Enkripsi sisi server default — Detail enkripsi untuk bucket.
- Tag Bucket — Daftar tag yang dilampirkan pada sumber daya ini, tercantum dalam format `key:value`.
- Izin Efektif – Evaluasi dari semua izin dan kebijakan efektif pada bucket yang menunjukkan apakah bucket yang terlibat diekspos secara publik. Nilai dapat bersifat publik atau tidak publik.

## S3Object

- Detail objek S3 - Termasuk informasi berikut tentang objek S3 yang dipindai:
  - ARN— Nama Sumber Daya Amazon (ARN) dari objek S3 yang dipindai.
  - Kunci — Nama yang ditetapkan ke file saat dibuat di bucket S3.

- **Id Versi** — Bila Anda telah mengaktifkan versi bucket, bidang ini menunjukkan Id versi yang terkait dengan versi terbaru dari objek S3 yang dipindai. Untuk informasi selengkapnya, lihat [Menggunakan pembuatan versi di bucket S3 di Panduan Pengguna Amazon S3](#).
- **eTag**— Merupakan versi spesifik dari objek S3 yang dipindai.
- **Hash** — Hash dari ancaman yang terdeteksi dalam temuan ini.
- **Detail bucket S3** — Menyertakan informasi berikut tentang bucket Amazon S3 yang terkait dengan objek S3 yang dipindai:
  - **Nama** - Menunjukkan nama bucket S3 yang berisi objek.
  - **ARN**— Nama Sumber Daya Amazon (ARN) dari ember S3.
  - **Pemilik** — Id Canonical dari pemilik bucket S3.

## EKSCluster

Detail klaster Kubernetes:

- **Nama** — Nama cluster Kubernetes.
- **ARN**— ARN Yang mengidentifikasi cluster.
- **Created At** — Waktu dan tanggal ketika cluster ini dibuat.

### Note

Stempel waktu untuk temuan di GuardDuty konsol muncul di zona waktu lokal Anda, sementara JSON ekspor dan CLI output menampilkan stempel waktu masuk. UTC

- **VPCID** — ID VPC yang terkait dengan cluster Anda.
- **Status** — Status cluster saat ini.
- **Tag** — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format `key:value`. Anda bisa menentukan kunci dan nilai.

Tag cluster tidak menyebar ke sumber daya lain yang terkait dengan cluster.

Detail beban kerja Kubernetes:

- **Jenis** - Jenis beban kerja Kubernetes, seperti pod, deployment, dan job.

- Nama — Nama beban kerja Kubernetes.
- Uid — ID unik dari beban kerja Kubernetes.
- Dibuat pada - Waktu dan tanggal ketika beban kerja ini dibuat.
- Label — Pasangan nilai kunci yang melekat pada beban kerja Kubernetes.
- Container — Detail kontainer yang berjalan sebagai bagian dari beban kerja Kubernetes.
- Namespace — Beban kerja milik namespace Kubernetes ini.
- Volume — Volume yang digunakan oleh beban kerja Kubernetes.
  - Jalur host - Merupakan file atau direktori yang sudah ada sebelumnya di mesin host tempat volume dipetakan.
  - Nama — Nama volume.
- konteks keamanan pod — Mendefinisikan pengaturan privilege dan akses control untuk semua kontainer dalam sebuah pod.
- Jaringan host — Setel ke `true` jika pod disertakan dalam beban kerja Kubernetes.

#### Detail pengguna Kubernetes:

- Grup — Kubernetes RBAC (kontrol berbasis akses peran) kelompok pengguna yang terlibat dalam aktivitas yang menghasilkan temuan.
- ID — ID unik dari pengguna Kubernetes.
- Nama pengguna — Nama pengguna Kubernetes yang terlibat dalam aktivitas yang menghasilkan temuan.
- Nama sesi — Entitas yang mengambil IAM peran dengan izin KubernetesRBAC.

## ECSCluster

#### ECSrincian cluster:

- ARN— ARN Yang mengidentifikasi cluster.
- Nama — Nama cluster.
- Status — Status cluster saat ini.
- Jumlah layanan aktif — Jumlah layanan yang berjalan di cluster dalam suatu ACTIVE keadaan. Anda dapat melihat layanan ini dengan [ListServices](#)
- Jumlah instans kontainer terdaftar — Jumlah instance kontainer yang terdaftar ke dalam klaster. Ini termasuk instance kontainer di keduanya ACTIVE dan DRAINING status.

- Menjalankan tugas menghitung — Jumlah tugas di cluster yang berada dalam RUNNING status.
- Tag — Metadata yang Anda terapkan ke cluster untuk membantu Anda mengkategorikan dan mengaturnya. Setiap tag terdiri dari kunci dan nilai opsional, yang tercantum dalam format `key:value`. Anda bisa menentukan kunci dan nilai.
- Kontainer — Detail tentang wadah yang terkait dengan tugas:
  - Nama kontainer — Nama wadah.
  - Gambar kontainer — Gambar wadah.
- Detail tugas — Detail tugas dalam sebuah cluster.
  - ARN— Nama Sumber Daya Amazon (ARN) dari tugas.
  - Definisi ARN — Nama Sumber Daya Amazon (ARN) dari definisi tugas yang membuat tugas.
  - Versi - Penghitung versi untuk tugas tersebut.
  - Tugas dibuat di — Stempel waktu Unix saat tugas dibuat.
  - Tugas dimulai pada — Stempel waktu Unix saat tugas dimulai.
  - Tugas dimulai oleh — Tag yang ditentukan saat tugas dimulai.

## Container

### Detail kontainer:

- Container runtime — Container runtime (seperti `docker` atau `containerd`) yang digunakan untuk menjalankan container.
- ID - ID contoh kontainer atau ARN entri lengkap untuk instance kontainer.
- Nama — Nama wadah.

Bila tersedia, bidang ini menampilkan nilai `labelio.kubernetes.container.name`.

- Gambar - Gambar dari contoh kontainer.
- Volume mount — Daftar dudukan volume kontainer. Sebuah wadah dapat memasang volume di bawah sistem file-nya.
- Konteks keamanan — Konteks keamanan kontainer mendefinisikan hak istimewa dan pengaturan kontrol akses untuk kontainer.
- Detail proses — Menjelaskan detail proses yang terkait dengan temuan.

## RDSDBInstance

RDSDBInstancerincian:

### Note

Sumber daya ini tersedia dalam temuan RDS Perlindungan yang terkait dengan instance database.

- Database Instance ID — Pengidentifikasi yang terkait dengan instance database yang terlibat dalam GuardDuty temuan.
- Engine — Nama mesin database dari instance database yang terlibat dalam temuan. Nilai yang mungkin adalah Aurora My SQL -Compatible atau Aurora Postgre -Compatible. SQL
- Versi mesin — Versi mesin database yang terlibat dalam GuardDuty temuan.
- Database cluster ID — Pengidentifikasi cluster database yang berisi ID instance database yang terlibat dalam GuardDuty temuan.
- Database instance ARN — ARN Yang mengidentifikasi instance database yang terlibat dalam GuardDuty temuan.

## Lambda

Detail fungsi Lambda

- Nama fungsi — Nama fungsi Lambda yang terlibat dalam temuan.
- Versi fungsi — Versi fungsi Lambda yang terlibat dalam temuan.
- Deskripsi fungsi — Deskripsi fungsi Lambda yang terlibat dalam temuan.
- Fungsi ARN — Nama Sumber Daya Amazon (ARN) dari fungsi Lambda yang terlibat dalam temuan.
- ID Revisi — ID revisi versi fungsi Lambda.
- Peran — Peran eksekusi fungsi Lambda yang terlibat dalam temuan.
- VPCkonfigurasi - VPC Konfigurasi Amazon, termasuk VPC ID, grup keamanan, dan subnet yang IDs terkait dengan fungsi Lambda Anda.
- VPCID — ID Amazon VPC yang terkait dengan fungsi Lambda yang terlibat dalam temuan.

- Subnet IDs — ID subnet yang terkait dengan fungsi Lambda Anda.
- Grup Keamanan — Kelompok keamanan yang melekat pada fungsi Lambda yang terlibat. Ini termasuk nama grup keamanan dan ID grup.
- Tag — Daftar tag yang dilampirkan ke sumber daya ini, tercantum dalam format `key: value` pasangan.

## RDSdatabase (DB) detail pengguna

### Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan fitur RDS Perlindungan di GuardDuty. Untuk informasi selengkapnya, lihat [GuardDuty RDSPerlindungan](#).

GuardDuty Temuan ini memberikan rincian pengguna dan otentikasi berikut dari database yang berpotensi dikompromikan.

- Pengguna — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
- Aplikasi — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
- Database — Nama instance database yang terlibat dalam upaya login anomali.
- SSL— Versi Secure Socket Layer (SSL) yang digunakan untuk jaringan.
- Metode autentikasi — Metode otentikasi yang digunakan oleh pengguna yang terlibat dalam temuan.

## Detail penemuan Runtime Monitoring

### Note

Detail ini mungkin tersedia hanya jika GuardDuty menghasilkan salah satu [Jenis penemuan Runtime Monitoring](#).

Bagian ini berisi rincian runtime seperti detail proses dan konteks yang diperlukan. Detail proses menjelaskan informasi tentang proses yang diamati dan konteks runtime menjelaskan informasi tambahan apa pun tentang aktivitas yang berpotensi mencurigakan.

## Detail proses

- Nama — Nama proses.
- Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
- Executable SHA -256 — SHA256 Hash dari proses yang dapat dieksekusi.
- Namespace PID — ID proses proses di namespace sekunder selain PID namespace tingkat host. PID Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
- Direktori kerja saat ini — Direktori kerja saat ini dari proses.
- ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
- startTime— Waktu ketika proses dimulai. Ini dalam format string UTC tanggal (2023-03-22T19:37:20.168Z).
- UUID— ID unik yang ditetapkan untuk proses oleh GuardDuty.
- Induk UUID — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
- Pengguna — Pengguna yang menjalankan proses.
- User ID — ID pengguna yang menjalankan proses.
- ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.
- Silsilah — Informasi tentang nenek moyang proses.
  - ID Proses — ID yang ditetapkan untuk proses oleh sistem operasi.
  - UUID— ID unik yang ditetapkan untuk proses oleh GuardDuty.
  - Jalur yang dapat dieksekusi — Jalur absolut dari file yang dapat dieksekusi proses.
  - ID pengguna yang efektif — ID pengguna yang efektif dari proses pada saat acara berlangsung.
  - Induk UUID — ID unik dari proses induk. ID ini ditetapkan ke proses induk oleh GuardDuty.
  - Waktu Mulai — Waktu ketika proses dimulai.
  - Namespace PID — ID proses proses di namespace sekunder selain PID namespace tingkat host. PID Untuk proses di dalam wadah, itu adalah ID proses yang diamati di dalam wadah.
  - User ID — User ID pengguna yang menjalankan proses.
  - Nama — Nama proses.

## Konteks runtime

Dari bidang berikut, temuan yang dihasilkan mungkin hanya mencakup bidang-bidang yang relevan dengan jenis temuan.

- Mount Source - Jalur pada host yang dipasang oleh wadah.
- Mount Target - Jalur dalam wadah yang dipetakan ke direktori host.
- Jenis Sistem File - Merupakan jenis sistem file yang dipasang.
- Bendera - Merupakan opsi yang mengontrol perilaku acara yang terlibat dalam temuan ini.
- Memodifikasi Proses — Informasi tentang proses yang membuat atau memodifikasi biner, skrip, atau pustaka, di dalam wadah saat runtime.
- Modified At — Stempel waktu di mana proses membuat atau memodifikasi biner, skrip, atau pustaka di dalam wadah saat runtime. Bidang ini dalam format string UTC tanggal (2023-03-22T19:37:20.168Z).
- Library Path — Jalur ke perpustakaan baru yang dimuat.
- LD Preload Value — Nilai variabel LD\_PRELOAD lingkungan.
- Socket Path — Jalur ke soket Docker yang diakses.
- Runc Binary Path — Jalan menuju runc biner.
- Release Agent Path - Jalur ke file agen cgroup rilis.
- Contoh Baris Perintah — Contoh baris perintah yang terlibat dalam aktivitas yang berpotensi mencurigakan.
- Kategori Alat - Kategori yang dimiliki alat tersebut. Beberapa contohnya adalah Backdoor Tool, Pentest Tool, Network Scanner, dan Network Sniffer.
- Nama Alat — Nama alat yang berpotensi mencurigakan.
- Script Path — Jalur ke skrip yang dieksekusi yang menghasilkan temuan.
- Threat File Path — Jalur mencurigakan di mana rincian intelijen ancaman ditemukan.
- Nama Layanan — Nama layanan keamanan yang telah dinonaktifkan.

## EBSdetail pemindaian volume

### Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai. [Perlindungan Malware untuk EC2](#)

Pemindaian EBS volume memberikan detail tentang EBS volume yang dilampirkan pada EC2 instans atau beban kerja kontainer yang berpotensi dikompromikan.



- Scan ID — Pengidentifikasi pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu ketika pemindaian malware dimulai.
- Pemindaian selesai pada — Tanggal dan waktu pemindaian malware selesai.
- Trigger Finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.
- Sumber — Nilai potensial adalah `Bitdefender` dan `Amazon`.
- Deteksi pemindaian — Tampilan lengkap detail dan hasil untuk setiap pemindaian malware.
  - Jumlah item yang dipindai - Jumlah total file yang dipindai. Ini memberikan rincian seperti `totalGb`, `files`, dan `volumes`.
  - Jumlah item yang terdeteksi ancaman — Jumlah total berbahaya yang `files` terdeteksi selama pemindaian.
  - Detail ancaman tingkat keparahan tertinggi — Rincian ancaman tingkat keparahan tertinggi yang terdeteksi selama pemindaian dan jumlah file berbahaya. Ini memberikan rincian seperti `severity`, `threatName`, dan `count`.
  - Ancaman terdeteksi oleh Nama - Elemen kontainer mengelompokkan ancaman dari semua tingkat keparahan. Ini memberikan rincian seperti `itemCount`, `uniqueThreatNameCount`, `shortened`, dan `threatNames`.

## Perlindungan Malware untuk EC2 menemukan detail

### Note

Bagian ini berlaku untuk temuan saat Anda mengaktifkan GuardDuty pemindaian malware yang dimulai. [Perlindungan Malware untuk EC2](#)

Saat Perlindungan Malware untuk EC2 pemindaian mendeteksi malware, Anda dapat melihat detail pemindaian dengan memilih temuan yang sesuai di halaman Temuan di <https://console.aws.amazon.com/guardduty/konsol>. Tingkat keparahan Perlindungan Malware Anda untuk EC2 menemukan tergantung pada tingkat keparahan GuardDuty temuan.

### Note

`GuardDutyFindingDetectedTag` menentukan bahwa snapshot berisi malware.

Informasi berikut tersedia di bawah bagian Ancaman terdeteksi di panel detail.

- Nama — Nama ancaman, diperoleh dengan mengelompokkan file dengan deteksi.
- Keparahan — Tingkat keparahan ancaman yang terdeteksi.
- Hash — The SHA -256 dari file.
- Jalur file — Lokasi file berbahaya dalam EBS volume.
- Nama file — Nama file di mana ancaman terdeteksi.
- Volume ARN — ARN Volume yang dipindai EBS.

Informasi berikut tersedia di bawah bagian Detail pemindaian Malware di panel detail.

- Scan ID — ID pemindaian dari pemindaian malware.
- Pemindaian dimulai pada — Tanggal dan waktu pemindaian dimulai.
- Pemindaian selesai pada — Tanggal dan waktu pemindaian selesai.
- File yang dipindai — Jumlah total file dan direktori yang dipindai.
- Total GB yang dipindai — Jumlah penyimpanan yang dipindai selama proses berlangsung.
- Trigger finding ID — ID temuan dari GuardDuty temuan yang memulai pemindaian malware ini.
- Informasi berikut tersedia di bawah bagian Detail volume di panel detail.
  - Volume ARN — Nama Sumber Daya Amazon (ARN) dari volume.
  - Snapshot ARN — Snapshot dari volume. ARN EBS
  - Status — Status pemindaian volume, seperti `Running`, `Skipped`, dan `Completed`.
  - Jenis enkripsi — Jenis enkripsi yang digunakan untuk mengenkripsi volume. Misalnya, `CMMK`.
  - Nama perangkat — Nama perangkat. Misalnya, `/dev/xvda`.

## Perlindungan Malware untuk detail penemuan S3

Detail pemindaian malware berikut tersedia saat Anda mengaktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3 di: Akun AWS

- Ancaman — Daftar ancaman yang terdeteksi selama pemindaian malware.

Untuk informasi tentang jumlah ancaman yang dapat disertakan dalam temuan tersebut, lihat [Kuota dalam Perlindungan Malware untuk S3](#).

- Jalur item - Daftar jalur item bersarang dan detail hash dari objek S3 yang dipindai.

- Jalur item bersarang - Jalur item dari objek S3 yang dipindai tempat ancaman terdeteksi.

Nilai bidang ini hanya tersedia jika objek tingkat atas adalah arsip dan jika ancaman terdeteksi di dalam arsip.

- Hash — Hash dari ancaman yang terdeteksi dalam temuan ini.
- Sumber — Nilai potensial adalah Bitdefender dan Amazon.


## Tindakan

Tindakan temuan memberikan rincian tentang jenis aktivitas yang memicu temuan. Informasi yang tersedia bervariasi berdasarkan tipe tindakan.

Tipe tindakan – Tipe aktivitas temuan. Nilai ini bisa NETWORK\_CONNECTION, PORT\_PROBE, DNS\_REQUEST, AWS\_API\_CALL, atau RDS\_LOGIN\_ATTEMPT. Informasi yang tersedia bervariasi berdasarkan tipe tindakan:

- NETWORK\_CONNECTION — Menunjukkan bahwa lalu lintas jaringan dipertukarkan antara EC2 instance yang diidentifikasi dan host jarak jauh. Tipe tindakan ini memiliki informasi tambahan berikut:
  - Arah koneksi — Arah koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan. Nilai bisa jadi salah satu dari nilai berikut:
    - INBOUND— Menunjukkan bahwa host jarak jauh memulai koneksi ke port lokal pada EC2 instance yang diidentifikasi di akun Anda.
    - OUTBOUND— Menunjukkan bahwa EC2 instance yang diidentifikasi memulai koneksi ke host jarak jauh.
    - UNKNOWN— Menunjukkan bahwa tidak GuardDuty dapat menentukan arah koneksi.
  - Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
  - IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya alamat IP dari sebuah EKS pod sebagai lawan dari alamat IP dari instance di mana EKS pod berjalan.
  - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- PORT\_PROBE — Menunjukkan bahwa host jarak jauh memeriksa EC2 instance yang diidentifikasi pada beberapa port terbuka. Tipe tindakan ini memiliki informasi tambahan berikut:

- IP lokal — Alamat IP sumber asli dari lalu lintas yang memicu temuan. Info ini dapat digunakan untuk membedakan antara alamat IP dari lapisan perantara yang dilalui arus lalu lintas, dan alamat IP sumber asal dari lalu lintas yang memicu temuan. Misalnya alamat IP dari sebuah EKS pod sebagai lawan dari alamat IP dari instance di mana EKS pod berjalan.
- Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- DNS\_REQUEST — Menunjukkan bahwa EC2 instance yang diidentifikasi menanyakan nama domain. Tipe tindakan ini memiliki informasi tambahan berikut:
  - Protokol — Protokol koneksi jaringan diamati dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
  - Diblokir – Menunjukkan apakah port yang ditargetkan diblokir.
- AWS\_API\_CALL — Menunjukkan bahwa AWS API an dipanggil. Tipe tindakan ini memiliki informasi tambahan berikut:
  - API— Nama API operasi yang dipanggil dan dengan demikian diminta GuardDuty untuk menghasilkan temuan ini.

 Note

Operasi ini juga dapat mencakup API non-peristiwa yang ditangkap oleh AWS CloudTrail. Untuk informasi selengkapnya, lihat [API Non-event yang ditangkap oleh CloudTrail](#).

- User Agent — Agen pengguna yang membuat API permintaan. Nilai ini memberi tahu Anda apakah panggilan dilakukan dari, AWS layanan AWS SDKs, atau AWS CLI. AWS Management Console
- ERRORCODE— Jika temuan dipicu oleh API panggilan gagal, ini menampilkan kode kesalahan untuk panggilan itu.
- Nama layanan — DNS Nama layanan yang mencoba melakukan API panggilan yang memicu temuan.
- RDS\_LOGIN\_ATTEMPT - Menunjukkan bahwa upaya login dilakukan ke database yang berpotensi dikompromikan dari alamat IP jarak jauh.
  - Alamat IP — Alamat IP jarak jauh yang digunakan untuk melakukan upaya login yang berpotensi mencurigakan.

## Aktor atau Target

Temuan memiliki bagian Aktor jika peran Sumber Daya adalah TARGET. Ini menunjukkan bahwa sumber daya Anda ditargetkan oleh aktivitas mencurigakan, dan bagian Aktor berisi detail tentang entitas yang menargetkan sumber daya Anda.

Temuan memiliki bagian Target jika peran Sumber Daya adalah ACTOR. Hal ini menunjukkan bahwa sumber daya Anda terlibat dalam aktivitas yang mencurigakan terhadap host jarak jauh, dan bagian ini berisi informasi tentang IP atau domain yang ditargetkan sumber daya Anda.

Informasi yang tersedia di bagian Aktor atau Target dapat mencakup hal-hal berikut:

- Afiliasi — Detail tentang apakah AWS akun API penelepon jarak jauh terkait dengan lingkungan Anda GuardDuty . Jika nilai `init>true`, API penelepon berafiliasi dengan akun Anda dalam beberapa cara; jika `false`, API penelepon berasal dari luar lingkungan Anda.
- ID Akun Jarak Jauh — ID akun yang memiliki alamat IP keluar yang digunakan untuk mengakses sumber daya di jaringan akhir.
- Alamat IP — Alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Lokasi — Informasi lokasi untuk alamat IP yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.
- Organisasi — informasi ISP organisasi dari alamat IP yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Port — Nomor port yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Domain — Domain yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Domain dengan akhiran — Domain tingkat kedua dan teratas yang terlibat dalam aktivitas yang berpotensi mendorong GuardDuty untuk menghasilkan temuan. [Untuk daftar domain tingkat atas dan tingkat kedua, lihat daftar akhiran publik.](#)

## Informasi tambahan

Semua temuan memiliki bagian Informasi tambahan yang dapat mencakup informasi berikut:

- Nama daftar ancaman — Nama daftar ancaman yang mencakup alamat IP atau nama domain yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

- Sampel — Nilai benar atau salah yang menunjukkan apakah ini adalah temuan sampel.
- Diarsipkan — Nilai benar atau salah yang menunjukkan apakah temuan ini telah diarsipkan.
- Tidak biasa — Detail aktivitas yang tidak diamati secara historis. Ini dapat mencakup pengguna yang tidak biasa (sebelumnya tidak diamati), lokasi, waktu, bucket, perilaku login, atau ASN Org.
- Protokol yang tidak biasa — Protokol koneksi jaringan yang terlibat dalam aktivitas yang mendorong GuardDuty untuk menghasilkan temuan.
- Detail agen — Detail tentang agen keamanan yang saat ini digunakan di EKS cluster di Anda Akun AWS. Ini hanya berlaku untuk jenis pencarian EKS Runtime Monitoring.
  - Versi agen — Versi agen GuardDuty keamanan.
  - Agen Id — Identifier unik dari agen GuardDuty keamanan.

## Bukti

Temuan berdasarkan intelijen ancaman memiliki bagian Bukti yang mencakup informasi berikut:

- Detail intelijen ancaman — Nama daftar ancaman tempat yang dikenali Threat name muncul.
- Nama ancaman — Nama keluarga malware atau pengenalan lain yang terkait dengan ancaman.
- File ancaman SHA256 — SHA256 dari file yang menghasilkan temuan.

## Perilaku anomali

Jenis temuan yang berakhir AnomalousBehavior menunjukkan bahwa temuan tersebut dihasilkan oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API permintaan ke akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan taktik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta.

Detail tentang faktor API permintaan yang tidak biasa untuk identitas CloudTrail pengguna yang memanggil permintaan dapat ditemukan dalam rincian temuan. Identitas didefinisikan oleh [CloudTrail userIdentity Elemen](#), dan nilai yang mungkin adalah:Root,,IAMUser,AssumedRole, FederatedUserAWSAccount, atauAWSService.

Selain rincian yang tersedia untuk semua GuardDuty temuan yang terkait dengan API aktivitas, AnomalousBehavior temuan memiliki rincian tambahan yang diuraikan di bagian berikut. Detail ini dapat dilihat di konsol dan juga tersedia di temuanJSON.

- Anomali APIs — Daftar API permintaan yang dipanggil oleh identitas pengguna di dekat API permintaan utama yang terkait dengan temuan. Panel ini selanjutnya memecah detail API acara dengan cara berikut.
  - Yang pertama API terdaftar adalah yang utama API, yang merupakan API permintaan yang terkait dengan aktivitas diamati dengan risiko tertinggi. Ini adalah API yang memicu temuan dan berkorelasi dengan tahap serangan dari jenis temuan. Ini juga API yang dirinci di bawah bagian Tindakan di konsol, dan di temuannya JSON.
  - Yang APIs terdaftar lainnya adalah anomali tambahan APIs dari identitas pengguna yang terdaftar yang diamati di dekat primer. API Jika hanya ada satu dalam API daftar, model ML tidak mengidentifikasi API permintaan tambahan apa pun dari identitas pengguna tersebut sebagai anomali.
  - Daftar APIs dibagi berdasarkan apakah an berhasil API dipanggil, atau jika tidak berhasil dipanggil, yang berarti respons kesalahan diterima. API Jenis respon kesalahan yang diterima tercantum di atas setiap gagal dipanggil API. Jenis respon kesalahan yang mungkin adalah: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found`, dan `operation not permitted`.
  - APIs dikategorikan oleh layanan terkait mereka.
  - Untuk konteks lebih lanjut, pilih Historis APIs untuk melihat detail tentang bagian atas APIs, hingga maksimum 20, biasanya terlihat untuk identitas pengguna dan semua pengguna dalam akun. Ditandai Langka (kurang dari sebulan sekali), Jarang (beberapa kali sebulan), atau Sering (harian hingga mingguan), tergantung pada seberapa sering mereka digunakan dalam akun Anda. APIs
- Perilaku Tidak Biasa (Akun) — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk akun Anda.


#### Perilaku yang diprofilkan

GuardDuty terus belajar tentang aktivitas dalam akun Anda berdasarkan peristiwa yang disampaikan. Kegiatan ini dan frekuensi yang diamati dikenal sebagai perilaku yang diprofilkan.

Informasi yang dilacak di panel ini mencakup:

- ASN Org — ASN Org tempat API panggilan anomali dibuat.

- Nama Pengguna — Nama pengguna yang melakukan panggilan anomaliAPI.
- Agen Pengguna — Agen pengguna yang digunakan untuk melakukan panggilan anomaliAPI. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
- Jenis Pengguna — Jenis pengguna yang melakukan panggilan anomaliAPI. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.
- Bucket — Nama bucket S3 yang sedang diakses.
- Perilaku Tidak Biasa (Identitas Pengguna) - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk Identitas Pengguna yang terlibat dengan temuan tersebut. Ketika perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak melihat identitas pengguna ini membuat API panggilan ini dengan cara ini dalam periode pelatihan. Berikut adalah detail tambahan tentang Identitas Pengguna yang tersedia:
  - ASNOrg — ASN Org dari mana API panggilan anomali dibuat.
  - Agen Pengguna — Agen pengguna yang digunakan untuk melakukan panggilan anomaliAPI. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
  - Bucket — Nama bucket S3 yang sedang diakses.
- Perilaku Tidak Biasa (Bucket) — Bagian ini memberikan detail tambahan tentang perilaku yang diprofilkan untuk bucket S3 yang terkait dengan temuan tersebut. Ketika suatu perilaku tidak diidentifikasi sebagai historis, ini berarti model GuardDuty ML sebelumnya tidak pernah melihat API panggilan yang dibuat ke bucket ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak di bagian ini meliputi:
  - ASNOrg — ASN Org dari mana API panggilan anomali dibuat.
  - Nama Pengguna — Nama pengguna yang melakukan panggilan anomaliAPI.
  - Agen Pengguna — Agen pengguna yang digunakan untuk melakukan panggilan anomaliAPI. Agen pengguna adalah metode yang digunakan untuk membuat panggilan seperti `aws-cli` atau `Botocore`.
  - Jenis Pengguna — Jenis pengguna yang melakukan panggilan anomaliAPI. Kemungkinan nilainya adalah `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER`, atau `ROLE`.

 Note

Untuk konteks lebih lanjut tentang perilaku historis, pilih Perilaku historis di bagian Perilaku Tidak Biasa (Akun), ID Pengguna, atau Bucket untuk melihat detail tentang perilaku yang



diharapkan di akun Anda untuk masing-masing kategori berikut: Langka (kurang dari sebulan sekali), Jarang (beberapa kali sebulan), atau Sering (harian hingga mingguan), tergantung seberapa sering mereka digunakan dalam akun Anda.

- Perilaku Tidak Biasa (Database) - Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk instance database yang terkait dengan temuan. Ketika perilaku tidak diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak melihat upaya login yang dilakukan ke instance database ini dengan cara ini dalam periode pelatihan. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:
  - Nama pengguna — Nama pengguna yang digunakan untuk melakukan upaya login anomali.
  - ASNOrg — ASN Org tempat upaya login anomali dibuat.
  - Nama aplikasi — Nama aplikasi yang digunakan untuk melakukan upaya login anomali.
  - Nama database — Nama instance database yang terlibat dalam upaya login anomali.

Bagian perilaku historis memberikan lebih banyak konteks tentang nama Pengguna, ASNOrg, nama Aplikasi, dan nama Database yang diamati sebelumnya untuk database terkait. Setiap nilai unik memiliki hitungan terkait yang mewakili berapa kali nilai ini diamati dalam peristiwa login yang berhasil.

- Perilaku yang tidak biasa (klaster Akun Kubernetes, namespace Kubernetes, dan nama pengguna Kubernetes) — Bagian ini memberikan rincian tambahan tentang perilaku yang diprofilkan untuk klaster Kubernetes dan namespace yang terkait dengan temuan tersebut. Ketika perilaku tidak diidentifikasi sebagai historis, itu berarti bahwa model GuardDuty ML sebelumnya tidak mengamati akun, klaster, namespace, atau nama pengguna ini dengan cara ini. Informasi yang dilacak untuk bagian ini di panel temuan meliputi:
  - Username — Pengguna yang memanggil Kubernetes yang API terkait dengan temuan tersebut.
  - Nama Pengguna yang Ditiru - Pengguna yang ditiru oleh. `username`
  - Namespace — Namespace Kubernetes di dalam klaster Amazon tempat aksi terjadi. EKS
  - User Agent — Agen pengguna yang terkait dengan panggilan KubernetesAPI. Agen pengguna adalah metode yang digunakan untuk melakukan panggilan seperti `kubectl`.
  - API— Kubernetes API dipanggil oleh `username` dalam cluster Amazon. EKS
  - ASNInformasi — ASN Informasi, seperti Organisasi danISP, terkait dengan alamat IP pengguna yang melakukan panggilan ini.
  - Hari dalam seminggu — Hari dalam seminggu ketika API panggilan Kubernetes dilakukan.

- Izin — Kata kerja dan sumber daya Kubernetes yang diperiksa untuk mengindikasikan apakah Kubernetes `username` dapat menggunakan Kubernetes atau tidak. API
- Nama Akun Layanan — Akun layanan yang terkait dengan beban kerja Kubernetes yang memberikan identitas pada beban kerja.
- Registry — Registry container yang terkait dengan image container yang di-deploy dalam beban kerja Kubernetes.
- Image - Gambar kontainer, tanpa tag dan intisari terkait, yang digunakan dalam beban kerja Kubernetes.
- Image Prefix Config - Awalan gambar dengan konfigurasi keamanan kontainer dan beban kerja diaktifkan, `hostNetwork` seperti `privileged` atau, untuk wadah yang menggunakan gambar.
- Nama Subjek — Subjek, seperti `usergroup`, atau `serviceAccountName` yang terikat pada peran referensi dalam `RoleBinding` atau `ClusterRoleBinding`.
- Nama Peran — Nama peran yang terlibat dalam pembuatan atau modifikasi peran atau `roleBindingAPI`.

## Anomali berbasis volume S3

Bagian ini merinci informasi kontekstual untuk anomali berbasis volume S3. Temuan berbasis volume ([Exfiltration:S3/AnomalousBehavior](#)) memantau jumlah API panggilan S3 yang tidak biasa yang dilakukan ke bucket S3 oleh pengguna, menunjukkan potensi eksfiltrasi data. API Panggilan S3 berikut dipantau untuk deteksi anomali berbasis volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Metrik berikut akan membantu membangun dasar perilaku biasa saat IAM entitas mengakses bucket S3. Untuk mendeteksi eksfiltrasi data, temuan deteksi anomali berbasis volume mengevaluasi semua aktivitas terhadap garis dasar perilaku yang biasa. Pilih Perilaku historis di bagian Perilaku Tidak Biasa (Identitas Pengguna), Volume yang Diamati (Identitas Pengguna), dan Volume Teramati (Bucket) untuk melihat metrik berikut.

- Jumlah `s3-api-name` API panggilan yang dipanggil oleh IAM pengguna atau IAM peran (tergantung pada panggilan mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.

- Jumlah `s3-api-name` API panggilan yang dipanggil oleh IAM pengguna atau IAM peran (tergantung pada mana yang dikeluarkan) terkait dengan semua bucket S3 selama 24 jam terakhir.
- Jumlah `s3-api-name` API panggilan di semua IAM pengguna atau IAM peran (tergantung pada mana yang dikeluarkan) terkait dengan bucket S3 yang terpengaruh selama 24 jam terakhir.

## RDS anomali berbasis aktivitas login

Bagian ini merinci jumlah upaya login yang dilakukan oleh aktor yang tidak biasa dan dikelompokkan berdasarkan hasil upaya login. [Jenis temuan Perlindungan RDS](#) Mengidentifikasi perilaku anomali dengan memantau peristiwa login untuk pola yang tidak biasa `successfulLoginCount`, `failedLoginCount`, dan `incompleteConnectionCount`

- `successfulLoginCount`— Penghitung ini mewakili jumlah koneksi yang berhasil (kombinasi atribut login yang benar) yang dibuat ke instance database oleh aktor yang tidak biasa. Atribut login termasuk nama pengguna, kata sandi, dan nama database.
- `failedLoginCount`— Penghitung ini mewakili jumlah upaya login gagal (gagal) yang dilakukan untuk membuat koneksi ke instance database. Ini menunjukkan bahwa satu atau lebih atribut dari kombinasi login, seperti nama pengguna, kata sandi, atau nama database tidak benar.
- `incompleteConnectionCount`— Penghitung ini mewakili jumlah upaya koneksi yang tidak dapat diklasifikasikan sebagai berhasil atau gagal. Koneksi ini ditutup sebelum database memberikan respons. Misalnya, pemindaian port di mana port database terhubung tetapi tidak ada informasi yang dikirim ke database, atau koneksi dibatalkan sebelum login selesai dalam upaya yang berhasil atau gagal.

## GuardDuty menemukan agregasi

Semua temuan bersifat dinamis, artinya, jika GuardDuty mendeteksi aktivitas baru yang terkait dengan masalah keamanan yang sama, itu akan memperbarui temuan asli dengan informasi baru, alih-alih menghasilkan temuan baru. Perilaku ini memungkinkan Anda mengidentifikasi masalah yang sedang berlangsung, tanpa perlu melihat beberapa laporan serupa, dan mengurangi kebisingan keseluruhan dari masalah keamanan yang sudah Anda ketahui.

Misalnya, untuk `UnauthorizedAccess:EC2/SSHBruteForce` menemukan, beberapa upaya akses terhadap instans Anda akan digabungkan ke ID temuan yang sama, meningkatkan jumlah Hitungan dalam detail temuan. Ini karena temuan itu mewakili masalah keamanan tunggal dengan instance yang menunjukkan bahwa SSH port pada instance tidak diamankan dengan benar terhadap

jenis aktivitas ini. Namun, jika GuardDuty mendeteksi aktivitas SSH akses yang menargetkan instance baru di lingkungan Anda, itu akan membuat temuan baru dengan ID temuan unik untuk mengingatkan Anda tentang fakta bahwa ada masalah keamanan yang terkait dengan sumber daya baru.

Ketika sebuah temuan dikumpulkan, temuan tersebut diperbarui dengan informasi dari kejadian terbaru dari aktivitas tersebut. Ini berarti bahwa dalam contoh di atas, jika instans Anda adalah target upaya brute force dari aktor baru, detail temuan akan diperbarui untuk mencerminkan IP jarak jauh dari sumber terbaru dan informasi lama akan diganti. Informasi lengkap tentang upaya aktivitas individu akan tetap tersedia di Log VPC Aliran CloudTrail atau Anda.

Kriteria yang mengingatkan GuardDuty untuk menghasilkan temuan baru alih-alih menggabungkan yang sudah ada tergantung pada jenis temuan. Kriteria agregasi untuk setiap tipe temuan ditentukan oleh teknisi keamanan kami untuk memberikan gambaran terbaik tentang masalah keamanan yang berbeda dalam akun Anda.

## Tipe temuan

Untuk informasi tentang perubahan penting pada jenis GuardDuty temuan, termasuk jenis temuan yang baru ditambahkan atau yang sudah pensiun, lihat [Riwayat dokumen untuk Amazon GuardDuty](#).

Untuk informasi tentang menemukan jenis yang sekarang sudah pensiun, lihat [Tipe temuan yang sudah dihentikan](#).

## GuardDuty Jenis temuan EC2

Temuan berikut ini khusus untuk sumber daya Amazon EC2 dan selalu memiliki Tipe Sumber Daya Instance. Tingkat kepelikan dan detail temuan berbeda berdasarkan Peran Sumber Daya, yang menunjukkan apakah sumber daya EC2 adalah target aktivitas mencurigakan atau aktor yang melakukan aktivitas tersebut.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya tentang sumber data dan model, lihat [GuardDuty sumber data dasar](#).

### Note

Detail instans mungkin hilang untuk beberapa temuan EC2 jika instance telah dihentikan atau jika panggilan API yang mendasarinya adalah bagian dari panggilan API Lintas wilayah yang berasal dari instans EC2 di Wilayah yang berbeda.

Untuk semua temuan EC2, disarankan untuk memeriksa sumber daya yang bersangkutan untuk menentukan apakah sumber daya tersebut berperilaku seperti dengan yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan Aturan Penekanan atau daftar IP Tepercaya untuk mencegah notifikasi positif palsu untuk sumber daya tersebut. Jika aktivitas tidak terduga, praktik keamanan terbaik adalah menganggap instans telah disusupi dan mengambil tindakan seperti yang diuraikan dalam [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

### Topik

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)

- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [Behavior:EC2/NetworkPortUnusual](#)
- [Behavior:EC2/TrafficVolumeUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)
- [Recon:EC2/PortProbeEMRUnprotectedPort](#)
- [Recon:EC2/PortProbeUnprotectedPort](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)

- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/MetadataDNSRebind](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)

## Backdoor:EC2/C&CActivity.B

Instans EC2 menanyakan IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan terdistribusi (DDoS).

### Note

Jika IP yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `Service.additionalInfo.threatListName = Amazon`

- `Service.additionalInfo.ThreatName = Log4j Terkait`

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/C&CActivity.B!DNS

Instans EC2 menanyakan nama domain yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans yang tercantum dalam lingkungan AWS Anda menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Instans yang tercantum mungkin disusupi. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan terdistribusi (DDoS).

### Note

Jika nama domain yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `Service.additionalInfo.threatListName = Amazon`
- `Service.additionalInfo.ThreatName = Log4j Terkait`



**Note**

Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat permintaan DNS dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain `guarddutyactivityb.com` pengujian.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/DenialOfService.Dns

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas DNS keluar dalam volume yang besar. Ini mungkin menunjukkan bahwa instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol DNS.

**Note**

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/DenialOfService.Tcp

Instans EC2 berperilaku dengan cara yang menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas TCP keluar dalam volume yang besar. Ini mungkin menunjukkan bahwa instance dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol TCP.

### Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/DenialOfService.Udp


Instans EC2 berperilaku dengan cara yang menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol UDP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas UDP keluar dalam volume yang besar. Ini mungkin menunjukkan bahwa

instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP.

 Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).


## Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol UDP pada port TCP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menghasilkan lalu lintas UDP keluar dalam volume yang besar yang ditargetkan ke port yang biasanya digunakan untuk komunikasi TCP. Ini mungkin menunjukkan bahwa instance yang terdaftar dikompromikan dan digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol UDP pada port TCP.

 Note

Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/DenialOfService.UnusualProtocol

Instans EC2 berperilaku dengan cara yang mungkin menunjukkan bahwa sedang digunakan untuk melakukan serangan Denial of Service (DoS) menggunakan protokol yang tidak biasa.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar di lingkungan AWS Anda menghasilkan lalu lintas keluar dalam volume yang besar dari tipe protokol yang tidak biasa yang tidak biasanya digunakan oleh instans EC2, seperti Protokol Manajemen Grup Internet. Ini mungkin menunjukkan bahwa instance dikompromikan dan sedang digunakan untuk melakukan serangan denial-of-service (DoS) menggunakan protokol yang tidak biasa. Temuan ini mendeteksi serangan DoS hanya terhadap alamat IP yang dapat dirutekan secara publik, yang merupakan target utama dari serangan DoS.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/Spambot

Instans EC2 menunjukkan perilaku yang tidak biasa karena berkomunikasi dengan host jarak jauh pada port 25.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berkomunikasi dengan host jarak jauh pada port 25. Perilaku ini tidak biasa karena instans EC2 ini

tidak memiliki riwayat komunikasi sebelumnya pada port 25. Port 25 umumnya digunakan oleh server e-mail untuk komunikasi SMTP. Temuan ini menunjukkan bahwa instans EC2 Anda mungkin disusupi dan digunakan untuk mengirimkan spam.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Behavior:EC2/NetworkPortUnusual

Instans EC2 berkomunikasi dengan host jarak jauh pada port server yang tidak biasa.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat komunikasi pada port jarak jauh ini.

### Note

Jika instans EC2 dikomunikasikan pada port 389 atau port 1389, maka tingkat keparahan temuan terkait akan dimodifikasi menjadi Tinggi, dan bidang temuan akan mencakup nilai berikut:

- `Service.additionAlInfo.Context` = Kemungkinan panggilan balik log4j

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Behavior:EC2/TrafficVolumeUnusual

Instans EC2 menghasilkan lalu lintas jaringan dalam jumlah besar yang tidak biasa ke host jarak jauh.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat pengiriman lalu lintas sebanyak ini ke host jarak jauh ini sebelumnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## CryptoCurrency:EC2/BitcoinTool.B

Instans EC2 menanyakan alamat IP yang terkait dengan aktivitas mata uang kripto.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda menanyakan Alamat IP yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini bisa jadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## CryptoCurrency:EC2/BitcoinTool.B!DNS

Instans EC2 menanyakan nama domain yang terkait dengan aktivitas mata uang kripto.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini bisa jadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## DefenseEvasion:EC2/UnusualDNSResolver

Instans Amazon EC2 berkomunikasi dengan resolver DNS publik yang tidak biasa.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang terdaftar di lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari perilaku dasar. Instans EC2 ini tidak memiliki riwayat komunikasi terbaru dengan resolver DNS publik ini. Bidang yang tidak biasa di panel detail pencarian di GuardDuty konsol dapat memberikan informasi tentang penyelesai DNS yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## DefenseEvasion:EC2/UnusualDoHActivity

Instans Amazon EC2 melakukan DNS yang tidak biasa melalui komunikasi HTTPS (DoH).

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang terdaftar di lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat DNS terbaru melalui komunikasi HTTPS (DoH) dengan server DoH publik ini. Bidang yang tidak biasa dalam rincian temuan dapat memberikan informasi tentang server DoH yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## DefenseEvasion:EC2/UnusualDoTActivity

Instans Amazon EC2 melakukan komunikasi DNS yang tidak biasa melalui TLS (DoT).

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC



Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda berperilaku dengan cara yang menyimpang dari garis dasar yang ditetapkan. Instans EC2 ini tidak memiliki riwayat terbaru DNS melalui komunikasi TLS (DoT) dengan server DoT publik ini. Bidang yang tidak biasa di panel rincian temuan dapat memberikan informasi tentang server DoT yang ditanyakan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Impact:EC2/AbusedDomainRequest.Reputation

Instans EC2 menanyakan nama domain bereputasi rendah yang terkait dengan domain yang diketahui disalahgunakan.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans Amazon EC2 dalam lingkungan AWS Anda menanyakan nama domain bereputasi rendah yang terkait dengan domain atau alamat IP yang diketahui disalahgunakan. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLD) dan nama domain tingkat kedua (2LDs) yang menyediakan pendaftaran subdomain gratis serta penyedia DNS dinamis. Aktor ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain bereputasi rendah dalam kategori ini mungkin juga merupakan domain kedaluwarsa yang mencari alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. Instans Amazon EC2 yang terdaftar dapat disusupi karena pelaku ancaman biasanya menggunakan layanan registrar ini atau layanan untuk distribusi C&C dan malware.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Impact:EC2/BitcoinDomainRequest.Reputation

Instans EC2 menanyakan nama domain dengan reputasi rendah yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans Amazon EC2 yang terdaftar dalam lingkungan AWS Anda menanyakan nama domain bereputasi rendah yang terkait dengan Bitcoin atau aktivitas mata uang kripto lainnya. Bitcoin adalah cryptocurrency di seluruh dunia dan sistem pembayaran digital yang dapat ditukar dengan mata uang, produk, dan layanan lainnya. Bitcoin adalah hadiah untuk penambangan bitcoin dan sangat dicari oleh para pelaku ancaman.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika Anda menggunakan instans EC2 ini untuk menambang atau mengelola mata uang kripto, atau jika instans ini terlibat dalam aktivitas blockchain, temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Impact : EC2/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus menggunakan ID Instans dari instans yang terlibat dalam aktivitas blockchain. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Impact:EC2/MaliciousDomainRequest.Reputation

Instans EC2 menanyakan domain bereputasi rendah yang terkait dengan domain berbahaya yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans Amazon EC2 yang terdaftar dalam lingkungan AWS Anda menanyakan nama domain bereputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang dikenal. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang dikenal. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh aktor ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritme pembuatan domain yang dikenal.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Impact:EC2/PortSweep

Instans EC2 memeriksa port pada sejumlah besar alamat IP.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda memeriksa port pada sejumlah besar alamat IP yang dapat dirutekan secara publik. Tipe aktivitas ini biasanya digunakan untuk menemukan host yang rentan untuk dieksploitasi. Di panel detail pencarian di GuardDuty konsol Anda, hanya alamat IP jarak jauh terbaru yang ditampilkan

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Impact:EC2/SuspiciousDomainRequest.Reputation

Instans EC2 menanyakan nama domain bereputasi rendah yang mencurigakan karena usia, atau popularitasnya yang rendah.

Tingkat keparahan default: Rendah

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans Amazon EC2 yang terdaftar di lingkungan AWS Anda menanyakan nama domain dengan reputasi rendah yang diduga jahat. Perhatikan karakteristik domain ini yang konsisten dengan domain berbahaya yang diamati sebelumnya, namun, model reputasi kami tidak dapat secara definitif menghubungkannya dengan ancaman yang diketahui. Domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.


Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Impact:EC2/WinRMBruteForce

Instans EC2 melakukan serangan brute force Windows Remote Management keluar.

Tingkat keparahan default: Rendah\*

 Note

Tingkat keparahan temuan ini rendah jika instans EC2 Anda adalah target dari serangan brute force. Tingkat keparahan temuan ini tinggi jika instans EC2 Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda melakukan serangan brute force Windows Remote Management (WinRM) yang bertujuan untuk mendapatkan akses ke layanan Windows Remote Management pada sistem berbasis Windows.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

### Recon:EC2/PortProbeEMRUnprotectedPort

Instans EC2 memiliki port EMR yang tidak dilindungi yang sedang diperiksa oleh host berbahaya yang dikenal.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa port sensitif terkait EMR pada instans EC2 yang terdaftar yang merupakan bagian dari cluster di lingkungan AWS Anda tidak diblokir oleh grup keamanan, daftar kontrol akses (ACL), atau firewall on-host seperti Linux IPTables. Temuan ini juga menginformasikan bahwa pemindai yang dikenal di Internet secara aktif menyelidiki port ini. Port yang dapat memicu temuan ini, seperti port 8088 (YARN Web UI port), berpotensi digunakan untuk eksekusi kode jarak jauh.

## Rekomendasi remediasi:

Anda harus memblokir akses terbuka ke port pada klaster dari internet dan membatasi akses hanya ke alamat IP tertentu yang memerlukan akses ke port ini. Untuk informasi selengkapnya, lihat [Grup Keamanan untuk Klaster EMR](#).

### Recon:EC2/PortProbeUnprotectedPort

Instans EC2 memiliki port yang tidak dilindungi yang sedang diperiksa oleh host berbahaya yang dikenal.

Tingkat keparahan default: Rendah\*

#### Note

Tingkat keparahan default temuan ini Rendah. Namun, jika port yang sedang diselidiki, digunakan oleh Elasticsearch (9200 atau 9300), tingkat keparahan temuannya Tinggi.

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa port pada instans EC2 yang terdaftar dalam lingkungan AWS Anda tidak diblokir oleh grup keamanan, daftar kontrol akses (ACL), atau firewall on-host seperti Linux IPTables, dan pemindai yang dikenal di internet memeriksanya secara aktif.

Jika port tidak terlindungi yang teridentifikasi adalah 22 atau 3389 dan Anda menggunakan port ini agar terhubung ke instans Anda, Anda masih dapat membatasi eksposur dengan mengizinkan akses ke port ini hanya untuk alamat IP dari ruang alamat IP jaringan perusahaan Anda. Untuk membatasi akses ke port 22 di Linux, lihat [Otorisasi Lalu Lintas Masuk untuk Instans Linux Anda](#). Untuk membatasi akses ke port 3389 pada Windows, lihat [Otorisasi Lalu Lintas Masuk untuk Instans Windows Anda](#).

GuardDuty tidak menghasilkan temuan ini untuk port 443 dan 80.

Rekomendasi remediasi:

Mungkin terdapat kasus ketika instans sengaja diekspos, misalnya ketika instans menghosting server web. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk mengatur aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai Recon:EC2/PortProbeUnprotectedPort. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Recon:EC2/Portscan

Instans EC2 melakukan pemindaian port keluar ke host jarak jauh.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda kemungkinan terlibat dalam serangan pemindaian port karena mencoba untuk menghubungkan ke beberapa port dalam waktu yang singkat. Tujuan serangan pemindaian port adalah untuk menemukan port terbuka guna menemukan layanan mana yang dijalankan mesin dan untuk mengidentifikasi sistem operasinya.

Rekomendasi remediasi:

Temuan ini bisa menjadi positif palsu ketika aplikasi penilaian kerentanan diterapkan pada instans EC2 di lingkungan Anda karena aplikasi ini melakukan pemindaian port untuk mengingatkan Anda tentang port terbuka yang salah konfigurasi. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk menetapkan aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai Recon:EC2/Portscan. Kriteria filter kedua harus sesuai dengan instans yang menghosting alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak terduga, instans Anda kemungkinan disusupi, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/BlackholeTraffic

Instans EC2 mencoba untuk berkomunikasi dengan alamat IP dari host jarak jauh yang dikenal sebagai black hole.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host yang ditugaskan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/BlackholeTraffic!DNS

Instans EC2 menanyakan nama domain yang sedang diarahkan ke alamat IP black hole.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini memberi tahu Anda bahwa instans EC2 yang terdaftar di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DGADomainRequest.B

Instans EC2 menanyakan domain yang dihasilkan dengan algoritme. Domain tersebut umumnya digunakan oleh malware dan dapat menjadi indikasi instans EC2 yang disusupi.

Tingkat keparahan default: Tinggi


- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). Instans EC2 Anda mungkin disusupi.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server



perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

 Note

Temuan ini didasarkan pada analisis nama domain menggunakan heuristik lanjutan dan dapat mengidentifikasi domain DGA baru yang tidak terdapat dalam umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DGADomainRequest.C!DNS

Instans EC2 menanyakan domain yang dihasilkan dengan algoritme. Domain tersebut umumnya digunakan oleh malware dan dapat menjadi indikasi instans EC2 yang disusupi.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mencoba menanyakan domain algoritme pembuatan domain (DGA). Instans EC2 Anda mungkin disusupi.

DGAs digunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan

botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

**Note**

Temuan ini didasarkan pada domain DGA yang diketahui dari GuardDuty umpan intelijen ancaman.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DNSDataExfiltration

Instans EC2 mengekstraksi data melalui kueri DNS.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda menjalankan malware yang menggunakan kueri DNS untuk transfer data keluar. Tipe transfer data ini merupakan indikasi dari instans yang disusupi dan dapat mengakibatkan eksfiltrasi data. Lalu lintas DNS biasanya tidak diblokir oleh firewall. Misalnya, malware dalam instans EC2 yang disusupi dapat mengkodekan data, (seperti nomor kartu kredit Anda), menjadi kueri DNS dan mengirimkannya ke server DNS jarak jauh yang dikendalikan oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DriveBySourceTraffic!DNS

Instans EC2 menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan unduhan Drive-By yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 yang terdaftar dalam lingkungan AWS Anda mungkin disusupi karena menanyakan nama domain dari host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Ini merupakan unduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memicu penginstalan virus, spyware, atau malware secara otomatis.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DropPoint

Instans EC2 mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/DropPoint!DNS

Instans EC2 menanyakan nama domain dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda menanyakan nama domain dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Trojan:EC2/PhishingDomainRequest!DNS

Instans EC2 menanyakan domain yang terlibat dalam serangan phishing. Instans EC2 Anda mungkin disusupi.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa terdapat instans EC2 dalam lingkungan AWS Anda yang mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang menyamar sebagai institusi yang sah untuk membujuk individu agar memberikan data sensitif, seperti informasi pengenalan pribadi, detail kartu kredit dan perbankan, serta kata sandi. Instans EC2 Anda mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba membuat situs web phishing. Instans EC2 Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Instans EC2 membuat koneksi ke alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Sedang

- Sumber data: log alur VPC

Temuan ini meninformasikan bahwa instans EC2 dalam lingkungan AWS Anda berkomunikasi dengan alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Dalam GuardDuty, daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman yang diunggah. Daftar ancaman yang digunakan untuk menghasilkan temuan ini akan tercantum dalam detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## UnauthorizedAccess:EC2/MetadataDNSRebind

Instans EC2 melakukan pencarian DNS untuk layanan metadata instans.

Tingkat keparahan default: Tinggi

- Sumber data: log DNS

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda menanyakan domain yang mencari alamat IP (169.254.169.254) metadata EC2. Kueri DNS semacam ini dapat menunjukkan bahwa instans adalah target dari teknik rebinding DNS. Teknik ini dapat digunakan untuk mendapatkan metadata dari instans EC2, termasuk kredensial IAM yang terkait dengan instans.

Rebinding DNS melibatkan pemalsuan aplikasi yang berjalan pada instans EC2 untuk memuat data yang dikembalikan dari URL, di mana nama domain di URL ditujukan ke alamat IP (169.254.169.254) metadata EC2. Hal ini menyebabkan aplikasi mengakses metadata EC2 dan mungkin membuatnya tersedia untuk penyerang.

Dimungkinkan untuk mengakses metadata EC2 menggunakan rebinding DNS hanya jika instans EC2 menjalankan aplikasi rentan yang memungkinkan injeksi URL, atau jika seseorang mengakses URL di browser web yang berjalan pada instans EC2.

## Rekomendasi remediasi:

Menanggapi temuan ini, Anda harus mengevaluasi apakah ada aplikasi rentan yang berjalan pada instans EC2, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, Anda harus memperbaiki kerentanannya. Jika seseorang menjelajahi domain yang diidentifikasi, Anda harus memblokir domain atau mencegah pengguna mengaksesnya. Jika Anda menentukan temuan ini terkait dengan kedua kasus di atas, [cabut sesi yang terkait dengan instans EC2](#).

Beberapa pelanggan AWS sengaja memetakan alamat IP metadata ke nama domain di server DNS otoritatif mereka. Jika hal ini dilakukan di lingkungan Anda, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Kriteria filter kedua harus menggunakan Domain permintaan DNS dan nilainya harus sesuai dengan domain yang telah Anda petakan ke alamat IP (169.254.169.254) metadata. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

## UnauthorizedAccess:EC2/RDPBruteForce

Instans EC2 telah terlibat dalam serangan brute force RDP.

Tingkat keparahan default: Rendah\*

### Note

Tingkat kepelikan temuan ini rendah jika instans EC2 Anda adalah target dari serangan brute force. Tingkat kepelikan temuan ini tinggi jika instans EC2 Anda adalah aktor yang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda terlibat dalam serangan brute force yang bertujuan untuk mendapatkan kata sandi ke layanan RDP pada sistem berbasis Windows. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

## Rekomendasi remediasi:

Jika Peran Sumber Daya instans Anda adalah ACTOR, hal ini mengindikasikan bahwa instans Anda telah digunakan untuk melakukan serangan brute force RDP. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai Target, Anda disarankan untuk menganggap bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

Jika Peran Sumber Daya instans Anda adalah TARGET, temuan ini dapat diperbaiki dengan mengamankan port RDP Anda hanya ke IP yang tepercaya melalui Grup Keamanan, ACL, atau firewall. Untuk informasi selengkapnya, lihat [Tip untuk mengamankan instans EC2 Anda \(Linux\)](#).

## UnauthorizedAccess:EC2/SSHBruteForce

Instans EC2 telah terlibat dalam serangan brute force SSH.

Tingkat keparahan default: Rendah\*

### Note

Tingkat kepelikan temuan ini rendah jika serangan brute force ditujukan pada salah satu instans EC2 Anda. Tingkat kepelikan temuan ini tinggi jika instans EC2 Anda sedang digunakan untuk melakukan serangan brute force.

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda terlibat dalam serangan brute force yang bertujuan untuk mendapatkan kata sandi ke layanan SSH pada sistem berbasis Linux. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

### Note

Temuan ini dihasilkan hanya melalui pemantauan lalu lintas pada port 22. Jika layanan SSH Anda dikonfigurasi untuk menggunakan port lain, temuan ini tidak dihasilkan.

Rekomendasi remediasi:

Jika target dari upaya brute force adalah host bastion, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan AWS Anda. Jika demikian, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruTeForce`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Untuk informasi selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

Jika aktivitas ini tidak diharapkan untuk lingkungan Anda dan jika Peran Sumber Daya instans Anda adalah TARGET, temuan ini dapat diperbaiki dengan mengamankan port SSH Anda hanya ke IP yang tepercaya melalui Grup Keamanan, ACL, atau firewall. Untuk informasi selengkapnya, lihat [Tip untuk mengamankan instans EC2 Anda \(Linux\)](#).

Jika Peran Sumber Daya instans Anda adalah ACTOR, hal ini mengindikasikan bahwa instans telah digunakan untuk melakukan serangan brute force SSH. Kecuali instans ini memiliki alasan yang sah untuk menghubungi alamat IP yang terdaftar sebagai Target, Anda disarankan untuk menganggap bahwa instans Anda telah disusupi dan mengambil tindakan yang tercantum di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## UnauthorizedAccess:EC2/TorClient

Instans EC2 Anda membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda membuat koneksi ke Tor Guard atau node Otoritas. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat mengindikasikan bahwa instans EC2 ini telah disusupi dan bertindak sebagai klien pada jaringan Tor. Temuan ini mungkin mengindikasikan akses yang tidak sah ke sumber daya AWS Anda yang bertujuan untuk menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).



## UnauthorizedAccess:EC2/TorRelay

Instans EC2 Anda membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Sumber data: log alur VPC

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda membuat koneksi ke jaringan Tor dengan cara yang mengindikasikan bahwa instans bertindak sebagai relay Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relay Tor ke relay lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Lihat informasi yang lebih lengkap di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## GuardDuty IAM menemukan jenis

Temuan berikut khusus untuk IAM entitas dan kunci akses dan selalu memiliki Jenis Sumber DayaAccessKey. Tingkat kepelikan dan detail temuan berbeda berdasarkan tipe temuan.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi selengkapnya, lihat [GuardDuty sumber data dasar](#).

Untuk semua temuan IAM terkait, kami menyarankan Anda memeriksa entitas yang bersangkutan dan memastikan bahwa izin mereka mengikuti praktik terbaik dengan hak istimewa yang paling sedikit. Jika aktivitas tidak terduga, kredensial mungkin disusupi. Untuk informasi tentang remediasi temuan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

Topik

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)

- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [PenTest:IAMUser/KaliLinux](#)
- [PenTest:IAMUser/ParrotLinux](#)
- [PenTest:IAMUser/PentoolLinux](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [Policy:IAMUser/RootCredentialUsage](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Recon:IAMUser/MaliciousIPCaller](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

## CredentialAccess:IAMUser/AnomalousBehavior

API Digunakan untuk mendapatkan akses ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan tahap akses kredensial serangan ketika musuh mencoba mengumpulkan

kata sandi, nama pengguna, dan kunci akses untuk lingkungan Anda. APIs dalam kategori ini adalah `GetPasswordData`, `GetSecretValue`, `BatchGetSecretValue`, dan `GenerateDbAuthToken`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## DefenseEvasion:IAMUser/AnomalousBehavior

API Digunakan untuk menghindari tindakan defensif digunakan dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menutupi jejak mereka dan menghindari deteksi. APIs dalam kategori ini biasanya menghapus, menonaktifkan, atau menghentikan operasi, seperti, `DeleteFlowLogs`, `DisableAlarmActions`, atau `StopLogging`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Discovery: IAMUser/AnomalousBehavior

API yang umum digunakan untuk menemukan sumber daya dipanggil dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. API dalam kategori ini biasanya mendapatkan, mendeskripsikan, atau daftar operasi, seperti, `DescribeInstances`, `GetRolePolicy`, atau `ListAccessKeys`.

API permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Exfiltration: IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan taktik eksfiltrasi di mana musuh mencoba mengumpulkan data dari jaringan Anda menggunakan pengemasan dan enkripsi untuk menghindari deteksi. APIs untuk jenis temuan ini hanya operasi manajemen (bidang kontrol) dan biasanya terkait dengan S3, snapshot, dan database, seperti `PutBucketReplication`, `CreateSnapshot`, `RestoreDBInstanceFromDBSnapshot`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Impact: IAMUser/AnomalousBehavior

API yang biasa digunakan untuk mengutak-atik data atau proses dalam suatu AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba mengganggu operasi dan memanipulasi, menyela, atau menghancurkan data di akun

Anda. APIs untuk jenis temuan ini biasanya menghapus, memperbarui, atau menempatkan operasi, seperti, `DeleteSecurityGroup`, `UpdateUser`, atau `PutBucketPolicy`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## InitialAccess:IAMUser/AnomalousBehavior

API yang umum digunakan untuk mendapatkan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan tahap akses awal serangan ketika musuh mencoba untuk membangun akses ke lingkungan Anda. API dalam kategori ini biasanya mendapatkan token, atau operasi sesi, seperti, `GetFederationToken`, `StartSession`, atau `GetAuthorizationToken`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## PenTest:IAMUser/KaliLinux

An API dipanggil dari mesin Kali Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux melakukan API panggilan menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Kali Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## PenTest:IAMUser/ParrotLinux

An API dipanggil dari mesin Parrot Security Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux melakukan API panggilan menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Parrot Security Linux adalah alat pengujian penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## PenTest:IAMUser/PentooLinux

An API dipanggil dari mesin Pentoo Linux.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan API panggilan menggunakan kredensial milik AWS akun yang terdaftar di lingkungan Anda. Pentoo Linux adalah alat pengujian penetrasi populer yang digunakan oleh para profesional keamanan untuk mengidentifikasi kelemahan dalam EC2 kasus yang memerlukan penambalan. Penyerang juga menggunakan alat ini untuk menemukan kelemahan EC2 konfigurasi dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Persistence:IAMUser/AnomalousBehavior

API yang umum digunakan untuk mempertahankan akses tidak sah ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh



[identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan taktik ketekunan di mana musuh telah mendapatkan akses ke lingkungan Anda dan berusaha mempertahankan akses itu. API dalam kategori ini biasanya membuat, mengimpor, atau memodifikasi operasi, seperti `CreateAccessKey`, `ImportKeyPair`, atau `ModifyInstanceAttribute`.

API Permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Policy: IAMUser/RootCredentialUsage

An API dipanggil menggunakan kredensial masuk pengguna root.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa CloudTrail data

Temuan ini memberi tahu Anda bahwa kredensial masuk pengguna root dari yang tercantum Akun AWS di lingkungan Anda digunakan untuk membuat permintaan ke layanan. AWS Disarankan agar pengguna tidak pernah menggunakan kredensial masuk pengguna root untuk mengakses layanan. AWS Sebagai gantinya, AWS layanan harus diakses menggunakan kredensial sementara hak istimewa terkecil dari AWS Security Token Service (). STS Untuk situasi di AWS STS mana tidak didukung, kredensial IAM pengguna direkomendasikan. Untuk informasi selengkapnya, lihat [Praktik IAM Terbaik](#).

