AWS 凭据

Set up and administration

NetApp
April 01, 2022

目录

AWS 凭据

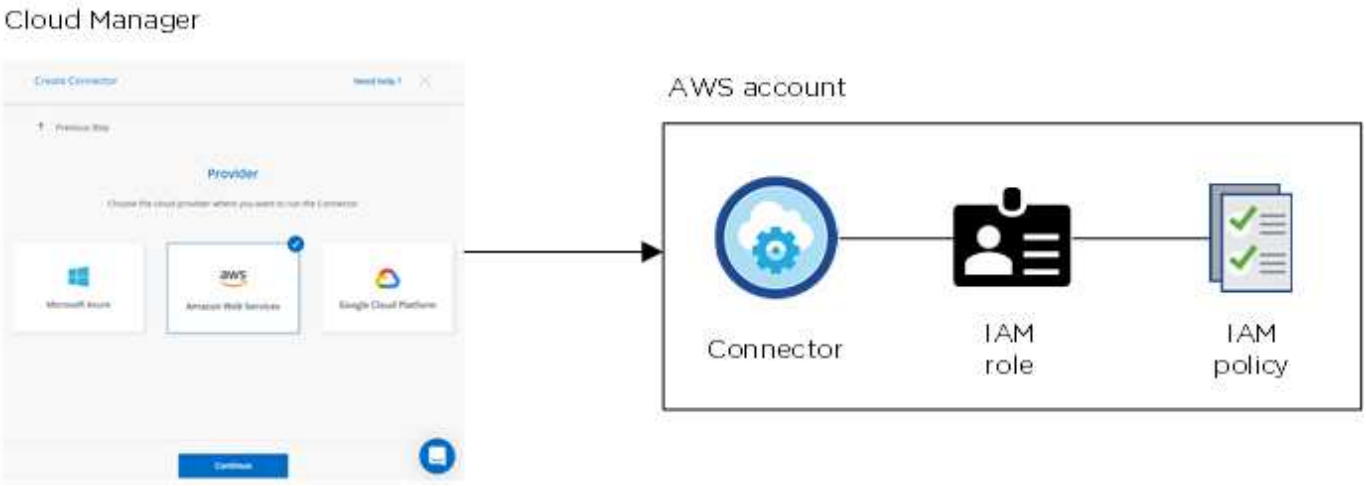
AWS 凭据和权限

通过 Cloud Manager ，您可以选择部署 Cloud Volumes ONTAP 时要使用的 AWS 凭据。您可以使用初始 AWS 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭据。

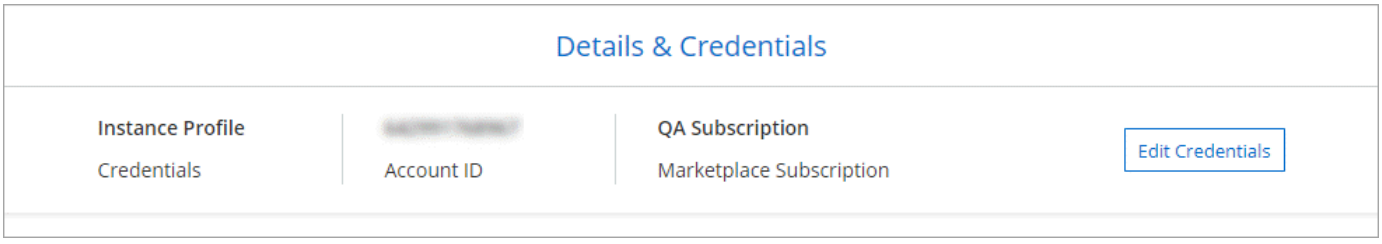
初始 AWS 凭据

从 Cloud Manager 部署 Connector 时，您需要使用有权启动 Connector 实例的 AWS 帐户。中列出了所需的权限 "AWS 的连接器部署策略"。

