管理NetApp Console

NetApp Console setup and administration

NetApp
December 12, 2025

目录

管理NetApp Console

身份和访问管理

了解NetApp Console身份和访问管理

NetApp Console中的身份和访问管理 (IAM) 使您能够组织和控制对NetApp资源的访问。您可以根据组织的层次结构来组织资源。例如，您可以按地理位置、站点或业务部门组织资源。然后，您可以将 IAM 角色分配给层次结构特定部分的成员，从而阻止访问层次结构其他部分的资源。

- "了解控制台部署模式"

IAM 的工作原理

IAM 允许您通过将用户访问角色分配给层次结构的特定部分来授予资源访问权限。例如，可以为成员分配具有五种资源的项目的文件夹或项目管理员角色。

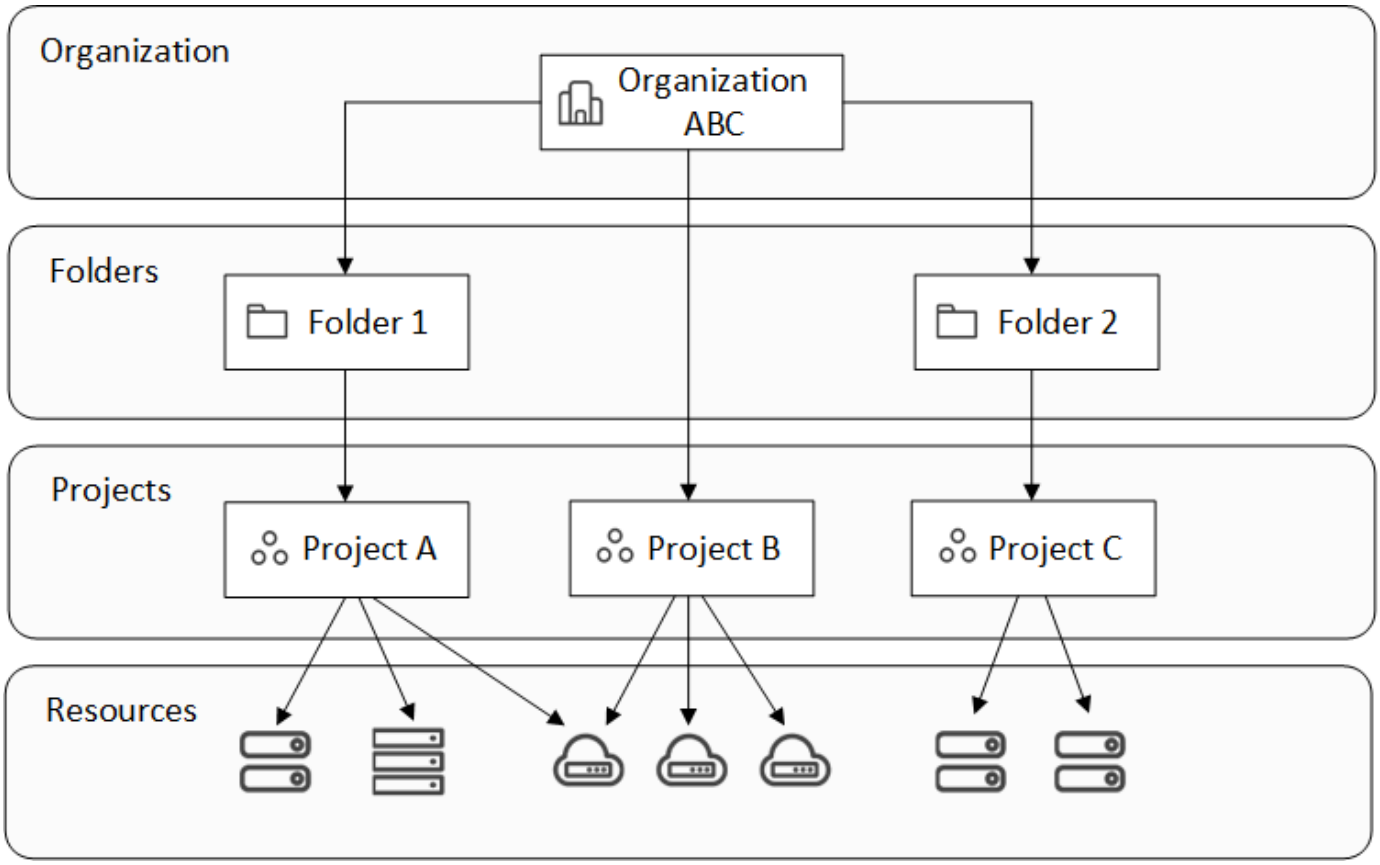
使用 IAM 时，您可以管理以下组件：

- 该组织
- 文件夹
- 项目
- 资源
- 成员
- 角色和权限
- 控制台代理

资源按层次结构组织：

- 该组织处于层级结构的顶端。
- 文件夹是组织或其他文件夹的子文件夹。
- 项目是组织或文件夹的子项。
- 资源与一个或多个文件夹或项目相关联。

下图从基本层面说明了这一层次结构。



组织

_组织_是控制台 IAM 系统的顶层，通常代表您的公司。您的组织由文件夹、项目、成员、角色和资源组成。代理与组织内的特定项目相关联。

文件夹

_文件夹_使您能够将相关项目分组在一起，并将它们与组织中的其他项目分开。例如，文件夹可能代表地理位置（欧盟或美国东部）、站点（伦敦或多伦多）或业务部门（工程或营销）。

您可以组织文件夹以包含项目、其他文件夹或两者。它们是可选的。

项目

_项目_代表控制台中的一个工作区，组织成员可以从*系统*页面访问该工作区以管理资源。例如，一个项目可以包括一个Cloud Volumes ONTAP系统、一个本地ONTAP集群或一个 FSx for ONTAP文件系统。