### Note

Jika deteksi ancaman S3 diaktifkan untuk akun, temuan ini dapat dihasilkan sebagai tanggapan atas upaya untuk menjalankan operasi bidang data S3 pada sumber daya S3 menggunakan kredensial masuk pengguna root dari. Akun AWS API Panggilan yang digunakan

akan tercantum dalam detail temuan. Jika deteksi ancaman S3 tidak diaktifkan, temuan ini hanya dapat dipicu oleh log APIs Peristiwa. Untuk informasi selengkapnya tentang deteksi ancaman S3, lihat perlindungan [S3](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## PrivilegeEscalation:IAMUser/AnomalousBehavior

API yang umum digunakan untuk mendapatkan izin tingkat tinggi ke AWS lingkungan dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API permintaan anomali diamati di akun Anda. Temuan ini dapat mencakup satu API atau serangkaian API permintaan terkait yang dibuat di dekat oleh [identitas pengguna](#) tunggal. Yang API diamati umumnya dikaitkan dengan taktik eskalasi hak istimewa di mana musuh berusaha mendapatkan izin tingkat yang lebih tinggi ke suatu lingkungan. API dalam kategori ini biasanya melibatkan operasi yang mengubah IAM kebijakan, peran, dan pengguna, seperti `AssociateIamInstanceProfile`, `AddUserToGroup`, atau `PutUserPolicy`.

API permintaan ini diidentifikasi sebagai anomali dengan GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor API permintaan, seperti, pengguna yang membuat permintaan, lokasi permintaan dibuat, dan spesifik API yang diminta. Detail tentang faktor API permintaan yang tidak biasa untuk identitas pengguna yang memanggil permintaan dapat ditemukan dalam [rincian temuan](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/MaliciousIPCaller

An API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi yang dapat mencantumkan atau menjelaskan AWS sumber daya di akun di lingkungan Anda dipanggil dari alamat IP yang disertakan dalam daftar ancaman. Penyerang dapat menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/MaliciousIPCaller.Custom

An API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi yang dapat mencantumkan atau menjelaskan AWS sumber daya di akun di lingkungan Anda dipanggil dari alamat IP yang disertakan dalam daftar ancaman khusus. Daftar ancaman yang digunakan akan tercantum dalam detail temuan. Seorang penyerang mungkin menggunakan kredensial curian untuk melakukan jenis pengintaian AWS sumber daya Anda untuk menemukan kredensial yang lebih berharga atau menentukan kemampuan kredensial yang sudah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/TorIPCaller

An API dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi yang dapat mencantumkan atau mendeskripsikan AWS sumber daya di akun dalam lingkungan Anda dipanggil dari alamat IP node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Penyerang akan menggunakan Tor untuk menutupi identitas mereka yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail logging dinonaktifkan.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa CloudTrail jejak di AWS lingkungan Anda dinonaktifkan. Ini bisa menjadi upaya penyerang untuk menonaktifkan pencatatan log untuk menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka sekaligus mendapatkan akses ke sumber daya AWS Anda untuk tujuan berbahaya. Temuan ini dapat dipicu oleh penghapusan atau pembaruan jejak yang berhasil. Temuan ini juga dapat dipicu oleh penghapusan bucket S3 yang berhasil menyimpan log dari jejak yang terkait dengannya. GuardDuty

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Stealth:IAMUser/PasswordPolicyChange

Kebijakan kata sandi akun dilemahkan.

Tingkat keparahan default: Rendah\*

### Note

Tingkat keparahan temuan ini bisa Rendah, Sedang, atau Tinggi tergantung pada tingkat keparahan perubahan yang dibuat pada kebijakan kata sandi.

- Sumber data: acara CloudTrail manajemen

Kebijakan kata sandi AWS akun dilemahkan pada akun yang terdaftar di AWS lingkungan Anda. Misalnya, kata sandi dihapus atau diperbarui untuk memerlukan lebih sedikit karakter, tidak memerlukan simbol dan angka, atau diperlukan untuk memperpanjang masa kedaluwarsa kata sandi. Temuan ini juga dapat dipicu oleh upaya untuk memperbarui atau menghapus kebijakan kata sandi AWS akun Anda. Kebijakan kata sandi AWS akun menentukan aturan yang mengatur jenis kata sandi apa yang dapat ditetapkan untuk pengguna Anda IAM. Kebijakan kata sandi yang lebih lemah memungkinkan pembuatan kata sandi yang mudah diingat dan berpotensi lebih mudah ditebak, sehingga menimbulkan risiko keamanan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Beberapa login konsol yang berhasil di seluruh dunia diamati.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa beberapa login konsol yang berhasil untuk IAM pengguna yang sama diamati sekitar waktu yang sama di berbagai lokasi geografis. Pola lokasi akses anomali dan berisiko seperti itu menunjukkan potensi akses tidak sah ke sumber daya Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Kredensial yang dibuat secara eksklusif untuk sebuah EC2 instance melalui peran peluncuran Instance digunakan dari akun lain di dalamnya. AWS

Tingkat keparahan default: Tinggi\*

### Note

Tingkat keparahan default temuan ini adalah Tinggi. Namun, jika dipanggil API oleh akun yang berafiliasi dengan AWS lingkungan Anda, tingkat keparahannya adalah Medium.

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa data S3

Temuan ini memberi tahu Anda kapan kredensi EC2 instans Anda digunakan untuk memanggil APIs dari alamat IP yang dimiliki oleh AWS akun yang berbeda dari yang dijalankan EC2 instans terkait.

AWS tidak merekomendasikan untuk mendistribusikan ulang kredensi sementara di luar entitas yang membuatnya (misalnya, AWS aplikasi, EC2 atau Lambda). Namun, pengguna yang berwenang dapat mengeksport kredensial dari EC2 instans mereka untuk melakukan panggilan yang sah. API Jika `remoteAccountDetails.Affiliated` bidangnya API dipanggil `True` dari akun yang terkait dengan AWS lingkungan Anda. Untuk mengesampingkan potensi serangan dan memverifikasi legitimasi aktivitas, hubungi IAM pengguna yang diberi kredensi ini.

### Note

Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty

akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

#### Rekomendasi remediasi:

Menanggapi temuan ini, Anda dapat menggunakan alur kerja berikut untuk menentukan tindakan:

1. Identifikasi akun jarak jauh yang terlibat dari `service.action.awsApiCallAction.remoteAccountDetails.accountId` lapangan.
2. Selanjutnya tentukan apakah akun itu berafiliasi dengan GuardDuty lingkungan Anda dari `service.action.awsApiCallAction.remoteAccountDetails.affiliated` lapangan.
3. Jika akun tersebut berafiliasi, hubungi pemilik akun jarak jauh, dan pemilik kredensi EC2 instans untuk menyelidiki.
4. Jika akun tidak berafiliasi, evaluasi pertama adalah bahwa akun dikaitkan dengan organisasi Anda tetapi bukan bagian dari pengaturan GuardDuty multi-akun Anda, atau jika GuardDuty belum diaktifkan di akun. Jika tidak, hubungi pemilik EC2 kredensial untuk menentukan apakah ada kasus penggunaan untuk akun jarak jauh untuk menggunakan kredensi ini.
5. Jika pemilik kredensial tidak mengenali akun jarak jauh, kredensialnya mungkin telah dikompromikan oleh aktor ancaman yang beroperasi di dalamnya. AWS Anda harus mengambil langkah-langkah yang direkomendasikan [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#) untuk mengamankan lingkungan Anda.

Selain itu, Anda dapat [mengirimkan laporan penyalahgunaan](#) ke tim AWS Trust and Safety untuk memulai penyelidikan ke akun jarak jauh. Saat mengirimkan laporan Anda ke AWS Trust and Safety, sertakan JSON detail lengkap temuan tersebut.

## UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Kredensial yang dibuat secara eksklusif untuk sebuah EC2 instance melalui peran peluncuran Instans sedang digunakan dari alamat IP eksternal.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail manajemen atau peristiwa data S3

Temuan ini memberi tahu Anda bahwa host di luar AWS telah mencoba menjalankan AWS API operasi menggunakan AWS kredensial sementara yang dibuat pada EC2 instance di lingkungan Anda. AWS EC2Instance yang terdaftar mungkin dikompromikan, dan kredensial sementara dari instance ini mungkin telah diekstraksi ke host jarak jauh di luar. AWS tidak merekomendasikan untuk mendistribusikan ulang kredensial sementara di luar entitas yang membuatnya (misalnya, AWS aplikasi, EC2 atau Lambda). Namun, pengguna yang berwenang dapat mengeksport kredensial dari EC2 instans mereka untuk melakukan panggilan yang sah. API Untuk mengesampingkan serangan potensial dan memverifikasi legitimasi aktivitas, validasi jika penggunaan kredensial instance dari IP jarak jauh dalam temuan diharapkan.

#### Note

Jika GuardDuty mengamati aktivitas lanjutan dari akun jarak jauh, model pembelajaran mesin (ML) akan mengidentifikasi ini sebagai perilaku yang diharapkan. Oleh karena itu, GuardDuty akan berhenti menghasilkan temuan ini untuk aktivitas dari akun jarak jauh itu. GuardDuty akan terus menghasilkan temuan untuk perilaku baru dari akun jarak jauh lainnya dan akan mengevaluasi kembali akun jarak jauh yang dipelajari saat perilaku berubah seiring waktu.

#### Rekomendasi remediasi:

Temuan ini dihasilkan ketika jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway lokal dan bukan dari VPC Internet Gateway (). IGW Konfigurasi umum, seperti menggunakan, atau VPC VPN koneksi [AWS Outposts](#), dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, kami sarankan Anda menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah IPv4Alamat API pemanggil dengan alamat IP atau CIDR rentang gateway internet lokal Anda. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

#### Note

Jika GuardDuty mengamati aktivitas lanjutan dari sumber eksternal, model pembelajaran mesinnya akan mengidentifikasi ini sebagai perilaku yang diharapkan dan berhenti menghasilkan temuan ini untuk aktivitas dari sumber itu. GuardDuty akan terus menghasilkan



temuan untuk perilaku baru dari sumber lain, dan akan mengevaluasi kembali sumber yang dipelajari saat perilaku berubah dari waktu ke waktu.

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/MaliciousIPCaller

An API dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi (misalnya, upaya untuk meluncurkan EC2 instance, membuat IAM pengguna baru, atau memodifikasi AWS hak istimewa Anda) dipanggil dari alamat IP berbahaya yang diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

An API dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi (misalnya, upaya untuk meluncurkan EC2 instance, membuat IAM pengguna baru, atau memodifikasi AWS hak istimewa) dipanggil dari alamat IP yang disertakan pada daftar ancaman yang Anda unggah. Di , daftar ancaman terdiri dari alamat

IP berbahaya yang diketahui. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya dalam lingkungan Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/TorIPCaller

An API dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa API operasi (misalnya, upaya untuk meluncurkan EC2 instance, membuat IAM pengguna baru, atau memodifikasi AWS hak istimewa Anda) dipanggil dari alamat IP node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Temuan ini mungkin mengindikasikan akses yang tidak sah ke sumber daya AWS Anda yang bertujuan untuk menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensi Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## GuardDuty Jenis temuan S3

Temuan berikut khusus untuk sumber daya Amazon S3 dan akan memiliki Jenis Sumber Daya **S3Bucket** jika sumber data adalah peristiwa CloudTrail data untuk S3, atau **AccessKey** jika sumber data adalah CloudTrail peristiwa manajemen. Tingkat kepelikan dan detail temuan akan berbeda berdasarkan tipe temuan dan izin yang terkait dengan bucket.

Temuan yang tercantum di sini termasuk sumber data dan model yang digunakan untuk menghasilkan tipe temuan. Untuk informasi lebih lanjut sumber dan model data, lihat [GuardDuty sumber data dasar](#).

**⚠ Important**

Temuan dengan sumber data peristiwa CloudTrail data untuk S3 hanya dihasilkan jika Anda mengaktifkan perlindungan S3. GuardDuty Perlindungan S3 diaktifkan secara default di semua akun yang dibuat setelah 31 Juli 2020. Untuk informasi tentang cara mengaktifkan atau menonaktifkan perlindungan S3, lihat [GuardDuty Perlindungan S3](#)

Untuk semua S3Bucket jenis temuan, Anda disarankan untuk memeriksa izin pada bucket yang bersangkutan dan izin dari setiap pengguna yang terlibat dalam temuan, jika aktivitas tidak terduga, lihat rekomendasi remediasi yang dirinci di [Memulihkan bucket S3 yang berpotensi dikompromikan](#)

**Topik**

- [Discovery:S3/AnomalousBehavior](#)
- [Discovery:S3/MaliciousIPCaller](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:S3/MaliciousIPCaller](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/MaliciousIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [PenTest:S3/ParrotLinux](#)
- [PenTest:S3/PentooLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)

## Discovery:S3/AnomalousBehavior

API yang biasa digunakan untuk menemukan objek S3 dipanggil dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa entitas IAM telah memanggil API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListObjects`. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Discovery:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk menemukan sumber daya di AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi tentang AWS lingkungan Anda. Contohnya termasuk `GetObjectAcl` dan `ListObjects`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Discovery:S3/MaliciousIPCaller.Custom

API S3 dipanggil dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa API S3, seperti `GetObjectAcl` atau `ListObjects`, dipanggil dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini. Tipe aktivitas ini terkait dengan tahap penemuan serangan ketika penyerang mengumpulkan informasi untuk menentukan apakah lingkungan AWS Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Discovery:S3/TorIPCaller

API S3 dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa API S3, seperti `GetObjectACL` atau `ListObjects`, dipanggil dari alamat IP node keluar Tor. Jenis aktivitas ini dikaitkan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah AWS lingkungan Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Exfiltration:S3/AnomalousBehavior

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM melakukan panggilan API yang melibatkan bucket S3 dan aktivitas ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan tahap eksfiltrasi serangan, di mana penyerang mencoba mengumpulkan data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Exfiltration:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk mengumpulkan data dari AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya berkaitan dengan taktik eksfiltrasi ketika musuh mencoba mengumpulkan data dari jaringan Anda. Contohnya termasuk `GetObject` dan `CopyObject`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Impact:S3/AnomalousBehavior.Delete

Entitas IAM memanggil API S3 yang mencoba menghapus data dengan cara yang mencurigakan.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang

mencoba menghapus data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk menentukan apakah versi objek sebelumnya dapat atau harus dipulihkan.

## Impact:S3/AnomalousBehavior.Permission

API yang biasa digunakan untuk mengatur izin daftar kontrol akses (ACL) dipanggil dengan cara yang tidak wajar.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda telah mengubah kebijakan bucket atau ACL pada bucket S3 yang terdaftar. Perubahan ini dapat mengekspos bucket S3 Anda secara publik ke semua pengguna yang diautentikasi. AWS

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat,



API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa tidak ada objek yang secara tidak terduga diizinkan untuk diakses secara publik.

## Impact:S3/AnomalousBehavior.Write

Entitas IAM memanggil API S3 yang mencoba menulis data dengan cara yang mencurigakan.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa entitas IAM di AWS lingkungan Anda melakukan panggilan API yang melibatkan bucket S3, dan perilaku ini berbeda dari baseline yang ditetapkan entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan serangan yang mencoba menulis data. Aktivitas ini mencurigakan karena entitas IAM memanggil API dengan cara yang tidak biasa. Misalnya, entitas IAM tanpa riwayat sebelumnya memanggil API S3, atau entitas IAM memanggil API S3 dari lokasi yang tidak biasa.

API ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua permintaan API di akun Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh musuh. Ini melacak berbagai faktor permintaan API, seperti pengguna yang membuat permintaan, lokasi dari mana permintaan dibuat, API spesifik yang diminta, bucket yang diminta, dan jumlah panggilan API yang dibuat. Untuk informasi selengkapnya tentang faktor permintaan API yang tidak biasa untuk identitas pengguna yang memanggil permintaan, lihat [Menemukan detail](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

Kami merekomendasikan audit konten bucket S3 Anda untuk memastikan bahwa panggilan API ini tidak menulis data berbahaya atau tidak sah.

## Impact:S3/MaliciousIPCaller

API S3 yang biasa digunakan untuk mengutak-atik data atau proses di AWS lingkungan dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3 dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API yang diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, menyela, atau menghancurkan data dalam lingkungan Anda. AWS Contohnya termasuk PutObject dan PutObjectACL.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## PenTest:S3/KaliLinux

API S3 dipanggil dari mesin Kali Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Kali Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Kali Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi

kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## PenTest:S3/ParrotLinux

API S3 dipanggil dari mesin Parrot Security Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Parrot Security Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Parrot Security Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan memperoleh akses yang tidak sah ke lingkungan AWS Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## PenTest:S3/PentooLinux

API S3 dipanggil dari mesin Pentoo Linux.

Tingkat keparahan default: Sedang

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan panggilan API S3 menggunakan kredensial milik akun Anda. AWS Kredensial Anda mungkin disusupi. Pentoo Linux adalah alat uji penetrasi populer yang digunakan para profesional keamanan untuk mengidentifikasi kelemahan dalam instans EC2 yang memerlukan patching. Penyerang juga menggunakan alat ini untuk menemukan kelemahan konfigurasi EC2 dan mendapatkan akses tidak sah ke lingkungan Anda. AWS

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Policy:S3/AccountBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan S3 Block Public Access pada akun.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa Blokir Akses Publik Amazon S3 dinonaktifkan pada tingkat akun. Ketika pengaturan Blokir Akses Publik S3 diaktifkan, ini digunakan untuk memfilter kebijakan atau daftar kontrol akses (ACL) pada bucket sebagai tindakan keamanan untuk mencegah eksposur data publik yang tidak disengaja.

Biasanya, Blokir Akses Umum S3 dinonaktifkan pada akun untuk memungkinkan akses publik ke bucket atau ke objek dalam bucket. Ketika Blokir Akses Publik S3 dinonaktifkan pada akun, akses ke bucket Anda dikendalikan oleh kebijakan, ACL, atau pengaturan Blokir Akses Publik tingkat bucket diterapkan ke bucket individu Anda. Ini tidak berarti bahwa bucket dibagikan secara publik, tetapi bahwa Anda harus mengaudit izin yang diterapkan ke bucket untuk mengonfirmasi bahwa mereka menyediakan tingkat akses yang sesuai.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Policy:S3/BucketAnonymousAccessGranted

Prinsipal IAM telah memberikan akses ke bucket S3 ke internet dengan mengubah kebijakan bucket atau ACL.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa bucket S3 yang terdaftar telah dibuat agar dapat diakses secara publik di internet karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket tersebut. Setelah perubahan kebijakan atau ACL terdeteksi, menggunakan penalaran otomatis yang didukung oleh [Zelkova](#), untuk menentukan apakah bucket dapat diakses oleh publik.

### Note

Jika kebijakan ACL atau bucket bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semuanya, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan pengaturan [Akses Publik Blok S3](#) yang mungkin telah diaktifkan untuk bucket S3 Anda. Dalam kasus seperti itu, `effectivePermission` nilai dalam temuan akan ditandai sebagai `UNKNOWN`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Policy:S3/BucketBlockPublicAccessDisabled

Entitas IAM memanggil API yang digunakan untuk menonaktifkan S3 Block Public Access pada bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini menginformasikan bahwa Blokir Akses Publik dinonaktifkan untuk bucket S3 yang terdaftar. Jika diaktifkan, pengaturan Blokir Akses Publik S3 digunakan untuk memfilter kebijakan atau daftar kontrol akses (ACL) yang diterapkan ke bucket sebagai tindakan keamanan untuk mencegah eksposur data publik yang tidak disengaja.

Biasanya, Blokir Akses Publik S3 dinonaktifkan pada bucket untuk memungkinkan akses publik ke bucket atau ke objek di dalamnya. Ketika Blokir Akses Publik S3 dinonaktifkan pada bucket, akses ke bucket dikendalikan oleh kebijakan atau ACL yang diterapkan padanya. Ini tidak berarti bahwa bucket dibagikan secara publik, tetapi Anda harus mengaudit kebijakan dan ACL yang diterapkan ke bucket untuk mengonfirmasi bahwa izin yang sesuai diterapkan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Policy:S3/BucketPublicAccessGranted

Prinsipal IAM telah memberikan akses publik ke bucket S3 kepada semua AWS pengguna dengan mengubah kebijakan bucket atau ACL.

Tingkat keparahan default: Tinggi

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa bucket S3 yang terdaftar telah diekspos secara publik ke semua AWS pengguna yang diautentikasi karena entitas IAM telah mengubah kebijakan bucket atau ACL pada bucket S3 tersebut. Setelah perubahan kebijakan atau ACL terdeteksi, menggunakan penalaran otomatis yang didukung oleh [Zelkova](#), untuk menentukan apakah bucket dapat diakses oleh publik.

### Note

Jika kebijakan ACL atau bucket bucket dikonfigurasi untuk secara eksplisit menolak atau menolak semuanya, temuan ini mungkin tidak mencerminkan status bucket saat ini. Temuan ini tidak akan mencerminkan pengaturan [Akses Publik Blok S3](#) yang mungkin telah diaktifkan

untuk bucket S3 Anda. Dalam kasus seperti itu, `effectivePermission` nilai dalam temuan akan ditandai sebagai `UNKNOWN`.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Stealth:S3/ServerAccessLoggingDisabled

Pencatatan log akses server S3 dinonaktifkan untuk bucket.

Tingkat keparahan default: Rendah

- Sumber data: acara CloudTrail manajemen

Temuan ini memberi tahu Anda bahwa pencatatan akses server S3 dinonaktifkan untuk ember di lingkungan Anda AWS . Jika dinonaktifkan, tidak ada log permintaan web yang dibuat untuk setiap upaya mengakses bucket S3 yang diidentifikasi, namun, panggilan API manajemen S3 ke bucket, seperti [DeleteBucket](#), masih dilacak. Jika pencatatan peristiwa data S3 diaktifkan CloudTrail untuk bucket ini, permintaan web untuk objek di dalam bucket akan tetap dilacak. Menonaktifkan pencatatan log adalah teknik yang digunakan oleh pengguna yang tidak sah untuk menghindari deteksi. Untuk mempelajari selengkapnya tentang log S3, lihat [Pencatatan Log Akses Server S3](#) dan [Opsis Pencatatan Log S3](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## UnauthorizedAccess:S3/MaliciousIPCaller.Custom

API S3 dipanggil dari alamat IP yang termasuk dalam daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3, seperti PutObject atau PutObjectAcl, dipanggil dari alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi tambahan dari detail temuan ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## UnauthorizedAccess:S3/TorIPCaller

API S3 dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Sumber data: peristiwa CloudTrail data untuk S3

Temuan ini menginformasikan bahwa operasi API S3, seperti PutObject atau PutObjectAcl, dipanggil dari alamat IP node keluar Tor. Tor adalah perangkat lunak yang memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Temuan ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:


Jika aktivitas ini tidak terduga untuk prinsipal terkait, ini mungkin menunjukkan bahwa kredensial telah diekspos atau izin S3 Anda tidak cukup membatasi. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## EKSjenis pencarian log audit

Temuan berikut khusus untuk sumber daya Kubernetes dan memiliki resource\_type. EKSCluster Tingkat keparahan dan detail temuan berbeda berdasarkan jenis temuan.



Untuk semua temuan tipe Kubernetes, kami sarankan Anda memeriksa sumber daya yang dimaksud untuk menentukan apakah aktivitas tersebut diharapkan atau berpotensi berbahaya. Untuk panduan tentang remediasi sumber daya Kubernetes yang dikompromikan yang diidentifikasi oleh sebuah temuan, lihat. GuardDuty [Memediasi temuan Pemantauan Log Audit EKS](#)

 Note

Jika aktivitas yang menghasilkan temuan ini diharapkan, pertimbangkan [Aturan penekanan](#) untuk menambahkan untuk mencegah peringatan masa depan.

## Topik

- [CredentialAccess:Kubernetes/MaliciousIPCaller](#)
- [CredentialAccess:Kubernetes/MaliciousIPCaller.Custom](#)
- [CredentialAccess:Kubernetes/SuccessfulAnonymousAccess](#)
- [CredentialAccess:Kubernetes/TorIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom](#)
- [DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess](#)
- [DefenseEvasion:Kubernetes/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Impact:Kubernetes/SuccessfulAnonymousAccess](#)
- [Impact:Kubernetes/TorIPCaller](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Persistence:Kubernetes/MaliciousIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/SuccessfulAnonymousAccess](#)

- [Persistence:Kubernetes/TorIPCaller](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated](#)
- [Execution:Kubernetes/AnomalousBehavior.ExecInPod](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer](#)
- [Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount](#)
- [Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated](#)
- [Discovery:Kubernetes/AnomalousBehavior.PermissionChecked](#)

#### Note

Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup ini dikaitkan dengan dan secara default. `system:discovery system:basic-user` ClusterRoles Asosiasi ini memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan cluster tidak mencabut izin ini. Bahkan jika Anda memperbarui kluster Anda ke versi 1.14 atau lebih tinggi, izin ini mungkin masih diaktifkan. Kami menyarankan Anda untuk memisahkan izin ini dari grup. `system:unauthenticated` Untuk panduan tentang mencabut izin ini, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

## CredentialAccess:Kubernetes/MaliciousIPCaller

APIUmumnya digunakan untuk mengakses kredensi atau rahasia di kluster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. API Observasi biasanya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

API Umumnya digunakan untuk mengakses kredensial atau rahasia di kluster Kubernetes dipanggil dari alamat IP pada daftar ancaman kustom.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. API Observasi biasanya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di bawah *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas

berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

APIUmumnya digunakan untuk mengakses kredensi atau rahasia di klaster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi berhasil dipanggil oleh pengguna. `system:anonymous` APIpanggilan yang dilakukan oleh tidak `system:anonymous` diautentikasi. Observasi biasanya API dikaitkan dengan taktik akses kredenal di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk klaster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada API tindakan yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredenal Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di klaster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## CredentialAccess:Kubernetes/TorIPCaller

APIUmumnya digunakan untuk mengakses kredensi atau rahasia dalam klaster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah API dipanggil dari alamat IP node keluar Tor. API Observasi biasanya dikaitkan dengan taktik akses kredensial di mana musuh mencoba mengumpulkan kata sandi, nama pengguna, dan kunci akses untuk kluster Kubernetes Anda. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya kluster Kubernetes Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## DefenseEvasion:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. Yang API diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang

diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

APIBiasanya digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. Yang API diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

APIYang biasa digunakan untuk menghindari tindakan defensif dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi berhasil dipanggil oleh pengguna. `system:anonymous` API panggilan yang dilakukan oleh tidak `system:anonymous` diautentikasi. Yang diamati umumnya API dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada API tindakan yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di kluster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## DefenseEvasion:Kubernetes/TorIPCaller

API yang umum digunakan untuk menghindari tindakan defensif dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah API dipanggil dari alamat IP node keluar Tor. Yang API diamati umumnya dikaitkan dengan taktik penghindaran pertahanan di mana musuh mencoba menyembunyikan tindakan mereka untuk menghindari deteksi. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke kluster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di `KubernetesUserDetails` bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API

dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Discovery:Kubernetes/MaliciousIPCaller

Sumber daya yang API umum digunakan untuk menemukan sumber daya dalam kluster Kubernetes dipanggil dari alamat IP.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. Observasi API biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas.

### Untuk akses yang tidak diautentikasi

MaliciousIPCallertemuan tidak dihasilkan untuk akses yang tidak diautentikasi.

SuccessfulAnonymousAccessTemuan dihasilkan untuk akses yang tidak diautentikasi atau anonim.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).



## Discovery:Kubernetes/MaliciousIPCaller.Custom

Sumber daya yang API umum digunakan untuk menemukan sumber daya di kluster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa a dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. API Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. Observasi API biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Discovery:Kubernetes/SuccessfulAnonymousAccess

API yang umum digunakan untuk menemukan sumber daya di kluster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi berhasil dipanggil oleh pengguna. *system:anonymous* API panggilan yang dilakukan oleh tidak *system:anonymous* diautentikasi. Yang API diamati umumnya dikaitkan dengan tahap penemuan serangan ketika musuh

mengumpulkan informasi di cluster Kubernetes Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada API tindakan yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Jenis temuan ini tidak termasuk API titik akhir pemeriksaan kesehatan seperti `/healthz`, `/livez/readyz`, dan `/version`

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di kluster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Discovery:Kubernetes/TorIPCaller

API yang umum digunakan untuk menemukan sumber daya dalam kluster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah API dipanggil dari alamat IP node keluar Tor. Observasi API biasanya digunakan dengan tahap penemuan serangan di mana penyerang mengumpulkan informasi untuk menentukan apakah cluster Kubernetes Anda rentan terhadap serangan yang lebih luas. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Hal ini dapat menunjukkan akses tidak sah ke kluster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di `KubernetesUserDetails` bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan

pencabutan izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Execution:Kubernetes/ExecInKubeSystemPod

Sebuah perintah dieksekusi di dalam pod di dalam **kube-system** namespace

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah perintah dieksekusi di sebuah pod di dalam **kube-system** namespace menggunakan Kubernetes exec. API `kube-systemnamespace` adalah ruang nama default, yang terutama digunakan untuk komponen tingkat sistem seperti `dan.kube-dns` `kube-proxy`. Sangat jarang untuk mengeksekusi perintah di dalam pod atau kontainer di bawah `kube-system` namespace dan mungkin menunjukkan aktivitas yang mencurigakan.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensi identitas pengguna yang digunakan untuk menjalankan perintah dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Impact:Kubernetes/MaliciousIPCaller

API yang biasa digunakan untuk mengutak-atik sumber daya di kluster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. Yang diamati umumnya API dikaitkan dengan taktik dampak di

mana musuh mencoba memanipulasi, menyela, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Impact:Kubernetes/MaliciousIPCaller.Custom

API yang biasa digunakan untuk mengutak-atik sumber daya di kluster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. Yang diamati umumnya API dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi, menyela, atau menghancurkan data dalam lingkungan Anda. AWS

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Impact:Kubernetes/SuccessfulAnonymousAccess

API yang biasa digunakan untuk mengutak-atik sumber daya di klaster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi berhasil dipanggil oleh pengguna. `system:anonymous` API panggilan yang dilakukan oleh `system:anonymous` tidak diautentikasi. Yang API diamati umumnya dikaitkan dengan tahap dampak serangan ketika musuh merusak sumber daya di cluster Anda. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada API tindakan yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna di klaster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Impact:Kubernetes/TorIPCaller

API yang umum digunakan untuk mengutak-atik sumber daya di cluster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah API dipanggil dari alamat IP node keluar Tor. Yang API diamati umumnya dikaitkan dengan taktik dampak di mana musuh mencoba memanipulasi,

menyela, atau menghancurkan data dalam lingkungan Anda. AWS Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke klaster Kubernetes Anda dengan maksud menyembunyikan identitas asli musuh.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Persistence:Kubernetes/ContainerWithSensitiveMount

Sebuah wadah diluncurkan dengan jalur host eksternal sensitif yang dipasang di dalamnya.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa wadah diluncurkan dengan konfigurasi yang menyertakan jalur host sensitif dengan akses tulis di `volumeMounts` bagian tersebut. Ini membuat jalur host sensitif dapat diakses dan dapat ditulis dari dalam wadah. Teknik ini biasanya digunakan oleh musuh untuk mendapatkan akses ke sistem file host.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan yang terdiri dari kriteria filter berdasarkan

`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter `imagePrefix` bidang harus sama dengan yang `imagePrefix` ditentukan dalam temuan. Untuk mempelajari selengkapnya tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).

## Persistence:Kubernetes/MaliciousIPCaller

APIBiasanya digunakan untuk mendapatkan akses persisten ke kluster Kubernetes dipanggil dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang terkait dengan aktivitas berbahaya yang diketahui. Yang API diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke cluster Kubernetes Anda dan berusaha mempertahankan akses itu.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah `system:anonymous`, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Persistence:Kubernetes/MaliciousIPCaller.Custom

APIBiasanya digunakan untuk mendapatkan akses persisten ke kluster Kubernetes dipanggil dari alamat IP pada daftar ancaman khusus.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi dipanggil dari alamat IP yang disertakan dalam daftar ancaman yang Anda unggah. Daftar ancaman yang terkait dengan temuan ini tercantum di bagian Informasi Tambahan dari detail temuan. Yang API diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke cluster Kubernetes Anda dan berusaha mempertahankan akses itu.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Persistence:Kubernetes/SuccessfulAnonymousAccess

API Biasanya digunakan untuk mendapatkan izin tingkat tinggi ke klaster Kubernetes dipanggil oleh pengguna yang tidak diautentikasi.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi berhasil dipanggil oleh pengguna. *system:anonymous* API panggilan yang dilakukan oleh tidak *system:anonymous* diautentikasi. Yang API diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke cluster Anda dan berusaha mempertahankan akses itu. Aktivitas ini menunjukkan bahwa akses anonim atau tidak diautentikasi diizinkan pada API tindakan yang dilaporkan dalam temuan dan mungkin diizinkan pada tindakan lain. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada *system:anonymous* pengguna di klaster Anda dan memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, Anda harus mencabut akses pengguna dan membalikkan perubahan apa pun yang dibuat oleh



musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Persistence:Kubernetes/TorIPCaller

APIBiasanya digunakan untuk mendapatkan akses persisten ke cluster Kubernetes dipanggil dari alamat IP node keluar Tor.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah API dipanggil dari alamat IP node keluar Tor. Yang API diamati umumnya dikaitkan dengan taktik persistensi di mana musuh telah mendapatkan akses ke cluster Kubernetes Anda dan berusaha mempertahankan akses itu. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Rekomendasi remediasi:

Jika pengguna yang dilaporkan dalam temuan di *KubernetesUserDetails* bagian ini adalah *system:anonymous*, selidiki mengapa pengguna anonim diizinkan untuk memanggil API dan mencabut izin, jika diperlukan, dengan mengikuti petunjuk dalam [Praktik terbaik Keamanan untuk Amazon di EKS](#) Panduan Pengguna Amazon. EKS Jika pengguna adalah pengguna yang diautentikasi, selidiki untuk menentukan apakah aktivitas tersebut sah atau berbahaya. Jika aktivitas berbahaya, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Akun layanan default diberikan hak istimewa admin pada kluster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa akun layanan default untuk namespace di kluster Kubernetes Anda telah diberikan hak istimewa admin. Kubernetes membuat akun layanan default untuk semua namespace di cluster. Ini secara otomatis menetapkan akun layanan default sebagai identitas ke pod yang belum secara eksplisit dikaitkan dengan akun layanan lain. Jika akun layanan default memiliki hak istimewa admin, hal itu dapat mengakibatkan pod diluncurkan secara tidak sengaja dengan hak istimewa admin. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Rekomendasi remediasi:

Anda tidak boleh menggunakan akun layanan default untuk memberikan izin ke pod. Sebagai gantinya, Anda harus membuat akun layanan khusus untuk setiap beban kerja dan memberikan izin ke akun tersebut berdasarkan kebutuhan. Untuk memperbaiki masalah ini, Anda harus membuat akun layanan khusus untuk semua pod dan beban kerja Anda dan memperbarui pod dan beban kerja untuk bermigrasi dari akun layanan default ke akun khusus mereka. Maka Anda harus menghapus izin admin dari akun layanan default. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Policy:Kubernetes/AnonymousAccessGranted

**system:anonymous** Pengguna diberikan API izin pada kluster Kubernetes.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa pengguna di kluster Kubernetes Anda berhasil membuat `ClusterRoleBinding` atau mengikat pengguna `RoleBinding` ke peran. `system:anonymous` Ini memungkinkan akses yang tidak diautentikasi ke API operasi yang diizinkan oleh peran. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan

Rekomendasi remediasi:

Anda harus memeriksa izin yang telah diberikan kepada `system:anonymous` pengguna atau `system:unauthenticated` grup di kluster Anda dan mencabut akses anonim yang tidak perlu. Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan EKS Pengguna Amazon. Jika izin diberikan secara berbahaya, Anda harus mencabut akses pengguna

yang memberikan izin dan membalikkan perubahan apa pun yang dibuat oleh musuh ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Policy:Kubernetes/ExposedDashboard

Dasbor untuk cluster Kubernetes terpapar ke internet

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa dasbor Kubernetes untuk kluster Anda diekspos ke internet oleh layanan Load Balancer. Dasbor yang terbuka membuat antarmuka manajemen cluster Anda dapat diakses dari internet dan memungkinkan musuh untuk mengeksploitasi kesenjangan otentikasi dan kontrol akses apa pun yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubernetes. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Policy:Kubernetes/KubeflowDashboardExposed

Dasbor Kubeflow untuk cluster Kubernetes diekspos ke Internet

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa dasbor Kubeflow untuk kluster Anda diekspos ke Internet oleh layanan Load Balancer. Dasbor Kubeflow yang terbuka membuat antarmuka manajemen lingkungan Kubeflow Anda dapat diakses dari Internet dan memungkinkan musuh untuk mengeksploitasi celah otentikasi dan kontrol akses apa pun yang mungkin ada.

Rekomendasi remediasi:

Anda harus memastikan bahwa otentikasi dan otorisasi yang kuat diberlakukan di Dasbor Kubeflow. Anda juga harus menerapkan kontrol akses jaringan untuk membatasi akses ke dasbor dari alamat IP tertentu.

Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## PrivilegeEscalation:Kubernetes/PrivilegedContainer

Kontainer istimewa dengan akses tingkat root diluncurkan di klaster Kubernetes Anda.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa kontainer istimewa diluncurkan di klaster Kubernetes Anda menggunakan gambar yang belum pernah digunakan sebelumnya untuk meluncurkan kontainer istimewa di klaster Anda. Wadah istimewa memiliki akses tingkat root ke host. Musuh dapat meluncurkan wadah istimewa sebagai taktik eskalasi hak istimewa untuk mendapatkan akses ke dan kemudian membahayakan tuan rumah.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung dapat dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh musuh ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Kubernetes yang API biasa digunakan untuk mengakses rahasia dipanggil dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi anomali untuk mengambil rahasia cluster sensitif telah dipanggil oleh pengguna Kubernetes di cluster Anda. Yang diamati umumnya API

dikaitkan dengan taktik akses kredensial yang dapat menyebabkan eskalasi istimewa dan akses lebih lanjut dalam cluster Anda. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensial Anda dikompromikan.

Yang diamati API diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API aktivitas pengguna dalam EKS kluster Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML melacak beberapa faktor API operasi seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes di kluster Anda dan pastikan bahwa semua izin ini diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensialnya dikompromikan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Sebuah RoleBinding atau ClusterRoleBinding ke peran yang terlalu permisif atau namespace yang sensitif telah dibuat atau dimodifikasi di kluster Kubernetes Anda.

Tingkat keparahan default: Sedang\*

### Note

Tingkat keparahan default temuan ini adalah Medium. Namun, jika RoleBinding atau ClusterRoleBinding melibatkan ClusterRoles `admin` atau `cluster-admin`, tingkat keparahannya Tinggi.

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa pengguna di klaster Kubernetes Anda membuat `RoleBinding` atau `ClusterRoleBinding` untuk mengikat pengguna ke peran dengan izin admin atau ruang nama sensitif. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensial Anda dikompromikan.

Yang diamati API diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API aktivitas pengguna dalam EKS klaster Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes. Izin ini didefinisikan dalam peran dan subjek yang terlibat dalam `RoleBinding` dan `ClusterRoleBinding`. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensialnya dikompromikan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

## Execution:Kubernetes/AnomalousBehavior.ExecInPod

Sebuah perintah dieksekusi di dalam pod dengan cara yang anomali.

Tingkat keparahan default: Sedang

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa sebuah perintah dijalankan di sebuah pod menggunakan Exec Kubernetes. API Exec Kubernetes API memungkinkan menjalankan perintah arbitrer dalam sebuah pod. Jika perilaku ini tidak diharapkan untuk pengguna, namespace, atau pod, ini mungkin menunjukkan kesalahan konfigurasi atau AWS kredensialmu disusupi.

Yang diamati API diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API aktivitas pengguna dalam EKS klaster Anda.

Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika eksekusi perintah ini tidak terduga, kredensial identitas pengguna yang digunakan untuk menjalankan perintah mungkin telah dikompromikan. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensialnya dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Beban kerja diluncurkan dengan wadah istimewa dengan cara yang anomali.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan wadah istimewa di klaster Amazon Anda. EKS Wadah istimewa memiliki akses tingkat root ke host. Pengguna yang tidak sah dapat meluncurkan kontainer istimewa sebagai taktik eskalasi hak istimewa untuk terlebih dahulu mendapatkan akses ke host dan kemudian mengkompromikannya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas image pengguna API dan container dalam EKS cluster Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

## Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensialnya dikompromikan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

## Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Beban kerja diterapkan dengan cara yang anomali, dengan jalur host sensitif dipasang di dalam beban kerja.

Tingkat keparahan default: Tinggi

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa beban kerja diluncurkan dengan wadah yang menyertakan jalur host sensitif di bagian tersebut `volumeMounts`. Ini berpotensi membuat jalur host sensitif dapat diakses dan dapat ditulis dari dalam wadah. Teknik ini biasanya digunakan oleh pengguna yang tidak sah untuk mendapatkan akses ke sistem file host.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas image pengguna API dan container dalam EKS cluster Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda,



dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).


Jika AWS kredensialnya dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Beban kerja diluncurkan dengan cara yang anomali.

Tingkat keparahan default: Rendah\*

 Note

Tingkat keparahan default adalah Rendah. Namun, jika beban kerja berisi nama gambar yang berpotensi mencurigakan, seperti alat pentest yang dikenal, atau wadah yang menjalankan perintah yang berpotensi mencurigakan saat peluncuran, seperti perintah shell terbalik, maka tingkat keparahan jenis temuan ini akan dianggap sebagai Medium.

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa beban kerja Kubernetes dibuat atau dimodifikasi dengan cara yang tidak wajar, seperti API aktivitas, gambar kontainer baru, atau konfigurasi beban kerja

berisiko, di dalam klaster Amazon Anda. EKS Pengguna yang tidak sah dapat meluncurkan kontainer sebagai taktik untuk mengeksekusi kode arbitrer untuk terlebih dahulu mendapatkan akses ke host dan kemudian mengkompromikannya.

Pembuatan atau modifikasi wadah yang diamati diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua aktivitas image pengguna API dan container dalam EKS cluster Anda. Model ML ini juga mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika peluncuran kontainer ini tidak terduga, kredensial identitas pengguna yang digunakan untuk meluncurkan penampung mungkin telah disusupi. Cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensialnya dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

Jika peluncuran kontainer ini diharapkan, Anda disarankan untuk menggunakan aturan penekanan dengan kriteria filter berdasarkan `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` bidang. Dalam kriteria filter, `imagePrefix` bidang harus memiliki nilai yang sama dengan `imagePrefix` bidang yang ditentukan dalam temuan. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Peran yang sangat permisif atau ClusterRole diciptakan atau dimodifikasi dengan cara yang anomali.

Tingkat keparahan default: Rendah

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa API operasi anomali untuk membuat Role atau ClusterRole dengan izin berlebihan dipanggil oleh pengguna Kubernetes di cluster Amazon Anda. EKS Aktor dapat menggunakan pembuatan peran dengan izin yang kuat untuk menghindari penggunaan peran mirip admin bawaan dan menghindari deteksi. Izin yang berlebihan dapat menyebabkan eskalasi istimewa, eksekusi kode jarak jauh, dan berpotensi mengontrol namespace atau cluster. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda dikompromikan.

Yang diamati API diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API aktivitas pengguna dalam EKS klaster Amazon Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, agen pengguna yang digunakan, gambar kontainer yang diamati di akun Anda, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang ditentukan dalam Role atau ClusterRole untuk memastikan bahwa semua izin diperlukan dan ikuti prinsip hak istimewa paling sedikit. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke klaster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

## Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Seorang pengguna memeriksa izin akses mereka dengan cara yang tidak wajar.

Tingkat keparahan default: Rendah

- Fitur: log EKS audit

Temuan ini memberi tahu Anda bahwa pengguna di klaster Kubernetes Anda berhasil memeriksa apakah izin kuat yang diketahui yang dapat menyebabkan eskalasi istimewa dan eksekusi kode jarak jauh, diizinkan atau tidak. Misalnya, perintah umum yang digunakan untuk memeriksa izin bagi pengguna adalah `kubectl auth can-i`. Jika perilaku ini tidak diharapkan, ini mungkin menunjukkan kesalahan konfigurasi atau kredensial Anda telah disusupi.

Yang diamati API diidentifikasi sebagai anomali oleh model pembelajaran mesin deteksi GuardDuty anomali (ML). Model ML mengevaluasi semua API aktivitas pengguna dalam EKS kluster Amazon Anda dan mengidentifikasi kejadian anomali yang terkait dengan teknik yang digunakan oleh pengguna yang tidak sah. Model ML juga melacak beberapa faktor API operasi, seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, izin diperiksa, dan namespace yang dioperasikan pengguna. Anda dapat menemukan detail API permintaan yang tidak biasa, di panel detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Periksa izin yang diberikan kepada pengguna Kubernetes untuk memastikan bahwa semua izin diperlukan. Jika izin diberikan secara keliru atau jahat, cabut akses pengguna dan balikkan perubahan apa pun yang dibuat oleh pengguna yang tidak sah ke kluster Anda. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

Jika AWS kredensi Anda dikompromikan, lihat. [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)

## Jenis penemuan Runtime Monitoring

Amazon GuardDuty menghasilkan temuan Runtime Monitoring berikut untuk menunjukkan potensi ancaman berdasarkan perilaku tingkat sistem operasi dari EC2 host dan container Amazon di EKS kluster Amazon, beban kerja Fargate dan Amazon, serta instans ECS Amazon Anda. EC2

### Note

Jenis pencarian Runtime Monitoring didasarkan pada log runtime yang dikumpulkan dari host. Log berisi bidang seperti jalur file yang dapat dikontrol oleh aktor jahat. Bidang ini juga termasuk dalam GuardDuty temuan untuk memberikan konteks runtime. Saat memproses temuan Runtime Monitoring di luar GuardDuty konsol, Anda harus membersihkan bidang pencarian. Misalnya, Anda dapat HTML menyandikan bidang pencarian saat menampilkannya di halaman web.

Topik

- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)

- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [DefenseEvasion:Runtime/ProcessInjection.Proc](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [DefenseEvasion:Runtime/FilelessExecution](#)
- [Impact:Runtime/CryptoMinerExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)

- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

## CryptoCurrency:Runtime/BitcoinTool.B

EC2Instance Amazon atau container menanyakan alamat IP yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan Alamat IP yang terkait dengan aktivitas terkait cryptocurrency. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini atau wadah untuk menambang atau mengelola cryptocurrency, atau salah satu dari ini terlibat dalam aktivitas blockchain, CryptoCurrency:Runtime/BitcoinTool.B temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai. CryptoCurrency:Runtime/BitcoinTool.B Kriteria filter kedua harus berupa ID Instance dari instance atau Container Image ID dari container yang terlibat dalam cryptocurrency atau aktivitas terkait blockchain. Untuk informasi selengkapnya, lihat [Aturan penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Backdoor:Runtime/C&CActivity.B

EC2Instance Amazon atau wadah menanyakan IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda sedang menanyakan IP yang terkait dengan server perintah dan kontrol (C&C) yang diketahui. Instance atau wadah yang terdaftar mungkin berpotensi dikompromikan. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan () terdistribusi. DDoS

### Note

Jika IP yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## UnauthorizedAccess:Runtime/TorRelay

EC2 Instance Amazon Anda atau wadah membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance atau wadah di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relay Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor meningkatkan anonimitas komunikasi dengan meneruskan lalu lintas klien yang kemungkinan terlarang dari satu relay Tor ke relay lainnya.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## UnauthorizedAccess:Runtime/TorClient

EC2 Instance Amazon atau container Anda membuat koneksi ke Tor Guard atau node Authority.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance atau wadah di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway



awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa EC2 instance atau wadah ini berpotensi dikompromikan dan bertindak sebagai klien di jaringan Tor. Temuan ini mungkin menunjukkan akses tidak sah ke AWS sumber daya Anda dengan maksud menyembunyikan identitas asli penyerang.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/BlackholeTraffic

EC2Instance Amazon atau wadah mencoba berkomunikasi dengan alamat IP host jarak jauh yang merupakan lubang hitam yang dikenal.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda EC2 contoh yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena mencoba berkomunikasi dengan alamat IP lubang hitam (atau lubang wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host yang ditugaskan.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/DropPoint

EC2Instans Amazon atau wadah mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui memiliki kredensyal dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance atau wadah di AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP host jarak jauh yang diketahui menyimpan kredensyal dan data curian lainnya yang ditangkap oleh malware.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## CryptoCurrency:Runtime/BitcoinTool.B!DNS

EC2Instance Amazon atau container menanyakan nama domain yang terkait dengan aktivitas cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

## Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance atau wadah ini untuk menambang atau mengelola cryptocurrency, atau salah satu dari ini terlibat dalam aktivitas blockchain, `CryptoCurrency:Runtime/BitcoinTool.B!DNS` temuan ini bisa menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Kriteria filter kedua harus berupa ID Instance dari instance atau Container Image ID dari container yang terlibat dalam aktivitas cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat [Aturan Penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Backdoor:Runtime/C&CActivity.B!DNS

EC2Instance Amazon atau container menanyakan nama domain yang dikaitkan dengan server perintah dan kontrol yang dikenal.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. EC2Instance yang terdaftar atau wadah mungkin dikompromikan. Server perintah dan kontrol adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet yang mungkin termasuk PCs, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh jenis malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung pada tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai serangan penolakan layanan () terdistribusi. DDoS

### Note

Jika nama domain yang ditanyakan terkait log4j, maka bidang temuan terkait akan mencakup nilai-nilai berikut:

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

### Note

Untuk menguji bagaimana GuardDuty menghasilkan jenis temuan ini, Anda dapat membuat DNS permintaan dari instance Anda (menggunakan `dig` untuk Linux atau `nslookup` untuk Windows) terhadap domain pengujianguarddutyb.com.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/BlackholeTraffic!DNS

EC2Instance Amazon atau wadah menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain yang sedang dialihkan ke alamat IP lubang hitam. Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dituju.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/DropPoint!DNS

EC2Instance Amazon atau kontainer menanyakan nama domain dari host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance atau wadah di AWS lingkungan Anda menanyakan nama domain host jarak jauh yang diketahui memiliki kredensial dan data curian lainnya yang ditangkap oleh malware.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/DGADomainRequest.C!DNS

EC2Instance Amazon atau container menanyakan domain yang dihasilkan secara algoritmik. Domain semacam itu biasanya digunakan oleh malware dan bisa menjadi indikasi EC2 instance yang dikompromikan atau wadah.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda sedang mencoba menanyakan domain algorithm (DGA) pembuatan domain. Sumber daya Anda mungkin telah dikompromikan.

DGAsdigunakan untuk secara berkala menghasilkan sejumlah besar nama domain yang dapat digunakan sebagai titik pertemuan dengan server perintah dan kontrol (C&C) mereka. Server

perintah dan kontrol adalah komputer yang mengeluarkan perintah kepada anggota botnet, yang merupakan kumpulan perangkat yang terhubung ke internet yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Banyaknya kemungkinan titik pertemuan menyulitkan untuk mematikan botnet secara efektif karena komputer yang terinfeksi berusaha menghubungi beberapa nama domain ini setiap hari untuk menerima pembaruan atau perintah.

#### Note

Temuan ini didasarkan pada DGA domain yang diketahui dari umpan intelijen GuardDuty ancaman.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/DriveBySourceTraffic!DNS

EC2Instance Amazon atau container menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan Drive-By yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah di AWS lingkungan Anda mungkin terganggu karena menanyakan nama domain host jarak jauh yang merupakan sumber serangan unduhan drive-by yang diketahui. Ini adalah unduhan perangkat lunak komputer yang tidak diinginkan dari internet yang dapat memulai instalasi otomatis virus, spyware, atau malware.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Trojan:Runtime/PhishingDomainRequest!DNS

EC2Instance Amazon atau container menanyakan domain yang terlibat dalam serangan phishing.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa ada EC2 instance atau wadah di AWS lingkungan Anda yang mencoba menanyakan domain yang terlibat dalam serangan phishing. Domain phishing dibuat oleh seseorang yang menyamar sebagai institusi yang sah untuk membujuk individu agar memberikan data sensitif, seperti informasi pengenal pribadi, detail kartu kredit dan perbankan, serta kata sandi. EC2Instance atau wadah Anda mungkin mencoba mengambil data sensitif yang disimpan di situs web phishing, atau mungkin mencoba menyiapkan situs web phishing. EC2Instance Anda atau wadah mungkin dikompromikan.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Impact:Runtime/AbusedDomainRequest.Reputation

EC2Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang dikaitkan dengan domain yang disalahgunakan yang diketahui.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain atau alamat IP yang disalahgunakan yang diketahui. Contoh domain yang disalahgunakan adalah nama domain tingkat atas (TLDs) dan nama domain tingkat kedua (2LDs) yang menyediakan pendaftaran subdomain gratis serta penyedia dinamis. DNS Aktor ancaman cenderung menggunakan layanan ini untuk mendaftarkan domain secara gratis atau dengan biaya rendah. Domain bereputasi rendah dalam kategori ini mungkin juga merupakan domain kedaluwarsa yang mencari alamat IP parkir registrar dan oleh karena itu mungkin tidak lagi aktif. IP parkir adalah tempat registrar mengarahkan lalu lintas untuk domain yang belum ditautkan ke layanan apa pun. EC2Instans Amazon yang terdaftar atau wadah dapat dikompromikan karena pelaku ancaman biasanya menggunakan registrar atau layanan ini untuk distribusi C&C dan malware.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Impact:Runtime/BitcoinDomainRequest.Reputation

EC2Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang terkait dengan aktivitas terkait cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan Bitcoin atau aktivitas terkait cryptocurrency lainnya. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.



Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika Anda menggunakan EC2 instance ini atau wadah untuk menambang atau mengelola cryptocurrency, atau jika sumber daya ini terlibat dalam aktivitas blockchain, temuan ini dapat mewakili aktivitas yang diharapkan untuk lingkungan Anda. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai `Impact:Runtime/BitcoinDomainRequest.Reputation`. Kriteria filter kedua harus berupa ID Instance dari instance atau ID Gambar Kontainer dari container terlibat dalam aktivitas terkait cryptocurrency atau blockchain. Untuk informasi selengkapnya, lihat [Aturan penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Impact:Runtime/MaliciousDomainRequest.Reputation

EC2Instance Amazon atau container menanyakan domain dengan reputasi rendah yang dikaitkan dengan domain berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang terkait dengan domain berbahaya atau alamat IP yang diketahui. Misalnya, domain dapat dikaitkan dengan alamat IP sinkhole yang dikenal. Domain sinkhole adalah domain yang sebelumnya dikendalikan oleh aktor ancaman, dan permintaan yang dibuat untuk domain tersebut dapat menunjukkan bahwa instans disusupi. Domain ini juga dapat dikorelasikan dengan kampanye berbahaya atau algoritme pembuatan domain yang dikenal.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Impact:Runtime/SuspiciousDomainRequest.Reputation

EC2Instance Amazon atau container menanyakan nama domain dengan reputasi rendah yang mencurigakan karena usianya, atau popularitasnya yang rendah.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa EC2 instance yang terdaftar atau wadah dalam AWS lingkungan Anda menanyakan nama domain dengan reputasi rendah yang diduga jahat. memperhatikan karakteristik domain ini yang konsisten dengan domain berbahaya yang diamati sebelumnya, namun, model reputasi kami tidak dapat secara definitif menghubungkannya dengan ancaman yang diketahui. Domain ini biasanya baru diamati atau menerima jumlah lalu lintas yang rendah.

Domain reputasi rendah didasarkan pada model skor reputasi. Model ini mengevaluasi dan memberi peringkat karakteristik domain untuk menentukan kemungkinannya berbahaya.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## UnauthorizedAccess:Runtime/MetadataDNSRebind

EC2Instance Amazon atau container sedang melakukan DNS pencarian yang menyelesaikan layanan metadata instance.

## Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

### Note

Saat ini, jenis temuan ini hanya didukung untuk AMD64 arsitektur.

Temuan ini memberi tahu Anda bahwa EC2 instance atau wadah di AWS lingkungan Anda menanyakan domain yang menyelesaikan alamat IP EC2 metadata (169.254.169.254). DNSKueri semacam ini dapat menunjukkan bahwa instance adalah target dari teknik DNS pengikatan ulang. Teknik ini dapat digunakan untuk mendapatkan metadata dari sebuah EC2 instance, termasuk IAM kredensial yang terkait dengan instance.

DNSrebinding melibatkan menipu aplikasi yang berjalan pada EC2 instance untuk memuat data yang dikembalikan dari aURL, di mana nama domain dalam URL menyelesaikan ke alamat IP EC2 metadata (). 169.254.169.254 Ini menyebabkan aplikasi mengakses EC2 metadata dan mungkin membuatnya tersedia untuk penyerang.

Dimungkinkan untuk mengakses EC2 metadata menggunakan DNS rebinding hanya jika EC2 instance menjalankan aplikasi rentan yang memungkinkan injeksiURLs, atau jika seseorang mengakses URL di browser web yang berjalan pada instance. EC2

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Menanggapi temuan ini, Anda harus mengevaluasi apakah ada aplikasi rentan yang berjalan pada EC2 instance atau pada wadah, atau jika seseorang menggunakan browser untuk mengakses domain yang diidentifikasi dalam temuan. Jika akar penyebabnya adalah aplikasi yang rentan, perbaiki kerentanan. Jika seseorang menelusuri domain yang diidentifikasi, blokir domain atau cegah pengguna mengaksesnya. Jika Anda menentukan temuan ini terkait dengan kedua kasus di atas, [Cabut sesi yang terkait dengan instance](#). EC2

Beberapa AWS pelanggan sengaja memetakan alamat IP metadata ke nama domain di server otoritatif mereka. DNS Jika hal ini dilakukan di lingkungan Anda, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua

kriteria filter. Kriteria filter pertama harus menggunakan atribut Finding type dengan nilai.

`UnauthorizedAccess:Runtime/MetaDataDNSRebind` Kriteria filter kedua harus domain DNS permintaan atau ID Gambar Kontainer wadah. Nilai domain DNS permintaan harus sesuai dengan domain yang telah Anda petakan ke alamat IP metadata (`.169.254.169.254`). Untuk informasi tentang membuat aturan penindasan, lihat Aturan [penindasan](#).

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/NewBinaryExecuted

File biner yang baru dibuat atau baru dimodifikasi dalam wadah telah dieksekusi.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa file biner yang baru dibuat atau yang baru saja dimodifikasi dalam wadah telah dieksekusi. Ini adalah praktik terbaik untuk menjaga kontainer tetap tidak berubah saat runtime, dan file biner, skrip, atau pustaka tidak boleh dibuat atau dimodifikasi selama masa pakai penampung. Perilaku ini menunjukkan bahwa aktor jahat yang telah memperoleh akses ke wadah, telah mengunduh, dan mengeksekusi malware atau perangkat lunak lain sebagai bagian dari potensi kompromi. Meskipun jenis aktivitas ini bisa menjadi indikasi kompromi, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/DockerSocketAccessed

Sebuah proses di dalam wadah berkomunikasi dengan daemon Docker menggunakan soket Docker.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Soket Docker adalah Unix Domain Socket yang digunakan Docker daemon (`dockerd`) untuk berkomunikasi dengan kliennya. Klien dapat melakukan berbagai tindakan, seperti membuat kontainer dengan berkomunikasi dengan daemon Docker melalui soket Docker. Sangat mencurigakan jika proses penampung mengakses soket Docker. Proses kontainer dapat keluar dari wadah dan mendapatkan akses tingkat host dengan berkomunikasi dengan soket Docker dan membuat wadah istimewa.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/RuncContainerEscape

Upaya pelarian kontainer melalui runC terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

runC adalah runtime kontainer tingkat rendah yang digunakan runtime kontainer tingkat tinggi, seperti Docker dan Containerd untuk menelurkan dan menjalankan container. RunC selalu dieksekusi dengan hak akses root karena perlu melakukan tugas tingkat rendah untuk membuat wadah. Aktor ancaman dapat memperoleh akses tingkat host dengan memodifikasi atau mengeksploitasi kerentanan dalam biner RuNC.

Temuan ini mendeteksi modifikasi biner runC dan upaya potensial untuk mengeksploitasi kerentanan RuNC berikut:

- [CVE-2019-5736](#)— Eksploitasi CVE-2019-5736 melibatkan penimpaan biner runC dari dalam wadah. Temuan ini dipanggil ketika biner runC dimodifikasi oleh proses di dalam wadah.

- [CVE-2024-21626](#) Eksploitasi CVE-2024-21626 melibatkan pengaturan direktori kerja saat ini (CWD) atau wadah ke `/proc/self/fd/FileDescriptor` deskriptor file terbuka. Temuan ini dipanggil ketika proses kontainer dengan direktori kerja saat ini di bawah `/proc/self/fd/` terdeteksi, misalnya, `/proc/self/fd/7`.

Temuan ini mungkin menunjukkan bahwa aktor jahat telah berusaha melakukan eksploitasi di salah satu jenis wadah berikut:

- Wadah baru dengan gambar yang dikendalikan penyerang.
- Wadah yang ada yang dapat diakses oleh aktor dengan izin menulis pada biner runC tingkat host.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Upaya pelarian kontainer melalui agen CGroups rilis terdeteksi.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa upaya untuk memodifikasi file agen rilis grup kontrol (cgroup) telah terdeteksi. Linux menggunakan kelompok kontrol (cgroups) untuk membatasi, memperhitungkan, dan mengisolasi penggunaan sumber daya dari kumpulan proses. Setiap cgroup memiliki file agen rilis (`release_agent`), skrip yang dijalankan Linux ketika proses apa pun di dalam cgroup berakhir. File agen rilis selalu dijalankan di tingkat host. Aktor ancaman di dalam wadah dapat melarikan diri ke host dengan menulis perintah arbitrer ke file agen rilis milik cgroup. Ketika proses di dalam cgroup itu berakhir, perintah yang ditulis oleh aktor dieksekusi.

Agan runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## DefenseEvasion:Runtime/ProcessInjection.Proc

Injeksi proses menggunakan sistem file proc terdeteksi dalam wadah atau instance Amazon. EC2

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Proc filesystem (procfs) adalah filesystem khusus di Linux yang menyajikan memori virtual proses sebagai file. Jalur file itu adalah `/proc/PID/mem`, di mana PID ID unik dari proses tersebut. Seorang aktor ancaman dapat menulis ke file ini untuk menyuntikkan kode ke dalam proses. Temuan ini mengidentifikasi upaya potensial untuk menulis ke file ini.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## DefenseEvasion:Runtime/ProcessInjection.Ptrace

Injeksi proses menggunakan panggilan sistem ptrace terdeteksi dalam wadah atau EC2 instance Amazon.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Suatu proses dapat menggunakan panggilan sistem `ptrace` untuk menyuntikkan kode ke proses lain. Temuan ini mengidentifikasi upaya potensial untuk menyuntikkan kode ke dalam proses menggunakan panggilan sistem `ptrace`.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Injeksi proses melalui penulisan langsung ke memori virtual terdeteksi dalam wadah atau EC2 instance Amazon.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Injeksi proses adalah teknik yang digunakan aktor ancaman untuk menyuntikkan kode ke dalam proses untuk menghindari pertahanan dan berpotensi meningkatkan hak istimewa. Suatu proses dapat menggunakan panggilan sistem seperti `process_vm_writew` untuk langsung menyuntikkan kode ke memori virtual proses lain. Temuan ini mengidentifikasi upaya potensial untuk menyuntikkan kode ke dalam proses menggunakan panggilan sistem untuk menulis ke memori virtual proses.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/ReverseShell

Proses dalam wadah atau EC2 instance Amazon telah membuat shell terbalik.



Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Shell terbalik adalah sesi shell yang dibuat pada koneksi yang dimulai dari host target ke host aktor. Ini berlawanan dengan cangkang normal yang dimulai dari host aktor ke host target. Aktor ancaman membuat shell terbalik untuk menjalankan perintah pada target setelah mendapatkan akses awal ke target. Temuan ini mengidentifikasi upaya potensial untuk membuat shell terbalik.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, jenis sumber daya Anda mungkin telah disusupi.

## DefenseEvasion:Runtime/FilelessExecution

Proses dalam wadah atau EC2 instance Amazon mengeksekusi kode dari memori.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda ketika suatu proses dijalankan menggunakan file yang dapat dieksekusi dalam memori pada disk. Ini adalah teknik penghindaran pertahanan umum yang menghindari penulisan executable berbahaya ke disk untuk menghindari deteksi berbasis pemindaian sistem file. Meskipun teknik ini digunakan oleh malware, ia juga memiliki beberapa kasus penggunaan yang sah. Salah satu contohnya adalah just-in-time (JIT) compiler yang menulis kode dikompilasi ke memori dan mengeksekusinya dari memori.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Impact:Runtime/CryptoMinerExecuted

Sebuah wadah atau EC2 instance Amazon mengeksekusi file biner yang terkait dengan aktivitas penambangan cryptocurrency.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa wadah atau EC2 instance di AWS lingkungan Anda mengeksekusi file biner yang terkait dengan aktivitas penambangan cryptocurrency. Aktor ancaman mungkin berusaha untuk mengambil kendali atas sumber daya komputasi untuk menggunakannya kembali secara jahat untuk penambangan cryptocurrency yang tidak sah.

Agen runtime memantau peristiwa dari beberapa jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya di panel temuan di GuardDuty konsol.

