aws

用户指南

AWS Secrets Manager

AWS Secrets Manager: 用户指南

Table of Contents

什么是 AWS Secrets Manager？

AWS Secrets Manager 帮助您在数据库凭证、应用程序凭证、OAuth 令牌、API 密钥和其他密钥的整个生命周期中对其进行管理、检索和轮换。许多 AWS 服务在 Secrets Manager 中存储和使用密钥。

Secrets Manager 无需应用程序源代码中的硬编码凭证，因此可帮助您改进安全状况。将凭证存储在 Secrets Manager 中有助于避免检查您应用程序或组件的任何人泄露这些凭证。您可以将硬编码凭证替换为对 Secrets Manager 服务的运行时系统调用，以便在需要时动态检索凭证。

使用 Secrets Manager，您可以为密钥配置自动轮换计划。这样，您就可以将长期密钥替换为短期密钥，从而显著降低泄露风险。由于凭证不再与应用程序存储在一起，所以轮换凭证不再需要更新应用程序并将更改部署到应用程序客户端。

对于您的组织可能拥有的其他类型的密钥：

- AWS 凭证 — 我们推荐AWS Identity and Access Management。
- 加密密钥 – 建议使用 AWS Key Management Service。
- SSH 密钥 – 建议使用 Amazon EC2 Instance Connect。
- 私有密钥和证书 – 建议使用 AWS Certificate Manager。

Secrets Manager 入门

如果你不熟悉 Secrets Manager，请从以下教程之一开始：

- the section called “替换硬编码的密钥 ”
- the section called “替换硬编码的数据库凭证 ”
- the section called “交替用户轮换”
- the section called “单用户轮换”

可使用密钥执行的其他任务：

- 创建和管理密钥
- 控制对密钥的访问
- 获取秘密
- 轮换 密钥

- 监控密钥
- 监控密钥的合规性
- 在中创建密钥 AWS CloudFormation

符合标准

AWS Secrets Manager 已经过多项标准的审计，当您需要获得合规性认证时，可以成为您的解决方案的一部分。有关更多信息，请参阅 合规性验证。

定价

使用 Secrets Manager 时，仅按实际使用量收费，无最低费用或设置费用。标记为已删除的密钥不收取任何费用。有关当前完整定价列表，请参阅 AWS Secrets Manager 定价。要监控您的成本，请参阅the section called “监控 Secrets Manager 成本”。

你可以使用 Secrets Manager 创建的来免费加密你的秘密。 AWS 托管式密钥 `aws/secretsmanager`如果您创建自己的 KMS 密钥来加密您的机密，则按当前费 AWS KMS 率向您 AWS 收费。有关更多信息，请参阅AWS Key Management Service 定价。

当您开启自动轮换（托管轮换除外）时，Secrets Manager 会使用 AWS Lambda 函数来轮换密钥，并按当前 Lambda 费率向您收取轮换功能的费用。有关更多信息，请参阅AWS Lambda 定价。

如果您 AWS CloudTrail 在自己的账户上启用，则可以获取 Secrets Manager 发送的 API 调用的日志。Secrets Manager 将所有事件记录为管理事件。 AWS CloudTrail 免费存储所有管理事件的第一份副本。但是，如果启用通知，可能会对 Amazon S3 的日志存储和 Amazon SNS 产生费用。此外，如果您设置了其他跟踪，管理事件的其他副本可能会产生费用。有关更多信息，请参阅AWS CloudTrail 定价。

访问权限 AWS Secrets Manager

您可以通过以下任何方式使用 Secrets Manager：

- Secrets Manager 控制台
- 命令行工具
- AWS 软件开发工具包
- HTTPS 查询 API
- AWS Secrets Manager 端点

Secrets Manager 控制台

您可以使用基于浏览器的 Secrets Manager 控制台管理密钥，并可使用该控制台执行与密钥相关的几乎所有任务。

命令行工具

AWS 命令行工具允许您在系统命令行中发出命令以执行 Secrets Manager 和其他 AWS 任务。与使用控制台相比，此方法更快、更方便。如果要生成脚本来执行 AWS 任务，则命令行工具可能很有用。

当您在命令 shell 中输入命令时，存在访问命令历史记录或实用程序可以访问您命令参数的风险。请参阅 the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

命令行工具会自动使用 AWS 区域中服务的默认终端节点。您可以为 API 请求指定其他端点。请参阅 the section called “Secrets Manager 端点”。

AWS 提供了两组命令行工具：

- AWS Command Line Interface (AWS CLI)
- AWS Tools for Windows PowerShell

AWS 软件开发工具包

S AWS DK 由适用于各种编程语言和平台的库和示例代码组成。开发工具包包括多个任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求。要下载并安装任何开发工具包，请参阅适用于 Amazon Web Services 的工具。

AWS 软件开发工具包会自动使用 AWS 区域中服务的默认终端节点。您可以为 API 请求指定其他端点。请参阅 the section called “Secrets Manager 端点”。

要获得开发工具包文档，请参阅：

- C++
- Go
- Java
- JavaScript
- 科特林
- .NET
- PHP
- Python (Boto3)
- Ruby
- Rust
- SAP ABAP
- Swift

HTTPS 查询 API

HTTPS 查询 API 允许你以编程方式访问 Secrets Manager 和 AWS。HTTPS 查询 API 允许您直接向服务发出 HTTPS 请求。

虽然您可以直接调用 Secrets Manager HTTPS 查询 API，但我们建议您使用开发工具包之一作为代替。开发工具包可以执行许多您必须手动执行的有用任务。例如，开发工具包可以自动对请求进行签名，并将响应转换为在语法上适合您的语言的结构。

要对 Secrets Manager 进行 HTTPS 调用，您需要连接到 ???。

AWS Secrets Manager 端点

要以编程方式连接到 Secrets Manager，您可以使用端点，即服务入口点的 URL。Secrets Manager 端点是双堆栈端点，这意味着它们同时支持 IPv4 和 IPv6。

Secrets Manager 在某些区域提供支持美国联邦信息处理标准 (FIPS) 140-2 的端点。

Secrets Manager 支持 TLS 1.2 和 1.3。Secrets Manager 在除中国区域之外的所有区域都支持 PQTLS。

> **Note**
>
> Python AWS SDK 以及按顺序调用 IPv6 和 IPv4 的 AWS CLI 尝试，因此，如果你没有启用 IPv6，则可能需要一段时间才能调用超时并使用 IPv4 重试。若要解决此问题，您可以完全禁用 IPv6 或迁移到 IPv6。

以下是 Secrets Manager 的服务端点。请注意，命名与典型的双堆栈命名约定不同。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	secretsmanager.us-east-2.amazonaws.com secretsmanager-fips.us-east-2.amazonaws.com	HTTPS HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	secretsmanager.us-east-1.amazonaws.com secretsmanager-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国西部（加利福尼亚北部）	us-west-1	secretsmanager.us-west-1.amazonaws.com secretsmanager-fips.us-west-1.amazonaws.com	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	secretsmanager.us-west-2.amazonaws.com secretsmanager-fips.us-west-2.amazonaws.com	HTTPS HTTPS
非洲（开普敦）	af-south-1	secretsmanager.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	secretsmanager.ap-east-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（海得拉巴）	ap-south-2	secretsmanager.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	secretsmanager.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	secretsmanager.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	secretsmanager.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	secretsmanager.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	secretsmanager.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	secretsmanager.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	secretsmanager.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	secretsmanager.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	secretsmanager.ca-central-1.amazonaws.com secretsmanager-fips.ca-central-1.amazonaws.com	HTTPS HTTPS

区域名称	区域	端点	协议
加拿大西部（卡尔加里）	ca-west-1	secretsmanager.ca-west-1.amazonaws.com	HTTPS
		secretsmanager-fips.ca-west-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	secretsmanager.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	secretsmanager.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	secretsmanager.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	secretsmanager.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	secretsmanager.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	secretsmanager.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	secretsmanager.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	secretsmanager.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	secretsmanager.il-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
中东（巴林）	me-south-1	secretsmanager.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	secretsmanager.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	secretsmanager.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	secretsmanager.us-gov-east-1.amazonaws.com secretsmanager-fips.us-gov-east-1.amazonaws.com	HTTPS HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	secretsmanager.us-gov-west-1.amazonaws.com secretsmanager-fips.us-gov-west-1.amazonaws.com	HTTPS HTTPS

Secrets Manager 的密钥里有什么？

在 Secrets Manager 中，密钥由密钥信息、密钥值和密钥元数据组成。密钥值可以是字符串或二进制值。

要在一个密钥中存储多个字符串值，我们建议您使用带有键值对的 JSON 文本字符串，例如：

```
{
  "host"       : "ProdServer-01.databases.example.com",
  "port"       : "8888",
  "username"   : "administrator",
  "password"   : "EXAMPLE-PASSWORD",
  "dbname"     : "MyDatabase",
  "engine"     : "mysql"
}
```

对于数据库密钥，如果要启用自动轮换，则该密钥必须以正确的 JSON 结构包含数据库的连接信息。有关更多信息，请参阅 the section called “密钥的 JSON 结构”。

Metadata

密钥元数据包括：

- 具有以下格式的 Amazon Resource Name (ARN)。

  ```
  arn:aws:secretsmanager:<Region>:<AccountId>:secret:SecretName-6RandomCharacters
  ```

  Secrets Manager 会在密钥名称末尾添加六个随机字符，以帮助确保密钥 ARN 的唯一性。如果删除了原始密钥，然后使用相同的名称创建了新密钥，则由于这些字符的原因，这两个密钥具有不同的 ARN。由于 ARN 不同，有权访问旧密钥的用户不会自动获得新密钥的访问权限。
- 密钥的名称、说明、资源策略和标签。
- 加密密钥的 ARN，Secrets Manager 使用它来加密和解密密钥值。 AWS KMS key Secrets Manager 始终以加密形式存储密钥文本，并在传输过程中加密密钥。请参阅 the section called “密钥加密和解密”。
- 如果设置了轮转，有关如何轮转密钥的信息。请参阅 轮换 密钥。

Secrets Manager 使用 IAM 权限策略来确保只有经过授权的用户才能访问或修改密钥。请参阅 的身份验证和访问控制 AWS Secrets Manager。

密钥具有保存加密密钥值副本的版本。更改密钥值或轮换密钥时，Secrets Manager 会创建一个新版本。请参阅 the section called “秘密版本”。

您可以通过复制多个密钥 AWS 区域 来使用该密钥。复制密钥时，您可以创建原始或主密钥称为副本密钥。副本密钥保持链接到主密钥上。请参阅跨区域复制密钥。

请参阅 创建和管理密钥。

秘密版本

密钥具有保存加密密钥值副本的版本。更改密钥值或轮换密钥时，Secrets Manager 会创建一个新版本。

Secrets Manager 不会存储带有版本的线性密钥历史记录。相反，它通过标记三个特定版本来跟踪它们：

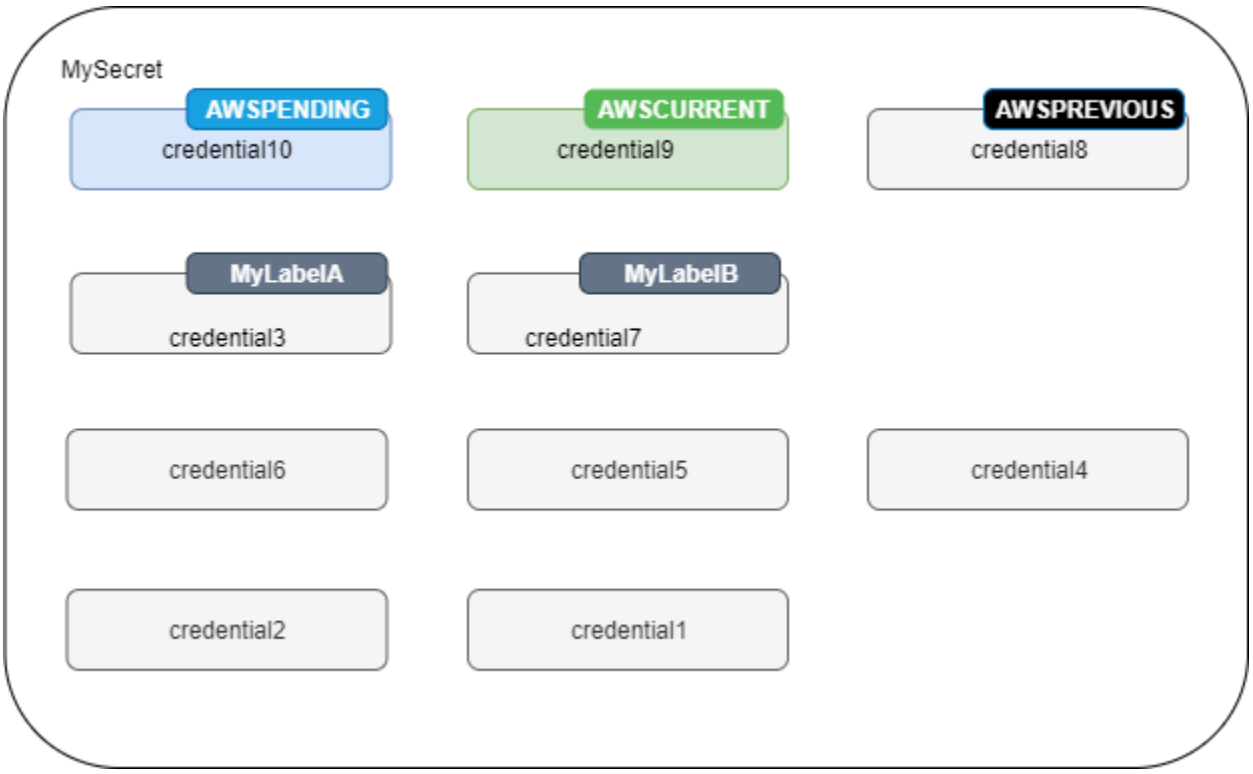
- 当前版本 – AWSCURRENT。
- 先前版本 – AWSPREVIOUS。
- 待处理版本（轮换期间）– AWSPENDING。

密钥始终有一个标记为 AWSCURRENT 的版本，Secrets Manager 会在您检索密钥值时默认返回该版本。

您也可以通过调update-secret-version-stage用自己的标签来为版本添加标签 AWS CLI。您最多可以为一个密钥附加 20 个版本标签。密钥的两个版本不能具有相同的暂存标注。版本可以有多个标签。

Secrets Manager 从不移除带标签的版本，但未标记的版本将被视为已弃用。如果版本超过 100 个，Secrets Manager 会移除已弃用的版本。Secrets Manager 不会移除 24 小时前创建的版本。

下图显示了一个 AWS 标有版本和客户标签版本的密钥。无标签的版本将被视为已弃用，Secrets Manager 将在某个未来的时间将其移除。


MySecret
AWSPENDING
credential10
AWSCURRENT
credential9
AWSPREVIOUS
credential8
MyLabelA
credential3
MyLabelB
credential7
credential6
credential5
credential4
credential2
credential1

AWS Secrets Manager 教程

主题

使用 Amazon CodeGuru Reviewer 查找代码中不受保护的密钥

Amazon CodeGuru Reviewer 服务使用程序分析和机器学习来检测开发人员难以找到的潜在缺陷，并提供改进 Java 和 Python 代码的建议。CodeGuru Reviewer 与 Secrets Manager 集成后，可以查找代码中不受保护的密钥。有关它能找到的密钥类型，请参阅《Amazon CodeGuru Reviewer 用户指南》中的CodeGuru Reviewer 可检测的密钥类型。

找到硬编码的密钥后，请立即将其替换：

- the section called “替换硬编码的数据库凭证 ”
- the section called “替换硬编码的密钥 ”

将硬编码的机密移至 AWS Secrets Manager

如果代码中存在明文密钥，我们建议将其轮换并存储到 Secrets Manager 中。将密钥移动到 Secrets Manager 后，您的代码将直接从 Secrets Manager 中检索密钥，从而解决了任何看到代码的人会看到密钥的问题。轮换密钥会吊销当前硬编码的密钥，使其不再有效。

关于数据库凭证密钥，请参见将硬编码的数据库凭据移至 AWS Secrets Manager。

在开始之前，您需要确定谁需要访问该密钥。我们建议使用两个 IAM 角色来管理密钥的权限：

- 负责管理组织中的密钥的角色。有关更多信息，请参阅 the section called “Secrets Manager 管理员权限”。您将使用此角色创建和轮换密钥。
- 可以在运行时使用密钥的角色，例如在本教程中使用的角色*RoleToRetrieveSecretAtRuntime*。您的代码将代入此角色以检索密钥。在本教程中，您将

向该角色仅授予检索一个密钥值的权限，并您将使用密钥的资源策略授予权限。有关其他替代方法，请参阅the section called “后续步骤”。

步骤：

- 第 1 步：创建密钥
- 第 2 步：更新代码
- 第 3 步：更新密钥
- 后续步骤

第 1 步：创建密钥

第一步是将现有硬编码的密钥复制到 Secrets Manager 中的密钥中。如果密钥与 AWS 资源相关，请将其存储在与该资源相同的区域。否则，请将其存储在您的用例延迟最低的区域。

创建密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于密钥类型，请选择其他密钥类型。
   b. 以 Key/value pairs（键值对）或者 Plaintext（明文）格式输入密钥。一些示例：

API 密钥键值对：

ClientID：*my_client_id*

ClientSecret ：*wjalrxutnfemi/k7mdeng/ cyexampleK bPxRfi* EY

凭证键值对：

Username：*saanvis*

Password：*EXAMPLE-PASSWORD*

API 密钥键值对：

ClientID：*my_client_id*

ClientSecret：*wjalrxutnfemi/k7mdeng/ cyexampleK bPxRfi* EY

OAuth 令牌明文：

AKIAI44QH8DHBEXAMPLE

数字证书明文：

```
-----BEGIN CERTIFICATE-----
EXAMPLE
-----END CERTIFICATE-----
```

私有密钥明文：

```
----BEGIN PRIVATE KEY ---
EXAMPLE
---- END PRIVATE KEY ----
```

c. 对于 Encryption key（加密密钥），选择 aws/secretsmanager 使用 Secrets Manager 的 AWS 托管式密钥。使用此密钥不产生任何费用。例如，您还可以使用自己的客户管理型密钥来访问来自其他 AWS 账户的密钥。有关使用客户托管密钥的成本的信息，请参阅 定价。

d. 选择下一步。

4. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：

a. 输入一个描述性的 Secret name（密钥名称）和 Description（说明）。

b. 在 Resource permissions（资源权限）中，选择 Edit permissions（编辑权限）。粘贴以下允许*RoleToRetrieveSecretAtRuntime*检索密钥的策略，然后选择“保存”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleToRetrieveSecretAtRuntime"
      },
```

```
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

c. 在页面底部，选择 Next。

5. 在 Configure rotation（配置轮换）页面上，将轮换禁用。选择下一步。
6. 在 Review (审核) 页上，审核您的密钥详细信息，然后选择 Store (存储)。

第 2 步：更新代码

您的代码必须担任 IAM 角色*RoleToRetrieveSecretAtRuntime*才能检索密钥。有关更多信息，请参阅切换到 IAM 角色 (AWS API)。

然后，您可以使用 Secrets Manager 提供的示例代码更新您的代码，以检索 Secrets Manager 中的密钥。

查找示例代码

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在密钥列表页上，选择您的密钥。
3. 向下滚动到 Sample code（示例代码）。选择您的编程语言，然后复制代码片段。

移除应用程序中的硬编码密钥并粘贴此代码片段。根据代码语言的不同，您可能需要在片段中添加对函数或方法的调用。

使用密钥代替硬编码密钥，测试您的应用程序是否符合预期。

第 3 步：更新密钥

最后一步是吊销并更新硬编码的密钥。请参阅密钥的来源以查找吊销和更新密钥的说明。例如，您可能需要停用当前密钥并生成一个新密钥。

用新值更新密钥

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 Secrets（密钥），然后选择该密钥。

3. 在 Secret details（密钥详细信息）页面上，向下滚动并选择 Retrieve secret value（检索密钥值），然后选择 Edit（编辑）。
4. 更新密钥然后选择 Save（保存）。

然后，测试您的应用程序按照预期那样在使用新密钥。

后续步骤

从代码中移除硬编码的密钥后，接下来需要注意以下事项：

- 要在你的 Java 和 Python 应用程序中查找硬编码的机密，我们建议使用 Amazon CodeGuru Reviewer。
- 您可以通过缓存密钥来提高性能并降低成本。有关更多信息，请参阅 获取秘密。
- 对于从多个区域访问的密钥，请考虑复制密钥以减少延迟。有关更多信息，请参阅 跨区域复制密钥。
- 在本教程中，您*RoleToRetrieveSecretAtRuntime*仅授予了检索密钥值的权限。要向角色授予更多权限（例如获取有关密钥的元数据或查看密钥列表），请参阅the section called “权限策略示例”。
- 在本教程中，您使用密钥的资源策略授予了权限。*RoleToRetrieveSecretAtRuntime*有关授予权限的其他方法，请参阅the section called “将权限策略附加到身份”。

将硬编码的数据库凭据移至 AWS Secrets Manager

如果代码中存在明文数据库凭证，我们建议您将凭证移动到 Secrets Manager，然后立即将其轮换。将凭证移动到 Secrets Manager 后，您的代码将直接从 Secrets Manager 中检索凭证，从而解决了任何看到代码的人会看到凭证的问题。轮换密钥会更新密码，然后吊销当前硬编码的密码，使其不再有效。

对于 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 数据库，请使用本页中的步骤将硬编码的凭证移动到 Secrets Manager。对于其他类型的凭证和其他密钥，请参阅the section called “替换硬编码的密钥 ”。

在开始之前，您需要确定谁需要访问该密钥。我们建议使用两个 IAM 角色来管理密钥的权限：

- 负责管理组织中的密钥的角色。有关更多信息，请参阅 the section called “Secrets Manager 管理员权限”。您将使用此角色创建和轮换密钥。
- 在本教程中，一个可以在运行时使用凭据*RoleToRetrieveSecretAtRuntime*的角色。您的代码将代入此角色以检索密钥。

步骤：

第 1 步：创建密钥

第一步是将现有硬编码的凭证复制到 Secrets Manager 中的密钥中。为了实现低延迟，可将密钥存储在与数据库相同的区域中。

创建密钥

1. 在 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于密钥类型，选择要存储的数据库凭证类型：
      - Amazon RDS 数据库
      - Amazon DocumentDB 数据库
      - 亚马逊 Redshift 数据仓库。
      - 有关其他类型的密钥，请参阅替换硬编码的密钥。
   b. 对于凭证，请输入数据库现有的硬编码凭证。
   c. 对于 Encryption key（加密密钥），选择 aws/secretsmanager 使用 Secrets Manager 的 AWS 托管式密钥 。使用此密钥不产生任何费用。例如，您还可以使用自己的客户管理型密钥来访问来自其他 AWS 账户的密钥。有关使用客户托管密钥的成本的信息，请参阅 定价。
   d. 对于 Database（数据库），请选择您的数据库。
   e. 选择下一步。
4. 在 Configure secret（配置密钥）页面上，执行以下操作：
   a. 输入一个描述性的 Secret name（密钥名称）和 Description（说明）。
   b. 在 Resource permissions（资源权限）中，选择 Edit permissions（编辑权限）。粘贴以下允许*RoleToRetrieveSecretAtRuntime*检索密钥的策略，然后选择 “保存”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleToRetrieveSecretAtRuntime"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

c. 在页面底部，选择 Next。

5. 在 Configure rotation（配置轮换）页面上，暂时将轮换禁用。稍后您会将其启用。选择下一步。
6. 在 Review (审核) 页上，审核您的密钥详细信息，然后选择 Store (存储)。

第 2 步：更新代码

您的代码必须担任 IAM 角色*RoleToRetrieveSecretAtRuntime*才能检索密钥。有关更多信息，请参阅切换到 IAM 角色 (AWS API)。

然后，您可以使用 Secrets Manager 提供的示例代码更新您的代码，以检索 Secrets Manager 中的密钥。

查找示例代码

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在密钥列表页上，选择您的密钥。
3. 向下滚动到 Sample code（示例代码）。选择您的语言，然后复制代码片段。

移除应用程序中的硬编码凭证并粘贴此代码片段。根据代码语言的不同，您可能需要在片段中添加对函数或方法的调用。

使用密钥代替硬编码凭证，测试您的应用程序是否符合预期。

步骤 3：轮换秘密

最后一步是通过轮换密钥来吊销硬编码的凭证。Rotation 是定期更新密钥的过程。轮换密钥时，您会同时更新密钥和数据库中的凭证。Secrets Manager 可以按照您设定的计划自动为您轮换密钥。

设置轮换包括确保 Lambda 轮换函数可以访问 Secrets Manager 和您的数据库。启用自动轮换后，Secrets Manager 会与您的数据库相同的 VPC 中创建 Lambda 轮换函数，以确保它拥有数据库的网络访问权限。Lambda 轮换函数还必须能够调用 Secrets Manager 以更新密钥。我们建议您在 VPC 中创建一个 Secrets Manager 终端节点，这样从 Lambda 到 Secrets Manager 的调用就不会离开基础架构 AWS 。有关说明，请参阅VPC 端点。

启用轮换

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在密钥列表页上，选择您的密钥。
3. 在 Secret details (密钥详细信息) 页上的 Rotation configuration (轮换配置) 部分中，选择 Edit rotation (编辑轮换)。
4. 在编辑轮换配置对话框中，执行以下操作：
   a. 启用 Automatic rotation（自动轮换）。
   b. 在 Rotation schedule（轮换计划）下，以 UTC 时区格式输入您的计划。
   c. 选择 Rotate immediately when the secret is stored（在存储密钥时立即轮换），以在保存更改时轮换密钥。
   d. 在 Rotation function（轮换函数）下，选择 Create a new Lambda function（创建新的 Lambda 函数），然后为新函数输入一个名称。Secrets Manager 将 "SecretsManager" 添加到您的函数名称的开头。
   e. 对于轮换策略，选择单用户。
   f. 选择保存。

检查密钥是否已轮换

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 Secrets（密钥），然后选择该密钥。
3. 在 Secret details（秘密详细信息）页面上，向下滚动并选择 Retrieve secret value（检索秘密值）。

如果密钥值改变，则说明轮换已经成功。如果密钥值没有更改，则需要 轮换问题排查查看轮换功能的 CloudWatch 日志。

测试您的应用程序按照预期那样在使用轮换后的密钥。

后续步骤

从代码中移除硬编码的密钥后，接下来需要注意以下事项：

- 您可以通过缓存密钥来提高性能并降低成本。有关更多信息，请参阅 获取秘密。
- 您可以选择不同的轮换计划。有关更多信息，请参阅 the section called “轮换时间表”。
- 要在你的 Java 和 Python 应用程序中查找硬编码的机密，我们建议使用 Amazon CodeGuru Reviewer。

为用户设置交替轮换 AWS Secrets Manager

在本教程中，您将学习如何为包含数据库凭证的秘密设置交替用户轮换。Alternating users rotation（交替用户轮换）是一种轮换策略，在该策略中，Secrets Manager 将克隆用户，然后替换被更新的那些用户凭证。如果您需要为密钥实现高可用性，则此策略是一个不错的选择，因为其中一个交替用户拥有数据库的最新凭证，而另一个则正在更新。有关更多信息，请参阅 the section called “交替用户”。

要设置交替用户轮换，您需要两个秘密：

- 其中一个秘密包含您想轮换的凭证。
- 具有管理员凭证的第二个密钥。

  此用户有权克隆第一个用户并更改第一个用户的密码。在本教程中，您将让 Amazon RDS 为管理员用户创建此密钥。Amazon RDS 还会管理管理员密码轮换。有关更多信息，请参阅 the section called “托管轮换”。

本教程的第一部分内容是介绍如何设置真实环境。为了向您展示轮换的工作原理，本教程使用了一个示例 Amazon RDS MySQL 数据库。为了安全起见，数据库位于限制入站互联网访问的 VPC 中。要通过互联网从本地电脑连接到数据库，请使用堡垒主机，它是 VPC 中可以连接到数据库的服务器，但也允许从互联网进行 SSH 连接。本教程中的堡垒主机是 Amazon EC2 实例，该实例的安全组会阻止其他类型的连接。

完成本教程后，我们建议您清理教程中的资源。请勿在生产环境中使用它们。

Secrets Manager 轮换使用 AWS Lambda 函数来更新密钥和数据库。有关使用 Lambda 函数的成本的信息，请参阅 定价。

教程：

- 权限
- 先决条件
- 步骤 1：创建 Amazon RDS 数据库用户
- 步骤 2：为用户凭证创建秘密
- 步骤 3：测试已轮换的秘密
- 步骤 4：清理资源
- 后续步骤

权限

本教程的先决条件为，您需要对 AWS 账户的管理权限。在生产环境中，最佳实践是为每个步骤使用不同的角色。例如，具有数据库管理员权限的角色将创建 Amazon RDS 数据库，而具有网络管理员权限的角色将设置 VPC 和安全组。在执行教程步骤时，我们建议您继续使用相同身份。

有关如何在生产环境中设置权限的信息，请参阅 身份验证和访问控制。

先决条件

在此教程中，您需要以下内容：

- 先决条件 A：Amazon VPC
- 先决条件 B：Amazon EC2 实例
- 先决条件 C：Amazon RDS 数据库和管理员凭证的 Secrets Manager 密钥
- 先决条件 D：允许本地计算机连接到 EC2 实例

先决条件 A：Amazon VPC

在此步骤中，您将创建可在其中启动 Amazon RDS 数据库和 Amazon EC2 实例的 VPC。在后续步骤中，您将使用计算机通过互联网连接到堡垒机，然后连接到数据库，因此您需要允许来自 VPC 的流

量。为此，Amazon VPC 会将互联网网关连接到 VPC 并在路由表中添加路由，以将发往 VPC 外部的流量发送到互联网网关。

在 VPC 中，您可以创建一个 Secrets Manager 端点和一个 Amazon RDS 端点。在稍后的步骤中设置自动轮换时，Secrets Manager 会在 VPC 内创建 Lambda 轮换函数，以便它可以访问数据库。Lambda 轮换函数还会调用 Secrets Manager 来更新密钥，并调用 Amazon RDS 来获取数据库连接信息。通过在 VPC 内创建终端节点，您可以确保从 Lambda 函数对 Secrets Manager 和 Amazon RDS 的调用不会离开 AWS 基础设施。相反，这些调用将被路由到 VPC 内的端点。

创建 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 选择创建 VPC。
3. 在 Create VPC（创建 VPC）页面上，选择 VPC and more（VPC 等）。
4. 在 Name tag auto-generation（名称标签自动生成）下的 Auto-generate（自动生成）下，输入 **SecretsManagerTutorial**。
5. 对于 DNS options（DNS 选项），请同时选择 **Enable DNS hostnames** 和 **Enable DNS resolution**。
6. 选择创建 VPC。

在 VPC 内创建 Secrets Manager 端点

1. 在 Amazon VPC 控制台的 Endpoints（端点）下，选择 Create Endpoint（创建端点）。
2. 在 Endpoint settings（端点设置）下，为 Name（名称）输入 **SecretsManagerTutorialEndpoint**。
3. 在 Services（服务）下，输入 **secretsmanager** 以筛选列表，然后在您的 AWS 区域中选择 Secrets Manager 端点。例如，在美国东部（弗吉尼亚北部），选择 `com.amazonaws.us-east-1.secretsmanager`。
4. 对于 VPC，选择 **vpc**** **(SecretsManagerTutorial)**。
5. 对于 Subnets（子网），选择所有 Availability Zones（可用性区域），然后对于每个区域，选择要包含的 Subnet ID（子网 ID）。
6. 对于 IP address type（IP 地址类型），选择 **IPv4**。
7. 对于 Security groups（安全组），选择默认安全组。
8. 对于 Policy（策略），选择 **Full access**。
9. 选择创建端点。

在 VPC 内创建 Amazon RDS 端点

1. 在 Amazon VPC 控制台的 Endpoints（端点）下，选择 Create Endpoint（创建端点）。
2. 在 Endpoint settings（端点设置）下，为 Name（名称）输入 **RDSTutorialEndpoint**。
3. 在 Services（服务）下，输入 **rds** 以筛选列表，然后在您的 AWS 区域中选择 Amazon RDS 端点。例如，在美国东部（弗吉尼亚北部），选择 com.amazonaws.us-east-1.rds。
4. 对于 VPC，选择 **vpc**** **(SecretsManagerTutorial)**。
5. 对于 Subnets（子网），选择所有 Availability Zones（可用性区域），然后对于每个区域，选择要包含的 Subnet ID（子网 ID）。
6. 对于 IP address type（IP 地址类型），选择 **IPv4**。
7. 对于 Security groups（安全组），选择默认安全组。
8. 对于 Policy（策略），选择 **Full access**。
9. 选择创建端点。

先决条件 B：Amazon EC2 实例

您在后续步骤中创建的 Amazon RDS 数据库将位于 VPC 中，因此要访问它，您需要堡垒主机。该堡垒主机也位于 VPC 中，但在稍后步骤中，您将配置一个安全组，以允许本地计算机使用 SSH 连接到堡垒主机。

为堡垒主机创建 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Instances（实例），然后选择 Launch Instances（启动实例）。
3. 在 Name and tags（名称和标签）下，对于 Name（名称），输入 **SecretsManagerTutorialInstance**。
4. 在 Application and OS Images（应用程序和操作系统映像）下，保留默认值 **Amazon Linux 2 AMI (HMV) Kernel 5.10**。
5. 在 Instance type（实例类型）下，保留默认值 **t2.micro**。
6. 在 Key pair（密钥对）下，选择 Create key pair（创建密钥对）。

   在 Create key pair（创建密钥对）对话框中，对于 Key pair name（密钥对名称），输入 **SecretsManagerTutorialKeyPair**，然后选择 Create key pair（创建密钥对）。

   此时会自动下载密钥对。

7. 在 Network settings（网络设置）下，选择 Edit（编辑），然后执行以下操作：
   a. 对于 VPC，选择 **vpc-**** SecretsManagerTutorial**。
   b. 对于 Auto-assign Public IP（自动分配公有 IP），选择 **Enable**。
   c. 对于 Firewall（防火墙），选择 Select existing security group（选择现有安全组）。
   d. 对于 Common security groups（常见安全组），选择 **default**。
8. 选择启动实例。

先决条件 C：Amazon RDS 数据库和管理员凭证的 Secrets Manager 密钥

在此步骤中，您将创建一个 AmazonRDS MySQL 数据库并对其进行配置，以便 AmazonRDS 创建包含管理员凭证的密钥。然后，Amazon RDS 会自动为您管理管理员密钥的轮换。有关更多信息，请参阅 托管轮换。

在创建数据库过程中，请指定您在上一步中创建的堡垒主机。然后，Amazon RDS 会设置安全组，以便数据库和实例能够相互访问。您可向连接到实例的安全组添加规则，以允许您的本地计算机也连接到该实例。

使用包含管理员凭证的 Secrets Manager 密钥创建 Amazon RDS 数据库

1. 在 Amazon RDS 控制台中，选择 Create database（创建数据库）。
2. 在 Engine options（引擎选项）部分，为 Engine type（引擎类型）选择 **MySQL**。
3. 在 Templates（模板）部分，选择 **Free tier**。
4. 在 Settings（设置）部分，执行以下操作：
   a. 对于 DB instance identifier（数据库实例标识符），输入 **SecretsManagerTutorial**。
   b. 在 “凭据设置” 下，选择中的管理主凭证。 AWS Secrets Manager
5. 在 Connectivity（连接）部分，对于 Computer resource（计算机资源），选择 Connect to an EC2 computer resource（连接到 EC2 计算机资源），然后对于 EC2 Instance（EC2 实例），选择 **SecretsManagerTutorialInstance**。
6. 选择创建数据库。

先决条件 D：允许本地计算机连接到 EC2 实例

在此步骤中，您将在“先决条件 B”中创建的 EC2 实例配置为允许本地计算机连接到该实例。为此，您将编辑 Amazon RDS 在“先决条件 C”中添加的安全组，使其包含允许您的计算机的 IP 地址与 SSH

连接的规则。该规则允许本地计算机（通过当前 IP 地址识别）通过 Internet 使用 SSH 连接到堡垒主机。

允许本地计算机连接到 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 EC2 实例上 SecretsManagerTutorialInstance，在 “安全” 选项卡上的 “安全组” 下，选择**sg-*** (ec2-rds-X)**。
3. 在 Input rules（输入规则）下，选择Edit inbound rules（编辑入站规则）。
4. 选择 Add rule（添加规则），然后对该规则执行以下操作：
   a. 对于类型，选择 **SSH**。
   b. 对于 Source type（源类型），选择 **My IP**。

步骤 1：创建 Amazon RDS 数据库用户

首先，您需要一个用户，其凭证将被存储在秘密中。要创建用户，请使用管理员凭证登录 Amazon RDS 数据库。为简单起见，在本教程中，您将创建具有数据库完全权限的用户。在生产环境中，这并不常见，建议您遵循最低权限原则。

要连接到数据库，请使用 MySQL 客户端工具。在本教程中，您将使用基于 GUI 的应用程序 MySQL Workbench。要安装 MySQL Workbench，请参阅下载 MySQL Workbench。

要连接到数据库，请在 MySQL Workbench 中创建连接配置。对于配置，您需要获得来自 Amazon EC2 和 Amazon RDS 的一些信息。

在 MySQL Workbench 中创建数据库连接

1. 在 MySQL Workbench 中，选择 MySQL Connections（MySQL 连接）旁边的 (+) 按钮。
2. 在 Setup New Connection（设置新连接）对话框中，执行以下操作：
   a. 对于 Connection Name（连接名称），输入 **SecretsManagerTutorial**。
   b. 对于 Connection Method（连接方法），选择 **Standard TCP/IP over SSH**。
   c. 在 Parameters（参数）选项卡上，执行以下操作：
      i. 对于 SSH Hostname（SSH 主机名），输入 Amazon EC2 实例的公有 IP 地址。

您可以通过选择实例在 Amazon EC2 控制台上找到 IP 地址SecretsManagerTutorialInstance。复制 Public IPv4 DNS（公有 IPv4 DNS）下的 IP 地址。

ii. 对于 SSH Username（SSH 用户名），输入 **ec2-user**。

iii. 对于 SSH Keyfile，请选择您在前面的先决条件中下载的密钥对文件 SecretsManagerTutorialKeyPair.pem。

iv. 对于 MySQL Hostname（MySQL 主机名），输入 Amazon RDS 端点地址。

您可以在 Amazon RDS 控制台上通过选择数据库实例 secretsmanagertutorialdb 查找端点地址。复制 Endpoint（端点）下的地址。

v. 对于 Username（用户名），输入 **admin**。

d. 选择 确定。

检索管理员密码

1. 在 Amazon RDS 控制台中，导航到您的数据库。
2. 在 Configuration（配置）选项卡的 Master Credentials ARN（主凭证 ARN）下，选择 Manage in Secrets Manager（在 Secrets Manager 中管理）。

   此时将打开 Secrets Manager 控制台。
3. 在密钥详细信息页面上，选择 Retrieve secret value（检索密钥值）。
4. 密码显示在 Secret value（密钥值）部分中。

创建数据库用户

1. 在 MySQL 工作台中，选择连接SecretsManagerTutorial。
2. 输入从密钥中检索到的管理员密码。
3. 在 MySQL Workbench 中，在 Query（查询）窗口中，输入以下命令（包括强密码），然后选择 Execute（执行）。

```
CREATE DATABASE myDB;
CREATE USER 'appuser'@'%' IDENTIFIED BY 'EXAMPLE-PASSWORD';
GRANT ALL PRIVILEGES ON myDB . * TO 'appuser'@'%';
```

   在 Output（输出）窗口中，您会看到这些命令执行成功。

步骤 2：为用户凭证创建秘密

接下来，您将创建秘密，用于存储您刚创建的用户凭证。这是您将要轮换的秘密。启用自动轮换，要指示交替用户策略，您应选择一个单独的超级用户秘密，它应有权限更改第一个用户的密码。

1. 在 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于 Secret type（秘密类型），选择 Credentials for Amazon RDS database（Amazon RDS 数据库凭证）。
   b. 对于 Credentials（凭证），输入用户名 **appuser**，以及您为使用 MySQL Workbench 创建的数据库用户输入的密码。
   c. 对于 Database（数据库），选择 secretsmanagertutorialdb。
   d. 选择下一步。
4. 在 Configure secret（配置密钥）页面上，对于 Secret name（密钥名称），输入 **SecretsManagerTutorialAppuser**，然后选择 Next（下一步）。
5. 在 Configure rotation（配置轮换）页面上，执行以下操作：
   a. 启用 Automatic rotation（自动轮换）。
   b. 对于 Rotation schedule（轮换计划），设置计划 Days（天数）：**2** 天，以及 Duration（持续时间）：**2h**。使 Rotate immediately（立即轮换）处于已选择状态。
   c. 对于 Rotation function（轮换函数），选择 Create a rotation function（创建轮换函数），然后对于函数名称，输入 **tutorial-alternating-users-rotation**。
   d. 对于轮换策略，选择交替用户，然后在管理员凭证密钥下，选择名为 rds!cluster...，并且描述包含您在本教程 **secretsmanagertutorial** 中所创建数据库的名称的密钥，例如 `Secret associated with primary RDS DB instance: arn:aws:rds:`*`Region`*`:`*`AccountId`*`:db:secretsmanagertutorial`。
   e. 选择下一步。
6. 在 Review（检查）页面上，选择 Store（存储）。

   Secrets Manager 返回到密钥详情页面。您可以在该页面顶部查看轮换配置状态。Secrets CloudFormation Manager 用于创建资源，例如 Lambda 轮换函数和运行 Lambda 函数的执行角色。 CloudFormation 完成后，横幅将变为预定轮换的 Secret。第一次轮换已完成。

步骤 3：测试已轮换的秘密

在密钥轮换后，您可以检查该密钥是否包含有效凭证。秘密中的密码已从原始凭证发生更改。

从秘密中检索新密码

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 Secrets（秘密），然后选择秘密 **SecretsManagerTutorialAppuser**。
3. 在 Secret details（秘密详细信息）页面上，向下滚动并选择 Retrieve secret value（检索秘密值）。
4. 在 Key/value（键/值）表中，为 **password** 复制 Secret value（秘密值）。

测试凭证

1. 在 MySQL Workbench 中，右键单击该连接，SecretsManagerTutorial然后选择 “编辑连接”。
2. 在 Manage Server Connections（管理服务器连接）对话框中，对于 Username（用户名），输入 **appuser**，然后选择 Close（关闭）。
3. 回到 MySQL 工作台，选择连接SecretsManagerTutorial。
4. 在 Open SSH Connection（打开 SSH 连接）对话框中，对于 Password（密码），粘贴您从秘密中检索到的密码，然后选择 OK（确定）。

   如果凭证有效，则 MySQL Workbench 将打开至数据库的设计页面。

这表明秘密轮换是成功的。秘密中的凭证已更新，它是用于连接到数据库的有效密码。

步骤 4：清理资源

如果您想尝试另一种轮换策略单用户轮换，请跳过清理资源，然后转到 the section called “单用户轮换”。

否则，为了避免潜在费用，并删除有权访问互联网的 EC2 实例，请删除您在本教程及其先决条件中创建的以下资源：

- Amazon RDS 数据库实例。有关说明，请参阅《Amazon RDS 用户指南》中的删除数据库实例。
- Amazon EC2 实例。有关说明，请参阅 Amazon EC2 用户指南中的终止实例。
- Secrets Manager 秘密 `SecretsManagerTutorialAppuser`。有关说明，请参阅the section called “删除密钥”。

- Secrets Manager 端点。有关说明，请参阅《AWS PrivateLink 指南》中的删除 VPC 端点。
- VPC 端点。有关说明，请参阅《AWS PrivateLink 指南》中的删除 VPC。

后续步骤

- 了解如何在您的应用程序中检索密钥。
- 了解其他轮换计划。

为 AWS Secrets Manager设置单用户轮换

在本教程中，您将学习如何为包含数据库凭证的密钥设置单用户轮换。单用户轮换是一种轮换策略，在该策略中，Secrets Manager 将同时在密钥和数据库中更新用户的凭证。有关更多信息，请参阅 the section called “单用户”。

完成本教程后，我们建议您清理教程中的资源。请勿在生产环境中使用它们。

Secrets Manager 轮换使用 AWS Lambda 函数来更新密钥和数据库。有关使用 Lambda 函数的成本的信息，请参阅 定价。

目录

权限

本教程的先决条件为，您需要对 AWS 账户的管理权限。在生产环境中，最佳实践是为每个步骤使用不同的角色。例如，具有数据库管理员权限的角色将创建 Amazon RDS 数据库，而具有网络管理员权限的角色将设置 VPC 和安全组。在执行教程步骤时，我们建议您继续使用相同身份。

有关如何在生产环境中设置权限的信息，请参阅 身份验证和访问控制。

先决条件

本教程的先决条件是 the section called “交替用户轮换”。在第一个教程结束时，请不要清理资源。在该教程之后，您将拥有一个现实环境，其中包含一个 AmazonRDS 数据库和一个内含数据库管理员凭证的 SecretsManager 密钥。您还有另一个密钥包含数据库用户的凭证，但您在本教程中不使用该密钥。

您还在 MySQL Workbench 中配置了一条连接，可以使用管理员凭证连接到数据库。

步骤 1：创建 Amazon RDS 数据库用户

首先，您需要一个用户，其凭证将被存储在秘密中。要创建用户，请使用存储在密钥中的管理员凭证登录 Amazon RDS 数据库。为简单起见，在本教程中，您将创建具有数据库完全权限的用户。在生产环境中，这并不常见，建议您遵循最低权限原则。

检索管理员密码

1. 在 Amazon RDS 控制台中，导航到您的数据库。
2. 在 Configuration（配置）选项卡的 Master Credentials ARN（主凭证 ARN）下，选择 Manage in Secrets Manager（在 Secrets Manager 中管理）。

   此时将打开 Secrets Manager 控制台。
3. 在密钥详细信息页面上，选择 Retrieve secret value（检索密钥值）。
4. 密码显示在 Secret value（密钥值）部分中。

创建数据库用户

1. 在 MySQL Workbench 中，右键单击该连接，SecretsManagerTutorial然后选择 “编辑连接”。
2. 在 Manage Server Connections（管理服务器连接）对话框中，对于 Username（用户名），输入 **admin**，然后选择 Close（关闭）。
3. 回到 MySQL 工作台，选择连接SecretsManagerTutorial。
4. 输入从密钥中检索到的管理员密码。
5. 在 MySQL Workbench 中，在 Query（查询）窗口中，输入以下命令（包括强密码），然后选择 Execute（执行）。

```
CREATE USER 'dbuser'@'%' IDENTIFIED BY 'EXAMPLE-PASSWORD';
GRANT ALL PRIVILEGES ON myDB . * TO 'dbuser'@'%';
```

在 Output（输出）窗口中，您会看到这些命令执行成功。

步骤 2：为数据库用户凭证创建密钥

接下来，您将创建一个密钥用于存储您刚创建的用户的凭证，并且将启用自动轮换（包括立即轮换）。Secrets Manager 会轮换密钥，这意味着密码是以编程方式生成的，没有人看到过这个新密码。立即开始轮换也可以帮助您确定轮换设置是否正确。

1. 在 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于 Secret type（秘密类型），选择 Credentials for Amazon RDS database（Amazon RDS 数据库凭证）。
   b. 对于 Credentials（凭证），输入用户名 **dbuser**，以及您为使用 MySQL Workbench 创建的数据库用户输入的密码。
   c. 对于 Database（数据库），选择 secretsmanagertutorialdb。
   d. 选择下一步。
4. 在 Configure secret（配置密钥）页面上，对于 Secret name（密钥名称），输入 **SecretsManagerTutorialDbuser**，然后选择 Next（下一步）。
5. 在 Configure rotation（配置轮换）页面上，执行以下操作：
   a. 启用 Automatic rotation（自动轮换）。
   b. 对于 Rotation schedule（轮换计划），设置计划 Days（天数）：**2** 天，以及 Duration（持续时间）：**2h**。使 Rotate immediately（立即轮换）处于已选择状态。
   c. 对于 Rotation function（轮换函数），选择 Create a rotation function（创建轮换函数），然后对于函数名称，输入 **tutorial-single-user-rotation**。
   d. 对于轮换策略，选择单用户。
   e. 选择下一步。
6. 在 Review（检查）页面上，选择 Store（存储）。

   Secrets Manager 返回到密钥详情页面。您可以在该页面顶部查看轮换配置状态。Secrets CloudFormation Manager 用于创建资源，例如 Lambda 轮换函数和运行 Lambda 函数的执行角色。 CloudFormation 完成后，横幅变为预定轮换的 Secret。第一次轮换已完成。

步骤 3：测试轮换的密码

在第一次密钥轮换（可能需要几秒钟）之后，您可以检查秘密是否仍包含有效凭证。秘密中的密码已从原始凭证发生更改。

从秘密中检索新密码

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 Secrets（秘密），然后选择秘密 **SecretsManagerTutorialDbuser**。
3. 在 Secret details（秘密详细信息）页面上，向下滚动并选择 Retrieve secret value（检索秘密值）。
4. 在 Key/value（键/值）表中，为 **password** 复制 Secret value（秘密值）。

测试凭证

1. 在 MySQL Workbench 中，右键单击该连接，SecretsManagerTutorial然后选择 “编辑连接”。
2. 在 Manage Server Connections（管理服务器连接）对话框中，对于 Username（用户名），输入 **dbuser**，然后选择 Close（关闭）。
3. 回到 MySQL 工作台，选择连接SecretsManagerTutorial。
4. 在 Open SSH Connection（打开 SSH 连接）对话框中，对于 Password（密码），粘贴您从秘密中检索到的密码，然后选择 OK（确定）。

   如果凭证有效，则 MySQL Workbench 将打开至数据库的设计页面。

步骤 4：清理资源

为避免潜在费用，请删除您在本教程中创建的秘密。有关说明，请参阅the section called “删除密钥”。

要清理前面教程中创建的资源，请参阅 the section called “步骤 4：清理资源”。

后续步骤

- 了解如何在您的应用程序中检索秘密。请参阅 获取秘密。
- 了解其他轮换计划。请参阅 the section called “轮换时间表”。

的身份验证和访问控制 AWS Secrets Manager

Secrets Manager 用AWS Identity and Access Management (IAM) 来保护密钥的访问权限。IAM 提供了身份验证和访问控制。身份验证确认个人请求的身份。Secrets Manager 使用密码、访问密钥登录过程和多重身份验证（MFA）令牌来验证用户身份。请参阅登录 AWS。访问控制确保只有获得批准的个人才能对密钥等 AWS 资源执行操作。Secrets Manager 使用策略来定义谁有权访问哪些资源，以及身份可以对这些资源执行哪些操作。参见 IAM 中的策略和权限。

Secrets Manager 管理员权限

如果要授予 Secrets Manager 管理员权限，请根据添加和删除 IAM 身份权限和下列策略进行操作：

- SecretsManagerReadWrite
- IAMFullAccess

我们建议您不要向最终用户授予管理员权限。尽管这样用户可以创建和管理密钥，但启用轮换所需的权限 (IAMFullAccess) 会授予不适合最终用户的重要权限。

访问密钥的权限

通过采用 IAM 权限策略，您可以控制哪些用户或服务有权访问您的密钥。权限策略描述了哪些人可以对哪些资源执行哪些操作。您可以：

- the section called “将权限策略附加到身份”
- the section called “将权限策略附加到密钥”