当 Cloud Manager 在 AWS 中启动 Connector 实例时，它会为此实例创建 IAM 角色和实例配置文件。它还会附加一个策略，为 Cloud Manager 提供管理该 AWS 帐户中资源和进程的权限。 "查看 Cloud Manager 如何使用权限"。

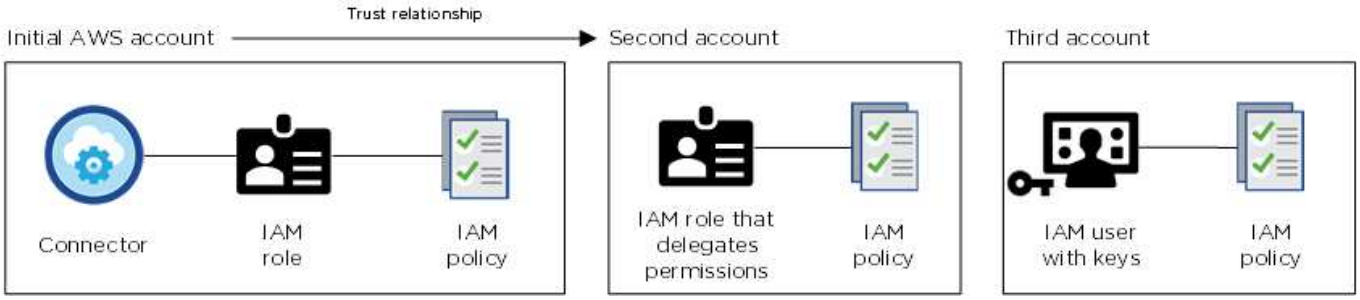


在为 Cloud Volumes ONTAP 创建新工作环境时， Cloud Manager 会默认选择以下 AWS 凭据：



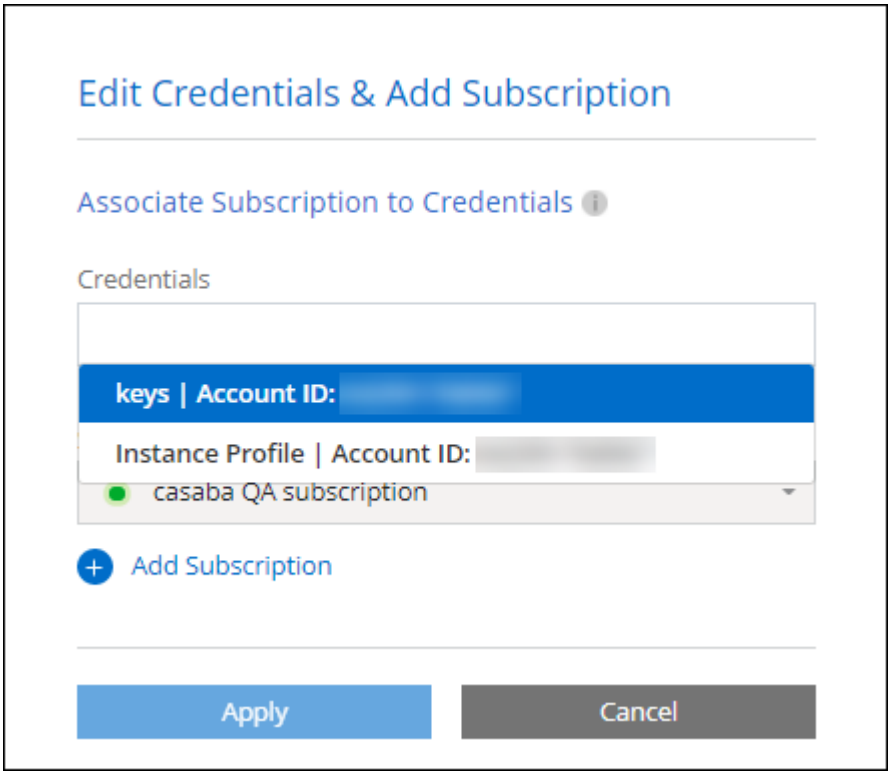
其他 AWS 凭据

如果您要在不同的 AWS 帐户中启动 Cloud Volumes ONTAP ，则可以选择一种 "为 IAM 用户或受信任帐户中某个角色的 ARN 提供 AWS 密钥"。下图显示了另外两个帐户，一个通过可信帐户中的 IAM 角色提供权限，另一个通过 IAM 用户的 AWS 密钥提供权限：