Rekomendasi remediasi:

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol dan lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/NewLibraryLoaded

Pustaka yang baru dibuat atau yang baru dimodifikasi dimuat oleh proses di dalam wadah.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa pustaka dibuat atau dimodifikasi di dalam wadah selama runtime dan dimuat oleh proses yang berjalan di dalam wadah. Praktik terbaik adalah menjaga kontainer tetap tidak berubah saat runtime, dan tidak membuat atau memodifikasi file biner, skrip, atau pustaka selama masa pakai penampung. Memuat pustaka yang baru dibuat atau dimodifikasi dalam wadah dapat menunjukkan aktivitas yang mencurigakan. Perilaku ini menunjukkan bahwa

aktor jahat berpotensi memperoleh akses ke wadah, telah mengunduh, dan mengeksekusi malware atau perangkat lunak lain sebagai bagian dari potensi kompromi. Meskipun jenis aktivitas ini bisa menjadi indikasi kompromi, ini juga merupakan pola penggunaan yang umum. Oleh karena itu, GuardDuty gunakan mekanisme untuk mengidentifikasi contoh mencurigakan dari aktivitas ini dan menghasilkan jenis temuan ini hanya untuk contoh yang mencurigakan.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Sebuah proses di dalam kontainer memasang sistem file host saat runtime.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Beberapa teknik pelarian kontainer melibatkan pemasangan sistem file host di dalam wadah saat runtime. Temuan ini memberi tahu Anda bahwa proses di dalam wadah berpotensi mencoba memasang sistem file host, yang mungkin menunjukkan upaya untuk melarikan diri ke host.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/UserfaultfdUsage

Sebuah proses yang digunakan **userfaultfd** sistem panggilan untuk menangani kesalahan halaman dalam ruang pengguna.

Tingkat keparahan default: Sedang

- Fitur: Pemantauan Runtime

Biasanya, kesalahan halaman ditangani oleh kernel di ruang kernel. Namun, panggilan `userfaultfd` sistem memungkinkan proses untuk menangani kesalahan halaman pada sistem file di ruang pengguna. Ini adalah fitur berguna yang memungkinkan implementasi sistem file ruang pengguna. Di sisi lain, ini juga dapat digunakan oleh proses yang berpotensi berbahaya untuk mengganggu kernel dari ruang pengguna. Menginterupsi kernel dengan menggunakan panggilan `userfaultfd` sistem adalah teknik eksploitasi umum untuk memperluas jendela balapan selama eksploitasi kondisi ras kernel. Penggunaan `userfaultfd` dapat menunjukkan aktivitas mencurigakan pada instans Amazon Elastic Compute Cloud EC2 (Amazon).

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/SuspiciousTool

Container atau EC2 instance Amazon menjalankan file biner atau skrip yang sering digunakan dalam skenario keamanan ofensif seperti keterlibatan pentesting.

Tingkat keparahan default: Variabel

Tingkat keparahan temuan ini bisa tinggi atau rendah, tergantung pada apakah alat mencurigakan yang terdeteksi dianggap penggunaan ganda atau hanya untuk penggunaan ofensif.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa alat yang mencurigakan telah dieksekusi pada EC2 instance atau wadah di lingkungan Anda AWS . Ini termasuk alat yang digunakan dalam keterlibatan pentesting, juga dikenal sebagai alat backdoor, pemindai jaringan, dan sniffer jaringan. Semua alat ini dapat digunakan dalam konteks jinak tetapi juga sering digunakan oleh pelaku ancaman dengan niat jahat. Mengamati alat keamanan ofensif dapat menunjukkan bahwa EC2 contoh atau wadah terkait telah dikompromikan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/SuspiciousCommand

Perintah mencurigakan telah dijalankan pada EC2 instance Amazon atau wadah yang menunjukkan kompromi.

Tingkat keparahan default: Variabel

Bergantung pada dampak dari pola berbahaya yang diamati, tingkat keparahan jenis temuan ini bisa rendah, sedang, atau tinggi.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah mencurigakan telah dijalankan dan ini menunjukkan bahwa EC2 instance Amazon atau wadah di AWS lingkungan Anda telah disusupi. Ini mungkin berarti bahwa file diunduh dari sumber yang mencurigakan dan kemudian dieksekusi, atau proses yang berjalan menampilkan pola berbahaya yang diketahui di baris perintahnya. Ini lebih lanjut menunjukkan bahwa malware berjalan di sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## DefenseEvasion:Runtime/SuspiciousCommand

Sebuah perintah telah dijalankan pada EC2 instance Amazon yang terdaftar atau wadah, ia mencoba untuk memodifikasi atau menonaktifkan mekanisme pertahanan Linux, seperti firewall atau layanan sistem penting.

Tingkat keparahan default: Variabel

Bergantung pada mekanisme pertahanan mana yang telah dimodifikasi atau dinonaktifkan, tingkat keparahan jenis temuan ini bisa tinggi, sedang, atau rendah.

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa perintah yang mencoba menyembunyikan serangan dari layanan keamanan sistem lokal, telah dieksekusi. Ini termasuk tindakan seperti menonaktifkan firewall Unix, memodifikasi tabel IP lokal, menghapus crontab entri, menonaktifkan layanan lokal, atau mengambil alih fungsi. LDPpreload Modifikasi apa pun sangat mencurigakan dan merupakan indikator kompromi yang potensial. Oleh karena itu, mekanisme ini mendeteksi atau mencegah kompromi lebih lanjut dari sistem.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## DefenseEvasion:Runtime/PtraceAntiDebugging

Proses dalam wadah atau EC2 instans Amazon telah menjalankan tindakan anti-debugging menggunakan panggilan sistem ptrace.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini menunjukkan bahwa proses yang berjalan pada EC2 instance Amazon atau wadah dalam AWS lingkungan Anda telah menggunakan panggilan sistem ptrace dengan PTRACE\_TRACEME opsi tersebut. Aktivitas ini akan menyebabkan debugger terlampir terlepas dari proses yang sedang berjalan. Jika tidak ada debugger yang terpasang, itu tidak berpengaruh. Namun, aktivitas itu sendiri menimbulkan kecurigaan. Ini mungkin menunjukkan bahwa malware berjalan di sistem. Malware sering menggunakan teknik anti-debugging untuk menghindari analisis, dan teknik ini dapat dideteksi saat runtime.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agen runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/MaliciousFileExecuted

File executable berbahaya yang diketahui telah dieksekusi pada EC2 instance Amazon atau wadah.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa executable berbahaya yang diketahui telah dieksekusi di EC2 instans Amazon atau wadah di lingkungan Anda. AWS Ini adalah indikator kuat bahwa instance atau wadah berpotensi dikompromikan dan malware telah dieksekusi.

Malware sering menggunakan teknik anti-debugging untuk menghindari analisis, dan teknik ini dapat dideteksi saat runtime.

GuardDuty memeriksa aktivitas dan konteks runtime terkait sehingga menghasilkan temuan ini hanya ketika aktivitas dan konteks terkait berpotensi mencurigakan.

Agan runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Execution:Runtime/SuspiciousShellCreated

Layanan jaringan atau proses yang dapat diakses jaringan pada EC2 instans Amazon, atau dalam wadah telah memulai proses shell interaktif.

Tingkat keparahan default: Rendah

- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa layanan yang dapat diakses jaringan pada EC2 instans Amazon atau dalam wadah di AWS lingkungan Anda telah meluncurkan shell interaktif. Dalam keadaan tertentu, skenario ini dapat mengindikasikan perilaku pasca-eksploitasi. Shell interaktif memungkinkan penyerang untuk mengeksekusi perintah arbitrer pada instance atau wadah yang dikompromikan.

Agan runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol. Anda dapat melihat informasi proses yang dapat diakses jaringan di detail proses induk.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## PrivilegeEscalation:Runtime/ElevationToRoot

Proses yang berjalan pada EC2 instans atau penampung Amazon yang terdaftar telah mengasumsikan hak akses root.

Tingkat keparahan default: Sedang



- Fitur: Pemantauan Runtime

Temuan ini memberi tahu Anda bahwa proses yang berjalan di Amazon yang terdaftar EC2 atau dalam wadah yang terdaftar di AWS lingkungan Anda telah mengasumsikan hak akses root melalui eksekusi biner yang tidak biasa atau mencurigakansetuid. Ini menunjukkan bahwa proses yang sedang berjalan berpotensi dikompromikan, EC2 misalnya melalui eksploitasi, atau melalui setuid eksploitasi. Dengan menggunakan hak akses root, penyerang berpotensi mengeksekusi perintah pada instance atau container.

Meskipun GuardDuty dirancang untuk tidak menghasilkan jenis temuan ini untuk aktivitas yang melibatkan penggunaan sudo perintah secara teratur, itu akan menghasilkan temuan ini ketika mengidentifikasi aktivitas sebagai tidak biasa atau mencurigakan.

GuardDuty memeriksa aktivitas dan konteks runtime terkait, dan menghasilkan jenis temuan ini hanya jika aktivitas dan konteks terkait tidak biasa atau mencurigakan.

Agan runtime memantau peristiwa dari berbagai sumber daya. Untuk mengidentifikasi sumber daya yang terpengaruh, lihat Jenis sumber daya dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, sumber daya Anda mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Remediasi temuan Runtime Monitoring](#).

## Perlindungan Malware untuk jenis pencarian EC2

GuardDuty Perlindungan Malware untuk EC2 menyediakan Perlindungan Malware tunggal untuk penemuan EC2 untuk semua ancaman yang terdeteksi selama pemindaian instans EC2 atau beban kerja kontainer. Temuan ini mencakup jumlah total deteksi yang dilakukan selama pemindaian, dan berdasarkan tingkat keparahannya, memberikan rincian untuk 32 ancaman teratas yang dideteksi. Tidak seperti GuardDuty temuan lain, Perlindungan Malware untuk temuan EC2 tidak diperbarui ketika instans EC2 atau beban kerja kontainer yang sama dipindai lagi.

Perlindungan Malware baru untuk temuan EC2 dihasilkan untuk setiap pemindaian yang mendeteksi malware. Perlindungan Malware untuk temuan EC2 mencakup informasi tentang pemindaian yang sesuai yang menghasilkan temuan serta GuardDuty temuan yang memulai pemindaian ini. Ini membuatnya lebih mudah untuk menghubungkan perilaku mencurigakan dengan malware yang terdeteksi.

**Note**

Saat GuardDuty mendeteksi aktivitas berbahaya pada beban kerja kontainer, Perlindungan Malware untuk EC2 tidak menghasilkan temuan tingkat EC2.

Temuan berikut khusus untuk Perlindungan GuardDuty Malware untuk EC2.

## Topik

- [Execution:EC2/MaliciousFile](#)
- [Execution:ECS/MaliciousFile](#)
- [Execution:Kubernetes/MaliciousFile](#)
- [Execution:Container/MaliciousFile](#)
- [Execution:EC2/SuspiciousFile](#)
- [Execution:ECS/SuspiciousFile](#)
- [Execution:Kubernetes/SuspiciousFile](#)
- [Execution:Container/SuspiciousFile](#)

## Execution:EC2/MaliciousFile

File berbahaya telah terdeteksi pada instans EC2.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada instans EC2 yang terdaftar di lingkungan Anda AWS . Contoh yang terdaftar ini mungkin dikompromikan. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Execution:ECS/MaliciousFile

File berbahaya telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik klaster ECS dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan cluster yang berpotensi dikompromikan ECS](#).

## Execution:Kubernetes/MaliciousFile

File berbahaya telah terdeteksi di klaster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer milik cluster Kubernetes. Jika ini adalah cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang sumber daya EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Execution:Container/MaliciousFile

File berbahaya telah terdeteksi pada wadah mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file berbahaya pada beban kerja kontainer dan tidak ada informasi cluster yang diidentifikasi. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).

## Execution:EC2/SuspiciousFile

File mencurigakan telah terdeteksi pada instans EC2.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada instans EC2. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

SuspiciousFileDeteksi jenis menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Execution:ECS/SuspiciousFile

File mencurigakan telah terdeteksi pada cluster ECS.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster ECS. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

`SuspiciousFile` jenis deteksi menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kontainer milik klaster ECS dapat dikompromikan. Untuk informasi selengkapnya, lihat [Memulihkan cluster yang berpotensi dikompromikan ECS](#).

## Execution:Kubernetes/SuspiciousFile

Sebuah file mencurigakan telah terdeteksi pada klaster Kubernetes.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah milik cluster Kubernetes. Jika ini adalah

cluster yang dikelola EKS, detail temuan akan memberikan informasi tambahan tentang EKS yang terkena dampak. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

`SuspiciousFile` jenis deteksi menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memediasi temuan Pemantauan Log Audit EKS](#).

## Execution:Container/SuspiciousFile

File mencurigakan telah terdeteksi pada wadah mandiri.

Tingkat keparahan default: Bervariasi tergantung pada ancaman yang terdeteksi.

- Fitur: Perlindungan Malware EBS

Temuan ini menunjukkan bahwa Perlindungan GuardDuty Malware untuk pemindaian EC2 telah mendeteksi satu atau lebih file mencurigakan pada wadah tanpa informasi cluster. Untuk informasi selengkapnya, lihat bagian Terdeteksi ancaman di detail temuan.

`SuspiciousFile` jenis deteksi menunjukkan bahwa program yang berpotensi tidak diinginkan seperti adware, spyware, atau alat penggunaan ganda hadir pada sumber daya yang terkena dampak. Program-program ini dapat berdampak negatif pada sumber daya Anda, atau digunakan oleh penyerang untuk tujuan jahat. Misalnya, alat jaringan dapat digunakan secara sah atau jahat oleh musuh sebagai alat hack untuk mencoba dan mengkompromikan sumber daya.

Ketika file mencurigakan telah terdeteksi, evaluasi apakah Anda berharap untuk melihat file yang terdeteksi di AWS lingkungan Anda. Jika file tidak terduga, ikuti rekomendasi remediasi yang disediakan di bagian selanjutnya.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, beban kerja kontainer Anda mungkin terganggu. Untuk informasi selengkapnya, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).

## Perlindungan Malware untuk tipe pencarian S3

GuardDuty menghasilkan temuan hanya ketika mendeteksi potensi ancaman keamanan di Anda Akun AWS. Perlindungan Malware untuk temuan S3 menunjukkan bahwa objek yang diunggah yang memulai pemindaian malware berisi file yang berpotensi berbahaya.

GuardDuty Agar Amazon dapat menghasilkan temuan di Anda Akun AWS, aktifkan keduanya GuardDuty dan Perlindungan Malware untuk S3. Praktik terbaik adalah mengaktifkan terlebih dahulu GuardDuty dan kemudian Perlindungan Malware untuk S3. Jika pesanan ini berbeda untuk Anda, pastikan untuk mengaktifkan GuardDuty sebelum objek S3 diunggah ke bucket Anda yang dilindungi.

### Note

GuardDuty tidak dapat menghasilkan temuan untuk objek S3 yang dipindai sebelum Anda mengaktifkan. GuardDuty Untuk memindai objek S3 yang ada, Anda dapat mengunggahnya lagi.

## Object:S3/MaliciousFile

File berbahaya telah terdeteksi pada objek S3 yang dipindai.

Tingkat keparahan default: Tinggi

- Fitur: Perlindungan Malware untuk S3

Temuan ini menunjukkan bahwa pemindaian malware telah mendeteksi objek S3 yang terdaftar sebagai berbahaya. Untuk informasi selengkapnya, lihat bagian Ancaman terdeteksi di panel rincian pencarian.

## Remediasi rekomendasi:

Jika temuan ini tidak terduga, objek S3 berpotensi berbahaya. Untuk informasi tentang langkah-langkah remediasi yang direkomendasikan, lihat [Memperbaiki objek S3 yang berpotensi berbahaya](#).

## GuardDutyJenis temuan Perlindungan RDS

GuardDutyRDS Protection mendeteksi perilaku login anomali pada instance database Anda. Temuan berikut ini khusus untuk [Basis data Amazon Aurora dan Amazon yang didukung RDS](#) dan akan memiliki Jenis Sumber DayadariRDSDBInstance. Tingkat keparahan dan detail temuan akan berbeda berdasarkan jenis temuan.

### Topik

- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.FailedLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce](#)
- [CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/MaliciousIPCaller.FailedLogin](#)
- [Discovery:RDS/MaliciousIPCaller](#)
- [CredentialAccess:RDS/TorIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/TorIPCaller.FailedLogin](#)
- [Discovery:RDS/TorIPCaller](#)

### CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Seorang pengguna berhasil login ke database RDS di akun Anda dengan cara yang anomali.

Tingkat keparahan default: Variabel

#### Note

Bergantung pada perilaku anomali yang terkait dengan temuan ini, tingkat keparahan default dapat Rendah, Sedang, dan Tinggi.

- Rendah- Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP yang dikaitkan dengan jaringan pribadi.
- Sedang- Jika nama pengguna yang terkait dengan temuan ini masuk dari alamat IP publik.
- Tinggi- Jika ada pola yang konsisten dari upaya login gagal dari alamat IP publik yang menunjukkan kebijakan akses yang terlalu permisif.



- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa login sukses anomali diamati pada database RDS di AndaAWSlingkungan. Ini mungkin menunjukkan bahwa pengguna tak terlihat sebelumnya login ke database RDS untuk pertama kalinya. Skenario umum adalah pengguna internal yang masuk ke database yang diakses secara terprogram oleh aplikasi dan bukan oleh pengguna individu.

Login yang berhasil ini diidentifikasi sebagai anomali olehGuardDutymodel pembelajaran mesin deteksi anomali (ML). Model MLmengevaluasi semua peristiwa login database di[Basis data Amazon Aurora dan Amazon yang didukung RDS](#)dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model MLmelacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang peristiwa login yang berpotensi tidak biasa, lihat[RDSanomali berbasis aktivitas login](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, disarankan untuk mengubah sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna anomali. Temuan tingkat keparahan sedang dan tinggi dapat mengindikasikan bahwa ada kebijakan akses yang terlalu permisif ke database, dan kredensi pengguna mungkin telah terungkap atau disusupi. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

## CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Satu atau lebih upaya login gagal yang tidak biasa diamati pada database RDS di akun Anda.

Tingkat keparahan default: Rendah

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa satu atau lebih login gagal anomali diamati pada database RDS di AndaAWSlingkungan. Upaya login yang gagal dari alamat IP publik dapat menunjukkan

bahwa database RDS di akun Anda telah mengalami percobaan serangan brute force oleh aktor yang berpotensi jahat.

Login yang gagal ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua peristiwa login database di [Basis data Amazon Aurora dan Amazon yang didukung RDS](#) dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Model ML melacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihat [RDS anomali berbasis aktivitas login](#).

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa database diekspos secara publik atau ada kebijakan akses yang terlalu permisif ke database. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

## CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Seorang pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP publik dengan cara yang anomali setelah pola yang konsisten dari upaya login gagal yang tidak biasa.

Tingkat keparahan default: Tinggi

- Fitur: Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa indikatif login anomali dari brute force yang berhasil diamati pada database RDS di Anda AWS lingkungan. Sebelum login berhasil anomali, pola konsisten dari upaya login gagal yang tidak biasa diamati. Ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan database RDS di akun Anda mungkin telah disusupi, dan database RDS mungkin telah diakses oleh aktor yang berpotensi jahat.

Login brute force yang berhasil ini diidentifikasi sebagai anomali oleh GuardDuty model pembelajaran mesin deteksi anomali (ML). Model ML mengevaluasi semua peristiwa login database di [Basis data Amazon Aurora dan Amazon yang didukung RDS](#) dan mengidentifikasi peristiwa anomali yang terkait

dengan teknik yang digunakan oleh musuh. Model MLmelacak berbagai faktor aktivitas login RDS seperti pengguna yang membuat permintaan, lokasi permintaan dibuat, dan detail koneksi database spesifik yang digunakan. Untuk informasi tentang aktivitas login RDS yang berpotensi tidak biasa, lihat [RDSanomali berbasis aktivitas login](#).

Rekomendasi remediasi:

Aktivitas ini menunjukkan bahwa kredensi database mungkin telah diekspos atau disusupi. Dianjurkan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang berpotensi disusupi. Pola yang konsisten dari upaya login gagal yang tidak biasa menunjukkan kebijakan akses yang terlalu permisif ke database atau database mungkin juga telah diekspos publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

## CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP berbahaya yang diketahui.

Tingkat keparahan default: Tinggi

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa aktivitas login RDS yang berhasil terjadi dari alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui di AndaAWSlingkungan. Ini menunjukkan bahwa pengguna dan kata sandi yang terkait dengan database RDS di akun Anda mungkin telah disusupi, dan database RDS mungkin telah diakses oleh aktor yang berpotensi jahat.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, aktivitas ini mungkin menunjukkan bahwa kredensi pengguna mungkin telah diekspos atau disusupi. Dianjurkan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas

hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

## CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui gagal mencoba masuk ke database RDS di akun Anda.

Tingkat keparahan default: Sedang

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui mencoba masuk ke database RDS di database AndaAWSlingkungan, tetapi gagal memberikan nama pengguna atau kata sandi yang benar. Ini menunjukkan bahwa aktor yang berpotensi jahat mungkin mencoba untuk membahayakan database RDS di akun Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

## Discovery:RDS/MaliciousIPCaller

Alamat IP yang dikaitkan dengan aktivitas berbahaya yang diketahui memeriksa database RDS di akun Anda; tidak ada upaya otentikasi yang dilakukan.

Tingkat keparahan default: Sedang

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP yang terkait dengan aktivitas berbahaya yang diketahui memeriksa database RDS di AndaAWSlingkungan, meskipun tidak ada upaya login yang dilakukan. Ini mungkin menunjukkan bahwa aktor yang berpotensi jahat sedang mencoba memindai infrastruktur yang dapat diakses publik.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

## CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Seorang pengguna berhasil masuk ke database RDS di akun Anda dari alamat IP node keluar Tor.

Tingkat keparahan default: Tinggi

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa pengguna berhasil masuk ke database RDS di AndaAWSlingkungan, dari alamat IP node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, aktivitas ini mungkin menunjukkan bahwa kredensi pengguna mungkin telah diekspos atau disusupi. Dianjurkan untuk mengubah kata sandi pengguna database terkait, dan meninjau log audit yang tersedia untuk aktivitas yang dilakukan oleh pengguna yang disusupi. Aktivitas ini juga dapat menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#).

## CredentialAccess:RDS/TorIPCaller.FailedLogin

Alamat IP Tor berusaha untuk tidak berhasil masuk ke database RDS di akun Anda.

Tingkat keparahan default: Sedang

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor mencoba masuk ke database RDS diAWSlingkungan, tetapi gagal memberikan nama pengguna atau kata sandi yang benar. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Hal ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli pengguna anonim.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

## Discovery:RDS/TorIPCaller

Alamat IP node keluar Tor memeriksa database RDS di akun Anda, tidak ada upaya otentikasi yang dilakukan.

Tingkat keparahan default: Sedang

- Fitur:Pemantauan aktivitas login RDS

Temuan ini memberi tahu Anda bahwa alamat IP node keluar Tor menyelidiki database RDS di AndaAWSlingkungan, meskipun tidak ada upaya login yang dilakukan. Ini mungkin menunjukkan bahwa aktor yang berpotensi jahat sedang mencoba memindai infrastruktur yang dapat diakses publik. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak memantul komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai nod keluar. Ini dapat menunjukkan akses tidak sah ke sumber daya RDS di akun Anda, dengan maksud menyembunyikan identitas asli aktor yang berpotensi jahat.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk database terkait, ini mungkin menunjukkan bahwa ada kebijakan akses yang terlalu permisif ke database atau database diekspos secara publik. Disarankan untuk menempatkan database di VPC pribadi, dan membatasi aturan grup keamanan untuk memungkinkan lalu lintas hanya dari sumber yang diperlukan. Untuk informasi selengkapnya, lihat [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#).

## Tipe temuan Lambda Protection

Bagian ini menjelaskan jenis temuan yang spesifik untuk AWS Lambda sumber daya Anda dan memiliki `resourceType` terdaftar sebagai Lambda. Untuk semua temuan Lambda, kami menyarankan Anda memeriksa sumber daya yang bersangkutan dan menentukan apakah sumber daya tersebut berperilaku seperti dengan yang diharapkan. Jika aktivitas diotorisasi, Anda dapat menggunakan [aturan Penekanan](#) atau [IP Tepercaya dan daftar ancaman](#) untuk mencegah notifikasi positif palsu untuk sumber daya tersebut.

Jika aktivitas tidak terduga, praktik keamanan terbaik adalah menganggap bahwa Lambda berpotensi disusupi dan mengikuti rekomendasi remediasi.

### Topik

- [Backdoor:Lambda/C&CActivity.B](#)
- [CryptoCurrency:Lambda/BitcoinTool.B](#)
- [Trojan:Lambda/BlackholeTraffic](#)
- [Trojan:Lambda/DropPoint](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:Lambda/TorClient](#)
- [UnauthorizedAccess:Lambda/TorRelay](#)

## Backdoor:Lambda/C&CActivity.B

Fungsi Lambda menanyakan alamat IP yang terkait dengan server perintah dan kontrol yang dikenal.

Tingkat kepelikan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda yang terdaftar dalam AWS lingkungan Anda menanyakan alamat IP yang terkait dengan server perintah dan kontrol (C&C) yang dikenal. Fungsi Lambda yang terkait dengan temuan yang dihasilkan berpotensi dikompromikan. Server C&C adalah komputer yang mengeluarkan perintah untuk anggota botnet.

Botnet adalah kumpulan perangkat yang terhubung ke internet, yang mungkin termasuk PC, server, perangkat seluler, dan perangkat Internet of Things, yang terinfeksi dan dikendalikan oleh tipe malware yang umum. Botnet sering digunakan untuk mendistribusikan malware dan mengumpulkan informasi yang disalahgunakan, seperti nomor kartu kredit. Tergantung tujuan dan struktur botnet, server C&C mungkin juga mengeluarkan perintah untuk memulai denial of service yang terdistribusi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## CryptoCurrency:Lambda/BitcoinTool.B

Fungsi Lambda menanyakan alamat IP yang terkait dengan aktivitas mata uang kripto.

Tingkat kepelikan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda yang tercantum dalam AWS lingkungan Anda menanyakan alamat IP yang terkait dengan Bitcoin atau aktivitas mata uang kripto lainnya. Pelaku ancaman dapat berusaha untuk mengambil kendali atas fungsi Lambda untuk menggunakan kembali mereka dengan jahat untuk penambangan cryptocurrency yang tidak sah.

Rekomendasi remediasi:

Jika Anda menggunakan fungsi Lambda ini untuk menambang atau mengelola mata uang kripto, atau jika fungsi ini terlibat dalam aktivitas blockchain, aktivitas ini berpotensi menjadi aktivitas yang diharapkan untuk lingkungan Anda. Jika hal ini dilakukan di lingkungan AWS Anda, kami menyarankan Anda untuk mengatur aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut tipe temuan dengan nilai CryptoCurrency:Lambda/BitcoinTool.B. Kriteria filter kedua harus menggunakan nama fungsi Lambda dari fungsi yang terlibat dalam aktivitas blockchain. Untuk informasi tentang cara membuat aturan penekanan, lihat [Aturan penekanan](#).



Jika aktivitas ini tidak terduga, fungsi Lambda Anda berpotensi disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## Trojan:Lambda/BlackholeTraffic

Fungsi Lambda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang dikenal sebagai black hole.

Tingkat kepelikan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda yang terdaftar dalam AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP dari black hole (atau wastafel). Lubang hitam adalah tempat di jaringan di mana lalu lintas masuk atau keluar dibuang secara diam-diam tanpa memberi tahu sumber bahwa data tidak mencapai penerima yang dimaksudkan. Alamat IP lubang hitam menentukan mesin host yang tidak berjalan atau alamat yang tidak ada host telah ditetapkan. Fungsi Lambda yang terdaftar berpotensi dikompromikan.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## Trojan:Lambda/DropPoint

Fungsi Lambda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Tingkat kepelikan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda yang terdaftar dalam AWS lingkungan Anda mencoba berkomunikasi dengan alamat IP dari host jarak jauh yang diketahui menyimpan kredensial dan data curian lainnya yang ditangkap oleh malware.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Fungsi Lambda membuat koneksi ke alamat IP pada daftar ancaman kustom.

Tingkat kepelikan default: Medium

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda dalam AWS lingkungan Anda berkomunikasi dengan alamat IP yang termasuk dalam daftar ancaman yang Anda unggah. Di GuardDuty, [daftar ancaman](#) terdiri dari alamat IP berbahaya yang diketahui. GuardDuty menghasilkan temuan berdasarkan daftar ancaman yang diunggah. Anda dapat melihat detail daftar ancaman dalam detail temuan di GuardDuty konsol.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## UnauthorizedAccess:Lambda/TorClient

Fungsi Lambda membuat koneksi ke Tor Guard atau node Authority.

Tingkat kepelikan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda dalam AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Node Tor Guards dan Authority bertindak sebagai gateway awal ke dalam jaringan Tor. Lalu lintas ini dapat menunjukkan bahwa fungsi Lambda ini berpotensi dikompromikan. Sekarang bertindak sebagai klien pada jaringan Tor.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## UnauthorizedAccess:Lambda/TorRelay

Fungsi Lambda membuat koneksi ke jaringan Tor sebagai relay Tor.

Tingkat kepelikan default: Tinggi

- Fitur: Pemantauan Aktivitas Jaringan Lambda

Temuan ini menginformasikan bahwa fungsi Lambda dalam AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang mengindikasikan bahwa fungsi ini bertindak sebagai relay Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Tor memungkinkan komunikasi anonim dengan meneruskan lalu lintas klien yang berpotensi terlarang dari satu relay Tor ke relay lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, fungsi Lambda Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#).

## Tipe temuan yang sudah dihentikan

Temuan adalah notifikasi yang berisi detail tentang potensi masalah keamanan yang GuardDuty ditemukan. Untuk informasi tentang perubahan penting pada tipe GuardDuty temuan, termasuk tipe temuan yang baru ditambahkan atau yang sudah dihentikan, lihat [Riwayat dokumen untuk Amazon GuardDuty](#).

Jenis temuan berikut ini pensiun dan tidak lagi dihasilkan oleh GuardDuty.

### Important

Anda tidak dapat mengaktifkan kembali jenis GuardDuty penemuan pensiunan.

Topik

- [Exfiltration:S3/ObjectRead.Unusual](#)
- [Impact:S3/PermissionsModification.Unusual](#)
- [Impact:S3/ObjectDelete.Unusual](#)
- [Discovery:S3/BucketEnumeration.Unusual](#)
- [Persistence:IAMUser/NetworkPermissions](#)
- [Persistence:IAMUser/ResourcePermissions](#)
- [Persistence:IAMUser/UserPermissions](#)
- [PrivilegeEscalation:IAMUser/AdministrativePermissions](#)
- [Recon:IAMUser/NetworkPermissions](#)
- [Recon:IAMUser/ResourcePermissions](#)
- [Recon:IAMUser/UserPermissions](#)
- [ResourceConsumption:IAMUser/ComputeResources](#)
- [Stealth:IAMUser/LoggingConfigurationModified](#)
- [UnauthorizedAccess:IAMUser/ConsoleLogin](#)
- [UnauthorizedAccess:EC2/TorIPCaller](#)
- [Backdoor:EC2/XORDDOS](#)
- [Behavior:IAMUser/InstanceLaunchUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.A](#)
- [UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

## Exfiltration:S3/ObjectRead.Unusual

Entitas IAM memanggil API S3 dengan cara yang mencurigakan.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

- Sumber data: peristiwaCloudTrail data untuk S3

Temuan ini menginformasikan bahwa entitas IAM di lingkungan AWS Anda membuat panggilan API yang melibatkan bucket S3 dan berbeda dari garis dasar yang ditetapkan oleh entitas tersebut. Panggilan API yang digunakan dalam aktivitas ini dikaitkan dengan tahap eksfiltrasi serangan, ketika penyerang sedang mencoba untuk mengumpulkan data. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, hal ini mungkin menunjukkan bahwa kredensial telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Impact:S3/PermissionsModification.Unusual

Entitas IAM memanggil API untuk mengubah izin pada satu sumber daya S3 atau lebih.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini menginformasikan bahwa entitas IAM membuat panggilan API yang dirancang untuk mengubah izin pada satu atau lebih bucket atau objek di lingkungan AWS Anda. Tindakan ini dapat dilakukan oleh penyerang untuk memungkinkan informasi dibagikan di luar akun. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, hal ini mungkin menunjukkan bahwa kredensial telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Impact:S3/ObjectDelete.Unusual

Entitas IAM memanggil API yang digunakan untuk menghapus data dalam bucket S3.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini menginformasikan bahwa entitas IAM tertentu di lingkungan AWS Anda membuat panggilan API yang bertujuan untuk menghapus data dalam bucket S3 yang terdaftar dengan cara menghapus bucket itu sendiri. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, hal ini mungkin menunjukkan bahwa kredensial telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Discovery:S3/BucketEnumeration.Unusual

Entitas IAM memanggil API S3 yang digunakan untuk menemukan bucket S3 dalam jaringan Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

**Note**

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini menginformasikan bahwa entitas IAM telah memanggil API S3 untuk menemukan bucket S3 dalam lingkungan Anda, seperti `ListBuckets`. Tipe aktivitas ini berkaitan dengan tahap penemuan serangan ketika musuh mengumpulkan informasi untuk menentukan apakah lingkungan AWS Anda rentan terhadap serangan yang lebih luas. Aktivitas ini mencurigakan karena cara entitas IAM memanggil API tidak biasa. Misalnya, entitas IAM ini sebelumnya tidak memiliki riwayat memanggil tipe API ini, atau API dipanggil dari lokasi yang tidak biasa.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga untuk prinsipal terkait, hal ini mungkin menunjukkan bahwa kredensial telah terekspos atau izin S3 Anda tidak cukup ketat. Untuk informasi selengkapnya, lihat [Memulihkan bucket S3 yang berpotensi dikompromikan](#).

## Persistence:IAMUser/NetworkPermissions

Entitas IAM memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACL di akun AWS Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

**Note**

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini mengindikasikan bahwa prinsipal tertentu (Pengguna root akun AWSIAM role, atau pengguna) diAWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika pengaturan konfigurasi jaringan berubah dalam keadaan yang mencurigakan, seperti ketika prinsipal memanggil API `CreateSecurityGroup` tanpa riwayat sebelumnya. Penyerang sering mencoba untuk mengubah grup keamanan untuk memungkinkan lalu lintas masuk tertentu pada berbagai port untuk meningkatkan kemampuannya untuk mengakses instans EC2.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Persistence:IAMUser/ResourcePermissions

Prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan dari berbagai sumber daya di AndaAkun AWS.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini mengindikasikan bahwa prinsipal tertentu (Pengguna root akun AWSIAM role, atau pengguna) diAWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika perubahan terdeteksi pada kebijakan atau izin yang melekat pada sumber daya AWS, seperti ketika prinsipal dalam lingkungan AWS Anda memanggil API `PutBucketPolicy` tanpa riwayat sebelumnya. Beberapa layanan, seperti Amazon S3, mendukung izin yang melekat pada sumber daya yang memberikan satu akses utama atau lebih ke sumber daya. Dengan kredensial curian, penyerang dapat mengubah kebijakan yang melekat pada sumber daya untuk memperoleh akses ke sumber daya tersebut.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).



## Persistence:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, mengubah, atau menghapus pengguna, grup, atau kebijakan IAM di akun AWS Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini mengindikasikan bahwa prinsipal tertentu (Pengguna root akun AWS IAM role, atau pengguna) di AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu oleh perubahan yang mencurigakan pada izin terkait pengguna dalam lingkungan AWS Anda, seperti ketika prinsipal dalam lingkungan AWS Anda memanggil API `AttachUserPolicy` tanpa riwayat sebelumnya. Penyerang dapat menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun, bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa pengguna atau kata sandi IAM tertentu telah dicuri dan menghapusnya dari akun. Namun, mereka mungkin tidak menghapus pengguna lain yang dibuat oleh prinsipal admin yang dibuat secara curang, sehingga akun AWS mereka dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## PrivilegeEscalation:IAMUser/AdministrativePermissions

Prinsipal telah berusaha untuk menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri.

## Tingkat kepelikan default Rendah\* Rendah

### Note

Tingkat kepelikan temuan ini Rendah jika upaya eskalasi hak istimewa tidak berhasil, dan Medium jika upaya eskalasi hak istimewa berhasil.

Temuan ini mengindikasikan bahwa entitas IAM tertentu dalam lingkungan AWS Anda menunjukkan perilaku yang mengindikasikan serangan eskalasi hak istimewa. Temuan ini dipicu ketika pengguna atau IAM role mencoba untuk menetapkan kebijakan yang sangat permisif untuk diri mereka sendiri. Jika pengguna atau peran yang dimaksud tidak dimaksudkan untuk memiliki hak administratif, kredensial pengguna dapat disusupi atau izin peran mungkin tidak dikonfigurasi dengan benar.

Penyerang akan menggunakan kredensial curian untuk membuat pengguna baru, menambahkan kebijakan akses ke pengguna yang ada, atau membuat kunci akses untuk memaksimalkan akses mereka ke akun bahkan jika titik akses asli mereka ditutup. Misalnya, pemilik akun mungkin memperhatikan bahwa kredensial pengguna IAM tertentu dicuri dan menghapusnya dari akun, tetapi mungkin tidak menghapus pengguna lain yang dibuat oleh kepala admin yang dibuat secara curang, sehingga AWS akun mereka masih dapat diakses oleh penyerang.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/NetworkPermissions

Prinsipal memanggil API yang biasa digunakan untuk mengubah izin akses jaringan untuk grup keamanan, rute, dan ACL di akun AWS Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini mengindikasikan bahwa prinsipal tertentu (Pengguna root akun AWSIAM role, atau pengguna) diAWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat sebelumnya. Penyerang mungkin menggunakan kredensial curian untuk melakukan tipe pengintaian ini terhadap sumber daya AWS Anda untuk memperoleh kredensial yang lebih berharga atau menentukan kemampuan kredensial yang telah mereka miliki.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/ResourcePermissions

Prinsipal memanggil API yang biasa digunakan untuk mengubah kebijakan akses keamanan dari berbagai sumber daya di akun AWS Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini mengindikasikan bahwa prinsipal tertentu (Pengguna root akun AWSIAM role, atau pengguna) diAWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini.

Temuan ini dipicu ketika izin akses sumber daya di akun AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal memanggil API `DescribeInstances` tanpa riwayat sebelumnya. Penyerang mungkin menggunakan kredensial curian untuk melakukan tipe pengintaian ini terhadap sumber daya AWS Anda untuk memperoleh kredensial yang lebih berharga atau menentukan kemampuan kredensial yang telah mereka miliki.

## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Recon:IAMUser/UserPermissions

Prinsipal memanggil API yang biasa digunakan untuk menambah, mengubah, atau menghapus pengguna, grup, atau kebijakan IAM di akun AWS Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini dipicu ketika izin pengguna dalam lingkungan AWS Anda diperiksa dalam keadaan yang mencurigakan. Misalnya, jika prinsipal (Pengguna root akun AWS IAM role, atau pengguna IAM) memanggil `ListInstanceProfilesForRole` API tanpa riwayat sebelumnya. Penyerang mungkin menggunakan kredensial curian untuk melakukan tipe pengintaian ini terhadap sumber daya AWS Anda untuk memperoleh kredensial yang lebih berharga atau menentukan kemampuan kredensial yang telah mereka miliki.

Temuan ini mengindikasikan bahwa prinsipal tertentu dalam lingkungan AWS Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini sebelumnya tidak memiliki riwayat memanggil API ini dengan cara ini.


## Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## ResourceConsumption:IAMUser/ComputeResources

Prinsipal memanggil API yang biasa digunakan untuk meluncurkan sumber daya komputasi seperti instans EC2.

Medium\* Medium\* Medium\* Medium\* Medium\*

 Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini dipicu ketika instans EC2 di akun yang terdaftar dalam lingkungan AWS Anda diluncurkan dalam keadaan yang mencurigakan. Temuan ini mengindikasikan bahwa prinsipal tertentu dalam AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan; misalnya, jika prinsipal (Pengguna root akun AWS IAM role, atau pengguna IAM) memanggil `RunInstances` API tanpa riwayat sebelumnya. Ini mungkin merupakan indikasi penyerang menggunakan kredensial curian untuk mencuri waktu komputasi (mungkin untuk penambangan mata uang kripto atau peretasan kata sandi). Hal ini juga dapat menjadi indikasi penyerang menggunakan instans EC2 dalam lingkungan AWS Anda dan kredensialnya untuk mempertahankan akses ke akun Anda.


Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## Stealth:IAMUser/LoggingConfigurationModified

Prinsipal memanggil API yang biasa digunakan untuk menghentikan CloudTrail Pencatatan, menghapus log yang ada, dan menghilangkan jejak aktivitas di AWS akun Anda.

Medium\* Medium\* Medium\* Medium\* Medium\*

 Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini dipicu ketika konfigurasi pencatatan log di akun AWS yang terdaftar dalam lingkungan Anda diubah dalam keadaan yang mencurigakan. Temuan ini menginformasikan bahwa prinsipal tertentu dalam AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan; misalnya, jika prinsipal (Pengguna root akun AWS IAM role, atau pengguna IAM) memanggil `StopLogging` API tanpa riwayat sebelumnya. Ini bisa menjadi indikasi penyerang yang mencoba menutupi jejak mereka dengan menghilangkan jejak aktivitas mereka.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:IAMUser/ConsoleLogin

Login konsol yang tidak biasa oleh prinsipal di akun AWS Anda diamati.

Medium\* Medium\* Medium\* Medium\* Medium\*

### Note

Tingkat kepelikan default temuan ini adalah Medium. Namun, jika API dipanggil menggunakan kredensial AWS sementara yang dibuat pada instans, tingkat kepelikan temuan Tinggi.

Temuan ini dipicu ketika login konsol terdeteksi dalam keadaan yang mencurigakan. Misalnya, jika prinsipal tanpa riwayat sebelumnya, memanggil `ConsoleLogin` API dari never-before-used klien atau lokasi yang tidak biasa. Ini bisa menjadi indikasi kredensial curian yang digunakan untuk memperoleh akses ke akun AWS Anda, atau pengguna valid yang mengakses akun dengan cara yang tidak valid atau kurang aman (misalnya, bukan melalui VPN yang disetujui).

Temuan ini menginformasikan bahwa prinsipal tertentu dalam lingkungan AWS Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Prinsipal ini tidak memiliki riwayat aktivitas login sebelumnya menggunakan aplikasi klien ini dari lokasi spesifik ini.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## UnauthorizedAccess:EC2/TorIPCaller

Instans EC2 Anda menerima koneksi masuk dari node keluar Tor.

Medium default Medium Medium Medium Medium

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda menerima koneksi masuk dari node keluar Tor. Tor adalah perangkat lunak untuk memungkinkan komunikasi anonim. Ini mengenkripsi dan secara acak mengalihkan komunikasi melalui relay antara serangkaian node jaringan. Node Tor terakhir disebut sebagai node keluar. Temuan ini mungkin mengindikasikan akses yang tidak sah ke sumber daya AWS Anda yang bertujuan untuk menyembunyikan identitas penyerang yang sebenarnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Backdoor:EC2/XORDDOS

Instans EC2 mencoba untuk berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS.

Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi

Temuan ini menginformasikan bahwa instans EC2 diAWS lingkungan Anda mencoba untuk berkomunikasi dengan alamat IP yang terkait dengan malware XOR DDoS. Instans EC2 ini mungkin disusupi. XOR DDoS adalah malware Trojan yang membajak sistem Linux. Untuk mendapatkan akses ke sistem, malware ini meluncurkan serangan brute force untuk memperoleh kata sandi ke layanan Secure Shell (SSH) di Linux. Setelah kredensial SSH diperoleh dan login berhasil, ia menggunakan hak akses pengguna akar untuk menjalankan skrip yang mengunduh dan menginstal XOR DDoS. Malware ini kemudian digunakan sebagai bagian dari botnet untuk meluncurkan serangan denial of service (DDoS) yang terdistribusi terhadap target lainnya.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## Behavior:IAMUser/InstanceLaunchUnusual

Pengguna meluncurkan instans EC2 dari tipe yang tidak biasa.

Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi

Temuan ini menginformasikan bahwa pengguna tertentu dalam AWS lingkungan Anda menunjukkan perilaku yang berbeda dari garis dasar yang ditetapkan. Pengguna ini sebelumnya tidak memiliki riwayat meluncurkan instans EC2 tipe ini. Kredensial masuk Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).

## CryptoCurrency:EC2/BitcoinTool.A

Instans EC2 berkomunikasi dengan kolam penambangan Bitcoin.

Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi

Temuan ini menginformasikan bahwa instans EC2 dalam lingkungan AWS Anda berkomunikasi dengan kolam penambangan Bitcoin. Di bidang penambangan mata uang kripto, kolam penambangan adalah kolam sumber daya penambang yang berbagi kekuatan pemrosesan mereka melalui jaringan untuk membagi hadiah sesuai dengan jumlah pekerjaan yang mereka kontribusikan untuk memecahkan blok. Kecuali Anda menggunakan instans EC2 ini untuk penambangan Bitcoin, instans EC2 Anda mungkin disusupi.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, instans Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).

## UnauthorizedAccess:IAMUser/UnusualASNCaller

API dipanggil dari alamat IP dari jaringan yang tidak biasa.

Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi Tinggi

Temuan ini menginformasikan bahwa aktivitas tertentu dipanggil dari alamat IP dari jaringan yang tidak biasa. Jaringan ini tidak pernah diamati di seluruh riwayat penggunaan AWS dari



pengguna yang dimaksud. Kegiatan ini dapat mencakup login konsol, upaya untuk meluncurkan instans EC2, membuat pengguna IAM baru, mengubah hak istimewa AWS Anda, dll. Hal ini dapat mengindikasikan akses yang tidak sah ke sumber daya AWS Anda.

Rekomendasi remediasi:

Jika aktivitas ini tidak terduga, kredensial Anda mungkin disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensial yang berpotensi dikompromikan AWS](#).

## Temuan berdasarkan tipe sumber daya

Halaman-halaman berikut dikategorikan berdasarkan jenis sumber daya yang terkait dengan GuardDuty temuan:

- [Tipe temuan EC2](#)
- [IAM menemukan jenis](#)
- [Tipe temuan S3](#)
- [EKS jenis pencarian log audit](#)
- [Jenis penemuan Runtime Monitoring](#)
- [Perlindungan Malware untuk jenis pencarian EC2](#)
- [Perlindungan Malware untuk tipe pencarian S3](#)
- [Jenis temuan Perlindungan RDS](#)
- [Tipe temuan Lambda Protection](#)

## Tabel temuan

Tabel berikut menunjukkan semua jenis temuan aktif yang diurutkan berdasarkan sumber atau fitur data dasar, sebagaimana berlaku. Beberapa jenis temuan berikut mungkin memiliki tingkat keparahan variabel, ditunjukkan dengan tanda bintang (\*). Untuk informasi tentang tingkat keparahan variabel dari jenis temuan, lihat deskripsi rinci dari jenis temuan tersebut.

| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar            | Menemukan tingkat keparahan |
|--|-------------------|------------------------------------|-----------------------------|
| <a href="#">Discovery:S3/AnomalousBehavior</a>         | Amazon S3         | CloudTrail peristiwa data untuk S3 | Rendah                      |
| <a href="#">Discovery:S3/MaliciousIPCaller</a>         | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Discovery:S3/MaliciousIPCaller.Custom</a>  | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Discovery:S3/TorIPCaller</a>               | Amazon S3         | CloudTrail peristiwa data untuk S3 | Sedang                      |
| <a href="#">Exfiltration:S3/AnomalousBehavior</a>      | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Exfiltration:S3/MaliciousIPCaller</a>      | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Impact:S3/AnomalousBehavior.Delete</a>     | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Impact:S3/AnomalousBehavior.Permission</a> | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">Impact:S3/Anomalous</a>                    | Amazon S3         | CloudTrail peristiwa data untuk S3 | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar            | Menemukan tingkat keparahan |
|---|-------------------|------------------------------------|-----------------------------|
| <a href="#">sBehavior</a><br><a href="#">.Write</a>             |                   |                                    |                             |
| <a href="#">Impact:S3</a><br><a href="#">/MaliciousIPCaller</a> | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">PenTest:S3/KaliLinux</a>                            | Amazon S3         | CloudTrail peristiwa data untuk S3 | Sedang                      |
| <a href="#">PenTest:S3/ParrotLinux</a>                          | Amazon S3         | CloudTrail peristiwa data untuk S3 | Sedang                      |
| <a href="#">PenTest:S3/PentoolLinux</a>                         | Amazon S3         | CloudTrail peristiwa data untuk S3 | Sedang                      |
| <a href="#">UnauthorizedAccess:S3/TorIPCaller</a>               | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">UnauthorizedAccess:S3/MaliciousIPCaller.Custom</a>  | Amazon S3         | CloudTrail peristiwa data untuk S3 | Tinggi                      |
| <a href="#">CredentialAccess:IAMUser/AnomalousBehavior</a>      | IAM               | CloudTrail manajemen acara         | Sedang                      |
| <a href="#">DefenseEvasion:IAMUser/AnomalousBehavior</a>        | IAM               | CloudTrail manajemen acara         | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar    | Menemukan tingkat keparahan |
|---|-------------------|----------------------------|-----------------------------|
| <a href="#">Discovery:IAMUser/AnomalousBehavior</a>     | IAM               | CloudTrail manajemen acara | Rendah                      |
| <a href="#">Exfiltration:IAMUser/AnomalousBehavior</a>  | IAM               | CloudTrail manajemen acara | Tinggi                      |
| <a href="#">Impact:IAMUser/AnomalousBehavior</a>        | IAM               | CloudTrail manajemen acara | Tinggi                      |
| <a href="#">InitialAccess:IAMUser/AnomalousBehavior</a> | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">PenTest:IAMUser/KaliLinux</a>               | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">PenTest:IAMUser/ParrrotLinux</a>            | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">PenTest:IAMUser/PentooLinux</a>             | IAM               | CloudTrail manajemen acara | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar    | Menemukan tingkat keparahan |
|---|-------------------|----------------------------|-----------------------------|
| <a href="#">Persisten ce:IAMUser/AnomalousBehavior</a>                              | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">Stealth:IAMUser/PasswordPolicyChange</a>                                | IAM               | CloudTrail manajemen acara | Rendah*                     |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS</a> | IAM               | CloudTrail manajemen acara | Tinggi*                     |
| <a href="#">Policy:S3/AccountBlockPublicAccessDisabled</a>                          | Amazon S3         | CloudTrail manajemen acara | Rendah                      |
| <a href="#">Policy:S3/BucketAnonymousAccessGranted</a>                              | Amazon S3         | CloudTrail manajemen acara | Tinggi                      |
| <a href="#">Policy:S3/BucketBlockPublicAccessDisabled</a>                           | Amazon S3         | CloudTrail manajemen acara | Rendah                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar    | Menemukan tingkat keparahan |
|---|-------------------|----------------------------|-----------------------------|
| <a href="#">Policy:S3/BucketPublicAccessGranted</a>           | Amazon S3         | CloudTrail manajemen acara | Tinggi                      |
| <a href="#">PrivilegeEscalation:IAMUser/AnomalousBehavior</a> | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">Recon:IAMUser/MaliciousIPCaller</a>               | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">Recon:IAMUser/MaliciousIPCaller.Custom</a>        | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">Recon:IAMUser/TorIPCaller</a>                     | IAM               | CloudTrail manajemen acara | Sedang                      |
| <a href="#">Stealth:IAMUser/CloudTrailLoggingDisabled</a>     | IAM               | CloudTrail manajemen acara | Rendah                      |
| <a href="#">Stealth:S3/ServerAccessLoggingDisabled</a>        | Amazon S3         | CloudTrail manajemen acara | Rendah                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar  | Menemukan tingkat keparahan |
|---|-------------------|--|-----------------------------|
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B</a>    | IAM               | CloudTrail manajemen acara   | Sedang                      |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller</a>        | IAM               | CloudTrail manajemen acara   | Sedang                      |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom</a> | IAM               | CloudTrail manajemen acara   | Sedang                      |
| <a href="#">UnauthorizedAccess:IAMUser/TorIPCaller</a>              | IAM               | CloudTrail manajemen acara   | Sedang                      |
| <a href="#">Policy:IAMUser/RootCredentialUsage</a>                  | IAM               | CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3 | Rendah                      |

| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar  | Menemukan tingkat keparahan |
|--|-------------------|--|-----------------------------|
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</a> | IAM               | CloudTrail peristiwa manajemen atau peristiwa CloudTrail data untuk S3 | Tinggi                      |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B!DNS</a>                                   | Amazon EC2        | DNSlog   | Tinggi                      |
| <a href="#">Cryptocurrency:EC2/BitcoinTool.B!DNS</a>                                 | Amazon EC2        | DNSlog   | Tinggi                      |
| <a href="#">Impact:EC2/AbusedDomainRequest.Reputation</a>                            | Amazon EC2        | DNSlog   | Sedang                      |
| <a href="#">Impact:EC2/BitcoinDomainRequest.Reputation</a>                           | Amazon EC2        | DNSlog   | Tinggi                      |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Reputation</a>                         | Amazon EC2        | DNSlog   | Tinggi                      |



| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">Impact:EC2/SuspiciousDomainRequest.Reputation</a> | Amazon EC2        | DNSlog                  | Rendah                      |
| <a href="#">Trojan:EC2/BlackholeTraffic!DNS</a>               | Amazon EC2        | DNSlog                  | Sedang                      |
| <a href="#">Trojan:EC2/DGADomainRequest.B</a>                 | Amazon EC2        | DNSlog                  | Tinggi                      |
| <a href="#">Trojan:EC2/DGADomainRequest.C!DNS</a>             | Amazon EC2        | DNSlog                  | Tinggi                      |
| <a href="#">Trojan:EC2/DNSDataExfiltration</a>                | Amazon EC2        | DNSlog                  | Tinggi                      |
| <a href="#">Trojan:EC2/DriveBySourceTraffic!DNS</a>           | Amazon EC2        | DNSlog                  | Tinggi                      |
| <a href="#">Trojan:EC2/DropPoint!DNS</a>                      | Amazon EC2        | DNSlog                  | Sedang                      |

| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan                        |
|--|-------------------|-------------------------|--|
| <a href="#">Trojan:EC2/PhishingDomainRequest!DNS</a>     | Amazon EC2        | DNSlog                  | Tinggi   |
| <a href="#">UnauthorizedAccess:EC2/MetadataDNSRebind</a> | Amazon EC2        | DNSlog                  | Tinggi   |
| <a href="#">Execution:Container/MaliciousFile</a>        | Kontainer         | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution:Container/SuspiciousFile</a>       | Kontainer         | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution:EC2/MaliciousFile</a>              | EC2               | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution:EC2/SuspiciousFile</a>             | EC2               | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan                        |
|---|-------------------|-------------------------|--|
| <a href="#">Execution</a><br><a href="#">:ECS/MaliciousFile</a>               | ECS               | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution</a><br><a href="#">:ECS/SuspiciousFile</a>              | ECS               | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution</a><br><a href="#">:Kubernetes/MaliciousFile</a>        | Kubernetes        | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">Execution</a><br><a href="#">:Kubernetes/SuspiciousFile</a>       | Kubernetes        | EBSPerlindungan Malware | Bervariasi tergantung pada ancaman yang terdeteksi |
| <a href="#">CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed</a> | Kubernetes        | EKSlog audit            | Sedang   |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller</a>                 | Kubernetes        | EKSlog audit            | Tinggi   |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller.Custom</a>  | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">CredentialAccess:Kubernetes/SuccessfulAnonymousAccess</a> | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">CredentialAccess:Kubernetes/TorIPCaller</a>               | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">DefenseEvolution:Kubernetes/MaliciousIPCaller</a>         | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">DefenseEvolution:Kubernetes/MaliciousIPCaller.Custom</a>  | Kubernetes        | EKSlog audit            | Tinggi                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">DefenseEv<br/>asion:Kub<br/>ernetes/S<br/>uccessful<br/>Anonymous<br/>Access</a>      | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">DefenseEv<br/>asion:Kub<br/>ernetes/T<br/>orIPCaller</a>                              | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Discovery<br/>:Kubernet<br/>es/Anomal<br/>ousBehavi<br/>or.Permis<br/>sionChecked</a> | Kubernetes        | EKSlog audit            | Rendah                      |
| <a href="#">Discovery<br/>:Kubernetes/<br/>MaliciousIPCall<br/>er</a>                             | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Discovery<br/>:Kubernetes/<br/>MaliciousIPCall<br/>er.Custom</a>                      | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Discovery<br/>:Kubernet<br/>es/Succes<br/>sfulAnony<br/>mousAccess</a>                | Kubernetes        | EKSlog audit            | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">Discovery</a><br><a href="#">:Kubernetes/TorIPCaller</a>                        | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Execution</a><br><a href="#">:Kubernetes/ExecInKubeSystemPod</a>                | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Execution</a><br><a href="#">:Kubernetes/AnomalousBehavior.ExecInPod</a>        | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Execution</a><br><a href="#">:Kubernetes/AnomalousBehavior.WorkloadDeployed</a> | Kubernetes        | EKSlog audit            | Rendah                      |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller</a>   | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller.Custom</a>                                  | Kubernetes        | EKSlog audit            | Tinggi                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">Impact:Kubernetes/SuccessfulAnonymousAccess</a>         | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Impact:Kubernetes/TorIPCaller</a>                       | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Persisten ce:Kubernetes/ContainerWithSensitiveMount</a> | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Persisten ce:Kubernetes/MaliciousIPCaller</a>           | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Persisten ce:Kubernetes/MaliciousIPCaller.Custom</a>    | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Persisten ce:Kubernetes/SuccessfulAnonymousAccess</a>   | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Persisten ce:Kubernetes/TorIPCaller</a>                 | Kubernetes        | EKSlog audit            | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">Policy:Kubernetes/AdminAccessToDefaultServiceAccount</a>                | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Policy:Kubernetes/AnonymousAccessGranted</a>                            | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Policy:Kubernetes/KubeflowDashboardExposed</a>                          | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">Policy:Kubernetes/ExposedDashboard</a>                                  | Kubernetes        | EKSlog audit            | Sedang                      |
| <a href="#">PrivilegeEscalation:Kubernetes/AnonymousBehavior.RoleBindingCreated</a> | Kubernetes        | EKSlog audit            | Sedang*                     |



| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|-------------------|-------------------------|-----------------------------|
| <a href="#">Privilege Escalation:Kubernetes/AnonymousBehavior.RoleCreated</a>                          | Kubernetes        | EKSlog audit            | Rendah                      |
| <a href="#">Persistence:Kubernetes/AnonymousBehavior.WorkloadDeployed!ContainerWithSensitiveMount</a>  | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Privilege Escalation:Kubernetes/AnonymousBehavior.WorkloadDeployed!PrivilegedContainer</a> | Kubernetes        | EKSlog audit            | Tinggi                      |
| <a href="#">Privilege Escalation:Kubernetes/PrivilegedContainer</a>                                    | Kubernetes        | EKSlog audit            | Sedang                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar              | Menemukan tingkat keparahan |
|---|-------------------|--------------------------------------|-----------------------------|
| <a href="#">Backdoor: Lambda/C&amp;CActivity.B</a>                  | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Tinggi                      |
| <a href="#">CryptoCurrency: Lambda/BitcoinTool.B</a>                | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Tinggi                      |
| <a href="#">Trojan: Lambda/BlackholeTraffic</a>                     | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Sedang                      |
| <a href="#">Trojan: Lambda/Drop Point</a>                           | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Sedang                      |
| <a href="#">UnauthorizedAccess: Lambda/MaliciousIPCaller.Custom</a> | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Sedang                      |
| <a href="#">UnauthorizedAccess: Lambda/TorClient</a>                | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Tinggi                      |
| <a href="#">UnauthorizedAccess: Lambda/TorRelay</a>                 | Lambda            | Pemantauan Aktivitas Jaringan Lambda | Tinggi                      |

| Tipe temuan   | Jenis sumber daya   | Sumber/fitur data dasar       | Menemukan tingkat keparahan |
|---|---|-------------------------------|-----------------------------|
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.FailedLogin</a>          | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Rendah                      |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce</a> | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Tinggi                      |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin</a>      | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Variabel*                   |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.FailedLogin</a>          | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Sedang                      |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin</a>      | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Tinggi                      |

| Tipe temuan   | Jenis sumber daya   | Sumber/fitur data dasar       | Menemukan tingkat keparahan |
|---|---|-------------------------------|-----------------------------|
| <a href="#">Credential Access:RDS/TorIPCaller.FailedLogin</a>     | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Sedang                      |
| <a href="#">Credential Access:RDS/TorIPCaller.SuccessfulLogin</a> | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Tinggi                      |
| <a href="#">Discovery:RDS/MaliciousIPCaller</a>                   | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Sedang                      |
| <a href="#">Discovery:RDS/TorIPCaller</a>                         | <a href="#">Basis data Amazon Aurora dan Amazon yang didukung RDS</a> | RDSPemantauan Aktivitas Login | Sedang                      |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B</a>                | Instance, EKS cluster, ECS cluster, atau kontainer                    | Pemantauan Runtime            | Tinggi                      |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B!DNS</a>            | Instance, EKS cluster, ECS cluster, atau kontainer                    | Pemantauan Runtime            | Tinggi                      |

| Tipe temuan  | Jenis sumber daya                                  | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|--|-------------------------|-----------------------------|
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B</a>                         | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B!DNS</a>                     | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">DefenseEvolution:Runtime/FilelessExecution</a>                   | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">DefenseEvolution:Runtime/ProcessInjection.Proc</a>               | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">DefenseEvolution:Runtime/ProcessInjection.Ptrace</a>             | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">DefenseEvolution:Runtime/ProcessInjection.VirtualMemoryWrite</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |

| Tipe temuan   | Jenis sumber daya                                  | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|--|-------------------------|-----------------------------|
| <a href="#">DefenseEv<br/>asion:Runtime/<br/>PtraceAntiDeb<br/>ugging</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Rendah                      |
| <a href="#">DefenseEv<br/>asion:Runtime/<br/>SuspiciousCom<br/>mand</a>   | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Execution<br/>:Runtime/<br/>Malicious<br/>FileExecuted</a>    | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Execution<br/>:Runtime/<br/>NewBinary<br/>Executed</a>        | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">Execution<br/>:Runtime/<br/>NewLibrar<br/>yLoaded</a>         | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">Execution<br/>:Runtime/<br/>Suspiciou<br/>sCommand</a>        | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Variabel                    |
| <a href="#">Execution<br/>:Runtime/<br/>Suspiciou<br/>sShellCreated</a>   | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Rendah                      |

| Tipe temuan  | Jenis sumber daya                                  | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|--|-------------------------|-----------------------------|
| <a href="#">Execution:Runtime/SuspiciousTool</a>                 | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Variabel                    |
| <a href="#">Execution:Runtime/ReverseShell</a>                   | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Impact:Runtime/AbusedDomainRequest.Reputation</a>    | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">Impact:Runtime/BitcoinDomainRequest.Reputation</a>   | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Impact:Runtime/CryptoMinerExecuted</a>               | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Impact:Runtime/MaliciousDomainRequest.Reputation</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |

| Tipe temuan  | Jenis sumber daya                                  | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|--|-------------------------|-----------------------------|
| <a href="#">Impact:Runtime/SuspiciousDomainRequest.Reputation</a>        | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Rendah                      |
| <a href="#">PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified</a>  | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">PrivilegeEscalation:Runtime/ContainerMountsHostDirectory</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">PrivilegeEscalation:Runtime/DockerSocketAccessed</a>         | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">PrivilegeEscalation:Runtime/ElevationToRoot</a>              | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |



| Tipe temuan  | Jenis sumber daya                                  | Sumber/fitur data dasar       | Menemukan tingkat keparahan |
|--|--|-------------------------------|-----------------------------|
| <a href="#">Privilege Escalation:Runtime/RuncContainerEscape</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Tinggi                      |
| <a href="#">Privilege Escalation:Runtime/UserfaultUsage</a>      | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Sedang                      |
| <a href="#">Object:S3/MaliciousFile</a>                          | S3Object   | Perlindungan Malware untuk S3 | Tinggi                      |
| <a href="#">Trojan:Runtime/BlackholeTraffic</a>                  | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Sedang                      |
| <a href="#">Trojan:Runtime/BlackholeTraffic!DNS</a>              | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Sedang                      |
| <a href="#">Trojan:Runtime/DropPoint</a>                         | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Sedang                      |
| <a href="#">Trojan:Runtime/DGA.DomainRequest.C!DNS</a>           | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime            | Tinggi                      |

| Tipe temuan  | Jenis sumber daya                                  | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|--|-------------------------|-----------------------------|
| <a href="#">Trojan:Runtime/DriveBySourceTraffic!DNS</a>      | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Trojan:Runtime/DropPoint!DNS</a>                 | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Sedang                      |
| <a href="#">Trojan:Runtime/PhishingDomainRequest!DNS</a>     | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">UnauthorizedAccess:Runtime/MetadataDNSRebind</a> | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">UnauthorizedAccess:Runtime/TorClient</a>         | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">UnauthorizedAccess:Runtime/TorRelay</a>          | Instance, EKS cluster, ECS cluster, atau kontainer | Pemantauan Runtime      | Tinggi                      |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B</a>               | EC2  | log alur VPC            | Tinggi                      |

| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|-------------------|-------------------------|-----------------------------|
| <a href="#">Backdoor:EC2/DenialOfService.Dns</a>             | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Backdoor:EC2/DenialOfService.Tcp</a>             | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Backdoor:EC2/DenialOfService.Udp</a>             | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Backdoor:EC2/DenialOfService.UdpOnTcpPorts</a>   | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Backdoor:EC2/DenialOfService.UnusualProtocol</a> | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Backdoor:EC2/Spambot</a>                         | EC2               | log alur VPC            | Sedang                      |
| <a href="#">Behavior:EC2/NetworkPortUnusual</a>              | EC2               | log alur VPC            | Sedang                      |
| <a href="#">Behavior:EC2/TrafficVolumeUnusual</a>            | EC2               | log alur VPC            | Sedang                      |

| Tipe temuan  | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|--|-------------------|-------------------------|-----------------------------|
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B</a>         | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">DefenseEvasion:EC2/UnusualDNSResolver</a>    | EC2               | log alur VPC            | Sedang                      |
| <a href="#">DefenseEvasion:EC2/UnusualDockerActivity</a> | EC2               | log alur VPC            | Sedang                      |
| <a href="#">DefenseEvasion:EC2/UnusualDockerActivity</a> | EC2               | log alur VPC            | Sedang                      |
| <a href="#">Impact:EC2/PortSweep</a>                     | EC2               | log alur VPC            | Tinggi                      |
| <a href="#">Impact:EC2/WinRMBruteForce</a>               | EC2               | log alur VPC            | Rendah*                     |
| <a href="#">Recon:EC2/PortProbeEMRUnprotectedPort</a>    | EC2               | log alur VPC            | Tinggi                      |

| Tipe temuan   | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">Recon:EC2/PortProbeUnprotectedPort</a>              | EC2               | log alur VPC            | Rendah*                     |
| <a href="#">Recon:EC2/Portscan</a>                              | EC2               | log alur VPC            | Sedang                      |
| <a href="#">Trojan:EC2/BlackholeTraffic</a>                     | EC2               | log alur VPC            | Sedang                      |
| <a href="#">Trojan:EC2/DropPoint</a>                            | EC2               | log alur VPC            | Sedang                      |
| <a href="#">UnauthorizedAccess:EC2/MaliciousIPCaller.Custom</a> | EC2               | log alur VPC            | Sedang                      |
| <a href="#">UnauthorizedAccess:EC2/RDPBruteForce</a>            | EC2               | log alur VPC            | Rendah*                     |
| <a href="#">UnauthorizedAccess:EC2/SSHBruteForce</a>            | EC2               | log alur VPC            | Rendah*                     |
| <a href="#">UnauthorizedAccess:EC2/TorClient</a>                | EC2               | log alur VPC            | Tinggi                      |

| Tipe temuan                                     | Jenis sumber daya | Sumber/fitur data dasar | Menemukan tingkat keparahan |
|---|-------------------|-------------------------|-----------------------------|
| <a href="#">UnauthorizedAccess:EC2/TorRelay</a> | EC2               | log alur VPC            | Tinggi                      |

# Mengelola GuardDuty temuan Amazon

GuardDuty menawarkan beberapa fitur penting untuk membantu Anda mengurutkan, menyimpan, dan mengelola temuan Anda. Fitur-fitur ini akan membantu Anda menyesuaikan temuan dengan lingkungan spesifik Anda, mengurangi kebisingan dari temuan nilai rendah, dan membantu Anda fokus pada ancaman terhadap lingkungan AWS yang unik. Tinjau topik di halaman ini untuk memahami bagaimana Anda dapat menggunakan fitur ini untuk meningkatkan nilai GuardDuty temuan.