Lambda 轮换函数的权限

Secrets Manager 使用 AWS Lambda 函数来轮换密钥。Lambda 函数必须具有对密钥以及密钥包含凭据的数据库或服务的访问权限。请参阅 轮换权限。

加密密钥权限

Secrets Manager 使用 AWS Key Management Service (AWS KMS) 密钥来加密机密。 AWS 托管式密钥 `aws/secretsmanager`自动具有正确的权限。如果您使用不同的 KMS 密钥，Secrets Manager 需要对该密钥的权限。请参阅 the section called “KMS 密钥的权限”。

复制权限

通过使用 IAM 权限策略，您可以控制哪些用户或服务可以将您的密钥复制到其他区域。请参阅 the section called “防止复制”。

将权限策略附加到身份

将权限策略附加到 IAM 身份、用户、用户组和角色。在基于身份的策略中，您指定该身份可以访问哪些密钥以及该身份可以对密钥执行哪些操作。有关更多信息，请参阅添加和删除 IAM 身份权限。

您可以向代表其他服务中的应用程序或用户的角色授予权限。例如，在 Amazon EC2 实例上运行的应用程序可能需要访问数据库。您可以创建附加到 EC2 实例配置文件的 IAM 角色，然后使用权限策略授予该角色对包含数据库凭证的密钥的访问权限。有关更多信息，请参阅使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。您可以附加角色的其他服务包括 Amazon Redshift、AWS Lambda 和 Amazon ECS。

您还可以通过除 IAM 以外的其他身份系统验证的用户授予权限。例如，您可以将 IAM 角色与使用 Amazon Cognito 登录的移动应用程序用户关联。角色向应用程序授予具有角色权限策略中权限的临时凭据。然后，您可以使用权限策略授予角色对密钥的访问权限。有关更多信息，请参阅身份提供者和联合身份验证。

您必须使用基于身份的策略来：

- 授予对多个密钥的身份访问权限。
- 控制哪些人可以创建新密钥，哪些人可以访问尚未创建的密钥。
- 授予 IAM 组对密钥的访问权限。

有关更多信息，请参阅the section called “权限策略示例”。

将权限策略附加到 AWS Secrets Manager 密钥

在基于资源的策略中，您可以指定谁可以访问密钥，以及他们可以对密钥执行哪些操作。您可以使用基于资源的策略来：

- 为多个用户或角色授予单个密钥的访问权限。
- 向其他 AWS 账户中的用户或角色授予访问权限。

请参阅 the section called “权限策略示例”。

当您将基于资源的策略附加到控制台中的密钥时，Secrets Manager 使用自动推理引擎 Zelkova 和 API `ValidateResourcePolicy`，防止您向各种 IAM 委托人授予对您的密钥的访问权限。您也可以调用带有来自 CLI 或 SDK `BlockPublicPolicy` 参数的 `PutResourcePolicy` API。

> **Important**
>
> 资源策略验证和`BlockPublicPolicy`参数可防止通过直接附加到您的密钥的资源策略授予公共访问权限，从而帮助保护您的资源。除了使用这些功能外，还要仔细检查以下政策，以确认它们不向公众授予访问权限：
>
> - 附加到关联 AWS 委托人（例如，IAM 角色）的基于身份的策略
> - 附加到关联资源的基于 AWS 资源的策略（例如， AWS Key Management Service (AWS KMS) 密钥）
>
> 要查看您的密钥的权限，请参阅确定谁有权限访问您的 密钥。

查看、更改或删除密钥的资源策略（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。
3. 进入密钥详细信息页面后，在概述选项卡的资源权限部分中，选择编辑权限。
4. 在代码字段中，执行以下操作之一，然后选择保存：
   - 要附加或修改资源策略，输入该策略。
   - 要删除策略，清除代码字段。

AWS CLI

Example 检索资源策略

以下 `get-resource-policy` 示例将检索附加到密钥的基于资源的策略。

```
aws secretsmanager get-resource-policy \
    --secret-id MyTestSecret
```

Example 删除资源策略

以下 delete-resource-policy 示例将删除附加到密钥的基于资源的策略。

```
aws secretsmanager delete-resource-policy \
    --secret-id MyTestSecret
```

Example 添加资源策略

以下 put-resource-policy 示例将向密钥添加权限策略，首先检查该策略是否不提供对该密钥的广泛访问权限。该策略是从文件中读取的。有关更多信息，请参阅《 AWS CLI 用户指南》中的从文件加载 AWS CLI 参数。

```
aws secretsmanager put-resource-policy \
    --secret-id MyTestSecret \
    --resource-policy file://mypolicy.json \
    --block-public-policy
```

mypolicy.json 的内容：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/MyRole"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
}
```

AWS SDK

要检索附加到密钥的策略，请使用 GetResourcePolicy。

要删除附加到密钥的策略，请使用 DeleteResourcePolicy。

要将策略附加到密钥，请使用 PutResourcePolicy。如果已经附加了策略，命令会将其替换为新策略。策略必须格式化为 JSON 结构化文本。请参阅 JSON 策略文档结构。使用 the section called “权限策略示例” 开始编写您的策略。

有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

AWS 的托管策略 AWS Secrets Manager

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： SecretsManagerReadWrite

该政策提供读/写权限 AWS Secrets Manager，包括描述亚马逊 RDS、Amazon Redshift 和 Amazon DocumentDB 资源的权限，以及 AWS KMS 用于加密和解密密密钥的权限。该策略还允许创建 AWS CloudFormation 更改集、从由管理的 Amazon S3 存储桶获取轮换模板 AWS、列出 AWS Lambda 函数以及描述 Amazon EC2 VPC。控制台需要这些权限才能使用现有的轮换函数设置轮换。

要创建新的轮换函数，您还必须拥有创建 AWS CloudFormation 堆栈和 AWS Lambda 执行角色的权限。您可以分配 IAM FullAccess 托管策略。请参阅 轮换权限。

权限详细信息

该策略包含以下权限。

- `secretsmanager` – 允许主体执行所有 Secrets Manager 操作。
- `cloudformation`— 允许委托人创建 AWS CloudFormation 堆栈。这是必需的，以便使用控制台开启轮换功能的委托人可以通过堆栈创建 Lambda 轮换函数 AWS CloudFormation 。有关更多信息，请参阅 the section called “Secrets Manager 如何使用 AWS CloudFormation”。

- `ec2` – 允许主体描述 Amazon EC2 VPC。这是必需的条件，这样使用控制台的主体才能在与其存储在密钥中的凭证数据库相同的 VPC 中创建轮换函数。
- `kms`— 允许委托人使用 AWS KMS 密钥进行加密操作。这是必需的条件，这样 Secrets Manager 才能加密和解密密钥。有关更多信息，请参阅 the section called “密钥加密和解密”。
- `lambda` – 允许主体列出 Lambda 轮换函数。这是必需的条件，以便使用控制台的主体可以选择现有的轮换函数。
- `rds` – 允许主体描述 Amazon RDS 中的集群和实例。这是必需的条件，以便使用控制台的主体可以选择 Amazon RDS 集群或实例。
- `redshift` – 允许主体描述 Amazon Redshift 中的集群。这是必需的条件，以便使用控制台的主体可以选择 Amazon Redshift 集群。
- `redshift-serverless`— 允许委托人在 Amazon Redshift Serverless 中描述命名空间。这是必需的，以便使用控制台的委托人可以选择 Amazon Redshift Serverless 命名空间。
- `docdb-elastic` – 允许主体描述 Amazon DocumentDB 中的弹性集群。这是必需的条件，以便使用控制台的主体可以选择 Amazon DocumentDB 弹性集群。
- `tag` – 允许主体获取账户中所有已标记的资源。
- `serverlessrepo`— 允许委托人创建 AWS CloudFormation 更改集。这是必需的条件，以便使用控制台的主体可以创建 Lambda 轮换函数。有关更多信息，请参阅 the section called “Secrets Manager 如何使用 AWS CloudFormation”。
- `s3`— 允许委托人从由 AWS管理的 Amazon S3 存储桶中获取对象。此存储桶包含 Lambda 轮换函数模板。此权限是必需的，这样使用控制台的主体才能根据存储桶中的模板创建 Lambda 轮换函数。有关更多信息，请参阅 the section called “Secrets Manager 如何使用 AWS CloudFormation”。

要查看该政策，请参阅 SecretsManagerReadWrite JSON 策略文档。

Secrets Manager 对 AWS 托管策略的更新

查看有关 Secrets Manager AWS 托管策略更新的详细信息。

更改	描述	日期
SecretsManagerReadWrite – 对现有策略的更新	此政策已更新，允许描述访问亚马逊 Redshift Serverless，以便主机用户在创建亚马逊 Redshift 密钥时可以选择亚	2024 年 3 月 12 日

更改	描述	日期
	马逊 Redshift 无服务器命名空间。	
SecretsManagerReadWrite – 更新了现有策略	此策略已更新，允许描述访问 Amazon DocumentDB 弹性集群的权限，以便控制台用户可在创建 Amazon DocumentDB 密钥时选择弹性集群。	2023 年 9 月 12 日
SecretsManagerReadWrite – 更新了现有策略	此策略已更新，允许描述访问 Amazon Redshift 的权限，以便控制台用户可在创建 Amazon Redshift 密钥时选择 Amazon Redshift 集群。此更新还增加了新的权限，允许对存储 Lambda 轮换函数模板 AWS 的 Amazon S3 存储桶进行读取访问。	2020 年 6 月 24 日
SecretsManagerReadWrite – 更新了现有策略	此策略已更新，允许描述访问 Amazon RDS 集群的权限，以便控制台用户可在创建 Amazon RDS 密钥时选择集群。	2018 年 5 月 3 日
SecretsManagerReadWrite：新策略	Secrets Manager 创建了一个策略，用于授予使用控制台所需的权限，并授予对 Secrets Manager 的所有读/写访问权限。	2018 年 04 月 4 日
Secrets Manager 开始跟踪更改	Secrets Manager 开始跟踪其 AWS 托管策略的更改。	2018 年 04 月 4 日

确定谁有权限访问您的 AWS Secrets Manager 密钥

预设情况下，IAM 身份无权限访问密钥。授权访问密钥时，Secrets Manager 会评估密钥基于资源的策略以及发送请求的 IAM 用户或角色的所有身份策略。为此，Secrets Manager 使用与 IAM 用户指南中确定请求是允许还是拒绝中描述过程类似的过程。

多个策略应用于请求时，Secrets Manager 会使用层次结构控制权限：

1. 如果任何策略中具有显式表达式的语句与请求操作和资源 deny 匹配：

   显式表达式 deny 覆盖其他所有内容并阻止操作。
2. 如果没有显式表达式 deny，但带有显式表达式 allow 与请求操作和资源匹配：

   显式表达式 allow 授予请求中的操作访问语句中资源的权限。

   如果身份和密钥在两个不同的帐户中，在密钥资源策略和附加到身份的策略中必须有 allow，否则 AWS 拒绝该请求。有关更多信息，请参见 跨账户存取。
3. 如果没有带显式表达式 allow 与请求操作和资源相匹配：

   AWS 在预设情况下拒绝请求，称为隐式拒绝。

查看密钥基于资源的策略

- 请执行下列操作之一：
  - 在网址 https://console.aws.amazon.com/secretsmanager/ 上打开 Secrets Manager 控制台。在您的密钥详细信息页面中，在资源权限部分，选择编辑权限。
  - 使用 AWS CLI 调用 `get-resource-policy`，或者使用 AWS SDK 调用 `GetResourcePolicy`。

确定哪些人可以通过基于身份的策略进行访问

- 使用 IAM policy simulator。参见用 IAM policy simulator 测试 IAM 策略

从其他账户访问 AWS Secrets Manager 密钥

一个账户中的用户可以访问另一个账户中的密钥（跨账户访问），您必须允许在资源策略和身份策略中进行访问。这与授予密钥所在账户中的身份访问权限不同。

您还必须允许身份使用密钥加密的 KMS 密钥。这是因为您不能使用 AWS 托管式密钥 (aws/secretsmanager) 进行跨账户访问。相反，您必须使用您创建的 KMS 密钥加密密钥，然后随附密钥策略。创建 KMS 密钥需支付费用。要更改密钥的加密密钥，请参阅 the section called “修改密钥”。

下列示例策略假定您在 Account1 中有密钥和加密密钥，而在 Account2 的身份希望有访问密钥值的权限。

步骤 1：将资源策略附加到 Account1 中的密钥

- 以下策略允许*## 2 ApplicationRole*中访问*##* 1 中的密钥。要使用该策略，请参阅 the section called “将权限策略附加到密钥”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

步骤 2：将语句添加到 Account1 中 KMS 密钥的密钥策略中

- *############ 2 ApplicationRole##### 1 ## KMS ####### 1 #####*要使用此语句，请将其添加到 KMS 密钥的密钥策略中。有关更多信息，请参阅更改密钥政策。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*"
```

```
}
```

步骤 3：将身份策略附加到 Account2 中的身份

- *######## 2 ApplicationRole##### 1 ############ 1 ##############*要使用该策略，请参阅 the section called “将权限策略附加到身份”。您可以在 Secrets Manager 控制台的密钥详细信息页面的密钥 ARN 下方找到您的密钥 ARN。此外，您也可以调用 `describe-secret`。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "SecretARN"
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:Region:Account1:key/EncryptionKey"
    }
  ]
}
```

从本地环境访问密钥

您可以使用 Ro AWS Identity and Access Management les Anywhere 在 IAM 中为在外部运行的服务器、容器和应用程序等工作负载获取临时安全证书 AWS。您的工作负载可以使用与 AWS 应用程序相同的 IAM 策略和 IAM 角色来访问 AWS 资源。借助 IAM Role AWS s Anywhere，您可以使用 Secrets Manager 来存储和管理可由应用程序服务器等本地设备中的资源访问的证书。有关更多信息，请参阅 IAM Roles Anywhere 用户指南。

的权限策略示例 AWS Secrets Manager

权限策略是 JSON 结构化文本。参见 JSON 策略文档结构。

附加到资源和身份上的权限策略非常相似。在访问密钥的策略中的一些元素包括：

- `Principal`：授予访问权限的用户。参见 IAM 用户指南中的指定委托人。您在身份上附加策略时，策略中不会包含 `Principal` 元素。
- `Action`：他们可以做什么。请参阅 the section called “Secrets Manager 操作”。
- `Resource`：他们可以访问哪些密钥。请参阅 the section called “Secrets Manager 资源”。

  根据您附加的策略，通配符 (*) 具有不同的含义：

  - 在附加到密钥的策略中，* 表示该策略适用于此密钥。
  - 在附加到身份的策略中，* 表示该策略适用于账户中的所有资源（包括密钥）。

要将策略附加到密钥中，请参阅 the section called “将权限策略附加到密钥”。

要将策略附加到密钥中，请参阅 the section called “将权限策略附加到身份”。

主题

示例：检索单个秘密值的权限

要授予检索密钥值的权限，您可以将策略附加到密钥或身份上。要帮助确定使用的策略类型，请参阅基于身份的策略和基于资源的策略。有关如何附加策略的信息，请参阅 the section called “将权限策略附加到密钥” 和 the section called “将权限策略附加到身份”。

以下示例说明了授予对密钥访问权限的两种不同方式。第一个示例是您可以附加到密钥上的基于资源的策略。当您希望向多个用户或角色授予单个密钥的访问权限时，此示例非常有用。第二个示例是基于身份的策略，您可以将其附加到 IAM 中的用户或角色。当您希望授予对 IAM 组的访问权限时，此示例非

常有用。要授予在批处理 API 调用中检索一组秘密的权限，请参阅 the section called “示例：批量检索一组机密值的权限”。

Example 读取一个密钥（附加到一个密钥）

通过将以下策略附加到密钥，你可以授予密钥的访问权限。要使用该策略，请参阅 the section called “将权限策略附加到密钥”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/EC2RoleToAccessSecrets"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Example 读取使用客户自主管理型密钥加密的秘密（附加到身份）

如果使用客户管理的密钥对密钥进行加密，则可以通过将以下策略附加到身份来授予读取该密钥的访问权限。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "SecretARN"
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "KMSKeyARN"
    }
  ]
}
```

示例：读取和描述个人机密的权限

Example 阅读并描述一个秘密（附在身份上）

通过将以下策略附加到身份，您可以授予密钥的访问权限。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "secretsmanager:GetSecretValue",
          "secretsmanager:DescribeSecret"
          ],
        "Resource": "SecretARN"
      }
    ]
  }
```

示例：批量检索一组机密值的权限

Example 批量读取一组秘密（附加到身份）

您可以通过将以下策略附加到身份来授予在批处理 API 调用中检索一组秘密的访问权限。该策略对调用方进行了限制，因此即使批量调用包含其他秘密，它们也只能检索 *SecretARN1*、*SecretARN2* 和 *SecretARN3* 指定的秘密。如果调用方还在批处理 API 调用中请求其他秘密，则 Secrets Manager 将不会返回它们。有关更多信息，请参阅BatchGetSecretValue。 。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:BatchGetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "SecretARN1",
        "SecretARN2",
        "SecretARN3"
        ]
    }
  ]
}
```

示例：通配符

您可以使用通配符在策略元素中包含一组值。

Example 访问路径中的所有密钥（附加到身份）

以下策略授予检索名称以 “*TestEnv/*” 开头的所有密钥的权限。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:Region:AccountId:secret:TestEnv/*"
  }
}
```

Example 访问所有密钥的元数据（附加到身份）

以下策略授予 `DescribeSecret` 和权限开头为 `List`：`ListSecrets` 和 `ListSecretVersionIds`。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

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

```
    "Effect": "Allow",
    "Action": [
      "secretsmanager:DescribeSecret",
      "secretsmanager:List*"
    ],
    "Resource": "*"
  }
}
```

Example 匹配密钥名称（附加到身份）

以下策略按名称授予密钥的所有 Secrets Manager 权限。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

要匹配密钥名称，可以通过将区域、账户 ID、机密名称和通配符 (?) 放在一起来匹配单个随机字符，从而为密钥创建 ARN。Secrets Manager 会将六个随机字符附加到密钥名称作为 ARN 的一部分，因此您可以使用此通配符来匹配这些字符。如果使用 `"another_secret_name-*"` 语法，Secrets Manager 不仅匹配具有 6 个随机字符的预期密钥，而且还匹配 `"another_secret_name-<anything-here>a1b2c3"`。

因为除了 6 个随机字符外，您可以预测密钥的所有 ARN 部分，所以使用通配符 `'??????'` 语法，您能够安全地将权限授予给尚不存在的密钥。但要注意，如果删除密钥并以相同名称重新创建，即使 6 个字符发生变化，用户也会自动获得新密钥的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:Region:AccountId:secret:a_specific_secret_name-a1b2c3",
        "arn:aws:secretsmanager:Region:AccountId:secret:another_secret_name-??????"
      ]
    }
  ]
}
```

示例：创建密钥的权限

要为用户授予权限创建密钥，我们建议您将权限策略附加到用户所属的 IAM 组。请参阅 IAM 用户组。

Example 创建密钥（附加到身份）

以下策略授予创建密钥和查看密钥列表的权限。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*"
    }
  ]
}
```

示例：拒绝使用特定 AWS KMS 密钥来加密机密

> **Important**
>
> 要拒绝客户托管密钥，我们建议您使用密钥策略或密钥授予来限制访问权限。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》 AWS KMS中的身份验证和访问控制。

Example 拒绝 AWS 托管密钥**aws/secretsmanager**（附加到身份）

以下策略说明如何拒绝使用 AWS 托管密钥aws/secretsmanager来创建或更新密钥。这意味着必须使用客户管理的密钥对机密进行加密。如果aws/secretsmanager密钥存在，则还必须包括其密钥 ID。您还需要添加空字符串，因为 Secrets Manager 将其解释为 AWS 托管密钥aws/secretsmanager。第二条语句拒绝创建不包含 KMS 密钥的密钥的请求，因为 Secrets Manager 将其解释为 AWS 托管密钥aws/secretsmanager。

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

```
            "Effect": "Deny",
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLikeIfExists": {
                    "secretsmanager:KmsKeyId": [
                        "*alias/aws/secretsmanager",
                        "*<key_ID_of_the_AWS_managed_key>",
                        ""
                    ]
                }
            }
        },
        {
            "Sid": "RequireKmsKeyIdParameterOnCreate",
            "Effect": "Deny",
            "Action": "secretsmanager:CreateSecret",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "secretsmanager:KmsKeyId": "true"
                }
            }
        }
    ]
}
```

示例：权限和 VPC

如果您需要在 VPC 内部访问 Secrets Manager，您可以通过在权限策略中包含条件来确保对 Secrets Manager 的请求来自 VPC。有关更多信息，请参阅 VPC 终端节点条件 和 VPC 端点。

请确保从其他 AWS 服务访问密钥的请求也来自 VPC，否则此策略将拒绝他们访问。

Example 请求应通过 VPC 终端节点（连接到密钥）

以下策略仅允许用户在请求通过 VPC 终端节点时执行 Secrets Manager 操作 *vpce-1234a5678b9012c*。要使用该策略，请参阅 the section called “将权限策略附加到密钥”。

```
{
```

```
  "Id": "example-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictGetSecretValueoperation",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1234a5678b9012c"
        }
      }
    }
  ]
}
```

Example 请求应来自 VPC（连接到密钥）

以下示例密钥策略仅允许来自 *vpc-12345678* 的命令创建和管理密钥。此外，只有在请求来自于 vpc-2b2b2b2b 时，该策略才允许使用访问密钥的加密值的操作。如果您在一个 VPC 中运行应用程序，但使用第二个隔离的 VPC 以提供管理功能，则可能会使用此类策略。要使用该策略，请参阅 the section called “将权限策略附加到密钥”。

```
{
  "Id": "example-policy-2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAdministrativeActionsfromONLYvpc-12345678",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "secretsmanager:Create*",
        "secretsmanager:Put*",
        "secretsmanager:Update*",
        "secretsmanager:Delete*",
        "secretsmanager:Restore*",
        "secretsmanager:RotateSecret",
        "secretsmanager:CancelRotate*",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-12345678"
        }
      }
    },
    {
      "Sid": "AllowSecretValueAccessfromONLYvpc-2b2b2b2b",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-2b2b2b2b"
        }
      }
    }
  ]
}
```

示例：使用标签控制对密钥的访问

您可以使用标签来控制对密钥的访问。使用标签控制权限在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。一种策略是将标签附加到密钥上，然后在密钥具有特定标签时向身份授予权限。

Example 允许访问带有特定标记的机密（附加到身份）

以下策略允许DescribeSecret使用密钥为 “” *ServerName*且值为 “*ServerABC*” 的标签的机密。要使用该策略，请参阅 the section called “将权限策略附加到身份”。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "secretsmanager:DescribeSecret",
    "Resource": "*",
```

```
    "Condition": {
      "StringEquals": {
        "secretsmanager:ResourceTag/ServerName": "ServerABC"
      }
    }
  }
}
```

示例：限制对标签与密钥标签匹配的标识的访问

一种策略是将标签附加到密钥和 IAM 身份上。然后，您可以创建权限策略，在身份的标签与密钥的标签匹配时允许操作。有关完整的教程，请参阅根据标签定义访问密钥的权限。

使用标签控制权限在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。有关更多信息，请参阅什么是适用于 AWS的 ABAC？

Example 允许访问与密钥具有相同标签的角色（附加到密钥）

仅当标签 *AccessProject* 对于密钥和角色具有相同的值时，以下策略才会向账户 *123456789012* 授予 GetSecretValue 权限。要使用该策略，请参阅 the section called “将权限策略附加到密钥”。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "123456789012"
    },
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AccessProject": "${ aws:PrincipalTag/AccessProject }"
      }
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
  }
}
```

示例：服务主体

如果附加到您的密钥的资源策略包含AWS 服务委托人，我们建议您使用 aws: SourceArn 和 aw s: SourceAccount 全局条件密钥。仅当请求是从另一项 AWS 服务发送到 Secrets Manager 时，ARN 和账户值才会包含在授权上下文中。这种条件的组合避免了潜在的混淆代理情况。

如果资源 ARN 包含资源策略中不允许使用的字符，则不能在 `aws:SourceArn` 条件键的值中使用该资源 ARN 。改为使用 `aws:SourceAccount` 条件键。有关更多信息，请参阅 IAM 要求。

在附加到机密的策略中，服务委托人通常不用作委托人，但有些 AWS 服务需要它。有关服务要求您附加到密钥的资源策略的信息，请参阅该服务的文档。

Example 允许服务使用服务主体访问密钥（附加到密钥）

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "service-name.amazonaws.com"
        ]
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:sourceArn": "arn:aws:service-name::123456789012:*"
        },
        "StringEquals": {
          "aws:sourceAccount": "123456789012"
        }
      }

    }
  ]
}
```

的权限参考 AWS Secrets Manager

要查看组成权限策略的元素，请参阅 JSON 策略文档结构和 IAM JSON 策略元素引用。

要开始编写您自己的权限策略，请参阅 the section called “权限策略示例”。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 Resource 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 Resource 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 Condition 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

Secrets Manager 操作

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
BatchGetSecretValue	授予检索密钥列表并进行解密的权限	列出			
CancelRotateSecret	授予权限以取消进行中的密钥轮换	写入	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
CreateSecret	授予权限以创建密钥，其中存储着可查询和轮换的加密数据	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:AddReplicaRegions secretsmanager:For	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				ceOverwriteReplicaSecret	
DeleteResourcePolicy	授予权限以删除附加到密钥的资源策略	权限管理	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
DeleteSecret	授予删除密钥的权限	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:Sec	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				retPrimaryRegion	
DescribeSecret	授予权限以检索密钥的元数据，但不包含加密数据	读取	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetRandomPassword	授予权限以生成随机字符串以用于创建密码	读取			
GetResourcePolicy	授予权限以获取附加到密钥的资源策略	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue	授予权限以检索和解密加密数据	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecretVersionIds	授予权限以列出可用的密钥版本	读取	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ListSecrets	授予权限以列出可用密钥	列出			
PutResourcePolicy	授予将资源策略附加到密钥的权限	权限管理	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	
PutSecretValue	授予权限以使用新的加密数据创建密钥的新版本	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	授予从复制中移除区域的权限	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ReplicateSecretToRegions	授予将现有密钥转换为多区域密钥并开始将该密钥复制到新区域列表的权限	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions secretsmanager:ForceOverwri	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				teReplicaSecret	
RestoreSecret	授予取消删除密钥的权限	写入	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RotateSecret	授予权限以启动轮换密钥	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:ModifyRotationRules	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:RotateImmediately	
StopReplicationToReplica	授予权限以从复制中删除密钥，并将该密钥提升为副本区域中的区域密钥	写入	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
TagResource	授予权限以将标签添加至密钥	标记	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UntagResource	授予权限以从密钥中删除标签	标记	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
UpdateSecret	授予权限以使用新的元数据或新版本的加密数据更新密钥	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
	授予权限以将阶段从一个密钥移动到另一个密钥	写入	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateSecretVersionStage				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
ValidateResourcePolicy	授予在附加策略之前验证资源策略的权限	权限管理	Secret*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Secrets Manager 资源

资源类型	ARN	条件键
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey}

资源类型	ARN	条件键
		aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn

Secrets Manager 在密钥名称末尾附加破折号和 6 个随机字母数字字符以构建密钥 ARN 的最后一部分。如果删除一个密钥，然后重新创建另一个同名密钥，该格式有助于确保具有原始密钥权限的个人不会自动获得新密钥的访问权限，因为 Secrets Manager 生成 6 个新的随机字符。

您可以在Secrets Manager 控制台的密钥详细信息页面上或 `DescribeSecret` 找到密钥的 ARN。

条件键

如果您将下表中的字符串条件包含在权限策略中，则 Secrets Manager 的调用者必须传递匹配参数，否则他们将被拒绝访问。为了避免由于缺少参数而拒绝调用者，请将 `IfExists` 添加到条件运算符名称（例如 `StringLikeIfExists`）的末尾。有关更多信息，请参阅 IAM JSON 策略元素：条件运算符。

条件键	描述	类型
aws:RequestTag/${TagKey}	根据用户向 Secrets Manager 服务发出的请求中的键筛选访问权限	String
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	String
aws:TagKeys	根据用户向 Secrets Manager 服务发出的请求中存在的所有标签键名称的列表筛选访问权限	ArrayOfString

条件键	描述	类型
secretsmanager:AddReplicaRegions	按要复制密钥的区域列表筛选访问权限	ArrayOfString
secretsmanager:BlockPublicPolicy	根据资源策略是否阻止广泛访问来筛选 AWS 账户 访问权限	布尔型
secretsmanager:Description	根据请求中的描述文本筛选访问权限	String
secretsmanager:ForceDeleteWithoutRecovery	按是否在没有任何恢复时段的情况下立即删除密钥以筛选访问权限	布尔型
secretsmanager:ForceOverwriteReplicaSecret	根据是否覆盖目标区域中具有相同名称的密钥来筛选访问权限	布尔型
secretsmanager:KmsKeyId	根据请求中的 KMS 密钥的 ARN 筛选访问权限	String
secretsmanager:ModifyRotationRules	按是否需要修改密钥轮换规则来筛选访问权限	布尔型
secretsmanager:Name	根据请求中易于识别的密钥名称筛选访问权限	String
secretsmanager:RecoveryWindowInDays	按 Secrets Manager 在删除密钥之前可以等待的天数筛选访问权限	数值

条件键	描述	类型
secretsmanager:ResourceTag/tag-key	按标签键值对筛选访问	String
secretsmanager:RotateImmediately	按是否需要立即轮换密钥来筛选访问权限	布尔型
secretsmanager:RotationLambdaARN	根据请求中轮换 Lambda 函数的 ARN 筛选访问权限	ARN
secretsmanager:SecretId	根据请求中的 SecretID 值筛选访问权限	ARN
secretsmanager:SecretPrimaryRegion	按创建密钥的主要区域筛选访问权限	String
secretsmanager:VersionId	根据请求中密钥版本的唯一标识符筛选访问权限	String
secretsmanager:VersionStage	根据请求中的版本阶段列表筛选访问权限	String
secretsmanager:resource/AllowRotationLambdaArn	根据与密钥关联的轮换 Lambda 函数的 ARN 筛选访问权限	ARN

使用 BlockPublicPolicy 条件阻止对密钥的广泛访问

在允许操作 PutResourcePolicy 的身份策略中，我们建议您使用 BlockPublicPolicy: true。这种情况意味着只有在策略不允许广泛访问的情况下，用户才能将资源策略附加到密钥。

Secrets Manager 使用 Zelkova 自动推理来分析资源策略，以确定是否存在宽泛访问权限问题。有关 Zelkova 的更多信息，请参阅安全博客上的 “如何 AWS 使用自动推理来帮助您实现大规模 AWS 安全”。

以下示例显示了如何使用 BlockPublicPolicy。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "secretsmanager:PutResourcePolicy",
        "Resource": "SecretId",
        "Condition": {
            "Bool": {
                "secretsmanager:BlockPublicPolicy": "true"
            }
        }
    }
}
```

IP 地址条件

在允许或拒绝访问 Secrets Manager 的策略语句中指定 IP 地址条件运算符或 aws:SourceIp 条件键时，请务必小心。例如，如果您将限制对来自公司网络 IP 地址范围的请求 AWS 执行操作的策略附加到密钥，则您作为 IAM 用户从公司网络调用请求的请求将按预期工作。但是，如果您允许其他服务代表您访问密钥，例如使用 Lambda 函数启用轮换，则该函数会从 AWS内部地址空间调用 Secrets Manager 操作。受该策略影响并使用 IP 地址筛选器的请求将会失败。

此外，当请求来自 Amazon VPC 终端节点时，aws:sourceIP 条件键也不起作用。要限制对特定 VPC 终端节点的请求，请使用 the section called “VPC 终端节点条件”。

VPC 终端节点条件

要允许或拒绝对来自特定 VPC 或 VPC 终端节点的请求的访问，请使用 aws:SourceVpc 来限制对来自指定 VPC 的请求的访问，或 aws:SourceVpce 来限制对来自指定 VPC 终端节点的请求的访问。请参阅 the section called “示例：权限和 VPC”。

- `aws:SourceVpc` 将访问限制为来自指定 VPC 的请求。
- `aws:SourceVpce` 将访问限制为来自指定 VPC 终端节点的请求。

如果在允许或拒绝访问 Secrets Manager 密钥的资源策略语句中使用这些条件键，可能会无意中拒绝访问代表您使用 Secrets Manager 访问密钥的服务。只有部分 AWS 服务可以在您的 VPC 内使用终端节点运行。如果将密钥的请求限制为 VPC 或 VPC 终端节点，则从未针对该服务配置的服务中调用 Secrets Manager 可能会失败。

请参阅 VPC 端点。

使用创建和管理密钥 AWS Secrets Manager

秘密可以是密码、一组凭证（如用户名和密码）、OAuth 令牌或以加密形式存储在 Secrets Manager 中的其他秘密信息。

主题

创建 AWS Secrets Manager 数据库密钥

在 Amazon RDS、Amazon Aurora、Amazon Redshift 或 Amazon DocumentDB 中创建用户后，您可以按照以下步骤将其凭证存储在 SSecrets Manager 中。使用 AWS CLI 或其中一个软件开发工具包存储密钥时，必须以正确的 JSON 结构提供密钥。当您使用控制台来存储某个数据库密钥时，Secrets Manager 会自动以正确的 JSON 结构创建该密钥。

> **Tip**
>
> 对于亚马逊 RDS 和 Amazon Redshift 管理员用户证书，我们建议您使用托管密钥。您可以通过管理服务创建托管密钥，然后可以使用托管轮换。

当存储复制到其他区域的源数据库的数据库凭证时，密钥将包含源数据库的连接信息。然后复制密钥时，副本将是源密钥的副本，并且包含相同的连接信息。您可以在密钥中添加其他键值对以记录区域连接信息。

要创建密钥，您需要获得授予的权限SecretsManagerReadWriteAWS 托管策略。

当你创建密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

创建密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于 Secret type（密钥类型）中，请选择要存储的数据库凭证类型：
      - Amazon RDS 数据库（包括 Aurora）
      - Amazon DocumentDB 数据库
      - 亚马逊 Redshift 数据仓库
   b. 对于 Credentials（凭证），请输入数据库的凭证。
   c. 对于加密密钥，选择 Secrets Manager 用来加密密钥值的。 AWS KMS key 有关更多信息，请参阅 密钥加密和解密。
      - 在大多数情况下，请选择 aws/secretsmanager 以将 AWS 托管式密钥 用于 Secrets Manager。使用此密钥不产生任何费用。
      - 如果您需要从其他密钥访问密钥 AWS 账户，或者想要使用自己的 KMS 密钥以便轮换密钥或对其应用密钥策略，请从列表中选择客户托管密钥或选择添加新密钥来创建一个。有关使用客户托管密钥的成本的信息，请参阅 定价。

        您必须具有 the section called “KMS 密钥的权限”。有关跨账户访问的更多信息，请参阅the section called “跨账户存取”。
   d. 对于 Database（数据库），请选择您的数据库。
   e. 选择下一步。
4. 在 Configure secret（配置密钥）页面上，执行以下操作：
   a. 输入一个描述性的 Secret name（密钥名称）和 Description（说明）。密钥名称必须包含 1-512 个 Unicode 字符。

b. （可选）在标签部分中，在您的密钥中添加一个或多个标签。有关标记策略，请参阅 the section called “标记 密钥”。请不要将敏感信息存储在标签中，因为它们未加密。

c. （可选）在资源权限，要将资源策略添加到您的密钥中，请选择编辑权限。有关更多信息，请参阅 the section called “将权限策略附加到密钥”。

d. （可选）在复制密钥中，要将您的密钥复制到另一个密钥 AWS 区域，请选择复制密钥。您可以现在复制密钥，也可以回头再复制。有关更多信息，请参阅 跨区域复制密钥。

e. 选择 下一步。

5. （可选）在 Configure rotation（配置轮换）页面上，您可以启用自动轮换。您也可以现在保持关闭轮换，然后稍后将其打开。有关更多信息，请参阅 轮换 密钥。选择 下一步。

6. 在 Review (审核) 页上，审核您的密钥详细信息，然后选择 Store (存储)。

   Secrets Manager 将返回到密钥列表。如果您的新密钥未显示，请选择 Refresh（刷新）按钮。

AWS CLI

当您在命令 shell 中输入命令时，存在访问命令历史记录或实用程序可以访问您命令参数的风险。请参阅 the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

Example 根据 JSON 文件中的凭证创建密钥

以下 `create-secret` 示例将根据文件中的凭证创建密钥。有关更多信息，请参阅《AWS CLI 用户指南》中的从文件加载 AWS CLI 参数。

要使 Secrets Manager 能够轮换密钥，您必须确保 JSON 符合密钥的 JSON 结构。

```
aws secretsmanager create-secret \
    --name MyTestSecret \
    --secret-string file://mycreds.json
```

mycreds.json 的内容：

```
{
    "engine": "mysql",
    "username": "saanvis",
    "password": "EXAMPLE-PASSWORD",
    "host": "my-database-endpoint.us-west-2.rds.amazonaws.com",
    "dbname": "myDatabase",
    "port": "3306"
```

```
}
```

AWS SDK

要使用其中一个 AWS SDK 创建密钥，请使用`CreateSecret`操作。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

AWS Secrets Manager 密钥的 JSON 结构

您可以在 Secrets Manager 密钥中存储任何文本或二进制数据。如果要为 Secrets Manager 密钥启用自动轮换，则它必须使用正确的 JSON 结构。在轮替期间，Secrets Manager 会使用密钥中的信息连接到凭证源并更新其中的凭证。JSON 密钥名称区分大小写。

请注意，当您使用控制台来存储某个数据库密钥时，Secrets Manager 会自动以正确的 JSON 结构创建该密钥。

您可以向密钥添加更多键值对（例如在数据库密钥中），以包含其他区域中副本数据库的连接信息。

主题

- Amazon RDS Db2 秘密结构
- Amazon RDS MariaDB 密钥结构
- Amazon RDS 和 Amazon Aurora MySQL 秘密结构
- Amazon RDS Oracle 密钥结构
- Amazon RDS 和 Amazon Aurora PostgreSQL 秘密结构
- Amazon RDS Microsoft SQLServer 密钥结构
- Amazon DocumentDB 密钥结构
- Amazon Redshift 密钥结构
- 亚马逊 Redshift 无服务器秘密结构
- 亚马逊的 ElastiCache 秘密结构
- 活动目录的秘密结构

Amazon RDS Db2 秘密结构

对于 Amazon RDS Db2 实例，由于用户无法更改自己的密码，因此您必须在单独的秘密中提供管理员凭证。

```
{
  "engine": "db2",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 3306>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

Amazon RDS MariaDB 密钥结构

```
{
  "engine": "mariadb",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 3306>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "mariadb",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 3306>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

Amazon RDS 和 Amazon Aurora MySQL 秘密结构

```
{
  "engine": "mysql",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
```

```
  "port": <TCP port number. If not specified, defaults to 3306>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "mysql",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 3306>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

Amazon RDS Oracle 密钥结构

```
{
  "engine": "oracle",
  "host": "<required: instance host name/resolvable DNS name>",
  "username": "<required: username>",
  "password": "<required: password>",
  "dbname": "<required: database name>",
  "port": <optional: TCP port number. If not specified, defaults to 1521>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "oracle",
  "host": "<required: instance host name/resolvable DNS name>",
  "username": "<required: username>",
  "password": "<required: password>",
  "dbname": "<required: database name>",
  "port": <optional: TCP port number. If not specified, defaults to 1521>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

Amazon RDS 和 Amazon Aurora PostgreSQL 秘密结构

```
{
```

```
  "engine": "postgres",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to 'postgres'>",
  "port": <TCP port number. If not specified, defaults to 5432>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "postgres",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to 'postgres'>",
  "port": <TCP port number. If not specified, defaults to 5432>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

Amazon RDS Microsoft SQLServer 密钥结构

```
{
  "engine": "sqlserver",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to 'master'>",
  "port": <TCP port number. If not specified, defaults to 1433>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "sqlserver",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to 'master'>",
  "port": <TCP port number. If not specified, defaults to 1433>,
  "masterarn": "<the ARN of the elevated secret>"
```

```
}
```

Amazon DocumentDB 密钥结构

```
{
  "engine": "mongo",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 27017>,
  "ssl": <true|false. If not specified, defaults to false>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "mongo",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 27017>,
  "masterarn": "<the ARN of the elevated secret>",
  "ssl": <true|false. If not specified, defaults to false>
}
```

Amazon Redshift 密钥结构

```
{
  "engine": "redshift",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 5439>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
```

```
  "engine": "redshift",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "port": <TCP port number. If not specified, defaults to 5439>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

亚马逊 Redshift 无服务器秘密结构

```
{
  "engine": "redshift",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "namespaceName": <namespace name>,
  "port": <TCP port number. If not specified, defaults to 5439>
}
```

要使用the section called “交替用户”，您需要masterarn为包含管理员或超级用户凭据的密钥添加。

```
{
  "engine": "redshift",
  "host": "<instance host name/resolvable DNS name>",
  "username": "<username>",
  "password": "<password>",
  "dbname": "<database name. If not specified, defaults to None>",
  "namespaceName": <namespace name>,
  "port": <TCP port number. If not specified, defaults to 5439>,
  "masterarn": "<the ARN of the elevated secret>"
}
```

亚马逊的 ElastiCache 秘密结构

```
{
  "password": "<password>",
  "username": "<username>"
  "user_arn": "ARN of the Amazon EC2 user"
}
```

有关更多信息，请参阅 Amazon 用户指南中的自动轮换 ElastiCache 用户密码。

活动目录的秘密结构

AWS Directory Service 使用密钥存储活动目录凭证。有关更多信息，请参阅《AWS Directory Service 管理指南》中的 “将 Amazon EC2 Linux 实例无缝加入您的托管 AD 活动目录”。无缝加入域名需要以下示例中的密钥名称。如果您不使用无缝域加入，则可以使用环境变量更改密钥的名称，如轮换函数模板代码中所述。

要轮换 Active Directory 密钥，您可以使用活动目录轮换模板。

活动目录凭证秘密结构

```
{
  "awsSeamlessDomainUsername": "<username>",
  "awsSeamlessDomainPassword": "<password>"
}
```

如果要轮换密钥，则需要包括域名目录 ID。

```
{
  "awsSeamlessDomainDirectoryId": "d-12345abc6e",
  "awsSeamlessDomainUsername": "<username>",
  "awsSeamlessDomainPassword": "<password>"
}
```

如果将该密钥与包含密钥表的密钥结合使用，则需要包含密钥表密钥 ARN。

```
{
  "awsSeamlessDomainDirectoryId": "d-12345abc6e",
  "awsSeamlessDomainUsername": "<username>",
  "awsSeamlessDomainPassword": "<password>",
  "directoryServiceSecretVersion": 1,
  "schemaVersion": "1.0",
  "keytabArns": [
    "<ARN of child keytab secret 1>,
    "<ARN of child keytab secret 2>,
    "<ARN of child keytab secret 3>,
  ],
  "lastModifiedDateTime": "2021-07-19 17:06:58"
}
```

活动目录密钥表密钥结构

有关使用密钥表文件对 Amazon EC2 上的活动目录账户进行身份验证的信息，请参阅在 Amazon Linux 2 上使用 SQL Server 2017 部署和配置活动目录身份验证。

```
{
  "awsSeamlessDomainDirectoryId": "d-12345abc6e",
  "schemaVersion": "1.0",
  "name": "< name>",
  "principals": [
    "aduser@MY.EXAMPLE.COM",
    "MSSQLSvc/test:1433@MY.EXAMPLE.COM"
  ],
  "keytabContents": "<keytab>",
  "parentSecretArn": "<ARN of parent secret>",
  "lastModifiedDateTime": "2021-07-19 17:06:58"
  "version": 1
}
```

创建密 AWS Secrets Manager 钥

要在 Secrets Manager 中存储 API 密钥、访问令牌、非用于数据库的凭证以及其他密钥，请按照以下步骤操作。对于 Amazon ElastiCache 密钥，如果您想启用轮换，则必须将该密钥存储在预期的 JSON 结构中。

要创建密钥，您需要获得授予的权限SecretsManagerReadWriteAWS 托管策略。

当你创建密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

创建密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 选择 存储新密钥。
3. 在 Choose secret type（选择密钥类型）页面上，执行以下操作：
   a. 对于密钥类型，请选择其他密钥类型。
   b. 在键值对中，请以 JSON 键值对格式输入密钥，或者选择明文选项卡，然后以任何格式输入密钥。您可以在密钥中存储最多 65536 个字节。一些示例：

API 密钥键值对：

ClientID：*my_client_id*

ClientSecret：*wjalrxutnfemi/k7mdeng/ cyexampleK bPxRfi* EY

凭证键值对：

Username：*saanvis*

Password：*EXAMPLE-PASSWORD*

OAuth 令牌明文：

AKIAI44QH8DHBEXAMPLE

数字证书明文：

```
-----BEGIN CERTIFICATE-----
EXAMPLE
-----END CERTIFICATE-----
```

私有密钥明文：

```
----BEGIN PRIVATE KEY ---
EXAMPLE
---- END PRIVATE KEY ----
```

c. 对于加密密钥，选择 Secrets Manager 用来加密密钥值的。 AWS KMS key 有关更多信息，请参阅 密钥加密和解密。

- 在大多数情况下，请选择 aws/secretsmanager 以将 AWS 托管式密钥 用于 Secrets Manager。使用此密钥不产生任何费用。
- 如果您需要从其他密钥访问密钥 AWS 账户，或者想要使用自己的 KMS 密钥以便轮换密钥或对其应用密钥策略，请从列表中选择客户托管密钥或选择添加新密钥来创建一个。有关使用客户托管密钥的成本的信息，请参阅 定价。

  您必须具有 the section called “KMS 密钥的权限”。有关跨账户访问的更多信息，请参阅the section called “跨账户存取”。

d. 选择下一步。

4. 在 Configure secret（配置密钥）页面上，执行以下操作：

   a. 输入一个描述性的 Secret name（密钥名称）和 Description（说明）。密钥名称必须包含 1-512 个 Unicode 字符。

   b. （可选）在标签部分中，在您的密钥中添加一个或多个标签。有关标记策略，请参阅 the section called “标记 密钥”。请不要将敏感信息存储在标签中，因为它们未加密。

   c. （可选）在资源权限，要将资源策略添加到您的密钥中，请选择编辑权限。有关更多信息，请参阅 the section called “将权限策略附加到密钥”。

   d. （可选）在复制密钥中，要将您的密钥复制到另一个密钥 AWS 区域，请选择复制密钥。您可以现在复制密钥，也可以回头再复制。有关更多信息，请参阅 跨区域复制密钥。

   e. 选择 下一步。

5. （可选）在 Configure rotation（配置轮换）页面上，您可以启用自动轮换。您也可以现在保持关闭轮换，然后稍后将其打开。有关更多信息，请参阅 轮换 密钥。选择 下一步。

6. 在 Review (审核) 页上，审核您的密钥详细信息，然后选择 Store (存储)。

   Secrets Manager 将返回到密钥列表。如果您的新密钥未显示，请选择 Refresh（刷新）按钮。

AWS CLI

当您在命令 shell 中输入命令时，存在访问命令历史记录或实用程序可以访问您命令参数的风险。请参阅 the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

Example 创建密钥

以下 `create-secret` 示例将创建包含两个键值对的密钥。

```
aws secretsmanager create-secret \
    --name MyTestSecret \
    --description "My test secret created with the CLI." \
    --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
```

Example 根据 JSON 文件中的凭证创建密钥

以下 `create-secret` 示例将根据文件中的凭证创建密钥。有关更多信息，请参阅《 AWS CLI 用户指南》中的从文件加载 AWS CLI 参数。

```
aws secretsmanager create-secret \
```

```
    --name MyTestSecret \
    --secret-string file://mycreds.json
```

mycreds.json 的内容：

```
{
    "username": "diegor",
    "password": "EXAMPLE-PASSWORD"
}
```

AWS SDK

要使用其中一个 AWS SDK 创建密钥，请使用`CreateSecret`操作。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

更新 AWS Secrets Manager 秘密的值

要更新您的秘密值，可以使用控制台、CLI 或 SDK。当您更新秘密值时，Secrets Manager 会使用暂存标签 `AWSCURRENT` 创建秘密的新版本。您仍然可以访问带有标签 `AWSPREVIOUS` 的旧版本。您也可以添加自己的标签。有关更多信息，请参阅 Secrets Manager 版本控制。

更新秘密值（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。
3. 进入密钥详细信息页面后，在概述选项卡中的密钥值部分，选择检索秘密值，然后选择编辑。

AWS CLI

更新秘密值 (AWS CLI)

- 当您在命令 shell 中输入命令时，存在访问命令历史记录或实用程序可以访问您命令参数的风险。请参阅the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

  以下 `put-secret-value` 将创建包含两个键值对的新版本密钥。

  ```
  aws secretsmanager put-secret-value \
  ```

```
      --secret-id MyTestSecret \
      --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
```

以下 put-secret-value 创建了一个带有自定义暂存标签的新版本。新版本将带有标签 MyLabel 和 AWSCURRENT。

```
aws secretsmanager put-secret-value \
      --secret-id MyTestSecret \
      --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
      --version-stages "MyLabel"
```

AWS SDK

我们建议您避免调用 PutSecretValue 或者 UpdateSecret 以持续速度为每 10 分钟一次以上。如果调用 PutSecretValue 或 UpdateSecret 更新密钥值，Secrets Manager 将创建密钥的新版本。当版本超过 100 个时，Secrets Manager 会删除未标记的版本，但不会删除 24 小时内创建的版本。如果每 10 分钟更新一次密钥值，则创建的版本多于 Secrets Manager 删除的版本，将达到密钥版本的配额。

要更新秘密值，请使用以下操作：UpdateSecret 或 PutSecretValue。有关更多信息，请参阅the section called “AWS 软件开发工具包”。

使用 Secrets Manager 生成密码

使用 Secrets Manager 的常见模式是在 Secrets Manager 中生成密码，然后在数据库或服务中使用该密码。您可以使用以下方法执行此操作：

- AWS CloudFormation — 请参阅AWS CloudFormation。
- AWS CLI — 请参阅get-random-password。
- AWS 软件开发工具包 — 请参阅GetRandomPassword。

将密钥回滚到之前的版本

您可以通过使用移动附加到密钥版本的标签，将密钥还原为先前版本 AWS CLI。有关 Secrets Manager 如何存储密钥版本的信息，请参阅the section called “秘密版本”。

以下update-secret-version-stage示例将 AWSCURRENT 暂存标签移动到密钥的先前版本，这会将密钥还原为先前的版本。要查找先前版本的 ID，请在 Secrets Manager 控制台中使用list-secret-version-ids或查看版本。

在本示例中，带有标签的版本是 a1b2c3d4-5678-90ab-CDEF-example11111，带有 AWSCURRENT 标签的版本是 a1b2c3d4-5678-90ab-cdef-example22222。 AWSPREVIOUS 在本示例中，您将 AWSCURRENT 标签从版本 11111 移动到 22222。由于 AWSCURRENT 标签已从版本中移除，因此update-secret-version-stage会自动将 AWSPREVIOUS 标签移至该版本 (11111)。结果是 AWSCURRENT 和 AWSPREVIOUS 版本被交换了。