您可以这样做 "将帐户凭据添加到 Cloud Manager" 指定 IAM 角色的 Amazon 资源名称（ ARN ）或 IAM 用户的 AWS 密钥。

添加另一组凭据后，您可以在创建新的工作环境时切换到这些凭据：



市场部署和内部部署如何?

以上各节介绍了 Cloud Manager 中建议的 Connector 部署方法。您也可以从在 AWS 中部署连接器 "AWS Marketplace" 您可以做到 "在内部安装 Connector"。

如果您使用 Marketplace ，则会以相同方式提供权限。您只需手动创建和设置 IAM 角色，然后为任何其他帐户提供权限即可。

对于内部部署，您不能为 Cloud Manager 系统设置 IAM 角色，但可以像为其他 AWS 帐户提供权限一样提供权限。

如何安全地轮换 **AWS** 凭据?

如上所述， Cloud Manager 支持您通过以下几种方式提供 AWS 凭据：与 Connector 实例关联的 IAM 角色，在可信帐户中承担 IAM 角色或提供 AWS 访问密钥。

对于前两个选项， Cloud Manager 使用 AWS 安全令牌服务获取持续轮换的临时凭据。这是最佳实践—它是自动的，安全的。

如果您为 Cloud Manager 提供了 AWS 访问密钥，则应定期在 Cloud Manager 中更新这些密钥以轮换使用。这是一个完全手动的过程。

管理 Cloud Manager 的 AWS 凭据和订阅

添加和管理 AWS 凭据，以便 Cloud Manager 拥有在 AWS 帐户中部署和管理云资源所需的权限。如果您管理多个 AWS 订阅，则可以从凭据页面将其中每个订阅分配给不同的 AWS 凭据。

概述

您可以将 AWS 凭据添加到现有 Connector 或直接添加到 Cloud Manager：

- 将 AWS 凭据添加到现有 Connector

  通过向现有连接器添加新的 AWS 凭据，您可以使用同一连接器在另一个 AWS 帐户中部署 Cloud Volumes ONTAP 。 了解如何将 AWS 凭据添加到 Connector。

- 将 AWS 凭据直接添加到 Cloud Manager

  通过向 Cloud Manager 添加新的 AWS 凭据，您可以创建适用于 ONTAP 的 FSX 工作环境。 了解如何向 Cloud Manager 添加 AWS 凭据。

如何轮换凭据

您可以通过 Cloud Manager 通过以下几种方式提供 AWS 凭据：与 Connector 实例关联的 IAM 角色，在可信帐户中担任 IAM 角色或提供 AWS 访问密钥。 "详细了解 AWS 凭据和权限"。

对于前两个选项， Cloud Manager 使用 AWS 安全令牌服务获取持续轮换的临时凭据。此过程是最佳实践，因为它是自动的，并且安全。

如果您为 Cloud Manager 提供了 AWS 访问密钥，则应定期在 Cloud Manager 中更新这些密钥以轮换使用。这是一个完全手动的过程。

向 Connector 添加凭据

添加 AWS 凭据以使 Connector 能够在其他 AWS 帐户中部署和管理 Cloud Volumes ONTAP 。您可以在其他帐户中提供 IAM 角色的 ARN ，也可以提供 AWS 访问密钥。