Topik:

## [Dasbor ringkasan](#)

Pelajari tentang komponen dasbor ringkasan yang tersedia di GuardDuty konsol.

## [Memfilter temuan](#)

Pelajari cara memfilter GuardDuty temuan berdasarkan kriteria yang Anda tentukan.

## [Aturan penekanan](#)

Pelajari cara memfilter temuan secara otomatis yang GuardDuty memberi tahu Anda melalui aturan penekanan. Aturan penekanan mengarsipkan temuan secara otomatis berdasarkan filter.

## [Bekerja dengan daftar IP tepercaya dan daftar ancaman](#)

Sesuaikan lingkup GuardDuty pemantauan menggunakan Daftar IP dan Daftar Ancaman berdasarkan alamat IP yang dapat dirutekan secara publik. Daftar IP tepercaya mencegah DNS non-temuan dihasilkan dari IP yang Anda anggap tepercaya, sementara Daftar Intel Ancaman akan GuardDuty mengingatkan Anda tentang aktivitas yang ditentukan penggunaIPs.

## [Mengekspor temuan](#)

Ekspor temuan yang dihasilkan ke bucket Amazon S3 sehingga Anda dapat menyimpan catatan melewati periode retensi temuan 90 hari di. GuardDuty Gunakan data historis ini untuk melacak potensi aktivitas mencurigakan di akun Anda dan mengevaluasi apakah langkah-langkah perbaikan yang disarankan berhasil.

## [Membuat tanggapan khusus terhadap GuardDuty temuan dengan Amazon CloudWatch Events](#)

Siapkan notifikasi otomatis untuk GuardDuty temuan melalui CloudWatch acara Amazon. Anda juga dapat mengotomatiskan tugas lain melalui CloudWatch Acara untuk membantu Anda menanggapi temuan.

## [Memahami CloudWatch Log dan alasan melewati sumber daya selama Perlindungan Malware untuk pemindaian EC2](#)

Pelajari cara mengaudit CloudWatch Log untuk Perlindungan GuardDuty Malware EC2 dan alasan mengapa EC2 instans Amazon atau EBS volume Amazon Anda yang terkena dampak mungkin telah dilewati selama proses pemindaian.

## [Melaporkan positif palsu dalam Perlindungan GuardDuty Malware untuk EC2](#)

Pelajari cara melaporkan potensi deteksi ancaman positif palsu di Perlindungan Malware untuk S3.

## Dasbor ringkasan

Dasbor Ringkasan memberikan tampilan agregat dari GuardDuty temuan yang dihasilkan di Wilayah Anda Akun AWS saat ini. Saat ini, dasbor mendukung volume hingga 5.000 temuan. Namun, Anda dapat melihat detail semua temuan dengan menggunakan halaman Temuan di GuardDuty konsol, atau [GetFindings](#) atau [ListFindings](#).

### Note

Ringkasan temuan hanya tersedia melalui GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Bagian berikut akan membantu Anda mengakses dasbor dan memahami komponennya.

### Daftar Isi

- [Mengakses dasbor Ringkasan](#)
- [Memahami dasbor Ringkasan](#)
- [Memberikan umpan balik di dasbor Ringkasan](#)



## Mengakses dasbor Ringkasan

Di GuardDuty konsol, dasbor Ringkasan menunjukkan tampilan konsolidasi hingga 5.000 GuardDuty temuan terakhir yang dihasilkan di Wilayah saat ini.

Untuk mengakses dasbor Ringkasan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Ringkasan. Saat Anda membuka konsol, GuardDuty menampilkan dasbor Ringkasan.
3. Secara default, ringkasan akan ditampilkan untuk hari yang sama — Hari ini. GuardDutyKonsol menyediakan opsi untuk melihat ringkasan selama 2 hari terakhir, 7 hari terakhir, dan 30 hari terakhir. Untuk mengubah rentang waktu default, pilih salah satu opsi dari dropdown di atas panel Ikhtisar.
4. Filter data
  - Akun dengan sebagian besar temuan, Sumber daya dengan sebagian besar temuan, dan widget temuan yang paling tidak terjadi membantu Anda memfilter data berdasarkan tingkat keparahan temuan.
  - Widget Sumber Daya dengan sebagian besar temuan juga membantu Anda memfilter data berdasarkan jenis sumber daya yang berpotensi terkena dampak.

Akun anggota dapat melihat detail sumber daya yang berpotensi terkena dampak milik akun mereka sendiri. Jika Anda adalah akun GuardDuty administrator dan ingin melihat detail sumber daya yang berpotensi terkena dampak, buka GuardDuty konsol menggunakan kredensial akun anggota terkait.

5. Cakupan rencana perlindungan

Cakupan paket perlindungan menyediakan jumlah akun anggota yang telah diaktifkan GuardDuty di organisasi Anda. Statistik hanya dapat dilihat oleh GuardDuty administrator yang didelegasikan.

## Memahami dasbor Ringkasan

Dasbor Ringkasan menunjukkan data agregat di bagian berikut. Sebelum Anda melanjutkan untuk melihat dan memahami ringkasan, pastikan untuk memilih yang diinginkan Wilayah AWS dari pemilih Wilayah di bagian atas konsol. Juga, pastikan untuk memilih rentang waktu yang diinginkan dari

menu tarik-turun yang disediakan di atas panel Ikhtisar. Jika tidak ada temuan yang dihasilkan untuk parameter yang dipilih, tidak ada data yang akan tersedia di salah satu widget.

Dari volume hingga 5.000 GuardDuty temuan terakhir, dasbor ringkasan dengan Akun dengan sebagian besar temuan, Sumber daya dengan sebagian besar temuan, dan Temuan yang paling tidak terjadi menunjukkan data berdasarkan dari 5 hasil teratas. Untuk analisis yang lebih dalam, lihat halaman Temuan di GuardDuty konsol.

## Gambaran Umum

Bagian ini menyediakan data berikut:

- Total temuan: Menunjukkan jumlah total temuan yang dihasilkan di akun Anda di Wilayah saat ini.
- Temuan tingkat keparahan tinggi: Menunjukkan jumlah GuardDuty temuan yang memiliki tingkat keparahan tinggi di Wilayah saat ini.
- Sumber daya dengan temuan: Menunjukkan jumlah sumber daya yang terkait dengan temuan dan berpotensi dikompromikan.
- Akun dengan temuan: Menunjukkan jumlah akun di mana setidaknya satu temuan dihasilkan. Jika Anda adalah akun mandiri, nilai di bidang ini adalah 1.

Untuk rentang waktu 7 hari terakhir dan 30 hari terakhir, panel Ikhtisar dapat menunjukkan perbedaan persentase dalam temuan yang dihasilkan minggu ke minggu (WoW) atau bulan ke bulan (MoM), masing-masing. Jika tidak ada temuan yang dihasilkan pada minggu atau bulan sebelumnya, maka tanpa data untuk membandingkan, perbedaan persentase mungkin tidak tersedia.

Jika Anda adalah akun GuardDuty administrator, semua bidang ini menyediakan data yang diringkas di semua akun anggota di organisasi Anda.

## Temuan berdasarkan tingkat keparahan

Bagian ini menampilkan diagram batang dengan jumlah total temuan terhadap rentang waktu yang dipilih. Anda dapat melihat jumlah temuan dengan tingkat keparahan rendah, sedang, atau tinggi, yang dihasilkan pada tanggal tertentu dalam rentang waktu yang dipilih.

## Jenis temuan paling umum

Bagian ini memberikan ilustrasi diagram lingkaran dari lima jenis temuan umum teratas seperti yang diamati dari volume hingga 5.000 GuardDuty temuan terakhir yang dihasilkan di Wilayah saat ini. Diagram lingkaran ini menampilkan data berikut saat mengarahkan kursor ke setiap sektor:

- Jumlah temuan: Menunjukkan berapa kali temuan ini dihasilkan dalam rentang waktu yang dipilih.
- Keparahan: Menunjukkan tingkat keparahan temuan - misalnya, Sedang dan Tinggi.
- Persentase: Menunjukkan bagian dari jenis temuan ini di diagram lingkaran.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir dihasilkan.

### Akun dengan sebagian besar temuan

Bagian ini menyediakan data berikut:

- Akun: Menunjukkan Akun AWS ID tempat temuan dibuat.
- Hitungan temuan: Menunjukkan berapa kali temuan dibuat untuk ID akun ini.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan terakhir dibuat untuk ID akun ini.
- Tingkat keparahan tinggi: Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Tingkat keparahan tinggi, Tingkat keparahan sedang, dan Semua tingkat keparahan.

### Sumber daya dengan temuan

Bagian ini menyediakan data berikut:

- Sumber Daya: Menunjukkan jenis sumber daya yang berpotensi terpengaruh dan jika sumber daya ini milik akun Anda, Anda dapat mengakses tautan cepat untuk melihat detail sumber daya. Jika Anda adalah akun GuardDuty administrator, Anda dapat melihat detail sumber daya yang berpotensi terkena dampak dengan mengakses GuardDuty konsol dengan kredensial akun anggota tempat sumber daya ini berada.
- Akun: Menunjukkan Akun AWS ID tempat sumber daya ini berada.
- Hitungan temuan: Menunjukkan berapa kali sumber daya ini dikaitkan dengan temuan.
- Terakhir dihasilkan: Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan yang terkait dengan sumber daya ini terakhir dihasilkan.
- Semua jenis sumber daya: Secara default, data ditampilkan untuk semua jenis sumber daya. Dengan menggunakan dropdown, Anda dapat melihat data untuk jenis sumber daya tertentu, seperti Instance,, AccessKeyLambda, dan lainnya.

- **Tingkat keparahan tinggi:** Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Dengan menggunakan dropdown, Anda dapat melihat data untuk tingkat keparahan lainnya. Opsi yang memungkinkan adalah Tingkat keparahan tinggi, Tingkat keparahan sedang, dan Semua tingkat keparahan.

### Temuan yang paling tidak terjadi

Bagian ini memberikan rincian jenis temuan yang tidak sering dihasilkan di AWS lingkungan Anda. Wawasan ini dapat membantu Anda menyelidiki dan mengambil tindakan terhadap pola ancaman yang muncul di lingkungan Anda. Tabel menunjukkan data berikut:

- **Jenis pencarian:** Menunjukkan nama tipe temuan.
- **Hitungan temuan:** Menunjukkan berapa kali jenis temuan ini dihasilkan dalam rentang waktu yang dipilih.
- **Terakhir dihasilkan:** Menunjukkan berapa banyak waktu yang telah berlalu sejak jenis temuan ini terakhir dihasilkan.
- **Tingkat keparahan tinggi:** Secara default, data ditampilkan untuk jenis temuan tingkat keparahan tinggi. Opsi yang memungkinkan untuk bidang ini adalah Tingkat keparahan tinggi, Tingkat keparahan sedang, dan Semua tingkat keparahan.

### Cakupan rencana perlindungan

Bagian ini menyediakan jumlah akun anggota aktif milik organisasi Anda dan telah mengaktifkan satu atau beberapa fitur dan fitur tambahan (sebagaimana berlaku) konfigurasi saat ini Wilayah AWS.

Hanya GuardDuty administrator yang didelegasikan yang dapat melihat statistik untuk akun anggota dalam organisasi mereka. Jika fitur tidak dikonfigurasi, pilih Konfigurasi di bawah kolom Tindakan.

Saat Anda membuat AWS organisasi baru, mungkin diperlukan waktu hingga 24 jam untuk menghasilkan statistik untuk seluruh organisasi.

## Memberikan umpan balik di dasbor Ringkasan

GuardDuty mendorong Anda untuk memberikan umpan balik tentang kegunaan, fitur, dan kinerja dasbor Ringkasan. Ini akan membantu kami meningkatkan dasbor.

Untuk memberikan umpan balik di dasbor Ringkasan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Di panel navigasi, pilih Ringkasan. Saat Anda membuka GuardDuty konsol, itu menunjukkan dasbor Ringkasan.
3. Pilih Umpan Balik di sudut kanan atas dasbor. Ini akan membuka formulir. Setelah Anda memberikan umpan balik, pilih Kirim.

## Memfilter temuan

Filter temuan memungkinkan Anda melihat temuan yang sesuai dengan kriteria yang Anda tentukan dan memfilter temuan yang tidak sesuai. Anda dapat dengan mudah membuat filter pencarian menggunakan GuardDuty konsol Amazon, atau Anda dapat membuatnya dengan [CreateFilter](#) API menggunakan JSON. Tinjau bagian berikut untuk memahami cara membuat filter di konsol. Untuk menggunakan filter ini untuk mengarsipkan temuan yang masuk secara otomatis, lihat [Aturan penekanan](#).

## Membuat filter di GuardDuty konsol

Filter pencarian dapat dibuat dan diuji melalui GuardDuty konsol. Anda dapat menyimpan filter yang dibuat melalui konsol untuk digunakan dalam aturan penekanan atau operasi filter mendatang. Filter terbuat dari setidaknya satu kriteria filter. Terdiri dari satu atribut filter yang dipasangkan dengan setidaknya satu nilai.

Saat membuat filter, perhatikan hal berikut:

- Filter tidak menerima wild card.
- Anda dapat menentukan minimum satu atribut dan maksimum hingga 50 atribut sebagai kriteria untuk filter tertentu.
- Saat menggunakan syarat sama dengan atau tidak sama dengan untuk memfilter nilai atribut, seperti ID Akun, Anda dapat menentukan maksimum 50 nilai.
- Setiap atribut kriteria filter dievaluasi sebagai operator AND. Beberapa nilai untuk atribut yang sama dievaluasi sebagai AND/OR.

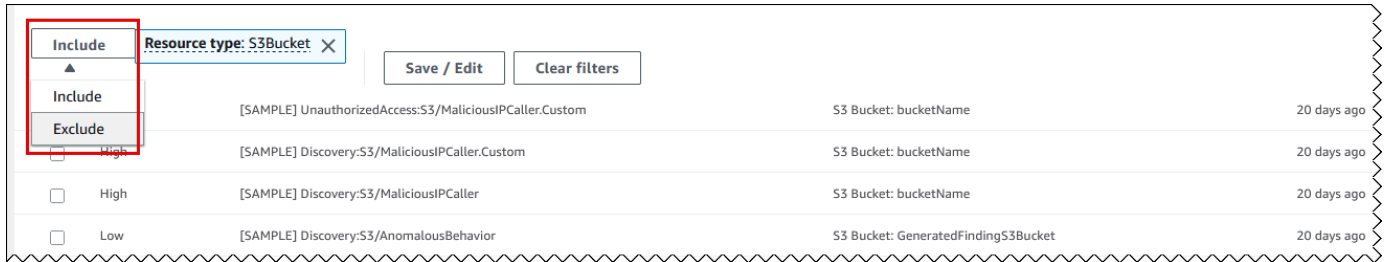
Untuk memfilter temuan (konsol)

1. Di bawah Filter menurut atribut, pilih Tambahkan kriteria filter. Ini akan menunjukkan daftar atribut filter yang diperluas.

2. Dari daftar atribut yang diperluas, pilih atribut yang ingin Anda tentukan sebagai kriteria untuk filter Anda, seperti ID Akun atau Jenis tindakan.

Untuk daftar lengkap atribut, lihat [Atribut filter](#).

3. Di bidang teks yang ditampilkan, tentukan nilai untuk atribut yang dipilih lalu pilih Terapkan.
4. Untuk menambahkan lebih dari satu kriteria filter, ulangi langkah 1-3.
5. Secara default, daftar menunjukkan temuan yang cocok dengan filter yang diterapkan. Jika Anda ingin melihat temuan yang tidak cocok dengan atribut filter, pilih Kecualikan di sebelah filter.



6. Simpan atribut dan nilai yang ditentukan sebagai filter
  - a. Untuk menyimpan atribut yang ditentukan dan nilainya (kriteria filter) sebagai filter, pilih Simpan/Edit.
  - b. Masukkan aturan filter Nama dan Deskripsi.
  - c. Pilih Simpan.

## Atribut filter

Saat Anda membuat filter atau mengurutkan temuan menggunakan API operasi, Anda harus menentukan kriteria filter diJSON. Kriteria filter ini berkorelasi dengan detail JSON temuan. Tabel berikut berisi daftar nama tampilan konsol untuk atribut filter dan nama JSON bidang yang setara.

| Nama bidang konsol | JSONnama bidang |
|--------------------|-----------------|
| account-id         | accountId       |
| ID Temuan          | id              |
| Wilayah            | region          |
| Kepelikan          | kepelikan       |

| Nama bidang konsol  | JSONnama bidang   |
|---------------------|---|
|                     | Anda dapat memfilter jenis temuan berdasarkan tingkat keparahan jenis temuan. Untuk informasi lebih lanjut tentang nilai keparahan, lihat <a href="#">Tingkat keparahan untuk GuardDuty temuan</a> . Jika Anda menggunakan severity dengan API, AWS CLI, atau AWS CloudFormation, itu diberikan nilai numerik. Untuk informasi selengkapnya, lihat <a href="#">findingCriteria</a> di GuardDuty API Referensi Amazon. |
| Tipe temuan         | jenis   |
| Diperbarui pada     | updatedAt   |
| Access key ID       | sumber daya. accessKeyDetails. accessKeyId  |
| ID utama            | sumber daya. accessKeyDetails. principalId  |
| nama pengguna       | sumber daya. accessKeyDetails. userName   |
| Jenis pengguna      | sumber daya. accessKeyDetails. userType   |
| IAMID profil contoh | sumber daya. instanceDetails. iamInstanceProfile.id   |
| ID Instans          | sumber daya. instanceDetails. instanceId  |
| ID citra instans    | sumber daya. instanceDetails. imageId   |
| Kunci tag contoh    | sumber daya. instanceDetails.tags.key   |
| Nilai tag instance  | sumber daya. instanceDetails.tags.value   |
| IPv6alamat          | sumber daya. instanceDetails. networkInterfaces.IPv6Alamat  |
| Alamat IPv4 pribadi | sumber daya. instanceDetails. networkInterfaces. privateIpAddresses. privateIpAddress   |

| Nama bidang konsol  | JSONnama bidang  |
|---------------------|--|
| DNSNama publik      | sumber daya. instanceDetails. networkInterfaces. publicDnsName             |
| IP Publik           | sumber daya. instanceDetails. networkInterfaces. publicIp                  |
| ID grup keamanan    | sumber daya. instanceDetails. networkInterfaces. securityGroups. groupId   |
| Nama grup keamanan  | sumber daya. instanceDetails. networkInterfaces. securityGroups. groupName |
| ID Subnet           | sumber daya. instanceDetails. networkInterfaces. subnetId                  |
| VPCID               | sumber daya. instanceDetails. networkInterfaces. vpcId                     |
| Pos terdepan ARN    | sumber daya. instanceDetails.pos terdepan ARN                              |
| Jenis sumber daya   | sumber daya. resourceType  |
| Izin bucket         | sumber BucketDetails daya.s3. publicAccess.effectivePermission             |
| Nama Bucket         | sumber BucketDetails daya.s3 .nama   |
| Kunci tanda bucket  | BucketDetailsresource.s3 .tags.key   |
| Nilai tanda bucket  | BucketDetailsresource.s3 .tags.value                                       |
| Tipe bucket         | sumber BucketDetails daya.s3 .type   |
| Tipe tindakan       | service.action. actionType   |
| API disebut         | service.action. awsApiCallAction.API                                       |
| API jenis penelepon | service.action. awsApiCallTindakan. callerType                             |



| Nama bidang konsol          | JSONnama bidang   |
|-----------------------------|---|
| APIKode Kesalahan           | service.action. awsApiCallTindakan. errorCode                               |
| APIkota penelepon           | service.action. awsApiCallTindakan. remotelpD<br>etails.kota. cityName      |
| APInegara penelepon         | service.action. awsApiCallTindakan. remotelpD<br>etails.negara. countryName |
| APIalamat penelepon IPv4    | service.action. awsApiCallTindakan. remotelpD<br>etails. ipAddressV4        |
| APIalamat penelepon IPv6    | service.action. awsApiCallTindakan. remotelpD<br>etails. ipAddressV6        |
| APIID penelepon ASN         | service.action. awsApiCallTindakan. remotelpD<br>etails.organisasi.asn      |
| APInama penelepon ASN       | service.action. awsApiCallTindakan. remotelpD<br>etails.organisasi. asnOrg  |
| APInama layanan penelepon   | service.action. awsApiCallTindakan. serviceNa<br>me                         |
| DNSpermintaan domain        | service.action. dnsRequestAction.domain                                     |
| DNSminta sufiks domain      | service.action. dnsRequestAction. domainWit<br>hSuffix                      |
| Koneksi jaringan diblokir   | service.action. networkConnectionAction.dib<br>lokir                        |
| Arah koneksi jaringan       | service.action. networkConnectionAction.<br>connectionDirection             |
| Port lokal koneksi jaringan | service.action. networkConnectionAction.<br>localPortDetails.pelabuhan      |

| Nama bidang konsol                      | JSONnama bidang   |
|---|---|
| Protokol koneksi jaringan               | service.action. networkConnectionAction.pro<br>tokol                            |
| Kota koneksi jaringan                   | service.action. networkConnectionAction.<br>remotelpDetails.kota. cityName      |
| Negara koneksi jaringan                 | service.action. networkConnectionAction.<br>remotelpDetails.negara. countryName |
| IPv4Alamat jarak jauh koneksi jaringan  | service.action. networkConnectionAction.<br>remotelpDetails. ipAddressV4        |
| IPv6Alamat jarak jauh koneksi jaringan  | service.action. networkConnectionAction.<br>remotelpDetails. ipAddressV6        |
| Koneksi jaringan remote IP ASN ID       | service.action. networkConnectionAction.<br>remotelpDetails.organisasi. asn     |
| Koneksi jaringan ASN nama IP jarak jauh | service.action. networkConnectionAction.<br>remotelpDetails.organisasi. asnOrg  |
| Port jarak jauh koneksi jaringan        | service.action. networkConnectionAction.<br>remotePortDetails.pelabuhan         |
| Akun jarak jauh berafiliasi             | service.action. awsApiCallTindakan. remoteAcc<br>ountDetails.berafiliasi        |
| Alamat penelepon Kubernetes API IPv4    | service.action. kubernetesApiCallTindakan.<br>remotelpDetails. ipAddressV4      |
| Alamat penelepon Kubernetes API IPv6    | service.action. kubernetesApiCallTindakan.<br>remotelpDetails. ipAddressV6      |
| Namespace Kubernetes                    | service.action. kubernetesApiCallAction.nam<br>espace                           |
| ID penelepon Kubernetes API ASN         | service.action. kubernetesApiCallTindakan.<br>remotelpDetails.organisasi. asn   |

| Nama bidang konsol                      | JSONnama bidang  |
|---|--|
| Permintaan panggilan Kubernetes API URI | service.action. kubernetesApiCallTindakan. requestUri                      |
| Kode status Kubernetes API              | service.action. kubernetesApiCallTindakan. statusCode                      |
| Koneksi jaringan IPv4 alamat lokal      | service.action. networkConnectionAction. localIpDetails. ipAddressV4       |
| Koneksi jaringan IPv6 alamat lokal      | service.action. networkConnectionAction. localIpDetails. ipAddressV6       |
| Protokol                                | service.action. networkConnectionAction.pro tokol                          |
| API nama layanan panggilan              | service.action. awsApiCallTindakan. serviceNa me                           |
| API ID akun penelepon                   | service.action. awsApiCallTindakan. remoteAcc ountDetails. accountId       |
| Nama daftar ancaman                     | layanan. additionalInfo. threatListName                                    |
| Peran sumber daya                       | layanan. resourceRole  |
| EKS nama cluster                        | sumber daya. eksClusterDetails.nama  |
| Nama beban kerja Kubernetes             | sumber daya. kubernetesDetails. kubernetesWorkloadDetails.nama             |
| Namespace beban kerja Kubernetes        | sumber daya. kubernetesDetails. kubernetesWorkloadDetails.namespace        |
| Nama pengguna Kubernetes                | sumber daya. kubernetesDetails. kubernetesUserDetails.nama pengguna        |
| Gambar kontainer Kubernetes             | sumber daya. kubernetesDetails. kubernetesWorkloadDetails.containers.image |

| Nama bidang konsol                 | JSONnama bidang  |
|------------------------------------|--|
| Awalan gambar kontainer Kubernetes | sumber daya. kubernetesDetails. kubernete<br>sWorkloadDetails.kontainer. imagePrefix                   |
| Pindai ID                          | layanan. ebsVolumeScanDetail. scanId   |
| EBSnama ancaman pemindaian volume  | layanan. ebsVolumeScanDetail. scanDetec<br>tions. threatDetectedByNama. threatNam<br>es.nama           |
| Nama ancaman pemindaian objek S3   | layanan. malwareScanDetails.ancaman.nama   |
| Tingkat keparahan ancaman          | layanan. ebsVolumeScanDetail. scanDetec<br>tions. threatDetectedByNama. threatNam<br>es.keparahan      |
| Berkas SHA                         | layanan. ebsVolumeScanDetail. scanDetec<br>tions. threatDetectedByNama. threatNames.<br>filePaths.hash |
| ECSnama cluster                    | sumber daya. ecsClusterDetails.nama  |
| ECSgambar kontainer                | sumber daya. ecsClusterDetails. taskDetai<br>ls.containers.image                                       |
| ECSdefinisi tugas ARN              | sumber daya. ecsClusterDetails. taskDetails.<br>definitionArn  |
| Gambar kontainer mandiri           | sumber daya. containerDetails.gambar   |
| Id Instans Database                | sumber daya. rdsDbInstanceDetail. dbInstanc<br>eIdentifier   |
| Id Kluster Basis Data              | sumber daya. rdsDbInstanceDetail. dbCluster<br>Identifier  |
| Mesin basis data                   | sumber daya. rdsDbInstanceDetail.Engine  |
| Pengguna basis data                | sumber daya. rdsDbUserDetail.pengguna  |

| Nama bidang konsol          | JSONnama bidang                                    |
|-----------------------------|--|
| Kunci tag contoh basis data | sumber daya. rdsDbInstancedetails.tags.key         |
| Nilai tag instance database | sumber daya. rdsDbInstancedetails.tags.value       |
| Dapat dieksekusi -256 SHA   | layanan. runtimeDetails.proses. executableSha256   |
| Nama proses                 | layanan. runtimeDetails.process.name               |
| Jalur yang dapat dieksekusi | layanan. runtimeDetails.proses. executablePath     |
| Nama fungsi Lambda          | sumber daya. lambdaDetails. functionName           |
| Fungsi Lambda ARN           | sumber daya. lambdaDetails. functionArn            |
| Tombol tag fungsi Lambda    | sumber daya. lambdaDetails.tags.key                |
| Nilai tag fungsi Lambda     | sumber daya. lambdaDetails.tags.value              |
| DNSpermintaan domain        | service.action. dnsRequestAction. domainWithSuffix |

## Aturan penekanan

Aturan penekanan adalah satu set kriteria, yang terdiri dari atribut filter yang dipasangkan dengan sebuah nilai, digunakan untuk memfilter temuan dengan secara otomatis mengarsipkan temuan baru yang sesuai dengan kriteria yang ditentukan. Aturan penekanan dapat digunakan untuk memfilter temuan bernilai rendah, temuan positif palsu, atau ancaman yang tidak ingin Anda tindaklanjuti, agar lebih mudah mengenali ancaman keamanan dengan dampak paling besar terhadap lingkungan Anda.

Setelah membuat aturan penekanan, temuan baru yang sesuai dengan kriteria yang ditentukan dalam aturan akan diarsipkan secara otomatis selama aturan penekanan berlaku. Anda dapat menggunakan filter yang ada untuk membuat aturan penekanan atau membuat aturan penekanan dari filter baru yang Anda tentukan. Anda dapat mengonfigurasi aturan penekanan untuk menekan seluruh tipe temuan, atau menentukan kriteria filter yang lebih terperinci guna menekan instans spesifik dari tipe temuan tertentu. Anda dapat mengedit aturan penindasan kapan saja.

Temuan yang ditekan tidak dikirim ke AWS Security Hub Amazon Simple Storage Service, Amazon Detective, atau EventBridge Amazon, sehingga mengurangi tingkat kebisingan jika Anda GuardDuty mengkonsumsi temuan melalui Security Hub, SIEM pihak ketiga, atau aplikasi peringatan dan tiket lainnya. Jika Anda telah mengaktifkan [Perlindungan Malware untuk EC2](#), GuardDuty temuan yang ditekan tidak akan memulai pemindaian malware.

GuardDuty terus menghasilkan temuan bahkan ketika mereka cocok dengan aturan penekanan Anda, namun, temuan tersebut secara otomatis ditandai sebagai diarsipkan. Temuan yang diarsipkan disimpan GuardDuty selama 90 hari dan dapat dilihat kapan saja selama periode tersebut. Anda dapat melihat temuan yang ditekan di GuardDuty konsol dengan memilih Diarsipkan dari tabel temuan, atau melalui GuardDuty API menggunakan [ListFindingsAPI](#) dengan `findingCriteria.kriteria sama dengan benar.service.archived`

#### Note

Dalam lingkungan multi-akun, hanya GuardDuty administrator yang dapat membuat aturan penindasan.

## Kasus penggunaan umum untuk aturan penekanan dan contoh

Jenis temuan berikut memiliki kasus penggunaan umum untuk menerapkan aturan penekanan. Pilih nama temuan untuk mempelajari lebih lanjut tentang temuan itu. Tinjau deskripsi kasus penggunaan untuk memutuskan apakah Anda ingin membuat aturan penekanan untuk tipe temuan tersebut.

#### Important

GuardDuty merekomendasikan agar Anda membangun aturan penekanan secara reaktif dan hanya untuk temuan yang telah berulang kali Anda identifikasi positif palsu di lingkungan Anda.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)— Gunakan aturan penekanan untuk secara otomatis mengarsipkan temuan yang dihasilkan saat VPC jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway lokal dan bukan dari Internet Gateway. VPC

Temuan ini dihasilkan ketika jaringan dikonfigurasi untuk merutekan lalu lintas internet sedemikian rupa sehingga keluar dari gateway lokal dan bukan dari VPC Internet Gateway ().

IGW Konfigurasi umum, seperti menggunakan, atau VPC VPN koneksi [AWS Outposts](#), dapat mengakibatkan lalu lintas dirutekan dengan cara ini. Jika ini adalah perilaku yang diharapkan, Anda disarankan untuk menggunakan aturan penekanan dan membuat aturan yang terdiri dari dua kriteria filter. Kriteria pertama adalah tipe temuan, yaitu `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Kriteria filter kedua adalah IPv4 alamat API pemanggil dengan alamat IP atau CIDR rentang gateway internet lokal Anda. Contoh di bawah ini mewakili filter yang akan Anda gunakan untuk menekan jenis temuan ini berdasarkan alamat IP API pemanggil.

Finding type: `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`  
API caller IPv4 address: `198.51.100.6`

#### Note

Untuk menyertakan beberapa API penelepon, IPs Anda dapat menambahkan filter IPv4 alamat API Penelepon baru untuk masing-masing.

- [Recon:EC2/Portscan](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis saat menggunakan aplikasi penilaian kerentanan.

Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/Portscan`. Kriteria filter kedua harus sesuai dengan instans yang menghosting alat penilaian kerentanan ini. Anda dapat menggunakan atribut ID gambar Instans atau atribut nilai Tanda, tergantung kriteria yang diidentifikasi dengan instans yang menghosting alat ini. Contoh di bawah ini mewakili filter yang akan Anda gunakan untuk menekan jenis temuan ini berdasarkan instance dengan tertentu. AMI

Finding type: `Recon:EC2/Portscan` Instance image ID: `ami-999999999`

- [UnauthorizedAccess:EC2/SSHBruteForce](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans bastion.

Jika target upaya brute force adalah host benteng, ini mungkin mewakili perilaku yang diharapkan untuk lingkungan Anda AWS . Jika demikian, kami menyarankan Anda untuk membuat aturan penekanan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `UnauthorizedAccess:EC2/SSHBruteForce`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung

kriteria yang diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan nilai tanda instans tertentu.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- [Recon:EC2/PortProbeUnprotectedPort](#) – Gunakan aturan penekanan untuk mengarsipkan temuan secara otomatis ketika ditargetkan ke instans yang sengaja diekspos.

Mungkin ada kasus di mana instans sengaja diekspos, misalnya jika instans meng-host server web. Jika ini terjadi di AWS lingkungan Anda, kami sarankan Anda membuat aturan penindasan untuk temuan ini. Aturan penekanan harus terdiri dari dua kriteria filter. Kriteria pertama harus menggunakan atribut Tipe temuan dengan nilai `Recon:EC2/PortProbeUnprotectedPort`. Kriteria filter kedua harus sesuai dengan instans yang berfungsi sebagai host bastion. Anda dapat menggunakan atribut ID citra instans atau atribut nilai Tanda, tergantung kriteria yang dapat diidentifikasi dengan instans yang meng-host alat ini. Contoh di bawah ini merupakan filter yang akan Anda gunakan untuk menekan tipe temuan ini berdasarkan instans dengan kunci tanda instans tertentu di konsol.

```
Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
```

## Aturan penekanan yang direkomendasikan untuk temuan Runtime Monitoring

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) dihasilkan ketika proses di dalam wadah berkomunikasi dengan soket Docker. Mungkin ada wadah di lingkungan Anda yang mungkin perlu mengakses soket Docker untuk alasan yang sah. Akses dari wadah tersebut akan menghasilkan `PrivilegeEscalation:Runtime/DockerSocketAccessed` temuan. Jika ini adalah kasus di AWS lingkungan Anda, kami sarankan Anda menyiapkan aturan penekanan untuk jenis temuan ini. Kriteria pertama harus menggunakan bidang Jenis Finding dengan nilai sama dengan `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Kriteria filter kedua adalah bidang jalur yang dapat dieksekusi dengan nilai yang sama dengan proses `executablePath` dalam temuan yang dihasilkan. Atau, kriteria filter kedua dapat menggunakan bidang Executable SHA -256 dengan nilai yang sama dengan proses `executableSha256` dalam temuan yang dihasilkan.
- Cluster Kubernetes menjalankan DNS server mereka sendiri sebagai pod, seperti. `coredns` Oleh karena itu, untuk setiap DNS pencarian dari sebuah pod, GuardDuty menangkap dua DNS



peristiwa — satu dari pod dan yang lainnya dari pod server. Ini dapat menghasilkan duplikat untuk DNS temuan berikut:

- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

Temuan duplikat akan mencakup pod, container, dan detail proses yang sesuai dengan pod DNS server Anda. Anda dapat membuat aturan penindasan untuk menekan temuan duplikat ini menggunakan bidang ini. Kriteria filter pertama harus menggunakan bidang Jenis Finding dengan nilai sama dengan tipe DNS temuan dari daftar temuan yang disediakan sebelumnya di bagian ini. Kriteria filter kedua dapat berupa jalur Executable dengan nilai yang sama dengan DNS server Anda `executablePath` atau Executable SHA -256 dengan nilai yang sama dengan DNS server Anda dalam temuan yang dihasilkan. `executableSHA256` Sebagai kriteria filter ketiga opsional, Anda dapat menggunakan kolom image kontainer Kubernetes dengan nilai yang sama dengan image kontainer pod DNS server Anda dalam temuan yang dihasilkan.

## Membuat aturan penekanan


Pilih metode akses pilihan Anda untuk membuat aturan penekanan untuk GuardDuty menemukan tipe.

### Console

Anda dapat memvisualisasikan, membuat, dan mengelola aturan penekanan menggunakan konsol. GuardDuty Aturan penekanan dibuat dengan cara yang sama seperti filter, dan filter tersimpan yang ada dapat digunakan sebagai aturan penekanan. Untuk informasi selengkapnya [tentang membuat filter](#), lihat [Memfilter temuan](#).

Untuk membuat aturan penekanan menggunakan konsol:

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, pilih Menekan temuan untuk membuka panel aturan penekanan.
3. Untuk membuka menu kriteria filter, **filter criteria** masukkan kriteria Tambahkan filter. Anda dapat memilih kriteria dari daftar. Masukkan nilai yang valid untuk kriteria yang dipilih.

 Note

Untuk menentukan nilai yang valid, lihat tabel temuan dan pilih temuan yang ingin Anda tekan. Tinjau detailnya di panel temuan.

Anda dapat menambahkan beberapa kriteria filter dan memastikan bahwa hanya temuan tersebut yang muncul di tabel yang ingin Anda tekan.

4. Masukkan Nama dan Deskripsi untuk aturan penindasan. Karakter yang valid termasuk karakter alfanumerik, periode (.), tanda hubung (-), garis bawah (\_), dan spasi putih.
5. Pilih Simpan.

Anda juga dapat membuat aturan penekanan dari filter tersimpan yang ada. Untuk informasi selengkapnya tentang membuat filter, lihat [Memfilter temuan](#).

Untuk membuat aturan penekanan dari filter tersimpan:

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, pilih Menekan Temuan untuk membuka panel aturan penekanan.
3. Dari tarik-turun Aturan tersimpan, pilih filter yang disimpan.
4. Anda juga dapat menambahkan kriteria filter baru. Jika Anda tidak memerlukan kriteria filter tambahan, lewati langkah ini.

Untuk membuka menu kriteria filter, **filter criteria** masukkan kriteria Tambahkan filter. Anda dapat memilih kriteria dari daftar. Masukkan nilai yang valid untuk kriteria yang dipilih.

**Note**

Untuk menentukan nilai yang valid, lihat tabel temuan dan pilih temuan yang ingin Anda tekan. Tinjau detailnya di panel temuan.

5. Masukkan Nama dan Deskripsi untuk aturan penindasan. Karakter yang valid termasuk karakter alfanumerik, periode (.), tanda hubung (-), garis bawah (\_), dan spasi putih.
6. Pilih Simpan.

## API/CLI

Untuk membuat aturan penindasan menggunakan API:

1. Anda dapat membuat aturan penindasan melalui [CreateFilter](#) API Untuk melakukannya, tentukan kriteria filter dalam JSON file mengikuti format contoh yang dirinci di bawah ini. Contoh di bawah ini akan menekan temuan tingkat keparahan rendah yang tidak diarsipkan yang memiliki DNS permintaan ke domain test.example.com. Untuk temuan tingkat keparahan sedang, daftar masukan adalah ["4", "5", "7"]. Untuk temuan tingkat keparahan tinggi, daftar masukan adalah ["6", "7", "8"]. Anda juga dapat memfilter berdasarkan satu nilai dalam daftar.

```
{
  "Criterion": {
    "service.archived": {
      "Eq": [
        "false"
      ]
    },
    "service.action.dnsRequestAction.domain": {
      "Eq": [
        "test.example.com"
      ]
    },
    "severity": {
      "Eq": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

```
}  
  }  
}
```

Untuk daftar nama JSON bidang dan padanan konsol mereka lihat [Atribut filter](#).

Untuk menguji kriteria filter Anda, gunakan JSON kriteria yang sama di [ListFindingsAPI](#), dan konfirmasi bahwa temuan yang benar telah dipilih. Untuk menguji kriteria filter Anda menggunakan AWS CLI ikuti contoh menggunakan file Anda sendiri detectorId dan .json.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
finding-criteria file://criteria.json
```

2. Unggah filter Anda untuk digunakan sebagai aturan penekanan dengan [CreateFilterAPI](#) atau dengan menggunakan contoh AWS CLI berikut ini dengan ID detektor Anda sendiri, nama untuk aturan penekanan, dan file.json.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

```
aws guardduty create-filter --action ARCHIVE --detector-  
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria  
file://criteria.json
```

Anda dapat melihat daftar filter Anda secara terprogram dengan file. [ListFilterAPI](#) Anda dapat melihat detail filter individual dengan memberikan nama filter ke file. [GetFilterAPI](#) Perbarui filter menggunakan [UpdateFilter](#) atau menghapusnya dengan file [DeleteFilterAPI](#).

## Menghapus aturan penekanan

Pilih metode akses pilihan Anda untuk menghapus aturan penekanan untuk GuardDuty menemukan jenis.

## Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada halaman Temuan, pilih Menekan Temuan untuk membuka panel aturan penekanan.
3. Dari tarik-turun Aturan tersimpan, pilih filter yang disimpan.
4. Pilih Hapus aturan.

## API/CLI

Jalankan [DeleteFilter](#) API. Tentukan nama filter dan ID detektor terkait untuk Wilayah tertentu.

Atau, Anda dapat menggunakan AWS CLI contoh berikut dengan mengganti nilai yang diformat *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

## Bekerja dengan daftar IP tepercaya dan daftar ancaman

Amazon GuardDuty memantau keamanan AWS lingkungan Anda dengan menganalisis dan memproses Log VPC Aliran, log AWS CloudTrail peristiwa, dan DNS log. Anda dapat menyesuaikan lingkup pemantauan ini dengan mengonfigurasi GuardDuty untuk menghentikan peringatan untuk dipercaya IPs dari daftar IP tepercaya Anda sendiri dan memperingatkan tentang bahaya yang diketahui IPs dari daftar ancaman Anda sendiri.

Daftar IP tepercaya dan daftar ancaman hanya berlaku untuk lalu lintas yang ditujukan untuk alamat IP yang dapat dirutekan secara publik. Efek dari daftar berlaku untuk semua VPC Flow Log dan CloudTrail temuan, tetapi tidak berlaku untuk DNS temuan.

GuardDuty dapat dikonfigurasi untuk menggunakan jenis daftar berikut.

### Daftar IP tepercaya

Daftar IP tepercaya terdiri dari alamat IP yang telah Anda percayai untuk komunikasi yang aman dengan AWS infrastruktur dan aplikasi Anda. GuardDuty tidak menghasilkan log VPC aliran atau

CloudTrail temuan untuk alamat IP pada daftar IP tepercaya. Anda dapat menyertakan maksimum 2000 alamat IP dan CIDR rentang dalam satu daftar IP tepercaya. Pada waktu tertentu, Anda hanya dapat memiliki satu daftar IP tepercaya yang diunggah per akun AWS per Wilayah.

## Daftar IP ancaman

Daftar ancaman terdiri dari alamat IP berbahaya yang diketahui. Daftar ini dapat disediakan oleh intelijen ancaman pihak ketiga atau dibuat khusus untuk organisasi Anda. Selain menghasilkan temuan karena aktivitas yang berpotensi mencurigakan, GuardDuty juga menghasilkan temuan berdasarkan daftar ancaman ini. Anda dapat menyertakan maksimum 250.000 alamat IP dan CIDR rentang dalam satu daftar ancaman. GuardDuty hanya menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP dan CIDR rentang dalam daftar ancaman Anda; temuan tidak dihasilkan berdasarkan nama domain. Pada titik waktu tertentu, Anda dapat memiliki hingga enam daftar ancaman yang diunggah Akun AWS per setiap Wilayah.

### Note

Jika Anda menyertakan IP yang sama pada daftar IP tepercaya dan daftar ancaman, IP tersebut akan diproses oleh daftar IP tepercaya terlebih dahulu, dan tidak akan menghasilkan temuan.

Di lingkungan multi-akun, hanya pengguna dari akun akun GuardDuty administrator yang dapat menambahkan dan mengelola daftar IP tepercaya dan daftar ancaman. Daftar IP tepercaya dan daftar ancaman yang diunggah oleh akun akun administrator dikenakan pada GuardDuty fungsionalitas di akun anggotanya. Dengan kata lain, di akun anggota GuardDuty menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP berbahaya yang diketahui dari daftar ancaman akun administrator dan tidak menghasilkan temuan berdasarkan aktivitas yang melibatkan alamat IP dari daftar IP tepercaya akun administrator. Untuk informasi selengkapnya, lihat [Mengelola banyak akun di Amazon GuardDuty](#).

## Format daftar

GuardDuty menerima daftar dalam format berikut.

Ukuran maksimum setiap file yang menghosting daftar IP tepercaya atau daftar IP ancaman Anda adalah 35MB. Dalam daftar IP tepercaya dan daftar IP ancaman Anda, alamat IP dan CIDR rentang harus muncul satu per baris. Hanya IPv4 alamat yang diterima.

- Plaintext () TXT

Format ini mendukung CIDR blok dan alamat IP individual. Daftar contoh berikut menggunakan format Plaintext (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Ekspresi Informasi Ancaman Terstruktur (STIX)

Format ini mendukung CIDR blok dan alamat IP individual. Daftar contoh berikut menggunakan STIX format.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:ttp="http://stix.mitre.org/TTP-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
    stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
    campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
    indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
    default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
    objects/Address/2.1/Address_Object.xsd"
  id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
  version="1.2">
  <stix:Observables cybox_major_version="1" cybox_minor_version="1">
    <cybox:Observable id="example:observable-80b26f43-
    dc41-43ff-861d-19aff31e0236">
      <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
```

```

        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">

  <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
    </cybox:Properties>
  </cybox:Object>
</cybox:Observable>
<cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
  <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
    <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
      <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </cybox:Observable>
  <cybox:Observable
id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
    <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
      <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
        <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
          </cybox:Properties>
        </cybox:Object>
      </cybox:Observable>
    </stix:Observables>
  </stix:STIX_Package>

```

- Buka Pertukaran Ancaman (OTX)<sup>™</sup> CSV

Format ini mendukung CIDR blok dan alamat IP individual. Daftar contoh berikut menggunakan OTX<sup>™</sup> CSV format.

| Indicator type | Indicator    | Description |
|----------------|--------------|-------------|
| CIDR           | 192.0.2.0/24 | example     |
| IPv4           | 198.51.100.1 | example     |
| IPv4           | 203.0.113.1  | example     |

- FireEye<sup>™</sup> dan Kecerdasan SIGHT Ancaman CSV





Format ini hanya mendukung alamat IP individual. Daftar contoh berikut menggunakan AlienVault format.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

## Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman

Berbagai IAM identitas memerlukan izin khusus untuk bekerja dengan daftar IP terpercaya dan daftar ancaman di GuardDuty Identitas dengan kebijakan [AmazonGuardDutyFullAccess](#) terkelola terlampir hanya dapat mengganti nama dan menonaktifkan daftar IP terpercaya yang diunggah dan daftar ancaman.

Untuk memberikan berbagai identitas akses penuh untuk bekerja dengan daftar IP terpercaya dan daftar ancaman (selain mengganti nama dan menonaktifkan, ini termasuk menambahkan, mengaktifkan, menghapus, dan memperbarui lokasi atau nama daftar), pastikan bahwa tindakan berikut ada dalam kebijakan izin yang dilampirkan ke pengguna, grup, atau peran:

```
{
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

### Important

Tindakan ini tidak termasuk dalam kebijakan yang AmazonGuardDutyFullAccess dikelola.

## Menggunakan enkripsi sisi server untuk daftar IP tepercaya dan daftar ancaman

GuardDuty mendukung jenis enkripsi berikut untuk daftar: SSE - AES256 dan SSE -KMS. SSE-C tidak didukung. Untuk informasi selengkapnya tentang jenis enkripsi untuk S3, lihat [Melindungi data menggunakan enkripsi sisi server](#).

Jika daftar Anda dienkripsi menggunakan enkripsi sisi server SSE - KMS Anda harus memberikan AWSServiceRoleForAmazonGuardDutyizin peran GuardDuty terkait layanan untuk mendekripsi file untuk mengaktifkan daftar. Tambahkan pernyataan berikut ke kebijakan KMS kunci dan ganti ID akun dengan milik Anda sendiri:

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guarddduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

## Menambahkan dan mengaktifkan daftar IP tepercaya atau daftar IP ancaman

Pilih salah satu metode akses berikut untuk menambahkan dan mengaktifkan daftar IP tepercaya atau daftar IP ancaman.

### Console

(Opsional) langkah 1: Mengambil lokasi URL daftar Anda

1. Buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Di panel navigasi, pilih Bucket.
3. Pilih nama bucket Amazon S3 yang berisi daftar spesifik yang ingin Anda tambahkan.
4. Pilih nama objek (daftar) untuk melihat detailnya.
5. Di bawah tab Properties, salin S3 URI untuk objek ini.

## Langkah 2: Menambahkan daftar IP tepercaya atau daftar ancaman

### Important

Secara default, pada titik waktu tertentu, Anda hanya dapat memiliki satu daftar IP tepercaya. Demikian pula, Anda dapat memiliki hingga enam daftar ancaman.

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih Tambahkan daftar IP tepercaya atau Tambahkan daftar ancaman.
4. Berdasarkan pilihan Anda, kotak dialog akan muncul. Lakukan langkah-langkah berikut:
  - a. Untuk nama Daftar, masukkan nama untuk daftar Anda.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (\_).

- b. Untuk Lokasi, berikan lokasi tempat Anda mengunggah daftar Anda. Jika Anda belum memilikinya, lihat [Step 1: Fetching location URL of your list](#).

#### Format lokasi URL

- <https://s3.amazonaws.com/bucket.name/file.txt>
  - <https://s3-aws-region.amazonaws.com/bucket.name/file.txt>
  - <http://bucket.s3.amazonaws.com/file.txt>
  - <http://bucket.s3-aws-region.amazonaws.com/file.txt>
  - <s3://bucket.name/file.txt>
- c. Pilih kotak centang Saya setuju.
  - d. Pilih Tambah daftar. Secara default, Status daftar yang ditambahkan tidak aktif. Agar daftar menjadi efektif, Anda harus mengaktifkan daftar.

## Langkah 3: Mengaktifkan daftar IP tepercaya atau daftar ancaman

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.

3. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda aktifkan.
4. Pilih Tindakan, lalu pilih Aktifkan. Mungkin diperlukan waktu hingga 15 menit agar daftar menjadi efektif.

## API/CLI

### Untuk daftar IP tepercaya

- Jalankan [CreateIPSet](#). Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar IP tepercaya ini.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (\_).

- Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut dan pastikan untuk mengganti `detector-id` dengan ID detektor dari akun anggota yang akan Anda perbarui daftar IP tepercaya.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

### Untuk daftar ancaman

- Jalankan [CreateThreatIntelSet](#). Pastikan untuk memberikan akun `detectorId` anggota yang ingin Anda buat daftar ancaman ini.
- Atau, Anda dapat melakukan ini dengan menjalankan AWS Command Line Interface perintah berikut. Pastikan untuk memberikan akun anggota yang ingin Anda buat daftar ancaman. `detectorId`

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/amzn-s3-demo-bucket2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

**Note**

Setelah Anda mengaktifkan atau memperbarui daftar IP apa pun, GuardDuty mungkin memerlukan waktu hingga 15 menit untuk menyinkronkan daftar.

## Memperbarui daftar IP tepercaya dan daftar ancaman

Anda dapat memperbarui nama daftar atau alamat IP yang ditambahkan ke daftar yang telah ditambahkan dan diaktifkan. Jika Anda memperbarui daftar, Anda harus mengaktifkannya lagi GuardDuty untuk menggunakan versi terbaru dari daftar.

Pilih salah satu metode akses untuk memperbarui IP tepercaya atau daftar ancaman.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih kumpulan IP tepercaya atau daftar ancaman yang ingin Anda perbarui.
4. Pilih Tindakan, dan kemudian pilih Edit.
5. Dalam kotak dialog Perbarui daftar, perbarui informasi sesuai kebutuhan.

Kendala penamaan daftar — Nama daftar Anda dapat mencakup huruf kecil, huruf besar, angka, tanda hubung (-), dan garis bawah (\_).

6. Pilih kotak centang Saya setuju, lalu pilih Perbarui daftar. Nilai di kolom Status akan berubah menjadi Tidak Aktif.
7. Mengaktifkan kembali daftar yang diperbarui
  - a. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda aktifkan lagi.
  - b. Pilih Tindakan, lalu pilih Aktifkan.

### API/CLI

1. Jalankan [UpdateIPSet](#) untuk memperbarui daftar IP tepercaya.

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP tepercaya.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

## 2. Jalankan [UpdateThreatIntelSet](#) untuk memperbarui daftar ancaman

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar ancaman dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar ancaman.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

## Menonaktifkan atau menghapus daftar IP tepercaya atau daftar ancaman

Pilih salah satu metode akses untuk menghapus (dengan menggunakan konsol) atau menonaktifkan (dengan menggunakan API/CLI) daftar IP tepercaya, atau daftar ancaman.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Di panel navigasi, pilih Daftar.
3. Pada halaman Manajemen daftar, pilih daftar yang ingin Anda hapus.
4. Pilih Tindakan, lalu pilih Hapus.
5. Konfirmasikan tindakan dan pilih Hapus. Daftar spesifik tidak akan lagi tersedia di tabel.

### API/CLI

1. Untuk daftar IP tepercaya

Jalankan [UpdateIPSet](#) untuk memperbarui daftar IP tepercaya.

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar IP tepercaya.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#).  
`detectorId`

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
--name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

## 2. Untuk daftar ancaman

Jalankan [UpdateThreatIntelSet](#) untuk memperbarui daftar ancaman

- Atau, Anda dapat menjalankan AWS CLI perintah berikut untuk memperbarui daftar IP tepercaya dan pastikan untuk mengganti `detector-id` dengan ID detektor akun anggota yang akan Anda perbarui daftar ancaman.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

## Mengekspor temuan

GuardDuty mempertahankan temuan yang dihasilkan untuk jangka waktu 90 hari. GuardDuty mengeksport temuan aktif ke Amazon EventBridge (EventBridge). Anda dapat secara opsional mengeksport temuan yang dihasilkan ke bucket Amazon Simple Storage Service (Amazon S3). Ini akan membantu Anda melacak data historis aktivitas yang berpotensi mencurigakan di akun Anda dan mengevaluasi apakah langkah-langkah perbaikan yang disarankan berhasil.

Setiap temuan aktif baru yang GuardDuty dihasilkan secara otomatis diekspor dalam waktu sekitar 5 menit setelah temuan dihasilkan. Anda dapat mengatur frekuensi seberapa sering pembaruan temuan aktif diekspor ke EventBridge. Frekuensi yang Anda pilih berlaku untuk mengeksport kemunculan baru temuan yang ada ke EventBridge, bucket S3 Anda (saat dikonfigurasi), dan Detektif (saat terintegrasi). Untuk informasi tentang bagaimana GuardDuty menggabungkan beberapa kejadian temuan yang ada, lihat. [GuardDuty menemukan agregasi](#)



Saat mengonfigurasi setelan untuk mengekspor temuan ke bucket Amazon S3, GuardDuty gunakan AWS Key Management Service (AWS KMS) untuk mengenkripsi data temuan di bucket S3. Ini mengharuskan Anda untuk menambahkan izin ke bucket S3 dan AWS KMS kuncinya sehingga GuardDuty dapat menggunakannya untuk mengekspor temuan di akun Anda.

## Daftar Isi

- [Pertimbangan](#)
- [Langkah 1 - Izin diperlukan untuk mengekspor temuan](#)
- [Langkah 2 — Melampirkan kebijakan ke kunci Anda KMS](#)
- [Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3](#)
- [Langkah 4 - Mengekspor temuan ke bucket S3 \(Konsol\)](#)
- [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#)

## Pertimbangan

Sebelum melanjutkan dengan prasyarat dan langkah-langkah untuk mengekspor temuan, pertimbangkan konsep-konsep kunci berikut:

- Pengaturan ekspor bersifat regional - Anda perlu mengonfigurasi opsi ekspor di setiap Wilayah tempat Anda menggunakan GuardDuty.
- Mengekspor temuan ke bucket Amazon S3 di Wilayah AWS berbagai (Lintas wilayah) GuardDuty — mendukung pengaturan ekspor berikut:
  - Bucket atau objek Amazon S3 Anda, dan AWS KMS kunci harus milik yang sama. Wilayah AWS
  - Untuk temuan yang dihasilkan di Wilayah komersial, Anda dapat memilih untuk mengekspor temuan ini ke ember S3 di Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan ini ke bucket S3 di Wilayah keikutsertaan.
  - Untuk temuan yang dihasilkan di Wilayah keikutsertaan, Anda dapat memilih untuk mengekspor temuan ini ke Wilayah keikutsertaan yang sama di mana mereka dihasilkan atau Wilayah komersial mana pun. Namun, Anda tidak dapat mengekspor temuan dari satu Wilayah keikutsertaan ke Wilayah keikutsertaan lainnya.
- Izin untuk mengekspor temuan — Untuk mengonfigurasi pengaturan untuk mengekspor temuan aktif, bucket S3 Anda harus memiliki izin yang memungkinkan GuardDuty untuk mengunggah objek. Anda juga harus memiliki AWS KMS kunci yang GuardDuty dapat digunakan untuk mengenkripsi temuan.

- Temuan yang diarsipkan tidak diekspor — Perilaku default adalah bahwa temuan yang diarsipkan, termasuk contoh baru dari temuan yang ditekan, tidak diekspor.

Ketika sebuah GuardDuty temuan dihasilkan sebagai Diarsipkan, Anda harus Membatalkan pengarsipannya. Ini mengubah status pencarian Filter menjadi Aktif. GuardDuty mengekspor pembaruan ke temuan yang tidak diarsipkan yang ada berdasarkan cara Anda mengonfigurasi.

#### [Langkah 5 - Frekuensi untuk mengekspor temuan](#)

- GuardDuty Akun administrator dapat mengekspor temuan yang dihasilkan di akun anggota terkait — Saat Anda mengonfigurasi temuan ekspor di akun administrator, semua temuan dari akun anggota terkait yang dihasilkan di Wilayah yang sama juga diekspor ke lokasi yang sama dengan yang Anda konfigurasi untuk akun administrator. Untuk informasi selengkapnya, lihat [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#).

## Langkah 1 - Izin diperlukan untuk mengekspor temuan

Saat mengonfigurasi setelan untuk mengekspor temuan, Anda memilih bucket Amazon S3 tempat Anda dapat menyimpan temuan dan kunci AWS KMS yang akan digunakan untuk enkripsi data. Selain izin untuk GuardDuty tindakan, Anda juga harus memiliki izin untuk tindakan berikut agar berhasil mengonfigurasi pengaturan untuk mengekspor temuan:

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`


## Langkah 2 — Melampirkan kebijakan ke kunci Anda KMS

GuardDuty mengenkripsi data temuan di bucket Anda dengan menggunakan AWS Key Management Service. Agar berhasil mengkonfigurasi pengaturan, Anda harus terlebih dahulu memberikan GuardDuty izin untuk menggunakan KMS kunci. Anda dapat memberikan izin dengan [melampirkan kebijakan ke kunci](#) Anda KMS.

Saat Anda menggunakan KMS kunci dari akun lain, Anda perlu menerapkan kebijakan kunci dengan masuk ke Akun AWS yang memiliki kunci tersebut. Saat mengonfigurasi pengaturan untuk mengekspor temuan, Anda juga memerlukan kunci ARN dari akun yang memiliki kunci tersebut.

Untuk mengubah kebijakan KMS utama GuardDuty untuk mengenkripsi temuan yang diekspor

1. Buka AWS KMS konsol di <https://console.aws.amazon.com/kms>.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pilih KMS kunci yang ada atau lakukan langkah-langkah untuk [Membuat kunci baru](#) di Panduan AWS Key Management Service Pengembang, yang akan Anda gunakan untuk mengenkripsi temuan yang diekspor.

 Note

KMSKunci Anda dan ember Amazon S3 harus sama. Wilayah AWS

Anda dapat menggunakan bucket S3 dan KMS key pair yang sama untuk mengekspor temuan dari Wilayah mana pun yang berlaku. Untuk informasi selengkapnya, lihat [Pertimbangan](#) untuk mengekspor temuan di seluruh Wilayah.

4. Di bagian Kebijakan kunci, pilih Edit.

Jika Beralih ke tampilan kebijakan ditampilkan, pilih untuk menampilkan Kebijakan kunci, lalu pilih Edit.

5. Salin blok kebijakan berikut ke kebijakan KMS kunci Anda, untuk memberikan GuardDuty izin untuk menggunakan kunci Anda.

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

6. Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:
  1. Ganti *KMS key ARN* dengan Nama Sumber Daya Amazon (ARN) dari KMS kuncinya. Untuk menemukan kunci ARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan AWS Key Management Service Pengembang.
  2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksport temuan.
  3. Ganti *Region2* dengan di Wilayah AWS mana GuardDuty temuan dihasilkan.
  4. Ganti *SourceDetectorID* dengan `detectorID` GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/> konsol, atau jalankan [ListDetectors](#) API. `detectorId`

#### Note

Jika Anda menggunakan GuardDuty di Wilayah keikutsertaan, ganti nilai untuk "Layanan" dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti dengan. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Untuk informasi tentang titik akhir untuk setiap Wilayah keikutsertaan, lihat [GuardDuty titik akhir](#) dan kuota.

7. Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa JSON sintaks kebijakan KMS kunci Anda valid.

Pilih Simpan.

8. (Opsional) salin kunci ARN ke notepad untuk digunakan pada langkah selanjutnya.

## Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3

Tambahkan izin ke bucket Amazon S3 tempat Anda akan mengeksport temuannya GuardDuty sehingga dapat mengunggah objek ke bucket S3 ini. Terlepas dari penggunaan bucket Amazon S3 milik akun Anda atau yang berbeda Akun AWS, Anda harus menambahkan izin ini.

Jika suatu saat, Anda memutuskan untuk mengekspor temuan ke bucket S3 yang berbeda, lalu untuk melanjutkan mengekspor temuan, Anda harus menambahkan izin ke bucket S3 tersebut dan mengonfigurasi pengaturan temuan ekspor lagi.

Jika Anda belum memiliki bucket Amazon S3 tempat Anda ingin mengekspor temuan ini, lihat [Membuat bucket](#) di Panduan Pengguna Amazon S3.

## Untuk melampirkan izin ke kebijakan bucket S3 Anda

1. Lakukan langkah-langkah di bawah [Untuk membuat atau mengedit kebijakan bucket](#) di Panduan Pengguna Amazon S3, hingga halaman Edit kebijakan bucket muncul.
2. Kebijakan contoh menunjukkan cara memberikan GuardDuty izin untuk mengekspor temuan ke bucket Amazon S3 Anda. Jika Anda mengubah jalur setelah mengonfigurasi temuan ekspor, Anda harus mengubah kebijakan untuk memberikan izin ke lokasi baru.