```
aws secretsmanager update-secret-version-stage \
  --secret-id MyTestSecret \
  --version-stage AWSCURRENT \
  --move-to-version-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --remove-from-version-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

更改密钥的加密 AWS Secrets Manager 密钥

Secrets Manager 使用带有 AWS KMS 密钥和数据密钥的信封加密来保护每个密钥值。对于每个秘密，您可以选择要使用的 KMS 密钥。你可以使用 AWS 托管式密钥 aws/secretsManager，也可以使用客户管理的密钥。大多数情况下，建议使用 aws/secretsmanager，并且使用它不产生任何成本。如果您需要从其他人访问密钥 AWS 账户，或者您想使用自己的 KMS 密钥以便轮换密钥或对其应用密钥策略，请使用 客户托管式密钥。您必须具有 the section called “KMS 密钥的权限”。有关使用客户托管密钥的成本的信息，请参阅 定价。

您可以更改秘密的加密密钥。例如，如果您想从其他账户访问密钥，并且该密钥当前已使用 AWS 托管密钥进行加密aws/secretsmanager，则可以切换到 客户托管式密钥。

> **Tip**
>
> 如果您想轮换 客户托管式密钥，我们建议使用 AWS KMS 自动密钥轮换。有关更多信息，请参阅轮换 AWS KMS 密钥。

当您更改加密密钥时，Secrets Manager 会使用新密钥重新加密AWSCURRENTAWSPENDING、和AWSPREVIOUS版本。为了避免将您锁定在密钥之外，Secrets Manager 会使用以前的密钥对所有现有版本进行加密。这意味着您可以使用先前的密钥或新密钥解密AWSCURRENTAWSPENDING、和AWSPREVIOUS版本。

要使其AWSCURRENT只能通过新的加密密钥解密，请使用新密钥创建新版本的密钥。然后，为了能够解AWSCURRENT密密密钥的版本，您必须拥有新密钥的权限。

如果停用以前的加密密钥，则除了 AWSCURRENT、AWSPENDING 和 AWSPREVIOUS 之外，您将无法解密任何秘密版本。如果想要保留对其他标有标签的秘密版本的访问权限，则需要使用 the section called “AWS CLI” 通过新的加密密钥重新创建这些版本。

更改秘密的加密密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。
3. 在秘密详细信息页面上的秘密详细信息部分中，选择操作，然后选择编辑加密密钥。

AWS CLI

如果更改秘密的加密密钥，然后停用了以前的加密密钥，则除了 AWSCURRENT、AWSPENDING 和 AWSPREVIOUS 之外，您将无法解密任何秘密版本。如果想要保留对其他标有标签的秘密版本的访问权限，则需要使用 the section called “AWS CLI” 通过新的加密密钥重新创建这些版本。

更改秘密的加密密钥 (AWS CLI)

1. 以下 `update-secret` 示例将更新用于加密密钥值的 KMS 密钥。该 KMS 密钥必须与加密密钥位于同一区域中。

```
aws secretsmanager update-secret \
      --secret-id MyTestSecret \
      --kms-key-id arn:aws:kms:us-west-2:123456789012:key/EXAMPLE1-90ab-cdef-fedc-
ba987EXAMPLE
```

2. （可选）如果您的秘密版本带有自定义标签，则要使用新密钥对其重新加密，则必须重新创建这些版本。

   当您在命令 shell 中输入命令时，存在访问命令历史记录或实用程序可以访问您命令参数的风险。请参阅 the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

   a. 获取秘密版本的值。

```
aws secretsmanager get-secret-value \
      --secret-id MyTestSecret \
```

```
    --version-stage MyCustomLabel
```

记下秘密值。

b. 创建具有该值的新版本。

```
aws secretsmanager put-secret-value \
    --secret-id testDescriptionUpdate \
    --secret-string "SecretValue" \
    --version-stages "MyCustomLabel"
```

修改密 AWS Secrets Manager 钥

您可以在创建密钥后修改其元数据，具体取决于密钥的创建者。对于由其他服务创建的密钥，您可能需要使用其他服务来更新或轮换它。

要确定谁管理密钥，您可以查看密钥名称。由其他服务管理的密钥以该服务的 ID 作为前缀。或者，在中 AWS CLI，调用 d escribe-secret，然后查看该字段。OwningService有关更多信息，请参阅 托管密钥。

对于您管理的密钥，您可以修改密钥的描述、基于资源的策略、加密密钥和标记。您还可以更改加密密钥值信息，但我们建议您轮换更新包含凭证的密钥值。轮换会更新 Secrets Manager 中的密钥以及数据库或服务上的凭据。这会自动保持同步这些密钥，以便在客户端请求密钥值时，始终检索一组正常工作的凭证。有关更多信息，请参阅 轮换 密钥。

当你修改密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

更新您管理的密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。
3. 在密钥详细信息页面上，执行以下操作之一：

   请注意，您无法更改 ARN 或密钥的名称。

   - 要更新描述，在密钥详细信息部分中，选择操作，然后选择编辑描述。
   - 要更新加密密钥，请参阅 the section called “更改秘密的加密密钥”。
   - 要更新标签，请在标签选项卡中，选择编辑标签。请参阅 the section called “标记 密钥”。

- 要更新秘密值，请参阅 the section called “更新秘密值”。
- 要更新密钥的权限，请在概述选项卡中选择编辑权限。请参阅 the section called “将权限策略附加到密钥”。

- 要更新密钥的轮换，请在轮换选项中选择编辑轮换。请参阅 轮换 密钥。
- 要将您的密钥复制到其他区域，请参阅 跨区域复制密钥。
- 如果您的密钥有副本，则您可以更改副本的加密密钥。在复制选项卡中，选择副本对应的单选按钮，然后在操作菜单中，选择编辑加密密钥。请参阅 the section called “密钥加密和解密”。
- 若要更改密钥以使其由其他服务管理，您需要在该服务中重新创建密钥。请参阅 托管密钥。

AWS CLI

Example 更新密钥说明

以下 `update-secret` 示例将更新密钥的描述。

```
aws secretsmanager update-secret \
    --secret-id MyTestSecret \
    --description "This is a new description for the secret."
```

AWS SDK

我们建议您避免以超过每 10 分钟一次的速率持续调用 `PutSecretValue` 或 `UpdateSecret`。如果调用 `PutSecretValue` 或 `UpdateSecret` 更新密钥值，Secrets Manager 将创建密钥的新版本。当版本超过 100 个时，Secrets Manager 会删除未标记的版本，但不会删除 24 小时内创建的版本。如果每 10 分钟更新一次密钥值，则创建的版本多于 Secrets Manager 删除的版本，将达到密钥版本的配额。

要更新秘密，请使用以下操作：`UpdateSecret` 或 `ReplicateSecretToRegions`。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

在里面寻找秘密 AWS Secrets Manager

如果搜索密钥时未设置筛选条件，Secrets Manager 会匹配密钥名称、描述、标签键和标签值中的关键字。未设置筛选条件的搜索不区分大小写，忽略空格、/、_、=、# 等特殊字符，并且仅使用数字和字母进行搜索。在不使用筛选条件的情况下进行搜索时，Secrets Manager 会分析搜索字符串以将其转换为单独的单词。这些单词通过从大写到小写、从字母到数字或从数字/字母到标点符号的任何

更改来进行分隔。例如，输入搜索词 credsDatabase#892 将会搜索名称、描述和标签键和值中的 creds、Database 和 892。

当你列出密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

您可以将以下筛选条件应用到搜索：

名称

匹配密钥名称的开头；区分大小写。例如，名称：**Data** 会返回名为 DatabaseSecret 的密钥，不返回名为 databaseSecret 或 MyData 的密钥。

描述

匹配密钥描述中的单词，不区分大小写。例如，描述：**My Description** 会匹配具有以下描述的密钥：

- My Description
- my description
- My basic description
- Description of my secret

由... 管理

查找由外部服务管理的密钥 AWS，例如 CyberArk 或 HashiCorp。

拥有服务

匹配管理服务 ID 前缀的开头，不区分大小写。例如，**my-ser** 将服务管理的密钥与前缀 my-serv 和 my-service 进行匹配。有关更多信息，请参阅 托管密钥。

已复制的密钥

您可以筛选主密钥、副本密钥或未复制的密钥。

标签键

匹配标签键的开头；区分大小写。例如，标签键：**Prod** 会返回带标签 Production 和 Prod1 的密钥，不返回带标签 prod 或 1 Prod 的密钥。

标签值

匹配标签值的开头；区分大小写。例如，标签值：**Prod** 会返回带标签 Production 和 Prod1 的密钥，不返回带标签值 prod 或 1 Prod 的密钥。

Secrets Manager 是一种区域服务，仅返回选定区域内的密钥。

AWS CLI

Example 列出您账户中的密钥

以下 `list-secrets` 示例获取了您账户中的密钥列表。

```
aws secretsmanager list-secrets
```

Example 筛选您账户中的密钥列表

以下 `list-secrets` 示例将获取您的账户中名称包含 Test 的密钥列表。按名称筛选区分大小写。

```
aws secretsmanager list-secrets \
    --filter Key="name",Values="Test"
```

Example 查找由其他 AWS 服务管理的机密

以下 `list-secrets` 示例获取服务管理的密钥列表。按 ID 指定服务。有关更多信息，请参阅 托管密钥。

```
aws secretsmanager list-secrets --filter Key="owning-service",Values="<service ID
 prefix>"
```

AWS SDK

要使用其中一个 AWS SDK 查找机密，请使用`ListSecrets`。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

删除密 AWS Secrets Manager 钥

由于机密的关键性， AWS Secrets Manager 故意使删除机密变得困难。Secrets Manager 不会立即删除密钥。而是Secrets Manager 会立即使这些密钥无法访问，并计划在恢复时段（最少 为 7 天）后删除这些密钥。在恢复时段结束后，您才能恢复以前删除的密钥。标记为已删除的密钥不收取任何费用。

如果已将主密钥复制到其他区域，则无法将其删除。首先删除副本，然后删除主密钥。在您删除副本时，该副本会被立即删除。

您无法直接删除某个密钥版本，相反，您可以使用 AWS CLI 或 AWS SDK 从版本中移除所有暂存标签。这会将该版本标记为已弃用，并允许 Secrets Manager 在后台自动删除该版本。

如果您不知道应用程序是否仍在使用密钥，则可以创建一个 Amazon CloudWatch 警报，提醒您在恢复时段内有人尝试访问密钥。有关更多信息，请参阅 监控计划删除的 AWS Secrets Manager 密钥何时被访问。

要删除密钥，您必须具有 `secretsmanager:ListSecrets` 和 `secretsmanager:DeleteSecret` 权限。

当您删除密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

删除密钥 (控制台)

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 在密钥列表中，选择要删除的密钥。
3. 在密钥详细信息部分中，选择操作，然后选择编辑描述。
4. 在禁用密钥和计划删除对话框中，在等待时间下，输入永久删除之前等待的天数。Secrets Manager 附加一个名为 `DeletionDate` 的字段，并将其设置为当前日期和时间加上为恢复时段指定的天数。
5. 选择计划删除。

查看已删除的密钥

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 在密钥页面上，选择偏好
   (
)。
3. 在“首选项”对话框中，选择显示计划删除的密钥，然后选择保存。

删除副本密钥

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择主密钥。
3. 在复制密钥密钥部分，选择副本密钥。
4. 从 Actions (操作) 菜单中选择 Delete Stack (删除副本)。

AWS CLI

Example 删除密钥

以下 delete-secret 示例将删除密钥。您可以在 DeletionDate 响应字段中的日期和时间restore-secret之前恢复密钥。要删除复制到其他区域的密钥，请先使用 remove-regions-from-replication 删除其副本，然后调用 delete-secret。

```
aws secretsmanager delete-secret \
    --secret-id MyTestSecret \
    --recovery-window-in-days 7
```

Example 立即删除密钥

以下 delete-secret 示例将立即删除密钥而没有恢复时段。您无法恢复此密钥。

```
aws secretsmanager delete-secret \
    --secret-id MyTestSecret \
    --force-delete-without-recovery
```

Example 删除副本密钥

以下 remove-regions-from-replication 示例将删除 eu-west-3 中的副本密钥。要删除复制到其他区域的主密钥，请先删除副本，然后调用 delete-secret。

```
aws secretsmanager remove-regions-from-replication \
    --secret-id MyTestSecret \
    --remove-replica-regions eu-west-3
```

AWS SDK

要删除密钥，请使用 DeleteSecret 命令。要删除密钥版本，请使用 UpdateSecretVersionStage 命令。要删除副本，请使用 StopReplicationToReplica 命令。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

恢复密 AWS Secrets Manager 钥

Secrets Manager 将计划删除的密钥视为已弃用，而不再直接访问该密钥。在恢复时段过后，Secrets Manager 将永久删除该密钥。在 Secrets Manager 删除密钥后，您无法恢复该密钥。在恢复时段结束

之前，您可以恢复密钥并再次使其可进行访问。这会删除 DeletionDate 字段，从而取消计划的永久删除。

要在控制台中恢复密钥和元数据，您必须具有 secretsmanager:ListSecrets 和 secretsmanager:RestoreSecret 权限：

当您恢复密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

要恢复密钥（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 在密钥列表中，选择要恢复的密钥名称。

   如果密钥列表中未显示删除的密钥，请选择偏好
   ( )。
   在“首选项”对话框中，选择显示计划删除的密钥，然后选择保存。
3. 在密钥详细信息部分中，选择取消删除。
4. 在取消密钥删除确认对话框中，选择取消删除。

AWS CLI

Example 恢复之前删除的密钥

以下 restore-secret 示例恢复了先前计划删除的密钥。

```
aws secretsmanager restore-secret \
    --secret-id MyTestSecret
```

AWS SDK

要恢复标记删除的密钥，请使用 RestoreSecret 命令。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

标记 AWS Secrets Manager 密钥

Secrets Manager 将标签定义为由您定义的密钥和可选值组成的标注。您可以使用标签来轻松管理、搜索和筛选 AWS 账户中的密钥和其他资源。标记密钥时，请在所有资源中使用标准命名方案。有关更多信息，请参阅 Tagging Best Practices（标记最佳实践）白皮书。

您可以检查附加到密钥的标签，以授予或拒绝该密钥的访问权限。有关更多信息，请参阅the section called “示例：使用标签控制对密钥的访问”。

您可以通过控制台、AWS CLI 和开发工具包中的标签查找密钥。AWS 还提供了资源组工具以便您创建自定义控制台，从而根据资源的标签整合与整理资源。要查找带有特定标签的密钥，请参阅 the section called “查找密钥”。Secrets Manager 不支持基于标签的成本分配。

切勿在标签中存储密钥的敏感信息。

有关标签配额和命名限制，请参阅 AWS 一般参考指南中的标记的服务配额。标签区分大小写。

当您标记或取消标记密钥时，Secrets Manager 会生成 CloudTrail 日志条目。有关更多信息，请参阅the section called “使用以下方式登录 AWS CloudTrail ”。

更改密钥的标签（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。
3. 在密钥详细信息页面的标签选项卡中，选择编辑标签。标签键名称和值区分大小写，标签键必须唯一。

AWS CLI

Example 向密钥添加标签

以下 `tag-resource` 示例说明了如何使用速记语法附加标签。

```
aws secretsmanager tag-resource \
            --secret-id MyTestSecret \
            --tags Key=FirstTag,Value=FirstValue
```

Example 向密钥添加多个标签

以下 `tag-resource` 示例将向密钥附加两个键值标签。

```
aws secretsmanager tag-resource \
            --secret-id MyTestSecret \
            --tags '[{"Key": "FirstTag", "Value": "FirstValue"}, {"Key": "SecondTag",
 "Value": "SecondValue"}]'
```

Example 从密钥中删除标签

以下 untag-resource 示例将从密钥中删除两个标签。对于每个标签，键和值都会被删除。

```
aws secretsmanager untag-resource \
            --secret-id MyTestSecret \
            --tag-keys '[ "FirstTag", "SecondTag"]'
```

AWS SDK

要更改您的密钥的标签，请使用 TagResource 或 UntagResource。有关更多信息，请参阅the section called “AWS 软件开发工具包”。

跨区域复制 AWS Secrets Manager 密钥

您可以将您的密钥分成多个复制 AWS 区域 ，以支持分布在这些地区的应用程序，从而满足区域访问和低延迟要求。如果以后需要，可以将副本密钥提升为独立密钥，然后将其设置为独立复制。Secrets Manager 可以跨指定区域复制加密密钥数据和元数据，例如标签和资源策略。

除区域外，副本密钥的 ARN 与主密钥相同，例如：

- 主密钥：`arn:aws:secretsmanager:Region1:123456789012:secret:MySecret-a1b2c3`
- 副本密钥：`arn:aws:secretsmanager:Region2:123456789012:secret:MySecret-a1b2c3`

有关副本密钥的定价信息，请参阅 AWS Secrets Manager 定价。

当存储复制到其他区域的源数据库的数据库凭证时，密钥将包含源数据库的连接信息。然后复制密钥时，副本将是源密钥的副本，并且包含相同的连接信息。您可以在密钥中添加其他键值对以记录区域连接信息。

如果您为主密钥启用轮换，Secrets Manager 将在主区域中进行密钥轮换，新的密钥值会传播到所有关联的副本密钥。您无需单独管理所有副本密钥的轮换。

您可以在所有已启用的 AWS 区域中复制密钥。但是，如果您在特殊 AWS 区域（例如 AWS GovCloud (US) 或中国区域）使用 Secrets Manager，则只能在这些特殊 AWS 区域内配置密钥和副本。您不能将已启用 AWS 区域中的密钥复制到专门区域，也不能将机密从专业区域复制到商业区域。

在将密钥复制到另一个区域之前，您必须启用该区域。有关更多信息，请参阅管理 AWS 区域。

通过调用存储密钥的区域中的 Secrets Manager 端点，则无需复制密钥即可在多个区域中使用密钥。有关 终端节点的列表，请参阅the section called “Secrets Manager 端点”。要使用复制来提高工作负载的弹性，请参阅第一部分：云端恢复策略中的灾难恢复 (DR) 架构。 AWS

当你复制密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

要将密钥复制到其他地区（控制台）

1. 通过 https://console.aws.amazon.com/secretsmanager/ 打开 Secrets Manager 控制台。
2. 从密钥列表上，选择您的密钥。

3. 在密钥详细信息页面的复制选项卡中，执行以下任意一项操作：
   - 如果未复制密钥，请选择 Replicate secret（复制密钥）。
   - 如果已复制密钥，请在 Replicate secret（复制密钥）部分，选择 Add Region（添加区域）。
4. 在 Add replica regions 对话框中，执行以下操作：
   a. 针对 AWS 区域，请选择要将密钥复制粘贴的区域。
   b. （可选）对于加密密钥中，选择用来加密密钥的 KMS 密钥。密钥必须位于副本区域中。
   c. （可选）要添加其他区域，请选择 Add more regions（添加更多区域）。
   d. 选择 Replicate（复制）。

   此时会返回到密钥详细信息页面。Replicate secret（复制密钥）部分会显示每个区域的 Replication status（复制状态）。

AWS CLI

Example 将密钥复制到其他区域

以下 `replicate-secret-to-regions` 示例将密钥复制到 eu-west-3。副本使用 AWS 托管密钥 aws/secretsmanager 进行加密。

```
aws secretsmanager replicate-secret-to-regions \
        --secret-id MyTestSecret \
        --add-replica-regions Region=eu-west-3
```

Example 创建密钥并复制它

以下示例创建了一个密钥并将其复制到 eu-west-3。副本使用 AWS 托管密钥 aws/secretsmanager 进行加密。

```
aws secretsmanager create-secret \
    --name MyTestSecret \
    --description "My test secret created with the CLI." \
    --secret-string "{\"user\":\"diegor\",\"password\":\"EXAMPLE-PASSWORD\"}"
    --add-replica-regions Region=eu-west-3
```

AWS SDK

要复制密钥，请使用 `ReplicateSecretToRegions` 命令。有关更多信息，请参阅 the section called “AWS 软件开发工具包”。

将副本密钥升级为 AWS Secrets Manager 中的独立密钥

副本密钥是从另一个 AWS 区域 中的主密钥复制而来的密钥。它具有与主密钥相同的密钥值和元数据，但对它的加密可以使用不同的 KMS 密钥。不能独立于主密钥更新副本密钥，但其加密密钥除外。副本密钥升级会断开副本密钥与主密钥的连接，并使副本机密成为独立密钥。对主密钥的更改不会复制到独立密钥。

在主密钥不可用的情况下，您可能希望将副本密钥升级为独立密钥，以此作为灾难恢复解决方案。或者，如果要为副本密钥启用轮换，您可能需要将副本密钥升级为独立密钥。

如您升级副本密钥，请务必更新相应的应用程序来使用独立密钥。

当您提升密钥时，Secrets Manager 会生成 CloudTrail 日志条目。有关更多信息，请参阅the section called “使用以下方式登录 AWS CloudTrail ”。

升级副本密钥（控制台）

1. 登录到 Secrets Manager https://console.aws.amazon.com/secretsmanager/。
2. 导航至副本区域。
3. 在 Secrets（密钥）列表页上，选择副本密钥。
4. 在副本密钥详细信息页面上，选择 Promote to standalone secret（升级为独立密钥）。
5. 在 Promote replica to standalone secret（将副本升级为独立密钥）对话框中，输入区域，然后选择 Promote replica（提升副本）。

AWS CLI

Example 将副本密钥提升为主密钥

以下 `stop-replication-to-replica` 示例将删除副本密钥与主密钥之间的链接。副本密钥在副本区域中被提升为主密钥。您必须从副本区域内调用 `stop-replication-to-replica`。

```
aws secretsmanager stop-replication-to-replica \
```

```
    --secret-id MyTestSecret
```

AWS SDK

要将副本密钥升级为独立密钥，请使用 StopReplicationToReplica 命令。您必须从副本密钥区域调用此命令。有关更多信息，请参阅the section called “AWS 软件开发工具包”。

防止 AWS Secrets Manager 复制

由于密钥可以使用ReplicateSecretToRegions或在使用创建时复制 CreateSecret，因此如果您想防止用户复制密钥，我们建议您阻止包含AddReplicaRegions参数的操作。您可以在权限策略中使用Condition声明，仅允许不添加副本区域的操作。有关您可以使用的条件声明，请参阅以下策略示例。

Example 阻止复制权限

以下策略示例显示如何允许所有不添加副本区域的操作。这可以防止用户同时通过ReplicateSecretToRegions和CreateSecret复制密钥。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": "*",
      "Condition": {
        "Null": {
          "secretsmanager:AddReplicaRegions": "true"
        }
      }
    }
  ]
}
```

Example 仅允许向特定区域提供复制权限

以下策略显示了如何允许以下所有内容：

- 无需复制即可创建密钥

- 通过复制到仅位于美国和加拿大的区域来创建密钥
- 仅将密钥复制到美国和加拿大的区域

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:ReplicateSecretToRegions"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringLike": {
          "secretsmanager:AddReplicaRegions": [
            "us-*",
            "ca-*"
          ]
        }
      }
    }
  ]
}
```

排除 AWS Secrets Manager 复制故障

以下是可能造成复制失败的一些原因。

选定区域中存在名称相同的密钥。

为此解决此问题，可以覆盖副本区域中的重复名称密钥。重试复制，然后在重试复制对话框中，选择覆盖。

KMS 密钥上没有可用的权限来完成复制。

Secrets Manager 首先解密密密钥，然后使用副本区域中的新 KMS 密钥重新加密。如果您在主区域中没有加密密钥的 `kms:Decrypt` 权限，则会遇到此错误。要使用 `aws/secretsmanager` 以外的 KMS 密钥对复制的秘密进行加密，您需要对密钥进行 `kms:GenerateDataKey` 和 `kms:Encrypt`。请参阅 the section called “KMS 密钥的权限”。

KMS 密钥已禁用或者未找到

如果主区域中的加密密钥被禁用或删除，则 Secrets Manager 将无法复制该秘密。即使您更改了加密密钥，如果秘密具有使用已禁用或删除的加密密钥加密的自定义标签版本，也可能发生此错误。有关 Secrets Manager 如何加密的信息，请参阅 the section called “密钥加密和解密”。要解决此问题，您可以重新创建秘密版本，以便 Secrets Manager 使用当前加密密钥对其进行加密。有关更多信息，请参阅更改秘密的加密密钥。然后重试复制。

```
aws secretsmanager put-secret-value \
  --secret-id testDescriptionUpdate \
  --secret-string "SecretValue" \
  --version-stages "MyCustomLabel"
```

您尚未启用要复制的区域。

有关如何启用区域的信息，请参阅管理 AWS 区域。 在《AWS 账户管理参考指南》中。

从中获取秘密 AWS Secrets Manager

当你检索密钥时，Secrets Manager 会生成一个 CloudTrail 日志条目。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

您可以使用以下方法检索机密值：

- 使用 Java 获取 Secrets Manager 的密钥值
- 使用 Python 获取 Secrets Manager 的密钥值
- 使用.NET 获取 Secrets Manager 密钥值
- 使用 Go 获取 Secrets Manager 的密钥值
- 使用 C++ AWS SDK 获取 Secrets Manager 密钥值
- 使用 JavaScript AWS SDK 获取 Secrets Manager 密钥值
- 使用 Kotlin AWS SDK 获取 Secrets Manager 的密钥值
- 使用 PHP AWS 开发工具包获取 Secrets Manager 密钥值
- 使用 Ruby AWS SDK 获取 Secrets Manager 密钥值
- 使用 Rust AWS SDK 获取 Secrets Manager 密钥值
- 使用获取秘密值 AWS CLI
- 使用 AWS 控制台获取密钥值
- 在中使用 AWS Secrets Manager 秘密 AWS Batch
- 在 AWS CloudFormation 资源中获取 AWS Secrets Manager 秘密
- 在亚马逊 Elastic Kubernetes Service 中使用 AWS Secrets Manager 密钥
- 在 GitHub 工作中使用 AWS Secrets Manager 秘密
- 在 AWS IoT Greengrass 中使用 AWS Secrets Manager 密钥
- 在 AWS Lambda 函数中使用 AWS Secrets Manager 密钥
- 使用 Parameter Store 中的 AWS Secrets Manager 密钥

使用 Java 获取 Secrets Manager 的密钥值

在应用程序中，您可以通过调用`GetSecretValue`或`BatchGetSecretValue`在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

要使用密钥中的凭据连接到数据库，可以使用 Secrets Manager SQL Connection 驱动程序，该驱动程序封装了基本 JDBC 驱动程序。它还使用客户端缓存，因此可以降低调用 Secrets Manager API 的成本。

主题

- 使用带有客户端缓存的 Java 获取 Secrets Manager 密钥值
- 使用密钥中的凭据使用 JDBC 连接到 SQL 数据库 AWS Secrets Manager
- 使用 Java AWS SDK 获取 Secrets Manager 密钥值

使用带有客户端缓存的 Java 获取 Secrets Manager 密钥值

在检索密钥时，您可以使用 Secrets Manager 基于 Java 的缓存组件来缓存密钥，以备将来使用。检索已缓存密钥比从 Secrets Manager 中检索密钥的速度要快。由于调用 Secrets Manager API 会产生费用，因此使用缓存可以降低成本。有关检索密钥的所有方法，请参阅 获取秘密。

缓存策略为“最近最少使用 (LRU)”，因此当缓存必须丢弃某个密钥时，它会丢弃最近使用最少的密钥。原定设置下，缓存会每小时刷新一次秘密。您可以配置在缓存中刷新密钥的频率，也可以挂钩到密钥检索中以添加更多功能。

一旦释放缓存引用，缓存便不会进行强制垃圾回收。缓存实施不包括缓存失效。缓存实现侧重于缓存本身，而不是侧重加强安全性或以安全性为重点。如果您需要额外的安全性（例如加密缓存中的项目），请使用提供的接口和抽象方法。

要使用该组件，您必须满足以下条件：

- Java 8 或更高版本的开发环境。请参阅 Oracle 网站上的 Java SE 下载。
- 适用于 Java AWS 的 SDK 1.x。你可以在项目中使用两个版本的 Java AWS SDK。有关更多信息，请参阅使用适用于 Java 的 SDK 1.x 和 2. side-by-side x。

要下载源代码，请参阅上的 S ecrets Manager 基于 Java 的缓存客户端组件。 GitHub

要将该组件添加到您的项目中，请在 Maven pom.xml 文件中包括以下依赖项。有关 Maven 的更多信息，请参阅 Apache Maven Project 网站上的《入门指南》。

```
<dependency>
  <groupId>com.amazonaws.secretsmanager</groupId>
  <artifactId>aws-secretsmanager-caching-java</artifactId>
```

```
  <version>1.0.2</version>
</dependency>
```

所需权限：

- `secretsmanager:DescribeSecret`
- `secretsmanager:GetSecretValue`

有关更多信息，请参阅 权限参考。

参考

- SecretCache
- SecretCacheConfiguration
- SecretCacheHook

Example 检索密钥

以下代码示例显示了检索密钥字符串的 Lambda 函数。它遵循在函数处理程序之外实例化缓存的最佳实践，因此如果您再次调用该 Lambda 函数，它不会继续调用该 API。

```
package com.amazonaws.secretsmanager.caching.examples;

    import com.amazonaws.services.lambda.runtime.Context;
    import com.amazonaws.services.lambda.runtime.RequestHandler;
    import com.amazonaws.services.lambda.runtime.LambdaLogger;

    import com.amazonaws.secretsmanager.caching.SecretCache;

    public class SampleClass implements RequestHandler<String, String> {

         private final SecretCache cache  = new SecretCache();

         @Override public String handleRequest(String secretId,  Context context) {
             final String secret  = cache.getSecretString(secretId);

            // Use the secret, return success;

        }
    }
```

SecretCache

适用于从 Secrets Manager 请求的密钥的内存中缓存。您使用 the section called “getSecretString” 或 the section called “getSecretBinary” 从缓存中检索密钥。您可以通过传入构造函数中的 the section called “SecretCacheConfiguration” 对象来配置缓存设置。

有关包括示例在内的更多信息，请参阅 the section called “带有客户端缓存功能的 Java”。

构造函数

`public SecretCache()`

适用于 `SecretCache` 对象的默认构造函数。

`public SecretCache(AWSSecretsManagerClientBuilder builder)`

使用 Secrets Manager 客户端（使用提供的 `AWSSecretsManagerClientBuilder` 创建）构造新缓存。使用此构造函数自定义 Secrets Manager 客户端，例如使用特定的区域或端点。

`public SecretCache(AWSSecretsManager client)`

请使用提供的 `AWSSecretsManagerClient` 构造新密钥缓存。使用此构造函数自定义 Secrets Manager 客户端，例如使用特定的区域或端点。

`public SecretCache(SecretCacheConfiguration config)`

请使用提供的 `the section called “SecretCacheConfiguration”` 构造新密钥缓存。

方法

getSecretString

`public String getSecretString(final String secretId)`

从 Secrets Manager 中检索字符串密钥。返回 `String`。

getSecretBinary

`public ByteBuffer getSecretBinary(final String secretId)`

从 Secrets Manager 中检索二进制密钥。返回 `ByteBuffer`。

refreshNow

```
public boolean refreshNow(final String secretId) throws
InterruptedException
```

强制刷新缓存。如果刷新完成没有错误，将返回 `true`，否则将返回 `false`。

close

```
public void close()
```

关闭缓存。

SecretCacheConfiguration

适用于 the section called “SecretCache” 的缓存配置选项，例如最大缓存大小和已缓存密钥的生存时间 (TTL)。

构造函数

```
public SecretCacheConfiguration
```

适用于 `SecretCacheConfiguration` 对象的默认构造函数。

方法

getClient

```
public AWSSecretsManager getClient()
```

返回缓存从中检索密钥的 `AWSSecretsManagerClient`。

setClient

```
public void setClient(AWSSecretsManager client)
```

设置缓存从中检索密钥的 `AWSSecretsManagerClient` 客户端。

getCacheHook

```
public SecretCacheHook getCacheHook()
```

返回用于挂钩缓存更新的 the section called “SecretCacheHook” 接口。

setCacheHook

```
public void setCacheHook(SecretCacheHook cacheHook)
```

设置用于挂钩缓存更新的 the section called “SecretCacheHook” 接口。

getMaxCache大小

```
public int getMaxCacheSize()
```

返回最大缓存大小。默认值为 1024 个密钥。

setMaxCache大小

```
public void setMaxCacheSize(int maxCacheSize)
```

设置最大缓存大小。默认值为 1024 个密钥。

getCacheItemTTL

```
public long getCacheItemTTL()
```

返回已缓存项目的 TTL（以毫秒为单位）。当已缓存密钥超过此 TTL 时，缓存将从 AWSSecretsManagerClient 中检索该密钥的新副本。默认值为 1 小时（以毫秒为单位）。

在 TTL 之后请求密钥时，缓存将同步刷新密钥。如果同步刷新失败，缓存将返回过时密钥。

setCacheItemTTL

```
public void setCacheItemTTL(long cacheItemTTL)
```

为已缓存项目设置 TTL（以毫秒为单位）。当已缓存密钥超过此 TTL 时，缓存将从 AWSSecretsManagerClient 中检索该密钥的新副本。默认值为 1 小时（以毫秒为单位）。

getVersionStage

```
public String getVersionStage()
```

返回您要缓存的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 "AWSCURRENT"。

setVersionStage

```
public void setVersionStage(String versionStage)
```

设置您要缓存的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 "AWSCURRENT"。

SecretCacheConfiguration 与客户一起

```
public SecretCacheConfiguration withClient(AWSSecretsManager client)
```

设置 AWSSecretsManagerClient 以从中检索密钥。返回具有新设置的更新后的 SecretCacheConfiguration 对象。

SecretCacheConfiguration withCacheHook

```
public SecretCacheConfiguration withCacheHook(SecretCacheHook cacheHook)
```

设置用于挂钩内存中缓存的接口。返回具有新设置的更新后的 SecretCacheConfiguration 对象。

SecretCacheConfiguration withMaxCache大小

```
public SecretCacheConfiguration withMaxCacheSize(int maxCacheSize)
```

设置最大缓存大小。返回具有新设置的更新后的 SecretCacheConfiguration 对象。

SecretCacheConfiguration withCacheItemTTL

```
public SecretCacheConfiguration withCacheItemTTL(long cacheItemTTL)
```

为已缓存项目设置 TTL（以毫秒为单位）。当已缓存密钥超过此 TTL 时，缓存将从 AWSSecretsManagerClient 中检索该密钥的新副本。默认值为 1 小时（以毫秒为单位）。返回具有新设置的更新后的 SecretCacheConfiguration 对象。

SecretCacheConfiguration withVersionStage

```
public SecretCacheConfiguration withVersionStage(String versionStage)
```

设置您要缓存的密钥的版本。有关更多信息，请参阅密钥版本。返回具有新设置的更新后的 SecretCacheConfiguration 对象。

SecretCacheHook

用于挂钩到 the section called “SecretCache” 中以便对存储于缓存中的密钥执行操作的接口。

put

```
Object put(final Object o)
```

准备对象以存储到缓存中。

返回要存储在缓存中的对象。

get

```
Object get(final Object cachedObject)
```

从已缓存对象派生对象。

返回要从缓存中返回的对象

使用密钥中的凭据使用 JDBC 连接到 SQL 数据库 AWS Secrets Manager

在 Java 应用程序中，你可以使用 Secrets Manager SQL Connection 驱动程序使用存储在 Secrets Manager 中的凭据连接到 MySQL、PostgreSQL、Oracle、mssqlServer、Db2 和 Redshift 数据库。每个驱动程序都会包装基本 JDBC 驱动程序，因此您可以使用 JDBC 调用来访问数据库。但是，您不必为连接传递用户名和密码，而是提供密钥的 ID。驱动程序将调用 Secrets Manager 来检索密钥值，然后使用密钥中的凭证连接到数据库。驱动程序还将使用 Java 客户端缓存库来缓存凭证，这样未来的连接就不需要调用 Secrets Manager。默认情况下，缓存会每小时刷新一次，此外在轮换密钥时也会刷新。要配置缓存，请参阅the section called “SecretCacheConfiguration”。

您可以从中下载源代码GitHub。

要使用 Secrets Manager SQL 连接驱动程序：

- 您的应用程序必须处于 Java 8 或更高版本中。
- 您的密钥必须为以下之一：
  - 预期 JSON 结构中的数据库密钥。要检查格式，请在 Secrets Manager 控制台中查看密钥并选择 Retrieve secret value（检索密钥值）。或者，在通话 AWS CLI中get-secret-value。
  - Amazon RDS 托管密钥。对于此类密钥，必须在建立连接时指定端点和端口。
  - 一个由亚马逊 Redshift 管理的机密。对于此类密钥，必须在建立连接时指定端点和端口。

如果您的数据库复制到其他区域，要连接到另一个区域中的副本数据库，请在创建连接时指定区域端点和端口。您可以在作为额外键值对的密钥中、SSM 参数存储参数或代码配置中存储区域连接信息。

要将驱动程序添加到项目中，请在 Maven 构建文件 `pom.xml` 中为该驱动程序添加以下依赖项。有关更多信息，请参阅 Maven Central 存储库网站上的 Secrets Manager SQL 连接库。

```
<dependency>
    <groupId>com.amazonaws.secretsmanager</groupId>
    <artifactId>aws-secretsmanager-jdbc</artifactId>
    <version>1.0.12</version>
</dependency>
```

驱动程序使用默认凭证提供程序链。如果您在 Amazon EKS 上运行驱动程序，它可能会获取正在运行的节点的凭证，而不会获取服务账户角色。要解决此问题，请将 com.amazonaws:aws-java-sdk-sts 的版本 1 作为依赖项添加到 Gradle 或 Maven 项目文件。

要在secretsmanager.properties文件中设置 AWS PrivateLink DNS 终端节点 URL 和区域，请执行以下操作：

```
drivers.vpcEndpointUrl = endpoint URL
drivers.vpcEndpointRegion = endpoint region
```

要覆盖主区域，请设置 AWS_SECRET_JDBC_REGION 环境变量或对 secretsmanager.properties 文件进行以下更改：

```
drivers.region = region
```

所需权限：

- secretsmanager:DescribeSecret
- secretsmanager:GetSecretValue

有关更多信息，请参阅 权限参考。

示例：

- 建立与数据库的连接
- 通过指定端点和端口建立连接
- 使用 c3p0 连接池建立连接
- 使用 c3p0 连接池通过指定端点和端口来建立连接

建立与数据库的连接

下面的示例演示了如何使用密钥中的凭证和连接信息建立与数据库的连接。建立连接后，您可使用 JDBC 调用来访问数据库。有关更多信息，请参阅 Java 文档网站上的 JDBC 基础知识。

MySQL

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerMySQLDriver" ).newInstance
```

```
// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

PostgreSQL

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerPostgreSQLDriver" ).newIns

// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Oracle

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerOracleDriver" ).newInstanc

// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

MSSQLServer

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerMSSQLServerDriver" ).newIn

// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Db2

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerDb2Driver" ).newInstance()

// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Redshift

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerRedshiftDriver" ).newInsta

// Retrieve the connection info from the secret using the secret ARN
String URL = "secretId";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
```

```
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

通过指定端点和端口建立连接

以下示例演示了如何使用密钥中的凭证以及指定的端点和端口建立与数据库的连接。

Amazon RDS 托管密钥不包括数据库的端点和端口。要使用由 Amazon RDS 管理的密钥中的主凭证连接到数据库，请在代码中指定这些凭证。

复制到其他区域的密钥可以降低连接到区域数据库的延迟，但复制的密钥将不包含与源密钥不同的连接信息。每个副本都与源密钥相同。要将区域连接信息存储到密钥中，请添加更多键值对来存储区域的端点和端口信息。

建立连接后，您可使用 JDBC 调用来访问数据库。有关更多信息，请参阅 Java 文档网站上的 JDBC 基础知识。

MySQL

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerMySQLDriver" ).newInstance

// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:mysql://example.com:3306";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

PostgreSQL

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerPostgreSQLDriver" ).newIns
```

```
// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:postgresql://example.com:5432/database";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Oracle

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerOracleDriver" ).newInstanc

// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:oracle:thin:@example.com:1521/ORCL";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

MSSQLServer

```
// Load the JDBC driver
Class.forName( "com.amazonaws.secretsmanager.sql.AWSSecretsManagerMSSQLServerDriver" ).newIn

// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:sqlserver://example.com:1433";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );
```

```
// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Db2

```
// Load the JDBC driver
Class.forName( "com.amazonaws.com.amazonaws.secretsmanager.sql.AWSSecretsManagerDb2Driver" )

// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:db2://example.com:50000";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

Redshift

```
// Load the JDBC driver
Class.forName( "com.amazonaws.com.amazonaws.secretsmanager.sql.AWSSecretsManagerRedshiftDriv

// Set the endpoint and port. You can also retrieve it from a key/value pair in the
 secret.
String URL = "jdbc-secretsmanager:redshift://example.com:5439";

// Populate the user property with the secret ARN to retrieve user and password from
 the secret
Properties info = new Properties( );
info.put( "user", "secretId" );

// Establish the connection
conn = DriverManager.getConnection(URL, info);
```

使用 c3p0 连接池建立连接

以下示例演示了如何使用 `c3p0.properties` 文件建立连接池，该文件使用驱动程序从密钥中检索凭证和连接信息。对于 `user` 和 `jdbcUrl`，请输入密钥 ID 以配置连接池。然后，您可以从该池中检索连

接，并将这些连接用作任何其他数据库连接。有关更多信息，请参阅 Java 文档网站上的 JDBC 基础知识。

有关 c3p0 的更多信息，请参阅 Machinery For Change 网站上的 c3p0。

MySQL

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerMySQLDriver
c3p0.jdbcUrl=secretId
```

PostgreSQL

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerPostgreSQLDriver
c3p0.jdbcUrl=secretId
```

Oracle

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerOracleDriver
c3p0.jdbcUrl=secretId
```

MSSQLServer

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerMSSQLServerDriver
c3p0.jdbcUrl=secretId
```

Db2

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerDb2Driver
c3p0.jdbcUrl=secretId
```

Redshift

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerRedshiftDriver
c3p0.jdbcUrl=secretId
```

使用 c3p0 连接池通过指定端点和端口来建立连接

以下示例说明如何使用文件建立连接池，该`c3p0.properties`文件使用驱动程序通过您指定的端点和端口检索密钥中的凭证。然后，您可以从该池中检索连接，并将这些连接用作任何其他数据库连接。有关更多信息，请参阅 Java 文档网站上的 JDBC 基础知识。

Amazon RDS 托管密钥不包括数据库的端点和端口。要使用由 Amazon RDS 管理的密钥中的主凭证连接到数据库，请在代码中指定这些凭证。

复制到其他区域的密钥可以降低连接到区域数据库的延迟，但复制的密钥将不包含与源密钥不同的连接信息。每个副本都与源密钥相同。要将区域连接信息存储到密钥中，请添加更多键值对来存储区域的端点和端口信息。

MySQL

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerMySQLDriver
c3p0.jdbcUrl=jdbc-secretsmanager:mysql://example.com:3306
```

PostgreSQL

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerPostgreSQLDriver
c3p0.jdbcUrl=jdbc-secretsmanager:postgresql://example.com:5432/database
```

Oracle

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerOracleDriver
c3p0.jdbcUrl=jdbc-secretsmanager:oracle:thin:@example.com:1521/ORCL
```

MSSQLServer

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerMSSQLServerDriver
c3p0.jdbcUrl=jdbc-secretsmanager:sqlserver://example.com:1433
```

Db2

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerDb2Driver
```

```
c3p0.jdbcUrl=jdbc-secretsmanager:db2://example.com:50000
```

Redshift

```
c3p0.user=secretId
c3p0.driverClass=com.amazonaws.secretsmanager.sql.AWSSecretsManagerRedshiftDriver
c3p0.jdbcUrl=jdbc-secretsmanager:redshift://example.com:5439
```

使用 Java AWS SDK 获取 Secrets Manager 密钥值

在应用程序中，您可以通过调用GetSecretValue或BatchGetSecretValue在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

- 如果您将数据库凭证存储在密钥中，请使用 Secrets Manager SQL 连接驱动程序借助密钥中的凭证连接到数据库。
- 对于其他类型的密钥，请使用基于 Java 的 Secrets Manager 缓存组件，或者使用GetSecretValue或BatchGetSecretValue直接调用 SDK。

以下代码示例演示如何使用 GetSecretValue。

所需权限：secretsmanager:GetSecretValue

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;
import software.amazon.awssdk.services.secretsmanager.model.SecretsManagerException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 * We recommend that you cache your secret values by using client-side caching.
 *
 * Caching secrets improves speed and reduces your costs. For more information,
```

```
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/secretsmanager/latest/userguide/retrieving-secrets.html
 */
public class GetSecretValue {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <secretName>\s

                Where:
                    secretName - The name of the secret (for example, tutorials/
MyFirstSecret).\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String secretName = args[0];
        Region region = Region.US_EAST_1;
        SecretsManagerClient secretsClient = SecretsManagerClient.builder()
                .region(region)
                .build();

        getValue(secretsClient, secretName);
        secretsClient.close();
    }

    public static void getValue(SecretsManagerClient secretsClient, String secretName)
 {
        try {
            GetSecretValueRequest valueRequest = GetSecretValueRequest.builder()
                    .secretId(secretName)
                    .build();

            GetSecretValueResponse valueResponse =
 secretsClient.getSecretValue(valueRequest);
            String secret = valueResponse.secretString();
            System.out.println(secret);

        } catch (SecretsManagerException e) {
```

```
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

使用 Python 获取 Secrets Manager 的密钥值

在应用程序中，您可以通过调用`GetSecretValue`或`BatchGetSecretValue`在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

主题

- 使用带有客户端缓存的 Python 获取 Secrets Manager 密钥值
- 使用 Python AWS SDK 获取 Secrets Manager 密钥值
- 使用 Python AWS SDK 获取一批 Secrets Manager 密钥值

使用带有客户端缓存的 Python 获取 Secrets Manager 密钥值

在检索密钥时，您可以使用 Secrets Manager 基于 Python 的缓存组件来缓存密钥，以备将来使用。检索已缓存密钥比从 Secrets Manager 中检索密钥的速度要快。由于调用 Secrets Manager API 会产生费用，因此使用缓存可以降低成本。有关检索密钥的所有方法，请参阅 获取秘密。

缓存策略为“最近最少使用 (LRU)”，因此当缓存必须丢弃某个密钥时，它会丢弃最近使用最少的密钥。原定设置下，缓存会每小时刷新一次秘密。您可以配置在缓存中刷新密钥的频率，也可以挂钩到密钥检索中以添加更多功能。

一旦释放缓存引用，缓存便不会进行强制垃圾回收。缓存实施不包括缓存失效。缓存实现侧重于缓存本身，而不是侧重加强安全性或以安全性为重点。如果您需要额外的安全性（例如加密缓存中的项目），请使用提供的接口和抽象方法。

要使用该组件，您必须满足以下条件：

- Python 3.6 或更高版本。
- botocore 1.12 或更高版本。请参阅适用于 Python 和 Botocore 的AWS SDK。
- setuptools_scm 3.2 或更高版本。请参阅 https://pypi.org/project/setuptools-scm/。

要下载源代码，请参阅上的 S ecrets Manager 基于 Python 的缓存客户端组件。 GitHub

要安装组件，请使用以下命令。

```
$ pip install aws-secretsmanager-caching
```

所需权限：

- `secretsmanager:DescribeSecret`
- `secretsmanager:GetSecretValue`

有关更多信息，请参阅 权限参考。

参考

- SecretCache
- SecretCacheConfig
- SecretCacheHook
- @InjectSecretString
- @InjectKeywordedSecretString

Example 检索密钥

下面的示例演示了如何获取名为 *mysecret* 的密钥的密钥值。

```
import botocore
import botocore.session
from aws_secretsmanager_caching import SecretCache, SecretCacheConfig

client = botocore.session.get_session().create_client('secretsmanager')
cache_config = SecretCacheConfig()
cache = SecretCache( config = cache_config, client = client)

secret = cache.get_secret_string('mysecret')
```

SecretCache

适用于从 Secrets Manager 检索的密钥的内存中缓存。您使用 the section called “get_secret_string” 或 the section called “get_secret_binary” 从缓存中检索密钥。您可以通过传入构造函数中的 the section called “SecretCacheConfig” 对象来配置缓存设置。

有关包括示例在内的更多信息，请参阅 the section called “带有客户端缓存功能的 Python”。

```
cache = SecretCache(
    config = the section called “SecretCacheConfig”,
    client = client
)
```

以下是可用方法：

- get_secret_string
- get_secret_binary

get_secret_string

检索密钥字符串值。

请求语法

```
response = cache.get_secret_string(
    secret_id='string',
    version_stage='string' )
```

参数

- secret_id (字符串) -- [必需] 密钥的名称或 ARN。
- version_stage (字符串) -- 您要检索的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 “AWSCURRENT”。

返回类型

字符串

get_secret_binary

检索密钥二进制值。

请求语法

```
response = cache.get_secret_binary(
    secret_id='string',
    version_stage='string'
```

```
)
```

参数

- secret_id (字符串) -- [必需] 密钥的名称或 ARN。
- version_stage (字符串) -- 您要检索的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 “AWSCURRENT”。

返回类型

base64 编码的字符串

SecretCacheConfig

适用于 the section called “SecretCache” 的缓存配置选项，例如最大缓存大小和已缓存密钥的存活时间 (TTL)。

参数

max_cache_size (int)

最大缓存大小。默认值为 1024 个密钥。

exception_retry_delay_base (int)

遇到异常后重试请求之前需要等待的秒数。默认值为 1。

exception_retry_growth_factor (int)pur

用于计算重试失败请求之间等待时间的增长系数。默认值为 2。

exception_retry_delay_max (int)

在失败请求之间需要等待的最长时间（以秒为单位）。默认值为 3600。

default_version_stage (str)

您要缓存的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 'AWSCURRENT'。

secret_refresh_interval (int)

刷新已缓存密钥信息之间需要等待的秒数。默认值为 3600。

secret_cache_hook (SecretCacheHook)

SecretCacheHook 抽象类的实施。默认值为 None。

SecretCacheHook

用于挂钩到 the section called “SecretCache” 中以便对存储于缓存中的密钥执行操作的接口。

以下是可用方法：

- put
- get

put

使对象为存储在缓存中做好准备。

请求语法

```
response = hook.put(
    obj='secret_object'
)
```

参数

- obj (对象) -- [必需] 密钥或包含密钥的对象。

返回类型

object

get

从已缓存对象派生对象。

请求语法

```
response = hook.get(
    obj='secret_object'
)
```

参数

- obj (对象) -- [必需] 密钥或包含密钥的对象。

返回类型

object

@InjectSecretString

此装饰器需要一个密钥 ID 字符串和 the section called “SecretCache” 作为前两个参数。该装饰器将返回密钥字符串值。密钥必须包含一个字符串。

```
from aws_secretsmanager_caching import SecretCache
from aws_secretsmanager_caching import InjectKeywordedSecretString,
 InjectSecretString

cache = SecretCache()

@InjectSecretString ( 'mysecret' ,  cache )
def function_to_be_decorated( arg1,  arg2,  arg3):
```

@InjectKeywordedSecretString

此装饰器需要一个密钥 ID 字符串和 the section called “SecretCache” 作为前两个参数。其余自变量将已包装函数中的参数映射到密钥中的 JSON 键。密钥必须包含一个 JSON 结构的字符串。

对于包含此 JSON 的密钥：

```
{
  "username": "saanvi",
  "password": "EXAMPLE-PASSWORD"
}
```

下面的示例演示了如何从密钥中提取 `username` 和 `password` 的 JSON 值。

```
from aws_secretsmanager_caching import SecretCache
  from aws_secretsmanager_caching import InjectKeywordedSecretString,
 InjectSecretString

  cache = SecretCache()

  @InjectKeywordedSecretString ( secret_id = 'mysecret' ,  cache = cache ,
 func_username = 'username' ,  func_password = 'password' )
  def function_to_be_decorated( func_username,  func_password):
       print( 'Do something with the func_username and func_password parameters')
```

使用 Python AWS SDK 获取 Secrets Manager 密钥值

在应用程序中，您可以通过调用GetSecretValue或BatchGetSecretValue在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

对于 Python 应用程序，请使用 Secrets Manager 基于 Python 的缓存组件或直接使用 get_secret_value 或 batch_get_secret_value 调用 SDK。

以下代码示例演示如何使用 GetSecretValue。

所需权限：secretsmanager:GetSecretValue

```
class GetSecretWrapper:
    def __init__(self, secretsmanager_client):
        self.client = secretsmanager_client


    def get_secret(self, secret_name):
        """
        Retrieve individual secrets from AWS Secrets Manager using the get_secret_value
 API.
        This function assumes the stack mentioned in the source code README has been
 successfully deployed.
        This stack includes 7 secrets, all of which have names beginning with
 "mySecret".