授予权限

在将其他 AWS 凭据添加到 Connector 之前，您需要提供所需的权限。通过这些权限， Cloud Manager 可以管理该 AWS 帐户中的资源和进程。如何提供权限取决于您是要为 Cloud Manager 提供受信任帐户或 AWS 密钥中某个角色的 ARN 。

从 Cloud Manager 部署 Connector 时， Cloud Manager 会自动为部署此 Connector 的帐户添加 AWS 凭据。如果您在现有系统上手动安装了 Connector 软件，则不会添加此初始帐户。 "了解 AWS 凭据和权限"。

- 选项 *
- [Grant permissions by assuming an IAM role in another account]
- [Grant permissions by providing AWS keys]

在另一个帐户中担任 **IAM** 角色以授予权限

您可以使用 IAM 角色在部署 Connector 实例的源 AWS 帐户与其他 AWS 帐户之间设置信任关系。然后，您可以为 Cloud Manager 提供可信帐户中 IAM 角色的 ARN 。

步骤

1. 转到要部署 Cloud Volumes ONTAP 的目标帐户中的 IAM 控制台。
2. 在访问管理下，单击 * 角色 > 创建角色 * ，然后按照步骤创建角色。

   请务必执行以下操作：

   - 在 * 可信实体类型 * 下，选择 * AWS 帐户 * 。
   - 选择 * 其他 AWS 帐户 * ，然后输入 Connector 实例所在帐户的 ID 。
   - 使用 Cloud Manager IAM 策略创建策略，该策略可从获得 "Cloud Manager 策略页面"。
3. 复制 IAM 角色的角色 ARN ，以便稍后将其粘贴到 Cloud Manager 中。

现在，此帐户具有所需权限。 现在，您可以将凭据添加到 Connector。

通过提供 **AWS** 密钥授予权限

如果要为 IAM 用户提供 Cloud Manager 的 AWS 密钥，则需要向该用户授予所需的权限。Cloud Manager IAM 策略定义了允许云管理器使用的 AWS 操作和资源。

步骤

1. 从下载 Cloud Manager IAM 策略 "Cloud Manager 策略页面"。
2. 从 IAM 控制台，通过从 Cloud Manager IAM 策略复制和粘贴文本来创建您自己的策略。

   "AWS 文档：创建 IAM 策略"

3. 将策略附加到 IAM 角色或 IAM 用户。
   - "AWS 文档：创建 IAM 角色"
   - "AWS 文档：添加和删除 IAM 策略"

现在，此帐户具有所需权限。 现在，您可以将凭据添加到 Connector。

添加凭据

在为 AWS 帐户提供所需权限后，您可以将该帐户的凭据添加到现有 Connector 。这样，您就可以使用同一个连接器在该帐户中启动 Cloud Volumes ONTAP 系统了。

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟的时间才能使用这些凭据。请等待几分钟，然后再将凭据添加到 Cloud Manager 。