一个组织可以有一个或多个项目。项目可以直接位于组织下或文件夹内。

资源

_资源_是您在控制台中创建或发现的系统。

当您创建或发现资源时，该资源将与当前选定的项目相关联。这可能是您想要与该资源关联的唯一项目。但您可以选择将该资源与您组织中的其他项目相关联。

例如，您可以将Cloud Volumes ONTAP系统与另一个项目或组织中的所有项目关联。如何关联资源取决于您组织的需求。

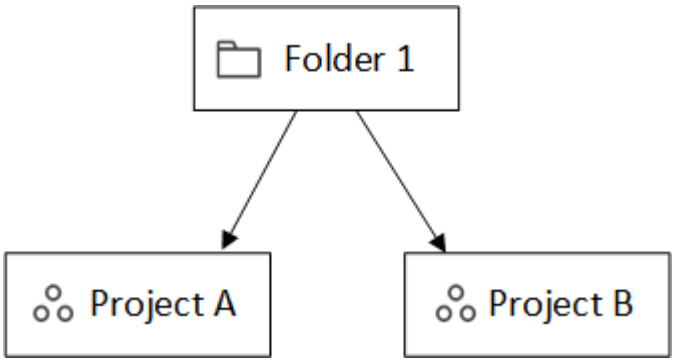
代理还可以与多个项目相关联。了解有关使用代理与 IAM 的更多信息 。

何时将资源与文件夹关联

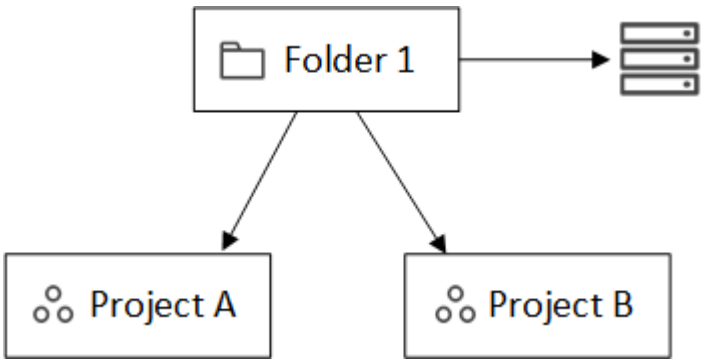
您还可以选择将资源与文件夹关联，但这是可选的，并且可以满足特定用例的需求。

_组织管理员_可以将资源与文件夹关联，以便_文件夹或项目管理员_可以将其链接到文件夹中的相应项目。

例如，假设您有一个包含两个项目的文件夹：

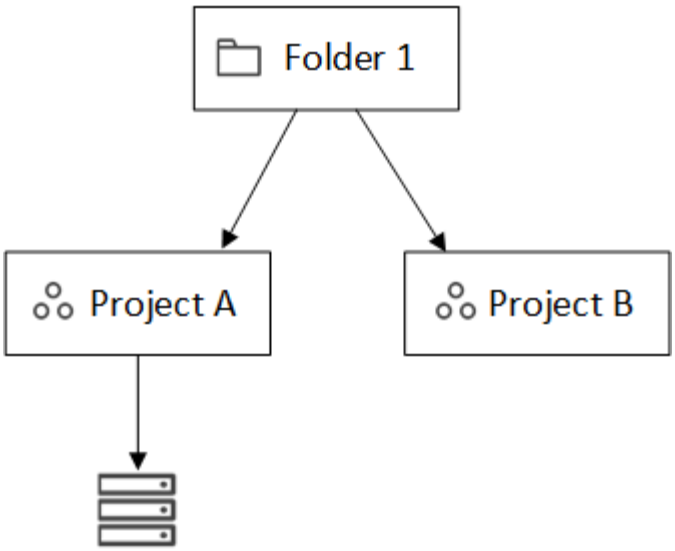


_组织管理员_可以将资源与文件夹关联：



将资源与文件夹关联并不会使所有项目都可以访问它；只有文件夹或项目管理员可以看到它。 _文件夹或项目管理员_决定哪些项目可以访问它，并将资源与适当的项目关联。

在此示例中，管理员将资源与项目 A 关联：



拥有项目 A 权限的成员现在可以访问该资源。

成员

您的组织的成员是用户帐户或服务帐户。应用程序通常使用服务帐户来完成指定的任务，而无需人工干预。

每个组织至少包含一个具有“组织管理员”角色的用户（控制台会自动将此角色分配给创建该组织的用户）。您可以将其他成员添加到组织并在资源层次结构的不同级别分配不同的权限。

角色和权限

您不能直接向组织成员授予权限。相反，您授予每个成员一个角色。角色包含一组权限，使成员能够在资源层次结构的特定级别执行特定操作。