        :param secret_name: The name of the secret fetched.
        :type secret_name: str
        """
        try:
            get_secret_value_response = self.client.get_secret_value(
                SecretId=secret_name
            )
            logging.info("Secret retrieved successfully.")
            return get_secret_value_response["SecretString"]
        except self.client.exceptions.ResourceNotFoundException:
            msg = f"The requested secret {secret_name} was not found."
            logger.info(msg)
            return msg
        except Exception as e:
            logger.error(f"An unknown error occurred: {str(e)}.")
            raise
```

使用 Python AWS SDK 获取一批 Secrets Manager 密钥值

以下代码示例演示了如何获取批量 Secrets Manager 密钥值。

所需权限：

- `secretsmanager:BatchGetSecretValue`
- `secretsmanager:GetSecretValue`您要检索的每个密钥的权限。
- 如果您使用筛选器，则还必须拥有 `secretsmanager:ListSecrets`。

有关权限策略的示例，请参阅 the section called “示例：批量检索一组机密值的权限”。

> **Important**
>
> 如果您的 VPCE 策略拒绝在您正在检索的群组中检索单个秘密的权限，则 `BatchGetSecretValue` 不会返回任何秘密值，并且会返回错误。

```
class BatchGetSecretsWrapper:
    def __init__(self, secretsmanager_client):
        self.client = secretsmanager_client


    def batch_get_secrets(self, filter_name):
        """
        Retrieve multiple secrets from AWS Secrets Manager using the
 batch_get_secret_value API.
        This function assumes the stack mentioned in the source code README has been
 successfully deployed.
        This stack includes 7 secrets, all of which have names beginning with
 "mySecret".

        :param filter_name: The full or partial name of secrets to be fetched.
        :type filter_name: str
        """
        try:
            secrets = []
```

```
            response = self.client.batch_get_secret_value(
                Filters=[{"Key": "name", "Values": [f"{filter_name}"]}]
            )
            for secret in response["SecretValues"]:
                secrets.append(json.loads(secret["SecretString"]))
            if secrets:
                logger.info("Secrets retrieved successfully.")
            else:
                logger.info("Zero secrets returned without error.")
            return secrets
        except self.client.exceptions.ResourceNotFoundException:
            msg = f"One or more requested secrets were not found with filter:
{filter_name}"
            logger.info(msg)
            return msg
        except Exception as e:
            logger.error(f"An unknown error occurred:\n{str(e)}.")
            raise
```

使用.NET 获取 Secrets Manager 密钥值

在应用程序中，您可以通过调用`GetSecretValue`或`BatchGetSecretValue`在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

主题

- 使用带有客户端缓存的.NET 获取 Secrets Manager 密钥值
- 使用.NET 软件开发工具包获取 AWS Secrets Manager 密钥值

使用带有客户端缓存的.NET 获取 Secrets Manager 密钥值

在检索密钥时，您可以使用 Secrets Manager 基于 .NET 的缓存组件来缓存密钥，以备将来使用。检索已缓存密钥比从 Secrets Manager 中检索密钥的速度要快。由于调用 Secrets Manager API 会产生费用，因此使用缓存可以降低成本。有关检索密钥的所有方法，请参阅 获取秘密。

缓存策略为“最近最少使用 (LRU)”，因此当缓存必须丢弃某个密钥时，它会丢弃最近使用最少的密钥。原定设置下，缓存会每小时刷新一次秘密。您可以配置在缓存中刷新密钥的频率，也可以挂钩到密钥检索中以添加更多功能。

一旦释放缓存引用，缓存便不会进行强制垃圾回收。缓存实施不包括缓存失效。缓存实现侧重于缓存本身，而不是侧重加强安全性或以安全性为重点。如果您需要额外的安全性（例如加密缓存中的项目），请使用提供的接口和抽象方法。

要使用该组件，您必须满足以下条件：

- .NET Framework 4.6.2 或更高版本，或者 .NET Standard 2.0 或更高版本。请参阅 Microsoft .NET 网站上的下载 .NET。
- 适用于.NET 的 AWS SDK。请参阅 the section called “AWS 软件开发工具包”。

要下载源代码，请参阅上的 “.NET 缓存客户端” GitHub。

要使用缓存，请先对其进行实例化，然后使用 `GetSecretString` 或 `GetSecretBinary` 检索密钥。在连续检索时，缓存将返回密钥的已缓存副本。

获取缓存包

- 请执行以下操作之一：
  - 在您的项目目录中运行下列 .NET CLI 命令。

    ```
    dotnet add package AWSSDK.SecretsManager.Caching --version 1.0.6
    ```

  - 将下列软件包引用添加到您的 `.csproj` 文件中。

    ```
    <ItemGroup>
        <PackageReference Include="AWSSDK.SecretsManager.Caching" Version="1.0.6" /
    >
    </ItemGroup>
    ```

所需权限：

- `secretsmanager:DescribeSecret`
- `secretsmanager:GetSecretValue`

有关更多信息，请参阅 权限参考。

参考

- SecretsManagerCache

- SecretCacheConfiguration
- 我 SecretCacheHook

Example 检索密钥

以下代码示例显示了一种检索名为*MySecret*的密钥的方法。

```
using Amazon.SecretsManager.Extensions.Caching;

namespace LambdaExample
{
    public class CachingExample
    {
        private const string MySecretName ="MySecret";

        private SecretsManagerCache cache = new SecretsManagerCache();

        public async Task<Response>  FunctionHandlerAsync(string input, ILambdaContext
 context)
        {
            string MySecret = await cache.GetSecretString(MySecretName);

            // Use the secret, return success

        }
    }
}
```

Example 配置生存时间 (TTL) 缓存刷新持续时间

以下代码示例显示了一种检索名为的密钥*MySecret*并将 TTL 缓存刷新持续时间设置为 24 小时的方法。

```
using Amazon.SecretsManager.Extensions.Caching;

namespace LambdaExample
{
    public class CachingExample
    {
        private const string MySecretName = "MySecret";
```

```
        private static SecretCacheConfiguration cacheConfiguration = new
 SecretCacheConfiguration
        {
            CacheItemTTL = 86400000
        };
        private SecretsManagerCache cache = new
 SecretsManagerCache(cacheConfiguration);
        public async Task<Response> FunctionHandlerAsync(string input, ILambdaContext
 context)
        {
            string mySecret = await cache.GetSecretString(MySecretName);

            // Use the secret, return success
        }
    }
}
```

SecretsManagerCache

适用于从 Secrets Manager 请求的密钥的内存中缓存。您使用 the section called “GetSecretString” 或 the section called “GetSecretBinary” 从缓存中检索密钥。您可以通过传入构造函数中的 the section called “SecretCacheConfiguration” 对象来配置缓存设置。

有关包括示例在内的更多信息，请参阅 the section called “带有客户端缓存的.NET”。

构造函数

`public SecretsManagerCache()`

适用于 `SecretsManagerCache` 对象的默认构造函数。

`public SecretsManagerCache(IAmazonSecretsManager secretsManager)`

使用使用提供的AmazonSecretsManagerClient创建的 Secrets Manager 客户端构造新的缓存。使用此构造函数可自定义 Secrets Manager 客户端，例如使用某一特定区域或终端节点。

参数

secretsManager

AmazonSecretsManagerClient要从中检索机密。

```
public SecretsManagerCache(SecretCacheConfiguration config)
```

使用提供的 the section called “SecretCacheConfiguration” 构造新密钥缓存。使用此构造函数来配置缓存，例如要缓存的密钥数量及其刷新频率。

参数

config

一个 the section called “SecretCacheConfiguration”，其中包含缓存的配置信息。

```
public SecretsManagerCache(IAmazonSecretsManager secretsManager,
SecretCacheConfiguration config)
```

使用使用提供的AmazonSecretsManagerClient和创建的 Secrets Manager 客户端构造新的缓存。the section called “SecretCacheConfiguration”使用此构造函数可自定义 Secrets Manager 客户端，例如使用某一特定区域或终端节点以及配置缓存，例如要缓存的密钥数量及其刷新频率。

参数

secretsManager

AmazonSecretsManagerClient要从中检索机密。

config

一个 the section called “SecretCacheConfiguration”，其中包含缓存的配置信息。

方法

GetSecretString

```
public async Task<String> GetSecretString(String secretId)
```

从 Secrets Manager 中检索字符串密钥。

参数

secretId

要检索的密钥的 ARN 或名称。

GetSecretBinary

```
public async Task<byte[]> GetSecretBinary(String secretId)
```

从 Secrets Manager 中检索二进制密钥。

参数

secretId

要检索的密钥的 ARN 或名称。

RefreshNowAsync

```
public async Task<bool> RefreshNowAsync(String secretId)
```

请从 Secrets Manager 请求密钥值，并使用任何更改更新缓存。如果没有现有的缓存条目，请创建一个新缓存条目。如果刷新成功，则返回 `true`。

参数

secretId

要检索的密钥的 ARN 或名称。

GetCachedSecret

```
public SecretCacheItem GetCachedSecret(string secretId)
```

返回指定密钥的缓存条目（如果缓存中存在该密钥）。否则，从 Secret Manager 中该检索密钥，并创建一个新缓存条目。

参数

secretId

要检索的密钥的 ARN 或名称。

SecretCacheConfiguration

适用于 the section called “SecretsManagerCache” 的缓存配置选项，例如最大缓存大小和已缓存密钥的存活时间 (TTL)。

属性

CacheItemTTL

```
public uint CacheItemTTL { get; set; }
```

缓存项目的 TTL（以毫秒为单位）。默认值为 3600000 毫秒或 1 小时。最大值为 4294967295 ms，约为 49.7 天。

MaxCacheSize

```
public ushort MaxCacheSize { get; set; }
```

最大缓存大小。默认值为 1024 个密钥。最大值为 65535。

VersionStage

```
public string VersionStage { get; set; }
```

您要缓存的密钥的版本。有关更多信息，请参阅密钥版本。默认值为 "AWSCURRENT"。

客户端

```
public IAmazonSecretsManager Client { get; set; }
```

AmazonSecretsManagerClient要从中检索机密。如果是 null，缓存将实例化一个新客户端。默认值为 null。

CacheHook

```
public ISecretCacheHook CacheHook { get; set; }
```

一个 the section called “我 SecretCacheHook”。

我 SecretCacheHook

用于挂钩到 the section called “SecretsManagerCache” 中以便对存储于缓存中的密钥执行操作的接口。

方法

Put

```
object Put(object o);
```

准备对象以存储到缓存中。

返回要存储在缓存中的对象。

获取

```
object Get(object cachedObject);
```

从已缓存对象派生对象。

返回要从缓存中返回的对象

使用.NET 软件开发工具包获取 AWS Secrets Manager 密钥值

在应用程序中，您可以通过调用GetSecretValue或BatchGetSecretValue在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

对于 .NET 应用程序，请使用 Secrets Manager 基于 .NET 的缓存组件或直接使用 GetSecretValue 或 BatchGetSecretValue 调用 SDK。

以下代码示例演示如何使用 GetSecretValue。

所需权限：secretsmanager:GetSecretValue

```
    using System;
    using System.IO;
    using System.Threading.Tasks;
    using Amazon.SecretsManager;
    using Amazon.SecretsManager.Model;

    /// <summary>
    /// This example uses the Amazon Web Service Secrets Manager to retrieve
    /// the secret value for the provided secret name.
    /// </summary>
    public class GetSecretValue
    {
        /// <summary>
        /// The main method initializes the necessary values and then calls
        /// the GetSecretAsync and DecodeString methods to get the decoded
        /// secret value for the secret named in secretName.
        /// </summary>
        public static async Task Main()
        {
            string secretName = "<<{{MySecretName}}>>";
            string secret;
```

```
            IAmazonSecretsManager client = new AmazonSecretsManagerClient();

            var response = await GetSecretAsync(client, secretName);

            if (response is not null)
            {
                secret = DecodeString(response);

                if (!string.IsNullOrEmpty(secret))
                {
                    Console.WriteLine($"The decoded secret value is: {secret}.");
                }
                else
                {
                    Console.WriteLine("No secret value was returned.");
                }
            }
        }

        /// <summary>
        /// Retrieves the secret value given the name of the secret to
        /// retrieve.
        /// </summary>
        /// <param name="client">The client object used to retrieve the secret
        /// value for the given secret name.</param>
        /// <param name="secretName">The name of the secret value to retrieve.</param>
        /// <returns>The GetSecretValueReponse object returned by
        /// GetSecretValueAsync.</returns>
        public static async Task<GetSecretValueResponse> GetSecretAsync(
            IAmazonSecretsManager client,
            string secretName)
        {
            GetSecretValueRequest request = new GetSecretValueRequest()
            {
                SecretId = secretName,
                VersionStage = "AWSCURRENT", // VersionStage defaults to AWSCURRENT if
unspecified.
            };

            GetSecretValueResponse response = null;

            // For the sake of simplicity, this example handles only the most
            // general SecretsManager exception.
```

```
            try
            {
                response = await client.GetSecretValueAsync(request);
            }
            catch (AmazonSecretsManagerException e)
            {
                Console.WriteLine($"Error: {e.Message}");
            }

            return response;
        }

        /// <summary>
        /// Decodes the secret returned by the call to GetSecretValueAsync and
        /// returns it to the calling program.
        /// </summary>
        /// <param name="response">A GetSecretValueResponse object containing
        /// the requested secret value returned by GetSecretValueAsync.</param>
        /// <returns>A string representing the decoded secret value.</returns>
        public static string DecodeString(GetSecretValueResponse response)
        {
            // Decrypts secret using the associated AWS Key Management Service
            // Customer Master Key (CMK.) Depending on whether the secret is a
            // string or binary value, one of these fields will be populated.
            if (response.SecretString is not null)
            {
                var secret = response.SecretString;
                return secret;
            }
            else if (response.SecretBinary is not null)
            {
                var memoryStream = response.SecretBinary;
                StreamReader reader = new StreamReader(memoryStream);
                string decodedBinarySecret =
System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(reader.ReadToEnd()));
                return decodedBinarySecret;
            }
            else
            {
                return string.Empty;
            }
        }
    }
```

使用 Go 获取 Secrets Manager 的密钥值

在应用程序中，您可以通过调用`GetSecretValue`或`BatchGetSecretValue`在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

主题

使用带有客户端缓存的 Go 获取 Secrets Manager 密钥值

在检索密钥时，您可以使用 Secrets Manager 基于 Go 的缓存组件来缓存密钥，以备将来使用。检索已缓存密钥比从 Secrets Manager 中检索密钥的速度要快。由于调用 Secrets Manager API 会产生费用，因此使用缓存可以降低成本。有关检索密钥的所有方法，请参阅 获取秘密。

缓存策略为“最近最少使用 (LRU)”，因此当缓存必须丢弃某个密钥时，它会丢弃最近使用最少的密钥。原定设置下，缓存会每小时刷新一次秘密。您可以配置在缓存中刷新密钥的频率，也可以挂钩到密钥检索中以添加更多功能。

一旦释放缓存引用，缓存便不会进行强制垃圾回收。缓存实施不包括缓存失效。缓存实现侧重于缓存本身，而不是侧重加强安全性或以安全性为重点。如果您需要额外的安全性（例如加密缓存中的项目），请使用提供的接口和抽象方法。

要使用该组件，您必须满足以下条件：

- AWS 适用于 Go 的 SDK。请参阅 the section called “AWS 软件开发工具包”。

要下载源代码，请参阅 S ecrets Manager Go 缓存客户端 GitHub。

要设置 Go 开发环境，请参阅 Go Programming Language 网站上的 Golang 入门。

所需权限：

- `secretsmanager:DescribeSecret`
- `secretsmanager:GetSecretValue`

有关更多信息，请参阅 权限参考。

参考

- type Cache
- 键入 CacheConfig
- 键入 CacheHook

Example 检索密钥

以下代码示例显示了检索密钥的 Lambda 函数。

```
package main

import (
  "github.com/aws/aws-lambda-go/lambda"
  "github.com/aws/aws-secretsmanager-caching-go/secretcache"
)

var (
  secretCache, _ = secretcache.New()
)

func HandleRequest(secretId string) string {
  result, _ := secretCache.GetSecretString(secretId)

  // Use the secret, return success
}

 func main() {
  lambda. Start( HandleRequest)
}
```

type Cache

适用于从 Secrets Manager 请求的密钥的内存中缓存。您使用 the section called “GetSecretString” 或 the section called “GetSecretBinary” 从缓存中检索密钥。

下面的示例演示了如何配置缓存设置。

```
// Create a custom secretsmanager client
client := getCustomClient()
```

```
// Create a custom CacheConfig struct
config := secretcache. CacheConfig{
    MaxCacheSize:  secretcache.DefaultMaxCacheSize + 10,
    VersionStage:  secretcache.DefaultVersionStage,
    CacheItemTTL:  secretcache.DefaultCacheItemTTL,
}

// Instantiate the cache
cache, _ := secretcache.New(
    func( c *secretcache.Cache) {  c. CacheConfig = config },
    func( c *secretcache.Cache) {  c. Client = client },
)
```

有关包括示例在内的更多信息，请参阅 the section called “使用客户端缓存”。

方法

New

```
func New(optFns ...func(*Cache)) (*Cache, error)
```

New 使用功能选项构造密钥缓存，否则将使用默认值。从新会话初始化 SecretsManager 客户端。初始化 CacheConfig 为默认值。使用默认最大大小初始化 LRU 缓存。

GetSecretString

```
func (c *Cache) GetSecretString(secretId string) (string, error)
```

GetSecretString 从缓存中获取给定密钥 ID 的秘密字符串值。返回密钥字符串，如果操作失败则返回错误。

GetSecretStringWithStage

```
func (c *Cache) GetSecretStringWithStage(secretId string, versionStage
string) (string, error)
```

GetSecretStringWithStage 从缓存中获取给定密钥 ID 和版本阶段的秘密字符串值。返回密钥字符串，如果操作失败则返回错误。

GetSecretBinary

```
func (c *Cache) GetSecretBinary(secretId string) ([]byte, error) {
```

GetSecretBinary 从缓存中获取给定密钥 ID 的秘密二进制值。返回密钥二进制值，如果操作失败则返回错误。

GetSecretBinaryWithStage

`func (c *Cache) GetSecretBinaryWithStage(secretId string, versionStage string) ([]byte, error)`

GetSecretBinaryWithStage 从缓存中获取给定密钥 ID 和版本阶段的秘密二进制值。返回密钥二进制值，如果操作失败则返回错误。

键入 CacheConfig

适用于缓存的缓存配置选项，例如最大缓存大小、默认版本阶段，以及已缓存密钥的存活时间 (TTL)。

```
type CacheConfig struct {

    // The maximum cache size. The default is 1024 secrets.
    MaxCacheSize int

    // The TTL of a cache item in nanoseconds. The default is
    // 3.6e10^12 ns or 1 hour.
    CacheItemTTL int64

    // The version of secrets that you want to cache. The default
    // is "AWSCURRENT".
    VersionStage string

    // Used to hook in-memory cache updates.
    Hook CacheHook
}
```

键入 CacheHook

用于挂钩到缓存中以便对存储于缓存中的密钥执行操作的接口。

方法

Put

`Put(data interface{}) interface{}`

使对象为存储在缓存中做好准备。

获取

`Get(data interface{}) interface{}`

从已缓存对象派生对象。

使用 Go AWS SDK 获取 Secrets Manager 密钥值

在应用程序中，您可以通过调用`GetSecretValue`或`BatchGetSecretValue`在任何 AWS SDK 中检索您的密钥。不过，我们建议您通过使用客户端缓存来缓存您的密钥值。缓存密钥可以提高速度并降低成本。

对于 Go 应用程序，请使用 Secrets Manager 基于 Go 的缓存组件或直接使用 `GetSecretValue` 或 `BatchGetSecretValue` 调用 SDK。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：`secretsmanager:GetSecretValue`

```
 // Use this code snippet in your app.
 // If you need more information about configurations or implementing the sample code,
visit the AWS docs:
 // https://aws.github.io/aws-sdk-go-v2/docs/getting-started/

 import (
   "context"
   "log"

   "github.com/aws/aws-sdk-go-v2/aws"
   "github.com/aws/aws-sdk-go-v2/config"
   "github.com/aws/aws-sdk-go-v2/service/secretsmanager"
 )

 func main() {
   secretName := "<<{{MySecretName}}>>"
   region := "<<{{MyRegionName}}>>"

   config, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion(region))
   if err != nil {
     log.Fatal(err)
   }

   // Create Secrets Manager client
```

```
    svc := secretsmanager.NewFromConfig(config)

    input := &secretsmanager.GetSecretValueInput{
      SecretId:     aws.String(secretName),
      VersionStage: aws.String("AWSCURRENT"), // VersionStage defaults to AWSCURRENT if
 unspecified
    }

    result, err := svc.GetSecretValue(context.TODO(), input)
    if err != nil {
      // For a list of exceptions thrown, see
      // https://<<{{DocsDomain}}>>/secretsmanager/latest/apireference/
API_GetSecretValue.html
      log.Fatal(err.Error())
    }

    // Decrypts secret using the associated KMS key.
    var secretString string = *result.SecretString

    // Your code goes here.
  }
```

使用 C++ AWS SDK 获取 Secrets Manager 密钥值

对于 C++ 应用程序，请使用GetSecretValue或直接调用 SDK BatchGetSecretValue。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：`secretsmanager:GetSecretValue`

```
//! Retrieve an AWS Secrets Manager encrypted secret.
/*!
  \param secretID: The ID for the secret.
  \return bool: Function succeeded.
 */
bool AwsDoc::SecretsManager::getSecretValue(const Aws::String &secretID,
                                            const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SecretsManager::SecretsManagerClient
 secretsManagerClient(clientConfiguration);

    Aws::SecretsManager::Model::GetSecretValueRequest request;
    request.SetSecretId(secretID);
```

```
    Aws::SecretsManager::Model::GetSecretValueOutcome getSecretValueOutcome =
 secretsManagerClient.GetSecretValue(
            request);
    if (getSecretValueOutcome.IsSuccess()) {
        std::cout << "Secret is: "
                  << getSecretValueOutcome.GetResult().GetSecretString() << std::endl;
    }
    else {
        std::cerr << "Failed with Error: " << getSecretValueOutcome.GetError()
                  << std::endl;
    }

    return getSecretValueOutcome.IsSuccess();
}
```

使用 JavaScript AWS SDK 获取 Secrets Manager 密钥值

对于 JavaScript 应用程序，请使用getSecretValue或直接调用 SDK batchGetSecretValue。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：secretsmanager:GetSecretValue

```
import {
  GetSecretValueCommand,
  SecretsManagerClient,
} from "@aws-sdk/client-secrets-manager";

export const getSecretValue = async (secretName = "SECRET_NAME") => {
  const client = new SecretsManagerClient();
  const response = await client.send(
    new GetSecretValueCommand({
      SecretId: secretName,
    }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '584eb612-f8b0-48c9-855e-6d246461b604',
  //     extendedRequestId: undefined,
```

```
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   ARN: 'arn:aws:secretsmanager:us-east-1:xxxxxxxxxxxx:secret:binary-
secret-3873048-xxxxxx',
  //   CreatedDate: 2023-08-08T19:29:51.294Z,
  //   Name: 'binary-secret-3873048',
  //   SecretBinary: Uint8Array(11) [
  //      98, 105, 110, 97, 114,
  //     121,  32, 100, 97, 116,
  //      97
  //   ],
  //   VersionId: '712083f4-0d26-415e-8044-16735142cd6a',
  //   VersionStages: [ 'AWSCURRENT' ]
  // }

  if (response.SecretString) {
    return response.SecretString;
  }

  if (response.SecretBinary) {
    return response.SecretBinary;
  }
};
```

使用 Kotlin AWS SDK 获取 Secrets Manager 的密钥值

对于 Kotlin 应用程序，请使用GetSecretValue或BatchGetSecretValue直接调用 SDK。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：`secretsmanager:GetSecretValue`

```
suspend fun getValue(secretName: String?) {
    val valueRequest =
        GetSecretValueRequest {
            secretId = secretName
        }

    SecretsManagerClient { region = "us-east-1" }.use { secretsClient ->
        val response = secretsClient.getSecretValue(valueRequest)
        val secret = response.secretString
```

```
        println("The secret value is $secret")
    }
}
```

使用 PHP AWS 开发工具包获取 Secrets Manager 密钥值

对于 PHP 应用程序，请直接使用 GetSecretValue 或 BatchGetSecretValue 调用 SDK。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：secretsmanager:GetSecretValue

```
<?php

  /**
    * Use this code snippet in your app.
    *
    * If you need more information about configurations or implementing the sample
 code, visit the AWS docs:
    * https://aws.amazon.com/developer/language/php/
    */

  require 'vendor/autoload.php';

  use Aws\SecretsManager\SecretsManagerClient;
  use Aws\Exception\AwsException;

  /**
    * This code expects that you have AWS credentials set up per:
    * https://<<{{DocsDomain}}>>/sdk-for-php/v3/developer-guide/guide_credentials.html
    */

  // Create a Secrets Manager Client
  $client = new SecretsManagerClient([
      'profile' => 'default',
      'version' => '2017-10-17',
      'region' => '<<{{MyRegionName}}>>',
  ]);

  $secret_name = '<<{{MySecretName}}>>';

  try {
      $result = $client->getSecretValue([
```

```
          'SecretId' => $secret_name,
      ]);
  } catch (AwsException $e) {
      // For a list of exceptions thrown, see
      // https://<<{{DocsDomain}}>>/secretsmanager/latest/apireference/
API_GetSecretValue.html
      throw $e;
  }

  // Decrypts secret using the associated KMS key.
  $secret = $result['SecretString'];

  // Your code goes here
```

使用 Ruby AWS SDK 获取 Secrets Manager 密钥值

对于 Ruby 应用程序，请直接使用 get_secret_value 或 batch_get_secret_value 调用 SDK。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：secretsmanager:GetSecretValue

```
  # Use this code snippet in your app.
  # If you need more information about configurations or implementing the sample code,
 visit the AWS docs:
  # https://aws.amazon.com/developer/language/ruby/

  require 'aws-sdk-secretsmanager'

  def get_secret
    client = Aws::SecretsManager::Client.new(region: '<<{{MyRegionName}}>>')

    begin
      get_secret_value_response = client.get_secret_value(secret_id:
 '<<{{MySecretName}}>>')
    rescue StandardError => e
      # For a list of exceptions thrown, see
      # https://<<{{DocsDomain}}>>/secretsmanager/latest/apireference/
API_GetSecretValue.html
      raise e
    end
```

```
    secret = get_secret_value_response.secret_string
    # Your code goes here.
  end
```

使用 Rust AWS SDK 获取 Secrets Manager 密钥值

对于 Rust 应用程序，请使用GetSecretValue或直接调用 SDK BatchGetSecretValue。

以下代码示例展示了如何获取 Secrets Manager 密钥值。

所需权限：secretsmanager:GetSecretValue

```
async fn show_secret(client: &Client, name: &str) -> Result<(), Error> {
    let resp = client.get_secret_value().secret_id(name).send().await?;

    println!("Value: {}", resp.secret_string().unwrap_or("No value!"));

    Ok(())
}
```

使用获取秘密值 AWS CLI

所需权限：secretsmanager:GetSecretValue

Example 检索密钥的加密密钥值

以下 get-secret-value 示例获取当前密钥值。

```
aws secretsmanager get-secret-value \
    --secret-id MyTestSecret
```

Example 检索之前的密钥值

以下 get-secret-value 示例获取之前的密钥值。

```
aws secretsmanager get-secret-value \
        --secret-id MyTestSecret
        --version-stage AWSPREVIOUS
```

使用批量获取一组机密 AWS CLI

所需权限：

- `secretsmanager:BatchGetSecretValue`
- `secretsmanager:GetSecretValue`您要检索的每个密钥的权限。
- 如果您使用筛选器，则还必须拥有 `secretsmanager:ListSecrets`。

有关权限策略的示例，请参阅 the section called “示例：批量检索一组机密值的权限”。

> **Important**
>
> 如果您的 VPCE 策略拒绝在您正在检索的群组中检索单个秘密的权限，则 `BatchGetSecretValue` 不会返回任何秘密值，并且会返回错误。

Example 检索按名称列出的一组秘密的秘密值

以下 `batch-get-secret-value` 示例获取三个秘密的秘密值。

```
aws secretsmanager batch-get-secret-value \
          --secret-id-list MySecret1 MySecret2 MySecret3
```

Example 检索筛选器选择的一组秘密的秘密值

以下 `batch-get-secret-value` 示例获取具有名为“Test”的标签的秘密的秘密值。

```
aws secretsmanager batch-get-secret-value \
          --filters Key="tag-key",Values="Test"
```

使用 AWS 控制台获取密钥值

检索密钥（控制台）

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在秘密列表中，选择要检索的秘密。
3. 在密钥值部分中，选择检索密钥值。

Secrets Manager 显示秘密的当前版本 (AWSCURRENT)。要查看秘密的其他版本，例如 AWSPREVIOUS 或带有自定义标签的版本，请使用 the section called “AWS CLI”。

在中使用 AWS Secrets Manager 秘密 AWS Batch

AWS Batch 可帮助您在上运行批量计算工作负载 AWS Cloud。使用 AWS Batch，您可以将敏感数据注入作业，方法是将敏感数据存储在 AWS Secrets Manager 机密中，然后在作业定义中引用它们。有关更多信息，请参阅使用 Secrets Manager 指定敏感数据。

在 AWS CloudFormation 资源中获取 AWS Secrets Manager 秘密

使用 AWS CloudFormation，您可以检索密钥以在其他 AWS CloudFormation 资源中使用。常见场景是首先使用 Secret Manager 生成的密码创建密钥，然后从该密钥中检索用户名和密码，以用作新数据库的凭证。有关使用创建密钥的信息 AWS CloudFormation，请参阅AWS CloudFormation。

要检索 AWS CloudFormation 模板中的密钥，请使用动态引用。创建堆栈时，动态引用会将密钥值提取到 AWS CloudFormation 资源中，因此您不必对机密信息进行硬编码。相反，您可以通过名称或 ARN 来引用密钥。您可以在任何资源属性中使用对密钥的动态引用。您不能在资源元数据（例如 AWS::CloudFormation::Init）中使用对密钥的动态引用，因为那样会使密钥值在控制台中可见。

密钥的动态引用模式如下：

```
{{resolve:secretsmanager:secret-id:SecretString:json-key:version-stage:version-id}}
```

secret-id

密钥的名称或 ARN。要访问您 AWS 账户中的密钥，您可以使用该密钥名称。要访问其他 AWS 账户中的密钥，请使用该密钥的 ARN。

json-key（可选）

要检索其值的键值对的键名称。如果未指定json-key，则 AWS CloudFormation 检索整个机密文本。此分段不得包含冒号字符（：）。

version-stage（可选）

要使用的密钥的版本。Secrets Manager 在轮换过程中使用暂存标注来跟踪不同的版本。如果您使用 version-stage，则不要指定 version-id。如果您既未指定 version-stage，也未指定 version-id，则原定设置将为 AWSCURRENT 版本。此分段不得包含冒号字符（：）。

version-id（可选）

要使用的密钥版本的唯一标识符。如果指定 `version-id`，则不要指定 `version-stage`。如果您既未指定 `version-stage`，也未指定 `version-id`，则原定设置将为 `AWSCURRENT` 版本。此分段不得包含冒号字符（：）。

有关更多信息，请参阅使用动态引用指定 Secrets Manager 秘密。

> **Note**
>
> 不要使用反斜杠(\)作为最终值来创建动态引用。 AWS CloudFormation 无法解析这些引用，这会导致资源故障。

在亚马逊 Elastic Kubernetes Service 中使用 AWS Secrets Manager 密钥

要将 Secrets Manager 中的密钥显示为挂载在 Amazon EK S 容器中的文件，你可以使用 Kubernetes S AWS ecrets Store CSI 驱动程序的密钥和配置提供程序 (ASCP)。ASCP 可与运行亚马逊 EC2 节点组的亚马逊 Elastic Kubernetes Service（亚马逊 EKS）1.17+ 配合使用。 AWS Fargate 不支持节点组。使用 ASCP，您可以在 Secrets Manager 中存储并管理密钥，然后通过 Amazon EKS 上运行的工作负载检索。如果密钥包含多个 JSON 格式的键/值对，您可以选择要在 Amazon EKS 中挂载的密钥/值对。ASCP 使用 JMESTath 语法来查询密钥中的键/值对。ASCP 还适用于 Parameter Store 参数。

如果您使用私有 Amazon EKS 集群，请确保该集群所在的 VPC 具有Secrets Manager 端点。Secrets Store CSI Driver 使用端点调用 Secrets Manager。有关在 VPC 中创建端点的信息，请参阅 VPC 端点。

如果对密钥使用 Secrets Manager 自动轮换，还可以使用 Secrets Store CSI Driver 轮换协调程序功能，确保从 Secrets Manager 中检索最新的密码。有关更多信息，请参阅已安装的内容和同步的 Kubernetes Secrets 的自动轮换。

主题

- 步骤 1：设置访问控制
- 步骤 2：安装和配置 ASCP
- 步骤 3：确定要挂载哪些密钥
- 第 4 步：将密钥作为文件挂载到 Amazon EKS 窗格中

- 故障排除
- SecretProviderClass

步骤 1：设置访问控制

ASCP 会检索 Amazon EKS 容器身份并将其交换为 IAM 角色。您可以在 IAM 策略中为该 IAM 角色设置权限。当 ASCP 担任 IAM 角色时，它可以访问您授权的密钥。除非将其与 IAM 角色关联，否则其他容器无法访问密钥。

如果 Kubernetes 限制了来自 ASCP 的查询区域和 IAM 角色的调用，则可以使用更改限制配额，如步骤 2 所示。`helm install`

向你的 Amazon EKS Pod 授予访问 Secrets Manager 中密钥的权限

1. 创建权限策略，向 Pod 需要访问的机密授予`secretsmanager:GetSecretValue`和`secretsmanager:DescribeSecret`权限。有关策略示例，请参阅the section called “示例：读取和描述个人机密的权限”。
2. 为集群创建 IAM OpenID Connect (OIDC) 提供商（如果还没有）。有关更多信息，请参阅 A mazon EKS 用户指南中的为您的集群创建 IAM OIDC 提供商。
3. 为服务账号创建 IAM 角色并将策略附加到该账户。有关更多信息，请参阅 A mazon EKS 用户指南中的为服务账户创建 IAM 角色。
4. 如果您使用私有 Amazon EKS 集群，请确保集群所在的 VPC 具有 AWS STS 终端节点。有关创建终端节点的信息，请参阅AWS Identity and Access Management 用户指南中的接口 VPC 终端节点。

步骤 2：安装和配置 ASCP

ASCP 可在 secrets-store-csi-provider-aws 存储 GitHub 库中找到。回购还包含用于创建和装载密钥的 YAML 文件示例。

在安装过程中，您可以将 ASCP 配置为使用 FIPS 端点。有关 终端节点的列表，请参阅the section called “Secrets Manager 端点”。

使用 Helm 安装 ASCP

1. 为确保存储库指向最新的图表，请使用 `helm repo update`.
2. 添加 Secrets Store CSI 驱动程序图表。

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
```

3. 安装图表。要配置限制，请添加以下标志：`--set-json 'k8sThrottlingParams={"qps": "<number of queries per second>", "burst": "<number of queries per second>"}'`

```
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
```

4. 添加 ASCP 图表。

```
helm repo add aws-secrets-manager https://aws.github.io/secrets-store-csi-driver-provider-aws
```

5. 安装图表。要使用 FIPS 端点，请添加以下标志：`--set useFipsEndpoint=true`

```
helm install -n kube-system secrets-provider-aws aws-secrets-manager/secrets-store-csi-driver-provider-aws
```

在存储库中使用 YAML 进行安装

- 使用以下命令。

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
kubectl apply -f https://raw.githubusercontent.com/aws/secrets-store-csi-driver-provider-aws/main/deployment/aws-provider-installer.yaml
```

步骤 3：确定要挂载哪些密钥

要确定 ASCP 将哪些密钥作为文件系统上的文件挂载在 Amazon EKS 中，您需要创建一个 the section called “SecretProviderClass” YAML 文件。列SecretProviderClass出了要装载的密钥和装载它们的文件名。SecretProviderClass 必须与该文件引用的 Amazon EKS 容器位于同一名称空间。

以下示例演示了如何使用 SecretProviderClass 来描述要挂载的密钥以及如何命名安装在 Amazon EKS 容器组中的文件。

示例：

- 示例：按名称或 ARN 挂载密钥
- 示例：从密钥挂载键/值对
- 示例：为多区域密钥定义失效转移区域
- 示例：选择要挂载的失效转移密钥

示例：按名称或 ARN 挂载密钥

以下示例显示了 SecretProviderClass，它将在 Amazon EKS 中挂载三个文件：

1. 由完整 ARN 指定的密钥。
2. 由名称指定的密钥。
3. 密钥的特定版本。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-secrets
spec:
  provider: aws
  parameters:
    objects: |
        - objectName: "arn:aws:secretsmanager:us-east-2:111122223333:secret:MySecret2-
d4e5f6"
        - objectName: "MySecret3"
          objectType: "secretsmanager"
        - objectName: "MySecret4"
          objectType: "secretsmanager"
          objectVersionLabel: "AWSCURRENT"
```

示例：从密钥挂载键/值对

以下示例显示了 SecretProviderClass，它将在 Amazon EKS 中挂载三个文件：

1. 由完整 ARN 指定的密钥。

2. username 键/值对来自同一个密钥。

3. password 键/值对来自同一个密钥。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-secrets
spec:
  provider: aws
  parameters:
    objects: |
      - objectName: "arn:aws:secretsmanager:us-east-2:111122223333:secret:MySecret-
a1b2c3"
        jmesPath:
            - path: username
              objectAlias: dbusername
            - path: password
              objectAlias: dbpassword
```

示例：为多区域密钥定义失效转移区域

为了在连接中断期间提供可用性或对于灾难恢复配置，ASCP 支持自动失效转移功能，以从辅助区域检索密钥。

以下示例显示了 SecretProviderClass，其检索复制到多个区域的密钥。在此示例中，ASCP 尝试从 us-east-1 和 us-east-2 中检索密钥。如果任一区域返回 4xx 错误（例如身份验证问题），ASCP 都不会挂载任何一个密钥。如果成功从 us-east-1 中检索到密钥，则 ASCP 会挂载该密钥值。如果未成功从 us-east-1 中检索到密钥，但已成功从 us-east-2 中检索到密钥，则 ASCP 会挂载该密钥值。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-secrets
spec:
  provider: aws
  parameters:
    region: us-east-1
    failoverRegion: us-east-2
    objects: |
```

```
      - objectName: "MySecret"
```

示例：选择要挂载的失效转移密钥

以下示例显示了 SecretProviderClass，它指定在失效转移时要挂载哪个密钥。失效转移密钥不是副本。在此示例中，ASCP 尝试检索 objectName 指定的两个密钥。如果任何一个返回 4xx 错误（例如身份验证问题），ASCP 都不会挂载任何一个密钥。如果成功从 us-east-1 中检索到密钥，则 ASCP 会挂载该密钥值。如果未成功从 us-east-1 中检索到密钥，但已成功从 us-east-2 中检索到密钥，则 ASCP 会挂载该密钥值。Amazon EKS 中挂载的文件名为 MyMountedSecret。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-secrets
spec:
  provider: aws
  parameters:
    region: us-east-1
    failoverRegion: us-east-2
    objects: |
      - objectName: "arn:aws:secretsmanager:us-east-1:111122223333:secret:MySecret-
a1b2c3"
        objectAlias: "MyMountedSecret"
        failoverObject:
          - objectName: "arn:aws:secretsmanager:us-
east-2:111122223333:secret:MyFailoverSecret-d4e5f6"
```

第 4 步：将密钥作为文件挂载到 Amazon EKS 窗格中

在 Amazon EKS 中挂载机密

1. 使用命令SecretProviderClass将应用于 pod kubectl apply -f ExampleSecretProviderClass.yaml。
2. 使用命令部署你的 pod kubectl apply -f ExampleDeployment.yaml。
3. ASCP 会装载这些文件。

故障排除

您可以通过描述容器部署来查看大多数错误。

查看容器的错误消息

1. 用以下命令获取容器名称列表。如果您没有使用默认命名空间，请使用 -n <NAMESPACE>。

```
kubectl get pods
```

2. 要描述容器，请在以下命令中为 *<PODID>* 使用在上一步中找到的容器 ID。如果没有使用默认命名空间，请使用 -n <NAMESPACE>。

```
kubectl describe pod/<PODID>
```

查看 ASCP 的错误

- 要在提供者日志中查找更多信息，请在以下命令中<PODID>使用 csi-secrets-store-provider-aws pod 的 ID。

```
kubectl -n kube-system get pods
kubectl -n kube-system logs pod/<PODID>
```

SecretProviderClass

您可以使用 YAML 来描述要使用 ASCP 在 Amazon EKS 中挂载哪些机密。有关示例，请参阅the section called “按名称或 ARN 挂载密钥”。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
   name: <NAME>
spec:
  provider: aws
  parameters:
    region:
    failoverRegion:
    pathTranslation:
    objects:
```

字段 parameters 包含挂载请求的详细信息。

region

（可选）密钥。 AWS 区域 如果不使用此字段，ASCP 将从节点上的注释中查找 “区域”。查找会增加挂载请求的开销，因此我们建议为使用大量容器的群集提供区域。

如果您还指定 `failoverRegion`，ASCP 会尝试从两个区域检索密钥。如果任一区域返回 4xx 错误（例如身份验证问题），ASCP 都不会挂载任何一个密钥。如果成功从 `region` 中检索到密钥，则 ASCP 会挂载该密钥值。如果未成功从 `region` 中检索到密钥，但已成功从 `failoverRegion` 中检索到密钥，则 ASCP 会挂载该密钥值。

failoverRegion

（可选）如果您包含此字段，ASCP 会尝试从 `region` 中定义的区域和此字段检索密钥。如果任一区域返回 4xx 错误（例如身份验证问题），ASCP 都不会挂载任何一个密钥。如果成功从 `region` 中检索到密钥，则 ASCP 会挂载该密钥值。如果未成功从 `region` 中检索到密钥，但已成功从 `failoverRegion` 中检索到密钥，则 ASCP 会挂载该密钥值。有关如何使用此字段的示例，请参阅 为多区域密钥定义失效转移区域。

pathTranslation

（可选）如果 Amazon EKS 中的文件名包含路径分隔符则要使用的单个替换字符，例如 Linux 上的斜杠 (/)。ASCP 无法创建包含路径分隔符的挂载文件。相反，ASCP 使用不同的字符替换路径分隔符。如果不使用此字段，替换字符为下划线 (_)，因此，例如 `My/Path/Secret` 挂载为 `My_Path_Secret`。

要防止字符替换，请输入字符串 `False`。

objects

包含要挂载密钥的 YAML 声明字符串。我们建议使用 YAML 多行字符串或竖线 (|) 字符。

objectName

密钥的名称或完整 ARN。如果使用 ARN，可以省略 `objectType`。除非指定 `objectAlias`，此字段将成为 Amazon EKS 容器组中密钥的文件名。如果使用 ARN，则 ARN 中的区域必须与字段 `region` 匹配。如果包括 `failoverRegion`，则此字段表示主 `objectName`。

objectType

如果不将 Secrets Manager ARN 用于 `objectName`，需要这个操作 可以是 `secretsmanager` 或 `ssmparameter`。

objectAlias

（可选）Amazon EKS 容器中密钥的文件名。如果不指定此字段，则 objectName 作为文件名显示。

ObjectVersion

（可选）密钥的版本 ID。不推荐，因为每次更新密钥时都必须更新版本 ID。默认情况下，使用最新版本。如果包括 failoverRegion，则此字段表示主 objectVersion。

objectVersionLabel

（可选）版本的别名。默认为最新版本 AWSCURRENT。有关更多信息，请参阅 the section called “秘密版本”。如果包括 failoverRegion，则此字段表示主 objectVersionLabel。

JMESPath

（可选）密钥中的键映射到要在 Amazon EKS 中挂载的文件。要使用此字段，密钥值必须采用 JSON 格式。如果使用此字段，必须包含子字段 path 和 objectAlias。

path

密钥值 JSON 中的键/值对中的键。如果该字段包含连字符，请使用单引号对其进行转义，例如：path: '"hyphenated-path"'

objectAlias

要挂载在 Amazon EKS 容器中的文件名。如果该字段包含连字符，请使用单引号对其进行转义，例如：objectAlias: '"hyphenated-alias"'

failoverObject

（可选）如果您指定此字段，ASCP 会尝试检索主 objectName 中指定的密钥和 failoverObject objectName 子字段中指定的密钥。如果任何一个返回 4xx 错误（例如身份验证问题），ASCP 都不会挂载任何一个密钥。如果成功从主 objectName 中检索到密钥，则 ASCP 会挂载该密钥值。如果未成功从主 objectName 中检索到密钥，但已成功从失效转移 objectName 中检索到密钥，则 ASCP 会挂载该密钥值。如果包含此字段，责必须包含字段 objectAlias。有关如何使用此字段的示例，请参阅 选择要挂载的失效转移密钥。

当失效转移密钥不是副本时，通常使用此字段。有关如何指定副本的示例，请参阅 为多区域密钥定义失效转移区域。

objectName

失效转移密钥的名称或完整 ARN。如果使用 ARN，则 ARN 中的区域必须与字段 failoverRegion 匹配。

ObjectVersion

（可选）密钥的版本 ID。必须与主 `objectVersion` 匹配。不推荐，因为每次更新密钥时都必须更新版本 ID。默认情况下，使用最新版本。

objectVersionLabel

（可选）版本的别名。默认为最新版本 AWSCURRENT。有关更多信息，请参阅 the section called “秘密版本”。

在 GitHub 工作中使用 AWS Secrets Manager 秘密

要在 GitHub 作业中使用密钥，您可以使用 GitHub 操作从 AWS Secrets Manager 中检索密钥并将其作为屏蔽的环境变量添加到 GitHub 工作流程中。有关 GitHub 操作的更多信息，请参阅了解GitHub 文档中的 GitHub 操作。

当你向 GitHub 环境中添加密钥时，该密钥可用于 GitHub 工作中的所有其他步骤。按照操作安全强化中的指导进行 GitHub 操作，以帮助防止环境中的密钥被滥用。

您可以将密钥值中的整个字符串设置为环境变量值，或者如果字符串为 JSON，则可以解析 JSON，以为每个 JSON 键值对设置单独的环境变量。如果密钥值是二进制，则操作会将密钥值转换为字符串。

若要查看从密钥创建的环境变量，请启用调试日志记录。有关更多信息，请参阅GitHub 文档中的启用调试日志记录。

要使用根据您的密钥创建的环境变量，请参阅GitHub 文档中的环境变量。

先决条件

要使用此操作，您首先需要配置 AWS 凭证，然后使用`configure-aws-credentials`步骤 AWS 区域 在您的 GitHub 环境中进行设置。按照配置 AWS 凭证操作中的说明进行 GitHub 操作，以便使用 GitHub OIDC 提供程序直接担任角色。这让您能够使用短期凭证，避免在 Secrets Manager 之外存储额外的访问密钥。

操作承担的 IAM 角色必须具有下列权限：

- 您要检索的密钥的 `GetSecretValue` 权限。
- 所有密钥的 `ListSecrets` 权限。
- （可选）`Decrypt`上 KMS key 是否使用加密密钥 客户托管式密钥。

有关更多信息，请参阅 身份验证和访问控制。

使用量

若要使用该操作，请在工作流程中添加一个使用以下语法的步骤。

```
- name: Step name
  uses: aws-actions/aws-secretsmanager-get-secrets@v2
  with:
    secret-ids: |
      secretId1
      ENV_VAR_NAME, secretId2
    name-transformation: (Optional) uppercase|lowercase|none
    parse-json-secrets: (Optional) true|false
```

参数

`secret-ids`

密钥 ARN、名称和名称前缀。

若要设置环境变量名称，请在密钥 ID 前输入该名称，然后输入逗号。例如，`ENV_VAR_1, secretId` 从密钥 `secretId` 中创建名为 ENV_VAR_1 的环境变量。环境变量的名称可以包含小写字母、数字和下划线。

若要使用前缀，请输入至少三个字符，然后输入星号。例如，`dev*` 匹配名称以 dev 开头的所有密钥。最多可以检索 100 个匹配密钥。如果您设置了变量名称，并且前缀与多个密钥匹配，则操作将失败。

`name-transformation`

默认情况下，该步骤从密钥名称创建每个环境变量名称，并转换为仅包含大写字母、数字和下划线，防止名称以数字开头。对于名称中的字母，您可以将步骤配置为使用小写字母，`lowercase`也可以不更改字母的大`none`小写。默认值为 `uppercase`。

`parse-json-secrets`

（可选）默认情况下，该操作将环境变量值设置为密钥值中的整个 JSON 字符串。设置`parse-json-secrets`为可`true`为 JSON 中的每个键值对创建环境变量。

请注意，如果 JSON 使用区分大小写的密钥（例如“name”和“Name”），则该操作将出现重复的名称冲突。在这种情况下，请将 `parse-json-secrets` 设置为 `false` 并单独解析 JSON 密钥值。

环境变量命名

操作创建的环境变量的命名与它们来自的密钥相同。环境变量的命名要求比机密更严格，因此该操作会转换机密名称以满足这些要求。例如，该操作将把小写字母转换为大写字母。例如MYSECRET_KEYNAME，如果您解析密钥的 JSON，则环境变量名称将同时包含密钥名称和 JSON 密钥名称。您可以将操作配置为不转换小写字母。

如果两个环境变量的名称相同，则操作将失败。在这种情况下，必须将要用于环境变量的名称指定为别名。

名称何时可能发生冲突的示例：

- 名为 “” MySecret 的密钥和名为 “mysecret” 的密钥都将成为名为 “MYSECRET” 的环境变量。
- 名为 “secret_keyname” 的密钥和名为 “Secret” 且密钥名为 “keyname” 的 JSON 解析密钥都将成为名为 “SECRET_KEYNAME” 的环境变量。