步骤

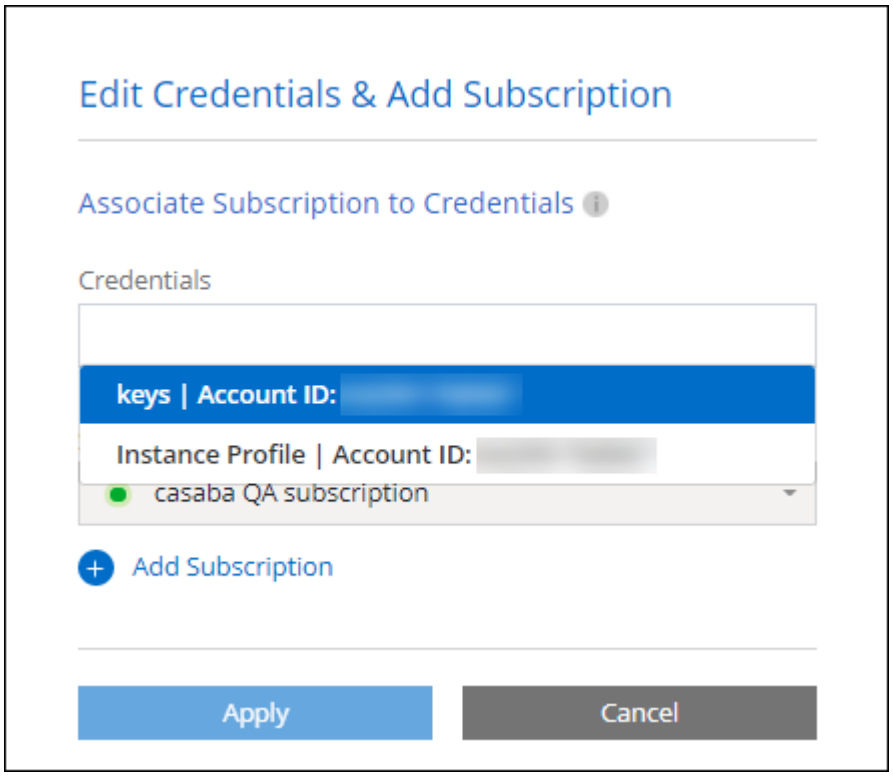
1. 确保当前已在 Cloud Manager 中选择正确的 Connector 。
2. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。

3. 单击 * 添加凭据 * ，然后按照向导中的步骤进行操作。
   a. * 凭据位置 * ： 选择 * Amazon Web Services > Connector* 。
   b. * 定义凭据 * ： 提供可信 IAM 角色的 ARN （ Amazon 资源名称），或者输入 AWS 访问密钥和机密密钥。
   c. * 市场订阅 * ： 通过立即订阅或选择现有订阅，将市场订阅与这些凭据相关联。

      要按每小时费率（ PAYGO ）或按年度合同支付 Cloud Volumes ONTAP 费用， AWS 凭据必须与 AWS Marketplace 中的 Cloud Volumes ONTAP 订阅相关联。

   d. * 查看 * ： 确认有关新凭据的详细信息，然后单击 * 添加 * 。

现在，在创建新的工作环境时，您可以从 " 详细信息和凭据 " 页面切换到另一组凭据：



向 Cloud Manager 添加凭据

通过提供 IAM 角色的 ARN ，为 Cloud Manager 提供为 ONTAP 工作环境创建 FSX 所需的权限，将 AWS 凭据添加到 Cloud Manager 。

设置 IAM 角色

设置一个 IAM 角色，使 Cloud Manager SaaS 能够承担此角色。

步骤

1. 转到目标帐户中的 IAM 控制台。
2. 在访问管理下，单击 * 角色 > 创建角色 * ，然后按照步骤创建角色。

   请务必执行以下操作：

   - 在 * 可信实体类型 * 下，选择 * AWS 帐户 * 。
   - 选择 * 其他 AWS 帐户 * 并输入 Cloud Manager SaaS 的 ID： 952013314444
   - 创建包含以下权限的策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "fsx:*",
                "ec2:Describe*",
                "ec2:CreateTags",
                "kms:Describe*",
                "kms:List*",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 复制 IAM 角色的角色 ARN ，以便您可以在下一步将其粘贴到 Cloud Manager 中。

IAM 角色现在具有所需的权限。 现在，您可以将其添加到 Cloud Manager 中。

添加凭据

为 IAM 角色提供所需权限后，将角色 ARN 添加到 Cloud Manager 中。

如果您刚刚创建了 IAM 角色，则可能需要几分钟的时间，直到这些角色可用为止。请等待几分钟，然后再将凭据添加到 Cloud Manager 。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。

2. 单击 * 添加凭据 * ，然后按照向导中的步骤进行操作。
   a. * 凭据位置 * ： 选择 * Amazon Web Services > Cloud Manager* 。
   b. * 定义凭据 * ： 提供 IAM 角色的 ARN （ Amazon 资源名称）。
   c. * 查看 * ： 确认有关新凭据的详细信息，然后单击 * 添加 * 。