在层次结构级别授予角色会限制成员对所需资源和服务的访问。

您可以在层次结构中分配角色

当您将成员与角色关联时，您需要选择整个组织、特定文件夹或特定项目。您选择的角色将授予成员对层次结构中选定部分中的资源的权限。

角色继承

当您分配角色时，该角色将在组织层次结构中继承：

组织

在组织级别授予成员访问角色将赋予他们访问所有文件夹、项目和资源的权限。

文件夹

当您在文件夹级别授予访问角色时，文件夹中的所有文件夹、项目和资源都会继承该角色。

例如，如果您在文件夹级别分配角色，并且该文件夹有三个项目，则该成员将对这三个项目和任何相关资源拥有权限。

项目

当您在项目级别授予访问角色时，与该项目相关的所有资源都会继承该角色。

多重角色

您可以为每个组织成员分配组织层次结构不同级别的角色。可以是相同的角色，也可以是不同的角色。例如，您可以为项目 1 和项目 2 分配成员角色 A。或者您可以为项目 1 分配成员角色 A，为项目 2 分配角色 B。

访问角色

控制台提供您可以分配给组织成员的访问角色。

"了解访问角色" 。

控制台代理

当“组织管理员”创建控制台代理时，控制台会自动将该代理与组织和当前选定的项目关联。 _组织管理员_可以从组织中的任何位置自动访问该代理。但是，如果您的组织中有具有不同角色的其他成员，则这些成员只能从创建该代理的项目访问该代理，除非您将该代理与其他项目关联。

在以下情况下，您可以为另一个项目提供控制台代理：

- 您希望允许组织中的成员使用现有代理来创建或发现另一个项目中的其他系统
- 您将现有资源与另一个项目关联，并且该资源由控制台代理管理

  如果使用控制台代理发现与其他项目关联的资源，那么您还需要将该代理与该资源现在关联的项目关联。否则，没有“组织管理员”角色的成员将无法从“系统”页面访问该代理及其关联资源。