您可以通过指定别名来设置环境变量名称，如以下示例所示，它会创建一个名为的变量ENV_VAR_NAME。

```
secret-ids: |
  ENV_VAR_NAME, secretId2
```

空白别名

- 如果您设置parse-json-secrets: true并输入空白别名，后跟逗号，然后输入密钥 ID，则操作会将环境变量命名为与解析后的 JSON 密钥相同。变量名不包括机密名称。

  如果密钥不包含有效的 JSON，则该操作会创建一个环境变量并将其命名为与密钥名称相同。
- 如果您设置parse-json-secrets: false并输入空白别名，后跟逗号和机密 ID，则操作会像未指定别名一样命名环境变量。

以下示例显示了一个空白的别名。

```
,secret2
```

示例

Example 1 按名称和 ARN 获取密钥

下列示例为按名称和 ARN 标识的密钥创建环境变量。

```
- name: Get secrets by name and by ARN
  uses: aws-actions/aws-secretsmanager-get-secrets@v2
  with:
    secret-ids: |
      exampleSecretName
      arn:aws:secretsmanager:us-east-2:123456789012:secret:test1-a1b2c3
      0/test/secret
      /prod/example/secret
      SECRET_ALIAS_1,test/secret
      SECRET_ALIAS_2,arn:aws:secretsmanager:us-east-2:123456789012:secret:test2-a1b2c3
      ,secret2
```

已创建的环境变量：

```
EXAMPLESECRETNAME: secretValue1
TEST1: secretValue2
_0_TEST_SECRET: secretValue3
_PROD_EXAMPLE_SECRET: secretValue4
SECRET_ALIAS_1: secretValue5
SECRET_ALIAS_2: secretValue6
SECRET2: secretValue7
```

Example 2 获取所有以前缀开头的密钥

下列示例为名称以 *beta* 开头的所有密钥创建环境变量。

```
- name: Get Secret Names by Prefix
  uses: 2
  with:
    secret-ids: |
      beta*    # Retrieves all secrets that start with 'beta'
```

已创建的环境变量：

```
BETASECRETNAME: secretValue1
BETATEST: secretValue2
```

```
BETA_NEWSECRET: secretValue3
```

Example 3 在密钥中解析 JSON

下列示例通过解析密钥中的 JSON 来创建环境变量。

```
- name: Get Secrets by Name and by ARN
  uses: aws-actions/aws-secretsmanager-get-secrets@v2
  with:
    secret-ids: |
      test/secret
      ,secret2
    parse-json-secrets: true
```

密钥 `test/secret` 具有下列密钥值。

```
{
  "api_user": "user",
  "api_key": "key",
  "config": {
    "active": "true"
  }
}
```

密钥 `secret2` 具有下列密钥值。

```
{
  "myusername": "alejandro_rosalez",
  "mypassword": "EXAMPLE_PASSWORD"
}
```

已创建的环境变量：

```
TEST_SECRET_API_USER: "user"
TEST_SECRET_API_KEY: "key"
TEST_SECRET_CONFIG_ACTIVE: "true"
MYUSERNAME: "alejandro_rosalez"
MYPASSWORD: "EXAMPLE_PASSWORD"
```

Example 4 环境变量名使用小写字母

以下示例创建了一个名称为小写的环境变量。

```
- name: Get secrets
  uses: aws-actions/aws-secretsmanager-get-secrets@v2
  with:
    secret-ids: exampleSecretName
    name-transformation: lowercase
```

环境变量已创建：

```
examplesecretname: secretValue
```

在 AWS IoT Greengrass 中使用 AWS Secrets Manager 密钥

AWS IoT Greengrass 是将云功能扩展到本地设备的软件。这使得设备可以更靠近信息源来收集和分析数据，自主响应本地事件，同时在本地网络上彼此安全地通信。

您可以从 Greengrass 设备对服务和应用程序进行身份验证，而无需对密码、令牌或其他密钥进行硬编码。您可以用 AWS Secrets Manager 在云中安全地存储和管理密钥。AWS IoT Greengrass 将 Secrets Manager 扩展到 Greengrass 核心设备，从而使连接器和 Lambda 函数可以使用本地密钥与服务和应用程序交互。

要将密钥集成到 Greengrass 组中，您需要创建一个引用 Secrets Manager 密钥的组资源。此密钥资源使用关联 ARN 引用云密钥。要了解如何创建、管理和使用密钥资源，请参阅 AWS IoT 开发人员指南中的使用密钥资源。

将密钥部署到 AWS IoT Greengrass 内核，请参阅将密钥部署到 AWS IoT Greengrass 核心。

在 AWS Lambda 函数中使用 AWS Secrets Manager 密钥

您可以使用 AWS 参数和密钥 Lambda 扩展来检索和缓存 Lambda 函数中的 AWS Secrets Manager 密钥，而无需使用软件开发工具包。检索已缓存密钥比从 Secrets Manager 中检索密钥的速度要快。由于调用 Secrets Manager API 会产生费用，因此使用缓存可以降低成本。该扩展可以检索 Secrets Manager 密钥和 Parameter Store 参数。有关 Parameter Store 的信息，请参阅《AWS Systems Manager 用户指南》中的 Parameter Store integration with Lambda extensions（Parameter Store 与 Lambda 扩展集成）。

Lambda 扩展是配套进程，其增加了 Lambda 函数的功能。有关更多信息，请参阅《Lambda 开发人员指南》中的 Lambda extensions（Lambda 扩展）。有关在容器镜像中使用扩展的信息，请参阅在容器镜像中使用 Lambda 层和扩展。Lambda 使用 Ama CloudWatch zon 日志记录有关扩展程序的执行信

息以及该函数。默认情况下，扩展程序只记录最少量的信息 CloudWatch。若要记录更多详细信息，请将环境变量 PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL 设置为 debug。

为提供用于参数和密钥的内存缓存，该扩展向 Lambda 环境公开了本地 HTTP 端点，即 localhost 端口 2773。您可以通过设置环境变量 PARAMETERS_SECRETS_EXTENSION_HTTP_PORT 来配置端口。

Lambda 会实例化与函数所需的并发级别相对应的单独实例。每个实例都是独立的，并维护自己的配置数据本地缓存。有关 Lambda 实例和并发的更多信息，请参阅《Lambda 开发人员指南》中的 Managing concurrency for a Lambda function（管理 Lambda 函数并发）。

若要为 ARM 添加扩展，您必须使用 Lambda 函数的 arm64 架构。有关更多信息，请参阅《Lambda 开发人员指南》中的 Lambda instruction set architectures（Lambda 指令集架构）。扩展支持 ARM 在以下区域可用：亚太地区（孟买）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、欧洲（苏黎世）、美国东部（弗吉尼亚州北部）、欧洲地区（伦敦）、欧洲（西班牙）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（海得拉巴）和亚太地区（悉尼）。

该扩展使用 AWS 客户端。有关配置 AWS 客户端的信息，请参阅 AWS SDK 和工具参考指南中的设置参考。如果您的 Lambda 函数在 VPC 中运行，则需要创建一个 VPC 终端节点，以便扩展程序可以调用 Secrets Manager。有关更多信息，请参阅 VPC 端点。

所需权限：

- Lambda 执行角色必须拥有该密secretsmanager:GetSecretValue钥的权限。
- 如果密钥是使用客户托管密钥而不是加密的 AWS 托管式密钥 aws/secretsmanager，则执行角色还需要kms:Decrypt获得 KMS 密钥的权限。

使用 AWS 参数和密钥 Lambda 扩展

1. 将名为 “AWS 参数和密钥 Lambda 扩展” 的AWS 层添加到您的函数中。有关说明，请参阅 Lambda 开发人员指南中的向函数添加层。如果您使用 AWS CLI 来添加图层，则需要扩展程序的 ARN。有关 ARN 的列表，请参阅《AWS Systems Manager 用户指南》中的 AWS 参数和秘密 Lambda 扩展 ARN。
2. 授予 Lambda 执行角色访问密钥的权限：
   - 密钥的 secretsmanager:GetSecretValue 权限。请参阅 the section called “示例：检索单个秘密值的权限”。
   - （可选）如果使用客户托管密钥而不是加密密钥 AWS 托管式密钥 aws/secretsmanager，则执行角色还需要kms:Decrypt获得 KMS 密钥的权限。

- 您可以将基于属性的访问权限控制（ABAC）与 Lambda 角色结合使用，以允许对账户中的密钥进行更精细的访问。有关更多信息，请参阅 the section called “示例：使用标签控制对密钥的访问” 和 the section called “示例：限制对标签与密钥标签匹配的标识的访问”。

3. 使用 Lambda 环境变量配置缓存。
4. 若要从扩展缓存中检索密钥，您首先需要将 `X-AWS-Parameters-Secrets-Token` 添加到请求标头中。将令牌设置为 `AWS_SESSION_TOKEN`，Lambda 为所有正在运行的函数提供此令牌。使用此标头表示调用方在 Lambda 环境中。

   下列 Python 示例说明如何添加标头。

   ```
   import os
   headers = {"X-Aws-Parameters-Secrets-Token": os.environ.get('AWS_SESSION_TOKEN')}
   ```

5. 若要在 Lambda 函数中检索密钥，请使用下列 HTTP GET 请求之一：

   - 要检索密钥，对于 `secretId`，请指定密钥的 ARN 或名称。

     ```
     GET: /secretsmanager/get?secretId=secretId
     ```

   - 要通过暂存标签检索先前的密钥值或特定版本，对于 `secretId`，请使用密钥的 ARN 或名称，对于 `versionStage`，请使用暂存标签。

     ```
     GET: /secretsmanager/get?secretId=secretId&versionStage=AWSPREVIOUS
     ```

   - 要通过 ID 检索特定密钥版本，对于 `secretId`，请使用密钥的 ARN 或名称，对于 `versionId`，请使用版本 ID。

     ```
     GET: /secretsmanager/get?secretId=secretId&versionId=versionId
     ```

   Example 检索密钥 (Python)

   下列 Python 示例说明如何使用 `json.loads` 检索密钥并解析结果。

   ```
   secrets_extension_endpoint = "http://localhost:" + \
       secrets_extension_http_port + \
       "/secretsmanager/get?secretId=" + \
       <secret_name>

     r = requests.get(secrets_extension_endpoint, headers=headers)
   ```

```
 secret = json.loads(r.text)["SecretString"] # load the Secrets Manager response
into a Python dictionary, access the secret
```

AWS 参数和密钥 Lambda Extension 环境变量

您可以使用下列环境变量配置扩展。

有关如何使用环境变量的更多信息，请参阅《Lambda 开发者指南》中的 Using Lambda environment variables（使用 Lambda 环境变量）。

`PARAMETERS_SECRETS_EXTENSION_CACHE_ENABLED`

设置为 true，以缓存参数和密钥。设置为 false，以不进行缓存。默认设置为 true。

`PARAMETERS_SECRETS_EXTENSION_CACHE_SIZE`

要缓存的密钥和参数的最大数量。值必须介于 0 到 1000 之间。值 0 表示无缓存。如果 `SSM_PARAMETER_STORE_TTL` 和 `SECRETS_MANAGER_TTL` 均为 0，则将忽略此变量。默认为 1000。

`PARAMETERS_SECRETS_EXTENSION_HTTP_PORT`

本地 HTTP 服务器的端口。默认为 2773。

`PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL`

扩展的日志记录级别为：`debug`、`info`、`warn`、`error` 或 `none`。设置为 `debug` 以查看缓存配置。默认值为 `info`。

`PARAMETERS_SECRETS_EXTENSION_MAX_CONNECTIONS`

扩展用于向 Parameter Store 或 Secrets Manager 发出请求的 HTTP 客户端的最大连接数。这是各个客户端的配置。默认为 3。

`SECRETS_MANAGER_TIMEOUT_MILLIS`

对 Secrets Manager 的请求超时（以毫秒为单位）。值 0 表示没有超时。默认值为 0。

`SECRETS_MANAGER_TTL`

缓存中密钥的 TTL（以秒为单位）。值 0 表示无缓存。最大值为 300 秒。如果 `PARAMETERS_SECRETS_CACHE_SIZE` 为 0，则将忽略此变量。默认为 300 秒。

`SSM_PARAMETER_STORE_TIMEOUT_MILLIS`

对 Parameter Store 的请求超时（以毫秒为单位）。值 0 表示没有超时。默认值为 0。

`SSM_PARAMETER_STORE_TTL`

缓存中参数的 TTL（以秒为单位）。值 0 表示无缓存。最大值为 300 秒。如果 `PARAMETERS_SECRETS_CACHE_SIZE` 为 0，则将忽略此变量。默认为 300 秒。

使用 Parameter Store 中的 AWS Secrets Manager 密钥

AWS Systems Manager Parameter Store 提供安全的分层存储，用于配置数据管理和密钥管理。也可以将密码、数据库字符串和许可证代码等数据存储为参数值。不过，Parameter Store 不会为存储的密钥提供自动轮换服务。相反，Parameter Store 允许您在 Secrets Manager 中存储密钥，然后以 Parameter Store 参数形式引用该密钥。

使用 Secrets Manager 配置 Parameter Store 时，`secret-id` Parameter Store 需要在名称字符串之前使用正斜杠 (/)。

有关更多信息，请参阅 AWS Systems Manager 用户指南中的 Parameter Store Parameters 密钥 AWS Secrets Manager 引用。

轮换 AWS Secrets Manager 秘密

Rotation 是定期更新密钥的过程。当轮换密钥时，会同时更新密钥和数据库或服务中的凭据。在 Secrets Manager 中，您可以为密钥设置自动轮换。轮换有两种形式：

- 托管轮换— 对于大多数托管密钥，您可以使用托管轮换，即服务为您配置和管理轮换。托管轮换不使用 Lambda 函数。
- the section called “通过 Lambda 函数进行旋转”— 对于其他类型的密钥，Secrets Manager 轮换使用 Lambda 函数来更新密钥以及数据库或服务。

AWS Secrets Manager 密钥的托管轮换

部分服务提供托管轮换，即服务为您配置和管理轮换。使用托管轮换，您无需使用 AWS Lambda 函数来更新数据库中的密钥和凭据。

以下服务提供托管轮换：

- Amazon Aurora 为主用户证书提供托管轮换。有关更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon Aurora 和 AWS Secrets Manager管理密码。
- Amazon ECS S ervice Connect 为 AWS Private Certificate Authority TLS 证书提供托管轮换。有关更多信息，请参阅《亚马逊弹性容器服务开发者指南》中的带有 Service Connect 的 TLS。
- Amazon RDS 为主用户证书提供托管轮换。有关更多信息，请参阅《Amazon RDS 用户指南》中的使用 Amazon RDS 和 AWS Secrets Manager管理密码。
- 亚马逊 Redshift 为管理员密码提供托管轮换。有关更多信息，请参阅《Amazon Redshift 管理指南》中的使用 AWS Secrets Manager管理 Amazon Redshift 管理员密码。

> **Tip**
>
> 有关所有其他类型的密钥，请参阅 the section called “通过 Lambda 函数进行旋转”。

托管秘密的轮换通常会在一分钟内完成。在轮换期间，检索秘密的新连接可能会获得先前版本的凭证。在应用程序中，我们强烈建议您遵循使用以您的应用程序所需的最低权限创建的数据库用户的最佳实践，而不是使用主用户。对于应用程序用户，为了获得最高可用性，可以使用交替用户轮换策略。

更改受控轮换的时间表

1. 在 Secrets Manager 控制台中打开托管密钥。您可以访问管理服务中的链接，也可以在 Secrets Manager 控制台中搜索密钥。
2. 在 Rotation schedule（轮换计划）下，在 Schedule expression builder（计划表达式生成器）或 Schedule expression（计划表达式）中，以 UTC 时区格式输入您的计划。Secrets Manager 会将您的计划存储为 `rate()` 或 `cron()` 表达式。轮换时段将自动从午夜开始，除非您指定 Start time（开始时间）。您可以每四小时轮换一次密钥。有关更多信息，请参阅 轮换时间表。
3. （可选）对于 Window duration（时段持续时间），选择您希望 Secrets Manager 在其间轮换密钥的时段长度，例如 **3h** 表示三个小时的时段。该时段不得延伸到下一个轮换时段。如果未指定 Window duration（时段持续时间），则对于以小时为单位的轮换计划，时段将在一小时后自动关闭。对于以天为单位的轮换计划，时段将在一天结束时自动关闭。
4. 选择保存。

更改托管轮换的计划 (AWS CLI)

- 调用 `rotate-secret`。以下示例在每月 1 日和 15 日 UTC 16:00 至 18:00 之间轮换密钥。有关更多信息，请参阅 轮换时间表。

```
aws secretsmanager rotate-secret \
    --secret-id MySecret \
    --rotation-rules "{\"ScheduleExpression\": \"cron(0 16 1,15 * ? *)\",
 \"Duration\": \"2h\"}"
```

通过 Lambda 函数进行旋转

对于许多类型的密钥，Secrets Manager 使用 AWS Lambda 函数来更新密钥以及数据库或服务。有关使用 Lambda 函数的成本的信息，请参阅 定价。

对于某些 托管密钥，可使用托管轮换。要使用 托管轮换，请首先通过管理服务来创建密钥。

在轮换期间，Secrets Manager 会录入指示轮换状态的事件。有关更多信息，请参阅 the section called “使用以下方式登录 AWS CloudTrail ”。

要轮换密钥，Secrets Manager 会根据你设置的轮换计划调用 Lambda 函数。如果在设置自动轮换时也手动更新密钥值，则 Secrets Manager 在计算下一次轮换日期时会认为这是有效的轮换。

在轮换过程中，Secrets Manager 调用几次同一函数，每次使用不同的参数。Secrets Manager 调用具有以下 JSON 请求参数结构的函数：

```
{
    "Step" : "request.type",
    "SecretId" : "string",
    "ClientRequestToken" : "string"
    }
```

如果任何轮换步骤失败，Secrets Manager 会多次重试整个轮换过程。

主题

- 为亚马逊 RDS、亚马逊 Aurora、Amazon Redshift 或亚马逊 DocumentDB 机密设置自动轮换
- 为非数据库 AWS Secrets Manager 密钥设置自动轮换
- 使用设置自动旋转 AWS CLI
- Lambda 函数轮换策略
- Lambda 旋转函数
- AWS Secrets Manager 旋转函数模板
- Lambda 轮换函数的执行角色权限 AWS Secrets Manager
- Lambda 轮换函数的网络访问权限
- 排除 AWS Secrets Manager 轮换故障

为亚马逊 RDS、亚马逊 Aurora、Amazon Redshift 或亚马逊 DocumentDB 机密设置自动轮换

本教程介绍如何设置the section called “通过 Lambda 函数进行旋转”数据库密钥。Rotation 是定期更新密钥的过程。轮换密钥时，您会同时更新密钥和数据库中的凭证。在 Secrets Manager 中，您可以为数据库密钥设置自动轮换。

要使用控制台设置轮换，您需要先选择轮换策略。然后配置密钥以进行轮换，如果您还没有 Lambda 轮换函数，这将创建一个 Lambda 轮换函数。控制台还会为 Lambda 函数执行角色设置权限。最后一步是确保 Lambda 轮换函数可以通过网络访问 Secrets Manager 和数据库。

> **Warning**
>
> 要启用自动轮换，您必须有权为 Lambda 轮换函数创建 IAM 执行角色并向其附加权限策略。您需要拥有 `iam:CreateRole` 和 `iam:AttachRolePolicy` 两个权限。授予这些权限允许身份向自己授予任何权限。

步骤：

步骤 1：选择轮换策略并（可选）创建超级用户密钥

有关 Secrets Manager 提供的策略的信息，请参阅the section called “Lambda 函数轮换策略”。

如果选择 alternating users strategy（交替用户策略），您必须 创建数据库密钥 并在其中存储数据库超级用户凭证。您需要一个包含超级用户凭证的密钥，因为轮换会克隆第一个用户，而大多数用户没有该权限。请注意，Amazon RDS 代理不支持交替用户策略。

步骤 2：配置轮换并创建轮换函数

为 Amazon RDS、Amazon DocumentDB 或 Amazon Redshift 密钥启用轮换

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在密钥列表页上，选择您的密钥。
3. 在 Secret details (密钥详细信息) 页上的 Rotation configuration (轮换配置) 部分中，选择 Edit rotation (编辑轮换)。
4. 在编辑轮换配置对话框中，执行以下操作：
   a. 启用 Automatic rotation（自动轮换）。
   b. 在 Rotation schedule（轮换计划）下，在 Schedule expression builder（计划表达式生成器）或 Schedule expression（计划表达式）中，以 UTC 时区格式输入您的计划。Secrets

Manager 会将您的计划存储为 `rate()` 或 `cron()` 表达式。轮换时段将自动从午夜开始，除非您指定 Start time（开始时间）。您可以每四小时轮换一次密钥。有关更多信息，请参阅 轮换时间表。

c. （可选）对于 Window duration（时段持续时间），选择您希望 Secrets Manager 在其间轮换密钥的时段长度，例如 **3h** 表示三个小时的时段。该时段不得延伸到下一个轮换时段。如果未指定 Window duration（时段持续时间），则对于以小时为单位的轮换计划，时段将在一小时后自动关闭。对于以天为单位的轮换计划，时段将在一天结束时自动关闭。

d. （可选）请选择 Rotate immediately when the secret is stored（在存储密钥时立即轮换），以在保存更改时轮换密钥。如果您清除该复选框，则第一次轮换将按照您设置的计划开始。

   如果轮换失败，例如因为步骤 3 和 4 尚未完成，Secrets Manager 会多次重试轮换过程。

e. 在 Rotation function（轮换函数）下，执行以下操作之一：

   - 选择 Create a new Lambda function（创建新的 Lambda 函数），然后输入新函数的名称。Secrets Manager 会将 `SecretsManager` 添加到函数名称的开头。Secrets Manager 会基于相应的模板创建函数并为 Lambda 执行角色设置必要的权限。
   - 选择 Use an existing Lambda function（使用现有 Lambda 函数），以重复使用用于另一个密钥的轮换函数。在 Recommended VPC configurations（建议的 VPC 配置）下列出的轮换函数，与数据库具有相同的 VPC 和安全组，有助于函数访问数据库。

f. 对于轮换策略，选择单用户或交替用户策略。有关更多信息，请参阅 the section called “步骤 1：选择轮换策略并（可选）创建超级用户密钥”。

5. 选择 Save（保存）。

第 3 步：（可选）为轮换函数设置额外的权限条件

我们建议您在轮换函数的资源策略中包括上下文密钥 `aws:SourceAccount`，以防止 Lambda 被用作混淆代理。对于某些 AWS 服务，为了避免混淆副手的情况， AWS 建议您同时使用`aws:SourceArn`和`aws:SourceAccount`全局条件键。但如果轮换函数策略中包括 `aws:SourceArn` 条件，则轮换函数只能用于轮换该 ARN 指定的密钥。我们建议您仅在其中包括上下文键 `aws:SourceAccount`，以便对多个密钥使用轮换函数。

更新轮换函数资源策略

1. 在 Secrets Manager 控制台中选择您的密钥，然后在详细信息页面中的 Rotation configuration（轮换配置）下，选择 Lambda 轮换函数。Lambda 控制台将打开。
2. 按照 Using resource-based policies for Lambda（将基于资源的策略用于 Lambda）中的说明添加 `aws:sourceAccount` 条件。

```
"Condition": {
    "StringEquals": {
        "AWS:SourceAccount": "123456789012"
    }
},
```

如果密钥使用 AWS 托管式密钥 `aws/secretsmanager` 以外的 KMS 密钥进行加密，则 Secrets Manager 会向 Lambda 执行角色授予使用该密钥的权限。您可以使用 SecretARN 加密上下文 来限制解密函数的使用，从而确保轮换函数角色只能解密其负责轮换的密钥。

更新轮换函数执行角色

1. 从 Lambda 轮换函数中选择配置，然后在执行角色下，选择角色名称。
2. 按照 修改角色权限策略 中的说明添加 `kms:EncryptionContext:SecretARN` 条件。

```
"Condition": {
    "StringEquals": {
        "kms:EncryptionContext:SecretARN": "SecretARN"
    }
},
```

步骤 4：为轮换函数设置网络访问

有关更多信息，请参阅 the section called “Lambda 轮换函数的网络访问权限”。

后续步骤

请参阅 the section called “ 轮换问题排查”。

为非数据库 AWS Secrets Manager 密钥设置自动轮换

本教程介绍如何设置the section called “通过 Lambda 函数进行旋转”非数据库密钥。Rotation 是定期更新密钥的过程。轮换密钥时，会同时更新密钥以及拥有密钥的数据库或服务中的凭证。

有关数据库密钥的信息，请参阅 自动轮换数据库密钥（控制台）。

> **Warning**
>
> 要启用自动轮换，您必须有权为 Lambda 轮换函数创建 IAM 执行角色并向其附加权限策略。您需要拥有 `iam:CreateRole` 和 `iam:AttachRolePolicy` 两个权限。授予这些权限允许身份向自己授予任何权限。

步骤：

步骤 1：创建通用旋转函数

首先，创建一个 Lambda 旋转函数。它里面没有用来轮换你的密钥的代码，所以你将在稍后的步骤中写出来。有关旋转函数的工作原理的信息，请参见the section called “Lambda 旋转函数”。

在支持的区域中 AWS Serverless Application Repository ，您可以使用从模板创建函数。有关支持的区域列表，请参阅AWS Serverless Application Repository 常见问题解答。在其他区域，您可以从头开始创建函数，然后将模板代码复制到函数中。

创建通用旋转函数

1. 要确定您所在的地区 AWS Serverless Application Repository 是否支持，请参阅《AWS 一般参考》中的AWS Serverless Application Repository 终端节点和配额。
2. 请执行以下操作之一：
   - 如果您 AWS Serverless Application Repository 所在的地区支持：
     a. 在 Lambda 控制台中，选择应用程序，然后选择创建应用程序。
     b. 在创建应用程序页面上，选择无服务器应用程序选项卡。
     c. 在 “公共应用程序” 下的搜索框中，输入**`SecretsManagerRotationTemplate`**。
     d. 选择显示创建自定义 IAM 角色或资源策略的应用程序。

e. 选择方SecretsManagerRotationTemplate块。

f. 在 “查看、配置和部署” 页面的 “应用程序设置” 栏中，填写必填字段。

- 对于终端节点，请输入您所在地区的终端节点，包括**https://**。有关 终端节点的列表，请参阅the section called “Secrets Manager 端点”。
- 要将 Lambda 函数放在 VPC 中，请添加 vpcSecurityGroupID 和。vpcSubnetIds

g. 选择部署。

- 如果您所在的地区 AWS Serverless Application Repository 不支持：

a. 在 Lambda 控制台中，选择函数，然后选择创建函数。

b. 在 Create function (创建函数) 页面上，执行以下操作：

i. 选择从头开始创作。

ii. 在 Function name（函数名称）中，输入轮换函数的名称。

iii. 对于 Runtime（运行时），选择 Python 3.9。

iv. 选择创建函数。

步骤 2：编写轮换函数代码

在此步骤中，您将编写更新密钥以及该密钥所针对的服务或数据库的代码。有关旋转函数的作用信息，包括编写自己的旋转函数的提示，请参阅the section called “Lambda 旋转函数”。您也可以使用 a 轮换函数模板 s 作为参考。

步骤 3：配置密钥以进行轮换

在此步骤中，您将为密钥设置轮换计划，并将轮换功能连接到该密钥。

配置轮换并创建空轮换函数

1. 打开 Secrets Manager 控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在密钥列表页上，选择您的密钥。
3. 在 Secret details (密钥详细信息) 页上的 Rotation configuration (轮换配置) 部分中，选择 Edit rotation (编辑轮换)。在编辑轮换配置对话框中，执行以下操作：

a. 启用 Automatic rotation（自动轮换）。

b. 在 Rotation schedule（轮换计划）下，在 Schedule expression builder（计划表达式生成器）或 Schedule expression（计划表达式）中，以 UTC 时区格式输入您的计划。Secrets

Manager 会将您的计划存储为 `rate()` 或 `cron()` 表达式。轮换时段将自动从午夜开始，除非您指定 Start time（开始时间）。您可以每四小时轮换一次密钥。有关更多信息，请参阅 轮换时间表。

c. （可选）对于 Window duration（时段持续时间），选择您希望 Secrets Manager 在其间轮换密钥的时段长度，例如 **3h** 表示三个小时的时段。该时段不得延伸到下一个轮换时段。如果未指定 Window duration（时段持续时间），则对于以小时为单位的轮换计划，时段将在一小时后自动关闭。对于以天为单位的轮换计划，时段将在一天结束时自动关闭。

d. （可选）请选择 Rotate immediately when the secret is stored（在存储密钥时立即轮换），以在保存更改时轮换密钥。如果您清除该复选框，则第一次轮换将按照您设置的计划开始。

e. 在旋转函数下，选择您在步骤 1 中创建的 Lambda 函数。

f. 选择保存。

第 4 步：允许轮换功能访问 Secrets Manager 以及你的数据库或服务

Lambda 轮换函数需要权限才能访问 Secrets Manager 中的密钥，并且需要权限才能访问您的数据库或服务。在此步骤中，您将向 Lambda 执行角色授予这些权限。如果密钥使用 AWS 托管式密钥 `aws/secretsmanager` 以外的 KMS 密钥进行加密，则您需要向 Lambda 执行角色授予使用该密钥的权限。您可以使用 SecretARN 加密上下文 来限制解密函数的使用，从而确保轮换函数角色只能解密其负责轮换的密钥。有关策略示例，请参阅 轮换权限。

有关说明，请参阅《AWS Lambda 开发人员指南》中的 Lambda 执行角色。

第 5 步：允许 Secrets Manager 调用轮换函数

要允许 Secrets Manager 按照您设置的轮换计划调用轮换函数，您需要在 Lambda 函数的资源策略中向 Secrets Manager 服务主体授予`lambda:InvokeFunction`权限。

我们建议您在轮换函数的资源策略中包括上下文密钥 `aws:SourceAccount`，以防止 Lambda 被用作混淆代理。对于某些 AWS 服务，为了避免混淆副手的情况， AWS 建议您同时使用`aws:SourceArn`和`aws:SourceAccount`全局条件键。但如果轮换函数策略中包括 `aws:SourceArn` 条件，则轮换函数只能用于轮换该 ARN 指定的密钥。我们建议您仅在其中包括上下文键 `aws:SourceAccount`，以便对多个密钥使用轮换函数。

要将资源策略附加到 Lambda 函数，请参阅将基于资源的策略用于 Lambda。

以下策略允许 Secrets Manager 调用 Lambda 函数。

```
{
```

```
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "Service": "secretsmanager.amazonaws.com"
            },
        "Action": "lambda:InvokeFunction",
        Condition": {
            "StringEquals": {
                "AWS:SourceAccount": "123456789012"
            }
        },
        "Resource": "LambdaRotationFunctionARN"
    }
    ]
}
```

步骤 6：为轮换功能设置网络访问权限

在此步骤中，您将允许轮换功能同时连接到 Secrets Manager 以及该密钥所针对的服务或数据库。轮换函数必须同时访问两者，才能轮换密钥。请参阅 the section called “Lambda 轮换函数的网络访问权限”。

后续步骤

在步骤 3 中配置轮换时，您可以设置轮换密钥的时间表。如果在计划轮换时失败，Secrets Manager 将多次尝试轮换。您也可以按照中的说明立即开始轮换立即轮换密钥。

如果旋转失败，请参阅 轮换问题排查。

使用设置自动旋转 AWS CLI

本教程介绍如何使用the section called “通过 Lambda 函数进行旋转”进行设置 AWS CLI。轮换密钥时，会同时更新密钥以及拥有密钥的数据库或服务中的凭证。

您也可以使用控制台设置轮换。有关数据库密钥的信息，请参阅 自动轮换数据库密钥（控制台）。有关所有其他类型的密钥，请参阅 自动轮换非数据库密钥（控制台）。

要使用设置轮换 AWS CLI，如果您要轮换数据库密钥，则首先需要选择轮换策略。如果选择 alternating users strategy（交替用户策略），您必须存储一个单独密钥，其中包含数据库超级用户

凭证。接下来，编写轮换函数代码。Secrets Manager 会提供模板，您可以基于该模板创建函数。然后，使用代码创建 Lambda 函数，并为 Lambda 函数和 Lambda 执行角色设置权限。下一步是确保 Lambda 函数可以通过网络访问 Secrets Manager 以及您的数据库或服务。最后，配置密钥以进行轮换。

步骤：

- 数据库密钥的先决条件：选择轮换策略
- 第 1 步：编写旋转函数代码
- 第 2 步：创建 Lambda 函数
- 步骤 3：设置网络访问权限
- 步骤 4：配置密钥以进行轮换
- 后续步骤

数据库密钥的先决条件：选择轮换策略

有关 Secrets Manager 提供的策略的信息，请参阅the section called “Lambda 函数轮换策略”。

选项 1：单用户策略

如果您选择单用户策略，则可以继续执行步骤 1。

选项 2：交替用户策略

如果您选择交替用户策略，则必须：

- 创建数据库密钥并在其中存储数据库超级用户凭据。您需要一个带有超级用户凭据的密钥，因为交替用户轮换会克隆第一个用户，而大多数用户没有该权限。
- 将超级用户密钥的 ARN 添加到原始密钥中。有关更多信息，请参阅 the section called “密钥的 JSON 结构”。

请注意，Amazon RDS 代理不支持交替用户策略。

第 1 步：编写旋转函数代码

要轮换密钥，您需要轮换函数。轮换函数是 Secrets Manager 为轮换密钥而调用的 Lambda 函数。有关更多信息，请参阅 the section called “通过 Lambda 函数进行旋转”。在此步骤中，您将编写更新密钥以及该密钥所针对的服务或数据库的代码。

Secrets Manager 为亚马逊 RDS、Amazon Aurora、Amazon Redshift 和亚马逊 DocumentDB 数据库密钥提供了模板。轮换函数模板

编写旋转函数代码

1. 请执行以下操作之一：
   - 查看旋转函数模板列表。如果有与您的服务和轮换策略相匹配的代码，请复制代码。
   - 对于其他类型的密钥，你可以自己编写轮换函数。有关说明，请参阅the section called “Lambda 旋转函数”。
2. 将该文件连同所有必需的依赖项一起保存在 ZIP 文件 *my-function.zip* 中。

第 2 步：创建 Lambda 函数

在此步骤中，您将使用在步骤 1 中创建的 ZIP 文件创建 Lambda 函数。您还可以设置 Lambda 执行角色，该角色是 Lambda 在调用函数时所扮演的角色。

创建 Lambda 轮换函数和执行角色

1. 为 Lambda 执行角色创建信任策略并将其另存为 JSON 文件。有关示例和更多信息，请参阅the section called “轮换权限”。该策略必须：
   - 允许角色对密钥调用 Secrets Manager 操作。
   - 允许该角色调用密钥所用的服务，例如，创建新密码。
2. 创建 Lambda 执行角色并通过调用应用您在上一步中创建的信任策略。`iam create-role`

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

3. 通过调用 `lambda create-function` 从 ZIP 文件创建 Lambda 函数。

```
aws lambda create-function \
  --function-name my-rotation-function \
  --runtime python3.7 \
  --zip-file fileb://my-function.zip \
  --handler .handler \
  --role arn:aws:iam::123456789012:role/service-role/rotation-lambda-role
```

4. 在 Lambda 函数上设置资源策略，以允许 Secrets Manager 通过调用 `lambda add-permission` 来调用该资源策略。

```
aws lambda add-permission \
  --function-name my-rotation-function \
  --action lambda:InvokeFunction \
  --statement-id SecretsManager \
  --principal secretsmanager.amazonaws.com \
  --source-account 123456789012
```

步骤 3：设置网络访问权限

有关更多信息，请参阅 the section called “Lambda 轮换函数的网络访问权限”。

步骤 4：配置密钥以进行轮换

要为密钥开启自动轮换功能，请调用 `rotate-secret`。您可以使用 `cron()` 或 `rate()` 计划表达式设置轮换计划，也可以设置轮换时段持续时间。有关更多信息，请参阅 the section called “轮换时间表”。

```
aws secretsmanager rotate-secret \
    --secret-id MySecret \
    --rotation-lambda-arn arn:aws:lambda:Region:123456789012:function:my-rotation-function \
    --rotation-rules "{\"ScheduleExpression\": \"cron(0 16 1,15 * ? *)\", \"Duration\": \"2h\"}"
```

后续步骤

请参阅 the section called “ 轮换问题排查”。

Lambda 函数轮换策略

对于the section called “通过 Lambda 函数进行旋转”，对于数据库密钥，Secrets Manager 提供了两种轮换策略。

轮换策略：单用户

此策略在一个密钥中更新一个用户的凭证。对于 Amazon RDS Db2 实例，由于用户无法更改自己的密码，因此您必须在单独的秘密中提供管理员凭证。这是最简单的轮换策略，适用于大多数使用场景。具体而言，建议您为一次性（临时）用户或交互式用户的凭证使用此策略。

轮换密钥时，不会删除打开的数据库连接。在进行轮换时，在数据库中的密码更改后一小段时间，相应的密码才会更新。在此期间，数据库有较低的风险拒绝使用轮换凭证的调用。您可以使用适当的重试策略来降低风险。轮换后，新连接将使用新凭证。

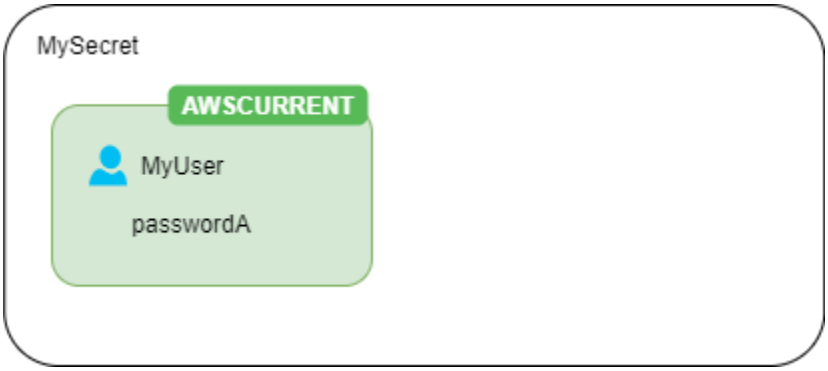
轮换策略：交替用户

此策略在一个密钥中更新两个用户的凭证。您创建第一个用户，然后在第一次轮换期间，轮换函数将进行克隆以创建第二个用户。每次轮换密钥时，轮换函数都会交替更新其更新的用户密码。由于大多数用户无权克隆自己，因此您必须在另一个密钥中为 `superuser` 提供凭证。如果数据库中的克隆用户与原始用户具有的权限不同，或者涉及一次性（临时）用户或交互式用户的凭证，我们建议使用单用户轮换策略。

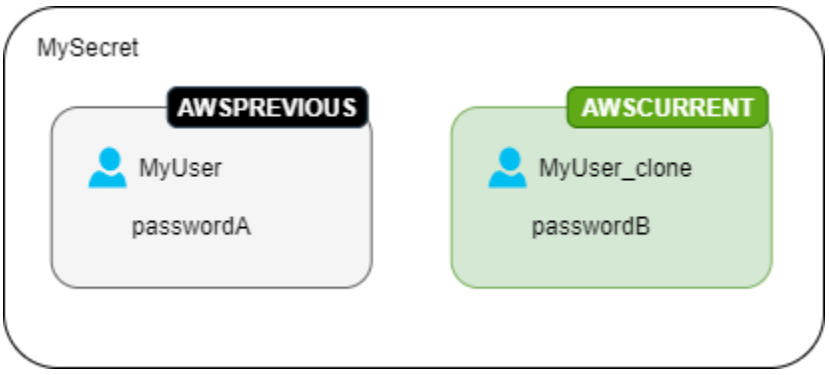
此策略适用于具有权限模型的数据库，其中一个角色拥有数据库表，而另一个角色具有访问数据库表的权限。其也适用于需要高可用性的应用程序。如果应用程序在轮换期间检索密钥，则该应用程序仍会获得一组有效的凭证。轮换后，`user` 和 `user_clone` 凭证均有效。在这种类型的轮换期间，应用程序获得拒绝的可能性甚至比单用户轮换获得拒绝的可能性更小。如果数据库托管在服务器场中，密码更改需要时间传播到所有服务器，则存在数据库拒绝使用新凭证的调用的风险。您可以使用适当的重试策略来降低风险。

Secrets Manager 将创建权限与原始用户相同的克隆用户。如果您在创建克隆用户后更改了原始用户的权限，则还必须更改克隆用户的权限。

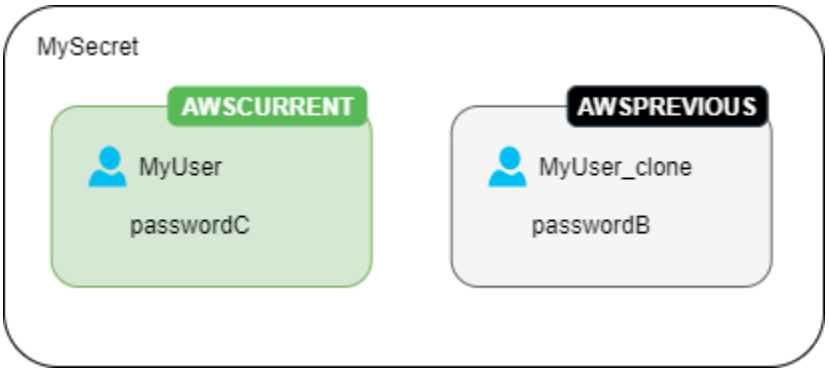
例如，假设您使用某个数据库用户的凭证创建了一个密钥，则该密钥包含一个带有这些凭证的版本。



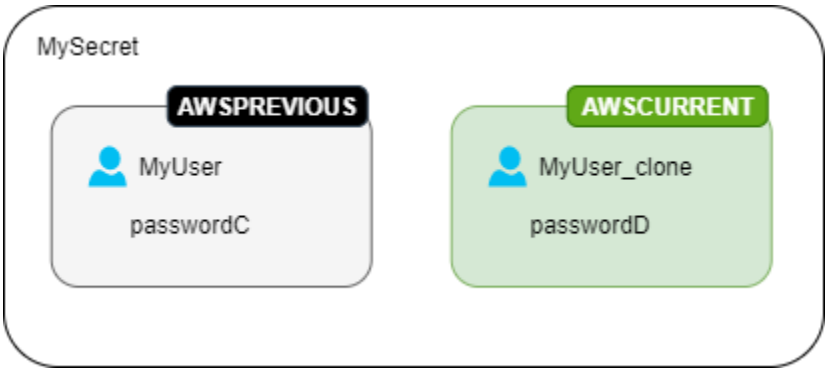
第一次轮换 – 轮换函数使用生成的密码创建克隆用户，这些凭证将成为当前的密钥版本。



第二次轮换 – 轮换函数更新原始用户的密码。



第三次轮换 – 轮换函数更新克隆用户的密码。



Lambda 旋转函数

在中the section called “通过 Lambda 函数进行旋转”，Lambda 函数负责轮换密钥。轮换过程中，Secrets Manager 用暂存标注标注密钥的不同版本。

如果 Secrets Manager 没有为你的密钥类型提供轮换函数模板，你可以创建一个轮换函数。编写旋转函数时，请按照每个步骤的指导进行操作。

编写自己的旋转函数的技巧

- 使用通用旋转模板作为起点来编写自己的旋转函数。
- 编写函数时，请谨慎包括调试或日志记录语句。这些语句可能会导致您的函数中的信息被写入 Amazon CloudWatch，因此您需要确保日志中不包含开发过程中收集的任何敏感信息。

  有关日志语句的示例，请参阅 the section called “轮换函数模板” 源代码。
- 出于安全考虑，Secrets Manager 仅允许 Lambda 轮换函数直接轮换密钥。轮换函数无法调用第二个 Lambda 函数来轮换密钥。
- 有关调试建议，请参阅测试和调试无服务器应用程序。
- 例如，如果您使用外部二进制文件和库来连接资源，则必须设法修补和保留它们。 up-to-date
- 将轮换函数连同任何所需的依赖项一同保存在 ZIP 文件 *my-function.zip* 中。

旋转功能的四个步骤

主题

- create_secret: 创建密钥的新版本
- set_secret：更改数据库或服务中的凭证
- test_secret: 测试新的秘密版本
- finish_secret: 完成旋转

create_secret: 创建密钥的新版本

该方法`create_secret`首先通过使用传`ClientRequestToken`入的调`get_secret_value`用来检查密钥是否存在。如果没有秘密，则它会创建一个新的密钥，`create_secret`并使用令牌作为`VersionId`。然后，它使用生成一个新的密钥值`get_random_password`。接下来，它调用`put_secret_value`将其与暂存标签`AWSPENDING`一起存储。将新的密钥值存储在 `AWSPENDING` 中有助于确保幂等性。如果由于任何原因轮换失败，您可以在后续调用中引用该密钥值。请参阅如何使我的 Lambda 函数具有幂等性。

编写自己的旋转函数的技巧

- 确保新的密钥值仅包含对数据库或服务有效的字符。使用 `ExcludeCharacters` 参数排除字符。
- 在测试函数时，使用查看版本阶段：调用`describe-secret`并查看`VersionIdsToStages`。AWS CLI

- 对于 Amazon RDS MySQL，在用户交替轮换中，Secrets Manager 会创建一个名称不超过 16 个字符的克隆用户。您可以修改轮换函数以允许使用更长的用户名。MySQL 5.7 及更高版本支持最多 32 个字符的用户名，但 Secrets Manager 会在用户名末尾附加“_clone”（六个字符），因此用户名最多必须保持在 26 个字符以内。

`set_secret`：更改数据库或服务中的凭证

该方法`set_secret`更改数据库或服务中的凭证，使其与密钥`AWSPENDING`版本中的新密钥值相匹配。

编写自己的旋转函数的技巧

- 如果您将语句传递给解释语句的服务（如数据库），请使用查询参数化。有关更多信息，请参阅 OWASP 网站上的查询参数化备忘单。
- 轮换函数作为特权代理，有权访问和修改 Secrets Manager 密钥和目标资源中的客户凭证。为防范潜在的混淆代理攻击，您需要确保攻击者无法使用该函数访问其他资源。在更新凭证之前：
  - 检查密钥 `AWSCURRENT` 版本中的凭证是否有效。如果 `AWSCURRENT` 凭证无效，请放弃轮换尝试。
  - 检查 `AWSCURRENT` 和 `AWSPENDING` 密钥值是否适用于同一资源。对于用户名和密码，检查 `AWSCURRENT` 和 `AWSPENDING` 用户名是否相同。
  - 检查目标服务资源是否相同。对于数据库，检查 `AWSCURRENT` 和 `AWSPENDING` 主机名是否相同。
- 在极少数情况下，您可能需要为数据库自定义现有的轮换函数。例如，对于交替用户轮换，Secrets Manager 通过复制第一个用户的运行时配置参数来创建克隆用户。如果要包含更多属性，或更改授予克隆用户的属性，则需要更新 `set_secret` 函数中的代码。

`test_secret`: 测试新的秘密版本

然后，Lambda 轮换函数将使用该密钥来访问数据库或服务，从而测试密钥的 `AWSPENDING` 版本。基于 轮换函数模板 测试的轮换函数使用读取访问权限测试新的密钥。

`finish_secret`: 完成旋转

最后，Lambda 轮换函数将标签 `AWSCURRENT` 从之前的密钥版本移动到此版本，这将同时在同一 API 调用中移除 `AWSPENDING` 标签。Secrets Manager 添加 `AWSPREVIOUS` 暂存标注到以前的版本，以便您保留密钥的上次已知良好的版本。

该方法finish_secret用于update_secret_version_stage将暂存标签AWSCURRENT从以前的密钥版本移动到新的密钥版本。Secrets Manager 会将 AWSPREVIOUS 暂存标签自动添加到早期版本，以便您保留上次已知良好的密钥版本。

编写自己的旋转函数的技巧

- 在此AWSPENDING之前不要将其删除，也不要使用单独的 API 调用将其删除，因为这可能会向 Secrets Manager 表明轮换未成功完成。Secrets Manager 添加 AWSPREVIOUS 暂存标注到以前的版本，以便您保留密钥的上次已知良好的版本。

成功轮换后，AWSPENDING 暂存标签可能附加到与 AWSCURRENT 版本相同的版本，也可能未附加到任何版本。如果 AWSPENDING 暂存标签存在但未附加到与 AWSCURRENT 相同的版本，则以后对轮换的任何调用都假定先前的轮换请求仍在进行中并返回错误。轮换不成功时，AWSPENDING 暂存标签可能会附加到空密钥版本。有关更多信息，请参阅 轮换问题排查。

AWS Secrets Manager 旋转函数模板

对于the section called “通过 Lambda 函数进行旋转”，Secrets Manager 提供了许多轮换函数模板。若要使用模板，请参阅：

- 自动轮换数据库密钥（控制台）
- 自动轮换非数据库密钥（控制台）

这些模板支持 Python 3.9。

要编写自己的旋转函数，请参阅编写旋转函数。

模板

- Amazon RDS 和 Amazon Aurora
  - Amazon RDS Db2 单用户
  - Amazon RDS Db2 交替用户
  - Amazon RDS MariaDB 单用户
  - Amazon RDS MariaDB 交替用户
  - Amazon RDS 和 Amazon Aurora MySQL 单用户
  - Amazon RDS 和 Amazon Aurora MySQL 交替用户
  - Amazon RDS Oracle 单用户

  - Amazon RDS Oracle 交替用户
  - Amazon RDS 和 Amazon Aurora PostgreSQL 单用户
  - Amazon RDS 和 Amazon Aurora PostgreSQL 交替用户
  - Amazon RDS Microsoft SQLServer 单用户
  - Amazon RDS Microsoft SQLServer 交替用户
- Amazon DocumentDB（与 MongoDB 兼容）
  - Amazon DocumentDB 单个用户
  - Amazon DocumentDB 交替用户
- Amazon Redshift
  - Amazon Redshift 单用户
  - Amazon Redshift 交替用户
- Amazon ElastiCache
- Active Directory
  - 活动目录凭证
  - 活动目录密钥表
- 其他密钥类型

Amazon RDS 和 Amazon Aurora

Amazon RDS Db2 单用户

- 模板名称： SecretsManagerrdsDb2 RotationSingleUser
- 轮换策略： 轮换策略：单用户。
- **`SecretString`** 结构：the section called “Amazon RDS Db2 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/rdsDb2 /lambda_function.py SecretsManager RotationSingleUser
- 依赖关系：python-ibmdb

Amazon RDS Db2 交替用户

- 模板名称： SecretsManagerrdsDb2 RotationMultiUser
- 轮换策略： the section called “交替用户”。

- **SecretString** 结构：the section called “Amazon RDS Db2 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rdsDb2 /lambda_function.py SecretsManager RotationMultiUser
- 依赖关系：python-ibmdb

Amazon RDS MariaDB 单用户

- 模板名称： SecretsManagerrdsmariaDB RotationSingleUser
- 轮换策略： 轮换策略：单用户。
- **SecretString** 结构：the section called “Amazon RDS MariaDB 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rdsmariaDB /lambda_function.py SecretsManager RotationSingleUser
- 依赖关系：PyMySQL 1.0.2。如果你使用 sha256 密码进行身份验证，则为 PyMy SQL [rsa]。有关在 Lambda 运行时中使用带有编译代码的包的信息，请参阅如何将包含已编译二进制文件的 Python 包添加到我的部署包并使该包与 Lambda 兼容？ 在AWS 知识中心中。