Salin contoh kebijakan berikut dan tempelkan ke editor kebijakan Bucket.

Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan bahwa JSON sintaks kebijakan KMS kunci Anda valid.

### Kebijakan contoh bucket S3

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGuardDutygetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": "Amazon S3 bucket ARN",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn":
            "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowGuardDutyPutObject",
    "Effect": "Allow",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012",
        "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
      }
    }
  },
  {
    "Sid": "DenyUnencryptedUploadsThis is optional",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "aws:kms"
      }
    }
  },
  {
    "Sid": "DenyIncorrectHeaderThis is optional",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
    "Condition": {

```

```

        "StringNotEquals": {
            "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
        }
    },
    {
        "Sid": "DenyNon-HTTPS",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    }
]
}

```

3. Edit kebijakan dengan mengganti nilai berikut yang diformat *red* dalam contoh kebijakan:

1. Ganti *Amazon S3 bucket ARN* dengan Nama Sumber Daya Amazon (ARN) dari ember Amazon S3. Anda dapat menemukan Bucket ARN di halaman kebijakan Edit bucket di <https://console.aws.amazon.com/s3/konsol>.
2. Ganti *123456789012* dengan Akun AWS ID yang memiliki GuardDuty akun yang mengeksport temuan.
3. Ganti *Region2* dengan di Wilayah AWS mana GuardDuty temuan dihasilkan.
4. Ganti *SourceDetectorID* dengan detectorID GuardDuty akun di Wilayah tertentu tempat temuan dihasilkan.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectorsAPI](#). detectorId

5. Ganti *[optional prefix]* bagian dari *S3 bucket ARN/[optional prefix]* nilai placeholder dengan lokasi folder opsional yang ingin Anda ekspor temuannya. Untuk informasi selengkapnya tentang penggunaan awalan, lihat [Mengatur objek menggunakan awalan](#) di Panduan Pengguna Amazon S3.

Bila Anda menyediakan lokasi folder opsional yang belum ada, GuardDuty akan membuat lokasi tersebut hanya jika akun yang terkait dengan bucket S3 sama dengan akun yang

mengekspor temuan. Saat Anda mengekspor temuan ke bucket S3 milik akun lain, lokasi folder harus sudah ada.

6. Ganti *KMS key ARN* dengan Amazon Resource Name (ARN) dari KMS kunci yang terkait dengan enkripsi temuan yang diekspor ke bucket S3. Untuk menemukan kunciARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan AWS Key Management Service Pengembang.

#### Note

Jika Anda menggunakan GuardDuty di Wilayah keikutsertaan, ganti nilai untuk “Layanan” dengan titik akhir Regional untuk Wilayah tersebut. Misalnya, jika Anda menggunakan GuardDuty di Wilayah Timur Tengah (Bahrain) (me-south-1), ganti dengan.  
"Service": "guardduty.amazonaws.com" "Service": "guardduty.me-south-1.amazonaws.com" Untuk informasi tentang titik akhir untuk setiap Wilayah keikutsertaan, lihat [GuardDuty titik akhir](#) dan kuota.

4. Pilih Simpan.

## Langkah 4 - Mengekspor temuan ke bucket S3 (Konsol)

GuardDuty memungkinkan Anda untuk mengekspor temuan ke ember yang ada di ember lain Akun AWS.

Saat membuat bucket S3 baru atau memilih bucket yang ada di akun Anda, Anda dapat menambahkan awalan opsional. Saat mengonfigurasi temuan ekspor, GuardDuty buat folder baru di bucket S3 untuk temuan Anda. Awalan akan ditambahkan ke struktur folder default yang GuardDuty dibuat. Misalnya, format awalan `/AWSLogs/123456789012/GuardDuty/Region` opsional.

Seluruh jalur objek S3 akan menjadi `amzn-s3-demo-bucket/prefix-name/UUID.json.gz`. UUID ini dihasilkan secara acak dan tidak mewakili ID detektor atau ID temuan.

#### Important

KMSKunci dan ember S3 harus berada di Wilayah yang sama.

Sebelum menyelesaikan langkah-langkah ini, pastikan Anda telah melampirkan kebijakan masing-masing ke KMS kunci dan bucket S3 yang ada.



Untuk mengonfigurasi temuan ekspor

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman Pengaturan, di bawah opsi ekspor temuan, untuk bucket S3, pilih Konfigurasi sekarang (atau Edit, sesuai kebutuhan).
4. Untuk ember S3 ARN, masukkan **bucket ARN** Untuk menemukan bucketARN, lihat [Melihat properti untuk bucket S3 di Panduan](#) Pengguna Amazon S3. Di tab Izin pada halaman Properti bucket terkait di <https://console.aws.amazon.com/guardduty/konsol>.
5. Untuk KMSkunci ARN, masukkan **key ARN**. Untuk menemukan kunciARN, lihat [Menemukan ID kunci dan ARN](#) di Panduan AWS Key Management Service Pengembang.
6. Lampirkan kebijakan
  - Lakukan langkah-langkah untuk melampirkan kebijakan bucket S3. Untuk informasi selengkapnya, lihat [Langkah 3 - Melampirkan kebijakan ke bucket Amazon S3](#).
  - Lakukan langkah-langkah untuk melampirkan kebijakan KMS utama. Untuk informasi selengkapnya, lihat [Langkah 2 — Melampirkan kebijakan ke kunci Anda KMS](#).
7. Pilih Simpan.

## Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui

Konfigurasi frekuensi untuk mengekspor temuan aktif yang diperbarui sesuai dengan lingkungan Anda. Secara default, temuan yang diperbarui diekspor setiap 6 jam. Ini berarti bahwa setiap temuan yang diperbarui setelah ekspor terbaru akan disertakan dalam ekspor berikutnya. Jika temuan yang diperbarui diekspor setiap 6 jam dan ekspor dilakukan pada pukul 12:00, setiap temuan yang Anda perbarui setelah pukul 12:00 akan diekspor pada pukul 18:00.

Untuk mengatur frekuensi

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pilih Pengaturan.

3. Di bagian Opsi ekspor temuan, pilih Frekuensi untuk temuan yang diperbarui. Ini menetapkan frekuensi untuk mengekspor temuan Aktif yang diperbarui ke keduanya EventBridge dan Amazon S3. Anda dapat memilih dari opsi berikut:
  - Perbarui EventBridge dan S3 setiap 15 menit
  - Update EventBridge dan S3 setiap 1 jam
  - Perbarui CWE dan S3 setiap 6 jam (default)
4. Pilih Simpan perubahan.

## Membuat tanggapan khusus terhadap GuardDuty temuan dengan Amazon CloudWatch Events

GuardDuty membuat acara untuk [CloudWatch Acara Amazon](#) ketika ada perubahan dalam temuan terjadi. Menemukan perubahan yang akan menciptakan suatu CloudWatch peristiwa termasuk temuan yang baru dihasilkan atau temuan agregat yang baru. Peristiwa dipancarkan atas dasar upaya terbaik.

Setiap GuardDuty temuan diberi ID temuan. GuardDuty membuat CloudWatch acara untuk setiap temuan dengan ID temuan unik. Semua peristiwa berikutnya dari temuan yang ada digabungkan ke temuan asli. Untuk informasi selengkapnya, lihat [GuardDuty menemukan agregasi](#).

### Note

Jika akun Anda adalah administrator yang GuardDuty didelegasikan, CloudWatch acara akan dipublikasikan ke akun Anda serta ke akun anggota tempat temuan itu dihasilkan.

Dengan menggunakan CloudWatch peristiwa dengan GuardDuty, Anda dapat mengotomatiskan tugas untuk membantu Anda menanggapi masalah keamanan yang diungkapkan oleh GuardDuty temuan.

Untuk menerima pemberitahuan tentang GuardDuty temuan berdasarkan CloudWatch Acara, Anda harus membuat aturan CloudWatch Acara dan target untuk GuardDuty. Aturan ini memungkinkan CloudWatch untuk mengirim pemberitahuan untuk temuan yang GuardDuty menghasilkan target yang ditentukan dalam aturan. Untuk informasi selengkapnya, lihat [Membuat aturan dan target CloudWatch Acara untuk GuardDuty \(CLI\)](#).

## Topik

- [CloudWatch Frekuensi pemberitahuan acara untuk GuardDuty](#)
- [CloudWatch format acara untuk GuardDuty](#)
- [Membuat aturan CloudWatch Acara untuk memberi tahu Anda tentang GuardDuty temuan \(konsol\)](#)
- [Membuat aturan dan target CloudWatch Acara untuk GuardDuty \(CLI\)](#)
- [CloudWatch Acara untuk lingkungan GuardDuty multi-akun](#)

## CloudWatch Frekuensi pemberitahuan acara untuk GuardDuty

Pemberitahuan untuk temuan baru yang dihasilkan dengan ID temuan unik

GuardDuty mengirimkan pemberitahuan berdasarkan CloudWatch acaranya dalam waktu 5 menit setelah temuan. Peristiwa ini (dan notifikasi ini) juga mencakup semua kejadian berikutnya dari temuan ini yang berlangsung dalam 5 menit pertama sejak temuan dengan ID unik ini dihasilkan.

### Note

Secara default, frekuensi pemberitahuan tentang temuan yang baru dihasilkan adalah 5 menit. Frekuensi ini tidak dapat diperbarui.

Pemberitahuan untuk kejadian temuan selanjutnya

Secara default, untuk setiap temuan dengan ID temuan unik, GuardDuty menggabungkan semua kejadian berikutnya dari jenis temuan tertentu yang terjadi dalam interval 6 jam menjadi satu peristiwa tunggal. GuardDuty kemudian mengirimkan pemberitahuan tentang kejadian berikutnya berdasarkan acara ini. Secara default, untuk kejadian berikutnya dari temuan yang ada, GuardDuty mengirimkan pemberitahuan berdasarkan CloudWatch peristiwa setiap 6 jam.

Hanya akun administrator yang dapat menyesuaikan frekuensi default pemberitahuan yang dikirim tentang kejadian temuan berikutnya ke CloudWatch peristiwa. Pengguna dari akun anggota tidak dapat menyesuaikan frekuensi ini. Nilai frekuensi yang ditetapkan oleh akun administrator di akunnya sendiri dikenakan pada GuardDuty fungsionalitas di semua akun anggotanya. Jika pengguna dari akun administrator menetapkan nilai frekuensi ini menjadi 1 jam, semua akun anggota juga akan memiliki frekuensi 1 jam untuk menerima pemberitahuan tentang kejadian temuan berikutnya. Untuk informasi selengkapnya, lihat [Mengelola banyak akun di Amazon GuardDuty](#).

**Note**

Sebagai akun administrator, Anda dapat menyesuaikan frekuensi default pemberitahuan tentang kejadian temuan berikutnya. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. Untuk informasi tentang menyetel frekuensi notifikasi ini, lihat [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#).

## Memantau GuardDuty temuan yang diarsipkan dengan Acara CloudWatch

Untuk temuan yang diarsipkan secara manual, kejadian awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) dikirim ke CloudWatch Peristiwa per frekuensi yang dijelaskan di atas.

Untuk temuan yang diarsipkan secara otomatis, kejadian awal dan semua kejadian selanjutnya dari temuan ini (dihasilkan setelah pengarsipan selesai) tidak dikirim ke Acara. CloudWatch

## CloudWatch format acara untuk GuardDuty

CloudWatch [Acara](#) untuk GuardDuty memiliki format berikut.

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
  "detail-type": "GuardDuty Finding",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

**Note**

Nilai detail mengembalikan detail JSON dari temuan tunggal sebagai objek, daripada mengembalikan nilai "temuan" yang dapat mendukung beberapa temuan dalam array.

Untuk daftar lengkap semua parameter yang disertakan `GUARDDUTY_FINDING_JSON_OBJECT`, lihat [GetFindings](#). Parameter `id` yang muncul di `GUARDDUTY_FINDING_JSON_OBJECT` adalah ID temuan yang telah dijelaskan sebelumnya.

## Membuat aturan CloudWatch Acara untuk memberi tahu Anda tentang GuardDuty temuan (konsol)

Anda dapat menggunakan CloudWatch Events with GuardDuty untuk menyiapkan peringatan pencarian otomatis dengan mengirimkan peristiwa GuardDuty pencarian ke pusat pesan untuk membantu meningkatkan visibilitas GuardDuty temuan. Topik ini menunjukkan cara mengirim peringatan temuan ke email, Slack, atau Amazon Chime dengan menyiapkan topik SNS dan kemudian menghubungkan topik tersebut ke CloudWatch aturan acara Acara.

### Mengatur topik Amazon SNS dan titik akhir


Untuk memulai, Anda harus terlebih dahulu mengatur topik di Amazon Simple Notification Service dan menambahkan titik akhir. Untuk informasi selengkapnya, lihat [Memulai](#) di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Prosedur ini menetapkan di mana Anda ingin mengirim data GuardDuty pencarian. Topik SNS dapat ditambahkan ke aturan CloudWatch Acara Acara selama atau setelah pembuatan Aturan Acara.

#### Email setup

##### Membuat topik SNS

1. Masuk ke konsol Amazon SNS di <https://console.aws.amazon.com/sns/v3/home>.
2. Pilih Topik dari panel navigasi, lalu Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama Topik, misalnya **GuardDuty\_to\_Email**. Detail lainnya bersifat opsional.
4. Pilih Buat Topik. Detail Topik untuk topik baru Anda akan terbuka.
5. Di bagian Langganan, pilih Buat Langganan
6.
  - a. Dari menu Protokol, pilih Email.
  - b. Di bidang Titik Akhir, tambahkan alamat email untuk menerima notifikasi.

 Note

Anda akan diminta untuk mengonfirmasi langganan Anda melalui klien email Anda setelah membuatnya.

- c. Pilih Buat langganan
7. Periksa pesan langganan di kotak masuk Anda dan pilih Konfirmasi Langganan


## Slack setup

### Membuat topik SNS

1. Masuk ke konsol Amazon SNS di <https://console.aws.amazon.com/sns/v3/home>.
2. Pilih Topik dari panel navigasi, lalu Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama Topik, misalnya **GuardDuty\_to\_Slack**. Detail lainnya bersifat opsional. Pilih Buat topik untuk menyelesaikan.

### Mengonfigurasi klien AWS Chatbot

1. Navigasikan ke konsol AWS Chatbot
2. Dari panel Klien yang dikonfigurasi, pilih Konfigurasi klien baru.
3. Pilih Slack dan konfirmasi dengan "Konfigurasi".

 Note

Saat memilih Slack, Anda harus mengonfirmasi izin untuk AWS Chatbot agar dapat mengakses saluran Anda dengan memilih "izinkan".

4. Pilih Konfigurasi saluran baru untuk membuka panel detail konfigurasi.
  - a. Masukkan nama untuk saluran.
  - b. Untuk saluran Slack, pilih saluran yang ingin Anda gunakan. Untuk menggunakan saluran Slack pribadi dengan AWS Chatbot, pilih Saluran pribadi.
  - c. Di Slack, salin ID Saluran dari saluran pribadi dengan mengklik kanan pada nama saluran dan memilih Salin Tautan.

- d. Pada Konsol Manajemen AWS, di jendela AWS Chatbot, tempel ID yang Anda salin dari slack ke bidang ID saluran pribadi.
  - e. Pada bagian Izin, pilih untuk membuat IAM role menggunakan templat, jika Anda belum memiliki peran.
  - f. Untuk templat Kebijakan, pilih Izin notifikasi. Berikut adalah templat kebijakan IAM untuk AWS Chatbot. Ini memberikan izin baca dan daftar yang diperlukan untuk CloudWatch alarm, peristiwa dan log, dan untuk topik Amazon SNS.
  - g. Pilih Wilayah tempat Anda membuat topik SNS sebelumnya, lalu pilih topik Amazon SNS yang Anda buat untuk mengirim notifikasi ke saluran Slack.
5. Pilih Konfigurasi.

## Chime setup

### Membuat topik SNS

1. Masuk ke konsol Amazon SNS di <https://console.aws.amazon.com/sns/v3/home>.
2. Pilih Topik dari panel navigasi, lalu Buat Topik.
3. Di bagian Buat topik, pilih Standar. Selanjutnya, masukkan nama Topik, misalnya **GuardDuty\_to\_Chime**. Detail lainnya bersifat opsional. Pilih Buat topik untuk menyelesaikan.

### Mengonfigurasi klien AWS Chatbot

1. Navigasikan ke konsol AWS Chatbot
2. Dari panel Klien yang dikonfigurasi, pilih Konfigurasi klien baru.
3. Pilih Chime dan konfirmasi dengan "Konfigurasi".
4. Dari panel Detail konfigurasi, masukkan nama untuk saluran.
5. Di Chime, buka ruang obrolan yang diinginkan
  - a. Pilih ikon roda gigi di sudut kanan atas dan pilih Kelola webhook dan bot.
  - b. Pilih Salin URL untuk menyalin URL webhook ke clipboard Anda.
6. Pada Konsol Manajemen AWS, di jendela AWS Chatbot, tempel URL yang Anda salin ke bidang URL Webhook.

7. Pada bagian Izin, pilih untuk membuat IAM role menggunakan templat, jika Anda belum memiliki peran.
8. Untuk templat Kebijakan, pilih Izin notifikasi. Berikut adalah templat kebijakan IAM untuk AWS Chatbot. Ini memberikan izin baca dan daftar yang diperlukan untuk CloudWatch alarm, peristiwa dan log, dan untuk topik Amazon SNS.
9. Pilih Wilayah tempat Anda membuat topik SNS sebelumnya, lalu pilih topik Amazon SNS yang Anda buat untuk mengirim notifikasi ke ruang Chime.
10. Pilih Konfigurasi.

## Siapkan CloudWatch acara untuk GuardDuty temuan

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Aturan dari panel navigasi, lalu Buat Aturan.
3. Dari menu Nama Layanan, pilih GuardDuty.
4. Dari menu Event Type, pilih GuardDutyFinding.
5. Pada bagian Pratinjau Pola Peristiwa, pilih Edit.
6. Tempel kode JSON berikut ke Pratinjau Pola Peristiwa dan pilih Simpan

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
    ]
  }
}
```



5,  
5.0,  
5.1,  
5.2,  
5.3,  
5.4,  
5.5,  
5.6,  
5.7,  
5.8,  
5.9,  
6,  
6.0,  
6.1,  
6.2,  
6.3,  
6.4,  
6.5,  
6.6,  
6.7,  
6.8,  
6.9,  
7,  
7.0,  
7.1,  
7.2,  
7.3,  
7.4,  
7.5,  
7.6,  
7.7,  
7.8,  
7.9,  
8,  
8.0,  
8.1,  
8.2,  
8.3,  
8.4,  
8.5,  
8.6,  
8.7,  
8.8,  
8.9

```
]
}
}
```

**Note**

Kode di atas akan memberikan peringatan untuk setiap temuan dengan tingkat Medium hingga Tinggi.

7. Di bagian Target, klik Tambah Target.
8. Dari menu Pilih Target, pilih Topik SNS.
9. Untuk bagian Pilih Topik, pilih nama topik SNS yang Anda buat di Langkah 1.
10. Konfigurasi input untuk peristiwa tersebut.
  - Jika Anda mengatur notifikasi untuk Chime atau Slack, lewati ke Langkah 11, tipe input default untuk Peristiwa yang cocok.
  - Jika Anda mengatur notifikasi untuk email melalui SNS, ikuti langkah-langkah di bawah ini untuk menyesuaikan pesan yang dikirim ke kotak masuk menggunakan langkah-langkah berikut:
    - a. Perluas Konfigurasi input lalu pilih Transformer Input.
    - b. Salin kode berikut dan tempelkan ke bidang Jalur Input.

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

- c. Salin kode berikut dan tempelkan ke bidang Templat Input untuk memformat email.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
<Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Klik Konfigurasi Detail.
12. Pada halaman Konfigurasi detail aturan, masukkan Nama dan Deskripsi untuk aturan, lalu pilih Buat Aturan.

## Membuat aturan dan target CloudWatch Acara untuk GuardDuty (CLI)

Prosedur berikut menunjukkan cara menggunakan AWS CLI perintah untuk membuat aturan CloudWatch Events dan target untuk GuardDuty. Secara khusus, prosedur ini menunjukkan kepada Anda cara membuat aturan yang memungkinkan CloudWatch untuk mengirim peristiwa untuk semua temuan yang GuardDuty menghasilkan dan menambahkan AWS Lambda fungsi sebagai target aturan.

### Note

Selain fungsi Lambda, GuardDuty dan CloudWatch mendukung jenis target berikut: instans Amazon EC2, aliran Amazon Kinesis, AWS Step Functions tugas Amazon ECS, mesin status, perintah, dan target bawaan. `run`

Anda juga dapat membuat aturan dan target CloudWatch Acara GuardDuty melalui konsol CloudWatch Acara. Untuk informasi selengkapnya dan langkah-langkah mendetail, lihat [Membuat aturan CloudWatch Acara yang memicu peristiwa](#). Di bagian Sumber Daya Peristiwa, pilih **GuardDuty** untuk Nama layanan dan **GuardDuty Finding** untuk Tipe Peristiwa.

Untuk membuat aturan dan target

1. Untuk membuat aturan yang memungkinkan CloudWatch untuk mengirim peristiwa untuk semua temuan yang GuardDuty dihasilkan, jalankan perintah CloudWatch CLI berikut.

```
AWS events put-rule --name Test --event-pattern "{\"source\":
[\"aws.guardduty\"]}"
```

**⚠ Important**

Anda dapat menyesuaikan aturan Anda lebih lanjut sehingga menginstruksikan CloudWatch untuk mengirim peristiwa hanya untuk subset dari temuan GuardDuty yang dihasilkan. Subset ini didasarkan pada atribut temuan atau atribut yang ditentukan dalam aturan. Misalnya, gunakan perintah CLI berikut untuk membuat aturan yang memungkinkan CloudWatch untuk hanya mengirim peristiwa untuk GuardDuty temuan dengan tingkat keparahan 5 atau 8:

```
AWS events put-rule --name Test --event-pattern "{\"source\": [\"aws.guardduty\"], \"detail-type\": [\"GuardDuty Finding\"], \"detail\": {\"severity\": [5, 8]}}"
```

Untuk tujuan ini, Anda dapat menggunakan salah satu nilai properti yang tersedia di JSON untuk GuardDuty temuan.

2. Untuk melampirkan fungsi Lambda sebagai target untuk aturan yang Anda buat di langkah 1, jalankan perintah CLI berikut CloudWatch .

```
AWS events put-targets --rule Test --targets Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

**📘 Note**

Pastikan untuk mengganti <your\_function> perintah di atas dengan fungsi Lambda Anda yang sebenarnya untuk acara tersebut. GuardDuty

3. Untuk menambahkan izin yang diperlukan untuk memanggil target, jalankan perintah CLI Lambda berikut.

```
AWS lambda add-permission --function-name <your_function> --statement-id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

**📘 Note**

Pastikan untuk mengganti <your\_function> perintah di atas dengan fungsi Lambda Anda yang sebenarnya untuk acara tersebut. GuardDuty

**Note**

Dalam prosedur di atas, kita menggunakan fungsi Lambda sebagai target untuk aturan yang memicu CloudWatch Peristiwa. Anda juga dapat mengonfigurasi AWS sumber daya lain sebagai target untuk memicu CloudWatch Peristiwa. Untuk informasi selengkapnya, lihat [PutTargets](#).

## CloudWatch Acara untuk lingkungan GuardDuty multi-akun

Sebagai GuardDuty administrator Aturan CloudWatch acara di akun Anda akan dipicu berdasarkan temuan yang berlaku dari akun anggota Anda. Ini berarti bahwa jika Anda mengatur pemberitahuan temuan melalui CloudWatch Acara di akun administrator Anda, sebagaimana dirinci di bagian sebelumnya, Anda akan diberitahu tentang temuan tingkat keparahan tinggi dan menengah yang dihasilkan oleh akun anggota Anda selain milik Anda sendiri.

Anda dapat mengidentifikasi akun anggota GuardDuty tempat temuan berasal dengan `accountId` bidang detail JSON temuan.

Untuk mulai menulis aturan peristiwa kustom untuk akun anggota tertentu dalam lingkungan Anda di konsol, buat aturan baru dan tempelkan templat berikut ke Pratinjau Pola Peristiwa, dan tambahkan ID akun dari akun anggota yang ingin Anda gunakan untuk memicu peristiwa.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

**Note**

Contoh ini akan memicu pada setiap temuan untuk ID akun yang terdaftar. Beberapa ID dapat ditambahkan, dipisahkan dengan koma mengikuti sintaks JSON.

## Memahami CloudWatch Log dan alasan melewatkan sumber daya selama Perlindungan Malware untuk pemindaian EC2

GuardDuty Perlindungan Malware untuk EC2 menerbitkan peristiwa ke grup CloudWatch log Amazon Anda `/aws/guardduty/. malware-scan-events` Untuk setiap peristiwa yang terkait dengan pemindaian malware, Anda dapat memantau status dan hasil pemindaian sumber daya yang terkena dampak. Sumber daya Amazon EC2 tertentu dan volume Amazon EBS mungkin telah dilewati selama pemindaian Perlindungan Malware untuk EC2.

## Mengaudit CloudWatch Log dalam Perlindungan GuardDuty Malware untuk EC2

Ada tiga jenis peristiwa pemindaian yang didukung di grup log `malware-scan-events` CloudWatch / `aws/guardduty/`.

| Perlindungan Malware untuk nama acara pemindaian EC2 | Penjelasan  |
|--|---|
| EC2_SCAN_STARTED                                     | Dibuat saat Perlindungan GuardDuty Malware untuk EC2 memulai proses pemindaian malware, seperti bersiap untuk mengambil snapshot dari volume EBS.   |
| EC2_SCAN_COMPLETED                                   | Dibuat saat Perlindungan GuardDuty Malware untuk pemindaian EC2 selesai untuk setidaknya satu volume EBS dari sumber daya yang terkena dampak. Acara ini juga mencakup <code>snapshotId</code> yang termasuk dalam volume EBS yang dipindai. Setelah pemindaian selesai, hasil pemindaian |

| Perlindungan Malware untuk nama acara pemindaian EC2 | Penjelasan  |
|--|---|
| EC2_SCAN_SKIPPED                                     | <p>n akan menjadi CLEAN, THREATS_FOUND , atau NOT_SCANNED .</p> <p>Dibuat saat Perlindungan GuardDuty Malware untuk pemindaian EC2 melewati semua volume EBS dari sumber daya yang terkena dampak. Untuk mengidentifikasi alasan lewati, pilih acara yang sesuai, dan lihat detailnya . Untuk informasi lebih lanjut tentang alasan lewati, lihat <a href="#">Alasan melewati sumber daya selama pemindaian malware</a> di bawah.</p> |

### Note

Jika Anda menggunakan AWS Organizations, CloudWatch log peristiwa dari akun anggota di Organizations akan dipublikasikan ke akun administrator dan grup log akun anggota.

Pilih metode akses pilihan Anda untuk melihat dan menanyakan CloudWatch acara.

### Console

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi, di bawah Log, pilih Grup log. Pilih grup /aws/guardduty/ malware-scan-events log untuk melihat peristiwa pemindaian untuk Perlindungan Malware untuk EC2 GuardDuty

Untuk menjalankan kueri, pilih Wawasan Log.

Untuk informasi tentang menjalankan kueri, lihat [Menganalisis data CloudWatch log dengan Wawasan Log](#) di Panduan CloudWatch Pengguna Amazon.

3. Pilih Pindai ID untuk memantau detail sumber daya yang terkena dampak dan temuan malware. Misalnya, Anda dapat menjalankan kueri berikut untuk memfilter peristiwa

CloudWatch log dengan menggunakan `scanId`. Pastikan untuk menggunakan *scan-id* Anda sendiri yang valid.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

## API/CLI

- Untuk bekerja dengan grup log, lihat [Menelusuri entri log menggunakan AWS CLI di Panduan CloudWatch Pengguna Amazon](#).

Pilih grup `/aws/guardduty/malware-scan-events` log untuk melihat peristiwa pemindaian untuk Perlindungan Malware untuk EC2. GuardDuty

- Untuk melihat dan memfilter peristiwa log, lihat [GetLogEvents](#) dan [FilterLogEvents](#), masing-masing, di Referensi Amazon CloudWatch API.

## GuardDuty Perlindungan Malware untuk retensi log EC2

Periode penyimpanan log default untuk grup `malware-scan-events/aws/guardduty/log` adalah 90 hari, setelah itu peristiwa log dihapus secara otomatis. Untuk mengubah kebijakan penyimpanan log untuk grup CloudWatch log Anda, lihat [Mengubah penyimpanan data CloudWatch log di Log](#) di Panduan CloudWatch Pengguna Amazon, atau [PutRetentionPolicy](#) di Referensi CloudWatch API Amazon.

## Alasan melewatkan sumber daya selama pemindaian malware

Dalam peristiwa yang terkait dengan pemindaian malware, sumber daya EC2 dan volume EBS tertentu mungkin telah dilewati selama proses pemindaian. Tabel berikut mencantumkan alasan mengapa Perlindungan GuardDuty Malware untuk EC2 mungkin tidak memindai sumber daya. Jika berlaku, gunakan langkah-langkah yang diusulkan untuk mengatasi masalah ini, dan pindai sumber daya ini saat berikutnya Perlindungan GuardDuty Malware untuk EC2 memulai pemindaian malware. Masalah lain digunakan untuk memberi tahu Anda tentang jalannya acara dan tidak dapat ditindaklanjuti.



| Alasan untuk melompat-lompat | Penjelasan  | Langkah-langkah yang diusulkan   |
|------------------------------|---|--|
| RESOURCE_NOT_FOUND           | Yang resourceArn disediakan untuk memulai pemindaian malware sesuai permintaan tidak ditemukan di lingkungan Anda AWS .   | Validasi instans Amazon EC2 atau beban kerja container Anda, dan coba lagi. resourceArn  |
| ACCOUNT_INELIGIBLE           | ID AWS akun tempat Anda mencoba memulai pemindaian malware On-Demand belum diaktifkan. GuardDuty  | Verifikasi yang GuardDuty diaktifkan untuk AWS akun ini.<br><br>Saat Anda mengaktifkan GuardDuty dalam yang baru, Wilayah AWS mungkin diperlukan waktu hingga 20 menit untuk menyinkronkan.                                    |
| UNSUPPORTED_KEY_ENCRYPTION   | GuardDuty Perlindungan Malware untuk EC2 mendukung volume yang tidak terenkripsi dan dienkripsi dengan kunci yang dikelola pelanggan. Itu tidak mendukung pemindaian volume EBS yang dienkripsi menggunakan enkripsi <a href="#">Amazon EBS</a> . | Ganti kunci enkripsi Anda dengan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang jenis enkripsi yang GuardDuty mendukung, lihat <a href="#">EBS Volume Amazon yang didukung untuk pemindaian malware</a> . |

| Alasan untuk melompat-lompat | Penjelasan   | Langkah-langkah yang diusulkan   |  |
|------------------------------|--|--|--|
|                              | <p>Saat ini, ada perbedaan regional di mana alasan lompatan ini tidak berlaku. Untuk informasi lebih lanjut tentang ini Wilayah AWS, lihat <a href="#">Ketersediaan fitur khusus wilayah</a>.</p>  |  |  |
| EXCLUDED_BY_SCAN_SETTINGS    | <p>Instans EC2 atau volume EBS dikecualikan selama pemindaian malware. Ada dua kemungkinan - baik tag ditambahkan ke daftar inklusi tetapi sumber daya tidak terkait dengan tag ini, tag ditambahkan ke daftar pengecualian dan sumber daya dikaitkan dengan tag ini, atau GuardDuty Excluded tag diatur true untuk sumber daya ini.</p> | <p>Perbarui opsi pemindaian atau tag yang terkait dengan sumber daya Amazon EC2 Anda. Untuk informasi selengkapnya, lihat <a href="#">Opsi pindai dengan tag yang ditentukan pengguna</a>.</p> |  |
| UNSUPPORTED_VOLUME_SIZE      | <p>Volumenya lebih besar dari 2048 GB.</p>   | <p>Tidak bisa ditindaklanjuti.</p>   |  |

| Alasan untuk melompat-lompat | Penjelasan   | Langkah-langkah yang diusulkan   |  |
|------------------------------|--|--|--|
| NO_VOLUME_S_ATTACHED         | GuardDuty Perlindungan Malware untuk EC2 menemukan instans di akun Anda tetapi tidak ada volume EBS yang dilampirkan ke instance ini untuk melanjutkan pemindaian.       | Tidak bisa ditindaklanjuti.  |  |
| UNABLE_TO_SCAN               | Ini adalah kesalahan layanan internal.   | Tidak bisa ditindaklanjuti.  |  |
| SNAPSHOT_NOT_FOUND           | Snapshot yang dibuat dari volume EBS dan dibagikan dengan akun layanan tidak ditemukan, dan Perlindungan GuardDuty Malware untuk EC2 tidak dapat melanjutkan pemindaian. | Periksa CloudTrail untuk memastikan bahwa snapshot tidak dihapus dengan sengaja. |  |

| Alasan untuk melompat-lompat           | Penjelasan  | Langkah-langkah yang diusulkan  |  |
|--|---|---|--|
| SNAPSHOT_QUOTA_REACHED                 | Anda telah mencapai volume maksimum yang diizinkan untuk snapshot untuk setiap Wilayah. Ini mencegah tidak hanya mempertahankan tetapi juga membuat snapshot baru.                              | Anda dapat menghapus snapshot lama atau meminta peningkatan kuota. Anda dapat melihat batas default untuk Snapshot per Wilayah dan cara meminta peningkatan kuota di bawah <a href="#">Kuota layanan</a> di Panduan Referensi AWS Umum. |  |
| MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED | Lebih dari 11 volume EBS dilampirkan ke instans EC2. GuardDuty Perlindungan Malware untuk EC2 memindai 11 volume EBS pertama, diperoleh dengan menyortir menurut abjad. <code>deviceName</code> | Tidak bisa ditindaklanjuti.   |  |

| Alasan untuk melompat-lompat          | Penjelasan   | Langkah-langkah yang diusulkan |
|---------------------------------------|--|--------------------------------|
| UNSUPPORT<br>ED_PRODUC<br>T_CODE_TYPE | <p>GuardDuty tidak mendukung pemindaian instance dengan <code>productCode asmarketplace</code>. Untuk informasi selengkapnya, lihat <a href="#">AMI Berbayar</a> di Panduan Pengguna Amazon EC2.</p> <p>Untuk informasi tentang <code>productCode</code>, lihat <a href="#">ProductCode</a> di Referensi API Amazon EC2.</p> | Tidak bisa ditindaklanjuti.    |


## Melaporkan positif palsu dalam Perlindungan GuardDuty Malware untuk EC2

GuardDuty Perlindungan Malware untuk pemindaian EC2 dapat mengidentifikasi file yang tidak berbahaya di instans Amazon EC2 atau beban kerja kontainer Anda sebagai berbahaya atau berbahaya. Untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan GuardDuty layanan, Anda dapat melaporkan hasil positif palsu jika Anda yakin bahwa file yang diidentifikasi berbahaya atau berbahaya selama pemindaian sebenarnya tidak mengandung malware.

### Pengajuan file positif palsu

1. Masuk ke konsol <https://console.aws.amazon.com/guardduty/>.
2. Ketika Anda mengidentifikasi apa yang tampak sebagai hasil positif palsu, hubungi AWS Support untuk memulai proses pengiriman file positif palsu.
3. Pilih Pemindaian Malware.

4. Pilih pemindaian untuk melihat ID Temuannya.
5. Berikan ID Finding. Anda juga harus memberikan hash SHA-256 dari file tersebut. Ini diperlukan untuk memastikan bahwa Perlindungan GuardDuty Malware untuk EC2 telah menerima file yang benar.
6. AWS Support Tim akan memberi Anda URL Amazon Simple Storage Service (S3) Amazon Simple Storage Service yang dapat Anda gunakan untuk mengunggah file dan hash SHA-256. Beri tahu AWS Support tim setelah Anda berhasil mengunggah file.

 Warning

Jangan langsung memberikan file atau SHA-256 hash ke AWS Support Anda hanya boleh mengunggah file dan hash ke Amazon S3 melalui URL yang disediakan. Jika Anda gagal mengunggah file dan hash dalam waktu tujuh hari setelah menerima URL, itu akan menjadi tidak valid. Jika URL menjadi tidak valid, Anda harus menghubungi AWS Support untuk menerima URL baru.

GuardDuty menyimpan file Anda selama tidak lebih dari 30 hari. GuardDuty Anggota tim akan menganalisis kiriman Anda dan mengambil langkah-langkah yang tepat untuk meningkatkan pengalaman Anda dengan Perlindungan Malware untuk EC2 dan layanan. GuardDuty

# Memperbaiki masalah keamanan yang ditemukan oleh GuardDuty

Amazon GuardDuty menghasilkan [temuan](#) yang menunjukkan potensi masalah keamanan. Dalam rilis ini GuardDuty, masalah keamanan potensial menunjukkan EC2 instans yang dikompromikan atau beban kerja kontainer, atau serangkaian kredensi yang dikompromikan di lingkungan Anda. AWS Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Jika ada alternatif skenario perbaikan, skenario tersebut akan dijelaskan dalam entri untuk tipe temuan spesifik tersebut. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari [tabel Tipe temuan aktif](#).

## Daftar Isi

- [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#)
- [Memulihkan bucket S3 yang berpotensi dikompromikan](#)
- [Memperbaiki objek S3 yang berpotensi berbahaya](#)
- [Memulihkan cluster yang berpotensi dikompromikan ECS](#)
- [Memulihkan kredensi yang berpotensi dikompromikan AWS](#)
- [Memulihkan wadah mandiri yang berpotensi dikompromikan](#)
- [Memediasi temuan Pemantauan Log Audit EKS](#)
- [Remediasi temuan Runtime Monitoring](#)
- [Memulihkan database yang berpotensi dikompromikan](#)
- [Memperbaiki fungsi Lambda yang berpotensi dikompromikan](#)

## Memperbaiki instans Amazon yang berpotensi dikompromikan EC2

Ikuti langkah-langkah yang disarankan ini untuk memulihkan EC2 instans yang berpotensi dikompromikan di lingkungan Anda AWS :

### 1. Identifikasi instans Amazon EC2 yang berpotensi dikompromikan

Selidiki instans yang berpotensi disusupi untuk malware dan menghapus malware yang ditemukan. Anda dapat menggunakannya [Pemindaian malware sesuai permintaan](#) untuk mengidentifikasi malware dalam EC2 contoh yang berpotensi dikompromikan, atau memeriksa

[AWS Marketplace](#) untuk melihat apakah ada produk mitra yang bermanfaat untuk mengidentifikasi dan menghapus malware.

## 2. Isolasi instans Amazon yang berpotensi dikompromikan EC2

Jika memungkinkan, gunakan langkah-langkah berikut untuk mengisolasi instance yang berpotensi dikompromikan:

1. Buat grup keamanan Isolasi khusus. Grup keamanan isolasi seharusnya hanya memiliki akses masuk dan keluar dari alamat IP tertentu. Pastikan bahwa tidak ada aturan inbound atau outbound yang memungkinkan lalu lintas untuk `0.0.0.0/0` (`0-65535`)
2. Kaitkan grup keamanan Isolasi dengan instance ini.
3. Hapus semua asosiasi grup keamanan selain grup keamanan Isolasi yang baru dibuat dari instance yang berpotensi dikompromikan.

### Note

Koneksi yang dilacak yang ada tidak akan dihentikan sebagai akibat dari perubahan kelompok keamanan - hanya lalu lintas masa depan yang akan diblokir secara efektif oleh grup keamanan baru.

Untuk informasi tentang koneksi yang dilacak dan tidak dilacak, lihat [Pelacakan koneksi grup EC2 keamanan Amazon](#) di Panduan Pengguna Amazon EC2.

Untuk informasi tentang memblokir lalu lintas lebih lanjut dari koneksi mencurigakan yang ada, lihat [Menegakkan NACLs berdasarkan jaringan loCs untuk mencegah lalu lintas lebih lanjut](#) di Playbook Respons Insiden.

## 3. Identifikasi sumber aktivitas yang mencurigakan

Jika malware terdeteksi, maka berdasarkan jenis temuan di akun Anda, identifikasi dan hentikan aktivitas yang berpotensi tidak sah pada EC2 instans Anda. Ini mungkin memerlukan tindakan seperti menutup port terbuka, mengubah kebijakan akses, dan meningkatkan aplikasi untuk memperbaiki kerentanan.

Jika Anda tidak dapat mengidentifikasi dan menghentikan aktivitas yang tidak sah pada EC2 instans yang berpotensi dikompromikan, sebaiknya Anda menghentikan instans yang disusupi dan menggantinya dengan EC2 instance baru sesuai kebutuhan. Berikut ini adalah sumber daya tambahan untuk mengamankan EC2 instans Anda:

- Bagian Keamanan dan Jaringan dalam [Praktik terbaik untuk Amazon EC2](#)



- [Grup EC2 keamanan Amazon untuk instans Linux](#) dan [grup EC2 keamanan Amazon untuk instans Windows](#)
- [Keamanan di Amazon EC2](#)
- [Kiat untuk mengamankan EC2 instans Anda \(Linux\)](#).
- [AWS praktik terbaik keamanan](#)
- [Insiden Domain Infrastruktur pada AWS](#)

#### 4. Jelajahi AWS re:Post

Jelajahi [AWS re:Post](#) untuk bantuan lebih lanjut.

#### 5. Kirim permintaan dukungan teknis

Jika Anda adalah pelanggan paket dukungan premium, Anda dapat mengirimkan permintaan [dukungan teknis](#).

## Memulihkan bucket S3 yang berpotensi dikompromikan

Ikuti langkah-langkah yang disarankan ini untuk memulihkan bucket Amazon S3 yang berpotensi dikompromikan di lingkungan Anda: AWS

#### 1. Identifikasi sumber daya S3 yang berpotensi dikompromikan.

GuardDuty Temuan untuk S3 akan mencantumkan bucket S3 terkait, Amazon Resource Name (ARN), dan pemiliknya dalam detail temuan.

#### 2. Identifikasi sumber aktivitas mencurigakan dan API panggilan yang digunakan.

API Panggilan yang digunakan akan dicantumkan seperti API pada detail temuan. Sumber akan menjadi IAM prinsipal (baik IAM peran, pengguna, atau akun) dan rincian identifikasi akan tercantum dalam temuan. Bergantung pada jenis sumbernya, alamat IP jarak jauh atau info domain sumber akan tersedia dan dapat membantu Anda mengevaluasi apakah sumber tersebut diotorisasi. Jika temuan melibatkan kredensial dari EC2 instance Amazon, detail untuk sumber daya itu juga akan disertakan.

#### 3. Tentukan apakah sumber panggilan diberi wewenang untuk mengakses sumber daya yang diidentifikasi.

Misalnya, pertimbangkan hal berikut:

- Jika IAM pengguna terlibat, mungkinkah kredensialnya berpotensi dikompromikan? Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).
  - Jika sebuah API dipanggil dari prinsipal yang tidak memiliki riwayat sebelumnya untuk memanggil jenis ini API, apakah sumber ini memerlukan izin akses untuk operasi ini? Dapatkah izin bucket dibatasi secara lebih lanjut?
  - Jika akses terlihat dari nama pengguna ANONYMOUS\_PRINCIPAL dengan tipe pengguna dari AWSAccount, ini menunjukkan bahwa bucket bersifat publik dan telah diakses. Haruskah bucket ini dibuat publik? Jika tidak, tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3.
  - Jika akses adalah PreflightRequest panggilan yang berhasil dilihat dari nama pengguna ANONYMOUS\_PRINCIPAL dengan tipe pengguna, AWSAccount ini menunjukkan bucket memiliki kumpulan kebijakan berbagi sumber daya lintas asal (CORS). Haruskah ember ini memiliki CORS kebijakan? Jika tidak, pastikan bucket tidak secara tidak sengaja dipublikasikan dan tinjau rekomendasi keamanan di bawah ini untuk solusi alternatif untuk berbagi sumber daya S3. Untuk informasi selengkapnya, CORS lihat [Menggunakan berbagi sumber daya lintas asal \(CORS\)](#) di panduan pengguna S3.
4. Tentukan apakah bucket S3 berisi data sensitif.

Gunakan [Amazon Macie](#) untuk menentukan apakah bucket S3 berisi data sensitif, seperti informasi identitas pribadi (PII), data keuangan, atau kredensial. Jika penemuan data sensitif otomatis diaktifkan untuk akun Macie Anda, tinjau detail bucket S3 untuk mendapatkan pemahaman yang lebih baik tentang konten bucket S3 Anda. Jika fitur ini dinonaktifkan untuk akun Macie Anda, kami sarankan untuk menyalakannya untuk mempercepat penilaian Anda. Atau, Anda dapat membuat dan menjalankan tugas penemuan data sensitif untuk memeriksa objek bucket S3 untuk data sensitif. Untuk informasi selengkapnya, lihat [Menemukan data sensitif dengan Macie](#).

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

Jika Anda menentukan bahwa data S3 Anda telah diekspos atau diakses oleh pihak yang tidak berwenang, tinjau rekomendasi keamanan S3 berikut untuk memperketat izin dan membatasi akses. Solusi perbaikan yang tepat akan bergantung pada kebutuhan lingkungan spesifik Anda.

## Rekomendasi berdasarkan kebutuhan akses bucket S3 tertentu

Daftar berikut memberikan rekomendasi berdasarkan kebutuhan akses bucket Amazon S3 tertentu:

- Untuk cara terpusat untuk membatasi akses publik ke penggunaan data S3 Anda, S3 memblokir akses publik. Blokir pengaturan akses publik dapat diaktifkan untuk titik akses, bucket, dan AWS Akun melalui empat pengaturan berbeda untuk mengontrol perincian akses. Untuk informasi selengkapnya, lihat [Pengaturan Blokir Akses Publik S3](#).
- AWS Kebijakan akses dapat digunakan untuk mengontrol bagaimana IAM pengguna dapat mengakses sumber daya Anda atau bagaimana bucket Anda dapat diakses. Untuk informasi selengkapnya, lihat [Menggunakan Kebijakan Bucket dan Kebijakan Pengguna](#).

Selain itu, Anda dapat menggunakan titik akhir Virtual Private Cloud (VPC) dengan kebijakan bucket S3 untuk membatasi akses ke titik akhir tertentu. VPC Untuk informasi selengkapnya, lihat [Contoh Kebijakan Bucket untuk VPC Titik Akhir untuk Amazon S3](#)

- Untuk mengizinkan akses sementara ke objek S3 Anda ke entitas tepercaya di luar akun Anda, Anda dapat membuat Presigned URL melalui S3. Akses ini dibuat menggunakan kredensial akun Anda dan bergantung pada kredensial yang digunakan dapat bertahan 6 jam hingga 7 hari. Untuk informasi selengkapnya, lihat [Menghasilkan presigned URLs dengan S3](#).
- Untuk kasus penggunaan yang mengharuskan berbagi objek S3 antara sumber yang berbeda, Anda dapat menggunakan S3 Access Points untuk membuat set izin yang membatasi akses hanya untuk mereka yang berada dalam jaringan pribadi Anda. Untuk informasi selengkapnya, lihat [Mengelola akses data dengan Amazon S3 access points](#).
- Untuk memberikan akses ke sumber daya S3 ke AWS Akun lain dengan aman, Anda dapat menggunakan daftar kontrol akses (ACL), untuk informasi selengkapnya lihat [Mengelola Akses S3](#) dengan ACLs

Untuk informasi selengkapnya tentang opsi keamanan S3, lihat praktik [terbaik Keamanan S3](#).

## Memperbaiki objek S3 yang berpotensi berbahaya

[Perlindungan Malware untuk tipe pencarian S3](#) Ketika dihasilkan di Anda Akun AWS, jenis sumber daya yang berpotensi berbahaya adalah S3Object.

Gunakan langkah-langkah yang disarankan berikut untuk berpotensi memulihkan temuan yang dihasilkan:

1. Identifikasi objek S3 yang berpotensi berbahaya dengan memeriksa S3 yang ObjectDetails terkait dengan temuan tersebut.
2. Isolasi objek S3 yang terkena dampak. Jika Anda telah mengaktifkan penandaan pada saat mengaktifkan Perlindungan Malware untuk S3 untuk bucket Amazon S3 terkait, GuardDuty harus menetapkan tag Berbahaya ke objek ini. Gunakan kontrol akses berbasis tag (TBAC) untuk membatasi akses ke objek S3 ini. Untuk informasi selengkapnya, lihat [Menggunakan kontrol akses berbasis tag \(\) TBAC](#).

Atau, jika Anda tidak memerlukan objek ini lagi, Anda juga dapat memilih untuk menghapusnya atau memindahkannya ke ember S3 yang terisolasi. Untuk informasi tentang pertimbangan untuk menghapus objek S3, lihat [Menghapus](#) objek di Panduan Pengguna Amazon S3.

## Memulihkan cluster yang berpotensi dikompromikan ECS

Ikuti langkah-langkah yang disarankan ini untuk memulihkan ECS klaster Amazon yang berpotensi dikompromikan di lingkungan Anda AWS :

1. Identifikasi ECS cluster yang berpotensi dikompromikan.

Perlindungan GuardDuty Malware untuk EC2 pencarian ECS menyediakan detail ECS klaster di panel detail temuan.

2. Evaluasi sumber malware

Evaluasi apakah malware yang terdeteksi ada di gambar wadah. Jika malware ada di gambar, identifikasi semua tugas lain yang berjalan menggunakan gambar ini. Untuk informasi tentang menjalankan tugas, lihat [ListTasks](#).

3. Mengisolasi tugas yang berpotensi terkena dampak

Mengisolasi tugas yang terkena dampak dengan menolak semua lalu lintas masuk dan keluar ke tugas. Menyangkal semua aturan lalu lintas dapat membantu Anda menghentikan serangan yang sudah berlangsung, dengan memutuskan semua koneksi ke tugas.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

# Memulihkan kredensi yang berpotensi dikompromikan AWS

Ikuti langkah-langkah yang disarankan ini untuk memulihkan kredensial yang berpotensi dikompromikan di lingkungan Anda: AWS

## 1. Identifikasi IAM entitas yang berpotensi dikompromikan dan API panggilan yang digunakan.

APIPanggilan yang digunakan akan dicantumkan seperti API pada detail temuan. IAMEntitas (baik IAM peran atau pengguna) dan informasi pengenalannya akan dicantumkan di bagian Sumber Daya dari rincian temuan. Jenis IAM entitas yang terlibat dapat ditentukan oleh bidang Jenis Pengguna, nama IAM entitas akan berada di bidang Nama pengguna. Jenis IAM entitas yang terlibat dalam temuan juga dapat ditentukan oleh ID kunci Access yang digunakan.

Untuk kunci yang diawali dengan AKIA:

Jenis kunci ini adalah kredensi jangka panjang yang dikelola pelanggan yang terkait dengan pengguna atau IAM. Pengguna root akun AWS Untuk informasi tentang mengelola kunci akses bagi IAM pengguna, lihat [Mengelola kunci akses untuk IAM pengguna](#).

Untuk kunci yang diawali dengan ASIA:

Tipe kunci ini adalah kredensial sementara jangka pendek yang dihasilkan oleh AWS Security Token Service. Kunci ini hanya ada untuk waktu yang singkat dan tidak dapat dilihat atau dikelola di Konsol AWS Manajemen. IAMperan akan selalu menggunakan AWS STS kredensial, tetapi juga dapat dibuat untuk IAM Pengguna, untuk informasi lebih lanjut tentang AWS STS lihat [IAM: Kredensial keamanan sementara](#).

Jika peran digunakan, bidang Nama pengguna akan menunjukkan nama dari peran yang digunakan. Anda dapat menentukan bagaimana kunci diminta AWS CloudTrail dengan memeriksa `sessionIssuer` elemen entri CloudTrail log, untuk informasi lebih lanjut lihat [IAM dan AWS STS informasi di CloudTrail](#).

## 2. Meninjau izin untuk IAM entitas.

Buka IAM konsol. Bergantung pada jenis entitas yang digunakan, pilih tab Pengguna atau Peran, dan temukan entitas yang terpengaruh dengan mengetikkan nama yang diidentifikasi ke dalam bidang pencarian. Gunakan tab Izin dan Penasihat Akses untuk meninjau izin efektif untuk entitas tersebut.

## 3. Tentukan apakah kredensial IAM entitas digunakan secara sah.

Hubungi pengguna kredensial untuk menentukan apakah aktivitas tersebut disengaja.

Misalnya, cari tahu apakah pengguna melakukan hal berikut:

- Memanggil API operasi yang tercantum dalam temuan GuardDuty
- Memanggil API operasi pada saat yang tercantum dalam temuan GuardDuty
- Memanggil API operasi dari alamat IP yang tercantum dalam temuan GuardDuty

Jika aktivitas ini adalah penggunaan AWS kredensial yang sah, Anda dapat mengabaikan temuan tersebut. GuardDuty <https://console.aws.amazon.com/guardduty/>Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

Jika Anda tidak dapat mengonfirmasi apakah aktivitas ini adalah penggunaan yang sah, itu bisa menjadi hasil dari kompromi ke kunci akses tertentu - kredensi login IAM pengguna, atau mungkin keseluruhan. Akun AWS Jika Anda mencurigai kredensial Anda telah disusupi, tinjau informasi di artikel [Saya Akun AWS dapat dikompromikan](#) untuk memperbaiki masalah ini.

## Memulihkan wadah mandiri yang berpotensi dikompromikan

### 1. Isolasi wadah yang berpotensi dikompromikan

Langkah-langkah berikut akan membantu Anda mengidentifikasi beban kerja kontainer yang berpotensi berbahaya:

- Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
- Pada halaman Temuan, pilih temuan yang sesuai untuk melihat panel temuan.
- Di panel temuan, di bawah bagian Resource affected, Anda dapat melihat ID dan Nama container.

Isolasi wadah ini dari beban kerja kontainer lainnya.

### 2. Jeda wadah

Tangguhkan semua proses dalam wadah Anda.

Untuk informasi tentang membekukan wadah Anda, lihat [Menjeda wadah](#).

Hentikan wadahnya

Jika langkah di atas gagal, dan penampung tidak berhenti, hentikan penampung agar tidak berjalan. Jika Anda telah mengaktifkan [Retensi snapshot](#) fitur tersebut, GuardDuty akan mempertahankan snapshot EBS volume Anda yang berisi malware.

Untuk informasi tentang menghentikan wadah, lihat [Menghentikan wadah](#).

### 3. Evaluasi keberadaan malware

Evaluasi apakah malware ada di gambar kontainer.

Jika akses diotorisasi, Anda dapat mengabaikan temuan tersebut. <https://console.aws.amazon.com/guardduty/> Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. GuardDuty Konsol memungkinkan Anda untuk mengatur aturan untuk sepenuhnya menekan temuan individu sehingga tidak lagi muncul. Untuk informasi selengkapnya, lihat [Aturan penekanan](#).

## Memediasi temuan Pemantauan Log Audit EKS

Amazon GuardDuty menghasilkan [temuan](#) yang menunjukkan potensi masalah keamanan Kubernetes saat Pemantauan Log Audit EKS diaktifkan untuk akun Anda. Untuk informasi selengkapnya, lihat [EKSPemantauan Log Audit](#). Bagian berikut menjelaskan langkah-langkah perbaikan yang disarankan untuk skenario ini. Tindakan remediasi khusus dijelaskan dalam entri untuk jenis temuan spesifik tersebut. Anda dapat mengakses informasi selengkapnya tentang tipe temuan dengan memilihnya dari [tabel Tipe temuan aktif](#).

Jika salah satu jenis temuan Pemantauan Log Audit EKS dihasilkan secara diharapkan, Anda dapat mempertimbangkan [Aturan penekanan](#) untuk menambahkan untuk mencegah peringatan di masa mendatang.

Berbagai jenis serangan dan masalah konfigurasi dapat memicu temuan GuardDuty Kubernetes. Panduan ini membantu Anda mengidentifikasi akar penyebab GuardDuty temuan terhadap cluster Anda dan menguraikan panduan remediasi yang tepat. Berikut ini adalah akar penyebab utama yang mengarah pada temuan GuardDuty Kubernetes:

- [Potensi masalah konfigurasi](#)
- [Memulihkan pengguna Kubernetes yang berpotensi dikompromikan](#)
- [Remediasi pod Kubernetes yang berpotensi dikompromikan](#)

- [Remediasi node Kubernetes yang berpotensi dikompromikan](#)
- [Memulihkan gambar kontainer yang berpotensi dikompromikan](#)

#### Note

Sebelum Kubernetes versi 1.14, `system:unauthenticated` grup ini dikaitkan dengan dan secara default. `system:discovery` `system:basic-user` ClusterRoles Ini memungkinkan akses yang tidak diinginkan dari pengguna anonim. Pembaruan klaster tidak mencabut izin ini, yang berarti bahwa meskipun Anda telah memperbarui klaster Anda ke versi 1.14 atau yang lebih baru, izin ini mungkin masih ada. Kami menyarankan Anda untuk memisahkan izin ini dari grup. `system:unauthenticated`

Untuk informasi selengkapnya tentang menghapus izin ini, lihat [Praktik terbaik keamanan untuk Amazon EKS](#) di Panduan Pengguna Amazon EKS.

## Potensi masalah konfigurasi

Jika temuan menunjukkan masalah konfigurasi, lihat bagian remediasi dari temuan tersebut untuk panduan penyelesaian masalah tertentu. Untuk informasi selengkapnya, lihat jenis temuan berikut yang menunjukkan masalah konfigurasi:

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Temuan apa pun yang berakhir di `SuccessfulAnonymousAccess`

## Memulihkan pengguna Kubernetes yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan pengguna Kubernetes yang disusupi ketika pengguna yang diidentifikasi dalam temuan tersebut telah melakukan tindakan API yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna Kubernetes dari detail temuan di konsol, atau di temuan `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` JSON. Detail pengguna ini mencakup `user name`, `uid`, dan grup Kubernetes yang menjadi milik pengguna.



Jika pengguna mengakses beban kerja menggunakan entitas IAM, Anda dapat menggunakan `Access Key details` bagian tersebut untuk mengidentifikasi detail peran IAM atau pengguna. Lihat jenis pengguna berikut dan panduan remediasinya.

#### Note

Anda dapat menggunakan Amazon Detective untuk menyelidiki lebih lanjut peran IAM atau pengguna yang diidentifikasi dalam temuan tersebut. Saat melihat detail temuan di GuardDuty konsol, pilih `Selidiki di Detektif`. Kemudian pilih AWS pengguna atau peran dari item yang terdaftar untuk menyelidikinya di Detektif.

Admin Kubernetes bawaan — Pengguna default yang ditetapkan oleh Amazon EKS ke identitas IAM yang membuat cluster. Jenis pengguna ini diidentifikasi oleh nama `kubernetes-admin`.

Untuk mencabut akses admin Kubernetes bawaan:

- Identifikasi `userType` dari `Access Key details` bagian.
  - Jika Peran **`userType`** is dan peran tersebut termasuk dalam peran instans EC2:
    - Identifikasi contoh itu kemudian ikuti instruksi di [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#).
  - Jika `userType` adalah Pengguna, atau Peran yang diasumsikan oleh pengguna:
    1. [Putar tombol akses](#) pengguna tersebut.
    2. Putar rahasia apa pun yang dapat diakses pengguna.
    3. Meninjau informasi di [AWS Akun saya dapat dikompromikan](#) untuk rincian lebih lanjut.

Pengguna yang diautentikasi OIDC — Pengguna diberikan akses melalui penyedia OIDC. Biasanya pengguna OIDC memiliki alamat email sebagai nama pengguna. Anda dapat memeriksa apakah cluster Anda menggunakan OIDC dengan perintah berikut: `aws eks list-identity-provider-configs --cluster-name your-cluster-name`

Untuk mencabut akses pengguna yang diautentikasi OIDC:

1. Putar kredensi pengguna tersebut di penyedia OIDC.
2. Putar rahasia apa pun yang dapat diakses pengguna.

AWS-Auth ConfigMap defined user — Pengguna IAM yang diberikan akses melalui -auth.

AWSConfigMap Untuk informasi selengkapnya, lihat [Mengelola pengguna atau peran IAM untuk klaster Anda](#) di panduan pengguna &EKS;. Anda dapat meninjau izin mereka menggunakan perintah berikut: `kubectl edit configmaps aws-auth --namespace kube-system`

Untuk mencabut akses pengguna: AWS ConfigMap

1. Gunakan perintah berikut untuk membuka ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifikasi peran atau entri pengguna di bagian MapRoles atau MapUsers dengan nama pengguna yang sama seperti yang dilaporkan di bagian detail pengguna Kubernetes pada temuan Anda. GuardDuty Lihat contoh berikut, di mana pengguna admin telah diidentifikasi dalam sebuah temuan.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Hapus pengguna itu dari ConfigMap. Lihat contoh berikut di mana pengguna admin telah dihapus.

```
apiVersion: v1
data:
  mapRoles: |
```

```
- rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE306UCF
  username: system:node:{{EC2PrivateDNSName}}
  groups:
    - system:bootstrappers
    - system:nodes
mapUsers: |
- userarn: arn:aws:iam::111122223333:user/ops-user
  username: ops-user
  groups:
    - system:masters
```

4. Jika `userType` adalah Pengguna, atau Peran yang diasumsikan oleh pengguna:
  - a. [Putar tombol akses](#) pengguna tersebut.
  - b. Putar rahasia apa pun yang dapat diakses pengguna.
  - c. Meninjau informasi di [AWS Akun saya dapat dikompromikan](#) untuk rincian lebih lanjut.

Jika temuan tidak memiliki `resource.accessKeyDetails` bagian, pengguna adalah akun layanan Kubernetes.

Akun layanan — Akun layanan menyediakan identitas untuk pod dan dapat diidentifikasi dengan nama pengguna dengan format

berikut: `system:serviceaccount:namespace:service_account_name`.

Untuk mencabut akses ke akun layanan:

1. Putar kredensial akun layanan.
2. Tinjau panduan untuk kompromi pod di bagian berikut.

## Remediasi pod Kubernetes yang berpotensi dikompromikan

Saat GuardDuty menentukan detail pod atau sumber daya beban kerja di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian tersebut, pod atau sumber daya beban kerja tersebut berpotensi dikompromikan. Sebuah GuardDuty temuan dapat menunjukkan bahwa satu pod telah dikompromikan atau bahwa beberapa pod telah dikompromikan melalui sumber daya tingkat yang lebih tinggi. Lihat skenario kompromi berikut untuk panduan tentang cara mengidentifikasi pod atau pod yang telah disusupi.

## Kompromi pod tunggal

Jika type bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian ini adalah pod, temuan tersebut mengidentifikasi satu pod. Field name adalah name dari pod dan namespace field adalah namespace-nya.

Untuk informasi tentang mengidentifikasi node pekerja yang menjalankan pod, lihat [Mengidentifikasi pod yang menyinggung dan node pekerja](#).

## Pod dikompromikan melalui sumber daya beban kerja

Jika type bidang di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails` bagian mengidentifikasi Sumber Daya Beban Kerja, seperti aDeployment, kemungkinan semua pod dalam sumber daya beban kerja tersebut telah dikompromikan.

Untuk informasi tentang mengidentifikasi semua Pod dari sumber daya beban kerja dan node yang dijelankannya, lihat [Mengidentifikasi Pod yang menyinggung dan node pekerja menggunakan nama beban kerja](#).

## Pod dikompromikan melalui akun layanan

Jika GuardDuty temuan mengidentifikasi Akun Layanan di `resource.kubernetesDetails.kubernetesUserDetails` bagian tersebut, kemungkinan pod yang menggunakan akun layanan yang diidentifikasi akan disusupi. Nama pengguna yang dilaporkan oleh temuan adalah akun layanan jika memiliki format berikut: `system:serviceaccount:namespace:service_account_name`.

Untuk informasi tentang mengidentifikasi semua pod menggunakan akun layanan dan node yang dijelankannya, lihat [Mengidentifikasi Pod yang menyinggung dan node pekerja menggunakan nama akun layanan](#).

Setelah Anda mengidentifikasi semua pod yang dikompromikan dan node tempat mereka berjalan, lihat [panduan praktik terbaik Amazon EKS](#) untuk mengisolasi pod, memutar kredensialnya, dan mengumpulkan data untuk analisis forensik.

Untuk memulihkan pod yang berpotensi dikompromikan:

1. Identifikasi kerentanan yang mengganggu pod.
2. Terapkan perbaikan untuk kerentanan itu dan mulai pod pengganti baru.
3. Hapus pod yang rentan.

Untuk informasi selengkapnya, lihat [Menerapkan ulang pod atau sumber daya beban kerja yang dikompromikan](#).

Jika node pekerja telah diberi peran IAM yang memungkinkan Pod mendapatkan akses ke AWS sumber daya lain, hapus peran tersebut dari instance untuk mencegah kerusakan lebih lanjut dari serangan. Demikian pula, jika Pod telah diberi peran IAM, evaluasi apakah Anda dapat menghapus kebijakan IAM dari peran dengan aman tanpa memengaruhi beban kerja lainnya.

## Memulihkan gambar kontainer yang berpotensi dikompromikan

Ketika sebuah GuardDuty temuan menunjukkan kompromi pod, gambar yang digunakan untuk meluncurkan pod berpotensi berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar kontainer di dalam `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` lapangan. Anda dapat menentukan apakah gambar tersebut berbahaya dengan memindai malware.

Untuk memulihkan gambar kontainer yang berpotensi dikompromikan:

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua pod menggunakan gambar yang berpotensi dikompromikan.