现在，您可以在创建适用于 ONTAP 的 FSX 工作环境时使用这些凭据。

关联 AWS 订阅

将 AWS 凭据添加到 Cloud Manager 后，您可以将 AWS Marketplace 订阅与这些凭据相关联。通过订阅，您可以按每小时费率（ PAYGO ）或使用年度合同为 Cloud Volumes ONTAP 付费，并使用其他 NetApp 云服务。

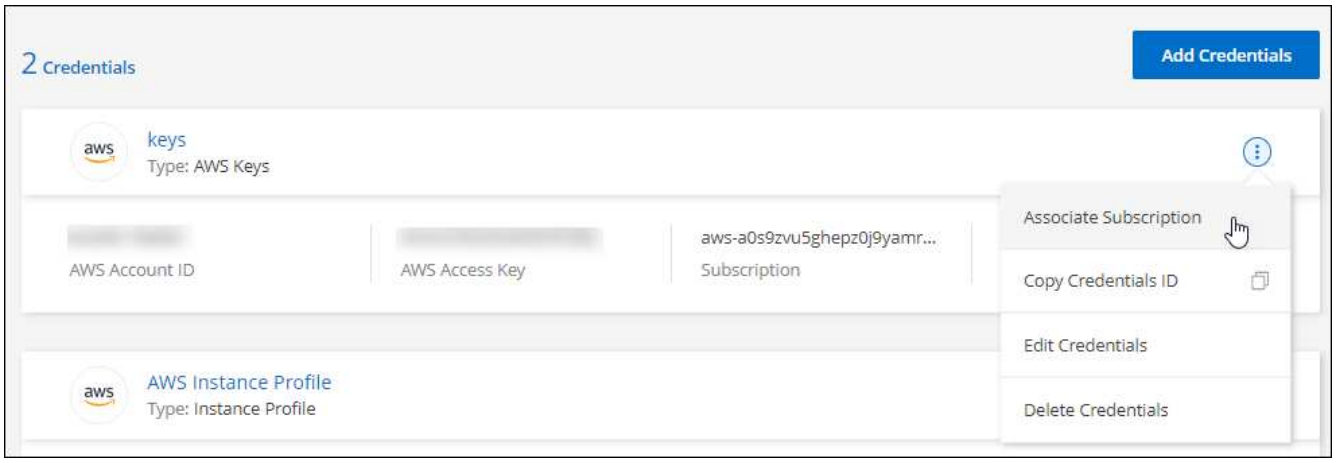
在以下两种情况下，您可能会在将凭据添加到 Cloud Manager 后关联 AWS Marketplace 订阅：

- 最初将凭据添加到 Cloud Manager 时，您未关联订阅。
- 您希望将现有 AWS Marketplace 订阅替换为新订阅。

您需要先创建 Connector ，然后才能更改 Cloud Manager 设置。 "了解如何创建 Connector"。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 关联订阅 * 。



3. 从下拉列表中选择现有订阅或单击 * 添加订阅 * ，然后按照步骤创建新订阅。

► https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 *(video)*

编辑凭据

通过更改帐户类型（ AWS 密钥或承担角色），编辑名称或更新凭据本身（密钥或角色 ARN ），在 Cloud Manager 中编辑 AWS 凭据。

您不能编辑与 Connector 实例关联的实例配置文件的凭据。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 编辑凭据 * 。
3. 进行所需的更改，然后单击 * 应用 * 。

正在删除凭据

如果您不再需要一组凭据，可以从 Cloud Manager 中删除这些凭据。您只能删除与工作环境无关的凭据。

您不能删除与 Connector 实例关联的实例配置文件的凭据。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 删除凭据 * 。
3. 单击 * 删除 * 进行确认。