Amazon RDS MariaDB 交替用户

- 模板名称： SecretsManagerrdsmariaDB RotationMultiUser
- 轮换策略： the section called “交替用户”。
- **SecretString** 结构：the section called “Amazon RDS MariaDB 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rdsmariaDB /lambda_function.py SecretsManager RotationMultiUser
- 依赖关系：PyMySQL 1.0.2。如果你使用 sha256 密码进行身份验证，则为 PyMy SQL [rsa]。有关在 Lambda 运行时中使用带有编译代码的包的信息，请参阅如何将包含已编译二进制文件的 Python 包添加到我的部署包并使该包与 Lambda 兼容？ 在AWS 知识中心中。

Amazon RDS 和 Amazon Aurora MySQL 单用户

- 模板名称： SecretsManagerrdsmySQL RotationSingleUser
- 轮换策略： the section called “单用户”。
- 预期的 **SecretString** 结构：the section called “Amazon RDS 和 Amazon Aurora MySQL 秘密结构”。

- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rdsmyS SecretsManager QL /lambda_function.py RotationSingleUser
- 依赖关系：PyMySQL 1.0.2。如果你使用 sha256 密码进行身份验证，则为 PyMy SQL [rsa]。有关在 Lambda 运行时中使用带有编译代码的包的信息，请参阅如何将包含已编译二进制文件的 Python 包添加到我的部署包并使该包与 Lambda 兼容？ 在AWS 知识中心中。

Amazon RDS 和 Amazon Aurora MySQL 交替用户

- 模板名称： SecretsManagerrdsmySQL RotationMultiUser
- 轮换策略： the section called “交替用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS 和 Amazon Aurora MySQL 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rdsmyS SecretsManager QL /lambda_function.py RotationMultiUser
- 依赖关系：PyMySQL 1.0.2。如果你使用 sha256 密码进行身份验证，则为 PyMy SQL [rsa]。有关在 Lambda 运行时中使用带有编译代码的包的信息，请参阅如何将包含已编译二进制文件的 Python 包添加到我的部署包并使该包与 Lambda 兼容？ 在AWS 知识中心中。

Amazon RDS Oracle 单用户

- 模板名称： SecretsManagerRDS OracleRotationSingleUser
- 轮换策略： the section called “单用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS Oracle 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ RDS /lambda_function.py SecretsManager OracleRotationSingleUser
- 依赖关系：python-or acledb 2.0.1

Amazon RDS Oracle 交替用户

- 模板名称： SecretsManagerRDS OracleRotationMultiUser
- 轮换策略： the section called “交替用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS Oracle 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ RDS /lambda_function.py SecretsManager OracleRotationMultiUser

- 依赖关系：python-or acledb 2.0.1

Amazon RDS 和 Amazon Aurora PostgreSQL 单用户

- 模板名称： SecretsManagerrdpostgreSQL RotationSingleUser
- 轮换策略： 轮换策略：单用户。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS 和 Amazon Aurora PostgreSQL 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rd SecretsManager spostgreSQL /lambda_function.py RotationSingleUser
- 依赖关系：PyGreSQL 5.0.7

Amazon RDS 和 Amazon Aurora PostgreSQL 交替用户

- 模板名称： SecretsManagerrdpostgreSQL RotationMultiUser
- 轮换策略： the section called “交替用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS 和 Amazon Aurora PostgreSQL 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ rd SecretsManager spostgreSQL /lambda_function.py RotationMultiUser
- 依赖关系：PyGreSQL 5.0.7

Amazon RDS Microsoft SQLServer 单用户

- 模板名称： SecretsManagerRDSSQ L ServerRotationSingleUser
- 轮换策略： the section called “单用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS Microsoft SQLServer 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ RDSSQL /lambda_function.py SecretsManager ServerRotationSingleUser
- 依赖关系：Pymssql 2.2.2

Amazon RDS Microsoft SQLServer 交替用户

- 模板名称： SecretsManagerRDSSQ L ServerRotationMultiUser

- 轮换策略： the section called “交替用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon RDS Microsoft SQLServer 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ RDSSQL /lambda_function.py SecretsManager ServerRotationMultiUser
- 依赖关系：Pymssql 2.2.2

Amazon DocumentDB（与 MongoDB 兼容）

Amazon DocumentDB 单个用户

- 模板名称： SecretsManagerMongoDB RotationSingleUser
- 轮换策略： the section called “单用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon DocumentDB 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ DB / lambda_function.py SecretsManagerMongo RotationSingleUser
- 依赖关系：Pymongo 3.2

Amazon DocumentDB 交替用户

- 模板名称： SecretsManagerMongoDB RotationMultiUser
- 轮换策略： the section called “交替用户”。
- 预期的 **`SecretString`** 结构：the section called “Amazon DocumentDB 密钥结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lambdas/tree/master/ DB / lambda_function.py SecretsManagerMongo RotationMultiUser
- 依赖关系：Pymongo 3.2

Amazon Redshift

Amazon Redshift 单用户

- 模板名称： SecretsManagerRedshiftRotationSingleUser
- 轮换策略： the section called “单用户”。
- 预期**`SecretString`**结构：the section called “Amazon Redshift 密钥结构”或the section called “亚马逊 Redshift 无服务器秘密结构”。

- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerRedshiftRotationSingleUser bdas/tree/master/ /lambda_function.py
- 依赖关系：PyGreSQL 5.0.7

Amazon Redshift 交替用户

- 模板名称： SecretsManagerRedshiftRotationMultiUser
- 轮换策略： the section called “交替用户”。
- 预期**`SecretString`**结构：the section called “Amazon Redshift 密钥结构”或the section called “亚马逊 Redshift 无服务器秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerRedshiftRotationMultiUser bdas/tree/master/ /lambda_function.py
- 依赖关系：PyGreSQL 5.0.7

Amazon ElastiCache

要使用此模板，请参阅 Amazon 用户指南中的自动轮换 ElastiCache 用户密码。

- 模板名称： SecretsManagerElasticacheUserRotation
- 预期的 **`SecretString`** 结构：the section called “亚马逊的 ElastiCache 秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerElasticacheUserRotation bdas/tree/master/ /lambda_function.py

Active Directory

活动目录凭证

- 模板名称： SecretsManagerActiveDirectoryRotationSingleUser
- 预期的 **`SecretString`** 结构：the section called “活动目录凭证秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerActiveDirectoryRotationSingleUser bdas/tree/master/ /lambda_function.py

活动目录密钥表

- 模板名称： SecretsManagerActiveDirectoryAndKeytabRotationSingleUser

- 预期的 **`SecretString`** 结构：the section called “活动目录的秘密结构”。
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerActiveDirectoryAndKeytabRotationSingleUser bdas/tree/master/ / lambda_function.py
- 依赖关系：msktut il

其他密钥类型

Secrets Manager 提供此模板作为您为任何类型密钥创建轮换函数的起点。

- 模板名称： SecretsManagerRotationTemplate
- 源代码：https://github.com/aws-samples/ aws-secrets-manager-rotation-lam SecretsManagerRotationTemplate bdas/tree/master/ /lambda_function.py

Lambda 轮换函数的执行角色权限 AWS Secrets Manager

因为the section called “通过 Lambda 函数进行旋转”，当 Secrets Manager 使用 Lambda 函数轮换密钥时，Lambda 将担任 IAM 执行角色并将这些证书提供给 Lambda 函数代码。有关如何设置自动旋转的说明，请参阅：

- 自动轮换数据库密钥（控制台）
- 自动轮换非数据库密钥（控制台）
- 自动轮换（AWS CLI）

以下示例显示了适用于 Lambda 轮换函数执行角色的内联策略。要创建执行角色并附加权限策略，请参阅 AWS Lambda 执行角色。

示例：

- 适用于 Lambda 轮换函数执行角色的策略
- 适用于客户托管密钥的策略语句
- 适用于交替用户策略的策略语句

适用于 Lambda 轮换函数执行角色的策略

以下示例策略允许轮换函数：

- 为 *SecretARN* 运行 Secrets Manager 操作。
- 创建新密码。
- 如果数据库或服务在 VPC 中运行，则设置所需的配置。请参阅配置 Lambda 函数以访问 VPC 中的资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:PutSecretValue",
                "secretsmanager:UpdateSecretVersionStage"
            ],
            "Resource": "SecretARN"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DetachNetworkInterface"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

适用于客户托管密钥的策略语句

如果密钥使用 AWS 托管式密钥 `aws/secretsmanager` 以外的 KMS 密钥进行加密，则您需要向 Lambda 执行角色授予使用该密钥的权限。您可以使用 SecretARN 加密上下文 来限制解密函数的使用，从而确保轮换函数角色只能解密其负责轮换的密钥。以下示例演示了要添加到执行角色策略中，以使用 KMS 密钥将密钥解密的语句。

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey"
            ],
            "Resource": "KMSKeyARN"
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:SecretARN": "SecretARN"
                }
            }
        }
```

要对使用客户托管密钥加密的多个密钥使用轮换函数，请添加如下示例所示的语句以允许执行角色解密该密钥。

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey"
            ],
            "Resource": "KMSKeyARN"
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:SecretARN": [
                        "arn1",
                        "arn2"
                    ]
                }
            }
        }
```

适用于交替用户策略的策略语句

有关交替用户轮换策略的信息，请参阅 the section called “Lambda 函数轮换策略”。

对于包含 Amazon RDS 凭证的密钥，如果您使用的是交替用户策略并且超级用户密钥由 Amazon RDS 管理，则还须允许轮换函数调用 Amazon RDS 上的只读 API，以便其获取数据库的连接信息。我们建议您附上 AWS 托管政策 AmazonRDS ReadOnlyAccess。

以下示例策略允许函数：

- 为 *SecretARN* 运行 Secrets Manager 操作。
- 在超级用户密钥中检索凭证。Secrets Manager 会使用超级用户密钥中的凭证更新轮换密钥中的凭证。
- 创建新密码。
- 如果数据库或服务在 VPC 中运行，则设置所需的配置。有关更多信息，请参阅配置 Lambda 函数以访问 VPC 中的资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DescribeSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:PutSecretValue",
                "secretsmanager:UpdateSecretVersionStage"
            ],
            "Resource": "SecretARN"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "SuperuserSecretARN"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DetachNetworkInterface"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Lambda 轮换函数的网络访问权限

因为the section called “通过 Lambda 函数进行旋转”，当 Secrets Manager 使用 Lambda 函数轮换密钥时，Lambda 轮换函数必须能够访问该密钥。如果您的密钥包含凭证，则 Lambda 函数还必须能够访问这些凭证的来源，例如数据库或服务。

访问密钥

Lambda 轮换功能必须能够访问 Secrets Manager 端点。如果您的 Lambda 函数可以访问互联网，则可以使用公共终端节点。若要查找端点，请参阅 the section called “Secrets Manager 端点”。

如果您的 Lambda 函数在不具备互联网访问权限的 VPC 中运行，我们建议您在 VPC 内配置 Secrets Manager 服务私有终端节点。然后，您的 VPC 可以拦截发往公共区域终端节点的请求并将其重定向到私有终端节点。有关更多信息，请参阅 VPC 端点。

或者，您可以通过向 VPC 添加 NAT 网关或互联网网关（这将允许来自您 VPC 的流量访问公有端点），允许 Lambda 函数访问 Secrets Manager 公有端点。这会使 VPC 面临一定的风险，因为网关的 IP 地址可能会受到来自公有 Internet 的攻击。

（可选）访问数据库或服务

对于诸如 API 密钥之类的密钥，无需随密钥更新源数据库或服务。

如果数据库或服务在 VPC 中的 Amazon EC2 实例上运行，建议将 Lambda 函数配置为在同一 VPC 中运行。然后轮换功能可以直接与您的服务通信。有关更多信息，请参阅配置 VPC 访问。

要允许 Lambda 函数访问数据库或服务，您必须确保附加到 Lambda 轮换函数的安全组允许与数据库或服务的出站连接。您还必须确保附加到数据库或服务的安全组允许来自 Lambda 轮换函数进行入站连接。

排除 AWS Secrets Manager 轮换故障

对于许多服务，Secrets Manager 使用 Lambda 函数来轮换密钥。有关更多信息，请参阅 the section called “通过 Lambda 函数进行旋转”。Lambda 轮换函数与拥有密钥的数据库或服务以及 Secrets Manager 交互。当轮换无法按预期进行时，应先检查日 CloudWatch 志。

> **Note**
>
> 某些服务可以为您管理密钥，包括管理自动轮换。有关更多信息，请参阅 the section called “托管轮换”。

查看 Lambda 函数的 CloudWatch 日志

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择您的密钥，然后在详细信息页面上的 Rotation configuration（轮换配置）下，选择 Lambda 轮换函数。Lambda 控制台将打开。
3. 在 “监控” 选项卡上，选择 “日志”，然后选择 “查看日志” CloudWatch。

   CloudWatch 控制台将打开并显示您的函数的日志。

解读日志

- “在环境变量中找到凭证”之后没有活动
- “createSecret”之后没有活动
- 错误：“不允许访问 KMS”
- 错误：“Key is missing from secret JSON（密钥 JSON 中缺少密钥）”
- 错误：“setSecret: Unable to log into database（setSecret：无法登录数据库）”
- 错误：“无法导入模块‘lambda_function’”
- 将现有的轮换函数版本从 Python 3.7 升级到 Python 3.9

“在环境变量中找到凭证”之后没有活动

如果“在环境变量中找到凭证”之后没有活动，并且任务持续时间很长，例如默认 Lambda 超时为 30000 毫秒，则 Lambda 函数可能会在尝试访问 Secrets Manager 端点时超时。

Lambda 轮换功能必须能够访问 Secrets Manager 端点。如果您的 Lambda 函数可以访问互联网，则可以使用公共终端节点。若要查找端点，请参阅 the section called “Secrets Manager 端点”。

如果您的 Lambda 函数在不具备互联网访问权限的 VPC 中运行，我们建议您在 VPC 内配置 Secrets Manager 服务私有终端节点。然后，您的 VPC 可以拦截发往公共区域终端节点的请求并将其重定向到私有终端节点。有关更多信息，请参阅 VPC 端点。

或者，您可以通过向 VPC 添加 NAT 网关或互联网网关（这将允许来自您 VPC 的流量访问公有端点），允许 Lambda 函数访问 Secrets Manager 公有端点。这会使 VPC 面临一定的风险，因为网关的 IP 地址可能会受到来自公有 Internet 的攻击。

“createSecret”之后没有活动

以下问题可能会在 createSecret 之后导致轮换停止：

VPC 网络 ACL 不允许 HTTPS 流量进出。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用网络 ACL 控制指向子网的流量。

Lambda 函数超时配置过短，无法执行任务。

有关更多信息，请参阅《AWS Lambda 开发人员指南》中的配置 Lambda 函数选项。

Secrets Manager VPC 端点不允许在分配的安全组入口处使用 VPC CIDR。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用安全组控制到资源的流量。

Secrets Manager VPC 端点策略不允许 Lambda 使用 VPC 端点。

有关更多信息，请参阅 VPC 端点。

该密钥使用交替用户轮换策略，超级用户密钥由 Amazon RDS 管理，并且 Lambda 函数无法访问 RDS API。

对于由其他 AWS 服务管理超级用户密钥的交替用户轮换，Lambda 轮换函数必须能够调用服务端点来获取数据库连接信息。我们建议您为数据库服务配置 VPC 端点。有关更多信息，请参阅：

- 《Amazon RDS 用户指南》中的 Amazon RDS API 和接口 VPC 端点。
- 《Amazon Redshift 管理指南》中的使用 VPC 端点。

错误：“不允许访问 KMS”

如果您看到 `ClientError: An error occurred (AccessDeniedException) when calling the GetSecretValue operation: Access to KMS is not allowed`，则轮换函数无权使用密钥加密所用的 KMS 密钥来将密钥解密。权限策略中可能存在将加密上下文限定为特定密钥的条件。有关所需权限的信息，请参阅 the section called “适用于客户托管密钥的策略语句”。

错误：“Key is missing from secret JSON（密钥 JSON 中缺少密钥）”

Lambda 轮换函数要求密钥值采用特定的 JSON 结构。如果显示此错误，则 JSON 可能缺少轮换函数尝试访问的密钥。有关每种密钥类型的 JSON 结构的信息，请参阅 the section called “密钥的 JSON 结构”。

错误：“setSecret: Unable to log into database（setSecret：无法登录数据库）”

以下问题可能导致此错误：

轮换函数无法访问数据库。

- 如果任务持续时间过长，例如超过 5000 毫秒，则 Lambda 轮换函数可能无法通过网络访问数据库。
- 如果数据库或服务在 VPC 中的 Amazon EC2 实例上运行，建议将 Lambda 函数配置为在同一 VPC 中运行。然后轮换功能可以直接与您的服务通信。有关更多信息，请参阅配置 VPC 访问。
- 要允许 Lambda 函数访问数据库或服务，您必须确保附加到 Lambda 轮换函数的安全组允许与数据库或服务的出站连接。您还必须确保附加到数据库或服务的安全组允许来自 Lambda 轮换函数进行入站连接。

密钥中的凭证有误。

- 如果任务持续时间过短，则 Lambda 轮换函数可能无法使用密钥中的凭证进行身份验证。使用 AWS CLI 命令使用密钥`AWSCURRENT`和`AWSPREVIOUS`版本中的信息手动登录，检查凭据`get-secret-value`。

数据库使用 **`scram-sha-256`** 加密密码。

- 如果您的数据库是 Aurora PostgreSQL 版本 13 或更高版本，并且使用 `scram-sha-256` 加密密码，但轮换函数使用不支持 `scram-sha-256` 的 `libpq` 版本 9 或更旧版本，则轮换函数无法连接到数据库。

确定哪些数据库用户使用 **scram-sha-256** 加密

- 请参阅博客 RDS for PostgreSQL 13 中的 SCRAM 身份验证中的检查使用非 SCRAM 密码的用户。

确定您的轮换函数使用哪个 **libpq** 版本

1. 在基于 Linux 的计算机上，在 Lambda 控制台上导航到您的轮换函数并下载部署包。将 zip 文件解压缩到工作目录中。
2. 在命令行上，在工作目录中运行：

   ```
   readelf -a libpq.so.5 | grep RUNPATH
   ```

3. 如果看到字符串 *PostgreSQL-9.4.x* 或任何低于 10 的主要版本，则轮换函数不支持 scram-sha-256。
   - 不支持 scram-sha-256 的轮换函数的输出：

     ```
     0x000000000000001d (RUNPATH) Library runpath: [/
     local/p4clients/pkgbuild-a1b2c/workspace/build/
     PostgreSQL/PostgreSQL-9.4.x_client_only.123456.0/AL2_x86_64/
     DEV.STD.PTHREAD/build/private/tmp/brazil-path/build.libfarm/lib:/
     local/p4clients/pkgbuild-a1b2c/workspace/src/PostgreSQL/build/
     private/install/lib]
     ```

   - 支持 scram-sha-256 的轮换函数的输出：

     ```
     0x000000000000001d (RUNPATH) Library runpath: [/
     local/p4clients/pkgbuild-a1b2c/workspace/build/
     PostgreSQL/PostgreSQL-10.x_client_only.123456.0/AL2_x86_64/
     DEV.STD.PTHREAD/build/private/tmp/brazil-path/build.libfarm/lib:/
     local/p4clients/pkgbuild-a1b2c/workspace/src/PostgreSQL/build/
     private/install/lib]
     ```

> **Note**
>
> 如果您在 2021 年 12 月 30 日之前设置了自动密钥轮换，则轮换函数捆绑了不支持 scram-sha-256 的旧版本 libpq。为了支持 scram-sha-256，您需要重新创建您的轮换函数。

数据库需要 SSL/TLS 访问权限。

如果您的数据库需要 SSL/TLS 连接，但轮换函数使用了未加密的连接，则轮换函数无法连接到数据库。适用于 Amazon RDS（Oracle 和 Db2 除外）和 Amazon DocumentDB 的轮换函数将自动使用安全套接字层 (SSL) 或传输层安全性协议 (TLS) 来连接到数据库（如果可用）。否则，他们将使用未加密的连接。

> **Note**
>
> 如果您在 2021 年 12 月 20 日之前设置了自动密钥轮换，则您的轮换函数可能基于不支持 SSL/TLS 的较旧模板。为了支持使用 SSL/TLS 的连接，您需要重新创建您的轮换函数。

确定您的轮换函数的创建时间

1. 在 Secrets Manager 控制台 https://console.aws.amazon.com/secretsmanager/ 中，打开您的密钥。在 Rotation configuration（轮换配置）中的 Lambda rotation function（Lambda 轮换函数）下，您将看到 Lambda function ARN（Lambda 函数 ARN），例如，`arn:aws:lambda:aws-region:123456789012:function:SecretsManagerMyRotationFunction`。在此示例 `SecretsManagerMyRotationFunction` 中，从 ARN 末尾复制函数名称。
2. 在 AWS Lambda 控制台 https://console.aws.amazon.com/lambda/ 的“函数”下，将您的 Lambda 函数名称粘贴到搜索框中，选择 Enter，然后选择 Lambda 函数。
3. 在函数详细信息页面中，在 Configuration（配置）选项卡上的 Tags（标签）下，复制键 aws:cloudformation:stack-name 旁边的值。
4. 在 AWS CloudFormation 控制台 https://console.aws.amazon.com/cloudformation 的 Stacks 下，将密钥值粘贴到搜索框中，然后选择 Enter。
5. 堆栈列表将进行筛选，以便只显示创建 Lambda 轮换函数的堆栈。在 Created date（创建日期）列中，查看堆栈的创建日期。这是 Lambda 轮换函数的创建日期。

错误：“无法导入模块‘lambda_function’”

如果您运行的是早期版本的 Lambda 函数，且该函数是从 Python 3.7 自动升级到更新版本的 Python 的，则可能会遇到此错误。要解决此错误，您可以将 Lambda 函数版本改回 Python 3.7，然后 the section called “将现有的轮换函数版本从 Python 3.7 升级到 Python 3.9”。要了解更多信息，请参阅 AWS re:Post 中的 为什么我的 Secrets Manager Lambda 函数轮换失败并出现“找不到 pg 模块”错误？。

将现有的轮换函数版本从 Python 3.7 升级到 Python 3.9

2022 年 11 月之前创建的部分轮换函数使用 Python 3.7。适用于 Python 的 AWS 软件开发工具包于 2023 年 12 月停止支持 Python 3.7。有关更多信息，请参阅软件开发工具包和 AWS 工具的 Python 支持政策更新。要切换到使用 Python 3.9 的新轮换函数，可以在现有轮换函数中添加运行时系统属性或重新创建轮换函数。

查找使用 Python 3.7 的 Lambda 轮换函数

1. 登录 AWS Management Console 并打开 AWS Lambda 控制台，网址为 https://console.aws.amazon.com/lambda/。
2. 在函数列表中，筛选 **SecretsManager**。
3. 在筛选后的函数列表中，在运行时系统下，查找 Python 3.7。

升级到 Python 3.9：

- 选项 1：使用重新创建旋转函数 AWS CloudFormation
- 选项 2：使用更新现有旋转函数的运行时间 AWS CloudFormation
- 选项 3：对于 AWS CDK 用户，升级 CDK 库

选项 1：使用重新创建旋转函数 AWS CloudFormation

当您使用 Secrets Manager 控制台开启轮换功能时，Secrets Manager 会使用 AWS CloudFormation 创建必要的资源，包括 Lambda 轮换函数。如果您使用控制台开启轮换，或者使用 AWS CloudFormation 堆栈创建了旋转功能，则可以使用相同的 AWS CloudFormation 堆栈重新创建具有新名称的旋转函数。新函数将使用最新版本的 Python。

查找创建旋转函数的 AWS CloudFormation 堆栈

- 在 Lambda 函数的详细信息页面的配置选项卡上，选择标签。查看 aws:cloudformation:stack-id 旁的 ARN。

  堆栈名称已嵌入在 ARN 中，如下例所示。

  - ARN：`arn:aws:cloudformation:us-west-2:408736277230:stack/`**`SecretsManagerRDSMySQLRotationSingleUser5c2-SecretRotationScheduleHostedRotationLambda`**`-3CUDHZMDMBO8/79fc9050-2eef-11ed-`

- 堆栈名称：**SecretsManagerRDSMySQLRotationSingleUser5c2-SecretRotationScheduleHostedRotationLambda**

重新创建轮换函数（AWS CloudFormation）

1. 在中 AWS CloudFormation，按名称搜索堆栈，然后选择更新。

   如果出现建议您更新根堆栈的对话框，请选择转到根堆栈，然后选择更新。

2. 在更新堆栈页面上，选择在设计器中编辑模板，然后选择在设计器中查看。
3. 进入设计器后，在模板代码 SecretRotationScheduleHostedRotationLambda 中将 `"functionName": "SecretsManagerTestRotationRDS"` 的值替换为新的函数名称，例如在 JSON 中 **`"functionName": "SecretsManagerTestRotationRDSupdated"`**
4. 继续完成 AWS CloudFormation 堆栈工作流程，然后选择提交。

选项 2：使用更新现有旋转函数的运行时间 AWS CloudFormation

当您使用 Secrets Manager 控制台开启轮换功能时，Secrets Manager 会使用 AWS CloudFormation 创建必要的资源，包括 Lambda 轮换函数。如果您使用控制台开启轮换，或者使用 AWS CloudFormation 堆栈创建了旋转函数，则可以使用相同的 AWS CloudFormation 堆栈来更新旋转功能的运行时间。

查找创建旋转函数的 AWS CloudFormation 堆栈

- 在 Lambda 函数的详细信息页面的配置选项卡上，选择标签。查看 aws:cloudformation:stack-id 旁的 ARN。

  堆栈名称已嵌入在 ARN 中，如下例所示。

  - ARN：`arn:aws:cloudformation:us-west-2:408736277230:stack/`**`SecretsManagerRDSMySQLRotationSingleUser5c2-SecretRotationScheduleHostedRotationLambda`**`-3CUDHZMDMBO8/79fc9050-2eef-11ed-`
  - 堆栈名称：**SecretsManagerRDSMySQLRotationSingleUser5c2-SecretRotationScheduleHostedRotationLambda**

更新轮换函数的运行时系统（AWS CloudFormation）

1. 在中 AWS CloudFormation，按名称搜索堆栈，然后选择更新。

如果出现建议您更新根堆栈的对话框，请选择转到根堆栈，然后选择更新。

2. 在更新堆栈页面上，选择在设计器中编辑模板，然后选择在设计器中查看。
3. 在设计器中，在模板 JSON 中，对于`SecretRotationScheduleHostedRotationLambda`、下方`Properties`、下方`Parameters`，添加 **`"runtime": "python3.9"`**
4. 继续完成 AWS CloudFormation 堆栈工作流程，然后选择提交。

选项 3：对于 AWS CDK 用户，升级 CDK 库

如果您使用 v2.94.0 AWS CDK 之前的版本为密钥设置轮换，则可以通过升级到 v2.94.0 或更高版本来更新 Lambda 函数。有关更多信息，请参见 AWS Cloud Development Kit (AWS CDK) v2 开发人员指南。

立即轮换 AWS Secrets Manager 密钥

您只能轮换已配置了轮换的密钥。要确定密钥是否已配置为轮换，请在控制台中查看密钥并向下滚动到 Rotation configuration（轮换配置）部分。如果 Rotation status（轮换状态）为 Enabled（启用），则密钥配置为轮换。如果不是，请参阅 轮换 密钥。

要立即轮换密码（控制台）

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择您的密钥。
3. 在密钥详细信息页面上，在旋转配置下方，选择立即轮换密钥。
4. 在轮换密钥对话框中，选择轮换。

AWS CLI

Example 立即轮换密钥

以下 `rotate-secret` 示例将立即开始轮换。密钥必须已配置轮换。

```
aws secretsmanager rotate-secret \
    --secret-id MyTestSecret
```

轮换时间表

在启用自动轮换时，可以使用 cron() 或 rate() 表达式来设置轮换密钥的计划。使用 rate 表达式，可以创建以小时或天为间隔重复的轮换计划。使用 cron 表达式，可以创建比轮换间隔更详细的轮换计划。Secrets Manager 轮换计划使用 UTC 时区。您可以每四小时轮换一次密钥。Secrets Manager 将在轮换时段内随时轮换密钥。

要启用轮换，请参阅：

- the section called “托管轮换”
- the section called “自动轮换数据库密钥（控制台）”
- the section called “自动轮换非数据库密钥（控制台）”

Rate 表达式

Secrets Manager rate 表达式采用以下格式，其中*#*是正整数，*##*可以是 `hour`、`hours`、`day` 或 `days`：

```
rate(Value Unit)
```

您可以每四小时轮换一次密钥。示例：

- `rate(4 hours)` 意味着密钥每四小时轮换一次。
- `rate(1 day)` 意味着密钥每天轮换一次。
- `rate(10 days)` 意味着密钥每 10 天轮换一次。

对于以小时为单位的费率，默认轮换时段从午夜开始，并在一小时后关闭。您可以设置 Window duration（时段持续时间）以更改轮换时段。该轮换时段不得延伸到下一个轮换时段。对此进行检查的一种方法是确认轮换时段小于或等于两次轮换之间的小时数。

对于以天为单位的费率，默认轮换时段从午夜开始，并在一天结束时关闭。您可以设置 Window duration（时段持续时间）以更改轮换时段。该轮换时段不得延伸到下一个 UTC 日。对此进行检查的一种方法是确认开始时间加上时段持续时间是否小于或等于 24 小时。

Cron 表达式

Cron 表达式采用以下格式：

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

包含小时增量的 cron 表达式每天都会重置。例如，`cron(0 4/12 * * ? *)` 表示凌晨 4:00、下午 4:00，然后是第二天凌晨 4:00、下午 4:00。Secrets Manager 轮换计划使用 UTC 时区。

对于以小时为单位的计划，默认轮换时段将在一小时后关闭。您可以设置 Window duration（时段持续时间）以更改轮换时段。该轮换时段不得进入下一个轮换时段。您可以每四小时轮换一次密钥。

示例计划	Expression
每八小时一次，从午夜开始。	`cron(0 /8 * * ? *)`
每八小时一次，从早上 8:00 开始。	`cron(0 8/8 * * ? *)`
每十小时一次，从凌晨 2:00 开始。 轮换时段将从 2:00、12:00 和 22:00 开始，然后在第二天的 2:00、12:00 和 22:00 进行。	`cron(0 2/10 * * ? *)`
每天上午 10:00。	`cron(0 10 * * ? *)`
每星期六下午 6:00。	`cron(0 18 ? * SAT *)`
每月第 1 天上午 8:00。	`cron(0 8 1 * ? *)`
每三个月第一个星期日凌晨 1:00。	`cron(0 1 ? 1/3 SUN#1 *)`
每月最后一天下午 5:00。	`cron(0 17 L * ? *)`
星期一到星期五上午 8:00。	`cron(0 8 ? * MON-FRI *)`
每月第 1 天和第 15 天下午 4:00。	`cron(0 16 1,15 * ? *)`
每月第一个星期日午夜。	`cron(0 0 ? * SUN#1 *)`

Secrets Manager 中的 Cron 表达式要求

Secrets Manager 对可以用于 cron 表达式的内容有一些限制。Secrets Manager 的 cron 表达式的分钟字段必须填写 0，因为 Secrets Manager 轮换时段在整点开始。其年份字段必须填写 *，因为 Secrets Manager 不支持相隔一年以上的轮换计划。下表显示了可以使用的选项。

字段	值	通配符
分钟	必须为 0	无
小时	0–23	使用 / (正斜杠) 指定增量。例如，2/10 意味着从凌晨 2:00 开始每 10 小时一次。您可以每四小时轮换一次密钥。
D ay-of-month	1-31	使用 , (逗号) 包含其他值。例如，1,15 当前当月的第 1 天和第 15 天。 使用 - (短划线) 指定范围。例如，1–15 表示当月的第 1 天到第 15 天。 使用 * (星号) 包含该字段中的所有值。例如，* 表示当月的每一天。 ? (问号) 通配符用于指定一个或另一个。您无法在同一 cron 表达式中为 Day-of-month 和 Day-of-week 字段同时指定值。如果您在其中一个字段中指定了值，则必须在另一个字段中使用 ? (问号)。 使用 / (正斜杠) 指定增量。例如，1/2 表示从第 1 天开始每两天一次，换句话说，第 1 天、第 3 天、第 5 天，依此类推。 使用 L 指定当月的最后一天。

字段	值	通配符
		使用 ***DAY***L 指定当月的最后一个命名日期。例如，SUNL 表示当月的最后一个星期日。
月份	1-12 或 JAN-DEC	使用 , (逗号) 包含其他值。例如，JAN,APR,JUL,OCT 表示一月、四月、七月和十月。 使用 - (短划线) 指定范围。例如，1–3 表示一年的第 1 个月至第 3 个月。 使用 * (星号) 包含该字段中的所有值。例如，* 表示每个月。 使用 / (正斜杠) 指定增量。例如，1/3 表示每三个月一次，从第 1 个月开始，即第 1、4、7 和 10 个月。

字段	值	通配符
D ay-of-week	1-7 或 SUN-SAT	使用 # 指定某个月内一周的星期几。例如，TUE#3 表示该月的第三个星期二。 使用 , (逗号) 包含其他值。例如，1,4 表示一周的第一天和第四天。 使用 - (短划线) 指定范围。例如，1–4 表示一周的第 1 天到第 4 天。 使用 * (星号) 包含该字段中的所有值。例如，* 表示一周的每一天。 ? (问号) 通配符用于指定一个或另一个。您无法在同一 cron 表达式中为 Day-of-month 和 Day-of-week 字段同时指定值。如果您在其中一个字段中指定了值，则必须在另一个字段中使用 ? (问号)。 使用 / (正斜杠) 指定增量。例如，1/2 表示一周的每隔一天，从第一天开始，即第 1 天、第 3 天、第 5 天和第 7 天。 使用 L 指定一周的最后一天。
年	必须是 *	无

查找未轮换的秘密

您可以使用 AWS Config 来评估您的密钥，以查看它们是否符合您的标准。您可以使用 AWS Config 规则定义对机密的内部安全和合规性要求。然后 AWS Config 可以识别不符合你规则的秘密。您还可以跟踪对密钥元数据、轮换配置、用于密钥加密的 KMS 密钥、Lambda 轮换函数以及与密钥关联的标签等进行的更改。

如果您的组织中有多个 AWS 账户 密钥，则可以聚合该配置和合规性数据。 AWS 区域 有关更多信息，请参阅多账户多区域数据聚合。

评估机密是否在轮换

1. 按照使用AWS Config 规则评估资源中的说明进行操作，并从以下规则中进行选择：
   - secretsmanager-rotation-enabled-check — 检查是否为存储在 Secrets Manager 中的密钥配置了轮换。
   - secretsmanager-scheduled-rotation-success-check— 检查上次成功的轮换是否在配置的轮换频率内。检查的最低频率为每天。
   - secretsmanager-secret-periodic-rotation — 检查是否已在指定的天数内轮换了密钥。
2. （可选）配置 AWS Config 为在密钥不合规时通知您。有关更多信息，请参阅AWS Config 发送至 Amazon SNS 主题的通知。

在 Secrets Manager 中取消自动轮换

如果您为密钥配置了自动轮换，并且想要停止轮换，则可以取消轮换。

取消自动旋转

1. 打开 Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择您的密钥。
3. 在密钥详细信息页面的轮换配置下，选择编辑轮换。
4. 在 “编辑旋转配置” 对话框中，关闭 “自动旋转”，然后选择 “保存”。

   Secrets Manager 会保留轮换配置信息，这样当你决定重新开启轮换功能时，你可以在将来使用这些信息。

AWS Secrets Manager 由其他 AWS 服务管理的机密

许多 AWS 服务在中存储和使用机密 AWS Secrets Manager。在某些情况下，这些密钥是托管密钥，这意味着创建这些密钥的服务可以帮助管理它们。例如，一些托管密钥包括托管轮换，因此您不必自己配置轮换。托管服务还可能限制您在没有恢复期的情况下更新密钥或删除它们，这有助于防止中断，因为托管服务依赖于密钥。

托管密钥使用包括管理服务 ID 的命名约定来帮助识别它们。

```
Secret name: ServiceID!MySecret
Secret ARN : arn:aws:us-east-1:ServiceID!MySecret-a1b2c3
```

管理密钥的服务的 ID

- `appflow` – the section called “Amazon AppFlow”
- `databrew` – the section called “AWS Glue DataBrew”
- `datasync` – the section called “AWS DataSync”
- `directconnect` – the section called “AWS Direct Connect”
- `ecs-sc` – the section called “Amazon Elastic Container Service”
- `events` – the section called “Amazon EventBridge”
- `marketplace-deployment` – the section called “AWS Marketplace”
- `opsworks-cm` – the section called “AWS OpsWorks for Chef Automate”
- `rds` – the section called “Amazon RDS”
- `redshift` – the section called “Amazon Redshift”
- `sqlworkbench` – the section called “Amazon Redshift 查询编辑器 v2”

要查找由其他 AWS 服务管理的密钥，请参阅查找托管密钥。

有关使用密钥的服务的完整列表，请参阅使用机密的服务。

AWS 使用 AWS Secrets Manager 机密的服务

获取有关以下各项如何与 Secrets Manager AWS 服务 集成的信息。

- 如何 AWS App Runner 使用 AWS Secrets Manager
- AWS App2Container 如何使用 AWS Secrets Manager
- 如何 AWS AppConfig 使用 AWS Secrets Manager
- 亚马逊如何 AppFlow 使用 AWS Secrets Manager
- 如何 AWS AppSync 使用 AWS Secrets Manager
- Amazon Athena 如何使用 AWS Secrets Manager
- 亚马逊 Aurora 是如何使用的 AWS Secrets Manager
- 如何 AWS CodeBuild 使用 AWS Secrets Manager
- Firehose 如何使用亚马逊数据 AWS Secrets Manager
- 如何 AWS DataSync 使用 AWS Secrets Manager
- 亚马逊如何 DataZone 使用 AWS Secrets Manager
- 如何 AWS Direct Connect 使用 AWS Secrets Manager
- 如何 AWS Directory Service 使用 AWS Secrets Manager
- Amazon DocumentDB（with MongoDB compatibility）如何使用 AWS Secrets Manager
- 如何 AWS Elastic Beanstalk 使用 AWS Secrets Manager
- Amazon 弹性容器注册表的使用方式 AWS Secrets Manager
- Amazon Elastic Container Service
- 亚马逊如何 ElastiCache 使用 AWS Secrets Manager
- 如何 AWS Elemental Live 使用 AWS Secrets Manager
- 如何 AWS Elemental MediaConnect 使用 AWS Secrets Manager
- 如何 AWS Elemental MediaConvert 使用 AWS Secrets Manager
- 如何 AWS Elemental MediaLive 使用 AWS Secrets Manager
- 如何 AWS Elemental MediaPackage 使用 AWS Secrets Manager
- 如何 AWS Elemental MediaTailor 使用 AWS Secrets Manager
- Amazon EMR 如何使用 Secrets Manager

- 亚马逊如何 EventBridge 使用 AWS Secrets Manager
- 亚马逊 FSx 如何使用机密 AWS Secrets Manager
- 如何 AWS Glue DataBrew 使用 AWS Secrets Manager
- AWS Glue Studio 如何使用 AWS Secrets Manager
- 如何 AWS IoT SiteWise 使用 AWS Secrets Manager
- 亚马逊 Kendra 是如何使用的 AWS Secrets Manager
- 亚马逊 Kinesis Video Streams 是如何使用的 AWS Secrets Manager
- 如何 AWS Launch Wizard 使用 AWS Secrets Manager
- Amazon Lookout for Metrics 如何使用 AWS Secrets Manager
- Amazon Managed Grafana 是如何使用的 AWS Secrets Manager
- 如何 AWS Managed Services 使用 AWS Secrets Manager
- Amazon Managed Streaming for Apache Kafka 如何使用 AWS Secrets Manager
- Apache Airflow 的亚马逊托管工作流程是如何使用的 AWS Secrets Manager
- AWS Marketplace
- 如何 AWS Migration Hub 使用 AWS Secrets Manager
- 如何 AWS Panorama 使用 Secrets Manager
- 如何 AWS ParallelCluster 使用 AWS Secrets Manager
- Amazon Q 如何使用 Secrets Manager
- 如何 AWS OpsWorks for Chef Automate 使用 AWS Secrets Manager
- 亚马逊如何 QuickSight 使用 AWS Secrets Manager
- Amazon RDS
- 亚马逊 Redshift 的使用方式 AWS Secrets Manager
- Amazon Redshift 查询编辑器 v2
- 亚马逊如何 SageMaker 使用 AWS Secrets Manager
- 如何 AWS Schema Conversion Tool 使用 AWS Secrets Manager
- 如何 AWS Toolkit for JetBrains 使用 AWS Secrets Manager
- 如何 AWS Transfer Family 使用 AWS Secrets Manager 秘密
- AWS Wickr 是如何使用秘密 AWS Secrets Manager 的

如何 AWS App Runner 使用 AWS Secrets Manager

AWS App Runner 是一项 AWS 服务，它提供了一种快速、简单且经济实惠的方式，可将源代码或容器映像直接部署到 AWS 云中可扩展且安全的 Web 应用程序。您无需学习新技术、决定使用哪种计算服务，也不需要知道如何预置和配置 AWS 资源。

使用 App Runner，您可以在创建服务或更新服务的配置时将密钥和配置引用为服务中的环境变量。有关更多信息，请参阅《AWS App Runner 开发人员指南》中的引用环境变量和管理环境变量。

AWS App2Container 如何使用 AWS Secrets Manager

AWS App2Container 是一款命令行工具，可帮助您提升和转移在本地数据中心或虚拟机上运行的应用程序，使其在由 Amazon ECS、Amazon EKS 或管理的容器中运行 AWS App Runner。

App2Container 使用 Secrets Manager 来管理用于将工件计算机连接到应用程序服务器的凭证，以便运行远程命令。有关更多信息，请参阅 App2Container 用户指南中的管理 AWS App2Contain AWS er 的密钥。

如何 AWS AppConfig 使用 AWS Secrets Manager

AWS AppConfig 是一种可用于创建、管理和快速部署应用程序配置的功能。 AWS Systems Manager 配置可包含存储在 Secrets Manager 中的凭证数据或其他敏感信息。当您创建自由格式配置文件时，可以选择 Secrets Manager 作为配置数据的来源。有关更多信息，请参阅《AWS AppConfig 用户指南》中的创建自由格式配置文件。有关如何 AWS AppConfig 处理开启自动轮换功能的密钥的信息，请参阅《AWS AppConfig 用户指南》中的 S ecrets Manager 密钥轮换。

亚马逊如何 AppFlow 使用 AWS Secrets Manager

亚马逊 AppFlow 是一项完全托管的集成服务，使您能够在软件即服务（SaaS）应用程序（例如 Salesforce）与亚马逊简单存储服务（Amazon S3）和 AWS 服务 Amazon Redshift等应用程序之间安全地交换数据。

在 Amazon 中 AppFlow，当您将一个 SaaS 应用程序配置为源或目标时，您就创建了一个连接。这包括连接到 SaaS 应用程序所需的信息，例如身份验证令牌、用户名和密码。亚马逊将您的连接数据 AppFlow 存储在带前缀的 Secrets Manager 托管密钥中`appflow`。存储密钥的费用已包含在亚马逊的费用中 AppFlow。有关更多信息，请参阅亚马逊 AppFlow 用户指南 AppFlow中的亚马逊数据保护。

如何 AWS AppSync 使用 AWS Secrets Manager

AWS AppSync 为应用程序开发人员提供了一个强大、可扩展的 GraphQL 接口，用于合并来自多个来源的数据，包括亚马逊 DynamoDB AWS Lambda和 HTTP API。

AWS AppSync 使用 CLI 命令使用密钥中的证书连接`rds execute-statement`到 Amazon RDS。有关更多信息，请参阅《AWS AppSync 开发人员指南》中的教程：Aurora Serverless。

Amazon Athena 如何使用 AWS Secrets Manager

Amazon Athena 是一种交互式查询服务，让您能够轻松使用标准 SQL 直接分析 Amazon Simple Storage Service（Amazon S3）中的数据。

Amazon Athena 数据源连接器可以将 Athena 联合查询功能与 Secrets Manager 密钥结合使用，从而查询数据。有关更多信息，请参阅《Amazon Athena 用户指南》中的使用 Amazon Athena 联合查询。

亚马逊 Aurora 是如何使用的 AWS Secrets Manager

Amazon Aurora 是一个与 MySQL 和 PostgreSQL 兼容的完全托管式的关系数据库引擎。

要管理 Aurora 的主用户证书，Aurora 可以为您创建托管密钥。您需要为此密钥支付费用。Aurora 还管理这些证书的轮换。有关更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon Aurora 和 AWS Secrets Manager管理密码。

有关其他 Aurora 凭证的信息，请参阅the section called “创建数据库密钥”。

调用 Amazon RDS Data API 时，您可以使用 Secrets Manager 中的密钥传递数据库的凭证。有关更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Aurora Serverless 数据 API。

使用 Amazon RDS 查询编辑器连接到数据库时，可以将数据库的凭证存储在 Secrets Manager 中。有关更多信息，请参阅 Amazon RDS 用户指南中的使用查询编辑器。

如何 AWS CodeBuild 使用 AWS Secrets Manager

AWS CodeBuild 是云端完全托管的生成服务。 CodeBuild 编译您的源代码，运行单元测试，并生成准备部署的工件。

您可以使用 Secrets Manager 存储私有注册表凭证。有关更多信息，请参阅《AWS CodeBuild 用户指南》 CodeBuild中的私有注册表及其 AWS Secrets Manager 示例。

Firehose 如何使用亚马逊数据 AWS Secrets Manager

您可以使用 Amazon Data Firehose 将实时流媒体数据传送到各种直播目的地。当目标需要凭据或密钥时，Firehose 会在运行时从 Secrets Manager 检索密钥以连接到目标。有关更多信息，请参阅《亚马逊数据 Fireh AWS Secrets Manager ose 开发者指南》中的使用亚马逊数据 Firehose 进行身份验证。

如何 AWS DataSync 使用 AWS Secrets Manager

AWS DataSync 是一项在线数据传输服务，可简化、自动化和加速存储系统和服务之间的数据移动。DataSync Discovery 可帮助您加快迁移到 AWS。

为了收集有关本地存储系统的信息， DataSync Discovery 使用存储系统管理界面的凭据。 DataSync 将这些凭据存储在带前缀的 Secret s Manager 托管密钥中`datasync`。您需要为此密钥支付费用。有关更多信息，请参阅AWS DataSync 用户指南中的将本地存储系统添加到 DataSync Discovery。

亚马逊如何 DataZone 使用 AWS Secrets Manager

Amazon DataZone 是一项数据管理服务，可让您对数据进行分类、发现、管理、共享和分析。您可以使用来自使用任务抓取的 Amazon Redshift 集群中的表和视图中的数据资产。 AWS Glue 爬网程序要连接亚马逊 Redshift，您需要在 Secrets Manager 密钥中提供亚马逊 DataZone凭证。有关更多信息，请参阅亚马逊 DataZone 用户指南中的使用新 AWS Glue 连接为 Amazon Redshift 数据库创建数据源。

如何 AWS Direct Connect 使用 AWS Secrets Manager

AWS Direct Connect 通过标准以太网光纤电缆将您的内部网络链接到某个 AWS Direct Connect 位置。通过此连接，您可以直接创建面向公众的虚拟接口 AWS 服务。

AWS Direct Connect 将连接关联密钥名称和连接关联密钥对（CKN/CAK 对）存储在带有前缀的托管密钥中。`directconnect`秘密的费用已包含在费用中 AWS Direct Connect。要更新密钥，必须使用 AWS Direct Connect 而不是 Secrets Manager。有关更多信息，请参阅 AWS Direct Connect 用户指南中的将 MACsec CKN/CAK 与 LAG 关联。

如何 AWS Directory Service 使用 AWS Secrets Manager

AWS Directory Service 提供了多种将 Microsoft Active Directory (AD) 与其他 AWS 服务一起使用的方法。您可以使用凭证的密钥将 Amazon EC2 实例加入到您的目录。有关更多信息，请参阅《AWS Direct Connect 用户指南》中的以下内容：

- 将 Linux EC2 实例无缝加入你的微软 AD AWS 托管目录
- 将 Linux EC2 实例无缝加入 AD Connector 目录
- 将 Linux EC2 实例无缝加入 Simple AD 目录

Amazon DocumentDB（with MongoDB compatibility）如何使用 AWS Secrets Manager

在 Amazon DocumentDB 中，用户与密码一起使用才能通过集群的身份验证。借助 AWS Secrets Manager，您可以将代码中的硬编码凭证（包括密码）替换为对 Secrets Manager 的 API 调用，从而以编程方式检索密钥。有关更多信息，请参阅《Amazon DocumentDB 开发人员指南》中的 the section called “创建数据库密钥” 和管理 Amazon DocumentDB 用户。

如何 AWS Elastic Beanstalk 使用 AWS Secrets Manager

借 AWS Elastic Beanstalk助，您可以快速部署和管理 AWS 云端应用程序，而不必了解运行这些应用程序的基础架构。Elastic Beanstalk 可通过生成 Dockerfile 中描述的映像或提取远程 Docker 映像来启动 Docker 环境。为了向托管私有存储库的在线注册表进行身份验证，Elastic Beanstalk 使用 Secrets Manager 密钥。有关更多信息，请参阅《AWS Elastic Beanstalk 开发人员指南》中的 Docker配置。

Amazon 弹性容器注册表的使用方式 AWS Secrets Manager

Amazon Elastic Container Registry (Amazon ECR) AWS 是一项安全、可扩展且可靠的托管容器镜像注册服务。您可以使用 Docker CLI 或首选客户端从存储库推送和提取镜像。对于包含您要在 Amazon ECR 私有注册表中缓存的映像的每个上游注册表，您必须创建缓存提取规则。对于需要身份验证的上游注册表，您必须以 Secrets Manager 密钥存储凭证。您可以在 Amazon ECR 或 Secrets Manager 控制台中创建 Secrets Manager 密钥。有关更多信息，请参阅 Amazon ECR 用户指南中的创建直通缓存规则。

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) 是一种完全托管式的容器编排服务，可以帮助您轻松部署、管理和扩展容器化应用程序。您可以通过引用 Secrets Manager 密钥将敏感数据注入容器。有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的以下页面：

- 教程：使用 Secrets Manager 密钥指定敏感数据

- 通过应用程序以编程方式检索密钥
- 通过环境变量检索密钥
- 检索日志记录配置的密钥

Amazon ECS 支持容器的 FSx for Windows File Server 卷。Amazon ECS 使用存储在 Secrets Manager 密钥中的凭证，用于域加入 Active Directory 和附加 FSx for Windows File Server 文件系统。有关更多信息，请参阅教程：将 FSx for Windows File Server 文件系统与 Amazon ECS 结合使用和《Amazon Elastic Container Service 开发人员指南》中的 FSx for Windows File Server 卷。

您可以通过使用带有注册表凭据的 Secrets Manager 密钥来引用需要身份验证的私有注册表中的容器镜像。 AWS 有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的任务的私有注册表身份验证。

当你使用 Amazon ECS Service Connect 时，Amazon ECS 使用 Secrets Manager 托管密钥来存储 AWS Private Certificate Authority TLS 证书。存储密钥的费用包含在 Amazon ECS 的费用中。要更新密钥，您必须使用 Amazon ECS 而不是 Secrets Manager。有关更多信息，请参阅《亚马逊弹性容器服务开发者指南》中的带有 Service Connect 的 TLS。

亚马逊如何 ElastiCache 使用 AWS Secrets Manager

在中， ElastiCache 您可以使用名为基于角色的访问控制 (RBAC) 的功能来保护集群。您可以将这些凭证存储在 Secrets Manager 中。Secrets Manager 为这种类型的密钥提供轮换模板。有关更多信息，请参阅 Amazon 用户指南中的自动轮换 ElastiCache 用户密码。

如何 AWS Elemental Live 使用 AWS Secrets Manager

AWS Elemental Live 是一项实时视频服务，可让您为广播和流媒体传输创建实时输出。

AWS Elemental Live 使用秘密 ARN 从 Secrets Manager 获取包含加密密钥的密钥。Elemental Live 使用加密密钥来加密/解密视频。有关更多信息，请参阅 Elemental Live 用户指南中的从 AWS Elemental Live 到的交付在运行时 MediaConnect 的工作原理。

如何 AWS Elemental MediaConnect 使用 AWS Secrets Manager

AWS Elemental MediaConnect 是一项服务，使广播公司和其他优质视频提供商可以轻松可靠地将直播视频摄入其中， AWS Cloud 并将其分发到内部或外部的多个目的地。 AWS Cloud

您可以使用静态密钥加密来保护源、输出和授权，并将加密密钥存储在 AWS Secrets Manager中。有关更多信息，请参阅《AWS Elemental MediaConnect 用户指南》 AWS Elemental MediaConnect中的静态密钥加密。

如何 AWS Elemental MediaConvert 使用 AWS Secrets Manager

AWS Elemental MediaConvert 是一种基于文件的视频处理服务，可为拥有任何规模媒体库的内容所有者和发行商提供可扩展的视频处理。 MediaConvert 要使用凯度水印进行编码，你可以使用 Secrets Manager 来存储你的凯度凭证。有关更多信息，请参阅《用户指南》中的 “使用Kantar在 AWS Elemental MediaConvert 输出中添加音频水印”AWS Elemental MediaConvert 。

如何 AWS Elemental MediaLive 使用 AWS Secrets Manager

AWS Elemental MediaLive 是一项实时视频服务，可让您为广播和流媒体传输创建实时输出。如果您的组织使用带有 AWS Elemental MediaLive 或的 AWS Elemental Link 设备 AWS Elemental MediaConnect，则必须部署设备并配置设备。有关更多信息，请参阅《MediaLive 用户指南》中的设置 MediaLive 为可信实体。

如何 AWS Elemental MediaPackage 使用 AWS Secrets Manager

AWS Elemental MediaPackage 是一项在中运行的 just-in-time 视频打包和创作 AWS Cloud服务。借MediaPackage助，您可以向各种播放设备和内容交付网络 (CDN) 提供高度安全、可扩展和可靠的视频流。有关更多信息，请参阅《AWS Elemental MediaPackage 用户指南》中的 S ecrets Manager 访问以获得 CDN 授权。

如何 AWS Elemental MediaTailor 使用 AWS Secrets Manager

AWS Elemental MediaTailor 是一项可扩展的广告插入和频道组装服务，运行在 AWS Cloud.