Untuk informasi selengkapnya, lihat [Mengidentifikasi pod dengan image kontainer dan node pekerja yang berpotensi rentan atau dikompromikan](#).

3. Isolasi pod yang berpotensi dikompromikan, putar kredensialnya, dan kumpulkan data untuk dianalisis. Untuk informasi selengkapnya, lihat [panduan praktik terbaik Amazon EKS](#).
4. Hapus semua pod menggunakan gambar yang berpotensi dikompromikan.

## Remediasi node Kubernetes yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan kompromi node jika pengguna yang diidentifikasi dalam temuan mewakili identitas node atau jika temuan menunjukkan penggunaan wadah istimewa.

Identitas pengguna adalah node pekerja jika bidang nama pengguna memiliki format berikut: `system:node:node name`. Misalnya, `system:node:ip-192-168-3-201.ec2.internal`. Hal ini menunjukkan bahwa musuh telah memperoleh akses ke node dan menggunakan kredensial node untuk berbicara dengan titik akhir API Kubernetes.

Temuan menunjukkan penggunaan wadah istimewa jika satu atau lebih kontainer yang tercantum dalam temuan memiliki bidang `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext`. Temuan yang disetel ke `True`.

Untuk memulihkan node yang berpotensi dikompromikan:

1. Isolasi pod, putar kredensialnya, dan kumpulkan data untuk analisis forensik.

Untuk informasi selengkapnya, lihat [panduan praktik terbaik Amazon EKS](#).

2. Identifikasi akun layanan yang digunakan oleh semua pod yang berjalan pada node yang berpotensi dikompromikan. Tinjau izin mereka dan putar akun layanan jika diperlukan.
3. Hentikan node yang berpotensi dikompromikan.

## Remediasi temuan Runtime Monitoring

Saat Anda mengaktifkan Runtime Monitoring untuk akun Anda, Amazon GuardDuty dapat menghasilkan [Jenis penemuan Runtime Monitoring](#) yang menunjukkan potensi masalah keamanan di AWS lingkungan Anda. Masalah keamanan potensial menunjukkan instans Amazon EC2 yang dikompromikan, beban kerja kontainer, kluster Amazon EKS, atau sekumpulan kredensial yang disusupi di lingkungan Anda. AWS Agen keamanan memantau peristiwa runtime dari berbagai jenis sumber daya. Untuk mengidentifikasi sumber daya yang berpotensi dikompromikan, lihat Jenis sumber daya dalam detail temuan yang dihasilkan di GuardDuty konsol. Bagian berikut menjelaskan langkah-langkah remediasi yang direkomendasikan untuk setiap jenis sumber daya.

### Instance

Jika tipe Resource dalam rincian temuan adalah Instance, ini menunjukkan bahwa baik instans EC2 atau node EKS berpotensi dikompromikan.

- Untuk memulihkan simpul EKS yang dikompromikan, lihat. [Remediasi node Kubernetes yang berpotensi dikompromikan](#)
- Untuk memulihkan instans EC2 yang dikompromikan, lihat. [Memperbaiki instans Amazon yang berpotensi dikompromikan EC2](#)

## EKS Cluster

Jika tipe Resource dalam detail temuan adalah Ekscluster, ini menunjukkan bahwa pod atau wadah di dalam cluster EKS berpotensi dikompromikan.

- Untuk memulihkan pod yang dikompromikan, lihat. [Remediasi pod Kubernetes yang berpotensi dikompromikan](#)
- Untuk memulihkan gambar kontainer yang dikompromikan, lihat. [Memulihkan gambar kontainer yang berpotensi dikompromikan](#)

## ECSCluster

Jika jenis Sumber Daya dalam rincian temuan adalah ECSCluster, ini menunjukkan bahwa tugas ECS atau wadah di dalam tugas ECS berpotensi dikompromikan.

### 1. Identifikasi cluster ECS yang terpengaruh

Temuan GuardDuty Runtime Monitoring memberikan detail cluster ECS di panel detail temuan atau di `resource.ecsClusterDetails` bagian di JSON temuan.

### 2. Identifikasi tugas ECS yang terpengaruh

Temuan GuardDuty Runtime Monitoring memberikan detail tugas ECS di panel detail temuan atau di `resource.ecsClusterDetails.taskDetails` bagian di JSON temuan.

### 3. Mengisolasi tugas yang terpengaruh

Mengisolasi tugas yang terkena dampak dengan menolak semua lalu lintas masuk dan keluar ke tugas. Menyangkal semua aturan lalu lintas dapat membantu menghentikan serangan yang sudah berlangsung, dengan memutuskan semua koneksi ke tugas.

### 4. Memulihkan tugas yang dikompromikan

- a. Identifikasi kerentanan yang mengganggu tugas.
- b. Terapkan perbaikan untuk kerentanan itu dan mulai tugas pengganti baru.
- c. Hentikan tugas yang rentan.

## Container

Jika tipe Resource dalam rincian temuan adalah Container, ini menunjukkan bahwa kontainer mandiri berpotensi dikompromikan.

- Untuk memulihkan, lihat [Memulihkan wadah mandiri yang berpotensi dikompromikan](#).
- Jika temuan dihasilkan di beberapa kontainer menggunakan gambar kontainer yang sama, lihat [Memulihkan gambar kontainer yang berpotensi dikompromikan](#).
- Jika penampung telah mengakses host EC2 yang mendasarinya, kredensial instans terkaitnya mungkin telah disusupi. Untuk informasi selengkapnya, lihat [Memulihkan kredensi yang berpotensi dikompromikan AWS](#).
- Jika aktor yang berpotensi berbahaya telah mengakses node EKS yang mendasarinya atau instans EC2, lihat remediasi yang disarankan di bawah tab EKSCluster dan Instance.

## Memulihkan gambar kontainer yang dikompromikan

Ketika sebuah GuardDuty temuan menunjukkan kompromi tugas, gambar yang digunakan untuk meluncurkan tugas bisa berbahaya atau dikompromikan. GuardDuty temuan mengidentifikasi gambar kontainer di dalam `resource.ecsClusterDetails.taskDetails.containers.image` lapangan. Anda dapat menentukan apakah gambar itu berbahaya atau tidak dengan memindainya untuk malware.

Untuk memulihkan gambar kontainer yang dikompromikan

1. Berhenti menggunakan gambar segera dan hapus dari repositori gambar Anda.
2. Identifikasi semua tugas yang menggunakan gambar ini.
3. Hentikan semua tugas yang menggunakan gambar yang disusupi. Perbarui definisi tugas mereka sehingga mereka berhenti menggunakan gambar yang disusupi.

## Memulihkan database yang berpotensi dikompromikan

GuardDuty menghasilkan [Jenis temuan Perlindungan RDS](#) yang menunjukkan perilaku login yang berpotensi mencurigakan dan anomali di Anda [Database yang didukung](#) setelah Anda mengaktifkan [RDSPerlindungan](#). Menggunakan aktivitas login RDS, GuardDuty analisis dan profil ancaman dengan mengidentifikasi pola yang tidak biasa dalam upaya login.

### Note

Anda dapat mengakses informasi lengkap tentang jenis temuan dengan memilihnya dari file [Tabel temuan](#).



Ikuti langkah-langkah yang disarankan ini untuk memulihkan database Amazon Aurora yang berpotensi dikompromikan di lingkungan Anda. AWS

## Topik

- [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil](#)
- [Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal](#)
- [Memulihkan kredensial yang berpotensi dikompromikan](#)
- [Batasi akses jaringan](#)

## Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang berhasil

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku tidak biasa terkait dengan peristiwa login yang berhasil.

### 1. Identifikasi database dan pengguna yang terpengaruh.

GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat [Detail temuan](#).

### 2. Konfirmasikan apakah perilaku ini diharapkan atau tidak terduga.

Daftar berikut menentukan skenario potensial yang mungkin menyebabkan GuardDuty untuk menghasilkan temuan:

- Seorang pengguna yang masuk ke database mereka setelah waktu yang lama berlalu.
- Seorang pengguna yang masuk ke database mereka sesekali, misalnya, seorang analis keuangan yang log in di setiap kuartal.
- Aktor yang berpotensi mencurigakan yang terlibat dalam upaya login yang berhasil berpotensi membahayakan database.

### 3. Mulailah langkah ini jika perilakunya tidak terduga.

#### 1. Batasi akses database

Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Lihat informasi yang lebih lengkap di [Memulihkan kredensial yang berpotensi dikompromikan](#) dan [Batasi akses jaringan](#).

2. Menilai dampak dan menentukan informasi apa yang diakses.
  - Jika tersedia, tinjau log audit untuk mengidentifikasi potongan-potongan informasi yang mungkin telah diakses. Untuk informasi selengkapnya, lihat [Memantau peristiwa, log, dan aliran di kluster DB Amazon Aurora](#) di Panduan Pengguna Amazon Aurora.
  - Tentukan apakah ada informasi sensitif atau dilindungi yang diakses atau dimodifikasi.

## Memulihkan database yang berpotensi dikompromikan dengan peristiwa login yang gagal

Langkah-langkah yang disarankan berikut dapat membantu Anda memulihkan database Aurora yang berpotensi dikompromikan yang menunjukkan perilaku yang tidak biasa terkait dengan peristiwa login yang gagal.

1. Identifikasi database dan pengguna yang terpengaruh.

GuardDuty Temuan yang dihasilkan memberikan nama database yang terpengaruh dan detail pengguna yang sesuai. Untuk informasi selengkapnya, lihat [Detail temuan](#).

2. Identifikasi sumber upaya login yang gagal.

GuardDuty Temuan yang dihasilkan menyediakan alamat IP dan organisasi ASN (jika itu adalah koneksi publik) di bawah bagian Aktor dari panel pencarian.

Autonomous System (AS) adalah sekelompok satu atau lebih awalan IP (daftar alamat IP yang dapat diakses pada jaringan) yang dijalankan oleh satu atau lebih operator jaringan yang mempertahankan kebijakan routing tunggal yang didefinisikan dengan jelas. Operator jaringan membutuhkan Autonomous System Numbers (ASN) untuk mengontrol routing dalam jaringan mereka dan untuk bertukar informasi routing dengan penyedia layanan internet (ISP) lainnya.

3. Konfirmasikan bahwa perilaku ini tidak terduga.

Periksa apakah aktivitas ini merupakan upaya untuk mendapatkan akses tidak sah tambahan ke database sebagai berikut:

- Jika sumbernya internal, periksa apakah aplikasi salah konfigurasi dan coba koneksi berulang kali.
- Jika ini adalah aktor eksternal, periksa apakah database yang sesuai menghadap publik atau salah konfigurasi dan dengan demikian memungkinkan pelaku jahat potensial untuk secara kasar memaksa nama pengguna umum.

#### 4. Mulailah langkah ini jika perilakunya tidak terduga.

##### 1. Batasi akses database

Batasi akses database untuk akun yang dicurigai dan sumber aktivitas login ini. Lihat informasi yang lebih lengkap di [Memulihkan kredensial yang berpotensi dikompromikan](#) dan [Batasi akses jaringan](#).

##### 2. Lakukan analisis akar penyebab dan tentukan langkah-langkah yang berpotensi menyebabkan aktivitas ini.

Siapkan peringatan untuk mendapatkan pemberitahuan saat aktivitas mengubah kebijakan jaringan dan membuat status tidak aman. Untuk informasi selengkapnya, lihat [Kebijakan Firewall AWS Network Firewall](#) di Panduan AWS Network Firewall Pengembang.

## Memulihkan kredensial yang berpotensi dikompromikan

GuardDuty Temuan dapat menunjukkan bahwa kredensial pengguna untuk database yang terpengaruh telah dikompromikan ketika pengguna yang diidentifikasi dalam temuan telah melakukan operasi database yang tidak terduga. Anda dapat mengidentifikasi pengguna di bagian detail pengguna RDS DB dalam panel pencarian di konsol, atau di `resource.rdsDbUserDetails` dalam temuan JSON. Detail pengguna ini termasuk nama pengguna, aplikasi yang digunakan, database diakses, versi SSL, dan metode otentikasi.

- Untuk mencabut akses atau memutar kata sandi untuk pengguna tertentu yang terlibat dalam temuan, lihat [Keamanan dengan Amazon Aurora MySQL, atau Keamanan dengan Amazon Aurora PostgreSQL di Panduan Pengguna Amazon Aurora](#).
- Gunakan AWS Secrets Manager untuk menyimpan dengan aman dan secara otomatis memutar rahasia untuk database Amazon Relational Database Service (RDS). Untuk informasi selengkapnya, lihat [AWS Secrets Manager tutorial](#) di Panduan AWS Secrets Manager Pengguna.
- Gunakan autentikasi basis data IAM untuk mengelola akses pengguna database tanpa perlu kata sandi. Untuk informasi selengkapnya, lihat [autentikasi database IAM](#) di Panduan Pengguna Amazon Aurora.

Untuk informasi selengkapnya, lihat [Praktik terbaik keamanan untuk Amazon Relational Database Service](#) di Panduan Pengguna Amazon RDS.

## Batasi akses jaringan

GuardDuty Temuan mungkin menunjukkan bahwa database dapat diakses di luar aplikasi Anda, atau Virtual Private Cloud (VPC). Jika alamat IP jarak jauh dalam temuan adalah sumber koneksi yang tidak terduga, audit grup keamanan. Daftar grup keamanan yang dilampirkan ke database tersedia di bawah Grup keamanan di konsol <https://console.aws.amazon.com/rds/>, atau di `resource.rdsDbInstanceDetails.dbSecurityGroups` temuan JSON. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan, lihat [Mengontrol akses dengan grup keamanan](#) di Panduan Pengguna Amazon RDS.

Jika Anda menggunakan firewall, batasi akses jaringan ke database dengan mengkonfigurasi ulang Network Access Control Lists (NACLs). Untuk informasi selengkapnya, lihat [Firewall AWS Network Firewall](#) di Panduan AWS Network Firewall Pengembang.

## Memperbaiki fungsi Lambda yang berpotensi dikompromikan

Saat GuardDuty menghasilkan temuan Perlindungan Lambda dan aktivitasnya tidak terduga, fungsi Lambda Anda dapat dikompromikan. Kami merekomendasikan untuk menyelesaikan langkah-langkah berikut untuk memulihkan fungsi Lambda yang dikompromikan.

Untuk memulihkan temuan Perlindungan Lambda

1. Identifikasi versi fungsi Lambda yang berpotensi dikompromikan.

GuardDuty Temuan untuk Perlindungan Lambda menyediakan nama, Nama Sumber Daya Amazon (ARN), versi fungsi, dan ID revisi yang terkait dengan fungsi Lambda yang tercantum dalam detail temuan.

2. Identifikasi sumber aktivitas yang berpotensi mencurigakan.
  - a. Tinjau kode yang terkait dengan versi fungsi Lambda yang terlibat dalam temuan.
  - b. Tinjau pustaka dan lapisan yang diimpor dari versi fungsi Lambda yang terlibat dalam temuan.
  - c. Jika Anda telah mengaktifkan [AWS Lambda fungsi Pemindaian dengan Amazon Inspector](#), tinjau temuan [Amazon Inspector](#) yang terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.
  - d. Tinjau AWS CloudTrail log untuk mengidentifikasi prinsipal yang menyebabkan pembaruan fungsi dan memastikan bahwa aktivitas tersebut diotorisasi atau diharapkan.

3. Memperbaiki fungsi Lambda yang berpotensi terganggu.
  - a. Nonaktifkan pemicu eksekusi fungsi Lambda yang terlibat dalam temuan. Untuk informasi lebih lanjut, lihat [DeleteFunctionEventInvokeConfig](#).
  - b. Tinjau kode Lambda dan perbarui impor pustaka dan lapisan [fungsi Lambda](#) untuk menghapus pustaka dan lapisan yang berpotensi mencurigakan.
  - c. Mengurangi temuan Amazon Inspector terkait dengan fungsi Lambda yang terlibat dalam temuan tersebut.

# Memperkirakan biaya GuardDuty

Selama uji coba gratis 30 hari, Anda dapat menggunakan GuardDuty konsol atau API operasi untuk memperkirakan biaya penggunaan rata-rata harian. GuardDuty Estimasi biaya memproyeksikan berapa perkiraan biaya Anda setelah masa percobaan. Namun, untuk meninjau perkiraan biaya yang akurat selama uji coba gratis, GuardDuty merekomendasikan untuk menggunakan AWS Billing at <https://console.aws.amazon.com/billing/>.

Saat Anda beroperasi di lingkungan beberapa akun, akun GuardDuty administrator dapat memantau metrik biaya untuk semua akun anggota.

## Catatan tentang Perlindungan Malware untuk biaya penggunaan S3

Biaya penggunaan untuk Perlindungan Malware untuk S3 tidak termasuk dalam Penggunaan di GuardDuty konsol. Untuk informasi selengkapnya, lihat [Melihat penggunaan dan biaya untuk Perlindungan Malware untuk S3](#).

Anda dapat melihat estimasi biaya berdasarkan metrik berikut:

- ID Akun — Daftar perkiraan biaya untuk akun Anda, atau untuk akun anggota Anda jika Anda beroperasi sebagai akun akun GuardDuty administrator.
- Sumber data - Daftar perkiraan biaya untuk setiap sumber data dasar - peristiwa AWS CloudTrail manajemen, log VPC aliran, dan log kueri Route53 DNS Resolver.
- Fitur - Daftar perkiraan biaya untuk GuardDuty fitur - peristiwa CloudTrail data untuk S3, Pemantauan Log EKS Audit, data EBS volume, aktivitas RDS login, Pemantauan Runtime, Pemantauan EKS Runtime Fargate, Pemantauan Waktu Proses, atau Pemantauan Aktivitas EC2 Jaringan Lambda.
- Bucket S3 — Daftar perkiraan biaya untuk kejadian data S3 pada bucket tertentu atau bucket termahal untuk akun di lingkungan Anda. Statistik ini hanya tersedia jika Anda mengaktifkan [Perlindungan S3](#) untuk file Akun AWS.

## Memahami cara GuardDuty menghitung biaya penggunaan

Perkiraan yang ditampilkan di GuardDuty konsol mungkin sedikit berbeda dari yang ada di AWS Billing and Cost Management konsol Anda. Daftar berikut menjelaskan bagaimana GuardDuty perkiraan biaya penggunaan:

- Perkiraan GuardDuty penggunaan hanya untuk Wilayah saat ini.
- Biaya GuardDuty penggunaan didasarkan pada 30 hari terakhir penggunaan.
- Perkiraan biaya penggunaan uji coba mencakup perkiraan untuk sumber data dasar dan fitur yang saat ini dalam masa uji coba. Setiap fitur dan sumber data di dalamnya GuardDuty memiliki masa uji coba sendiri tetapi mungkin tumpang tindih dengan periode uji coba GuardDuty atau fitur lain yang diaktifkan pada saat yang sama.
- Perkiraan GuardDuty penggunaan mencakup diskon harga GuardDuty volume per Wilayah, seperti yang dijelaskan di halaman [GuardDuty Harga Amazon](#), tetapi hanya untuk akun individu yang memenuhi tingkatan harga volume. Diskon harga volume tidak termasuk dalam perkiraan untuk penggunaan total gabungan antar akun dalam suatu organisasi. Untuk informasi tentang harga diskon volume penggunaan gabungan, lihat [Penagihan AWS : Diskon Volume](#).
- Jumlah biaya penggunaan untuk masing-masing Akun AWS di organisasi Anda mungkin tidak selalu sama dengan perkiraan biaya 30 hari terakhir untuk sumber data yang dipilih. Tingkat harga dapat berubah saat GuardDuty memproses lebih banyak peristiwa atau data. Untuk informasi selengkapnya, lihat [Tingkat Harga](#) di Panduan AWS Billing Pengguna.

Skenario ini menjelaskan bahwa untuk menghentikan biaya penggunaan untuk Runtime Monitoring, Anda harus menonaktifkan fitur Runtime Monitoring dan EKS Runtime Monitoring.

GuardDuty telah mengkonsolidasikan pengalaman konsol untuk EKS Runtime Monitoring ke Runtime Monitoring. GuardDuty merekomendasikan [Memeriksa EKS status konfigurasi Runtime Monitoring](#) dan [Migrasi dari EKS Runtime Monitoring ke Runtime Monitoring](#).

Sebagai bagian dari migrasi ke Runtime Monitoring, pastikan untuk [Nonaktifkan EKS Runtime Monitoring](#). Ini penting karena jika nanti Anda memilih untuk menonaktifkan Runtime Monitoring dan Anda tidak menonaktifkan EKS Runtime Monitoring, Anda akan terus mengeluarkan biaya penggunaan untuk Runtime Monitoring. EKS

## Runtime Monitoring - Bagaimana VPC flow log dari EC2 instans memengaruhi biaya penggunaan

Saat Anda mengelola agen keamanan (baik secara manual atau melalui GuardDuty) di EKS Runtime Monitoring atau Runtime Monitoring untuk EC2 instance, dan saat GuardDuty ini digunakan di instans EC2 Amazon dan menerima [Jenis acara runtime yang dikumpulkan](#) dari instance ini GuardDuty , Akun AWS Anda tidak akan membebankan biaya untuk analisis VPC log aliran dari instans Amazon ini. EC2 Ini membantu GuardDuty menghindari biaya penggunaan ganda di akun.

## Bagaimana GuardDuty memperkirakan biaya penggunaan untuk CloudTrail acara

Ketika Anda mengaktifkan GuardDuty, secara otomatis mulai menggunakan log AWS CloudTrail peristiwa yang direkam untuk akun Anda di yang dipilih Wilayah AWS. GuardDuty mereplikasi log [peristiwa layanan Global](#) dan kemudian memproses peristiwa ini secara independen di setiap Wilayah yang telah Anda GuardDuty aktifkan. Ini membantu GuardDuty menjaga profil pengguna dan peran di setiap Wilayah untuk mengidentifikasi anomali.

CloudTrail Konfigurasi Anda tidak memengaruhi biaya GuardDuty penggunaan atau cara GuardDuty memproses log peristiwa Anda. Biaya GuardDuty penggunaan Anda dipengaruhi oleh penggunaan AWS APIs log to Anda CloudTrail. Untuk informasi selengkapnya, lihat [AWS CloudTrail acara manajemen](#).

## Meninjau statistik GuardDuty penggunaan

Pilih metode akses pilihan Anda untuk meninjau statistik penggunaan GuardDuty akun Anda. Jika Anda adalah akun GuardDuty administrator, metode berikut akan membantu Anda meninjau statistik penggunaan untuk semua anggota.

### Console

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

Pastikan untuk menggunakan akun GuardDuty administrator.

2. Pada panel navigasi, pilih Penggunaan.
3. Pada halaman Penggunaan, akun GuardDuty administrator dengan akun anggota dapat melihat Perkiraan biaya organisasi selama 30 hari terakhir. Ini adalah perkiraan total biaya penggunaan untuk organisasi Anda.



4. GuardDuty akun administrator dengan anggota dapat melihat rincian biaya penggunaan berdasarkan sumber data atau oleh akun. Akun individu atau mandiri dapat melihat rincian berdasarkan sumber data.

Jika Anda memiliki akun anggota, Anda dapat melihat statistik untuk akun individual dengan memilih akun tersebut di tabel Akun.

Di bawah tab Berdasarkan sumber data, saat Anda memilih sumber data yang memiliki biaya penggunaan yang terkait dengannya, jumlah rincian biaya yang sesuai di tingkat akun mungkin tidak selalu sama.

## API/CLI

Jalankan [GetUsageStatistics](#) API operasi menggunakan kredensial akun GuardDuty administrator. Berikan informasi berikut untuk menjalankan perintah:

- (Wajib) berikan ID GuardDuty detektor Regional dari akun yang ingin Anda ambil statistiknya.
- (Wajib) berikan salah satu jenis statistik untuk diambil: `SUM_BY_ACCOUNT` | `SUM_BY_DATA_SOURCE` | `SUM_BY_RESOURCE` | `SUM_BY_FEATURE` | `TOP_ACCOUNTS_BY_FEATURE`.

Saat ini, `TOP_ACCOUNTS_BY_FEATURE` tidak mendukung pengambilan statistik penggunaan untuk `RDS_LOGIN_EVENTS`.

- (Wajib) menyediakan satu atau beberapa sumber data atau fitur untuk menanyakan statistik penggunaan Anda.
- (Opsional) berikan daftar akun IDs yang ingin Anda ambil statistik penggunaannya.

Anda juga dapat menggunakan AWS Command Line Interface. Perintah berikut adalah contoh tentang mengambil statistik penggunaan untuk semua sumber data dan fitur, dihitung oleh akun. Pastikan untuk mengganti `detector-id` dengan ID detektor valid Anda sendiri. Untuk akun mandiri, perintah ini mengembalikan biaya penggunaan selama 30 hari terakhir hanya untuk akun Anda. Jika Anda adalah akun GuardDuty administrator dengan akun anggota, Anda melihat biaya yang tercantum berdasarkan akun untuk semua anggota.

Untuk menemukan akun Anda dan Wilayah saat ini, lihat halaman Pengaturan di <https://console.aws.amazon.com/guardduty/konsol>, atau jalankan [ListDetectors](#) API. `detectorId`

Ganti `SUM_BY_ACCOUNT` dengan jenis yang Anda inginkan untuk menghitung statistik penggunaan.

Untuk memantau biaya hanya untuk sumber data

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
"EC2_MALWARE_SCAN"]}'
```

Untuk memantau biaya untuk fitur

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
--usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
"EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
"EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

# Keamanan di Amazon GuardDuty

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. [Model Tanggung Jawab Bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan-layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara rutin efektivitas keamanan kami sebagai bagian dari [program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku GuardDuty, lihat [AWSlayanan dalam cakupan melalui program kepatuhanAWS](#).
- 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 undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan GuardDuty. Dokumentasi ini juga menunjukkan kepada Anda cara mengonfigurasi GuardDuty untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan GuardDuty sumber daya Anda.

## Konten

- [Perlindungan data di Amazon GuardDuty](#)
- [Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail](#)
- [Identity and Access Management untuk Amazon GuardDuty](#)
- [Validasi kepatuhan untuk Amazon GuardDuty](#)
- [Ketahanan di Amazon GuardDuty](#)
- [Keamanan infrastruktur di Amazon GuardDuty](#)

# Perlindungan data di Amazon GuardDuty

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon GuardDuty. 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 GuardDuty 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.

## Enkripsi diam

Semua data GuardDuty pelanggan dienkripsi saat istirahat menggunakan solusi AWS enkripsi.

GuardDuty data, seperti temuan, dienkripsi saat istirahat menggunakan AWS Key Management Service (AWS KMS) menggunakan kunci yang dikelola pelanggan yang AWS dimiliki.

## Enkripsi bergerak

GuardDuty menganalisis data log dari layanan lain. Ini mengenkripsi semua data dalam perjalanan dari layanan ini dengan HTTPS dan KMS. Setelah GuardDuty mengekstrak informasi yang dibutuhkan dari log, mereka dibuang. Untuk informasi selengkapnya tentang cara GuardDuty menggunakan informasi dari layanan lain, lihat [sumber GuardDuty data](#).

GuardDuty data dienkripsi dalam perjalanan antar layanan.

## Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan

Anda dapat memilih untuk tidak menggunakan data Anda untuk mengembangkan dan meningkatkan GuardDuty dan layanan AWS keamanan lainnya dengan menggunakan kebijakan AWS Organizations opt-out. Anda dapat memilih untuk memilih keluar meskipun saat ini GuardDuty tidak mengumpulkan data tersebut. Untuk informasi selengkapnya tentang cara memilih keluar, lihat [kebijakan opt-out layanan AI](#) di AWS Organizations Panduan Pengguna.

### Note

Agar Anda dapat menggunakan kebijakan opt-out, AWS akun Anda harus dikelola secara terpusat oleh AWS Organizations. Jika Anda belum membuat organisasi untuk AWS akun Anda, lihat [Membuat dan mengelola organisasi](#) di Panduan AWS Organizations Pengguna.

Memilih keluar memiliki efek sebagai berikut:

- GuardDuty akan menghapus data yang dikumpulkan dan disimpan untuk tujuan peningkatan layanan sebelum Anda memilih keluar (jika ada).
- Setelah Anda memilih keluar, tidak GuardDuty akan lagi mengumpulkan atau menyimpan data ini untuk tujuan peningkatan layanan.

Topik berikut menjelaskan bagaimana setiap fitur dalam GuardDuty berpotensi menangani data Anda untuk peningkatan layanan.

## Daftar Isi

- [GuardDuty Pemantauan Runtime](#)
- [GuardDuty Perlindungan Malware](#)

## GuardDuty Pemantauan Runtime

GuardDuty Runtime Monitoring menyediakan deteksi ancaman runtime untuk AWS Fargate (Fargate) cluster Amazon Elastic Kubernetes Service (Amazon), EKS Amazon Elastic Container Service (Amazon) saja, dan instans ECS Amazon Elastic Compute Cloud (Amazon) di lingkungan Anda. EC2 AWS Setelah Anda mengaktifkan Runtime Monitoring dan menyebarkan agen GuardDuty keamanan untuk sumber daya Anda, GuardDuty mulai memantau dan menganalisis peristiwa runtime yang terkait dengan sumber daya Anda. Jenis acara runtime ini mencakup peristiwa proses, peristiwa kontainer, DNS acara, dan banyak lagi. Untuk informasi selengkapnya, lihat [Jenis acara runtime yang dikumpulkan yang menggunakan GuardDuty](#).

Meskipun GuardDuty sekarang mengumpulkan argumen baris perintah yang mungkin Anda arahkan ke beban kerja Anda, saat ini argumen ini tidak menggunakan argumen ini untuk tujuan peningkatan layanan (mungkin melakukannya di masa mendatang). Kami telah mulai mengumpulkan argumen baris perintah untuk mengantisipasi aturan deteksi ancaman baru dan temuan yang akan segera dirilis. Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas utama kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat [Privasi Data FAQ](#).

## GuardDuty Perlindungan Malware

GuardDuty Perlindungan Malware memindai dan mendeteksi malware yang terdapat dalam EBS volume yang dilampirkan ke instans EC2 Amazon dan beban kerja container yang berpotensi dikompromikan, serta file yang baru diunggah di bucket Amazon S3 pilihan Anda. Saat ini, GuardDuty tidak mengumpulkan atau menggunakan malware yang terdeteksi untuk peningkatan layanan. Namun, di masa depan, ketika Perlindungan GuardDuty Malware mengidentifikasi file EBS volume atau file S3 sebagai berbahaya atau berbahaya, Perlindungan GuardDuty Malware akan mengumpulkan dan menyimpan file ini untuk mengembangkan dan meningkatkan deteksi malware, dan layanannya. GuardDuty File ini juga dapat digunakan untuk mengembangkan dan meningkatkan layanan AWS keamanan lainnya. Kepercayaan, privasi, dan keamanan konten Anda adalah prioritas

utama kami, dan memastikan bahwa penggunaan kami sesuai dengan komitmen kami kepada Anda. Untuk informasi selengkapnya, lihat [Privasi Data FAQ](#).

## Mencatat panggilan GuardDuty API Amazon dengan AWS CloudTrail

Amazon GuardDuty terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di GuardDuty. CloudTrail menangkap semua panggilan API untuk GuardDuty sebagai peristiwa, termasuk panggilan dari GuardDuty konsol dan dari panggilan kode ke GuardDuty API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk acara untuk GuardDuty. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat GuardDuty, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat [Panduan AWS CloudTrail Pengguna](#).

### GuardDuty informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di GuardDuty, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk GuardDuty, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat :

- [Ikhtisar untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)

- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan pengguna root atau kredensial masuk pengguna IAM
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi selengkapnya, lihat elemen [CloudTrail UserIdentity](#).

## GuardDuty peristiwa pesawat kontrol di CloudTrail

Secara default, CloudTrail mencatat semua operasi GuardDuty API yang disediakan di [Referensi Amazon GuardDuty API](#) sebagai peristiwa dalam CloudTrail file.

## GuardDuty peristiwa data di CloudTrail

[GuardDuty Pemantauan Runtime](#) menggunakan agen GuardDuty keamanan yang diterapkan ke kluster Amazon Elastic Kubernetes Service (Amazon EKS), instans Amazon Elastic Compute Cloud (Amazon EC2), dan (Amazon Elastic Container Service (AWS FargateAmazon ECS) saja) `aws-guardduty-agent` tugas untuk mengumpulkan add-on () yang mengumpulkan beban kerja Anda dan kemudian mengirimkannya [Jenis acara runtime yang dikumpulkan](#) ke untuk deteksi dan analisis ancaman. AWS GuardDuty

## Pencatatan dan pemantauan peristiwa data

Anda dapat mengonfigurasi AWS CloudTrail log secara opsional untuk melihat peristiwa data untuk agen GuardDuty keamanan Anda.

Untuk membuat dan mengonfigurasi CloudTrail, lihat [Peristiwa data](#) di Panduan AWS CloudTrail Pengguna dan ikuti petunjuk untuk Mencatat peristiwa data dengan pemilih peristiwa lanjutan di AWS Management Console. Saat mencatat jejak, pastikan untuk membuat perubahan berikut:

- Untuk tipe peristiwa Data, pilih GuardDuty detektor.



- Untuk template pemilih Log, pilih Log semua peristiwa.
- Perluas tampilan JSON untuk konfigurasi. Ini harus mirip dengan JSON berikut:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

[Setelah Anda mengaktifkan pemilih untuk jejak, navigasikan ke konsol Amazon S3 di https://console.aws.amazon.com/s3/](https://console.aws.amazon.com/s3/). Anda dapat mengunduh peristiwa data dari bucket S3 yang dipilih pada saat mengonfigurasi log. CloudTrail

## Contoh: entri file GuardDuty log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa bidang data.

```
{
  "eventVersion": "1.08",
```

```
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
      "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
      "accountId": "111122223333",
      "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "111122223333:aws:ec2-instance",
          "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
          "accountId": "111122223333",
          "userName": "aws:ec2-instance"
        },
        "attributes": {
          "creationDate": "2023-03-05T04:00:21Z",
          "mfaAuthenticated": "false"
        },
        "ec2RoleDelivery": "2.0"
      }
    },
    "eventTime": "2023-03-05T06:03:49Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "SendSecurityTelemetry",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbb",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::GuardDuty::Detector",
      "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
```

```

    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
  }
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateIPThreatIntelSet tindakan (peristiwa bidang kontrol).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "userName": "Alice"
      }
    }
  },
  "eventTime": "2018-06-14T22:57:56Z",
  "eventSource": "guardduty.amazonaws.com",
  "eventName": "CreateThreatIntelSet",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "54.240.230.177",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
    "name": "Example",
    "format": "TXT",
    "activate": false,
    "location": "https://s3.amazonaws.com/bucket.name/file.txt"
  }
}

```

```
    },
    "responseElements": {
      "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
  }
```

Dari informasi acara ini, Anda dapat menentukan bahwa permintaan dibuat untuk membuat daftar ancaman Example di GuardDuty. Anda juga dapat melihat bahwa permintaan tersebut dibuat oleh pengguna bernama Alice pada 14 Juni 2018.

## Identity and Access Management untuk Amazon GuardDuty

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. GuardDuty IAM adalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

### Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon GuardDuty bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)
- [Menggunakan peran terkait layanan untuk Amazon GuardDuty](#)
- [AWS kebijakan terkelola untuk Amazon GuardDuty](#)
- [Memecahkan masalah GuardDuty identitas dan akses Amazon](#)

## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan GuardDuty.

Pengguna layanan — Jika Anda menggunakan GuardDuty layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak GuardDuty fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di GuardDuty, lihat [Memecahkan masalah GuardDuty identitas dan akses Amazon](#).

Administrator layanan — Jika Anda bertanggung jawab atas GuardDuty sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke GuardDuty. Tugas Anda adalah menentukan GuardDuty fitur dan sumber daya 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 menggunakannya IAM GuardDuty, lihat [Bagaimana Amazon GuardDuty bekerja dengan IAM](#).

IAM administrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses GuardDuty. Untuk melihat contoh kebijakan GuardDuty berbasis identitas yang dapat Anda gunakan, lihat. IAM [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

## 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

[IAM Pengguna](#) 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.

[IAM Grup](#) 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.

## IAM peran

[IAM Peran](#) 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.

IAM peran 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 mengautentikasi, 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 mengkorelasikan izin yang disetel ke peran. IAM 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 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. 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 instans yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat [Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon](#) di IAMPanduan 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 Anda lampirkan 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 dilampirkan 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

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 IAMPanduan Pengguna.

- 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 organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, 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 Amazon GuardDuty bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses GuardDuty, pelajari IAM fitur apa yang tersedia untuk digunakan GuardDuty.

## IAMfitur yang dapat Anda gunakan dengan Amazon GuardDuty

| IAMfitur                                       | GuardDuty dukungan |
|--|--------------------|
| <a href="#">Kebijakan berbasis identitas</a>   | Ya                 |
| <a href="#">Kebijakan berbasis sumber daya</a> | Tidak              |
| <a href="#">Tindakan kebijakan</a>             | Ya                 |
| <a href="#">Sumber daya kebijakan</a>          | Ya                 |
| <a href="#">Kunci kondisi kebijakan</a>        | Ya                 |
| <a href="#">ACLs</a>                           | Tidak              |
| <a href="#">ABAC(tag dalam kebijakan)</a>      | Parsial            |
| <a href="#">Kredensial sementara</a>           | Ya                 |
| <a href="#">Izin prinsipal</a>                 | Ya                 |
| <a href="#">Peran layanan</a>                  | Ya                 |
| <a href="#">Peran terkait layanan</a>          | Ya                 |

Untuk mendapatkan tampilan tingkat tinggi tentang cara GuardDuty dan AWS layanan lain bekerja dengan sebagian besar IAM fitur, lihat [AWS layanan yang berfungsi IAM](#) di Panduan IAM Pengguna.

### Kebijakan berbasis identitas untuk GuardDuty

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan 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 IAM Pengguna.

Contoh kebijakan berbasis identitas untuk GuardDuty

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

## Kebijakan berbasis sumber daya dalam GuardDuty

Mendukung kebijakan berbasis sumber daya: Tidak

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.

## Tindakan kebijakan untuk GuardDuty

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 GuardDuty tindakan, lihat [Tindakan yang ditentukan oleh Amazon GuardDuty](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan GuardDuty menggunakan awalan berikut sebelum tindakan:

```
guardduty
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
  "guardduty:action1",  
  "guardduty:action2"  
]
```

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

## Sumber daya kebijakan untuk GuardDuty

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 dan jenis GuardDuty sumber daya ARNs, lihat [Sumber daya yang ditentukan oleh Amazon GuardDuty](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh Amazon GuardDuty](#).

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

## Kunci kondisi kebijakan untuk GuardDuty

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 GuardDuty kondisi, lihat [Kunci kondisi untuk Amazon GuardDuty](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon GuardDuty](#).

Untuk melihat contoh kebijakan GuardDuty berbasis identitas, lihat. [Contoh kebijakan berbasis identitas untuk Amazon GuardDuty](#)

## Daftar kontrol akses (ACLs) di GuardDuty

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

## Kontrol akses berbasis atribut ( ) ABAC dengan GuardDuty

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 IAMPanduan Pengguna.



## Menggunakan kredensi Sementara dengan GuardDuty

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

## Izin utama lintas layanan untuk GuardDuty

Mendukung sesi akses maju (FAS): Ya

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 GuardDuty

Mendukung peran layanan: Ya

Peran layanan adalah [IAMperan](#) 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.

#### Warning

Mengubah izin untuk peran layanan dapat merusak GuardDuty fungsionalitas. Edit peran layanan hanya jika GuardDuty memberikan panduan untuk melakukannya.

## Peran terkait layanan untuk GuardDuty

Mendukung peran terkait layanan: Ya

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. IAM Administrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran GuardDuty terkait layanan, lihat [Menggunakan peran terkait layanan untuk Amazon GuardDuty](#)

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 Amazon GuardDuty

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi GuardDuty sumber daya. 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 GuardDuty, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Amazon GuardDuty](#) di Referensi Otorisasi Layanan.

## Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol GuardDuty](#)
- [Izin diperlukan untuk mengaktifkan GuardDuty](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [IAMKebijakan khusus untuk memberikan akses hanya-baca GuardDuty](#)
- [Tolak Akses ke GuardDuty Temuan](#)
- [Menggunakan IAM kebijakan khusus untuk membatasi akses ke GuardDuty sumber daya](#)

## Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus GuardDuty sumber daya 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 AWSAWS 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 tersebut mematuhi bahasa IAM kebijakan ( ) JSON dan praktik terbaik. IAM IAMAccess 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 dalam Anda 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 diIAM, lihat [Praktik terbaik keamanan IAM di](#) Panduan IAM Pengguna.

## Menggunakan konsol GuardDuty

Untuk mengakses GuardDuty konsol Amazon, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang GuardDuty sumber daya di 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 memastikan bahwa pengguna dan peran masih dapat menggunakan GuardDuty konsol, lampirkan juga kebijakan GuardDuty ConsoleAccess atau ReadOnly AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambahkan izin ke pengguna](#) di Panduan IAM Pengguna.

## Izin diperlukan untuk mengaktifkan GuardDuty

Untuk memberikan izin yang harus dimiliki oleh berbagai IAM identitas (pengguna, grup, dan peran), lampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) kebijakan yang diperlukan untuk mengaktifkan. GuardDuty

## Mengizinkan pengguna 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 atau. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "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": "*"
    }
  ]
}
```

## IAMKebijakan khusus untuk memberikan akses hanya-baca GuardDuty

Untuk memberikan akses hanya-baca ke GuardDuty Anda dapat menggunakan kebijakan AmazonGuardDutyReadOnlyAccess terkelola.

Untuk membuat kebijakan khusus yang memberikan akses hanya-baca IAM peran, pengguna, atau grup GuardDuty, Anda dapat menggunakan pernyataan berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:ListMembers",
        "guardduty:GetMembers",
        "guardduty:ListInvitations",
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "guardduty:ListFindings",
        "guardduty:GetFindings",
        "guardduty:ListIPSets",
        "guardduty:GetIPSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetInvitationsCount",
        "guardduty:GetFindingsStatistics",
        "guardduty:DescribeMalwareScans",
        "guardduty:UpdateMalwareScanSettings",
        "guardduty:GetMalwareScanSettings"
      ],
      "Resource": "*"
    }
  ]
}
```

## Tolak Akses ke GuardDuty Temuan

Anda dapat menggunakan kebijakan berikut untuk menolak akses IAM peran, pengguna, atau grup ke GuardDuty temuan. Pengguna tidak dapat melihat temuan atau detail tentang temuan, tetapi mereka dapat mengakses semua GuardDuty operasi lainnya:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty>DeleteDetector",
        "guardduty:UpdateDetector",
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:CreateIPSet",
        "guardduty>DeleteIPSet",
        "guardduty:UpdateIPSet",
        "guardduty:GetIPSet",
        "guardduty:ListIPSets",
        "guardduty:CreateThreatIntelSet",
        "guardduty>DeleteThreatIntelSet",
        "guardduty:UpdateThreatIntelSet",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:ArchiveFindings",
        "guardduty:UnarchiveFindings",
        "guardduty:CreateSampleFindings",
        "guardduty:CreateMembers",
        "guardduty:InviteMembers",
        "guardduty:GetMembers",
        "guardduty>DeleteMembers",
        "guardduty:DisassociateMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:ListMembers",
        "guardduty:GetMasterAccount",
        "guardduty:DisassociateFromMasterAccount",
        "guardduty:AcceptAdministratorInvitation",
        "guardduty:ListInvitations",
        "guardduty:GetInvitationsCount",
        "guardduty:DeclineInvitations",
        "guardduty>DeleteInvitations"
      ],
      "Resource": "*"
    },
    {
```

```
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "guardduty.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  }
]
```

## Menggunakan IAM kebijakan khusus untuk membatasi akses ke GuardDuty sumber daya

Untuk menentukan akses pengguna GuardDuty berdasarkan ID detektor, Anda dapat menggunakan semua [GuardDutyAPItindakan](#) dalam IAM kebijakan kustom, kecuali operasi berikut:

- guardduty:CreateDetector
- guardduty:DeclineInvitations
- guardduty>DeleteInvitations
- guardduty:GetInvitationsCount
- guardduty>ListDetectors
- guardduty>ListInvitations

Gunakan operasi berikut dalam IAM kebijakan untuk menentukan akses pengguna GuardDuty berdasarkan IPSet ID dan ThreatIntelSet ID:



- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Contoh berikut ini menunjukkan cara membuat kebijakan menggunakan beberapa operasi sebelumnya:

- Kebijakan ini memungkinkan pengguna untuk menjalankan operasi `guardduty:UpdateDetector`, menggunakan ID detektor 1234567 di Wilayah us-east-1:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor 1234567 dan ID 000000 di IPSet Wilayah us-east-1:

#### Note

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP terpercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman](#).

```
{
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "guardduty:UpdateIPSet",
        ],
        "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
      }
    ]
  }

```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor dan ID 000000 di Wilayah us-east-1: IPSet

#### Note

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP tepercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [izin yang diperlukan untuk mengunggah daftar IP tepercaya dan daftar ancaman](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
    }
  ]
}

```

- Kebijakan ini memungkinkan pengguna untuk menjalankan `guardduty:UpdateIPSet` operasi, menggunakan ID detektor dan IPSet ID apa pun di Wilayah us-east-1:

**Note**

Pastikan bahwa pengguna memiliki izin yang diperlukan untuk mengakses daftar IP terpercaya dan daftar ancaman di GuardDuty. Untuk informasi selengkapnya, lihat [Izin yang diperlukan untuk mengunggah daftar IP terpercaya dan daftar ancaman](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet",
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
    }
  ]
}
```

## Menggunakan peran terkait layanan untuk Amazon GuardDuty

Amazon GuardDuty menggunakan AWS Identity and Access Management (IAM) peran [terkait layanan](#). Peran terkait layanan (SLR) adalah jenis IAM peran unik yang ditautkan langsung ke GuardDuty. Peran terkait layanan telah ditentukan sebelumnya oleh GuardDuty dan menyertakan semua izin yang GuardDuty diperlukan untuk memanggil AWS layanan lain atas nama Anda.

Dengan peran terkait layanan, Anda dapat mengatur GuardDuty tanpa menambahkan izin yang diperlukan secara manual. GuardDuty mendefinisikan izin peran terkait layanan, dan kecuali izin ditentukan sebaliknya, hanya GuardDuty dapat mengambil peran tersebut. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas lain. IAM

GuardDuty mendukung penggunaan peran terkait layanan di semua Wilayah yang tersedia GuardDuty. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

Anda dapat menghapus peran GuardDuty terkait layanan hanya setelah pertama kali menonaktifkan GuardDuty di semua Wilayah yang diaktifkan. Ini melindungi GuardDuty sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengaksesnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang berfungsi IAM](#) di Panduan IAM Pengguna dan cari layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

## Izin peran terkait layanan untuk GuardDuty

GuardDuty menggunakan peran terkait layanan (SLR) bernama.

`AWSServiceRoleForAmazonGuardDuty` SLR memungkinkan GuardDuty untuk melakukan tugas-tugas berikut. Ini juga memungkinkan GuardDuty untuk memasukkan metadata yang diambil milik EC2 instance dalam temuan yang GuardDuty dapat menghasilkan tentang potensi ancaman. Peran terkait layanan `AWSServiceRoleForAmazonGuardDuty` memercayai layanan `guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin membantu GuardDuty melakukan tugas-tugas berikut:

- Gunakan EC2 tindakan Amazon untuk mengelola dan mengambil informasi tentang EC2 instans, gambar, dan komponen jaringan Anda seperti VPCs, subnet, dan gateway transit.
- Gunakan AWS Systems Manager tindakan untuk mengelola SSM asosiasi di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (`GuardDutyManaged:true`).
- Gunakan AWS Organizations tindakan untuk mendeskripsikan akun terkait dan ID organisasi.
- Gunakan tindakan Amazon S3 untuk mengambil informasi tentang bucket dan objek S3.
- Gunakan AWS Lambda tindakan untuk mengambil informasi tentang fungsi dan tag Lambda Anda.
- Gunakan EKS tindakan Amazon untuk mengelola dan mengambil informasi tentang EKS kluster dan mengelola [EKSSadd-on Amazon](#) di kluster. EKS EKSTindakan juga mengambil informasi tentang tag yang terkait GuardDuty dengan.
- Gunakan IAM untuk membuat Perlindungan Malware [Izin peran terkait layanan untuk Perlindungan Malware untuk EC2](#) EC2 setelah diaktifkan.
- Gunakan ECS tindakan Amazon untuk mengelola dan mengambil informasi tentang ECS kluster Amazon, dan mengelola setelan ECS akun Amazon. `guarddutyActivate` Tindakan yang

berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya.  
GuardDuty

Peran dikonfigurasi dengan [kebijakan AWS terkelola](#) berikut, bernama AmazonGuardDutyServiceRolePolicy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GuardDutyGetDescribeListPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource": "*"
    }
  ],
}
```

```
{
  "Sid": "GuardDutyCreateSLRPolicy",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
    }
  }
},
{
  "Sid": "GuardDutyCreateVpcEndpointPolicy",
  "Effect": "Allow",
  "Action": "ec2:CreateVpcEndpoint",
  "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": "GuardDutyManaged"
    },
    "StringLike": {
      "ec2:VpceServiceName": [
        "com.amazonaws.*.guardduty-data",
        "com.amazonaws.*.guardduty-data-fips"
      ]
    }
  }
},
{
  "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
  "Effect": "Allow",
  "Action": [
    "ec2:ModifyVpcEndpoint",
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/GuardDutyManaged": false
    }
  }
},
{
  "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
```

```

    "Effect": "Allow",
    "Action": [
      "ec2:CreateVpcEndpoint",
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:subnet/*"
    ]
  },
  {
    "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateVpcEndpoint"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutySecurityGroupManagementPolicy",
    "Effect": "Allow",
    "Action": [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup"
    ],
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "GuardDutyCreateSecurityGroupPolicy",

```

```

    "Effect": "Allow",
    "Action": "ec2:CreateSecurityGroup",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringLike": {
        "aws:RequestTag/GuardDutyManaged": "*"
      }
    }
  },
  {
    "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateSecurityGroup",
    "Resource": "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateSecurityGroup"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyCreateEksAddonPolicy",
    "Effect": "Allow",
    "Action": "eks:CreateAddon",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyManaged"
      }
    }
  },
  {
    "Sid": "GuardDutyEksAddonManagementPolicy",
    "Effect": "Allow",
    "Action": [

```



```

        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
    ],
    "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
},
{
    "Sid": "GuardDutyEksClusterTagResourcePolicy",
    "Effect": "Allow",
    "Action": "eks:TagResource",
    "Resource": "arn:aws:eks:*:*:cluster/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "GuardDutyManaged"
        }
    }
},
{
    "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
    "Effect": "Allow",
    "Action": "ecs:PutAccountSettingDefault",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "ecs:account-setting": [
                "guardDutyActivate"
            ]
        }
    }
},
{
    "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeAssociation",
        "ssm>DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
    ],
    "Resource": "arn:aws:ssm:*:*:association/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/GuardDutyManaged": "true"
        }
    }
}

```

```

    }
  }
},
{
  "Sid": "SsmAddTagsToResourcePermission",
  "Effect": "Allow",
  "Action": [
    "ssm:AddTagsToResource"
  ],
  "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
  "Condition":{
    "ForAllValues:StringEquals": {
      "aws:TagKeys": [
        "GuardDutyManaged"
      ]
    },
    "StringEquals": {
      "aws:ResourceTag/GuardDutyManaged": "true"
    }
  }
},
{
  "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
  "Effect": "Allow",
  "Action": [
    "ssm:CreateAssociation",
    "ssm:UpdateAssociation"
  ],
  "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
},
{
  "Sid": "SsmSendCommandPermission",
  "Effect": "Allow",
  "Action": "ssm:SendCommand",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
  ]
},
{
  "Sid": "SsmGetCommandStatus",
  "Effect": "Allow",

```

```

        "Action": "ssm:GetCommandInvocation",
        "Resource": "*"
    }
]
}

```

Berikut ini adalah kebijakan kepercayaan yang dilampirkan ke peran yang terhubung dengan layanan `AWSServiceRoleForAmazonGuardDuty`:

```

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

```

Untuk detail tentang pembaruan `AmazonGuardDutyServiceRolePolicy` kebijakan, lihat [GuardDuty pembaruan kebijakan AWS terkelola](#). Untuk peringatan otomatis tentang perubahan kebijakan ini, berlangganan RSS feed di [Riwayat dokumen](#) halaman.

### Membuat peran terkait layanan untuk GuardDuty


Peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan dibuat secara otomatis saat Anda mengaktifkan GuardDuty untuk pertama kalinya atau mengaktifkan GuardDuty di Wilayah yang didukung di mana Anda sebelumnya tidak mengaktifkannya. Anda juga dapat membuat peran terkait layanan secara manual menggunakan IAM konsol, file AWS CLI, atau IAM API

#### Important

Peran terkait layanan yang dibuat untuk akun administrator yang GuardDuty didelegasikan tidak berlaku untuk akun anggota. GuardDuty

Anda harus mengonfigurasi izin agar IAM prinsipal (seperti pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Agar peran

AWSServiceRoleForAmazonGuardDuty terkait layanan berhasil dibuat, IAM prinsipal yang Anda gunakan harus memiliki izin GuardDuty yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke pengguna, grup, atau peran ini:

 Note

Ganti sampel *account ID* dalam contoh berikut dengan ID AWS akun Anda yang sebenarnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
      ],
      "Resource": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
    }
  ]
}
```

```
]
}
```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat [Membuat peran terkait layanan](#) di IAMPanduan Pengguna.

### Mengedit peran terkait layanan untuk GuardDuty

GuardDuty tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) di IAMPanduan Pengguna.

### Menghapus peran terkait layanan untuk GuardDuty

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

#### Important

Jika Anda telah mengaktifkan Perlindungan Malware untuk EC2, menghapus `AWSServiceRoleForAmazonGuardDuty` tidak secara otomatis menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Jika ingin menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, lihat [Menghapus peran terkait layanan untuk Perlindungan Malware](#). EC2

Anda harus menonaktifkan GuardDuty terlebih dahulu di semua Wilayah di mana itu diaktifkan untuk menghapus `AWSServiceRoleForAmazonGuardDuty`. Jika GuardDuty layanan tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan akan gagal. Untuk informasi selengkapnya, lihat [Menangguhkan atau menonaktifkan GuardDuty](#).

Ketika Anda menonaktifkan GuardDuty, `AWSServiceRoleForAmazonGuardDuty` tidak akan dihapus secara otomatis. Jika Anda mengaktifkan GuardDuty lagi, itu akan mulai menggunakan yang sudah ada `AWSServiceRoleForAmazonGuardDuty`.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan IAM konsol, AWS CLI, atau IAM API untuk menghapus peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan di Panduan Pengguna IAM](#).

## Didukung Wilayah AWS

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDuty` terkait layanan di semua Wilayah AWS tempat yang GuardDuty tersedia. Untuk daftar Wilayah yang saat ini GuardDuty tersedia, lihat [GuardDuty titik akhir dan kuota Amazon](#) di Referensi Umum Amazon Web

## Izin peran terkait layanan untuk Perlindungan Malware untuk EC2

Perlindungan Malware untuk EC2 menggunakan peran terkait layanan (SLR) bernama `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Hal ini SLR memungkinkan Perlindungan Malware EC2 untuk melakukan pemindaian tanpa agen untuk mendeteksi malware di akun Anda. GuardDuty ini memungkinkan GuardDuty untuk membuat snapshot EBS volume di akun Anda, dan berbagi snapshot itu dengan akun GuardDuty layanan. Setelah GuardDuty mengevaluasi snapshot, itu termasuk EC2 instance yang diambil dan metadata beban kerja kontainer dalam Perlindungan Malware untuk temuan. EC2 Peran terkait layanan `AWSServiceRoleForAmazonGuardDutyMalwareProtection` memercayai layanan `malware-protection.guardduty.amazonaws.com` untuk menjalankan peran.

Kebijakan izin untuk peran ini membantu Perlindungan Malware EC2 untuk melakukan tugas-tugas berikut:

- Gunakan tindakan Amazon Elastic Compute Cloud (AmazonEC2) untuk mengambil informasi tentang EC2 instans, volume, dan snapshot Amazon Anda. Perlindungan Malware untuk EC2 juga memberikan izin untuk mengakses metadata ECS cluster Amazon EKS dan Amazon.
- Buat snapshot untuk EBS volume yang `GuardDutyExcluded` tag tidak disetel. `true` Secara default, snapshot dibuat dengan `GuardDutyScanId` tag. Jangan hapus tag ini, jika tidak, Perlindungan Malware for tidak EC2 akan memiliki akses ke snapshot.

### Important

Saat Anda menyetel `GuardDutyExcluded` ke `true`, GuardDuty layanan tidak akan dapat mengakses snapshot ini di masa mendatang. Ini karena pernyataan lain dalam peran

terkait layanan ini GuardDuty mencegah melakukan tindakan apa pun pada snapshot yang disetel ke `GuardDutyExcluded: true`

- Izinkan berbagi dan menghapus snapshot hanya jika `GuardDutyScanId` tag ada dan `GuardDutyExcluded` tag tidak disetel ke `true`

#### Note

Tidak mengizinkan Perlindungan Malware EC2 untuk membuat snapshot publik.

- Akses kunci terkelola pelanggan, kecuali yang memiliki `GuardDutyExcluded` tag yang disetel ke `true`, untuk memanggil `CreateGrant` untuk membuat dan mengakses EBS volume terenkripsi dari snapshot terenkripsi yang akan dibagikan dengan akun layanan. GuardDuty Untuk daftar akun GuardDuty layanan untuk setiap Wilayah, lihat [GuardDuty akun layanan oleh Wilayah AWS](#).
- Akses CloudWatch log pelanggan untuk membuat Perlindungan Malware untuk grup EC2 log serta menempatkan log peristiwa pemindaian malware di bawah grup `/aws/guardduty/malware-scan-events` log.
- Izinkan pelanggan untuk memutuskan apakah mereka ingin menyimpan snapshot di mana malware terdeteksi, di akun mereka. Jika pemindaian mendeteksi malware, peran terkait layanan memungkinkan GuardDuty untuk menambahkan dua tag ke snapshot - dan `GuardDutyFindingDetected` `GuardDutyExcluded`

#### Note

`GuardDutyFindingDetectedTag` menentukan bahwa snapshot berisi malware.

- Tentukan apakah volume dienkripsi dengan kunci EBS terkelola. GuardDuty melakukan `DescribeKey` tindakan untuk menentukan `KeyId` kunci EBS -managed di akun Anda.
- Ambil snapshot dari EBS volume yang dienkripsi menggunakan Kunci yang dikelola AWS, dari Anda Akun AWS dan salin ke file. [GuardDuty akun layanan](#) Untuk tujuan ini, kami menggunakan izin `GetSnapshotBlock` dan `ListSnapshotBlocks`. GuardDuty kemudian akan memindai snapshot di akun layanan. Saat ini, Perlindungan Malware untuk EC2 dukungan untuk memindai EBS volume yang dienkripsi Kunci yang dikelola AWS mungkin tidak tersedia di semua. Wilayah AWS Untuk informasi selengkapnya, lihat [Ketersediaan fitur khusus wilayah](#).
- Izinkan Amazon EC2 menelepon AWS KMS atas nama Perlindungan Malware EC2 untuk melakukan beberapa tindakan kriptografi pada kunci yang dikelola pelanggan. Tindakan seperti `kms:ReEncryptTo` dan `kms:ReEncryptFrom` diperlukan untuk berbagi snapshot yang

dienkripsi dengan kunci yang dikelola pelanggan. Hanya kunci tersebut yang dapat diakses yang GuardDutyExcluded tag tidak disetel true.

Peran dikonfigurasi dengan [kebijakan AWS terkelola](#) berikut, bernama AmazonGuardDutyMalwareProtectionServiceRolePolicy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DescribeAndListPermissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeVolumes",
      "ec2:DescribeSnapshots",
      "ecs:ListClusters",
      "ecs:ListContainerInstances",
      "ecs:ListTasks",
      "ecs:DescribeTasks",
      "eks:DescribeCluster"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CreateSnapshotVolumeConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/GuardDutyExcluded": "true"
      }
    }
  },
  {
    "Sid": "CreateSnapshotConditionalStatement",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": "GuardDutyScanId"
      }
    }
  }
}
```



```

    }
  }
},
{
  "Sid": "CreateTagsPermission",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:*:*:*/*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": "CreateSnapshot"
    }
  }
},
{
  "Sid": "AddTagsToSnapshotPermission",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GuardDutyScanId": "*"
    },
    "ForAllValues:StringEquals": {
      "aws:TagKeys": [
        "GuardDutyExcluded",
        "GuardDutyFindingDetected"
      ]
    }
  }
},
{
  "Sid": "DeleteAndShareSnapshotPermission",
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteSnapshot",
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GuardDutyScanId": "*"
    },
    "Null": {

```

```

        "aws:ResourceTag/GuardDutyExcluded": "true"
    }
}
},
{
    "Sid": "PreventPublicAccessToSnapshotPermission",
    "Effect": "Deny",
    "Action": [
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
        "StringEquals": {
            "ec2:Add/group": "all"
        }
    }
},
{
    "Sid": "CreateGrantPermission",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
        "Null": {
            "aws:ResourceTag/GuardDutyExcluded": "true"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:ebs:id": "snap-*"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
                "Decrypt",
                "CreateGrant",
                "GenerateDataKeyWithoutPlaintext",
                "ReEncryptFrom",
                "ReEncryptTo",
                "RetireGrant",
                "DescribeKey"
            ]
        },
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
}
}

```

```

    },
    {
      "Sid": "ShareSnapshotKMSPermission",
      "Effect": "Allow",
      "Action": [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        },
        "Null": {
          "aws:ResourceTag/GuardDutyExcluded": "true"
        }
      }
    },
    {
      "Sid": "DescribeKeyPermission",
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid": "GuardDutyLogGroupPermission",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid": "GuardDutyLogStreamPermission",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
  ],
}

```

```
{
  "Sid": "EBSDirectAPIPermissions",
  "Effect": "Allow",
  "Action": [
    "ebs:GetSnapshotBlock",
    "ebs:ListSnapshotBlocks"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
    "StringLike": {
      "aws:ResourceTag/GuardDutyScanId": "*"
    },
    "Null": {
      "aws:ResourceTag/GuardDutyExcluded": "true"
    }
  }
}
```


Kebijakan kepercayaan berikut dilampirkan pada peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan:

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


Membuat peran terkait layanan untuk Perlindungan Malware untuk EC2

Peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan dibuat secara otomatis saat Anda mengaktifkan Perlindungan Malware EC2 untuk pertama kalinya atau mengaktifkan Perlindungan Malware di Wilayah yang didukung EC2 di mana Anda sebelumnya tidak mengaktifkannya. Anda juga dapat membuat peran

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan secara manual menggunakan IAM konsol, file IAMCLI, atau IAM API

 Note

Secara default, jika Anda baru mengenal Amazon GuardDuty, Perlindungan Malware untuk EC2 diaktifkan secara otomatis.

 Important

Peran terkait layanan yang dibuat untuk akun GuardDuty administrator yang didelegasikan tidak berlaku untuk akun anggota GuardDuty

Anda harus mengonfigurasi izin agar IAM prinsipal (seperti pengguna, grup, atau peran) membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan berhasil dibuat, IAM identitas yang Anda gunakan harus memiliki GuardDuty izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut ke pengguna, grup, atau peran ini:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  }
],
}
```

```

    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:GetRole",
      "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
  ]
}

```

Untuk informasi selengkapnya tentang membuat peran secara manual, lihat [Membuat peran terkait layanan](#) di IAMPanduan Pengguna.

Mengedit peran terkait layanan untuk Perlindungan Malware untuk EC2

Perlindungan Malware for EC2 tidak memungkinkan Anda mengedit peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk Perlindungan Malware untuk EC2

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dikelola secara aktif.

**⚠ Important**

Untuk menghapus `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, Anda harus terlebih dahulu menonaktifkan Perlindungan Malware untuk EC2 di semua Wilayah di mana ia diaktifkan.

Jika Perlindungan Malware untuk EC2 tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan akan gagal. Untuk informasi selengkapnya, lihat [Untuk mengaktifkan atau menonaktifkan GuardDuty pemindaian malware yang dimulai](#).

Ketika Anda memilih Nonaktifkan untuk menghentikan Perlindungan Malware untuk EC2 layanan, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` tidak dihapus secara otomatis. Jika Anda kemudian memilih Aktifkan untuk memulai Perlindungan Malware untuk EC2 layanan lagi, GuardDuty akan mulai menggunakan yang ada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan IAM konsol, AWS CLI, atau IAM API untuk menghapus peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan di Panduan Pengguna IAM](#).

Didukung Wilayah AWS

Amazon GuardDuty mendukung penggunaan peran `AWSServiceRoleForAmazonGuardDutyMalwareProtection` terkait layanan di semua Wilayah AWS tempat Perlindungan Malware EC2 tersedia.

Untuk daftar Wilayah yang saat ini GuardDuty tersedia, lihat [GuardDuty titik akhir dan kuota Amazon](#) di Referensi Umum Amazon Web

**ℹ Note**

Perlindungan Malware untuk saat EC2 ini tidak tersedia di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

## AWS kebijakan terkelola untuk Amazon GuardDuty

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Butuh waktu dan keahlian untuk [membuat kebijakan terkelola IAM pelanggan](#) yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS [AWS terkelola](#), lihat [kebijakan terkelola](#) di Panduan IAM Pengguna.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk daftar dan deskripsi kebijakan fungsi pekerjaan, lihat [kebijakan AWS terkelola untuk fungsi pekerjaan](#) di Panduan IAM Pengguna.