MediaTailor 支持对你的来源位置进行 Secrets Manager 访问令牌身份验证。通过 Secrets Manager 访问令牌身份验证， MediaTailor 使用 Secrets Manager 密钥对发往您的来源的请求进行身份验证。有关更多信息，请参阅《AWS Elemental MediaTailor 用户指南》中的配置 AWS Secrets Manager 访问令牌身份验证。

Amazon EMR 如何使用 Secrets Manager

亚马逊 EMR 是一个平台，可简化大数据框架（例如 Apache Hadoop 和 Apache Spark）的运行，AWS 以处理和分析大量数据。使用这些框架和相关的开源项目（如 Apache Hive 和 Apache Pig）

時，您可以处理用于分析的数据和商业智能工作负载。您还可以使用 Amazon EMR 将大量数据转换进出其他 AWS 数据存储和数据库，例如 Amazon S3 和 Amazon DynamoDB。

在 Amazon EC2 上运行的 Amazon EMR 如何使用 Secrets Manager

在 Amazon EMR 中创建集群时，您可以使用 Secrets Manager 中的密钥向集群提供应用程序配置数据。有关更多信息，请参阅 Amazon EMR 管理指南 中的在 Secrets Manager 中存储敏感配置数据。

此外，当您创建 EMR Notebook 时，可以使用 Secrets Manager 存储基于 Git 的私有注册表凭证。有关更多信息，请参阅《Amazon EMR 管理指南》中的将基于 Git 的存储库添加到 Amazon EMR。

EMR Serverless 如何使用密 Secrets Manager

EMR Serverless 提供无服务器运行时环境以简化分析应用程序的操作，因此您无需配置、优化、保护或操作集群。

您可以将数据存储在中， AWS Secrets Manager 然后在 EMR Serverless 配置中使用该密钥 ID。这样，您就不会以明文形式传递敏感的配置数据，也不会将其公开给外部 API。

有关更多信息，请参阅 Amazon EMR Serverless 用户指南中的使用 EMR Serverless 进行数据保护的 Secrets Manager。

亚马逊如何 EventBridge 使用 AWS Secrets Manager

Amazon EventBridge 是一项无服务器事件总线服务，可用于将应用程序与来自各种来源的数据连接起来。

当您创建 Amazon EventBridge API 目标时，会将其连接 EventBridge 存储在带有前缀的 Secrets Manager 托管密钥中`events`。存储此密钥的成本包含在使用 API 目标的费用中。要更新密钥，必须使用 EventBridge而不是 Secrets Manager。有关更多信息，请参阅 Amazon EventBridge 用户指南中的 API 目的地。

亚马逊 FSx 如何使用机密 AWS Secrets Manager

适用于 Windows File Server 的 Amazon FSx 提供完全托管式的 Microsoft Windows 文件服务器，由完全原生的 Windows 文件系统提供支持。创建或管理文件共享时，您可以传递来自 AWS Secrets Manager 密钥的证书。有关更多信息，请参阅《Amazon FSx for Windows File Server 用户指南》中的文件共享和将文件共享配置迁移到 Amazon FSx。

如何 AWS Glue DataBrew 使用 AWS Secrets Manager

AWS Glue DataBrew 是一款可视化数据准备工具，无需编写任何代码即可使用它来清理和标准化数据。在中 DataBrew，一组数据转换步骤称为配方。 AWS Glue DataBrew 提供了DETERMINISTIC_DECRYPTDETERMINISTIC_ENCRYPT、和CRYPTOGRAPHIC_HASH配方步骤，用于对数据集中的个人身份信息 (PII) 执行转换，这些信息使用存储在 Secrets Manager 密钥中的加密密钥。如果您使用 DataBrew 默认密钥来存储加密密钥，则 DataBrew 会创建一个带有前缀的托管密钥`databrew`。存储密钥的费用包含在使用费用中 DataBrew。如果您创建新密钥来存储加密密钥，则 DataBrew 会创建一个带有前缀的密钥`AwsGlueDataBrew`。您需要为此密钥支付费用。

AWS Glue Studio 如何使用 AWS Secrets Manager

AWS Glue Studio 是一个图形界面，可以轻松地在中创建、运行和监控提取、转换和加载 (ETL) 作业。 AWS Glue通过在中配置 Elasticsearch Spark Connector，您可以将亚马逊 OpenSearch 服务用作提取、转换和加载 (ETL) 任务的数据存储。 AWS Glue Studio要连接到 OpenSearch 集群，你可以在 Secrets Manager 中使用密钥。有关更多信息，请参阅《AWS Glue 开发者指南》中的教程：使用适用于 Elasticsearch 的 AWS Glue 连接器。

如何 AWS IoT SiteWise 使用 AWS Secrets Manager

AWS IoT SiteWise 是一项托管服务，可让您大规模收集、建模、分析和可视化来自工业设备的数据。您可以使用 AWS IoT SiteWise 控制台创建网关。然后添加连接到网关的数据源、本地服务器或工业设备。如果您的源要求身份验证，请使用一个密钥来进行身份验证。有关更多信息，请参阅《AWS IoT SiteWise 用户指南》中的配置数据来源身份验证。

亚马逊 Kendra 是如何使用的 AWS Secrets Manager

Amazon Kendra 是一项高度准确且智能的搜索服务，可让用户使用自然语言处理和高级搜索算法搜索非结构化和结构化数据。

通过指定包含数据库凭证的密钥，您可以为存储在数据库中的文档建立索引。有关更多信息，请参阅 Amazon Kendra 用户指南中的使用数据库数据源。

亚马逊 Kinesis Video Streams 是如何使用的 AWS Secrets Manager

您可以使用 Amazon Kinesis Video Streams 连接到客户场所的 IP 摄像机，在本地录制和存储来自摄像机的视频，并将视频流式传输到云端进行长期存储、回放和分析处理。要录制和上传来自 IP 摄像机的媒体，请将 Kinesis Video Streams Edge Agent 部署到 AWS IoT Greengrass。您可以将访问流式传输到摄像机的媒体文件所需的凭证存储在 Secrets Manager 密钥中。有关更多信息，请参阅《Amazon Kinesis Video Streams 开发人员指南》中的将 Amazon Kinesis Video Streams Edge Agent 部署到 AWS IoT Greengrass。

如何 AWS Launch Wizard 使用 AWS Secrets Manager

AWS Launch Wizard for Active Directory 是一项应用 AWS Cloud 应用程序最佳实践的服务，可指导您在本地或内部设置新的 Active Directory 基础架构， AWS Cloud 或者向现有基础架构中添加域控制器。

AWS Launch Wizard 需要将域管理员凭据添加到 Secrets Manager 才能将您的域控制器加入活动目录。有关更多信息，请参阅《AWS Launch Wizard 用户指南》中的为 Active Directory AWS Launch Wizard 进行设置。

Amazon Lookout for Metrics 如何使用 AWS Secrets Manager

Amazon Lookout for Metrics 是一项可查找数据中的异常情况，确定其根本原因，并使您能够快速采取措施的服务。您可以将 Amazon Redshift 或 Amazon RDS 作为 Lookout for Metrics 检测器的数据源。要配置数据源，您可以使用包含数据库密码的密钥。有关更多信息，请参阅《Amazon Lookout for Metrics 开发人员指南》中的将 Amazon RDS 与 Lookout for Metrics 结合使用和将 Amazon Redshift 与 Lookout for Metrics 结合使用。

Amazon Managed Grafana 是如何使用的 AWS Secrets Manager

Amazon Managed Grafana 是一种安全的完全托管式数据可视化服务，您可以使用该服务即时查询、关联和可视化来自多个来源的运行指标、日志和跟踪。当您使用亚马逊 Redshift 作为数据源时，您可以使用密钥提供亚马逊 Redshift 证书。 AWS Secrets Manager 有关更多信息，请参阅《Amazon Managed Grafana 用户指南》中的 配置 Amazon Redshift。

如何 AWS Managed Services 使用 AWS Secrets Manager

AWS Managed Services 是一项企业服务，可为您的 AWS 基础架构提供持续管理。AMS 自助服务配置 (SSP) 模式提供对 AMS 托管账户中原生功能 AWS 服务 和 API 功能的完全访问权限。有关如何在 AMS 中请求 Secrets Manager 访问权限的信息，请参阅《AMS 高级用户指南》中的AWS Secrets Manager （ AMS 自助服务预置 ）。

Amazon Managed Streaming for Apache Kafka 如何使用 AWS Secrets Manager

Amazon Managed Streaming for Apache Kafka（ Amazon MSK ）是一项完全托管式服务，让您能够构建并运行使用 Apache Kafka 来处理串流数据的应用程序。您可以使用 AWS Secrets Manager来存储和保护用户名和密码，从而控制使用这些用户名和密码访问 Amazon MSK 集群的权限。有关更多信息，请参阅 Amazon Managed Streaming for Apache Kafka 开发人员指南中的使用 AWS Secrets Manager进行用户名和密码身份验证。

Apache Airflow 的亚马逊托管工作流程是如何使用的 AWS Secrets Manager

适用于 Apache Airflow 的亚马逊托管工作流程是 Apache Airflow 的托管编排服务，它可以更轻松地在云中大规模设置和操作 end-to-end 数据管道。

您可以使用 Secrets Manager 密钥配置 Apache Airflow 连接。有关更多信息，请参阅《适用于 Apache 气流的亚马逊托管工作流程用户指南》中的 AWS Secrets Manager “使用 Secrets Manager 密钥配置 Apache 气流连接” 和 “使用密钥获取 Ap ache 气流变量”。

AWS Marketplace

当您使用 AWS Marketplace Quick Launch 时， AWS Marketplace 会将您的软件与许可证密钥一起分发。 AWS Marketplace 将许可证密钥作为 Secrets Manager 托管密钥存储在你的账户中。存储密钥的费用包含在的费用中 AWS Marketplace。要更新密钥，必须使用 AWS Marketplace 而不是 Secrets Manager。有关更多信息，请参阅《AWS Marketplace 卖家指南》中的配置 Quick Launch。

如何 AWS Migration Hub 使用 AWS Secrets Manager

AWS Migration Hub 提供了一个位置来跟踪跨多个 AWS 工具和合作伙伴解决方案的迁移任务。

AWS Migration Hub Orchestrator 简化并自动将服务器和企业应用程序迁移到。 AWS Migration Hub Orchestrator 使用密钥来获取源服务器的连接信息。有关更多信息，请参阅《AWS Migration Hub 编排工具用户指南》中的以下内容：

- 将 SAP NetWeaver 应用程序迁移到 AWS
- 在 Amazon EC2 上为应用程序更换主机

Migration Hub Strategy Recommendations 为可行的应用程序转型路径提供了迁移和现代化策略建议。Strategy Recommendations 可以使用密钥来获取连接信息，从而分析 SQL Server 数据库。有关更多信息，请参阅 Strategy Recommendations 数据库分析。

如何 AWS Panorama 使用 Secrets Manager

AWS Panorama 是一项将计算机视觉引入本地摄像机网络的服务。您 AWS Panorama 用于注册设备、更新其软件以及向其部署应用程序。当您将视频流注册为应用程序的数据源时，如果该视频流受密码保护，则会将其凭据 AWS Panorama 存储在 Secrets Manager 密钥中。有关更多信息，请参阅《AWS Panorama 开发人员指南》中的管理 AWS Panorama 中的摄像机视频流。

如何 AWS ParallelCluster 使用 AWS Secrets Manager

AWS ParallelCluster 是一款开源集群管理工具，可用于在中部署和管理高性能计算 (HPC) 集群。AWS Cloud你可以创建一个多用户环境，其中包括与 AWS 托管 Microsoft AD（活动目录）集成的环境。 AWS ParallelCluster AWS ParallelCluster 使用 Secrets Manager 密钥来验证 Active Directory 的登录信息。有关更多信息，请参阅《AWS ParallelCluster 用户指南》中的集成 Active Directory。

Amazon Q 如何使用 Secrets Manager

要对 Amazon Q 进行身份验证以访问您的数据源，您需要使用 Secrets Manager 密钥向 Amazon Q 提供数据源访问凭证。如果您使用控制台，则可以选择创建新密钥或使用现有密钥。有关更多信息，请参阅 Amazon Q 开发者指南中的概念——身份验证。

如何 AWS OpsWorks for Chef Automate 使用 AWS Secrets Manager

AWS OpsWorks 是一项配置管理服务，可通过使用 OpsWorks Puppet Enterprise 或 AWS OpsWorks for Chef Automate，来帮助您在云企业中配置和操作应用程序。

当您在中创建新服务器时 AWS OpsWorks CM， OpsWorks CM 会将服务器的信息存储在 Secrets Manager 托管密钥中，前缀为前缀opsworks-cm。秘密的费用已包含在费用中 AWS OpsWorks。有关更多信息，请参阅 AWS OpsWorks 用户指南中的集成 AWS Secrets Manager。

亚马逊如何 QuickSight 使用 AWS Secrets Manager

Amazon QuickSight 是一项云规模的商业智能 (BI) 服务，可用于分析、数据可视化和报告。您可以在 Amazon 中使用各种数据源 QuickSight。如果您将数据库凭证存储在 Secrets Manager 密钥中，则亚马逊 QuickSight 可以使用这些密钥来连接数据库。有关更多信息，请参阅《亚马逊 QuickSight 用户指南》中的在亚马逊 QuickSight中使用 AWS Secrets Manager 密码代替数据库凭证。

Amazon RDS

Amazon Relational Database Service (Amazon RDS) 是一项 Web 服务，让用户能够在 AWS Cloud云中更轻松地设置、操作和扩展关系数据库。

要管理包括 Aurora 在内的亚马逊关系数据库服务 (Amazon RDS) 的主用户证书，Amazon RDS 可以为您创建托管密钥。您需要为此密钥支付费用。Amazon RDS 还管理这些凭证的轮换。有关更多信息，请参阅《Amazon RDS 用户指南》中的使用 Amazon RDS 和 AWS Secrets Manager管理密码。

有关其他 Amazon RDS 凭证，请参阅 the section called “创建数据库密钥”。

使用 Amazon RDS 查询编辑器连接到数据库时，可以将数据库的凭证存储在 Secrets Manager 中。有关更多信息，请参阅 Amazon RDS 用户指南中的使用查询编辑器。

亚马逊 Redshift 的使用方式 AWS Secrets Manager

Amazon Redshift 是云中一种完全托管的 PB 级数据仓库服务。

要管理亚马逊 Redshift 的管理员证书，亚马逊 Redshift 可以为您创建托管密钥。您需要为此密钥支付费用。亚马逊 Redshift 还管理这些证书的轮换。有关更多信息，请参阅《Amazon Redshift 管理指南》中的使用 AWS Secrets Manager管理 Amazon Redshift 管理员密码。

有关其他 Amazon Redshift 凭证，请参阅 the section called “创建数据库密钥”。

调用 Amazon Redshift Data API 时，您可以使用 Secrets Manager 中的密钥传递集群的凭证。有关更多信息，请参阅使用 Amazon Redshift Data API。

使用 Amazon Redshift 查询编辑器连接到数据库时，Amazon Redshift 可将您的凭证存储在带有前缀 `redshiftqueryeditor` 的 Secrets Manager 密钥中。您需要为此密钥支付费用。有关更多信息，请参阅《Amazon Redshift 管理指南》中的 使用查询编辑器查询数据库。

有关查询编辑器 v2，请参阅 the section called “Amazon Redshift 查询编辑器 v2”。

Amazon Redshift 查询编辑器 v2

Amazon Redshift 查询编辑器 v2 是一个单独的基于 Web 的 SQL 客户端应用程序，用于在 Amazon Redshift 数据仓库上创作和运行查询。当您使用 Amazon Redshift 查询编辑器 v2 连接到数据库时，Amazon Redshift 可以将您的凭证存储在带有前缀的 Secrets Manager 托管密钥中。`sqlworkbench`存储此密钥的成本包含在使用 Amazon Redshift 的费用中。要更新此密钥，您必须使用 Amazon Redshift 而非 Secrets Manager。有关更多信息，请参阅《Amazon Redshift 管理指南》中的 使用查询编辑器 v2。

有关之前的查询编辑器，请参阅 the section called “Amazon Redshift”。

亚马逊如何 SageMaker 使用 AWS Secrets Manager

SageMaker 是一项完全托管的机器学习服务。借 SageMaker助，数据科学家和开发人员可以快速轻松地构建和训练机器学习模型，然后将其直接部署到生产就绪的托管环境中。它提供了一个集成的 Jupyter 编写 Notebook 实例，供您轻松访问数据源以便进行探索和分析，因此您无需管理服务器。

您可以将 Git 存储库关联到 Jupyter notebook 实例，以将笔记本保存到即使您停止或删除笔记本电脑实例仍可持久保存的源代码控制环境中。您可以使用 Secrets Manager 管理私有存储库凭证。有关更多信息，请参阅《亚马逊 SageMaker 开发者指南》中的 “将 Git 存储库与亚马逊 SageMaker 笔记本实例关联”。

要从 Databricks 导入数据，Data Wrangler 会将您的 JDBC URL 存储在 Secrets Manager 中。有关更多信息，请参阅从 Databricks（JDBC）导入数据。

要从 Snowflake 导入数据，Data Wrangler 会将您的凭证存储在某个 Secrets Manager 密钥中。有关更多信息，请参阅从 Snowflake 导入数据。

如何 AWS Schema Conversion Tool 使用 AWS Secrets Manager

您可以使用 AWS Schema Conversion Tool (AWS SCT) 将现有数据库架构从一个数据库引擎转换为另一个数据库引擎。您可以转换关系 OLTP 架构或数据仓库架构。转换后的 Schema 适用

于 Amazon Relational Database Service（Amazon RDS）MySQL、MariaDB、Oracle、SQL Server、PostgreSQL 数据库、Amazon Aurora 数据库集群或Amazon Redshift 集群。转换后的架构也可以与 Amazon 弹性计算云实例上的数据库一起使用，或者作为数据存储在 S3 存储桶中。

转换数据库架构时，AWS SCT 可以使用存储在中的数据库凭据 AWS Secrets Manager。有关更多信息，请参阅《用户指南》 AWS Secrets Manager 中的在 AWS SCT 用户界面中AWS Schema Conversion Tool 使用。

如何 AWS Toolkit for JetBrains 使用 AWS Secrets Manager

AWS Toolkit for JetBrains 是用于集成开发环境 (IDE) 的开源插件 JetBrains。此工具包使开发人员能够更轻松地开发、调试和部署使用 AWS的无服务器应用程序。使用此工具包连接到 Amazon Redshift 集群时，您可以使用 Secrets Manager 密钥进行身份验证。有关更多信息，请参阅《AWS Toolkit for JetBrains 用户指南》中的访问 Amazon Redshift 集群。

如何 AWS Transfer Family 使用 AWS Secrets Manager 秘密

AWS Transfer Family 是一种安全的传输服务，使您能够将文件传入和传出 AWS 存储服务。

Transfer Family 现在支持对使用适用性声明 2 (AS2) 协议的服务器使用基本身份验证。您可以创建新的 Secrets Manager 密钥，也可以选择现有密钥作为凭证。有关更多信息，请参阅《AWS Transfer Family 用户指南》中的 AS2 连接器的基本身份验证。

要对 Transfer Family 用户进行身份验证，您可以 AWS Secrets Manager 将其用作身份提供者。有关更多信息，请参阅《AWS Transfer Family 用户指南》中的使用自定义身份提供商和博客文章启用密码身份验证以供 AWS Transfer Family 使用 AWS Secrets Manager。

您可以对 Transfer Family 通过工作流程处理的文件使用 Pretty Good Privacy (PGP) 解密。要在工作流程步骤中使用解密，您需要提供在 Secrets Manager 中管理的 PGP 密钥。有关更多信息，请参阅《AWS Transfer Family 用户指南》中的生成和管理 PGP 密钥。

AWS Wickr 是如何使用秘密 AWS Secrets Manager 的

AWS Wickr 是一项 end-to-end 加密服务，可帮助组织和政府机构通过群组消息、语音 one-to-one 和视频通话、文件共享、屏幕共享等进行安全通信。您可以使用 Wickr 数据留存机器人实现工作流的自动化。如果机器人可以访问 AWS 服务，那么你应该创建一个 Secrets Manager 密钥来存储机器人凭证。有关更多信息，请参阅《AWS Wickr 管理指南》中的 启动数据留存机器人。

使用 AWS Secrets Manager VPC 终端节点

我们建议您在无法从私有网络访问的专用网络上运行尽可能多的基础设施。您可以通过创建接口 VPC 终端节点在 VPC 与 Secrets Manager 之间建立私有连接。接口端点由 AWS PrivateLink 提供支持，该技术支持您通过私有连接访问 Secrets Manager API，而无需采用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与 Secrets Manager API 进行通信。您的 VPC 与 Secrets Manager 之间的流量不会离开 AWS 网络。有关更多信息，请参阅《Amazon VPC 用户指南》中的接口 VPC 端点 (AWS PrivateLink)。

当 Secrets Manager 使用 Lambda 轮换函数轮换密钥（例如包含数据库凭证的密钥）时，Lambda 函数将同时向数据库和 Secrets Manager 发出请求。在使用控制台启用自动轮换后，Secrets Manager 将在与您的数据库相同的 VPC 中创建 Lambda 函数。建议您在同一 VPC 中创建 Secrets Manager 端点，以便从 Lambda 轮换函数向 Secrets Manager 发出的请求不会传出 Amazon 网络。

如果为端点启用私有 DNS，则可以使用其原定设置的 DNS 名称用作区域名，向 Secrets Manager 发送 API 请求，例如 `secretsmanager.us-east-1.amazonaws.com`。有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口端点访问服务。

您可以通过在权限策略中包含条件来确保对 Secrets Manager 的请求来自 VPC 访问。有关更多信息，请参阅 the section called “示例：权限和 VPC”。

您还可以使用 AWS CloudTrail 日志来审计您通过 VPC 终端节点使用秘密的情况。

为 Secrets Manager 创建 VPC 端点

1. 请参阅 Amazon VPC 用户指南中的创建接口终端节点。使用服务名称：com.amazonaws.*region*.secretsmanager
2. 要控制对终端节点的访问，请参阅使用终端节点策略控制 VPC 终端节点的访问权限。

共享子网

您无法在与您共享的子网中创建、描述、修改或删除 VPC 端点。但是，您可以在与您共享的子网中使用 VPC 端点。有关 VPC 共享的信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的与其他账户共享 VPC。

在 AWS CloudFormation 中创建 AWS Secrets Manager 密钥

您可以使用 CloudFormation 模板中的 `AWS::SecretsManager::Secret` 资源在 CloudFormation 堆栈中创建密钥，如 创建密钥 中所示。

要为 Amazon RDS 或 Aurora 创建管理员密钥，建议您使用 `AWS::RDS::DBCluster` 中的 `ManageMasterUserPassword`。然后，Amazon RDS 为您创建密钥并管理轮换。有关更多信息，请参阅托管轮换。

对于 Amazon Redshift 和 Amazon DocumentDB 凭证，请首先使用 Secret Manager 生成的密码创建密钥，然后使用动态引用从该密钥中检索用户名和密码，以用作新数据库的凭证。接下来，使用 `AWS::SecretsManager::SecretTargetAttachment` 资源将有关数据库的详细信息添加到 Secrets Manager 需要轮换密钥的密钥。最后，要启用自动轮换，请使用 `AWS::SecretsManager::RotationSchedule` 资源并提供轮换函数和计划。请参阅以下示例：

- 使用 Amazon Redshift 凭证创建密钥
- 使用 Amazon DocumentDB 凭证创建密钥

要将资源策略附加到您的秘密，请使用 `AWS::SecretsManager::ResourcePolicy` 资源。

有关使用 AWS CloudFormation 创建资源的信息，请参阅《AWS CloudFormation 用户指南》中的了解模板基础知识。您也可以使用 AWS Cloud Development Kit (AWS CDK)。有关更多信息，请参阅 AWS Secrets Manager 构建库。

使用 AWS CloudFormation 创建 AWS Secrets Manager 密钥

此示例将创建一个名为 **CloudFormationCreatedSecret-*a1b2c3d4e5f6*** 的密钥。密码值是下面的 JSON，其中包含一个 32 个字符的密码，该密码是在创建密钥时生成的。

```
{
    "password": "EXAMPLE-PASSWORD",
    "username": "saanvi"
}
```

此示例使用以下 CloudFormation 资源：

- `AWS::SecretsManager::Secret`

有关使用 AWS CloudFormation 创建资源的信息，请参阅《AWS CloudFormation 用户指南》中的了解模板基础知识。

JSON

```
{
    "Resources": {
        "CloudFormationCreatedSecret": {
            "Type": "AWS::SecretsManager::Secret",
            "Properties": {
                "Description": "Simple secret created by AWS CloudFormation.",
                "GenerateSecretString": {
                    "SecretStringTemplate": "{\"username\": \"saanvi\"}",
                    "GenerateStringKey": "password",
                    "PasswordLength": 32
                }
            }
        }
    }
}
```

YAML

```
Resources:
  CloudFormationCreatedSecret:
    Type: 'AWS::SecretsManager::Secret'
    Properties:
      Description: Simple secret created by AWS CloudFormation.
      GenerateSecretString:
        SecretStringTemplate: '{"username": "saanvi"}'
        GenerateStringKey: password
        PasswordLength: 32
```

创建自动轮换的 AWS Secrets Manager 密钥，然后使用 AWS CloudFormation 创建 Amazon RDS MySQL 数据库实例

要为 Amazon RDS 或 Aurora 创建管理员密钥，建议您使用 `ManageMasterUserPassword`，如 `AWS::RDS::DBCluster` 中的示例为主密码创建 Secrets Manager 密钥所示。然后，Amazon RDS 为您创建密钥并管理轮换。有关更多信息，请参阅托管轮换。

使用创建 AWS Secrets Manager 密钥和亚马逊 Redshift 集群 AWS CloudFormation

要为 Amazon Redshift 创建管理员密钥，我们建议您使用和中的示例。AWS::Redshift::ClusterAWS::RedshiftServerless::Namespace

使用创建 AWS Secrets Manager 密钥和亚马逊文档数据库实例 AWS CloudFormation

此示例将创建一个秘密，并使用该秘密中的凭证作为用户和密码，创建一个 Amazon DocumentDB 实例。该密钥已附加用于指定谁可以访问密钥的基于资源的策略。该模板还可以从 轮换函数模板 创建 Lambda 轮换函数，并将秘密配置为协调世界时每月第一天上午 8:00 到 10:00 之间自动轮换。作为安全最佳实践，该实例位于 Amazon VPC 中。

此示例使用了 Secrets Manager 的以下 CloudFormation 资源：

- AWS::SecretsManager::Secret
- AWS::SecretsManager::SecretTargetAttachment
- AWS::SecretsManager::RotationSchedule

有关使用创建资源的信息 AWS CloudFormation，请参阅《 AWS CloudFormation 用户指南》中的 “学习模板基础知识”。

JSON

```
{
   "AWSTemplateFormatVersion":"2010-09-09",
   "Transform":"AWS::SecretsManager-2020-07-23",
   "Resources":{
      "TestVPC":{
         "Type":"AWS::EC2::VPC",
         "Properties":{
            "CidrBlock":"10.0.0.0/16",
            "EnableDnsHostnames":true,
            "EnableDnsSupport":true
         }
      },
      "TestSubnet01":{
```

```
         "Type":"AWS::EC2::Subnet",
         "Properties":{
            "CidrBlock":"10.0.96.0/19",
            "AvailabilityZone":{
               "Fn::Select":[
                  "0",
                  {
                     "Fn::GetAZs":{
                        "Ref":"AWS::Region"
                     }
                  }
               ]
            },
            "VpcId":{
               "Ref":"TestVPC"
            }
         }
      },
      "TestSubnet02":{
         "Type":"AWS::EC2::Subnet",
         "Properties":{
            "CidrBlock":"10.0.128.0/19",
            "AvailabilityZone":{
               "Fn::Select":[
                  "1",
                  {
                     "Fn::GetAZs":{
                        "Ref":"AWS::Region"
                     }
                  }
               ]
            },
            "VpcId":{
               "Ref":"TestVPC"
            }
         }
      },
      "SecretsManagerVPCEndpoint":{
         "Type":"AWS::EC2::VPCEndpoint",
         "Properties":{
            "SubnetIds":[
               {
                  "Ref":"TestSubnet01"
               },
```

```
            {
               "Ref":"TestSubnet02"
            }
         ],
         "SecurityGroupIds":[
            {
               "Fn::GetAtt":[
                  "TestVPC",
                  "DefaultSecurityGroup"
               ]
            }
         ],
         "VpcEndpointType":"Interface",
         "ServiceName":{
            "Fn::Sub":"com.amazonaws.${AWS::Region}.secretsmanager"
         },
         "PrivateDnsEnabled":true,
         "VpcId":{
            "Ref":"TestVPC"
         }
      }
   },
   "MyDocDBClusterRotationSecret":{
      "Type":"AWS::SecretsManager::Secret",
      "Properties":{
         "GenerateSecretString":{
            "SecretStringTemplate":"{\"username\": \"someadmin\",\"ssl\": true}",
            "GenerateStringKey":"password",
            "PasswordLength":16,
            "ExcludeCharacters":"\"@/\\"
         },
         "Tags":[
            {
               "Key":"AppName",
               "Value":"MyApp"
            }
         ]
      }
   },
   "MyDocDBCluster":{
      "Type":"AWS::DocDB::DBCluster",
      "Properties":{
         "DBSubnetGroupName":{
            "Ref":"MyDBSubnetGroup"
```

```
            },
            "MasterUsername":{
               "Fn::Sub":"{{resolve:secretsmanager:
${MyDocDBClusterRotationSecret}::username}}"
            },
            "MasterUserPassword":{
               "Fn::Sub":"{{resolve:secretsmanager:
${MyDocDBClusterRotationSecret}::password}}"
            },
            "VpcSecurityGroupIds":[
               {
                  "Fn::GetAtt":[
                     "TestVPC",
                     "DefaultSecurityGroup"
                  ]
               }
            ]
         }
      },
      "DocDBInstance":{
         "Type":"AWS::DocDB::DBInstance",
         "Properties":{
            "DBClusterIdentifier":{
               "Ref":"MyDocDBCluster"
            },
            "DBInstanceClass":"db.r5.large"
         }
      },
      "MyDBSubnetGroup":{
         "Type":"AWS::DocDB::DBSubnetGroup",
         "Properties":{
            "DBSubnetGroupDescription":"",
            "SubnetIds":[
               {
                  "Ref":"TestSubnet01"
               },
               {
                  "Ref":"TestSubnet02"
               }
            ]
         }
      },
      "SecretDocDBClusterAttachment":{
         "Type":"AWS::SecretsManager::SecretTargetAttachment",
```

```
         "Properties":{
            "SecretId":{
               "Ref":"MyDocDBClusterRotationSecret"
            },
            "TargetId":{
               "Ref":"MyDocDBCluster"
            },
            "TargetType":"AWS::DocDB::DBCluster"
         }
      },
      "MySecretRotationSchedule":{
         "Type":"AWS::SecretsManager::RotationSchedule",
         "DependsOn":"SecretDocDBClusterAttachment",
         "Properties":{
            "SecretId":{
               "Ref":"MyDocDBClusterRotationSecret"
            },
            "HostedRotationLambda":{
               "RotationType":"MongoDBSingleUser",
               "RotationLambdaName":"MongoDBSingleUser",
               "VpcSecurityGroupIds":{
                  "Fn::GetAtt":[
                     "TestVPC",
                     "DefaultSecurityGroup"
                  ]
               },
               "VpcSubnetIds":{
                  "Fn::Join":[
                     ",",
                     [
                        {
                           "Ref":"TestSubnet01"
                        },
                        {
                           "Ref":"TestSubnet02"
                        }
                     ]
                  ]
               }
            },
            "RotationRules":{
              "Duration": "2h",
              "ScheduleExpression": "cron(0 8 1 * ? *)"
            }
```

```
         }
      }
   }
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::SecretsManager-2020-07-23
Resources:
  TestVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
  TestSubnet01:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: 10.0.96.0/19
      AvailabilityZone: !Select
        - '0'
        - !GetAZs
          Ref: AWS::Region
      VpcId: !Ref TestVPC
  TestSubnet02:
    Type: AWS::EC2::Subnet
    Properties:
      CidrBlock: 10.0.128.0/19
      AvailabilityZone: !Select
        - '1'
        - !GetAZs
          Ref: AWS::Region
      VpcId: !Ref TestVPC
  SecretsManagerVPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      SubnetIds:
        - !Ref TestSubnet01
        - !Ref TestSubnet02
      SecurityGroupIds:
        - !GetAtt TestVPC.DefaultSecurityGroup
      VpcEndpointType: Interface
```

```
      ServiceName: !Sub com.amazonaws.${AWS::Region}.secretsmanager
      PrivateDnsEnabled: true
      VpcId: !Ref TestVPC
  MyDocDBClusterRotationSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      GenerateSecretString:
        SecretStringTemplate: '{"username": "someadmin","ssl": true}'
        GenerateStringKey: password
        PasswordLength: 16
        ExcludeCharacters: '"@/\'
      Tags:
        - Key: AppName
          Value: MyApp
  MyDocDBCluster:
    Type: AWS::DocDB::DBCluster
    Properties:
      DBSubnetGroupName: !Ref MyDBSubnetGroup
      MasterUsername: !Sub '{{resolve:secretsmanager:
${MyDocDBClusterRotationSecret}::username}}'
      MasterUserPassword: !Sub '{{resolve:secretsmanager:
${MyDocDBClusterRotationSecret}::password}}'
      VpcSecurityGroupIds:
        - !GetAtt TestVPC.DefaultSecurityGroup
  DocDBInstance:
    Type: AWS::DocDB::DBInstance
    Properties:
      DBClusterIdentifier: !Ref MyDocDBCluster
      DBInstanceClass: db.r5.large
  MyDBSubnetGroup:
    Type: AWS::DocDB::DBSubnetGroup
    Properties:
      DBSubnetGroupDescription: ''
      SubnetIds:
        - !Ref TestSubnet01
        - !Ref TestSubnet02
  SecretDocDBClusterAttachment:
    Type: AWS::SecretsManager::SecretTargetAttachment
    Properties:
      SecretId: !Ref MyDocDBClusterRotationSecret
      TargetId: !Ref MyDocDBCluster
      TargetType: AWS::DocDB::DBCluster
  MySecretRotationSchedule:
    Type: AWS::SecretsManager::RotationSchedule
```

```
    DependsOn: SecretDocDBClusterAttachment
    Properties:
      SecretId: !Ref MyDocDBClusterRotationSecret
      HostedRotationLambda:
        RotationType: MongoDBSingleUser
        RotationLambdaName: MongoDBSingleUser
        VpcSecurityGroupIds: !GetAtt TestVPC.DefaultSecurityGroup
        VpcSubnetIds: !Join
          - ','
          - - !Ref TestSubnet01
            - !Ref TestSubnet02
      RotationRules:
        Duration: 2h
        ScheduleExpression: cron(0 8 1 * ? *)
```

Secrets Manager 如何使用 AWS CloudFormation

当您使用控制台开启轮换功能时，Secrets Manager 会使用 AWS CloudFormation 为创建要用于轮换的资源。如果您在此过程中创建了新的轮换函数，则 AWS CloudFormation 会基于恰当的轮换函数模板 创建一个 `AWS::Serverless::Function`。然后 AWS CloudFormation 会设置 `RotationSchedule`，这将会设置密钥的轮换函数和轮换规则。开启自动轮换功能后，您可以选择横幅中的 View stack（查看堆栈）以查看 AWS CloudFormation 堆栈。

有关启用自动轮换功能的信息，请参阅 轮换 密钥。

在中创建 AWS Secrets Manager 密钥 AWS Cloud Development Kit (AWS CDK)

要在 CDK 应用程序中创建、管理和检索密钥，您可以使用 AWS Secrets Manager 构造库，其中包含了 `ResourcePolicy`、`RotationSchedule`、`Secret`、`SecretRotation` 和 `SecretTargetAttachment` 构造。

在 CDK 应用程序中使用密钥的一个好做法是先使用控制台或 CLI 创建密钥，然后将密钥导入到您的 CDK 应用程序中。

有关示例，请参阅：

- 创建密钥
- 导入密钥
- 检索密钥
- 授予使用密钥的权限
- 轮换密钥
- 轮换数据库密钥
- 将密钥复制到其他区域

有关 CDK 的更多信息，请参阅 AWS Cloud Development Kit (AWS CDK) v2 开发人员指南。

监控 AWS Secrets Manager 机密

AWS 提供监控工具，用于监视 Secrets Manager 的密钥，在出现问题时进行报告，并在适当时自动采取措施。如果您需要调查任何意外的使用或更改，您可以使用日志，并回滚不需要的更改。您还可以设置自动检查不当使用密钥的机制和任何尝试删除密钥的机制。

主题

使用记录 AWS Secrets Manager 事件 AWS CloudTrail

AWS CloudTrail 将 Secrets Manager 的所有 API 调用记录为事件，包括来自 Secrets Manager 控制台的调用，以及其他几个用于轮换和删除密钥版本的事件。有关 Secrets Manager 记录中日志条目的列表，请参阅CloudTrail 条目。

您可以使用 CloudTrail 控制台查看最近 90 天记录的事件。要持续记录您的 AWS 账户中的事件，包括 Secrets Manager 的事件，请创建一个跟踪，以便将日志文件 CloudTrail 传输到 Amazon S3 存储桶。请参阅为您的 AWS 账户创建跟踪。您也可以配置 CloudTrail 为接收来自多个 AWS 账户和的 CloudTrail 日志文件AWS 区域。

您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的数据。查看与 CloudTrail 日志的AWS 服务集成。当您向 Amazon S3 存储桶 CloudTrail 发布新的日志文件时，您还可以收到通知。有关信息，请参阅配置 Amazon SNS 通知。 CloudTrail

从 CloudTrail 日志中检索 Secrets Manager 事件（控制台）

1. 打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 确保控制台指向事件发生的地区。控制台仅显示选定区域中发生的事件。从控制台右上角的下拉列表中选择区域。
3. 在左侧导航窗格中，选择 Event history (事件历史记录)。

4. 选择 Filter (筛选) 条件和/或 Time range (时间范围) 以帮助您查找您在寻找的事件。例如：
   a. 要查看所有 Secrets Manager 事件，请在 “查找属性” 中选择 “事件源”。然后，对于 Enter event source (输入事件源)，选择 **`secretsmanager.amazonaws.com`**。
   b. 要查看密钥的所有事件，请在 “查找属性” 中选择 “资源名称”。然后，在 “输入资源名称” 中，输入密钥的名称。
5. 要查看更多详细信息，请选择活动旁边的展开箭头。要查看所有可用信息，请选择 View event (查看事件)。

AWS CLI

Example 从 CloudTrail 日志中检索 Secrets Manager 事件

以下 `lookup-events` 示例将查找 Secrets Manager 事件。

```
aws cloudtrail lookup-events \
    --region us-east-1 \
    --lookup-attributes
 AttributeKey=EventSource,AttributeValue=secretsmanager.amazonaws.com
```

AWS CloudTrail Secrets Manager 的参赛作品

AWS Secrets Manager 将所有 Secrets Manager 操作以及其他与轮换和删除相关的事件的条目写入您的 AWS CloudTrail 日志。有关对这些事件执行操作的信息，请参阅 将 Secrets Manager 活动与 EventBridge。

日志条目类型

- Secrets Manager 操作的日志条目
- 有关删除操作的日志条目
- 可用于复制的日志条目
- 有关轮换操作的日志条目

Secrets Manager 操作的日志条目

通过调用 Secrets Manager 操作生成的事件具有 `"detail-type": ["AWS API Call via CloudTrail"]`。

> **Note**
>
> 在 2024 年 2 月之前，一些 Secrets Manager 操作报告的事件中包含秘密 ARN 的 “arn” 而不是 “arn”。有关更多信息，请参阅 AWS re:Post。

以下是您或服务通过 API、SDK 或 CLI 调用 Secrets Manager 操作时生成的 CloudTrail 条目。

BatchGetSecretValue

由BatchGetSecretValue操作生成。有关检索密钥的信息，请参阅 获取秘密。

CancelRotateSecret

由CancelRotateSecret操作生成。有关轮换的更多信息，请参阅 轮换 密钥。

CreateSecret

由CreateSecret操作生成。有关创建密钥的信息，请参阅 创建和管理密钥。

DeleteResourcePolicy

由DeleteResourcePolicy操作生成。有关权限的信息，请参阅 身份验证和访问控制。

DeleteSecret

由DeleteSecret操作生成。有关删除密钥的信息，请参阅 the section called “删除密钥”。

DescribeSecret

由DescribeSecret操作生成。

GetRandomPassword

由GetRandomPassword操作生成。

GetResourcePolicy

由GetResourcePolicy操作生成。有关权限的信息，请参阅 身份验证和访问控制。

GetSecretValue

由GetSecretValue和BatchGetSecretValue操作生成。有关检索密钥的信息，请参阅 获取秘密。

ListSecrets

由ListSecrets操作生成。有关列出密钥的信息，请参阅 the section called “查找密钥”。

ListSecretVersionIds

由ListSecretVersionIds操作生成。

PutResourcePolicy

由PutResourcePolicy操作生成。有关权限的信息，请参阅 身份验证和访问控制。

PutSecretValue

由PutSecretValue操作生成。有关更新密钥的信息，请参阅 the section called “修改密钥”。

RemoveRegionsFromReplication

由RemoveRegionsFromReplication操作生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

ReplicateSecretToRegions

由ReplicateSecretToRegions操作生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

RestoreSecret

由RestoreSecret操作生成。有关还原已删除密钥的信息，请参阅 the section called “恢复密钥”。

RotateSecret

由RotateSecret操作生成。有关轮换的更多信息，请参阅 轮换 密钥。

StopReplicationToReplica

由StopReplicationToReplica操作生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

TagResource

由TagResource操作生成。有关标记密钥的信息，请参阅 the section called “标记 密钥”。

UntagResource

由UntagResource操作生成。有关取消密钥标签的信息，请参阅 the section called “标记 密钥”。

UpdateSecret

由UpdateSecret操作生成。有关更新密钥的信息，请参阅 the section called “修改密钥”。

UpdateSecretVersionStage

由UpdateSecretVersionStage操作生成。有关版本阶段的更多信息，请参阅 the section called “秘密版本”。

ValidateResourcePolicy

由ValidateResourcePolicy操作生成。有关权限的信息，请参阅 身份验证和访问控制。

有关删除操作的日志条目

除了生成与 Secrets Manager 操作有关的事件外，Secrets Manager 还会生成以下与删除有关的事件。这些事件具有 `"detail-type": ["AWS Service Event via CloudTrail"]`。

CancelSecretVersionDelete

由 Secrets Manager 服务生成。如果在具有版本的密钥上调用 `DeleteSecret`，然后再调用 `RestoreSecret`，则 Secrets Manager 会为还原的每个密钥版本记录此事件。有关还原已删除密钥的信息，请参阅 the section called “恢复密钥”。

EndSecretVersionDelete

在删除密钥版本时由 Secrets Manager 服务生成。有关更多信息，请参阅 the section called “删除密钥”。

StartSecretVersionDelete

在 Secrets Manager 开始删除密钥版本时由 Secrets Manager 服务生成。有关删除密钥的信息，请参阅 the section called “删除密钥”。

SecretVersionDeletion

在 Secrets Manager 删除已弃用的秘密版本时由 Secrets Manager 服务生成。有关更多信息，请参阅密钥版本。

可用于复制的日志条目

除了生成与 Secrets Manager 操作有关的事件外，Secrets Manager 还会生成以下与复制有关的事件。这些事件具有 `"detail-type": ["AWS Service Event via CloudTrail"]`。

ReplicationFailed

在复制失败时由 Secrets Manager 服务生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

ReplicationStarted

在 Secrets Manager 开始复制密钥时由 Secrets Manager 服务生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

ReplicationSucceeded

在成功复制密钥时由 Secrets Manager 服务生成。有关复制密钥的更多信息，请参阅 跨区域复制密钥。

有关轮换操作的日志条目

除了生成与 Secrets Manager 操作有关的事件外，Secrets Manager 还会生成以下与轮换有关的事件。这些事件具有 `"detail-type": ["AWS Service Event via CloudTrail"]`。

RotationStarted

在 Secrets Manager 开始轮换密钥时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 轮换 密钥。

RotationAbandoned

在 Secrets Manager 放弃轮换尝试并从密钥的某个现有版本删除 `AWSPENDING` 标签时由 Secrets Manager 服务生成。当您在轮换期间创建密钥的新版本时，Secrets Manager 会放弃轮换。有关轮换的更多信息，请参阅 轮换 密钥。

RotationFailed

在轮换失败时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 the section called “ 轮换问题排查”。

RotationSucceeded

在成功轮换密钥时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 轮换 密钥。

TestRotationStarted

在开始测试轮换某个尚未计划立即轮换的密钥时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 轮换 密钥。

TestRotationSucceeded

在成功测试轮换某个尚未计划立即轮换的密钥时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 轮换 密钥。

TestRotationFailed

在测试轮换某个尚未计划立即轮换的密钥但轮换失败时由 Secrets Manager 服务生成。有关轮换的更多信息，请参阅 the section called “ 轮换问题排查”。

AWS Secrets Manager 使用 Amazon 进行监控 CloudWatch

使用 Amazon CloudWatch，您可以监控 AWS 服务并创建警报，以便在指标发生变化时通知您。CloudWatch 将这些统计数据保留 15 个月，因此您可以访问历史信息并更好地了解 Web 应用程序或服务的性能。对于 AWS Secrets Manager，您可以监控账户中的密钥数量，包括标记为删除的密钥，以及对 Secrets Manager 的 API 调用，包括通过控制台进行的调用。有关如何监控指标的信息，请参阅CloudWatch 用户指南中的使用 CloudWatch 指标。

查找 Secrets Manager 指标

1. 在 CloudWatch 控制台的指标下，选择所有指标。
2. 在指标搜索框中，输入`secret`。
3. 执行以下操作：
   - 要监控您账户中的密钥数量，请选择 AWS/SecretsManager，然后选择SecretCount。该指标每小时发布一次。
   - 要监控对 Secrets Manager 的 API 调用，包括通过控制台进行的调用，请选择 “使用情况” > “按 AWS 资源”，然后选择要监控的 API 调用。有关 Secrets Manager API 的列表，请参阅 Secrets Manager 的操作。
4. 执行以下操作：
   - 要创建指标图表，请参阅 Amazon CloudWatch 用户指南中的绘制指标图表。
   - 要检测异常，请参阅 A ma CloudWatch zon 用户指南中的使用 CloudWatch 异常检测。
   - 要获取指标的统计数据，请参阅 Amazon CloudWatch 用户指南中的获取指标的统计信息。

CloudWatch 警报

您可以创建一个 CloudWatch 警报，当指标值发生变化并导致警报状态发生变化时，该警报会发送 Amazon SNS 消息。您可以对 Secrets Manager 指标设置警报`ResourceCount`，该指标是您账户中的密钥数量。您还可以在 “警报” 上设置警报，在您指定的时间段内监视指标，并根据该指标在多个时间段内相对于给定阈值的值执行操作。警报仅针对持续的状态变化调用操作。 CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。

有关更多信息，请参阅CloudWatch 用户指南中的使用 Amazon CloudWatch CloudWatch 警报和基于异常检测创建警报。

还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

将赛 AWS Secrets Manager 事与 Amazon 进行匹配 EventBridge

在亚马逊中 EventBridge，您可以匹配 CloudTrail 日志条目中的 Secrets Manager 事件。您可以配置 EventBridge 规则来查找这些事件，然后将新生成的事件发送到目标以采取行动。有关 Secrets Manager 记录的 CloudTrail 条目列表，请参阅CloudTrail 条目。有关设置说明 EventBridge，请参阅《EventBridge 用户指南》 EventBridge中的 “入门”。

将所有更改与指定密钥匹配

> **Note**
>
> 由于某些 Secrets Manager 事件返回的密钥 ARN 大小写不同，所以在匹配多个操作的事件模式中，您可能需要同时包含密钥 `arn` 和 `aRN` 才能通过 ARN 指定密钥。有关更多信息，请参阅 AWS re:Post。

以下示例显示了一种 EventBridge 事件模式，该模式与密钥更改的日志条目相匹配。

```
{
    "source": ["aws.secretsmanager"],
    "detail-type": ["AWS API Call via CloudTrail"],
    "detail": {
        "eventSource": ["secretsmanager.amazonaws.com"],
        "eventName": ["DeleteResourcePolicy", "PutResourcePolicy", "RotateSecret",
 "TagResource", "UntagResource", "UpdateSecret"],
        "responseElements": {
            "arn": ["arn:aws:secretsmanager:us-west-2:012345678901:secret:mySecret-
a1b2c3"]
        }
    }
}
```

在轮换密钥值时匹配事件

以下示例显示了一种 EventBridge 事件模式，该模式与因手动更新或自动轮换而发生的机密值更改的 CloudTrail 日志条目相匹配。由于有些事件来自 Secrets Manager 操作，有些则由 Secrets Manager 服务生成，因此两者都必须包含 `detail-type`。

```
{
```

```
    "source": ["aws.secretsmanager"],
    "$or": [
        { "detail-type": ["AWS API Call via CloudTrail"] },
        { "detail-type": ["AWS Service Event via CloudTrail"] }
    ],
    "detail": {
        "eventSource": ["secretsmanager.amazonaws.com"],
        "eventName": ["PutSecretValue", "UpdateSecret", "RotationSucceeded"]
    }
}
```

监控计划删除的 AWS Secrets Manager 密钥何时被访问

您可以结合使用 Amazon CloudWatch 日志和亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 来创建警报，通知您任何试图访问待删除的密钥的行为。 AWS CloudTrail如果您收到告警的通知，您可能需要取消删除密钥，以给自己更多时间来确定是否确实要将其删除。您的调查可能会导致密钥被恢复，因为您仍然需要它。或者，您可能需要使用所用的新密钥的详细信息来更新用户。

以下过程说明了当请求`GetSecretValue`操作导致将特定错误消息写入 CloudTrail 日志文件时，如何收到通知。可以对密钥执行其他 API 操作而不会触发告警。此 CloudWatch 警报检测到可能表明某人或应用程序使用过期凭证的使用情况。

在开始这些过程之前，您必须在要监控 AWS Secrets Manager API 请求的 AWS 区域 和账户 CloudTrail 中开启。有关说明，请参阅 AWS CloudTrail 《用户指南》中的首次创建跟踪。

步骤 1：配置 CloudTrail 日志文件传输到 CloudWatch 日志

您必须配置将 CloudTrail 日志文件传送到 CloudWatch 日志。这样做是为了让 CloudWatch Logs 可以监控它们是否有 Secrets Manager API 请求以检索待删除的密钥。

配置 CloudTrail 日志文件传输到 CloudWatch 日志

1. 打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在顶部导航栏上，选择 AWS 区域 要监控密钥。
3. 在左侧导航窗格中，选择 Tra il s，然后选择要为其配置的跟踪的名称 CloudWatch。
4. 在 T rails 配置页面上，向下滚动到 “CloudWatch 日志” 部分，然后选择编辑图标 (✏)。
5. 对于 New or existing log group (新的或现有的日志组)，键入日志组的名称，例如 **`CloudTrail/MyCloudWatchLogGroup`**。

6. 对于 IAM 角色，您可以使用名为 CloudTrail_ CloudWatchLogs _Role 的默认角色。此角色具有默认角色策略，该策略具有向日志组传送 CloudTrail 事件所需的权限。
7. 选择 Continue (继续) 以保存您的配置。
8. 在AWS CloudTrail 将与您账户中 API 活动关联 CloudTrail 的事件发送到 CloudWatch 日志日志组页面上，选择允许。

步骤 2：创建 CloudWatch警报

要在 Secrets Manager `GetSecretValue` API 操作请求访问待删除的密钥时收到通知，您必须创建 CloudWatch 警报并配置通知。

创建 CloudWatch 警报

1. 登录 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在顶部导航栏上，选择要监控密钥的 AWS 区域。
3. 在左侧导航窗格中，选择 Logs。
4. 在日志组列表中，选中您在上一个过程中创建的日志组旁边的复选框，例如 CloudTrail/MyCloudWatchLogGroup。选择创建指标筛选器。
5. 对于筛选模式，键入或粘贴以下内容：

   ```
   { $.eventName = "GetSecretValue" && $.errorMessage = "*secret because it was marked
    for deletion*" }
   ```

   选择 Assign Metric (分配指标)。
6. 在 Create Metric Filter and Assign a Metric 页面上，执行以下操作：

   a. 对于 Metric Namespace (指标命名空间)，键入 **CloudTrailLogMetrics**。

   b. 对于 Metric Name（指标名称），键入 **AttemptsToAccessDeletedSecrets**。

   c. 选择显示高级指标设置，如有必要，再为 Metric Value (指标值) 键入 **1**。

   d. 选择 Create Filter。
7. 在筛选器框中，选择 Create Alarm。
8. 在 Create Alarm 窗口中，执行以下操作：

   a. 对于名称，键入 **AttemptsToAccessDeletedSecretsAlarm**。

   b. 在 Whenever: (每当:) 下，为 is: (是:) 选择 **>=** 并键入 **1**。

c. 在 Send notification to: 旁，执行以下操作之一：

- 要创建并使用新的 Amazon SNS 主题，请选择新建列表，然后键入新主题的名称。对于 Email list:，键入至少一个电子邮件地址。您可以键入多个电子邮件地址，并使用逗号将它们隔开。
- 要使用现有 Amazon SNS 主题，请选择要使用的主题的名称。如果列表不存在，请选择 Select list (选择列表)。

d. 选择创建警报。

步骤 3：测试 CloudWatch警报

要测试告警，请创建密钥，并计划将其删除。然后，尝试检索密钥值。您在告警中配置的地址很快会收到一封电子邮件。它提醒您注意计划删除的密钥的使用情况。

使用以下方法监控 AWS Secrets Manager 密钥的合规性 AWS Config

您可以使用 AWS Config 来评估您的密钥，以查看它们是否符合您的标准。您可以使用 AWS Config 规则定义对机密的内部安全和合规性要求。然后 AWS Config 可以识别不符合你规则的秘密。您还可以跟踪机密元数据、轮换配置、用于秘密加密的 KMS 密钥、Lambda 轮换函数以及与密钥关联的标签的更改。

您可以配置 AWS Config 为将更改通知您。有关更多信息，请参阅AWS Config 发送至 Amazon SNS 主题的通知。

如果您的组织中有多个 AWS 账户 密钥，则可以聚合该配置和合规性数据。 AWS 区域 有关更多信息，请参阅多账户多区域数据聚合。

评估机密是否合规

- 按照使用AWS Config 规则评估资源中的说明进行操作，然后选择以下规则之一：
  - `secretsmanager-secret-unused` — 检查是否已在指定的天数内访问了密钥。
  - `secretsmanager-using-cmk`— 检查密钥是否使用您在中创建的客户托管密钥 AWS 托管式密钥 `aws/secretsmanager`或客户管理的密钥进行加密 AWS KMS。
  - `secretsmanager-rotation-enabled-check` — 检查是否为存储在 Secrets Manager 中的密钥配置了轮换。

- secretsmanager-scheduled-rotation-success-check— 检查上次成功的轮换是否在配置的轮换频率内。检查的最低频率为每天。
- secretsmanager-secret-periodic-rotation — 检查是否已在指定的天数内轮换了密钥。

监控 Secrets Manager 成本

您可以使用 Amazon CloudWatch 来监控预估 AWS Secrets Manager 费用。有关更多信息，请参阅CloudWatch 用户指南中的创建账单警报以监控您的预估 AWS 费用。

监控成本的另一种选择是 AWS 成本异常检测。有关更多信息，请参阅《成本管理用户指南》中的使用 AWS 成本异常检测检测异常支出。AWS

有关监控 Secrets Manager 使用情况的信息，请参阅the section called “使用监视器 CloudWatch”和the section called “使用以下方式登录 AWS CloudTrail ”。

有关 AWS Secrets Manager 定价的信息，请参阅the section called “定价”。

合规性验证 AWS Secrets Manager

您在使用 Secrets Manager 时的合规责任取决于您的数据的敏感度、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全性与合规性快速入门指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS上部署基于安全性和合规性的基准环境的步骤。
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了公司如何使用来 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS Config 会评估资源配置符合内部实践、行业指南和法规的情况。有关更多信息，请参阅 the section called “监控密钥的合规性”。
- AWS Security Hub提供了您的安全状态的全面视图 AWS ，可帮助您检查是否符合安全行业标准和最佳实践。有关使用 Security Hub 评估 Secrets Manager 资源的信息，请参阅《AWS Security Hub 用户指南》中的 AWS Secrets Manager 控件。
- IAM Access Analyzer 会分析允许外部实体访问密钥的策略，包括策略中的条件语句。有关更多信息，请参阅使用 Access Analyzer 预览访问权限。
- AWS Systems Manager 为 Secrets Manager 提供了预定义的运行手册。有关更多信息，请参阅适用于 Secrets Manager 的 Systems Manager 自动化运行手册参考。
- 您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

合规标准

AWS Secrets Manager 已经过以下标准的审计，当您需要获得合规性认证时，可以成为您的解决方案的一部分。

- HIPAA — AWS 已扩大其《健康保险流通与责任法案》（ HIPAA ）合规计划，将其列 AWS Secrets Manager 为符合HIPAA资格的服务。如果您与签订了商业伙伴协议 (BAA) AWS，则可以使用 Secrets Manager 来帮助构建符合 HIPAA 标准的应用程序。 AWS 为有兴趣进一步了解如何利用健康信息处理和存储的客户提供了一份以 HIPAA AWS 为重点的白皮书。有关更多信息，请参阅 HIPAA 合规性。
- PIC 参与组织 — AWS Secrets Manager 拥有服务提供商级别 1 的支付卡行业 (PCI) 数据安全标准 (DSS) 3.2 版合规认证。使用 AWS 产品和服务存储、处理或传输持卡人数据的客户可以在管理自己

的 PCI DSS 合规性认证时使用 AWS Secrets Manager 。有关 PCI DSS 的更多信息，包括如何申请 PCI Compliance Package 的副本，请参阅 AWS PCI DSS 第 1 级。

- ISO — AWS Secrets Manager 已成功完成 ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 和 ISO 9001 的合规认证。有关更多信息，请参阅 ISO 27001、ISO 27017、ISO 27018、ISO 9001。
- AICPA SOC — 系统和组织控制 (SOC) 报告是独立的第三方检查报告，展示了 Secrets Manager 如何实现关键合规控制和目标。这些报告的目的是帮助您和您的审计师了解为支持运营和合规而建立的 AWS 控制措施。有关更多信息，请参阅 SOC 合规性。
- Fed RAMP — 联邦风险和授权管理计划 (FedRAMP) 是一项政府范围的计划，为云产品和服务的安全评估、授权和持续监控提供标准化方法。FedRAMP计划还为东西方 GovCloud 服务和地区以及使用政府或监管数据提供了临时授权。有关更多信息，请参阅 FedRAMP 合规性。
- 国防部 — 国防部 (DoD) 云计算安全要求指南 (SRG) 为云服务提供商 (CSP) 提供了标准化的评估和授权流程，以获得国防部的临时授权，以便他们能够为国防部客户提供服务。有关更多信息，请参阅 DoD SRG 资源。
- IRAP — 信息安全注册评估员计划 (IRAP) 使澳大利亚政府客户能够验证适当的控制措施是否到位，并确定适当的责任模式，以满足澳大利亚网络安全中心 (ACSC) 编写的《澳大利亚政府信息安全手册》(ISM) 的要求。有关更多信息，请参阅 IRAP 资源。
- OSPAR — Amazon Web Services (AWS) 获得了外包服务提供商的审计报告 (OSPAR) 认证。 AWS 与新加坡银行协会（ABS）的《外包服务提供商控制目标和程序指南》（ABS 指南）保持一致，这向客户表明了他们 AWS 致力于满足新加坡金融服务行业对云服务提供商设定的高期望。有关更多信息，请参阅 OSPAR 资源。

AWS Secrets Manager 中的安全性

AWS 非常重视安全性。作为 AWS 客户，您会从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

您和 AWS 共担安全责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 AWS Secrets Manager 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 – 您的 AWS 服务决定您的责任。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

有关更多资源，请参阅安全性支柱-AWS Well-Architected 框架。

主题

降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险

使用 AWS Command Line Interface (AWS CLI) 调用 AWS 操作时，您会在命令 Shell 中输入这些命令。例如，您可以使用 Windows 命令提示符或 Windows PowerShell，或者 Bash 或 Z Shell，或者其他类型。其中的很多命令 Shell 包含旨在提高工作效率的功能。但其他人可能会使用该功能窃取您的密钥。例如，在大多数 Shell 中，您可以使用上箭头键查看最后输入的命令。访问不受保护的会话的任何人可能会利用命令历史记录功能。另外，在后台工作的其他实用程序可能有权访问您的命令参数，这些参数旨在帮助您更高效地执行任务。为了减轻此类风险，请确保执行以下步骤：

- 在离开计算机前始终记得锁定计算机。
- 卸载或禁用不需要或不再使用的控制台实用程序。
- 确保 Shell 或远程访问程序（如果您在使用其中之一）不会记录键入的命令。

- 使用一些方法传递 Shell 命令历史记录未捕获的参数。以下示例说明了如何在文本文件中键入密钥文本，然后将该文件传递给 AWS Secrets Manager 命令并立即销毁文件。这意味着典型的 Shell 历史记录不会捕获密钥文本。

  以下示例显示典型的 Linux 命令（但您的 shell 可能需要稍有不同的命令）：

```
$ touch secret.txt
        # Creates an empty text file
$ chmod go-rx secret.txt
        # Restricts access to the file to only the user
$ cat > secret.txt
        # Redirects standard input (STDIN) to the text file
ThisIsMyTopSecretPassword^D
        # Everything the user types from this point up to the CTRL-D (^D) is saved in
 the file
$ aws secretsmanager create-secret --name TestSecret --secret-string file://
secret.txt       # The Secrets Manager command takes the --secret-string parameter
 from the contents of the file
$ shred -u secret.txt
        # The file is destroyed so it can no longer be accessed.
```

运行这些命令后，在使用向上和向下箭头滚动命令历史记录时就不会在任何一行中看到密钥文本。

> **Important**
>
> 默认情况下，不能在 Windows 中使用这类技术，除非您先将命令历史记录的缓冲区大小减小为 1。

将 Windows 命令提示符配置为 1 条命令只有 1 条命令的历史记录缓冲区

1. 以管理员身份打开命令提示符（以管理员身份运行）。
2. 选择左上角的图标，然后选择属性。
3. 在选项选项卡上，将缓冲区大小和缓冲区数均设置为 **1**，然后选择确定。
4. 每次您必须键入不希望保留在历史记录中的命令时，请在紧靠该命令后面键入另一条命令，例如：

   ```
   echo.
   ```

   这可以确保您刷新敏感命令。

对于 Windows 命令提示符 Shell，您可以下载 SysInternals SDelete 工具，然后使用类似下面的命令：

```
C:\> echo. 2> secret.txt
        # Creates an empty file
C:\> icacls secret.txt /remove "BUILTIN\Administrators" "NT AUTHORITY/SYSTEM" /
inheritance:r   # Restricts access to the file to only the owner
C:\> copy con secret.txt /y
        # Redirects the keyboard to text file, suppressing prompt to overwrite
THIS IS MY TOP SECRET PASSWORD^Z
      # Everything the user types from this point up to the CTRL-Z (^Z) is saved in the
 file
C:\> aws secretsmanager create-secret --name TestSecret --secret-string file://
secret.txt      # The Secrets Manager command takes the --secret-string parameter from
 the contents of the file
C:\> sdelete secret.txt
        # The file is destroyed so it can no longer be accessed.
```

AWS Secrets Manager 中的数据保护

AWS责任共担模式适用于 AWS Secrets Manager 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。Secrets 在所有区域支持 TLS 1.2 和 1.3。Secrets Manager 还支持对传输层安全（TLS）网络加密协议使用混合后量子密钥交换选项（PQTLS）。
- 使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对以编程方式向 Secrets Manager 发出的请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。请参阅the section called “使用以下方式登录 AWS CloudTrail ”。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。请参阅the section called “Secrets Manager 端点”。

- 如果使用 AWS CLI 访问 Secrets Manager，the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

静态加密

Secrets Manager 使用通过 AWS Key Management Service (AWS KMS) 来保护静态数据的机密性。AWS KMS 提供由许多 AWS 服务使用的密钥存储和加密服务。Secrets Manager 中的每个密钥都使用唯一的数据密钥加密。每个数据密钥都由一个 KMS 密钥保护。您可以选择对账户使用 Secrets Manager AWS 托管式密钥 的默认加密，也可以在 AWS KMS 中创建自己的客户托管密钥。使用客户托管密钥可让您对 KMS 密钥活动进行更精细的授权控制。有关更多信息，请参阅the section called “密钥加密和解密”。

传输中加密

Secrets Manager 为传输中的加密数据提供安全的私有终端节点。通过安全的私有终端节点，AWS 可以保护向 Secrets Manager 发出的 API 请求的完整性。AWS 要求调用方使用 X.509 证书和/或 Secrets Manager 秘密访问密钥对 API 调用进行签名。签名版本 4 签名流程 (Sigv4) 中阐述了此要求。

如果您将 AWS Command Line Interface (AWS CLI) 或任何 AWS SDK 要调用 AWS 中，您可以配置要使用的访问密钥。然后，这些工具会自动使用访问密钥为您签署请求。请参阅the section called “降低使用 AWS CLI 存储 AWS Secrets Manager 密钥的风险”。

互联网络流量隐私

AWS 提供了多个用于在通过已知的私有网络路由来路由流量时维护隐私的选项。

服务与本地客户端和应用之间的流量

在您的私有网络和 AWS Secrets Manager 之间有两个连接选项：

- 一个 AWS Site-to-Site VPN连接。有关更多信息，请参阅什么是 AWS Site-to-Site VPN？
- AWS Direct Connect 连接。有关更多信息，请参阅什么是 AWS Direct Connect？

同一区域中 AWS 资源之间的流量

如果要保护 Secrets Manager 和 AWS 中的 API 客户端之间的流量，请设置一个 AWS PrivateLink 以私下访问 Secrets Manager API 端点。

加密密钥管理

当 Secrets Manager 需要加密受保护密钥数据的新版本，Secrets Manager 会将请求发送到 AWS KMS 在 KMS 密钥生成新的数据密钥。Secrets Manager 使用此数据密钥进行信封加密。Secrets Manager 将加密的数据密钥与加密的密钥储存在一起。密钥需要解密时，Secrets Manager 会询问 AWS KMS 来解密数据密钥。然后，Secrets Manager 使用解密的数据密钥来解密加密的密钥。Secrets Manager 从不以未加密的形式存储数据密钥，并尽快从内存中删除密钥。有关更多信息，请参阅the section called “密钥加密和解密”。

中的秘密加密和解密 AWS Secrets Manager

Secrets Manager 使用带有 AWS KMS 密钥和数据密钥的信封加密来保护每个密钥值。每当密钥中的密钥值发生变化时，Secrets Manager 都会向其请求一个新的数据密钥 AWS KMS 来保护它。然后，用 KMS 密钥加密数据密钥，存储在密钥元数据中。要解密密密钥，Secrets Manager 首先使用中的 KMS 密钥对加密的数据密钥进行解密。 AWS KMS

Secrets Manager 不使用 KMS 直接对密钥值加密。相反，它使用 KMS 密钥来生成和加密 256 位高级加密标准 (AES) 对称数据密钥，并使用数据密钥对密钥值加密。Secrets Manager 使用纯文本数据密钥对外部的密钥值进行加密 AWS KMS，然后将其从内存中删除。它将数据密钥的加密副本存储在密钥的元数据中。

主题

- 选择一把 AWS KMS 钥匙
- 什么是加密？
- 加密和解密流程
- KMS 密钥的权限
- Secrets Manager 如何使用您的 KMS 密钥
- AWS 托管式密钥 (aws/secretsmanager) 的密钥策略
- Secrets Manager 加密上下文
- 监控 Secrets Manager 的互动 AWS KMS

选择一把 AWS KMS 钥匙

创建密钥时，您可以选择 AWS 账户 和区域中的任何对称加密客户托管密钥，也可以使用 for Secrets Manager (`aws/secretsmanager`)。 AWS 托管式密钥 如果你选择但它还不存在 AWS 托管式密钥

aws/secretsmanager，则 Secrets Manager 会创建它并将其与密钥关联。可对您账户中的每个密钥使用相同的 KMS 密钥或不同的 KMS 密钥。您可能希望使用不同的 KMS 密钥为一组密钥设置密钥的自定义权限，或者如果您希望审计这些密钥的特定操作。Secrets Manager 仅支持对称加密 KMS 密钥。如果您在外部密钥存储中使用 KMS 密钥，则对 KMS 密钥的加密操作可能需要更长时间，而且可靠性和持久性会降低，因为请求必须在 AWS外部传输。

有关更改秘密的加密密钥的信息，请参阅 the section called “更改秘密的加密密钥”。

当您更改加密密钥时，Secrets Manager 会使用新密钥重新加密AWSCURRENTAWSPENDING、和AWSPREVIOUS版本。为了避免将您锁定在密钥之外，Secrets Manager 会使用以前的密钥对所有现有版本进行加密。这意味着您可以使用先前的密钥或新密钥解密AWSCURRENTAWSPENDING、和AWSPREVIOUS版本。

要使其AWSCURRENT只能通过新的加密密钥解密，请使用新密钥创建新版本的密钥。然后，为了能够解AWSCURRENT密密密钥的版本，您必须拥有新密钥的权限。

您可以拒绝访问权限， AWS 托管式密钥 aws/secretsmanager并要求使用客户托管密钥对机密进行加密。有关更多信息，请参阅 the section called “示例：拒绝使用特定 AWS KMS 密钥来加密机密”。

要查找与密钥关联的 KMS 密钥，请在控制台中查看密钥或致电ListSecrets或DescribeSecret。当密钥与 for Secrets Manager (aws/secretsmanager) 关联时，这些操作不会返回 KMS 密钥标识符。AWS 托管式密钥

什么是加密？

Secrets Manager 会加密密钥值，但不对以下项进行加密：

- 密钥名称和描述
- 轮换设置
- 与密钥关联的 KMS 密钥 ARN
- 任何附带的 AWS 标签

加密和解密流程

为了对密钥中的密钥值加密，Secrets Manager 使用以下过程。

1. Secrets Manager 使用密钥的 KMS 密钥的 ID 调用该 AWS KMS GenerateDataKey操作，并请求提供 256 位 AES 对称密钥。 AWS KMS 返回一个纯文本数据密钥和使用 KMS 密钥加密的该数据密钥的副本。

2. Secrets Manager 使用纯文本数据密钥和高级加密标准 (AES) 算法对外部的密钥值进行加密。 AWS KMS然后，它将尽快从内存中删除明文密钥。
3. Secrets Manager 将加密的数据密钥存储在密钥的元数据中，使其可用于解密密钥值。但是，任何一个 Secrets Manager API 均不会返回加密的密钥或加密的数据密钥。

对已加密的密钥值解密：

1. Secrets Manager 调用 AWS KMS 解密操作并传入加密的数据密钥。
2. AWS KMS 使用密钥的 KMS 密钥来解密数据密钥。它将返回明文数据密钥。
3. Secrets Manager 使用该明文数据密钥来解密密钥值。然后，它会尽快从内存中删除数据密钥。

KMS 密钥的权限

当 Secrets Manager 在加密操作中使用 KMS 密钥时，它会代表创建或更新密钥值的用户执行操作。您可以在 IAM policy 或密钥政策中提供这些权限。以下 Secrets Manager 操作需要 AWS KMS 权限。

- CreateSecret
- GetSecretValue
- PutSecretValue
- UpdateSecret
- ReplicateSecretToRegions

要允许 KMS 密钥仅用于源自 Secrets Manager 的请求，可以在权限策略中使用带有`secretsmanager.<Region>.amazonaws.com`值的 k m ViaService s: 条件密钥。

您还可以在加密上下文中将密钥或值用作将 KMS 密钥用于加密操作的条件。例如，可在 IAM 或密钥策略文档中使用字符串条件运算符，或在授权中使用授权约束。KMS 密钥授权传播可能需要长达五分钟的时间。有关更多信息，请参阅CreateGrant。

Secrets Manager 如何使用您的 KMS 密钥

Secrets Manager 使用你的 KMS 密钥调用以下 AWS KMS 操作。

GenerateDataKey

Secrets Manager 调用该 AWS KMS GenerateDataKey操作是为了响应以下 Secrets Manager 操作。

- CreateSecret— 如果新密钥包含密钥值，则 Secrets Manager 会请求新的数据密钥对其进行加密。
- PutSecretValue— Secrets Manager 请求新的数据密钥来加密指定的密钥值。
- ReplicateSecretToRegions— 要加密复制的密钥，Secrets Manager 在副本区域中请求一个 KMS 密钥的数据密钥。
- UpdateSecret— 如果您更改了密钥值或 KMS 密钥，Secrets Manager 会请求新的数据密钥来加密新的密钥值。

该RotateSecret操作不会调用GenerateDataKey，因为它不会更改密钥值。但是，如果 RotateSecret 调用更改了秘密值的 Lambda 轮换函数，则其调用 PutSecretValue 操作时将触发 GenerateDataKey 请求。

Decrypt

Secrets Manager 调用 Decrypt 操作来响应以下 Secrets Manager 操作。

- GetSecretValue和 BatchGetSecretValue— Secrets Manager 在将密钥值返回给调用者之前对其进行解密。要解密加密的密钥值，Secrets Manager 会调用 AWS KMS Decrypt 操作来解密密密钥中的加密数据密钥。然后，它使用明文数据密钥来对已加密密钥值解密。对于批处理命令，Secrets Manager 可以重复使用解密后的密钥，因此并非所有调用都会产生 Decrypt 请求。
- PutSecretValue和 UpdateSecret— 大多数 PutSecretValue UpdateSecret and 请求不会触发Decrypt操作。但是，当 PutSecretValue 或 UpdateSecret 请求尝试更改现有密钥版本中的密钥值时，Secrets Manager 将对现有密钥值解密并将其与请求中的密钥值比较，以确认两者是否相同。此操作可确保 Secrets Manager 操作为幂等操作。要解密加密的密钥值，Secrets Manager 会调用 AWS KMS Decrypt 操作来解密密密钥中的加密数据密钥。然后，它使用明文数据密钥来对已加密密钥值解密。
- ReplicateSecretToRegions— Secrets Manager 首先解密主区域中的密钥值，然后在副本区域中使用 KMS 密钥重新加密密钥值。

Encrypt

Secrets Manager 调用 Encrypt 操作来响应以下 Secrets Manager 操作：

- UpdateSecret— 如果您更改 KMS 密钥，Secrets Manager 会使用新密钥重新加密保护AWSCURRENTAWSPREVIOUS、和AWSPENDING机密版本的数据密钥。
- ReplicateSecretToRegions— Secrets Manager 在复制过程中使用副本区域中的 KMS 密钥对数据密钥进行重新加密。

DescribeKey

当你在 Secrets Manager 控制台中创建或编辑密钥时，Secrets Manager 调用该DescribeKey操作来确定是列出 KMS 密钥。

验证对 KMS 密钥的访问

当您建立或更改与密钥关联的 KMS 密钥时，Secrets Manager 将用指定的 KMS 调用 `GenerateDataKey` 和 `Decrypt` 操作。这些调用确认调用方是否有权将该 KMS 密钥用于这些操作。Secrets Manager 将放弃这些操作的结果；它不在任何加密操作中使用这些结果。

您可以识别这些验证调用，因为这些请求中 `SecretVersionId` 密钥加密上下文的值为 `RequestToValidateKeyAccess`。

> **Note**
>
> 过去，Secrets Manager 验证调用不包含加密上下文。您可能会在较早的 AWS CloudTrail 日志中发现没有加密上下文的呼叫。

AWS 托管式密钥 (`aws/secretsmanager`) 的密钥策略

仅当 Secrets Manager 代表用户发出请求时，for Secrets Manager (`aws/secretsmanager`) 的密钥策略才允许用户使用 KMS 密钥进行指定操作。 AWS 托管式密钥 密钥策略不允许任何用户直接使用 KMS 密钥。

此密钥策略与所有 AWS 托管式密钥 策略类似，均由该服务来建立。您无法更改密钥策略，但可以随时查看。有关详细信息，请参阅查看密钥策略。

密钥策略中的策略语句具有以下影响：

- 仅当 Secrets Manager 代表账户中的用户发出请求时，才允许这些用户使用 KMS 密钥执行加密操作。`kms:ViaService` 条件密钥可强制实施此限制。
- 允许该 AWS 账户创建 IAM 策略，允许用户查看 KMS 密钥属性和撤消授权。
- 尽管 Secrets Manager 不使用授权来获取 KMS 密钥的访问权限，但该策略还允许 Secrets Manager 代表用户创建 KMS 密钥授权，并允许帐户撤销任何允许 Secrets Manager 使用 KMS 密钥的授权。这些是 AWS 托管式密钥的策略文档的标准元素。

以下是 Secrets Manager 示例 AWS 托管式密钥 的关键策略。

```
{
  "Id": "auto-secretsmanager-2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow access through AWS Secrets Manager for all principals in the
 account that are authorized to use AWS Secrets Manager",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "111122223333",
          "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "Allow access through AWS Secrets Manager for all principals in the
 account that are authorized to use AWS Secrets Manager",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": "kms:GenerateDataKey*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "111122223333"
        },
```

```
        "StringLike": {
          "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "Allow direct access to key metadata to the account",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
      ],
      "Resource": "*"
    }
  ]
}
```

Secrets Manager 加密上下文

加密上下文 是一组包含任意非机密数据的键值对。当您在加密数据的请求中包含加密上下文时，会以加密 AWS KMS 方式将加密上下文绑定到加密数据。要解密数据，您必须传入相同的加密上下文。

在对的请求GenerateDataKey和解密请求中 AWS KMS，Secrets Manager 使用具有两个名称-值对的加密上下文，用于标识密钥及其版本，如以下示例所示。名称不会变化，但与其组合的加密上下文会因每个密钥值而异。

```
"encryptionContext": {
    "SecretARN": "arn:aws:secretsmanager:us-east-2:111122223333:secret:test-secret-
a1b2c3",
    "SecretVersionId": "EXAMPLE1-90ab-cdef-fedc-ba987SECRET1"
}
```

您可以使用加密上下文在审计记录和日志（例如和 Amazon CloudWatch Logs）中识别这些加密操作，并作为策略和授权中的授权条件。AWS CloudTrail

Secrets Manager 加密上下文包含两个名称–值对。

- SecretARN – 第一个名称–值对标识密钥。键是 SecretARN。该值是密钥的 Amazon Resource Name (ARN)。

  ```
  "SecretARN": "ARN of an Secrets Manager secret"
  ```

  例如，如果密钥的 ARN 是 arn:aws:secretsmanager:us-east-2:111122223333:secret:test-secret-a1b2c3，加密上下文将包括以下对。

  ```
  "SecretARN": "arn:aws:secretsmanager:us-east-2:111122223333:secret:test-secret-a1b2c3"
  ```

- SecretVersionId— 第二个名称-值对标识密钥的版本。键是 SecretVersionId。该值为版本 ID。

  ```
  "SecretVersionId": "<version-id>"
  ```

  例如，如果密钥的版本 ID 是 EXAMPLE1-90ab-cdef-fedc-ba987SECRET1，加密上下文将包括以下对。

  ```
  "SecretVersionId": "EXAMPLE1-90ab-cdef-fedc-ba987SECRET1"
  ```

当您建立或更改密钥的 KMS 密钥时，Secrets Manager 会向发送GenerateDataKey和解密请求，AWS KMS 以验证调用者是否有权使用 KMS 密钥进行这些操作。它将放弃响应，并且不对密钥值使用这些响应。

在这些验证请求中，SecretARN 的值是密钥的实际 ARN，但 SecretVersionId 值为 RequestToValidateKeyAccess，如以下加密上下文示例中所示。此特殊值可帮助您在日志和审核跟踪中标识验证请求。

```
"encryptionContext": {
    "SecretARN": "arn:aws:secretsmanager:us-east-2:111122223333:secret:test-secret-a1b2c3",
    "SecretVersionId": "RequestToValidateKeyAccess"
}
```

> **Note**
>
> 在过去，Secrets Manager 验证请求不包含加密上下文。您可能会在较早的 AWS CloudTrail 日志中发现没有加密上下文的呼叫。

监控 Secrets Manager 的互动 AWS KMS

您可以使用 AWS CloudTrail 和 Amazon CloudWatch Logs 来跟踪 Secrets Manager AWS KMS 代表您发送的请求。有关监测密钥使用的更多信息，请参阅 监控密钥。

GenerateDataKey

当您在密钥中创建或更改密钥值时，Secrets Manager 会向发送一个GenerateDataKey请求 AWS KMS ，为该密钥指定 KMS 密钥。

记录 `GenerateDataKey` 操作的事件与以下示例事件类似。该请求由 `secretsmanager.amazonaws.com` 调用。参数包括密钥的 KMS 密钥的 Amazon Resource Name (ARN)、需要 256 位密钥的密钥说明符以及标识密钥和版本的加密上下文。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AROAIGDTESTANDEXAMPLE:user01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/user01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-05-31T23:23:41Z"
            }
        },
        "invokedBy": "secretsmanager.amazonaws.com"
    },
    "eventTime": "2018-05-31T23:23:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "secretsmanager.amazonaws.com",
    "userAgent": "secretsmanager.amazonaws.com",
```

```
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "keySpec": "AES_256",
        "encryptionContext": {
            "SecretARN": "arn:aws:secretsmanager:us-east-2:111122223333:secret:test-
secret-a1b2c3",
            "SecretVersionId": "EXAMPLE1-90ab-cdef-fedc-ba987SECRET1"
        }
    },
    "responseElements": null,
    "requestID": "a7d4dd6f-6529-11e8-9881-67744a270888",
    "eventID": "af7476b6-62d7-42c2-bc02-5ce86c21ed36",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Decrypt

当您获取或更改密钥的密钥值时，Secrets Manager 会向发送解密请求 AWS KMS 以解密加密的数据密钥。对于批处理命令，Secrets Manager 可以重复使用解密后的密钥，因此并非所有调用都会产生 `Decrypt` 请求。

记录 `Decrypt` 操作的事件与以下示例事件类似。用户是您 AWS 账户中访问表格的委托人。这些参数包括加密的表密钥（作为密文 blob）以及标识表和账户的加密上下文。 AWS AWS KMS 从密文中获取 KMS 密钥的 ID。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AROAIGDTESTANDEXAMPLE:user01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/user01",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-05-31T23:36:09Z"
            }
        },
        "invokedBy": "secretsmanager.amazonaws.com"
    },
    "eventTime": "2018-05-31T23:36:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "secretsmanager.amazonaws.com",
    "userAgent": "secretsmanager.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "SecretARN": "arn:aws:secretsmanager:us-east-2:111122223333:secret:test-
secret-a1b2c3",
            "SecretVersionId": "EXAMPLE1-90ab-cdef-fedc-ba987SECRET1"
        }
    },
    "responseElements": null,
    "requestID": "658c6a08-652b-11e8-a6d4-ffee2046048a",
    "eventID": "f333ec5c-7fc1-46b1-b985-cbda13719611",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Encrypt

当您更改与密钥关联的 KMS 密钥时，Secrets Manager 会向发送加密请求，要求使用新密钥重新加AWSPENDING密AWSCURRENTAWSPREVIOUS、和密钥版本。 AWS KMS 当您将密钥复制到另一个区域时，Secrets Manager 还会向 AWS KMS 发送 Encrypt 请求。

记录 Encrypt 操作的事件与以下示例事件类似。用户是您 AWS 账户中访问表格的委托人。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AROAIGDTESTANDEXAMPLE:user01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/user01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-06-09T18:11:34Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "secretsmanager.amazonaws.com"
    },
    "eventTime": "2023-06-09T18:11:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "secretsmanager.amazonaws.com",
    "userAgent": "secretsmanager.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-east-2:111122223333:key/EXAMPLE1-f1c8-4dce-8777-
aa071ddefdcc",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "SecretARN": "arn:aws:secretsmanager:us-
east-2:111122223333:secret:ChangeKeyTest-5yKnKS",
            "SecretVersionId": "EXAMPLE1-5c55-4d7c-9277-1b79a5e8bc50"
        }
    },
    "responseElements": null,
    "requestID": "129bd54c-1975-4c00-9b03-f79f90e61d60",
    "eventID": "f7d9ff39-15ab-47d8-b94c-56586de4ab68",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/EXAMPLE1-f1c8-4dce-8777-
aa071ddefdcc"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

AWS Secrets Manager 中的基础设施安全性

作为一项托管式服务，AWS Secrets Manager 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

通过网络访问 Secrets Manager 是通过 AWS 使用 TLS 发布的 API 进行的。Secrets Manager API 可以从任何网络位置调用。然而，Secrets Manager 支持基于资源的访问策略，其中可以包含基于源 IP 地址的限制。您还可以使用 Secrets Manager 资源策略来控制来自特定虚拟私有云（VPC）端点或特定 VPC 的密钥访问。实际上，这隔离了 AWS 网络中仅从特定 VPC 到给定密钥的网络访问。有关更多信息，请参阅VPC 端点。

灵活性 AWS Secrets Manager

AWS 围绕 AWS 区域 可用区构建全球基础架构。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区可连接低延迟、高吞吐量和高度冗余的网络。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区为您提供了更高的可用性、容错功能和可扩展性。

有关弹性和灾难恢复的更多信息，请参阅可靠性支柱——Well-Architecte AWS d Framework。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

后量子 TLS

Secrets Manager 支持对传输层安全 (TLS) 网络加密协议使用混合后量子密钥交换选项。当您连接到 Secrets Manager API 终端节点时，可以使用此 TLS 选项。我们在标准化后量子算法之前提供了此功能，因此您可以开始测试这些密钥交换协议对 Secrets Manager 调用产生的影响。这些混合后量子密钥交换功能是可选的，至少与我们目前使用的 TLS 加密一样安全，并且有可能会提供额外的安全优势。不过，与目前使用的传统密钥交换协议相比，它们会影响延迟和吞吐量性能。

为了保护今天加密的数据，让这些数据在未来免受可能的攻击，AWS 正在积极参与密码社区，一起开发抗量子密码算法或后量子算法。我们已经在 Secrets Manager 端点中实施了混合后量子密钥交换密码套件。这些混合密码套件将传统加密算法与后量子算法相结合，可确保 TLS 连接至少与传统密码套件一样强大。不过，由于混合密码套件的性能特征及带宽要求与传统密钥交换机制的性能特征及带宽要求有所不同，我们建议您针对 API 调用开展测试。

Secrets Manager 在除中国区域之外的所有区域都支持 PQTLS。

配置混合后量子 TLS

1. 将 AWS 公共运行时客户端添加到您的 Maven 依赖项中。我们建议您使用最新可用版本。例如，以下语句将添加版本 2.20.0。

```
<dependency>
  <groupId>software.amazon.awssdk</groupId>
  <artifactId>aws-crt-client</artifactId>
  <version>2.20.0</version>
</dependency>
```

2. 将 AWS SDK for Java 2.x 添加到项目并对其进行初始化。在 HTTP 客户端上启用混合后量子密码套件。

```
SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
            .postQuantumTlsEnabled(true)
            .build();
```

3. 创建 Secrets Manager 异步客户端。

```
SecretsManagerAsyncClient SecretsManagerAsync = SecretsManagerAsyncClient.builder()
            .httpClient(awsCrtHttpClient)
            .build();
```

   现在，当您调用 Secrets Manager API 操作时，您的调用将通过混合后量子 TLS 传输到 Secrets Manager 端点。

有关使用混合后量子 TLS 的更多信息，请参阅：

- AWS SDK for Java 2.x 开发人员指南和AWS SDK for Java 2.x 已发布博客帖子。
- s2n-tls 简介，新的开源 TLS 实施和使用 s2n-tls。
- 美国国家标准和技术研究院 (NIST) 的后量子密码学。

- 适合传输层安全 1.2 (TLS) 的混合后量子密钥封装方法 (PQ KEM)。

Secrets Manager 的后量子 TLS 在所有 AWS 区域 中都可用，但中国除外。

故障排除 AWS Secrets Manager

使用此处的信息可帮助您诊断和修复您在使用 Secrets Manager 时可能遇到的问题。

有关轮换的问题，请参阅 the section called “ 轮换问题排查”。

主题

“访问被拒绝” 消息

当你向 Secrets Manager 进行诸如 GetSecretValue 或 CreateSecret 之类的 API 调用时，你必须具有 IAM 权限才能进行该调用。当您使用控制台时，控制台会代表您进行相同的 API 调用，因此您还必须拥有 IAM 权限。管理员可以通过将 IAM 策略附加到您的 IAM 用户或您所属的群组来授予权限。如果授予这些权限的政策声明包含任何条件，例如 time-of-day 或 IP 地址限制，则您在发送请求时也必须满足这些要求。有关查看或修改适用于 IAM 用户、组或角色的策略的信息，请参阅《IAM 用户指南》中的使用策略。有关 Secrets Manager 所需权限的信息，请参阅 身份验证和访问控制。

如果您手动对 API 请求进行签名而不使用 AWS SDK，请确认您已正确对请求进行签名。

对于临时安全凭证的“拒绝访问”

请确认用于发出请求的 IAM 用户或角色具有正确的权限。临时安全凭证的权限来自于 IAM 用户或角色。这意味着，权限仅限于为 IAM 用户或角色授予的权限。有关临时安全凭证权限的确定方式的更多信息，请参阅 IAM 用户指南中的控制临时安全凭证的权限。

确认已正确对请求进行签名，并且请求格式正确无误。有关详细信息，请参阅所选软件开发工具包的工具包文档，或者 IAM 用户指南中的使用临时安全证书请求 AWS 资源访问权限。

验证您的临时安全凭证没有过期。有关更多信息，请参阅《IAM 用户指南》中的请求临时安全凭证。

有关 Secrets Manager 所需权限的信息，请参阅 身份验证和访问控制。

并非始终立即显示我所做的更改。

Secrets Manager 使用名为最终一致性的分布式计算模型。你在 Secrets Manager（或其他 AWS 服务）中所做的任何更改都需要一段时间才能从所有可能的端点中看见。它在服务器与服务器之间、复制区域与复制区域之间，以及全球的区域与区域之间发送数据需要时间，这会造成一定的延迟。Secrets Manager 也使用缓存来提高性能，但在某些情况下，这可能会增加时间。在之前缓存的数据超时之前，更改可能不可见。

在设计全球应用程序时应考虑到这些可能的延迟。此外，确保应用程序可以按预期工作，即使在一个位置进行的更改不能立即在其他位置可见。

有关最终一致性如何影响其他一些 AWS 服务的更多信息，请参阅：

- Amazon Redshift 数据库开发人员指南中的管理数据一致性
- Amazon Simple Storage Service 用户指南中的 Amazon S3 数据一致性模型
- AWS 大数据博客中的 Ensuring Consistency When Using Amazon S3 and Amazon EMR for ETL Workflows
- Amazon EC2 API 引用中的 Amazon EC2 最终一致性

在创建秘密时收到“Cannot generate a data key with an asymmetric KMS key”（无法使用非对称 KMS 密钥生成数据密钥）

Secrets Manager 使用与密钥关联的对称加密 KMS 密钥来为每个密钥值生成数据密钥。不能使用非对称 KMS 密钥。确认您使用的是对称加密 KMS 密钥，而不是非对称 KMS 密钥。有关说明，请参阅识别非对称 KMS 密钥。

AWS CLI 或 S AWS DK 操作无法从部分 ARN 中找到我的秘密

在许多情况下，Secrets Manager 可以从不完整的 ARN 中找到密钥，而无需完整的 ARN。但如果密钥名称以连字符后跟六个字符结尾，Secrets Manager 可能无法仅从一部分 ARN 中找到密钥。我们建议您改用完整的 ARN 或密钥名称。

更多详细信息

Secrets Manager 会在密钥名称末尾添加六个随机字符，以帮助确保密钥 ARN 的唯一性。如果删除了原始密钥，然后使用相同的名称创建了新密钥，则由于这些字符的原因，这两个密钥具有不同的 ARN。由于 ARN 不同，有权访问旧密钥的用户不会自动获得新密钥的访问权限。

Secrets Manager 可为密钥构建 ARN，其中包含区域、账户、密钥名称，后跟连字符和六个字符，如下所示：

```
arn:aws:secretsmanager:us-east-2:111122223333:secret:SecretName-abcdef
```

如果密钥名称以连字符和六个字符结尾，当您仅使用一部分 ARN 时，在 Secrets Manager 看来您似乎指定了完整的 ARN。例如，您可能具有一个名为 `MySecret-abcdef` 的密钥，其 ARN 如下：

```
arn:aws:secretsmanager:us-east-2:111122223333:secret:MySecret-abcdef-nutBrk
```

当您调用以下操作（此操作仅使用一部分密钥 ARN）时，Secrets Manager 可能会找不到密钥。

```
$ aws secretsmanager describe-secret --secret-id arn:aws:secretsmanager:us-
east-2:111122223333:secret:MySecret-abcdef
```

此密钥由 AWS 服务管理，您必须使用该服务对其进行更新。

如果您在尝试修改密钥时遇到此消息，则只能使用消息中列出的管理服务来更新密钥。有关更多信息，请参阅 托管密钥。

要确定谁管理密钥，您可以查看密钥名称。由其他服务管理的密钥以该服务的 ID 作为前缀。或者，在中 AWS CLI，调用 d escribe-secret，然后查看该字段。`OwningService`

AWS Secrets Manager 配额

Secrets Manager 读取 API 具有较高的 TPS 限额，而不常调用的控制面板 API 的 TPS 限额则较低。我们建议您避免以超过每 10 分钟一次的速率持续调用 `PutSecretValue` 或 `UpdateSecret`。如果调用 `PutSecretValue` 或 `UpdateSecret` 更新密钥值，Secrets Manager 将创建密钥的新版本。当版本超过 100 个时，Secrets Manager 会删除未标记的版本，但不会删除 24 小时内创建的版本。如果每 10 分钟更新一次密钥值，则创建的版本多于 Secrets Manager 删除的版本，将达到密钥版本的配额。

您可以在您的账户中运行多个区域，并且每个限额是特定于每个区域的。

当一个 AWS 账户 中的应用程序使用其他账户拥有的秘密时，这称为跨账户请求。对于跨账户请求，Secrets Manager 将限制发出请求的身份的账户，而不是拥有该秘密的账户。例如，如果账户 A 中的某一身份使用账户 B 中的某一秘密，则该秘密的使用将仅应用于账户 A 中的配额。

Secrets Manager 配额

名称	默认值	可调整	描述
DeleteResourcePolicy、GetResourcePolicy、PutResourcePolicy 和 ValidateResourcePolicy API 请求的组合速率	每个支持的区域：每秒 50 个	否	DeleteResourcePolicy、GetResourcePolicy、PutResourcePolicy 和 ValidateResourcePolicy API 请求组合的每秒最大事务数。
DescribeSecret 和 GetSecretValue API 请求的组合速率	每个支持的区域：每秒 1 万个	否	DescribeSecret 和 GetSecretValue API 请求组合的每秒最大事务数。
PutSecretValue、RemoveRegionsFromReplication、ReplicateSecretToRegion、StopReplicationToReplica、UpdateSecret 和	每个支持的区域：每秒 50 个	否	PutSecretValue、RemoveRegionsFromReplication、ReplicateSecretToRegion、StopReplicationToRepli

名称	默认值	可调整	描述
UpdateSecretVersionStage API 请求的组合速率			ca、UpdateSecret 和 UpdateSecretVersionStage API 请求组合的每秒最大事务数。
RestoreSecret API 请求的组合速率	每个支持的区域：每秒 50 个	否	RestoreSecret API 请求的每秒最大事务数。
RotateSecret 和 CancelRotateSecret API 请求的组合速率	每个支持的区域：每秒 50 个	否	RotateSecret 和 CancelRotateSecret API 请求组合的每秒最大事务数。
TagResource 和 UntagResource API 请求的组合速率	每个支持的区域：每秒 50 个	否	TagResource 和 UntagResource API 请求组合的每秒最大事务数。
BatchGetSecretValue API 请求的速率	每个支持的区域：每秒 100 个	否	BatchGetSecretValue API 请求的每秒最大事务数。
CreateSecret API 请求的速率	每个支持的区域：每秒 50 个	否	CreateSecret API 请求的每秒最大事务数。
DeleteSecret API 请求的速率	每个支持的区域：每秒 50 个	否	DeleteSecret API 请求的每秒最大事务数。
GetRandomPassword API 请求的速率	每个支持的区域：每秒 50 个	否	GetRandomPassword API 请求的每秒最大事务数。
ListSecretVersionIds API 请求的速率	每个支持的区域：每秒 50 个	否	ListSecretVersionIds API 请求的每秒最大事务数。
ListSecrets API 请求的速率	每个支持的区域：每秒 100 个	否	ListSecrets API 请求的每秒最大事务数。

名称	默认值	可调整	描述
基于资源的策略长度	每个支持的区域：2.048 万个	否	附加到秘密的基于资源的权限策略的最大字符数量。
秘密值大小	每个支持的区域：6.5536 万字节	否	加密秘密值的最大大小。如果秘密值是字符串，则它是该秘密值中允许的字符数。
密文	每个支持的区域：500 万个	否	此 AWS 账户的每个 AWS 区域中秘密的最大数量。
所有密钥版本中附上的标签数	每个支持的区域：20 个	否	秘密的所有版本附加的暂存标签的最大数量。
每个密钥的版本数	每个支持的区域：100 个	否	秘密的版本的最大数量。

将重试添加到您的应用程序

您的 AWS 客户端可能由于客户端存在意外问题而导致 Secrets Manager 调用失败。或者，调用可能由于 Secrets Manager 存在速率限制而失败。当您超过 API 请求配额时，Secrets Manager 会限制请求。它拒绝了一个原本有效的请求并返回 throttling 错误消息。对于两种失败，我们建议您在短暂的等待时间后重试呼叫。这被称为退避和重试策略。

如果您遇到以下错误，您可能需要将重试添加到您的应用程序代码：

瞬时错误和异常

- `RequestTimeout`
- `RequestTimeoutException`
- `PriorRequestNotComplete`
- `ConnectionError`

- HTTPClientError

服务端节流和限制错误与异常

- Throttling
- ThrottlingException
- ThrottledException
- RequestThrottledException
- TooManyRequestsException
- ProvisionedThroughputExceededException
- TransactionInProgressException
- RequestLimitExceeded
- BandwidthLimitExceeded
- LimitExceededException
- RequestThrottled
- SlowDown

有关重试、指数回退和抖动的详细信息以及示例代码，请参阅以下资源：

- 指数回退和抖动
- 超时、重试和回退并抖动
- AWS 中的错误重试和指数回退

文档历史记录

下表描述了自上次发布以来对文档所做的重要更改 AWS Secrets Manager。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
Secrets Manager 改为 AWS 托管策略	`SecretsManagerReadWrite` 托管策略现在包括`redshift-serverless` 权限。有关更多信息，请参阅以下内容的AWS 托管策略 AWS Secrets Manager	2024 年 3 月 12 日

早期更新

下表描述了 2024 年 2 月之前每个版本的《 AWS Secrets Manager 用户指南》中的重要更改。

更改	描述	日期
正式发布	这是 Secrets Manager 的首次公开发布。	2018年4月4日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。