Elemen kebijakan `Version` menetapkan aturan sintaksis bahasa yang akan digunakan untuk memproses kebijakan. Kebijakan berikut mencakup versi saat ini yang IAM mendukung. Untuk informasi selengkapnya, lihat [elemen IAM JSON kebijakan: Versi](#).

### AWS kebijakan terkelola: `AmazonGuardDutyFullAccess`

Anda dapat melampirkan `AmazonGuardDutyFullAccess` kebijakan ke IAM identitas Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan pengguna mengakses penuh ke semua GuardDuty tindakan.

#### Detail izin

Kebijakan ini mencakup izin berikut.

- `GuardDuty`— Memungkinkan pengguna akses penuh ke semua GuardDuty tindakan.



- **IAM:**
  - Memungkinkan pengguna untuk membuat peran GuardDuty terkait layanan.
  - Memungkinkan akun administrator GuardDuty untuk mengaktifkan akun anggota.
  - Memungkinkan pengguna untuk meneruskan peran GuardDuty yang menggunakan peran ini untuk mengaktifkan fitur Perlindungan GuardDuty Malware untuk S3. Ini terlepas dari bagaimana Anda mengaktifkan Perlindungan Malware untuk S3 - dalam GuardDuty layanan atau secara independen.
- **Organizations**— Memungkinkan pengguna untuk menunjuk administrator yang didelegasikan dan mengelola anggota untuk organisasi. GuardDuty

Izin untuk melakukan `iam:GetRole` tindakan

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` menetapkan apakah peran terkait layanan (SLR) untuk Perlindungan Malware untuk EC2 ada di akun.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AmazonGuardDutyFullAccessSid1",
    "Effect": "Allow",
    "Action": "guardduty:*",
    "Resource": "*"
  },
  {
    "Sid": "CreateServiceLinkedRoleSid1",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "guardduty.amazonaws.com",
          "malware-protection.guardduty.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "ActionsForOrganizationsSid1",
    "Effect": "Allow",
```

```

    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IamGetRoleSid1",
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
  },
  {
    "Sid": "AllowPassRoleToMalwareProtectionPlan",
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
      }
    }
  }
]
}

```

## AWS kebijakan terkelola: AmazonGuardDutyReadOnlyAccess

Anda dapat melampirkan AmazonGuardDutyReadOnlyAccess kebijakan ke IAM identitas Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat GuardDuty temuan dan detail organisasi Anda. GuardDuty

### Detail izin

Kebijakan ini mencakup izin berikut.

- **GuardDuty** Memungkinkan pengguna untuk melihat GuardDuty temuan dan melakukan API operasi yang dimulai dengan `GetList`, atau `Describe`
- **Organizations**— Memungkinkan pengguna untuk mengambil informasi tentang konfigurasi GuardDuty organisasi Anda, termasuk rincian akun administrator yang didelegasikan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    }
  ]
}
```

## AWS kebijakan terkelola: AmazonGuardDutyServiceRolePolicy

Anda tidak dapat melampirkan `AmazonGuardDutyServiceRolePolicy` ke IAM entitas Anda. Kebijakan AWS terkelola ini dilampirkan pada peran terkait layanan yang memungkinkan Anda

GuardDuty melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [Izin peran terkait layanan untuk GuardDuty](#).

## GuardDuty pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola GuardDuty sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS feed di halaman Riwayat GuardDuty dokumen.

| Perubahan  | Deskripsi  | Tanggal          |
|--|--|------------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> — Pembaruan ke kebijakan yang sudah ada | Menambahkan <code>ec2:DescribeVpcs</code> izin. Ini memungkinkan GuardDuty untuk melacak VPC pembaruan, seperti mengambil file. VPC CIDR | Agustus 22, 2024 |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> – Pembaruan ke kebijakan yang ada       | Menambahkan izin yang memungkinkan Anda meneruskan IAM peran GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3.             | Juni 10, 2024    |

```

{
    "Sid":
    "AllowPassRoleToMalwareProtectionPlan",
    "Effect":
    "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource":
    "arn:aws:iam::*:role/*",
    "Condition": {

```

| Perubahan  | Deskripsi  | Tanggal                 |
|--|--|-------------------------|
|  | <pre> "StringEquals": {   "iam:PassedToService": "guardduty.amazonaws.com" } } </pre>  |                         |
| <p><a href="#">AmazonGuardDutyServiceRolePolicy</a>— Perbarui ke kebijakan yang ada.</p> | <p>Gunakan AWS Systems Manager tindakan untuk mengelola SSM asosiasi di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (GuardDuty Managed :true).</p> | <p>Maret 26, 2024</p>   |
| <p><a href="#">AmazonGuardDutyServiceRolePolicy</a>— Perbarui ke kebijakan yang ada.</p> | <p>GuardDuty telah menambahkan izin baru - <code>organization:DescribeOrganization</code> untuk mengambil ID organisasi dari VPC akun Amazon bersama dan menetapkan kebijakan VPC titik akhir Amazon dengan ID organisasi.</p>   | <p>Februari 9, 2024</p> |

| Perubahan   | Deskripsi   | Tanggal           |
|---|---|-------------------|
| <a href="#">AmazonGuardDutyMalwareProtectionServiceRolePolicy</a> — Perbarui ke kebijakan yang ada. | Perlindungan Malware for EC2 telah menambahkan dua izin - GetSnapshotBlock dan ListSnapshotBlocks untuk mengambil snapshot EBS volume (dienkripsi menggunakan Kunci yang dikelola AWS) dari Anda Akun AWS dan menyalinnya ke akun GuardDuty layanan sebelum memulai pemindaian malware. | 25 Jan 2024       |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> – Pembaruan ke kebijakan yang ada                  | Menambahkan izin baru GuardDuty untuk memungkinkan menambahkan guarddutyActivate setelah ECS akun Amazon, dan melakukan daftar dan menjelaskan operasi di ECS klaster Amazon.   | November 26, 2023 |
| <a href="#">AmazonGuardDutyReadOnlyAccess</a> – Pembaruan ke kebijakan yang ada                     | GuardDuty menambahkan kebijakan baru untuk organizations untukListAccounts .  | 16 November 2023  |
| <a href="#">AmazonGuardDutyFullAccess</a> – Pembaruan ke kebijakan yang ada                         | GuardDuty menambahkan kebijakan baru untuk organizations untukListAccounts .  | 16 November 2023  |

| Perubahan  | Deskripsi  | Tanggal          |
|--|--|------------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> – Pembaruan ke kebijakan yang ada | GuardDuty menambahkan izin baru untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang.   | 8 Maret 2023     |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> – Pembaruan ke kebijakan yang ada | <p>GuardDuty telah menambahkan izin baru untuk memungkinkan membuat <a href="#">peran terkait Layanan GuardDuty untuk Perlindungan Malware untuk EC2</a>. Ini akan membantu GuardDuty merampingkan proses mengaktifkan Perlindungan Malware untuk EC2.</p> <p>GuardDuty sekarang dapat melakukan IAM tindakan berikut:</p> | 21 Februari 2023 |

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
    }
  }
}
```

| Perubahan  | Deskripsi   | Tanggal     |
|--|---|-------------|
| <a href="#">AmazonGuardDutyFullAccess</a><br>– Pembaruan ke kebijakan yang ada | GuardDuty diperbarui ARN untuk <code>iam:GetRole</code> ke <code>*AWSServiceRoleForAmazonGuardDutyMalwareProtection</code> .  | 26 Jul 2022 |
| <a href="#">AmazonGuardDutyFullAccess</a><br>– Pembaruan ke kebijakan yang ada | GuardDuty menambahkan yang baru <code>AWSServiceName</code> untuk memungkinkan pembuatan peran terkait layanan menggunakan Perlindungan GuardDuty Malware <code>iam:CreateServiceLinkedRole</code> untuk layanan. EC2<br><br>GuardDuty sekarang dapat melakukan <code>iam:GetRole</code> tindakan untuk mendapatkan informasi untuk <code>AWSServiceRole</code> . | 26 Jul 2022 |



| Perubahan  | Deskripsi  | Tanggal         |
|--|--|-----------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> – Pembaruan ke kebijakan yang ada | <p>GuardDuty menambahkan izin baru GuardDuty untuk memungkinkan penggunaan tindakan EC2 jaringan Amazon untuk meningkatkan temuan.</p> <p>GuardDuty sekarang dapat melakukan EC2 tindakan berikut untuk mendapatkan informasi tentang bagaimana EC2 instans Anda berkomunikasi. Informasi ini digunakan untuk meningkatkan akurasi penemuan.</p> <ul style="list-style-type: none"> <li>• <code>ec2:DescribeVpcEndpoints</code></li> <li>• <code>ec2:DescribeSubnets</code></li> <li>• <code>ec2:DescribeVpcPeeringConnections</code></li> <li>• <code>ec2:DescribeTransitGatewayAttachments</code></li> </ul> | Agustus 3, 2021 |
| GuardDuty mulai melacak perubahan  | GuardDuty mulai melacak perubahan untuk kebijakan yang AWS dikelola.   | Agustus 3, 2021 |

## Memecahkan masalah GuardDuty identitas dan akses Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan GuardDuty dan IAM.

### Topik

- [Saya tidak berwenang untuk melakukan tindakan di GuardDuty](#)
- [Saya tidak berwenang untuk melakukan iam:PassRole.](#)
- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses GuardDuty sumber daya saya.](#)

## Saya tidak berwenang untuk melakukan tindakan di GuardDuty

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 guardduty: *GetWidget* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty: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 guardduty: *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 yang tidak diizinkan untuk melakukan iam:PassRole tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran GuardDuty.

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 GuardDuty. 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 GuardDuty sumber daya 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 GuardDuty mendukung fitur-fitur ini, lihat [Bagaimana Amazon GuardDuty 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


## Validasi kepatuhan untuk Amazon GuardDuty

Untuk mempelajari apakah an AWS layanan berada dalam lingkup program kepatuhan tertentu, lihat [AWS layanan di Lingkup oleh Program Kepatuhan AWS layanan](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#) .

Tanggung jawab kepatuhan Anda saat menggunakan AWS layanan ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- [Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services](#) — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

 Note

Tidak semua AWS layanan HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat [Referensi Layanan yang HIPAA Memenuhi Syarat](#).

- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Panduan Kepatuhan Pelanggan](#) - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan AWS layanan dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini AWS layanan memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).
- [Amazon GuardDuty](#) — Ini AWS layanan mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.

- [AWS Audit Manager](#) Ini AWS layanan membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

## Ketahanan di Amazon GuardDuty

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Availability Zone lebih tersedia, memiliki toleransi kesalahan, dan dapat diskalakan dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur global AWS](#).

## Keamanan infrastruktur di Amazon GuardDuty

Sebagai layanan terkelola, Amazon GuardDuty 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 GuardDuty 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.

# Mengintegrasikan AWS layanan dengan GuardDuty

GuardDuty dapat diintegrasikan dengan layanan AWS keamanan lainnya. Layanan ini dapat menyerap data dari GuardDuty untuk memungkinkan Anda melihat temuan dengan cara baru. Tinjau opsi integrasi berikut untuk mempelajari lebih lanjut tentang cara layanan tersebut disiapkan untuk bekerja dengannya GuardDuty.

## Integrasi dengan GuardDuty AWS Security Hub

AWS Security Hub mengumpulkan data keamanan dari seluruh AWS akun, layanan, dan produk mitra pihak ketiga yang didukung untuk menilai keadaan keamanan lingkungan Anda sesuai dengan standar industri dan praktik terbaik. Selain mengevaluasi postur keamanan Anda, Security Hub menciptakan lokasi terpusat untuk temuan di semua AWS layanan terintegrasi Anda, dan produk AWS Mitra. Mengaktifkan Security Hub dengan GuardDuty akan secara otomatis memungkinkan data GuardDuty temuan dicerna oleh Security Hub.

Untuk informasi selengkapnya tentang menggunakan Security Hub dengan GuardDuty lihat [Integrasi dengan AWS Security Hub](#).

## Integrasi GuardDuty dengan Amazon Detective

Amazon Detective menggunakan data log dari seluruh AWS akun Anda untuk membuat visualisasi data untuk sumber daya dan alamat IP yang berinteraksi dengan lingkungan Anda. Visualisasi Detective membantu Anda menyelidiki masalah keamanan dengan cepat dan mudah. Anda dapat beralih dari GuardDuty menemukan detail ke informasi di konsol Detektif setelah kedua layanan diaktifkan.

Untuk informasi lebih lanjut tentang menggunakan Detektif dengan GuardDuty lihat. [Integrasi dengan Amazon Detective](#)

## Integrasi dengan AWS Security Hub

[AWS Security Hub](#) memberi Anda gambaran menyeluruh tentang status keamanan Anda dalam AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub mengumpulkan data keamanan dari berbagai AWS akun, layanan, dan produk mitra pihak ketiga yang didukung serta membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

GuardDuty Integrasi Amazon dengan Security Hub memungkinkan Anda mengirim temuan dari Security Hub GuardDuty ke Security Hub. Security Hub kemudian dapat menyertakan temuan tersebut dalam analisis postur keamanan Anda.

## Daftar Isi

- [Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub](#)
  - [Jenis temuan yang GuardDuty dikirim ke Security Hub](#)
    - [Latensi untuk mengirimkan temuan baru](#)
    - [Mencoba kembali saat Security Hub tidak tersedia](#)
    - [Memperbarui temuan yang ada di Security Hub](#)
  - [Melihat GuardDuty temuan di AWS Security Hub](#)
    - [Menafsirkan GuardDuty menemukan nama di AWS Security Hub](#)
    - [Temuan standar dari GuardDuty](#)
  - [Mengaktifkan dan mengonfigurasi integrasi](#)
  - [Menggunakan GuardDuty kontrol di Security Hub](#)
  - [Menghentikan publikasi temuan ke Security Hub](#)

## Bagaimana Amazon GuardDuty mengirimkan temuan ke AWS Security Hub

Pada tahun AWS Security Hub, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub menyediakan alat untuk mengelola temuan dari seluruh sumber tersebut. Anda dapat melihat dan mem-filter daftar temuan dan melihat detail suatu temuan. Untuk informasi lebih lanjut, lihat [Melihat temuan](#) dalam Panduan Pengguna AWS Security Hub . Anda juga dapat melacak status penyelidikan temuan. Untuk informasi lebih lanjut, lihat [Mengambil tindakan pada temuan](#) dalam Panduan Pengguna AWS Security Hub .

Semua temuan di Security Hub menggunakan JSON format standar yang disebut AWS Security Finding Format (ASFF). ASFF termasuk rincian tentang sumber masalah, sumber daya yang terpengaruh, dan status temuan saat ini. Lihat [AWS Security Finding Format \(ASFF\)](#) di Panduan AWS Security Hub Pengguna.

Amazon GuardDuty adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub.



## Jenis temuan yang GuardDuty dikirim ke Security Hub

Setelah Anda mengaktifkan GuardDuty dan Security Hub di akun yang sama dalam akun yang sama Wilayah AWS, GuardDuty mulailah mengirimkan semua temuan yang dihasilkan ke Security Hub. Temuan ini dikirim ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#). DiASFF, Types bidang menyediakan jenis temuan.

### Latensi untuk mengirimkan temuan baru

Saat GuardDuty membuat temuan baru, biasanya dikirim ke Security Hub dalam waktu lima menit.

### Mencoba kembali saat Security Hub tidak tersedia

Jika Security Hub tidak GuardDuty tersedia, coba lagi mengirimkan temuan sampai diterima.

### Memperbarui temuan yang ada di Security Hub

Setelah mengirimkan temuan ke Security Hub, GuardDuty mengirimkan pembaruan untuk mencerminkan pengamatan tambahan dari aktivitas temuan ke Security Hub. Pengamatan baru dari temuan ini dikirim ke Security Hub berdasarkan [Langkah 5 - Frekuensi untuk mengeksport temuan](#) pengaturan di Anda Akun AWS.


Saat Anda mengarsipkan atau membatalkan arsip temuan, GuardDuty tidak akan mengirim temuan itu ke Security Hub. Temuan yang tidak diarsipkan secara manual yang nantinya menjadi aktif tidak GuardDuty dikirim ke Security Hub.

## Melihat GuardDuty temuan di AWS Security Hub

Untuk melihat GuardDuty temuan Anda di Security Hub, pilih Lihat Temuan di bawah Amazon GuardDuty dari halaman ringkasan. Atau, Anda dapat memilih Temuan dari panel navigasi dan memfilter temuan untuk hanya menampilkan GuardDuty temuan dengan memilih bidang Nama produk: dengan nilaiGuardDuty.

## Menafsirkan GuardDuty menemukan nama di AWS Security Hub

GuardDuty mengirimkan temuan ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#). DiASFF, Types bidang menyediakan jenis temuan. ASFFtipe menggunakan skema penamaan yang berbeda dari GuardDuty tipe. Tabel di bawah ini merinci semua jenis GuardDuty temuan dengan ASFF rekan mereka saat muncul di Security Hub.

 Note

Untuk beberapa jenis GuardDuty temuan Security Hub menetapkan nama ASFF temuan yang berbeda tergantung pada apakah Peran Sumber Daya detail temuan itu ACTOR atau TARGET. Untuk informasi selengkapnya, lihat [Detail temuan](#).

| GuardDuty menemukan jenis                                    | ASFF menemukan jenis  |
|--|---|
| <a href="#">Backdoor:EC2/C&amp;CActivity.B</a>               | TTPs/Command and Control/Backdoor:EC2-C&CActivity.B                   |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B!DNS</a>           | TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS               |
| <a href="#">Backdoor:EC2/DenialOfService.Dns</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns             |
| <a href="#">Backdoor:EC2/DenialOfService.Tcp</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp             |
| <a href="#">Backdoor:EC2/DenialOfService.Udp</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp             |
| <a href="#">Backdoor:EC2/DenialOfService.UdpOnTcpPorts</a>   | TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts   |
| <a href="#">Backdoor:EC2/DenialOfService.UnusualProtocol</a> | TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol |
| <a href="#">Backdoor:EC2/Spambot</a>                         | TTPs/Command and Control/Backdoor:EC2-Spambot                         |
| <a href="#">Behavior:EC2/NetworkPortUnusual</a>              | Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual                  |
| <a href="#">Behavior:EC2/TrafficVolumeUnusual</a>            | Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual                |

| GuardDuty menemukan jenis   | ASFFmenemukan jenis   |
|---|---|
| <a href="#">Backdoor:Lambda/C&amp;CActivity.B</a>                             | TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B                      |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B</a>                            | TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B                     |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B!DNS</a>                        | TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS                 |
| <a href="#">CredentialAccess:IAMUser/AnomalousBehavior</a>                    | TTPs/Credential Access/IAMUser-AnomalousBehavior                            |
| <a href="#">CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed</a> | TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed          |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller</a>                 | TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller         |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller.Custom</a>          | TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom  |
| <a href="#">CredentialAccess:Kubernetes/SuccessfulAnonymousAccess</a>         | TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess |
| <a href="#">CredentialAccess:Kubernetes/TorIPCaller</a>                       | TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller               |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.FailedLogin</a>            | TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin   |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce</a>   | TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce           |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin</a>        | TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin                |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.FailedLogin</a>            | TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin                    |

| GuardDuty menemukan jenis  | ASFFmenemukan jenis  |
|--|--|
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin</a> | TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin   |
| <a href="#">CredentialAccess:RDS/TorIPCaller.FailedLogin</a>           | TTPs/Credential Access/RDS-TorIPCaller.FailedLogin   |
| <a href="#">CredentialAccess:RDS/TorIPCaller.SuccessfulLogin</a>       | TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin   |
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B</a>                       | TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B  |
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B!DNS</a>                   | TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS  |
| <a href="#">CryptoCurrency:Lambda/BitcoinTool.B</a>                    | TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B<br><br>Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B</a>                   | TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B  |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B!DNS</a>               | TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS  |
| <a href="#">DefenseEvasion:EC2/UnusualDNSResolver</a>                  | TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver   |
| <a href="#">DefenseEvasion:EC2/UnusualDoHActivity</a>                  | TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity   |
| <a href="#">DefenseEvasion:EC2/UnusualDoTActivity</a>                  | TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity   |
| <a href="#">DefenseEvasion:IAMUser/AnomalousBehavior</a>               | TTPs/Defense Evasion/IAMUser-AnomalousBehavior   |

| GuardDuty menemukan jenis  | ASFFmenemukan jenis   |
|--|---|
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCaller</a>                | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller                 |
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom</a>         | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom          |
| <a href="#">DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess</a>        | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess         |
| <a href="#">DefenseEvasion:Kubernetes/TorIPCaller</a>                      | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller                       |
| <a href="#">DefenseEvasion:Runtime/FilelessExecution</a>                   | TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution                   |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Proc</a>               | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc               |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Ptrace</a>             | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace             |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite</a> | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite |
| <a href="#">DefenseEvasion:Runtime/PtraceAntiDebugging</a>                 | TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging                  |
| <a href="#">DefenseEvasion:Runtime/SuspiciousCommand</a>                   | TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand                    |
| <a href="#">Penemuan:IAMUser/AnomalousBehavior</a>                         | TTPs/Discovery/IAMUser-AnomalousBehavior  |
| <a href="#">Discovery:Kubernetes/AnomalousBehavior.PermissionChecked</a>   | TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked                   |
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller</a>                     | TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller                           |

| GuardDuty menemukan jenis   | ASFFmenemukan jenis   |
|---|---|
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller.Custom</a>           | TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom  |
| <a href="#">Discovery:Kubernetes/SuccessfulAnonymousAccess</a>          | TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess |
| <a href="#">Discovery:Kubernetes/TorIPCaller</a>                        | TTPs/Discovery/Discovery:Kubernetes-TorIPCaller               |
| <a href="#">Discovery:RDS/MaliciousIPCaller</a>                         | TTPs/Discovery/RDS-MaliciousIPCaller                          |
| <a href="#">Discovery:RDS/TorIPCaller</a>                               | TTPs/Discovery/RDS-TorIPCaller                                |
| <a href="#">Discovery:S3/AnomalousBehavior</a>                          | TTPs/Discovery:S3-AnomalousBehavior                           |
| <a href="#">Discovery:S3/BucketEnumeration.Unusual</a>                  | TTPs/Discovery:S3-BucketEnumeration.Unusual                   |
| <a href="#">Discovery:S3/MaliciousIPCaller.Custom</a>                   | TTPs/Discovery:S3-MaliciousIPCaller.Custom                    |
| <a href="#">Discovery:S3/TorIPCaller</a>                                | TTPs/Discovery:S3-TorIPCaller                                 |
| <a href="#">Discovery:S3/MaliciousIPCaller</a>                          | TTPs/Discovery:S3-MaliciousIPCaller                           |
| <a href="#">Exfiltration:IAMUser/AnomalousBehavior</a>                  | TTPs/Exfiltration/IAMUser-AnomalousBehavior                   |
| <a href="#">Execution:Kubernetes/ExecInKubeSystemPod</a>                | TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod       |
| <a href="#">Execution:Kubernetes/AnomalousBehavior.ExecInPod</a>        | TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod         |
| <a href="#">Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed</a> | TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed  |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller</a>                     | TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller               |

| GuardDuty menemukan jenis   | ASFF menemukan jenis   |
|---|--|
| <a href="#">Impact:Kubernetes/MaliciousIPCaller.Custom</a>  | TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom                                     |
| <a href="#">Impact:Kubernetes/SuccessfulAnonymousAccess</a>   | TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess                                    |
| <a href="#">Impact:Kubernetes/TorIPCaller</a>   | TTPs/Impact/Impact:Kubernetes-TorIPCaller  |
| <a href="#">Persistence:Kubernetes/ContainerWithSensitiveMount</a>                                    | TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount                        |
| <a href="#">Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount</a> | TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer</a> | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller</a>  | TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller                                  |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller.Custom</a>                                       | TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom                           |
| <a href="#">Persistence:Kubernetes/SuccessfulAnonymousAccess</a>                                      | TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess                          |
| <a href="#">Persistence:Kubernetes/TorIPCaller</a>  | TTPs/Persistence/Persistence:Kubernetes-TorIPCaller  |
| <a href="#">Execution:EC2/MaliciousFile</a>   | TTPs/Execution/Execution:EC2-MaliciousFile   |
| <a href="#">Execution:ECS/MaliciousFile</a>   | TTPs/Execution/Execution:ECS-MaliciousFile   |
| <a href="#">Execution:Kubernetes/MaliciousFile</a>  | TTPs/Execution/Execution:Kubernetes-MaliciousFile  |

| GuardDuty menemukan jenis                                | ASFF menemukan jenis                                    |
|--|---|
| <a href="#">Execution:Container/MaliciousFile</a>        | TTPs/Execution/Execution:Container-MaliciousFile        |
| <a href="#">Execution:EC2/SuspiciousFile</a>             | TTPs/Execution/Execution:EC2-SuspiciousFile             |
| <a href="#">Execution:ECS/SuspiciousFile</a>             | TTPs/Execution/Execution:ECS-SuspiciousFile             |
| <a href="#">Execution:Kubernetes/SuspiciousFile</a>      | TTPs/Execution/Execution:Kubernetes-SuspiciousFile      |
| <a href="#">Execution:Container/SuspiciousFile</a>       | TTPs/Execution/Execution:Container-SuspiciousFile       |
| <a href="#">Execution:Runtime/MaliciousFileExecuted</a>  | TTPs/Execution/Execution:Runtime-MaliciousFileExecuted  |
| <a href="#">Execution:Runtime/NewBinaryExecuted</a>      | TTPs/Execution/Execution:Runtime-NewBinaryExecuted      |
| <a href="#">Execution:Runtime/NewLibraryLoaded</a>       | TTPs/Execution/Execution:Runtime-NewLibraryLoaded       |
| <a href="#">Execution:Runtime/ReverseShell</a>           | TTPs/Execution/Execution:Runtime-ReverseShell           |
| <a href="#">Execution:Runtime/SuspiciousCommand</a>      | TTPs/Execution/Execution:Runtime-SuspiciousCommand      |
| <a href="#">Execution:Runtime/SuspiciousShellCreated</a> | TTPs/Execution/Execution:Runtime-SuspiciousShellCreated |
| <a href="#">Execution:Runtime/SuspiciousTool</a>         | TTPs/Execution/Execution:Runtime-SuspiciousTool         |
| <a href="#">Exfiltration:S3/AnomalousBehavior</a>        | TTPs/Exfiltration:S3-AnomalousBehavior                  |
| <a href="#">Exfiltration:S3/ObjectRead.Unusual</a>       | TTPs/Exfiltration:S3-ObjectRead.Unusual                 |



| GuardDuty menemukan jenis   | ASFFmenemukan jenis   |
|---|---|
| <a href="#">Exfiltration:S3/MaliciousIPCaller</a>                 | TTPs/Exfiltration:S3-MaliciousIPCaller                        |
| <a href="#">Impact:EC2/AbusedDomainRequest.Reputation</a>         | TTPs/Impact:EC2-AbusedDomainRequest.Reputation                |
| <a href="#">Impact:EC2/BitcoinDomainRequest.Reputation</a>        | TTPs/Impact:EC2-BitcoinDomainRequest.Reputation               |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Reputation</a>      | TTPs/Impact:EC2-MaliciousDomainRequest.Reputation             |
| <a href="#">Impact:EC2/PortSweep</a>                              | TTPs/Impact/Impact:EC2-PortSweep                              |
| <a href="#">Impact:EC2/SuspiciousDomainRequest.Reputation</a>     | TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation            |
| <a href="#">Impact:EC2/WinRMBruteForce</a>                        | TTPs/Impact/Impact:EC2-WinRMBruteForce                        |
| <a href="#">Dampak:IAMUser/AnomalousBehavior</a>                  | TTPs/Impact/IAMUser-AnomalousBehavior                         |
| <a href="#">Impact:Runtime/AbusedDomainRequest.Reputation</a>     | TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation     |
| <a href="#">Impact:Runtime/BitcoinDomainRequest.Reputation</a>    | TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation    |
| <a href="#">Impact:Runtime/CryptoMinerExecuted</a>                | TTPs/Impact/Impact:Runtime-CryptoMinerExecuted                |
| <a href="#">Impact:Runtime/MaliciousDomainRequest.Reputation</a>  | TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation  |
| <a href="#">Impact:Runtime/SuspiciousDomainRequest.Reputation</a> | TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputation |
| <a href="#">Impact:S3/AnomalousBehavior.Delete</a>                | TTPs/Impact:S3-AnomalousBehavior.Delete                       |

| GuardDuty menemukan jenis                                 | ASFFmenemukan jenis                                      |
|---|--|
| <a href="#">Impact:S3/AnomalousBehavior.Permission</a>    | TTPs/Impact:S3-AnomalousBehavior.Permission              |
| <a href="#">Impact:S3/AnomalousBehavior.Write</a>         | TTPs/Impact:S3-AnomalousBehavior.Write                   |
| <a href="#">Impact:S3/ObjectDelete.Unusual</a>            | TTPs/Impact:S3-ObjectDelete.Unusual                      |
| <a href="#">Impact:S3/PermissionsModification.Unusual</a> | TTPs/Impact:S3-PermissionsModification.Unusual           |
| <a href="#">Impact:S3/MaliciousIPCaller</a>               | TTPs/Impact:S3-MaliciousIPCaller                         |
| <a href="#">InitialAccess:IAMUser/AnomalousBehavior</a>   | TTPs/Initial Access/IAMUser-AnomalousBehavior            |
| <a href="#">Object:S3/MaliciousFile</a>                   | TTPs/Object/Object:S3-MaliciousFile                      |
| <a href="#">PenTest:IAMUser/KaliLinux</a>                 | TTPs/PenTest:IAMUser/KaliLinux                           |
| <a href="#">PenTest:IAMUser/ParrotLinux</a>               | TTPs/PenTest:IAMUser/ParrotLinux                         |
| <a href="#">PenTest:IAMUser/PentooLinux</a>               | TTPs/PenTest:IAMUser/PentooLinux                         |
| <a href="#">PenTest:S3/KaliLinux</a>                      | TTPs/PenTest:S3-KaliLinux                                |
| <a href="#">PenTest:S3/ParrotLinux</a>                    | TTPs/PenTest:S3-ParrotLinux                              |
| <a href="#">PenTest:S3/PentooLinux</a>                    | TTPs/PenTest:S3-PentooLinux                              |
| <a href="#">Kegigihan:/IAMUserAnomalousBehavior</a>       | TTPs/Persistence/IAMUser-AnomalousBehavior               |
| <a href="#">Persistence:IAMUser/NetworkPermissions</a>    | TTPs/Persistence/Persistence:IAMUser-NetworkPermissions  |
| <a href="#">Persistence:IAMUser/ResourcePermissions</a>   | TTPs/Persistence/Persistence:IAMUser-ResourcePermissions |

| GuardDuty menemukan jenis   | ASFFmenemukan jenis  |
|---|--|
| <a href="#">Persistence:IAMUser/UserPermissions</a>                   | TTPs/Persistence/Persistence:IAMUser-UserPermissions   |
| <a href="#">Policy:IAMUser/RootCredentialUsage</a>                    | TTPs/Policy:IAMUser-RootCredentialUsage  |
| <a href="#">Policy:Kubernetes/AdminAccessToDefaultServiceAccount</a>  | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount |
| <a href="#">Policy:Kubernetes/AnonymousAccessGranted</a>              | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted             |
| <a href="#">Policy:Kubernetes/ExposedDashboard</a>                    | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard                   |
| <a href="#">Policy:Kubernetes/KubeflowDashboardExposed</a>            | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed           |
| <a href="#">Policy:S3/AccountBlockPublicAccessDisabled</a>            | TTPs/Policy:S3-AccountBlockPublicAccessDisabled  |
| <a href="#">Policy:S3/BucketAnonymousAccessGranted</a>                | TTPs/Policy:S3-BucketAnonymousAccessGranted  |
| <a href="#">Policy:S3/BucketBlockPublicAccessDisabled</a>             | Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled  |
| <a href="#">Policy:S3/BucketPublicAccessGranted</a>                   | TTPs/Policy:S3-BucketPublicAccessGranted   |
| <a href="#">PrivilegeEscalation:IAMUser/AnomalousBehavior</a>         | TTPs/Privilege Escalation/IAMUser-AnomalousBehavior  |
| <a href="#">PrivilegeEscalation:IAMUser/AdministrativePermissions</a> | TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions                                    |

| GuardDuty menemukan jenis   | ASFF menemukan jenis   |
|---|--|
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated</a> | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated           |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated</a>        | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated                  |
| <a href="#">PrivilegeEscalation:Kubernetes/PrivilegedContainer</a>                  | TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer        |
| <a href="#">PrivilegeEscalation:Runtime/ContainerMountsHostDirectory</a>            | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory |
| <a href="#">PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified</a>             | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified  |
| <a href="#">PrivilegeEscalation:Runtime/DockerSocketAccessed</a>                    | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed         |
| <a href="#">PrivilegeEscalation:Runtime/ElevationToRoot</a>                         | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot              |
| <a href="#">PrivilegeEscalation:Runtime/RuncContainerEscape</a>                     | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape          |
| <a href="#">PrivilegeEscalation:Runtime/UserfaultfdUsage</a>                        | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage             |
| <a href="#">Recon:EC2/PortProbeEMRUnprotectedPort</a>                               | TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort                               |
| <a href="#">Recon:EC2/PortProbeUnprotectedPort</a>                                  | TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort                                  |
| <a href="#">Recon:EC2/Portscan</a>  | TTPs/Discovery/Recon:EC2-Portscan  |
| <a href="#">Recon:IAMUser/MaliciousIPCaller</a>                                     | TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller                                     |

| GuardDuty menemukan jenis                                    | ASFF menemukan jenis  |
|--|---|
| <a href="#">Recon:IAMUser/MaliciousIPCaller.Custom</a>       | TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom               |
| <a href="#">Recon:IAMUser/NetworkPermissions</a>             | TTPs/Discovery/Recon:IAMUser-NetworkPermissions                     |
| <a href="#">Recon:IAMUser/ResourcePermissions</a>            | TTPs/Discovery/Recon:IAMUser-ResourcePermissions                    |
| <a href="#">Recon:IAMUser/TorIPCaller</a>                    | TTPs/Discovery/Recon:IAMUser-TorIPCaller                            |
| <a href="#">Recon:IAMUser/UserPermissions</a>                | TTPs/Discovery/Recon:IAMUser-UserPermissions                        |
| <a href="#">ResourceConsumption:IAMUser/ComputeResources</a> | Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources |
| <a href="#">Stealth:IAMUser/CloudTrailLoggingDisabled</a>    | TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled      |
| <a href="#">Stealth:IAMUser/LoggingConfigurationModified</a> | TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified   |
| <a href="#">Stealth:IAMUser/PasswordPolicyChange</a>         | TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange           |
| <a href="#">Stealth:S3/ServerAccessLoggingDisabled</a>       | TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled         |
| <a href="#">Trojan:EC2/BlackholeTraffic</a>                  | TTPs/Command and Control/Trojan:EC2-BlackholeTraffic                |
| <a href="#">Trojan:EC2/BlackholeTraffic!DNS</a>              | TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS            |
| <a href="#">Trojan:EC2/DGADomainRequest.B</a>                | TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B              |

| GuardDuty menemukan jenis                               | ASFFmenemukan jenis  |
|---|--|
| <a href="#">Trojan:EC2/DGADomainRequest.C!DNS</a>       | TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS     |
| <a href="#">Trojan:EC2/DNSDataExfiltration</a>          | TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration        |
| <a href="#">Trojan:EC2/DriveBySourceTraffic!DNS</a>     | TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS        |
| <a href="#">Trojan:EC2/DropPoint</a>                    | Effects/Data Exfiltration/Trojan:EC2-DropPoint                 |
| <a href="#">Trojan:EC2/DropPoint!DNS</a>                | Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS             |
| <a href="#">Trojan:EC2/PhishingDomainRequest!DNS</a>    | TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS  |
| <a href="#">Trojan:Lambda/BlackholeTraffic</a>          | TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic        |
| <a href="#">Trojan:Lambda/DropPoint</a>                 | Effects/Data Exfiltration/Trojan:Lambda-DropPoint              |
| <a href="#">Trojan:Runtime/BlackholeTraffic</a>         | TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic       |
| <a href="#">Trojan:Runtime/BlackholeTraffic!DNS</a>     | TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS   |
| <a href="#">Trojan:Runtime/DGADomainRequest.C!DNS</a>   | TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS |
| <a href="#">Trojan:Runtime/DriveBySourceTraffic!DNS</a> | TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS    |
| <a href="#">Trojan:Runtime/DropPoint</a>                | Effects/Data Exfiltration/Trojan:Runtime-DropPoint             |

| GuardDuty menemukan jenis  | ASFFmenemukan jenis  |
|--|--|
| <a href="#">Trojan:Runtime/DropPoint!DNS</a>   | Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS   |
| <a href="#">Trojan:Runtime/PhishingDomainRequest!DNS</a>                             | TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS                              |
| <a href="#">UnauthorizedAccess:EC2/MaliciousIPCaller.Custom</a>                      | TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom                       |
| <a href="#">UnauthorizedAccess:EC2/MetadataDNSRebind</a>                             | TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind  |
| <a href="#">UnauthorizedAccess:EC2/RDPBruteForce</a>                                 | TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce                                       |
| <a href="#">UnauthorizedAccess:EC2/SSHBruteForce</a>                                 | TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce                                       |
| <a href="#">UnauthorizedAccess:EC2/TorClient</a>                                     | Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient                                  |
| <a href="#">UnauthorizedAccess:EC2/TorRelay</a>                                      | Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay                                   |
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLogin</a>                              | Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin                                |
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B</a>                     | TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B  |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</a> | Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</a> | Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS |

| GuardDuty menemukan jenis   | ASFFmenemukan jenis   |
|---|---|
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller</a>        | TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller                           |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom</a> | TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom                    |
| <a href="#">UnauthorizedAccess:IAMUser/TorIPCaller</a>              | TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller             |
| <a href="#">UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom</a>  | TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom |
| <a href="#">UnauthorizedAccess:Lambda/TorClient</a>                 | Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient            |
| <a href="#">UnauthorizedAccess:Lambda/TorRelay</a>                  | Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay             |
| <a href="#">UnauthorizedAccess:Runtime/MetadataDNSRebind</a>        | TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind                           |
| <a href="#">UnauthorizedAccess:Runtime/TorRelay</a>                 | Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay            |
| <a href="#">UnauthorizedAccess:Runtime/TorClient</a>                | Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient           |
| <a href="#">UnauthorizedAccess:S3/MaliciousIPCaller.Custom</a>      | TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom                         |
| <a href="#">UnauthorizedAccess:S3/TorIPCaller</a>                   | TTPs/UnauthorizedAccess:S3-TorIPCaller                                      |

## Temuan standar dari GuardDuty

GuardDuty mengirimkan temuan ke Security Hub menggunakan [AWS Security Finding Format \(ASFF\)](#).

Berikut adalah contoh temuan khas dari GuardDuty.



```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
"Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
"199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
"46717",

```

```
"aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
  "aws/guardduty/service/serviceName": "guardduty",
  "aws/guardduty/service/evidence": "",
  "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
  "172.31.43.6",
  "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
  "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
  "INBOUND",
  "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
  "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
  "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
  "SSH",
  "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
  "aws/guardduty/service/additionalInfo": "",
  "aws/guardduty/service/resourceRole": "TARGET",
  "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
  "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
  "aws/guardduty/service/count": "74",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
  "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "aws/securityhub/ProductName": "GuardDuty",
  "aws/securityhub/CompanyName": "Amazon"
},
"Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
    "Partition": "aws",
    "Region": "us-east-1",
    "Tags": {
      "Name": "kubect1"
    },
    "Details": {
      "AwsEc2Instance": {
```

```
    "Type": "t2.micro",
    "ImageId": "ami-02354e95b39ca8dec",
    "IPv4Addresses": [
      "18.234.130.16",
      "172.31.43.6"
    ],
    "VpcId": "vpc-a0c2d7c7",
    "SubnetId": "subnet-4975b475",
    "LaunchedAt": "2020-08-03T23:21:57Z"
  }
}
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE"
}
```

## Mengaktifkan dan mengonfigurasi integrasi

Untuk menggunakan integrasi dengan AWS Security Hub, Anda harus mengaktifkan Security Hub. Untuk informasi tentang cara mengaktifkan Security Hub, lihat [Menyiapkan Security Hub](#) di Panduan Pengguna AWS Security Hub .

Saat Anda mengaktifkan keduanya GuardDuty dan Security Hub, integrasi diaktifkan secara otomatis. GuardDuty segera mulai mengirim temuan ke Security Hub.

## Menggunakan GuardDuty kontrol di Security Hub

AWS Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Anda dapat menggunakan kontrol yang terkait dengan GuardDuty sumber daya dan rencana perlindungan yang dipilih. Untuk informasi selengkapnya, lihat [GuardDuty kontrol Amazon](#) di Panduan AWS Security Hub Pengguna.

Untuk daftar semua kontrol di seluruh AWS layanan dan sumber daya, lihat [referensi kontrol Security Hub](#) di Panduan AWS Security Hub Pengguna.

## Menghentikan publikasi temuan ke Security Hub

Untuk menghentikan pengiriman temuan ke Security Hub, Anda dapat menggunakan konsol Security Hub atau konsolAPI.

Lihat [Menonaktifkan dan mengaktifkan aliran temuan dari integrasi \(konsol\)](#) atau [Menonaktifkan aliran temuan dari integrasi \(Security HubAPI, AWS CLI\)](#) di Panduan Pengguna.AWS Security Hub

## Integrasi dengan Amazon Detective

[Amazon Detective](#) membantu Anda menganalisis dan menyelidiki peristiwa keamanan dengan cepat di satu atau beberapa AWS akun dengan menghasilkan visualisasi data yang mewakili cara sumber daya Anda berperilaku dan berinteraksi dari waktu ke waktu. Detective menciptakan visualisasi temuan. GuardDuty

Detective menyerap rincian pencarian untuk semua jenis temuan, dan menyediakan akses ke profil entitas untuk menyelidiki entitas berbeda yang terlibat dengan temuan tersebut. Entitas dapat berupa Akun AWS, AWS sumber daya dalam akun, atau Alamat IP eksternal yang telah berinteraksi dengan sumber daya Anda. GuardDuty Konsol mendukung pivoting ke Amazon Detective dari entitas berikut, tergantung pada jenis pencarian:., peran, pengguna Akun AWS, atau sesi IAM peran, agen pengguna, pengguna federasi, instans EC2 Amazon, atau alamat IP.

### Daftar Isi

- [Mengaktifkan integrasi](#)
- [Berputar ke Detektif Amazon dari sebuah temuan GuardDuty](#)
- [Menggunakan integrasi dengan lingkungan GuardDuty multi-akun](#)

## Mengaktifkan integrasi

Untuk menggunakan Amazon Detective dengan GuardDuty Anda harus terlebih dahulu mengaktifkan Amazon Detective. Untuk informasi tentang cara mengaktifkan Detective, lihat [Mengatur Amazon Detective](#) di Panduan Administrasi Amazon Detective.

Saat Anda mengaktifkan keduanya GuardDuty dan Detektif, integrasi diaktifkan secara otomatis. Setelah diaktifkan, Detective akan segera menelan data temuan Anda GuardDuty .

**Note**

GuardDuty mengirimkan temuan ke Detective berdasarkan frekuensi ekspor GuardDuty temuan. Secara default, frekuensi ekspor untuk pembaruan temuan yang ada adalah 6 jam. Untuk memastikan Detektif menerima pembaruan terbaru untuk temuan Anda, disarankan agar Anda mengubah frekuensi ekspor menjadi 15 menit di setiap wilayah tempat Anda menggunakan Detektif. GuardDuty Untuk informasi selengkapnya, lihat [Langkah 5 - Mengatur frekuensi untuk mengekspor temuan aktif yang diperbarui](#).

## Berputar ke Detektif Amazon dari sebuah temuan GuardDuty

1. Masuk ke <https://console.aws.amazon.com/guardduty/konsol>.
2. Pilih satu temuan dari tabel temuan Anda.
3. Pilih Selidiki dengan Detektif dari panel rincian temuan.
4. Pilih aspek temuan untuk diselidiki dengan Amazon Detective. Konsol Detective akan terbuka untuk temuan atau entitas tersebut.

Jika pivot tidak berperilaku seperti yang diharapkan, lihat [Memecahkan masalah pivot di Panduan Pengguna Detektif Amazon](#).


**Note**

Jika Anda mengarsipkan GuardDuty temuan di konsol Detektif, temuan itu akan diarsipkan di GuardDuty konsol juga.

## Menggunakan integrasi dengan lingkungan GuardDuty multi-akun

Jika Anda mengelola lingkungan multi-akun di GuardDuty, Anda harus menambahkan akun anggota Anda ke Amazon Detective untuk melihat visualisasi data Detektif untuk temuan dan entitas di akun tersebut.

Disarankan agar Anda menggunakan akun GuardDuty Administrator yang sama dengan akun administrator untuk Detektif. Untuk informasi selengkapnya tentang cara menambahkan akun anggota di Detective, lihat [Mengundang akun anggota](#).

 **Note**

Detective adalah layanan regional. Artinya, Anda harus mengaktifkan Detective dan menambahkan akun anggota Anda di setiap wilayah tempat Anda ingin menggunakan integrasi.

# Menangguhkan atau menonaktifkan GuardDuty

Anda dapat menggunakan GuardDuty konsol untuk menangguhkan atau menonaktifkan GuardDuty layanan. Anda tidak dikenakan biaya untuk menggunakan GuardDuty ketika layanan ditangguhkan.

- Semua akun anggota harus dipisahkan atau dihapus sebelum Anda dapat menangguhkan atau menonaktifkan GuardDuty.
- Jika Anda menangguhkan GuardDuty, itu tidak lagi memantau keamanan AWS lingkungan Anda atau menghasilkan temuan baru. Temuan Anda yang ada tetap utuh dan tidak terpengaruh oleh GuardDuty penangguhan. Anda dapat memilih untuk mengaktifkan kembali GuardDuty nanti.
- Ketika Anda menonaktifkan GuardDuty di akun, itu akan dinonaktifkan hanya untuk yang saat ini dipilih Wilayah AWS. Jika Anda ingin menonaktifkan sepenuhnya GuardDuty, Anda harus menonaktifkannya di setiap Wilayah tempat diaktifkan.
- Jika Anda menonaktifkan GuardDuty, temuan Anda yang ada dan GuardDuty konfigurasi hilang dan tidak dapat dipulihkan. Jika Anda ingin menyimpan temuan yang ada, Anda harus mengekspornya sebelum mengonfirmasi untuk menonaktifkan GuardDuty. Untuk informasi tentang cara mengekspor temuan, lihat [Mengekspor temuan](#).
- Jika Anda telah mengaktifkan Perlindungan Malware untuk S3 untuk satu atau beberapa bucket yang dilindungi di akun Anda, maka menangguhkan atau menonaktifkan GuardDuty tidak memengaruhi status bucket yang dilindungi di bawah Perlindungan Malware untuk S3. Bahkan setelah menangguhkan atau menonaktifkan GuardDuty, akun Anda akan terus mengeluarkan biaya penggunaan yang terkait dengan fitur Perlindungan Malware untuk S3. Untuk informasi tentang menonaktifkan Perlindungan Malware untuk S3, lihat [Nonaktifkan Perlindungan Malware untuk S3 untuk bucket yang dilindungi](#).

Untuk menangguhkan atau menonaktifkan GuardDuty

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di GuardDuty bagian Tangguhkan, pilih Tangguhkan GuardDuty atau Nonaktifkan GuardDuty, lalu Konfirmasikan tindakan Anda.

Untuk mengaktifkan kembali GuardDuty setelah menangguhkan

1. Buka GuardDuty konsol di <https://console.aws.amazon.com/guardduty/>.

2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih Aktifkan kembali GuardDuty.



# Berlangganan pengumuman Amazon SNS GuardDuty

Bagian ini memberikan informasi tentang berlangganan Amazon SNS (Layanan Pemberitahuan Sederhana) untuk GuardDuty pengumuman untuk menerima pemberitahuan tentang jenis temuan yang baru dirilis, pembaruan untuk jenis temuan yang ada, dan perubahan fungsionalitas lainnya. Pemberitahuan tersedia dalam semua format yang SNS didukung Amazon.

GuardDuty SNSMengirim pengumuman tentang pembaruan ke GuardDuty layanan di seluruh AWS akun berlangganan apa pun. Untuk menerima pemberitahuan tentang temuan dalam akun Anda, lihat[Membuat tanggapan khusus terhadap GuardDuty temuan dengan Amazon CloudWatch Events](#).

## Note

IAMPengguna Anda harus memiliki `sns::subscribe` izin untuk berlangganan fileSNS.

Anda dapat berlangganan SQS antrian Amazon ke topik notifikasi ini, tetapi Anda harus menggunakan topik ARN yang ada di Wilayah yang sama. Untuk informasi selengkapnya, lihat [Tutorial: Berlangganan SQS antrian Amazon ke SNS topik Amazon](#) di panduan pengembang Amazon Simple Queue Service.

Anda juga dapat menggunakan AWS Lambda fungsi untuk memicu peristiwa saat pemberitahuan diterima. Untuk informasi selengkapnya, lihat [Memanggil fungsi Lambda menggunakan notifikasi SNS Amazon](#) di panduan pengembang Layanan Antrian Sederhana Amazon.

SNSTopik Amazon ARNs untuk setiap Wilayah ditunjukkan di bawah ini.

| AWS Wilayah | SNSTopik Amazon ARN                                       |
|-------------|---|
| us-east-1   | arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements |
| us-east-2   | arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements |

| AWS Wilayah  | SNSTopik Amazon ARN  |
|--------------|--|
| us-west-1    | arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements    |
| us-west-2    | arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements    |
| ca-central-1 | arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements |
| ca-west-1    | arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements    |
| eu-north-1   | arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements   |
| eu-west-1    | arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements    |
| eu-west-2    | arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements    |

| AWS Wilayah    | SNSTopik Amazon ARN  |
|----------------|--|
| eu-west-3      | arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements      |
| eu-central-1   | arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements   |
| eu-central-2   | arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements   |
| ap-east-1      | arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements      |
| ap-northeast-1 | arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements |
| ap-northeast-2 | arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements |
| ap-southeast-1 | arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements |

| AWS Wilayah    | SNSTopik Amazon ARN  |
|----------------|--|
| ap-southeast-2 | arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements       |
| ap-south-1     | arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements           |
| sa-east-1      | arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements            |
| us-gov-west-1  | arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements |
| cn-north-1     | arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements        |
| cn-northwest-1 | arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements    |
| me-south-1     | arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements           |

| AWS Wilayah    | SNSTopik Amazon ARN  |
|----------------|--|
| me-central-1   | arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements   |
| eu-south-1     | arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements     |
| eu-south-2     | arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements     |
| us-gov-east-1  | arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements  |
| ap-northeast-3 | arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements |
| ap-southeast-3 | arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements |
| ap-south-2     | arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements     |

| AWS Wilayah    | SNSTopik Amazon ARN  |
|----------------|--|
| ap-southeast-4 | arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements |
| il-central-1   | arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements   |

Untuk berlangganan email pemberitahuan GuardDuty pembaruan di AWS Management Console

1. Buka SNS konsol Amazon di <https://console.aws.amazon.com/sns/v3/home>.
2. Dalam daftar Wilayah, pilih Wilayah yang sama dengan topik ARN yang akan dilanggan. Contoh ini menggunakan Wilayah us-west-2.
3. Di sebelah kiri panel navigasi, pilih Berlangganan, Buat berlangganan.
4. Di kotak dialog Buat Langganan, untuk Topik ARN, tempel topikARN:arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements.
5. Untuk Protokol, pilih Email. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
6. Pilih Buat langganan.
7. Di aplikasi email Anda, buka pesan dari AWS Pemberitahuan dan buka tautan untuk mengonfirmasi langganan Anda.

Browser web Anda menampilkan respons konfirmasi dari AmazonSNS.

Untuk berlangganan email pemberitahuan GuardDuty pembaruan dengan AWS CLI

1. Jalankan perintah berikut dengan AWS CLI:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

- Di aplikasi email Anda, buka pesan dari AWS Pemberitahuan dan buka tautan untuk mengonfirmasi langganan Anda.

Browser web Anda menampilkan respons konfirmasi dari AmazonSNS.

## Format SNS pesan Amazon

Contoh pesan pemberitahuan GuardDuty umum:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"GENERAL\", \"message\": [{ \"title\": \"Updated AmazonGuardDutyFullAccess policy\", \"body\": \"Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.\", \"links\": [ \"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess\" ] ] }",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0X1o/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrljlg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  "version": "1",
  "type": "GENERAL",
  "message": [
    {
      "title": "Updated AmazonGuardDutyFullAccess policy",
```

```

        "body": "Added permission that allows you to pass an IAM role to
GuardDuty when you enable Malware Protection for S3.",
        "links": [
            "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess"
        ]
    }
}

```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang temuan baru ditunjukkan di bawah ini:

```

{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
environment is making connections to a Tor Guard or an Authority node. Tor is software
for enabling anonymous communication. Tor Guards and Authority nodes act as initial
gateways into a Tor network. This traffic can indicate that this EC2 instance is
acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised.\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}

```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:



```
{
  "version": "1",
  "type": "NEW_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "findingDescription": "This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance is acting as a client on a Tor network. A common use for a Tor client is to circumvent network monitoring and filter for access to unauthorized or illicit content. Tor clients can also generate nefarious Internet traffic, including attacking SSH servers. This activity can indicate that your EC2 instance is compromised."
  }]
}
```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang pembaruan GuardDuty fungsionalitas ditunjukkan di bawah ini:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FEATURES\", \"featureDetails\": [{\"featureDescription\":\"Customers with high-volumes of global CloudTrail events should see a net positive impact on their GuardDuty costs.\", \"featureLink\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-sources.html#guardduty_controlplane\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0X1o/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
```

```
}

```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  "version": "1",
  "type": "NEW_FEATURES",
  "featureDetails": [{
    "featureDescription": "Customers with high-volumes of global CloudTrail events
should see a net positive impact on their GuardDuty costs.",
    "featureLink": "https://docs.aws.amazon.com/guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
  }]
}
```

Contoh pesan pemberitahuan GuardDuty pembaruan tentang temuan yang diperbarui ditunjukkan di bawah ini:

```
{
  "Type": "Notification",
  "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\\\"findingDetails\\\":[{\\\"link\\\":\\\"https://docs.aws.amazon.com/guardduty/latest/ug/
guardduty_unauthorized.html\\\",\\\"findingType\\\":\\\"UnauthorizedAccess:EC2/TorClient\\\",
\\\"description\\\":\\\"Increased severity value from 5 to 8.\\\"}]}\",
  "Timestamp": "2018-03-09T00:25:43.483Z",
  "SignatureVersion": "1",
  "Signature": "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Nilai Pesan yang diuraikan (dengan tanda kutip yang lolos dihapus) ditunjukkan di bawah ini:

```
{
  "version": "1",
  "type": "UPDATED_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "description": "Increased severity value from 5 to 8."
  }]
}
```

# GuardDuty Kuota Amazon

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. AWS layanan Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota GuardDuty, buka konsol [Service Quotas](#). Di panel navigasi, pilih AWS layanandan pilih Amazon GuardDuty.

Untuk meminta penambahan kuota, lihat [Meminta penambahan kuota](#) di Panduan Pengguna Service Quotas.

Anda Akun AWS memiliki kuota berikut untuk Amazon GuardDuty per Wilayah.

## Note

- Untuk kuota khusus untuk Perlindungan GuardDuty Malware untuk EC2, lihat. [Perlindungan Malware untuk EC2 kuota](#)
- Untuk kuota khusus untuk Perlindungan Malware untuk S3, lihat. [Kuota dalam Perlindungan Malware untuk S3](#)

## GuardDuty kuota per Wilayah

| Sumber Daya | Default | Komentar  |
|-------------|---------|---|
| Detektor    | 1       | Jumlah maksimum sumber daya detektor yang dapat Anda buat per akun AWS per Wilayah.<br><br>Anda tidak dapat meminta kenaikan kuota. |
| Filter      | 100     | Jumlah maksimum filter yang disimpan  |

| Sumber Daya  | Default | Komentar   |
|--|---------|--|
|  |         | <p>per AWS akun per Wilayah.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p>   |
| Menemukan periode retensi                          | 90 hari | <p>Jumlah maksimum hari temuan dipertahankan.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p>  |
| Alamat IP dan rentang CIDR per Daftar IP Tepercaya | 2.000   | <p>Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam satu Daftar IP Tepercaya.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p> |
| Alamat IP dan rentang CIDR per Daftar Ancaman      | 250.000 | <p>Jumlah maksimum alamat IP dan rentang CIDR yang dapat Anda sertakan dalam Daftar Ancaman.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p>           |

| Sumber Daya                    | Default | Komentar  |
|--------------------------------|---------|---|
| Ukuran file maksimum           | 35 MB   | <p>Ukuran file maksimum untuk file yang digunakan untuk mengunggah daftar alamat IP atau rentang CIDR yang disertakan dalam Daftar IP Terpercaya atau Daftar Ancaman.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p> |
| Akun anggota (dengan undangan) | 5000    | <p>Jumlah maksimum akun anggota yang terkait dengan akun administrator.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p>   |

| Sumber Daya  | Default | Komentar  |
|--------------|---------|---|
| Akun anggota | 50.000  | <p>Jumlah maksimum akun anggota yang terkait dengan akun administrator melalui AWS Organizations. Ini termasuk akun anggota yang ditambahkan ke organisasi melalui undangan.</p> <p>Nilai default ini tergantung pada kuota Anda saat ini untuk akun anggota di AWS Organizations. Jumlah akun anggota GuardDuty yang ditambahkan tidak AWS Organizations dapat melebihi jumlah akun anggota di organisasi Anda. Untuk informasi tentang jumlah Akun AWS dalam organisasi, lihat <a href="#">Nilai maksimum dan minimum</a> dalam Panduan AWS Organizations Pengguna.</p> |

| Sumber Daya       | Default | Komentar   |
|-------------------|---------|--|
| Ancaman intel set | 6       | <p>Jumlah maksimum set intel Ancaman yang dapat Anda tambahkan per akun AWS per Wilayah.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p>         |
| Set IP tepercaya  | 1       | <p>Jumlah maksimum set IP tepercaya yang dapat diunggah dan diaktifkan per AWS akun per Wilayah.</p> <p>Anda tidak dapat meminta kenaikan kuota.</p> |



# Memecahkan Masalah Amazon GuardDuty

Saat Anda menerima masalah yang terkait dengan melakukan tindakan khusus GuardDuty, lihat topik di bagian ini.

Topik

- [Masalah umum di GuardDuty](#)
- [Perlindungan Malware untuk masalah EC2](#)
- [Masalah Runtime Monitoring](#)
- [Mengelola beberapa masalah akun](#)
- [Masalah pemecahan masalah lainnya](#)

## Masalah umum di GuardDuty

Saya mendapatkan kesalahan akses saat mengekspor GuardDuty temuan. Bagaimana saya bisa menyelesaikan ini?

Setelah Anda mengonfigurasi pengaturan untuk mengekspor temuan, jika GuardDuty tidak dapat mengekspor temuan, akan menampilkan pesan kesalahan pada halaman Pengaturan di GuardDuty konsol. Hal ini berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses sumber daya target, misalnya, jika bucket Amazon S3 Anda telah dihapus atau izin untuk mengakses bucket telah diubah. Ini juga berpotensi terjadi ketika tidak GuardDuty dapat lagi mengakses AWS KMS kunci yang digunakan untuk mengenkripsi data di bucket Amazon S3 Anda. Ketika GuardDuty tidak dapat mengekspor, ia mengirimkan pemberitahuan ke email yang terkait dengan akun untuk memberikan informasi tentang masalah ini.

Untuk mengatasi masalah ini, pastikan sumber daya yang sesuai ada dan GuardDuty memiliki izin untuk mengakses sumber daya yang diperlukan. Jika Anda tidak menyelesaikan masalah sebelum periode retensi temuan 90 hari selesai GuardDuty, temuan Anda tidak akan diekspor. GuardDuty akan menonaktifkan pencarian pengaturan ekspor untuk akun ini di Wilayah tertentu. Bahkan di luar tanggal retensi ini, Anda dapat memperbarui pengaturan konfigurasi untuk memulai ulang mengekspor temuan di Wilayah tertentu.

Untuk informasi selengkapnya, lihat [Mengekspor temuan](#).

## Perlindungan Malware untuk masalah EC2

Saya memulai pemindaian malware On-Demand tetapi menghasilkan kesalahan izin yang diperlukan hilang.

Jika Anda menerima kesalahan yang menunjukkan bahwa Anda tidak memiliki izin yang diperlukan untuk memulai pemindaian malware Sesuai Permintaan pada instans Amazon EC2, verifikasi bahwa Anda telah melampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) kebijakan tersebut ke peran IAM Anda.

Jika Anda anggota AWS organisasi dan masih menerima kesalahan yang sama, sambungkan dengan akun manajemen Anda. Untuk informasi selengkapnya, lihat [AWS Organizations SCP—Akses ditolak](#).

Saya menerima **iam:GetRole** kesalahan saat bekerja dengan Perlindungan Malware untuk EC2.

Jika Anda menerima kesalahan ini —Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection, itu berarti Anda kehilangan izin untuk mengaktifkan pemindaian malware yang GuardDuty dimulai atau menggunakan pemindaian malware sesuai permintaan. Verifikasi bahwa Anda telah melampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) kebijakan ke peran IAM Anda.

Saya adalah akun GuardDuty administrator yang perlu mengaktifkan GuardDuty pemindaian malware yang dimulai tetapi tidak menggunakan kebijakan AWS terkelola: AmazonGuardDutyFullAccess untuk mengelola GuardDuty

- Konfigurasi peran IAM yang Anda gunakan GuardDuty untuk memiliki izin yang diperlukan untuk mengaktifkan pemindaian malware GuardDuty yang dimulai. Untuk informasi selengkapnya tentang izin yang diperlukan, lihat [Membuat peran terkait layanan untuk Perlindungan Malware untuk EC2](#).
- Lampirkan [AWS kebijakan terkelola: AmazonGuardDutyFullAccess](#) ke peran IAM Anda. Ini akan membantu Anda mengaktifkan GuardDuty pemindaian malware yang dimulai untuk akun anggota.

# Masalah Runtime Monitoring

## AWS Step Functions Alur kerja saya gagal secara tak terduga

Jika GuardDuty kontainer berkontribusi pada kegagalan alur kerja, lihat [Memecahkan masalah cakupan](#). Jika masalah berlanjut, maka untuk mencegah kegagalan alur kerja karena GuardDuty penampung, lakukan salah satu langkah berikut:

- Tambahkan `false` tag `GuardDutyManaged:` ke cluster Amazon ECS terkait.
- Nonaktifkan konfigurasi agen otomatis untuk AWS Fargate (khusus ECS) di tingkat akun. Tambahkan tag inklusi `GuardDutyManaged: true` ke cluster Amazon ECS terkait yang ingin Anda lanjutkan pemantauan dengan agen GuardDuty otomatis.

## Memecahkan masalah kesalahan memori di Runtime Monitoring (hanya mendukung Amazon EC2)

Bagian ini menyediakan langkah-langkah pemecahan masalah ketika Anda mengalami kesalahan kehabisan memori berdasarkan [CPU dan batas memori](#) untuk menyebarkan agen GuardDuty keamanan secara manual.

Jika `systemd` menghentikan GuardDuty agen karena `out-of-memory` masalah dan Anda mengevaluasi bahwa memberikan lebih banyak memori kepada GuardDuty agen masuk akal, Anda dapat memperbarui batasnya.

1. Dengan izin root, buka `/lib/systemd/system/amazon-guardduty-agent.service`.
2. Temukan `MemoryLimit` dan `MemoryMax`, dan perbarui kedua nilainya.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Setelah memperbarui nilai, restart GuardDuty agen dengan menggunakan perintah berikut:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Jalankan perintah berikut untuk melihat status:

```
sudo systemctl status amazon-guardduty-agent
```

Output yang diharapkan akan menunjukkan batas memori baru:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

## Mengelola beberapa masalah akun

Saya ingin mengelola banyak akun tetapi tidak memiliki izin AWS Organizations manajemen yang diperlukan.

Jika Anda menerima kesalahan ini —`The request failed because you do not have required AWS Organization master permission.`, itu berarti Anda kehilangan izin untuk mengaktifkan GuardDuty pemindaian malware yang dimulai untuk beberapa akun di organisasi Anda. Untuk informasi selengkapnya tentang memberikan izin ke akun manajemen, lihat [Membangun akses tepercaya untuk mengaktifkan GuardDuty pemindaian malware yang dimulai](#).

## Masalah pemecahan masalah lainnya

Jika Anda tidak menemukan skenario yang sesuai dengan masalah Anda, lihat opsi pemecahan masalah berikut:

- Untuk masalah IAM umum saat Anda mengakses <https://console.aws.amazon.com/guardduty/>, lihat [Memecahkan masalah GuardDuty identitas dan akses Amazon](#).
- Untuk masalah autentikasi dan otorisasi saat Anda mengakses AWS AWS Console Home, lihat [Memecahkan Masalah IAM](#).

## Wilayah dan titik akhir

Untuk melihat di Wilayah AWS mana Amazon GuardDuty tersedia, lihat [GuardDuty titik akhir Amazon](#) di. Referensi Umum Amazon Web Services

Kami menyarankan Anda mengaktifkan semua GuardDuty yang didukung Wilayah AWS. Hal ini memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau AWS CloudTrail peristiwa yang didukung Wilayah AWS, kemampuannya untuk mendeteksi aktivitas yang melibatkan layanan global berkurang.

## Ketersediaan fitur khusus wilayah

Daftar perbedaan regional untuk menentukan ketersediaan GuardDuty fitur.

ListFindings dan GetFindingsStatistics API

[ListFindings](#) API [GetFindingsStatistics](#) dan memiliki `consoleOnly` bendera sementara. Bila Anda menggunakan salah satu atau kedua API ini, `consoleOnly` tanda berarti API dapat mengambil hasil hingga batas maksimum 1000.

GuardDuty fitur dengan disparitas Wilayah

[Perlindungan Malware untuk EC2](#)

GuardDuty mendukung Perlindungan Malware untuk fitur EC2 di [AWS Dedicated Local Zones](#).

Dukungan API umum

API berikut dalam Referensi Amazon GuardDuty API mungkin memiliki perbedaan regional karena tidak tersedianya beberapa sumber data atau fitur yang ditentukan Wilayah AWS sebelumnya:

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)

- [DescribeOrganizationConfiguration](#)

Jenis penemuan Amazon EC2 — dan [DefenseEvasion:EC2/UnusualDoHActivity](#)  
[DefenseEvasion:EC2/UnusualDoTActivity](#)

Tabel berikut menunjukkan di Wilayah AWS mana GuardDuty tersedia tetapi kedua jenis temuan Amazon EC2 ini belum didukung.

| Wilayah AWS            | Kode Wilayah   |
|------------------------|----------------|
| Asia Pasifik (Seoul)   | ap-northeast-2 |
| Asia Pacific (Osaka)   | ap-northeast-3 |
| Asia Pasifik (Jakarta) | ap-southeast-3 |

AWS GovCloud (US) Daerah

Untuk informasi terbaru, lihat [Amazon GuardDuty](#) di Panduan AWS GovCloud (US) Pengguna.

Wilayah China

Untuk informasi terbaru, lihat [Ketersediaan fitur dan perbedaan implementasi](#).

## GuardDuty tindakan dan parameter warisan

Amazon GuardDuty telah menghentikan beberapa tindakan dan parameter API tetapi masih mendukungnya. Praktik terbaik adalah menggunakan tindakan dan parameter API baru yang menggantikan opsi lama. Tabel berikut membandingkan tindakan dan parameter lama dan baru.

| Tindakan/<br>parameter lama  | Tindakan/parameter baru                              | Perbandingan  |
|--|--|---|
| <a href="#">DisassociateFromMasterAccount</a>  | <a href="#">DisassociateFromAdministratorAccount</a> | Dengan implementasi yang sama di kedua tindakan, GuardDuty gunakan istilah Administrator dalam <code>DisassociateFromAdministratorAccount</code> .  |
| autoEnable parameter dalam <a href="#">DescribeOrganizationConfiguration</a> dan <a href="#">UpdateOrganizationConfiguration</a> | <a href="#">autoEnableOrganizationMembers</a>        | Dengan <code>autoEnableOrganizationMembers</code> , akun GuardDuty administrator dapat mengaudit dan menegakkan GuardDuty semua akun anggota ke salah satu nilai. Menggunakan API, mungkin diperlukan waktu hingga 24 jam untuk memperbarui konfigurasi untuk semua akun anggota. Untuk informasi selengkapnya tentang kemungkinan nilai <code>autoEnableOrganizationMembers</code> bidang, lihat <a href="#">autoEnableOrganizationAnggota</a> |
| dataSource parameter dalam API yang tercantum dalam <a href="#">GuardDuty</a>  | <a href="#">features</a>                             | Mulai Maret 2023, Anda dapat mengonfigurasi <a href="#">GuardDuty Perlindungan Malware untuk EC2</a> dan menggunakan features paket GuardDuty perlindungan baru. Rencana perlindungan yang diluncurkan sebelum Maret 2023,  |

| Tindakan/<br>parameter lama                   | Tindakan/parameter baru | Perbandingan  |
|---|-------------------------|---|
| <a href="#">API perubahan<br/>Maret 2023.</a> |                         | termasuk Perlindungan Malware untuk EC2 masih mendukung penggunaan konfigurasi. <code>dataSources</code> Jika Anda menggunakan API untuk mengonfigurasi paket perlindungan, setiap permintaan API dapat menyertakan <code>dataSources</code> atau <code>features</code> , tidak keduanya. |



# Riwayat dokumen untuk Amazon GuardDuty

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Panduan GuardDuty Pengguna Amazon. Untuk pemberitahuan tentang pembaruan dokumentasi ini, Anda dapat berlangganan RSS umpan.

| Perubahan  | Deskripsi   | Tanggal          |
|--|---|------------------|
| <a href="#">Peran GuardDuty terkait layanan yang diperbarui () SLR</a> | GuardDuty telah memperbarui SLR untuk menyertakan <code>ec2:Describe:Vpcs</code> izin dalam EC2 tindakan Amazon. Untuk informasi selengkapnya, lihat <a href="#">Izin peran terkait layanan</a> untuk GuardDuty   | Agustus 22, 2024 |
| <a href="#">Penambahan konten yang signifikan</a>                      | <p>GuardDuty menambahkan pembaruan konten yang signifikan ke fitur Perlindungan Malware untuk S3.</p> <ul style="list-style-type: none"><li>• Menambahkan contoh baru skema pemberitahuan sampel untuk menyiapkan EventBridge aturan Amazon agar menerima pemberitahuan terkait status sumber daya paket Perlindungan Malware dan hasil pemindaian objek S3. Untuk informasi selengkapnya, lihat <a href="#">Memantau pemindaian objek S3 dengan Amazon EventBridge</a></li><li>• Menambahkan informasi tentang <a href="#">pemecahan</a></li></ul> | Agustus 20, 2024 |

---

|  |   |                  |
|--|---|------------------|
|  | <a href="#">masalah kegagalan tag pasca-pemindaian objek S3.</a>  |                  |
| <a href="#">Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EC2</a> | Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya AmazonEC2. Untuk informasi selengkapnya tentang catatan rilis, lihat <a href="#">agen GuardDuty keamanan untuk Amazon EC2</a> .  | Agustus 19, 2024 |
| <a href="#">Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Amazon EKS</a> | Runtime Monitoring merilis agen baru versi 1.7.0 untuk sumber daya Amazon. EKS Untuk informasi selengkapnya tentang catatan rilis, lihat <a href="#">agen GuardDuty keamanan untuk EKS klaster Amazon</a> .   | Agustus 17, 2024 |
| <a href="#">Penambahan konten yang signifikan</a>  | GuardDuty menambahkan informasi baru tentang metodologi deteksi malware dan mesin pemindaian yang digunakannya untuk Perlindungan Malware untuk S3 dan Perlindungan Malware untuk EC2 fitur. Untuk informasi selengkapnya, lihat <a href="#">mesin pemindaian deteksi GuardDuty malware</a> . | Agustus 15, 2024 |

[Fitur baru - Melindungi beban kerja AI](#)

GuardDuty deteksi ancaman dasar dan Perlindungan Lambda membantu Anda mengamankan dan mendeteksi ancaman terhadap beban kerja AI yang dibangun dengan lebih baik. AWS Untuk informasi selengkapnya, lihat [Melindungi beban kerja AI dengan GuardDuty](#).

Agustus 14, 2024

[Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate \(hanya AmazonECS\)](#)

Runtime Monitoring merilis agen baru versi 1.3.0 untuk sumber daya (ECS khusus AWS Fargate Amazon). Untuk informasi lebih lanjut tentang catatan rilis, lihat [agen GuardDuty keamanan untuk Fargate- ECS](#).

Agustus 9, 2024

[Fungsionalitas yang diperbarui - Perlindungan Malware untuk S3](#)

GuardDuty Perlindungan Malware untuk S3 meningkatkan jumlah maksimum kuota bucket S3 dari 10 menjadi 25 bucket. Kuota ini berlaku untuk Akun AWS per masing-masing Wilayah AWS. Untuk informasi selengkapnya, lihat [Perlindungan Malware untuk S3](#).

Agustus 8, 2024

### [Diperbarui - Jenis temuan baru di Runtime Monitoring](#)

GuardDuty telah menambahkan dua jenis temuan Pemantauan Runtime baru yang akan membantu Anda mendeteksi ancaman yang melibatkan pembuatan shell yang mencurigakan pada sumber daya yang dipantau, dan eskalasi hak istimewa di mana suatu proses secara mencurigakan meningkatkan hak istimewanya untuk melakukan root.

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

Agustus 6, 2024

### [Diperbarui - Integrasi dengan AWS Security Hub](#)

AWS Security Hub menyediakan daftar kontrol GuardDuty keamanan untuk mengevaluasi sumber daya Anda, dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk informasi selengkapnya, lihat [Menggunakan GuardDuty kontrol di Security Hub](#).

Juli 11, 2024

### [Skrip GuardDuty tester yang diperbarui untuk temuan](#)

GuardDuty sekarang mendukung lebih dari 100 temuan dengan AWS sumber daya yang berbeda di akun khusus. Gunakan [amazon-guardduty-tester](#) repositori dan ikuti langkah-langkah untuk menguji temuan dan meninjaunya untuk memahami detail temuan. Untuk informasi selengkapnya, lihat [GuardDuty Temuan uji di akun khusus](#).

Juni 28, 2024

### [Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen keamanan baru versi 1.2.0 untuk sumber daya AmazonEC2. Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#). Untuk informasi tentang memperbarui agen keamanan ke versi rilis ini secara manual, lihat [Mengelola agen keamanan secara manual untuk EC2 instans Amazon](#).

Juni 13, 2024

[Fitur baru - Perlindungan  
Malware untuk ketersediaan  
Wilayah S3](#)

GuardDuty Perlindungan Malware untuk S3 sekarang tersedia di semua Wilayah komersial di mana GuardDuty tersedia. Fitur ini membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencurigakan, dan mengambil tindakan untuk mengisolasi sebelum dimasukkan ke dalam proses hilir. Untuk informasi tentang mengaktifkan Perlindungan Malware untuk S3, lihat [Perlindungan GuardDuty Malware untuk S3](#).

Juni 12, 2024

## [Fitur baru - Perlindungan Malware untuk S3](#)

Juni 11, 2024

GuardDuty mengumumkan ketersediaan umum Perlindungan Malware untuk S3 yang membantu Anda memindai objek yang baru diunggah ke bucket Amazon S3 untuk mencari potensi malware dan unggahan yang mencurigakan, dan mengambil tindakan untuk mengisolasinya sebelum tertelan ke dalam proses hilir. Fitur ini sepenuhnya dikelola oleh AWS. GuardDuty menerbitkan hasil pemindaian objek S3 ke bus acara EventBridge default Anda. Anda dapat mengizinkan GuardDuty untuk menambahkan tag ke objek S3 yang dipindai. Anda dapat membuat alur kerja hilir, seperti isolasi ke bucket karantina, atau menentukan kebijakan bucket menggunakan tag yang mencegah pengguna atau aplikasi mengakses objek tertentu. Untuk informasi selengkapnya, lihat [Perlindungan GuardDuty Malware untuk S3](#). Saat ini, tersedia di Wilayah berikut:

- AS Timur (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Europe (Ireland)

- Eropa (Frankfurt)
- Eropa (Stockholm)
- Asia Pasifik (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Singapore)  
(Asia Pacific (Singapore))

[AmazonGuardDutyFullAccessKebijakan yang diperbarui](#)

Menambahkan izin yang memungkinkan Anda meneruskan IAM peran GuardDuty saat Anda mengaktifkan Perlindungan Malware untuk S3. Untuk informasi selengkapnya tentang pembaruan kebijakan ini, lihat [GuardDuty pembaruan kebijakan AWS terkelola](#).

Juni 10, 2024

[Fungsionalitas yang diperbarui dalam GuardDuty RDS Perlindungan](#)

RDSPerlindungan memperluas dukungan untuk memantau aktivitas login pada database RDS SQL Postgre Anda. Sebagai bagian dari ekspansi ini, secara otomatis GuardDuty akan mulai memantau data login dari RDS SQL database Postgre untuk akun yang telah mengaktifkan Perlindungan. GuardDuty RDS Untuk informasi selengkapnya, lihat [RDSPerlindungan](#).

Juni 6, 2024



|   |   |             |
|---|---|-------------|
| <a href="#">Fungsionalitas yang diperbarui dalam GuardDuty Runtime Monitoring - Fargate (hanya AmazonECS)</a> | Runtime Monitoring merilis agen baru versi 1.2.0 untuk sumber daya (ECS khusus AWS Fargate Amazon). Untuk informasi lebih lanjut tentang catatan rilis, lihat <a href="#">agen GuardDuty keamanan untuk Fargate- ECS</a> .  | 31 Mei 2024 |
| <a href="#">Fungsionalitas yang diperbarui dalam Perlindungan GuardDuty Malware untuk EC2</a>                 | Untuk setiap EBS volume Amazon yang dilampirkan ke EC2 instans Amazon dan beban kerja kontainer Anda, Perlindungan GuardDuty Malware untuk EC2 telah meningkatkan ukuran EBS volume yang dipindai hingga 2048 GB. Untuk informasi tentang pemindaian EBS volume Amazon yang dilampirkan ke instans Anda, lihat <a href="#">Perlindungan GuardDuty Malware untuk EC2</a> . | 29 Mei 2024 |
| <a href="#">Fungsionalitas yang diperbarui di Runtime Monitoring</a>  | Runtime Monitoring untuk Amazon ECS - Fargate resource sekarang mendukung pendeteksian potensi ancaman pada tugas yang diluncurkan oleh dan. AWS Batch AWS CodePipeline Untuk informasi selengkapnya, lihat <a href="#">Cara Runtime Monitoring bekerja dengan Fargate (hanya ECS Amazon)</a> .   | 28 Mei 2024 |

|  |  |             |
|--|--|-------------|
| <a href="#">Fungsionalitas yang diperbarui di Runtime Monitoring</a>     | Runtime Monitoring merilis agen baru versi 1.6.1 untuk sumber daya Amazon. EKS Untuk informasi tentang catatan rilis, lihat <a href="#">riwayat rilis agen EKS add-on</a> .  | 14 Mei 2024 |
| <a href="#">Dukungan Wilayah yang Diperluas untuk Runtime Monitoring</a> | GuardDuty memperluas dukungan untuk Runtime Monitoring ke Wilayah Kanada Barat (Calgary) . Untuk informasi tentang memulai Runtime Monitoring, lihat <a href="#">Mengaktifkan Runtime Monitoring</a> .   | 7 Mei 2024  |
| <a href="#">Dukungan Wilayah yang Diperluas untuk RDS Perlindungan</a>   | GuardDuty memperluas dukungan RDS Perlindungan menjadi berikut: Wilayah AWS <ul style="list-style-type: none"><li>• Kanada Barat (Calgary)</li><li>• Asia Pasifik (Hyderabad)</li><li>• Eropa (Spanyol)</li><li>• Eropa (Zürich)</li><li>• Timur Tengah (UAE)</li><li>• Israel (Tel Aviv)</li><li>• Asia Pasifik (Melbourne)</li></ul> Untuk informasi tentang mengaktifkan fitur ini, lihat <a href="#">RDSPerlindungan</a> . | 3 Mei 2024  |

|  |   |                |
|--|---|----------------|
| <a href="#">Fungsionalitas yang diperbarui di Runtime Monitoring</a>                 | Runtime Monitoring merilis agen baru versi 1.1.0 untuk sumber daya (ECS khusus AWS Fargate Amazon). Untuk informasi lebih lanjut tentang catatan rilis, lihat <a href="#">agen GuardDuty keamanan untuk Fargate- ECS</a> .            | 1 Mei 2024     |
| <a href="#">Fungsionalitas yang diperbarui di Runtime Monitoring</a>                 | Runtime Monitoring merilis agen baru versi 1.6.0 untuk sumber daya Amazon. EKS Untuk informasi tentang catatan rilis, lihat <a href="#">riwayat rilis agen EKS add-on</a> .   | April 29, 2024 |
| <a href="#">Support untuk IPAddressv6</a>  | GuardDuty telah menambahkan IPAddressv6 dukungan untuk detail IP lokal dan jarak jauh. Anda dapat menggunakan <a href="#">atribut Filter</a> terkait untuk memfilter GuardDuty temuan atau <a href="#">membuat aturan penekanan</a> . | April 18, 2024 |
| <a href="#">Pengalaman konsol yang diperbarui untuk mengonfigurasi temuan ekspor</a> | GuardDuty telah memperbaiki pengalaman konsol untuk mengeksport temuan yang dihasilkan di Akun AWS ember Amazon S3 Anda. Untuk informasi lebih lanjut, lihat <a href="#">Mengekspor GuardDuty temuan</a> .                            | April 1, 2024  |

## [Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen keamanan baru versi 1.1.0 untuk sumber daya AmazonEC2. Versi ini mendukung konfigurasi agen GuardDuty otomatis dalam Runtime Monitoring untuk EC2 instans Amazon. Untuk informasi tentang catatan rilis, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#).

Maret 28, 2024

[Ketersediaan umum Runtime Monitoring untuk instans Amazon EC2](#)

Maret 28, 2024

GuardDuty mengumumkan ketersediaan umum (GA) dari Runtime Monitoring untuk instans AmazonEC2. Sekarang, Anda memiliki opsi untuk [mengaktifkan konfigurasi agen otomatis](#) yang memungkinkan GuardDuty untuk menginstal dan mengelola agen keamanan untuk EC2 instans Amazon Anda atas nama Anda. Dengan agen GuardDuty otomatis, Anda juga dapat menggunakan tag inklusi atau pengecualian untuk menginformasikan GuardDuty agar menginstal dan mengelola agen keamanan hanya pada EC2 instans Amazon tertentu. Untuk informasi selengkapnya, lihat [Cara kerja Runtime Monitoring dengan EC2 instans Amazon](#).

Daftar jenis temuan baru yang dirilis bersama dengan GA ini

- [Eksekusi:Runtime/SuspiciousTool](#)
- [Eksekusi:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)

- [Eksekusi:Runtime/ Malicious FileExecuted](#)

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(\) SLR](#)

Maret 26, 2024

Gunakan AWS Systems Manager tindakan untuk mengelola SSM asosiasi di EC2 instans Amazon saat Anda mengaktifkan Pemantauan GuardDuty Waktu Proses dengan agen otomatis untuk Amazon. EC2 Ketika konfigurasi agen GuardDuty otomatis dinonaktifkan, GuardDuty pertimbangkan hanya EC2 instance yang memiliki tag inklusi (GuardDuty Managed :true).

- Daftar berikut menunjukkan izin baru:

```
"ssm:DescribeAssociation",  
"ssm:DeleteAssociation",  
"ssm:UpdateAssociation",  
"ssm:CreateAssociation",  
"ssm:StartAssociationsOnce",  
"ssm:AddTagsToResource",  
"ssm:CreateAssociation",  
"ssm:UpdateAssociation",  
"ssm:SendCommand",  
"ssm:GetCommandInvocation"
```

### [Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Dengan rilis v1.5.0 agen GuardDuty keamanan terbaru (add-on) untuk AmazonEKS, Runtime Monitoring sekarang mendukung konfigurasi parameter spesifik agen GuardDuty keamanan Anda, seperti pengaturan memori, pengaturan, CPU dan PriorityClass pengaturan kebijakan. DNS Untuk informasi selengkapnya, lihat [Mengonfigurasi GuardDuty parameter agen keamanan \(EKSadd-on\)](#).

7 Maret 2024

### [Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen baru versi 1.5.0 untuk sumber daya AmazonEKS. Untuk informasi tentang catatan rilis, lihat [riwayat rilis agen EKS add-on](#).

7 Maret 2024

### [Support untuk Canada West \(Calgary\)](#)

Amazon sekarang GuardDuty tersedia di Wilayah Kanada Barat (Calgary). Beberapa rencana perlindungan di dalamnya GuardDuty mungkin tidak tersedia di Wilayah ini. Untuk informasi terbaru, lihat [Wilayah dan titik akhir](#).

Maret 6, 2024



[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Agen GuardDuty keamanan versi 1.0.0 dan 1.1.0 untuk EKS cluster Amazon tidak akan lagi didukung mulai 14 Mei 2024. Untuk informasi tentang langkah-langkah apa yang dapat Anda ambil sebelum akhir dukungan standar, lihat [agen GuardDuty keamanan untuk EKS klaster Amazon](#).

Februari 16, 2024

[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring mendukung [Kubernetes versi 1.29 terbaru dengan agen keamanan versi 1.4.1](#) yang ada. Dukungan telah tersedia sejak peluncuran versi Kubernetes ini. Untuk informasi tentang versi Kubernetes yang didukung, lihat Versi [Kubernetes](#) yang didukung oleh agen keamanan. GuardDuty

Februari 16, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional](#)

GuardDuty Runtime Monitoring sekarang mendukung Amazon bersama VPC dalam hal yang sama AWS Organizations. [GuardDuty peran terkait layanan \(SLR\)](#) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk VPC akun Amazon bersama untuk menetapkan kebijakan titik akhir. [Untuk informasi tentang prasyarat untuk menggunakan VPC endpoint Amazon bersama di Runtime Monitoring, lihat Support for shared Amazon VPC](#) Kemampuan ini tersedia di semua Wilayah yang GuardDuty mendukung Runtime Monitoring.

Februari 12, 2024

[Fungsionalitas yang diperbarui dalam Runtime Monitoring - Ketersediaan regional](#)

GuardDuty Runtime Monitoring sekarang mendukung Amazon bersama VPC dalam hal yang sama AWS Organizations. [GuardDuty peran terkait layanan \(SLR\)](#) memiliki izin baru — `organizations:DescribeOrganization` yang membantu mengambil ID organisasi untuk VPC akun Amazon bersama untuk menetapkan kebijakan titik akhir. [Untuk informasi tentang prasyarat untuk menggunakan VPC endpoint Amazon bersama di Runtime Monitoring, lihat Support for shared Amazon. VPC](#) Saat ini, kemampuan ini tersedia di beberapa Wilayah AWS. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

Februari 9, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

Perlindungan Malware untuk EC2 saat ini mendukung pemindaian EBS volume yang dienkripsi Kunci yang dikelola AWS di Wilayah AS Barat (Oregon).

Februari 6, 2024

Februari 5, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian EBS volume yang dienkripsi sebagai Kunci yang dikelola AWS berikut: Wilayah AWS](#)

- Asia Pacific (Singapore) (ap-southeast-1 )
- Europe (Frankfurt) (eu-central-1 )
- Asia Pacific (Osaka) (ap-northeast-3 )
- US East (Ohio) (us-east-2 )
- Europe (Milan) (eu-south-1 )
- Asia Pacific (Tokyo) (ap-northeast-1 )
- Asia Pacific (Seoul) (ap-northeast-2 )
- Canada (Central) (ca-central-1 )
- Europe (Ireland) (eu-west-1 )
- US East (N. Virginia) (us-east-1 )

## Fungsionalitas yang diperbarui di Runtime Monitoring

GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.2) untuk instans AmazonEC2. Versi agen ini mencakup dukungan untuk Amazon terbaru ECSAMIs. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#).

Februari 2, 2024

Januari 31, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS - Perlindungan Malware untuk EC2](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian EBS volume Amazon yang dienkripsi dengan berikut Kunci yang dikelola AWS ini: Wilayah AWS](#)

- Europe (London) (eu-west-2 )
- Europe (Stockholm) (eu-north-1 )
- Asia Pacific (Hong Kong) (ap-east-1 )
- Africa (Cape Town) (af-south-1 )
- Middle East (Bahrain) (me-south-1 )
- Asia Pasifik (Hyderabad) (ap-south-2 )
- Eropa (Spanyol) (eu-south-2 )
- Asia Pasifik (Melbourne) (ap-southeast-4 )
- Asia Pacific (Sydney) (ap-southeast-2 )
- Israel (Tel Aviv) (il-central-1 )

[Mengelola akun yang diperbarui dengan AWS Organizations](#)

Menata ulang konten di bawah [Mengelola akun dengan AWS Organizations](#) , menambahkan langkah-langkah untuk mengubah akun GuardDuty administrator yang didelegasikan, dan diperbarui [Memahami hubungan antara akun GuardDuty administrator dan akun anggota](#).

Januari 30, 2024

[Fungsionalitas yang diperbarui dengan dukungan untuk yang baru Wilayah AWS](#)

[Perlindungan Malware untuk EC2 saat ini mendukung pemindaian EBS volume yang dikripsi sebagai Kunci yang dikelola AWS berikut: Wilayah AWS](#)

Januari 29, 2024

- Asia Pasifik (Jakarta) (ap-southeast-3 )
- US West (N. California) (us-west-1 )
- Timur Tengah (UAE) (me-central-1 )
- Eropa (Zurich) (eu-central-2 )
- Asia Pacific (Mumbai) (ap-south-1 )
- South America (São Paulo) (sa-east-1 )

### [Fungsionalitas yang diperbarui dalam Perlindungan Malware untuk EC2](#)

Perlindungan Malware untuk EC2 saat ini mendukung pemindaian EBS volume yang dienkripsi menggunakan Kunci yang dikelola AWS [Perlindungan Malware untuk peran EC2 terkait layanan \(SLR\)](#) memiliki dua izin baru — dan. `GetSnapshotBlock` `ListSnapshots` `hotBlocks` Izin ini akan membantu GuardDuty mengambil snapshot EBS volume (dienkripsi menggunakan Kunci yang dikelola AWS) dari Akun AWS dan menyalinnya ke [akun GuardDuty layanan sebelum memulai pemindaian malware](#). Saat ini, fungsi ini hanya tersedia di Eropa (Paris) (eu-west-3 ). Untuk informasi selengkapnya, lihat [Volume yang didukung untuk pemindaian malware](#).

Januari 25, 2024

### [Fungsionalitas yang diperbarui di Runtime Monitoring](#)

GuardDuty Runtime Monitoring telah merilis versi agen GuardDuty keamanan baru (v1.0.1) dengan penyetelan dan peningkatan kinerja umum. Untuk informasi selengkapnya tentang riwayat rilis agen, lihat [agen GuardDuty keamanan untuk EC2 instans Amazon](#).

23 Januari 2024



[Fungsionalitas yang diperbarui di Runtime Monitoring](#)

Runtime Monitoring merilis agen baru versi 1.4.1 untuk sumber daya AmazonEKS. Untuk informasi selengkapnya, lihat [riwayat rilis agen EKS add-on](#).

Januari 16, 2024

[Runtime Monitoring merilis agen baru v1.4.0 untuk sumber daya Amazon EKS](#)

Runtime Monitoring merilis agen baru versi 1.4.0 untuk sumber daya AmazonEKS. Untuk informasi selengkapnya, lihat [riwayat rilis agen EKS add-on](#).

21 Desember 2023

[Menambahkan jenis temuan berbasis S3 dan pembelajaran AWS CloudTrail mesin \(ML\) ke Eropa \(Zurich\), Eropa \(Spanyol\), Asia Pasifik \(Hyderabad\), Asia Pasifik \(Melbourne\), dan Israel \(Tel Aviv\)](#)

S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunakan model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Eropa (Zurich), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), dan Israel (Tel Aviv): GuardDuty

21 Desember 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)

- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty mendukung 50.000 akun anggota melalui AWS Organizations](#)

GuardDuty Administrator yang didelegasikan sekarang dapat mengelola maksimal 50.000 akun anggota melalui AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.

20 Desember 2023

[GuardDuty Dukungan Runtime Monitoring diperluas menjadi 19 Wilayah AWS](#)

Runtime Monitoring sekarang tersedia di Asia Pasifik (Jakarta), Eropa (Paris), Asia Pasifik (Osaka), Asia Pasifik (Seoul), Timur Tengah (Bahrain), Eropa (Spanyol), Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Israel (Tel Aviv), AS Barat (California N.), Eropa (London), Asia Pasifik (Hong Kong), Eropa (Milan), Timur Tengah (), Selatan Amerika (São PauloUAE), Asia Pasifik (Mumbai), Kanada (Tengah), Afrika (Cape Town), Eropa (Zurich).

6 Desember 2023

[GuardDuty memperluas kemampuan Runtime Monitoring](#)

Selain mendeteksi ancaman terhadap EKS kluster Amazon Anda, GuardDuty mengumumkan ketersediaan umum Runtime Monitoring untuk mendeteksi ancaman terhadap ECS beban kerja Amazon Anda dan rilis pratinjau untuk mendeteksi ancaman terhadap instans Amazon Anda. EC2 Untuk informasi selengkapnya tentang yang Wilayah AWS saat ini mendukung Runtime Monitoring, lihat [Wilayah dan titik akhir](#).

26 November 2023

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(\) SLR](#)

GuardDuty telah menambahkan izin baru untuk menggunakan ECS tindakan Amazon untuk mengelola dan mengambil informasi tentang ECS kluster Amazon, dan mengelola setelan ECS akun Amazon dengan. guardduty Activate Tindakan yang berkaitan dengan Amazon ECS juga mengambil informasi tentang tag yang terkait dengannya. GuardDuty

26 November 2023

- Izin berikut telah ditambahkan sebagai bagian dari GuardDuty perluasan kemampuan [Runtime Monitoring](#):

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

[Memperbarui kebijakan AWS terkelola](#)

GuardDuty menambahkan izin baru, `organizations:ListAccounts` ke [AmazonGuardDutyFullAccessPolicy](#) dan [AmazonGuardDutyReadOnlyAccess](#).

16 November 2023

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

November 11, 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Melbourne) (ap-southeast-4).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

10 November 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut di Asia Pasifik (Hyderabad) (ap-south-2 ), Eropa (Zurich) (eu-central-2 ), dan Eropa (Spanyol) (eu-south-2) Wilayah.

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty merilis jenis temuan baru yang menggunakan EKS Audit Log Monitoring.](#)

8 November 2023

EKS Audit Log Monitoring sekarang mendukung jenis temuan berikut. Jenis temuan ini belum tersedia di Asia Pasifik (Hyderabad) (ap-south-2), Eropa (Zurich) (), Eropa (Spain) (eu-central-1-2) (eu-south-2), dan Asia Pasifik (Melbourne) ().

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated



- Discovery:Kubernetes/  
AnomalousBehavior.PermissionChecked

[EKSRuntime Monitoring  
merilis agen baru v1.3.1](#)

EKSRuntime Monitoring merilis agen baru versi 1.3.1 yang mencakup patch dan pembaruan keamanan penting.

23 Oktober 2023

[Atribut filter baru untuk menemukan](#)

GuardDuty telah menambahkan kriteria baru untuk menyaring temuan yang dihasilkan. DNSsahiran domain permintaan menyediakan domain tingkat kedua dan atas yang terlibat dalam aktivitas yang diminta GuardDuty untuk menghasilkan temuan.

17 Oktober 2023

[EKSRuntime Monitoring  
merilis agen baru v1.3.0 yang  
mendukung Kubernetes versi  
1.28](#)

EKSRuntime Monitoring merilis agen baru versi 1.3.0 yang mendukung Kubernetes versi 1.28. Menambahkan dukungan untuk Ubuntu. Untuk informasi selengkapnya, lihat [riwayat rilis agen EKS add-on](#).

5 Oktober 2023

[Menambahkan jenis temuan berbasis S3 dan AWS CloudTrail machine learning \(ML\) ke Wilayah Asia Pasifik \(Jakarta\) dan Timur Tengah \(UAE\)](#)

20 September 2023

S3 berikut dan CloudTrail temuan yang mengidentifikasi perilaku anomali menggunakan model pembelajaran mesin deteksi anomali (ML) sekarang tersedia di Wilayah Asia Pasifik (Jakarta) dan Timur Tengah (UAE): GuardDuty UAE

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)

- [Discovery:IAMUser/  
AnomalousBehavior](#)

[GuardDuty EKSRuntime  
Monitoring memperkenalkan  
agen GuardDuty keamanan  
pengelola di tingkat cluster](#)

EKSRuntime Monitoring menambahkan dukungan untuk mengelola agen GuardDuty keamanan untuk masing-masing EKS cluster untuk memantau peristiwa runtime hanya dari cluster selektif ini. EKSRuntime Monitoring memperluas kemampuan ini dengan dukungan tag.

13 September 2023

[GuardDuty Perlindungan  
Malware untuk EC2  
memperluas dukungan ke  
lebih Wilayah AWS](#)

Perlindungan Malware untuk sekarang EC2 tersedia di Asia Pasifik (Hyderabad), Asia Pasifik (Melbourne), Eropa (Zurich), dan Eropa (Spanyol).

11 September 2023

[GuardDuty sekarang tersedia di Israel \(Tel Aviv\) Region](#)

Menambahkan Wilayah Israel (Tel Aviv) ke daftar Wilayah AWS tempat sekarang GuardDuty tersedia. Rencana perlindungan berikut juga tersedia di Wilayah Israel (Tel Aviv):

24 Agustus 2023

- [EKSPerindungan](#) mencakup Pemantauan Log EKS Audit dan Pemantauan EKS Runtime.
- [Perlindungan Lambda](#).
- [Perlindungan Malware untuk EC2](#).
- [Perlindungan S3](#).

Untuk informasi lebih lanjut tentang ketersediaan rencana perlindungan di Wilayah Israel (Tel Aviv), lihat [Wilayah dan titik akhir](#).

[GuardDuty menambahkan konfigurasi aktifkan otomatis untuk organisasi Anda di tingkat rencana perlindungan](#)

Perbarui konfigurasi organisasi untuk paket perlindungan di Wilayah Anda. Opsi konfigurasi yang memungkinkan adalah mengaktifkan semua akun, mengaktifkan otomatis untuk akun baru, atau tidak mengaktifkan otomatis untuk akun apa pun di organisasi Anda.

16 Agustus 2023

[Jenis temuan S3 yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali \(ML\) sekarang tersedia di Asia Pasifik \(Osaka\)](#)

Jenis temuan berikut sekarang tersedia di Wilayah Asia Pasifik (Osaka):

10 Agustus 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[EKSRuntime Monitoring sekarang tersedia di Asia Pasifik \(Melbourne\)](#)

EKSRuntime Monitoring dalam GuardDuty EKS Protection menyediakan deteksi ancaman runtime untuk EKS kluster Amazon Anda di lingkungan. AWS Sekarang didukung di Wilayah Asia Pasifik (Melbourne).

8 Agustus 2023

[Memperbarui daftar GuardDuty temuan yang memanggil pemindaian malware GuardDuty yang dimulai](#)

Jenis pencarian EKS Runtime Monitoring tertentu sekarang dapat memanggil pemindaian malware GuardDuty yang dimulai di situs Anda. Akun AWS

Juli 19, 2023

[GuardDuty mendukung 10.000 akun anggota melalui AWS Organizations](#)

Akun GuardDuty administrator sekarang dapat mengelola maksimal 10.000 akun anggota melalui AWS Organizations. Ini juga termasuk maksimal 5000 akun anggota yang terkait dengan akun GuardDuty administrator melalui undangan.

29 Juni 2023

[EKSRuntime Monitoring mengumumkan tiga jenis temuan baru.](#)

EKSRuntime Monitoring mendukung tiga jenis temuan baru yang didasarkan pada teknik injeksi proses. Jenis temuan baru adalah: Runtime/DefenseEvasion, Proc, Runtime/.Ptrace, dan Runtime/.ProcessInjection, DefenseEvasion, ProcessInjection, DefenseEvasion, ProcessInjection, VirtualMemoryWrite.

22 Juni 2023

[EKSRuntime Monitoring merilis agen baru v1.2.0 yang mendukung Kubernetes versi 1.27](#)

EKSRuntime Monitoring merilis agen baru versi 1.2.0 yang juga mendukung instance ARM64 berbasis. Ditambahkan dukungan untuk Bottlerocket. Untuk informasi selengkapnya, lihat [riwayat rilis agen EKS add-on](#).

Juni 16, 2023

[GuardDuty konsol memberikan pandangan ringkasan dari temuan Anda.](#)

Dasbor ringkasan di GuardDuty konsol memberikan tampilan agregat GuardDuty temuan. Saat ini, dasbor menampilkan data melalui berbagai widget untuk 10.000 temuan terakhir yang dihasilkan untuk akun Anda (atau akun anggota jika Anda adalah akun GuardDuty administrator) untuk Wilayah saat ini.

12 Juni 2023

[EKSAudit Log Monitoring sekarang tersedia di Asia Pasifik \(Hyderabad\), Asia Pasifik \(Melbourne\), Eropa \(Zurich\), dan Eropa \(Spanyol\)](#)

Aktifkan Pemantauan Log EKS Audit (dalam EKS Perlindungan) untuk akun Anda untuk memantau log EKS audit dari EKS kluster Amazon Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.

1 Juni 2023

[EKSAudit Log Monitoring sekarang tersedia di Timur Tengah \(UAE\)](#)

EKSAudit Log Monitoring sekarang tersedia di Timur Tengah (UAE). Aktifkan Pemantauan Log EKS Audit untuk akun Anda untuk memantau log EKS audit dari EKS kluster Amazon Anda dan menganalisisnya untuk aktivitas yang berpotensi berbahaya dan mencurigakan.

3 Mei 2023

[GuardDuty Perlindungan Malware untuk EC2 mengumumkan pemindaian malware sesuai permintaan](#)

27 April 2023

Perlindungan Malware untuk EC2 membantu Anda mendeteksi potensi keberadaan malware dalam EBS volume Amazon yang dilampirkan ke EC2 instans Amazon dan beban kerja kontainer Anda. Sekarang menawarkan dua jenis pemindaian — GuardDuty dimulai dan sesuai permintaan. GuardDuty Pemindaian malware yang dimulai memulai pemindaian tanpa agen di EBS volume Amazon secara otomatis hanya ketika GuardDuty menghasilkan salah satu [Temuan yang memanggil pemindaian malware yang dimulai](#). GuardDuty Anda dapat memulai pemindaian malware sesuai permintaan untuk EC2 instans Amazon di akun Anda dengan memberikan Nama Sumber Daya Amazon (ARN) yang terkait dengan instans Amazon tersebut. Untuk informasi selengkapnya tentang perbedaan kedua jenis pemindaian, lihat [Perlindungan Malware untuk EC2](#).

- [GuardDuty-pemindaian malware yang dimulai](#)



---

|   |  |               |
|---|--|---------------|
| <a href="#">GuardDuty mengumumkan Perlindungan Lambda</a>                       | <ul style="list-style-type: none"><li>• <a href="#">Pemindaian malware sesuai permintaan</a></li></ul> <p>Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan dalam fungsi Anda AWS Lambda .</p> <ul style="list-style-type: none"><li>• <a href="#">Tipe temuan Lambda Protection</a></li><li>• <a href="#">Memperbaiki fungsi Lambda yang berpotensi dikompromikan</a></li></ul> | 20 April 2023 |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Asia Pasifik (Melbourne)</a> | <p>Menambahkan Asia Pasifik (Melbourne) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi tentang fitur yang tersedia di Wilayah ini, lihat <a href="#">Wilayah dan titik akhir</a>.</p>  | 19 April 2023 |

### [GuardDuty menambahkan 3 jenis EC2 temuan baru](#)

GuardDuty memperkenalkan jenis temuan baru untuk mendeteksi penggunaan DNS resolver eksternal dan teknologi terenkripsi. DNS Untuk informasi tentang Wilayah AWS di mana jenis temuan ini didukung, lihat [Wilayah dan titik akhir](#).

5 April 2023

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

[GuardDuty mengumumkan EKS Runtime Monitoring dalam Perlindungan EKS](#)

EKS Runtime Monitoring dalam EKS Protection menyediakan an deteksi ancaman runtime untuk EKS klaster Amazon Anda di lingkungan. AWS Ini menggunakan agen EKS add-on Amazon (aws-guardduty-agent ) yang mengumpulkan [peristiwa Runtime](#) dari beban kerja Anda. EKS Setelah GuardDuty menerima peristiwa runtime ini, ia memantau dan menganalisisnya untuk mengidentifikasi potensi ancaman keamanan yang mencurigakan. Untuk informasi selengkapnya, lihat [Menemukan detail](#) dan [jenis pencarian EKS Runtime Monitoring](#).

30 Maret 2023

## [GuardDuty menambahkan fungsionalitas baru - autoEnableOrganizationMembers](#)

Maret 23, 2023

Amazon GuardDuty menambahkan opsi konfigurasi organisasi baru yang membantu akun GuardDuty administrator mengaudit dan menegakkan (jika diperlukan) yang GuardDuty diaktifkan untuk ALL anggota organisasi mereka. Praktik terbaik sekarang adalah menggunakan `autoEnableOrganizationMembers` alih-alih `autoEnable`. `autoEnable` sudah usang tetapi masih didukung. Berikut ini APIs dipengaruhi oleh fungsionalitas baru ini:

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[Fitur RDS Perlindungan di Amazon sekarang GuardDuty tersedia secara umum](#)

GuardDuty RDSProtection memantau dan memprofilkan aktivitas RDS login untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Untuk informasi tentang yang Wilayah AWS mendukung RDS Perlindungan, lihat [Wilayah dan titik akhir](#).

16 Maret 2023

[GuardDuty mengumumkan aktivasi fitur](#)

Secara historis, konfigurasi yang GuardDuty API diizinkan dari fitur dan sumber data, tetapi sekarang, semua jenis GuardDuty perlindungan baru akan dikonfigurasi sebagai fitur dan bukan sebagai sumber data. GuardDuty masih mendukung sumber data melalui API tetapi tidak akan menambahkan yang baru API. Aktivasi fitur mempengaruhi perilaku yang APIs digunakan untuk mengaktifkan GuardDuty atau jenis perlindungan di dalamnya GuardDuty. Jika Anda mengelola GuardDuty akun Anda melalui API, SDK, atau CFN templat, lihat [GuardDuty API perubahan pada Maret 2023](#).

16 Maret 2023

[GuardDuty Perlindungan Malware untuk sekarang EC2 tersedia di Wilayah Timur Tengah \(UAE\)](#)

Perlindungan Malware untuk EC2 fitur di GuardDuty didukung di Wilayah Timur Tengah (UAE). Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

13 Maret 2023

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(\) SLR](#)

GuardDuty menambahkan izin baru berikut untuk mendukung fitur GuardDuty EKS Runtime Monitoring yang akan datang.

8 Maret 2023

- Gunakan EKS tindakan Amazon untuk mengelola dan mengambil informasi tentang EKS kluster, dan mengelola EKS add-on pada kluster. EKS EKSTindakan juga mengambil informasi tentang tag yang terkait dengan GuardDuty.

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty telah memperbarui peran terkait Layanan \(\) SLR](#)

GuardDuty SLRTelah diperbarui untuk memungkinkan pembuatan Perlindungan Malware EC2 SLR setelah Perlindungan Malware untuk EC2 diaktifkan.

21 Februari 2023

|  |   |                   |
|--|---|-------------------|
| <a href="#">GuardDuty membutuhkan TLS v1.2 atau yang lebih baru</a>                  | Untuk berkomunikasi dengan AWS sumber daya, GuardDuty membutuhkan dan mendukung TLS v1.2 atau yang lebih baru. Untuk informasi selengkapnya, lihat <a href="#">Perlindungan data</a> dan <a href="#">Keamanan infrastruktur</a> . | 14 Februari 2023  |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Asia Pasifik (Hyderabad)</a>      | Menambahkan Wilayah Asia Pasifik (Hyderabad) ke daftar Wilayah AWS tempat GuardDuty tersedia. Untuk informasi selengkapnya, lihat <a href="#">Wilayah dan titik akhir</a> .   | 14 Februari 2023  |
| <a href="#">Panduan GuardDuty Pengguna Amazon selaras dengan praktik IAM terbaik</a> | Panduan yang diperbarui untuk menyelaraskan dengan praktik IAM terbaik. Untuk informasi selengkapnya, lihat <a href="#">Praktik terbaik keamanan di IAM</a> .   | Februari 10, 2023 |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Eropa (Spanyol)</a>               | Menambahkan Eropa (Spanyol) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat <a href="#">Wilayah dan titik akhir</a> .   | Februari 8, 2023  |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Eropa (Zurich)</a>                | Menambahkan Eropa (Zurich) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat <a href="#">Wilayah dan titik akhir</a> .  | 12 Desember 2022  |

[Pratinjau rilis fitur baru -  
GuardDuty RDS Perlindungan](#)

GuardDuty RDSProtection memantau dan memprofilkan aktivitas RDS login untuk mengidentifikasi perilaku login yang mencurigakan pada instans database Amazon Aurora Anda. Saat ini, tersedia untuk rilis pratinjau dalam lima Wilayah AWS. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

30 November 2022

[GuardDuty sekarang tersedia  
di Wilayah Timur Tengah  
\(UAE\)](#)

Ditambahkan Timur Tengah (UAE) ke daftar Wilayah AWS di mana GuardDuty tersedia. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#).

6 Oktober 2022



[Menambahkan konten untuk fitur baru - Perlindungan GuardDuty Malware untuk EC2](#)

26 Juli 2022

GuardDuty Perlindungan Malware for EC2 adalah peningkatan opsional untuk Amazon GuardDuty . Sementara GuardDuty mengidentifikasi sumber daya yang berisiko, Perlindungan Malware untuk EC2 mendeteksi malware yang mungkin menjadi sumber kompromi. Dengan Perlindungan Malware untuk EC2 diaktifkan, setiap kali GuardDuty mendeteksi perilaku mencurigakan pada EC2 instans Amazon atau beban kerja kontainer yang menunjukkan GuardDuty malware, Perlindungan Malware untuk EC2 memulai pemindaian tanpa agen pada EBS volume yang dilampirkan pada EC2 instans yang terkena dampak atau beban kerja kontainer untuk mendeteksi keberadaan malware. Untuk informasi tentang cara EC2 kerja Perlindungan Malware dan mengonfigurasi fitur ini, lihat [Perlindungan GuardDuty Malware untuk EC2](#).

- Untuk informasi tentang Perlindungan Malware

untuk EC2 temuan, lihat [Menemukan detail](#).

- Untuk informasi tentang memulihkan EC2 instans yang dikompromikan dan wadah mandiri, lihat [Memperbaiki masalah keamanan yang ditemukan](#) oleh GuardDuty
- Untuk informasi tentang mengaudit CloudWatch log untuk pemindaian malware dan alasan melewatkan sumber daya selama pemindaian malware, lihat [Memahami CloudWatch Log dan](#) lewati alasannya.
- Untuk informasi tentang deteksi ancaman positif palsu, lihat [Melaporkan positif palsu di Perlindungan GuardDuty Malware](#) untuk EC2

[Pensiunan satu jenis temuan](#)

[Exfiltration:S3/ObjectRead.](#)  
[Unusual](#)telah pensiun.

Juli 5, 2022

[Menambahkan jenis temuan S3 baru yang mengidentifikasi perilaku anomali menggunakan GuardDuty model pembelajaran mesin deteksi anomali \(ML\).](#)

Menambahkan jenis temuan S3 baru berikut. Jenis temuan ini mengidentifikasi jika API permintaan memanggil IAM entitas dengan cara yang anomali. Model ML mengevaluasi semua API permintaan di akun Anda dan mengidentifikasi peristiwa anomali yang terkait dengan teknik yang digunakan oleh musuh. Untuk mempelajari lebih lanjut tentang masing-masing temuan baru ini, lihat [tipe temuan S3](#).

Juli 5, 2022

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Ditambahkan konten GuardDuty EKS Perlindungan untuk GuardDuty](#)

GuardDuty sekarang dapat menghasilkan temuan untuk EKS sumber daya Amazon Anda melalui pemantauan log EKS audit. Untuk mempelajari cara mengonfigurasi fitur ini, lihat [EKSPerlindungan di Amazon GuardDuty](#). Untuk daftar temuan yang GuardDuty dapat dihasilkan untuk EKS sumber daya Amazon, lihat temuan [Kubernetes](#). Panduan remediasi baru telah ditambahkan untuk mendukung remediasi temuan ini dalam panduan remediasi temuan [Kubernetes](#).

Januari 25, 2022

[Ditambahkan 1 temuan baru](#)

Temuan baru UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS telah ditambahkan. Temuan ini memberi tahu Anda kapan kredensi instans Anda diakses oleh AWS akun di luar lingkungan Anda. AWS

20 Januari 2022

[Memperbarui jenis temuan untuk membantu mengidentifikasi masalah yang terkait dengan log4j](#)

Amazon GuardDuty telah memperbarui jenis temuan berikut untuk membantu mengidentifikasi dan memprioritaskan masalah yang terkait dengan CVE-2021-44228 dan CVE-2021-45046: Backdoor: /C & .B; Backdoor: /C & .B! EC2 CActivity EC2 CActivity DNS; Perilaku:EC2/NetworkPortUnusual.

Desember 22, 2021

[Menemukan Perubahan](#)

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration telah diubah menjadi UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Versi temuan yang disempurnakan ini mempelajari lokasi khas yang digunakan kredensial Anda untuk mengurangi temuan dari lalu lintas yang diarahkan melalui jaringan premis.

[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 September 2021

[Perbarui ke GuardDuty SLR](#)

GuardDuty SLR telah diperbarui dengan tindakan baru untuk meningkatkan akurasi penemuan.

Agustus 3, 2021

---

|  |   |               |
|--|---|---------------|
| <a href="#">Menambahkan informasi sumber data untuk setiap jenis temuan.</a> | Menemukan deskripsi sekarang berisi informasi tentang sumber data yang GuardDuty digunakan untuk menghasilkan temuan itu.   | 10 Mei 2021   |
| <a href="#">Pensiunan 13 jenis pencarian.</a>                                | 13 temuan telah pensiun untuk diganti dengan Anomalous Behavoir temuan baru.<br><a href="#">Persistence:IAMUser/NetworkPermissions</a> , <a href="#">Persistence:IAMUser/ResourcePermissions</a> , <a href="#">Persistence:IAMUser/UserPermissions</a> , <a href="#">PrivilegeEscalation:IAMUser/AdministrativePermissions</a> , <a href="#">Recon:IAMUser/NetworkPermissions</a> , <a href="#">Recon:IAMUser/ResourcePermissions</a> , <a href="#">Recon:IAMUser/UserPermissions</a> , <a href="#">ResourceConsumption:IAMUser/ComputeResources</a> , <a href="#">Stealth:IAMUser/LoggingConfigurationModified</a> , <a href="#">Discovery:S3/BucketEnumeration.Unusual</a> , <a href="#">Impact:S3/ObjectDelete.Unusual</a> , <a href="#">Impact:S3/PermissionsModification.Unusual</a> . | 12 Maret 2021 |

[Menambahkan 8 jenis temuan baru untuk perilaku anomali.](#)

Menambahkan 8 jenis IAMUser temuan baru berdasarkan perilaku anomali untuk IAM kepala sekolah. [CredentialAccess:IAMUser/AnomalousBehavior](#), [DefenseEvasion:IAMUser/AnomalousBehavior](#), [Discovery:IAMUser/AnomalousBehavior](#), [Exfiltration:IAMUser/AnomalousBehavior](#), [Impact:IAMUser/AnomalousBehavior](#), [InitialAccess:IAMUser/AnomalousBehavior](#), [Persistence:IAMUser/AnomalousBehavior](#), [PrivilegeEscalation:IAMUser/AnomalousBehavior](#).

12 Maret 2021

[Menambahkan EC2 temuan berdasarkan reputasi domain.](#)

Menambahkan 4 tipe temuan Impact yang baru berdasarkan reputasi domain. [Impact:EC2/AbusedDomainRequest.Reputation](#), [Impact:EC2/BitcoinDomainRequest.Reputation](#), [Impact:EC2/MaliciousDomainRequest.Reputation](#). Juga menambahkan EC2 temuan baru untuk C & CActivity. [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

27 Januari 2021

|  |  |                   |
|--|--|-------------------|
| <a href="#">Ditambahkan 4 jenis temuan baru.</a>   | Menambahkan 3 aliciousIP Caller temuan S3 M baru. <a href="#">Discovery:S3/MaliciousIP Caller</a> , <a href="#">Exfiltration:S3/MaliciousIP Caller</a> , <a href="#">Impact:S3/MaliciousIP Caller</a> . Juga menambahkan EC2 temuan baru untuk C & CActivity. <a href="#">Backdoor:EC2/C&amp;CActivity.B</a> | 21 Desember 2020  |
| <a href="#">Pensiun tipe UnauthorizedAccess:EC2/TorIPCaller temuan.</a>                      | Jenis UnauthorizedAccess:EC2/TorIPCaller temuan sekarang sudah pensiun dari GuardDuty. <a href="#">Pelajari selengkapnya</a> .   | 1 Oktober 2020    |
| <a href="#">Menambahkan jenis Impact:EC2/WinRmBruteForce temuan.</a>                         | Menambahkan temuan Dampak baru, Impact:EC2/WinRmBruteForce. <a href="#">Pelajari selengkapnya</a> .  | 17 September 2020 |
| <a href="#">Menambahkan jenis Impact:EC2/PortSweep temuan.</a>                               | Menambahkan temuan Dampak baru, Impact:EC2/PortSweep. <a href="#">Pelajari selengkapnya</a> .  | 17 September 2020 |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Afrika (Cape Town) dan Eropa (Milan).</a> | Menambahkan Afrika (Cape Town) dan Eropa (Milan) ke daftar AWS Wilayah di mana GuardDuty tersedia. <a href="#">Pelajari selengkapnya</a>   | 31 Juli 2020      |



[Menambahkan detail penggunaan baru untuk memantau GuardDuty biaya.](#)

Sekarang Anda dapat menggunakan metrik baru untuk menanyakan data biaya GuardDuty penggunaan untuk akun dan akun yang Anda kelola. Gambaran umum baru tentang biaya penggunaan tersedia di konsol di <https://console.aws.amazon.com/guardduty/>. Informasi lebih rinci dapat diakses melalui API.

31 Juli 2020

[Menambahkan konten yang mencakup perlindungan S3 melalui pemantauan peristiwa data S3 di GuardDuty](#)

GuardDuty S3 Protection sekarang tersedia melalui pemantauan peristiwa pesawat data S3 sebagai sumber data baru. Akun baru akan mengaktifkan fitur ini secara otomatis. Jika Anda sudah menggunakan GuardDuty, Anda dapat mengaktifkan sumber data baru untuk diri sendiri atau akun anggota Anda.

31 Juli 2020

[Menambahkan 14 Temuan S3 baru.](#)

14 tipe temuan S3 yang baru telah ditambahkan untuk bidang kendali S3 dan sumber bidang data.

31 Juli 2020

[Menambahkan dukungan tambahan untuk temuan S3 dan mengubah 2 nama tipe temuan yang ada.](#)

GuardDuty temuan sekarang mencakup rincian lebih lanjut untuk temuan yang melibatkan ember S3. Jenis temuan yang ada yang terkait dengan aktivitas S3 telah diganti namanya: Policy:IAMUser/S3BlockPublicAccessDisabled telah diubah menjadi Policy:S3/BucketBlockPublicAccessDisabled Stealth:IAMUser/S3ServerAccessLoggingDisabled telah diubah menjadi Stealth:S3/ServerAccessLoggingDisabled

28 Mei 2020

[Menambahkan konten untuk AWS Organizations integrasi.](#)

GuardDuty sekarang terintegrasi dengan administrator AWS Organizations yang didelegasikan untuk memungkinkan Anda mengelola GuardDuty akun dalam organisasi Anda. Ketika Anda menetapkan administrator yang didelegasikan sebagai akun GuardDuty administrator, Anda dapat secara otomatis mengaktifkan GuardDuty anggota organisasi mana pun yang akan dikelola oleh akun administrator yang didelegasikan. Anda juga dapat mengaktifkan secara otomatis GuardDuty di akun AWS Organizations anggota baru. [Pelajari selengkapnya.](#)

20 April 2020

|   |   |                  |
|---|---|------------------|
| <a href="#">Menambahkan konten untuk fitur temuan ekspor.</a>                           | Menambahkan konten yang menjelaskan fitur Temuan Ekspor dari GuardDuty.   | 14 November 2019 |
| <a href="#">Menambahkan jenis UnauthorizedAccess:EC2/MetadataDNSRebind temuan.</a>      | Menambahkan temuan Tidak Sah baru, UnauthorizedAccess:EC2/MetadataDNSRebind. <a href="#">Pelajari selengkapnya.</a>   | 10 Oktober 2019  |
| <a href="#">Menambahkan jenis Stealth:IAMUser/S3ServerAccessLoggingDisabled temuan.</a> | Menambahkan temuan Stealth baru, Stealth:IAMUser/S3ServerAccessLoggingDisabled. <a href="#">Pelajari selengkapnya.</a>  | 10 Oktober 2019  |
| <a href="#">Menambahkan jenis Policy:IAMUser/S3BlockPublicAccessDisabled temuan.</a>    | Menambahkan temuan Kebijakan baru, Policy:IAMUser/S3BlockPublicAccessDisabled. <a href="#">Pelajari selengkapnya.</a>   | 10 Oktober 2019  |
| <a href="#">Pensiun tipe Backdoor:EC2/XORDDOS temuan.</a>                               | Jenis Backdoor:EC2/XORDDOS temuan sekarang sudah pensiun dari GuardDuty. <a href="#">Pelajari lebih lanjut</a>  | 12 Juni 2019     |
| <a href="#">Menambahkan jenis PrivilegeEscalation temuan.</a>                           | Jenis PrivilegeEscalation temuan mendeteksi ketika pengguna mencoba untuk menetapkan hak istimewa yang meningkat dan lebih permisif ke akun mereka. <a href="#">Pelajari selengkapnya</a> | 14 Mei 2019      |
| <a href="#">GuardDuty sekarang tersedia di Wilayah Eropa (Stockholm).</a>               | Menambahkan Europe (Stockholm) ke daftar AWS Wilayah di mana GuardDuty tersedia. <a href="#">Pelajari selengkapnya</a>  | 9 Mei 2019       |

[Menambahkan jenis temuan baru, Recon:EC2/PortProbeEMRUnprotectedPort.](#)

Temuan ini memberi tahu Anda bahwa port sensitif EMR terkait pada EC2 Instance tidak diblokir dan sedang diselidiki secara aktif. [Pelajari selengkapnya](#)

8 Mei 2019

[Menambahkan 5 jenis temuan baru yang mendeteksi jika EC2 instans Anda berpotensi digunakan untuk serangan denial of service \(DoS\).](#)

Temuan ini memberi tahu Anda tentang EC2 kejadian di lingkungan Anda yang berperilaku dengan cara yang mungkin menunjukkan bahwa mereka digunakan untuk melakukan serangan Denial of Service (DoS). [Pelajari selengkapnya](#)

8 Maret 2019

[Menambahkan jenis temuan baru: Policy:IAMUser/RootCredentialUsage](#)

Policy:IAMUser/RootCredentialUsage jenis pencarian memberi tahu Anda bahwa kredensial masuk pengguna root Anda Akun AWS sedang digunakan untuk membuat permintaan terprogram ke layanan. AWS [Pelajari selengkapnya](#)

24 Januari 2019

[UnauthorizedAccess:IAMUser/UnusualASNCaller tipe temuan telah pensiun](#)

Jenis UnauthorizedAccess :IAMUser/UnusualASNCaller temuan telah pensiun. Anda sekarang akan diberi tahu tentang aktivitas yang dipanggil dari jaringan yang tidak biasa melalui jenis GuardDuty temuan aktif lainnya. Jenis temuan yang dihasilkan akan didasarkan pada kategori API yang dipanggil dari jaringan yang tidak biasa. [Pelajari selengkapnya](#)

21 Desember 2018

[Menambahkan dua jenis temuan baru: PenTest:IAMUser/ParrotLinux dan PenTest:IAMUser/PentooLinux](#)

PenTest:IAMUser/ParrotLinux jenis pencarian memberi tahu Anda bahwa komputer yang menjalankan Parrot Security Linux melakukan API panggilan menggunakan kredensial milik akun Anda. AWS PenTest:IAMUser/PentooLinux jenis pencarian memberi tahu Anda bahwa mesin yang menjalankan Pentoo Linux melakukan API panggilan menggunakan kredensial milik akun Anda. AWS [Pelajari selengkapnya](#)

21 Desember 2018

[Menambahkan dukungan untuk topik GuardDuty pengumuman SNS Amazon](#)

Anda sekarang dapat berlangganan SNS topik GuardDuty pengumuman untuk menerima pemberitahuan tentang jenis temuan yang baru dirilis, pembaruan untuk jenis temuan yang ada, dan perubahan fungsionalitas lainnya. Pemberitahuan tersedia dalam semua format yang SNS didukung Amazon. [Pelajari selengkapnya](#)

21 November 2018

[Menambahkan dua jenis temuan baru: UnauthorizedAccess:EC2/TorClient dan UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClient jenis pencarian memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke Tor Guard atau node Authority. UnauthorizedAccess:EC2/TorRelay jenis pencarian memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda membuat koneksi ke jaringan Tor dengan cara yang menunjukkan bahwa itu bertindak sebagai relai Tor. [Pelajari selengkapnya](#)

16 November 2018

[Menambahkan jenis temuan baru: Cryptocurrency:EC2/BitcoinTool.B](#)

Temuan ini memberi tahu Anda bahwa sebuah EC2 instance di AWS lingkungan Anda menanyakan nama domain yang terkait dengan Bitcoin, atau aktivitas terkait cryptocurrency lainnya. [Pelajari selengkapnya](#)

9 November 2018

[Menambahkan dukungan untuk memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara](#)

Anda sekarang dapat memperbarui frekuensi pemberitahuan yang dikirim ke CloudWatch Acara untuk kejadian berikutnya dari temuan yang ada. Nilai yang mungkin adalah 15 menit, 1 jam, atau default 6 jam. [Pelajari selengkapnya](#)

9 Oktober 2018

[Ditambahkan dukungan Wilayah](#)

Menambahkan dukungan Wilayah untuk AWS GovCloud (AS-Barat) [Pelajari lebih lanjut](#)

25 Juli 2018

[Ditambahkan dukungan untuk AWS CloudFormation StackSets di GuardDuty](#)

Anda dapat menggunakan GuardDuty template Aktifkan Amazon untuk mengaktifkan GuardDuty secara bersamaan di beberapa akun. [Pelajari selengkapnya](#)

25 Juni 2018

[Menambahkan dukungan untuk aturan GuardDuty arsip otomatis](#)

Pelanggan kini dapat membuat aturan pengarsipan otomatis granular untuk penekanan temuan. Untuk temuan yang cocok dengan aturan arsip otomatis, tandai GuardDuty secara otomatis sebagai diarsipkan. Hal ini memungkinkan pelanggan untuk lebih menyesuaikan GuardDuty untuk menyimpan hanya temuan yang relevan dalam tabel temuan saat ini. [Pelajari selengkapnya](#)

4 Mei 2018

[GuardDuty tersedia di Wilayah Eropa \(Paris\)](#)

GuardDuty sekarang tersedia di Eropa (Paris), memungkinkan Anda untuk memperluas pemantauan keamanan berkelanjutan dan deteksi ancaman di Wilayah ini. [Pelajari selengkapnya](#)

29 Maret 2018

[Membuat akun GuardDuty administrator dan akun anggota AWS CloudFormation sekarang didukung.](#)

Untuk informasi selengkapnya, silakan lihat [AWS::GuardDuty::master](#) dan [AWS::GuardDuty::member](#).

6 Maret 2018

[Menambahkan sembilan deteksi anomali CloudTrail berbasis baru.](#)

Jenis temuan baru ini diaktifkan secara otomatis GuardDuty di semua Wilayah yang didukung. [Pelajari selengkapnya](#)

28 Februari 2018



[Menambahkan tiga deteksi intelijen ancaman baru \(tipe pencarian\).](#)

Jenis temuan baru ini diaktifkan secara otomatis GuardDuty di semua Wilayah yang didukung. [Pelajari lebih lanjut](#)

5 Februari 2018

[Batasi kenaikan untuk akun GuardDuty anggota.](#)

Dengan rilis ini, Anda dapat memiliki hingga 1000 akun GuardDuty anggota ditambahkan per AWS akun (akun akun GuardDuty administrator). [Pelajari selengkapnya](#)

25 Januari 2018

[Perubahan dalam unggahan dan pengelolaan lebih lanjut dari daftar IP tepercaya dan daftar ancaman untuk akun GuardDuty administrator dan akun anggota.](#)

Dengan rilis ini, Pengguna dari akun GuardDuty akun administrator dapat mengunggah dan mengelola daftar IP tepercaya dan daftar ancaman. Pengguna dari GuardDuty akun anggota tidak dapat mengunggah dan mengelola daftar. Daftar IP tepercaya dan daftar ancaman yang diunggah oleh akun akun administrator dikenakan pada GuardDuty fungsionalitas di akun anggotanya. [Pelajari selengkapnya](#)

25 Januari 2018

## Pembaruan sebelumnya

| Perubahan      | Deskripsi   | Tanggal          |
|----------------|---|------------------|
| Publikasi awal | Publikasi awal Panduan GuardDuty Pengguna Amazon. | 28 November 2017 |

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.