您可以从控制台 IAM 中的“代理”页面创建关联：

- 将控制台代理与项目关联

  当您将控制台代理与项目关联时，可以在查看项目时从*系统*页面访问该代理。

- 将控制台代理与文件夹关联

  将控制台代理与文件夹关联并不会自动使文件夹中的所有项目都可以访问该代理。组织成员无法从项目访问控制台代理，除非您将代理与特定项目关联。

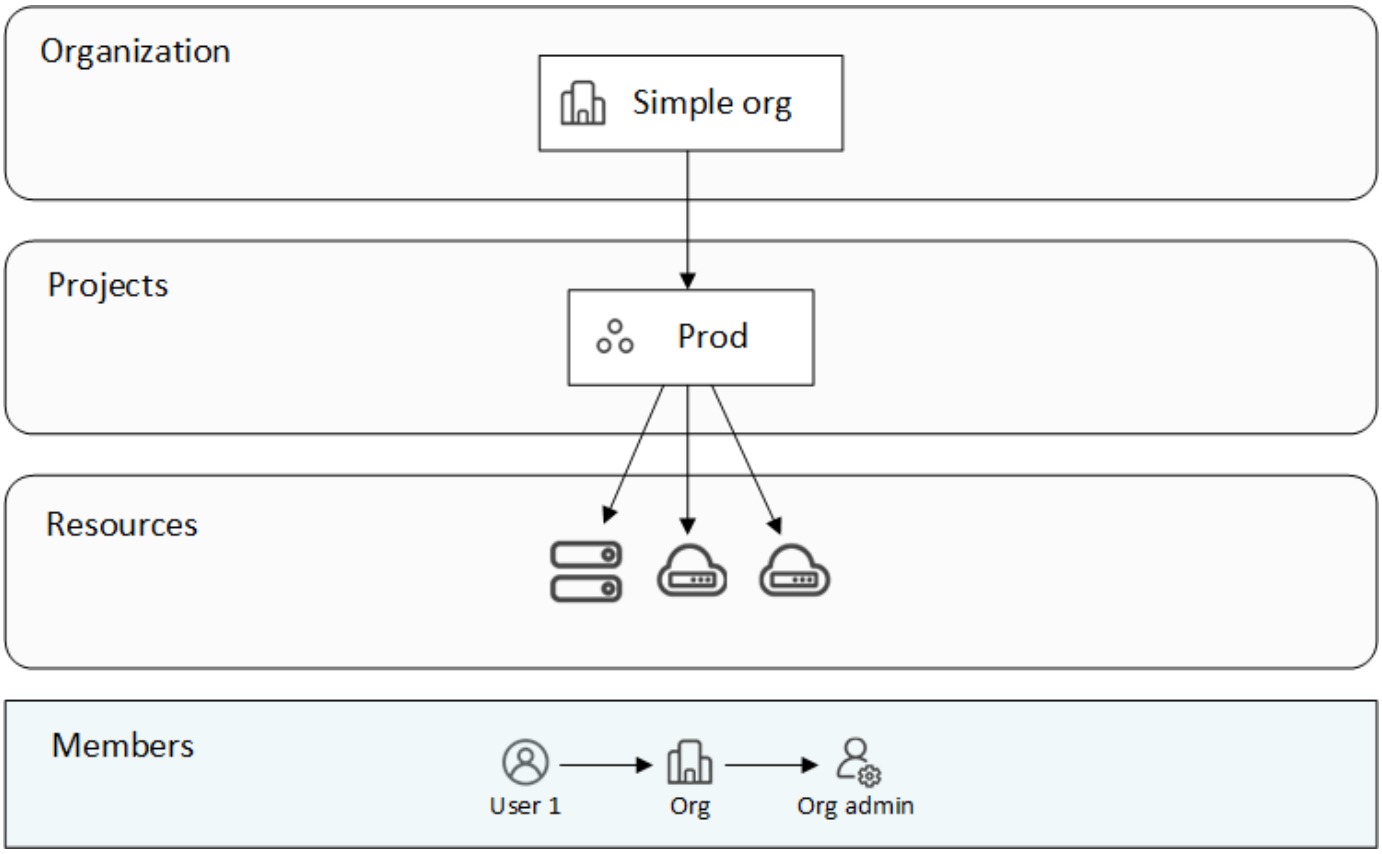
  _组织管理员_可能会将控制台代理与文件夹关联，以便_文件夹或项目管理员_可以决定将该代理与文件夹中的相应项目关联。

IAM 示例

这些示例演示了如何建立您的组织。

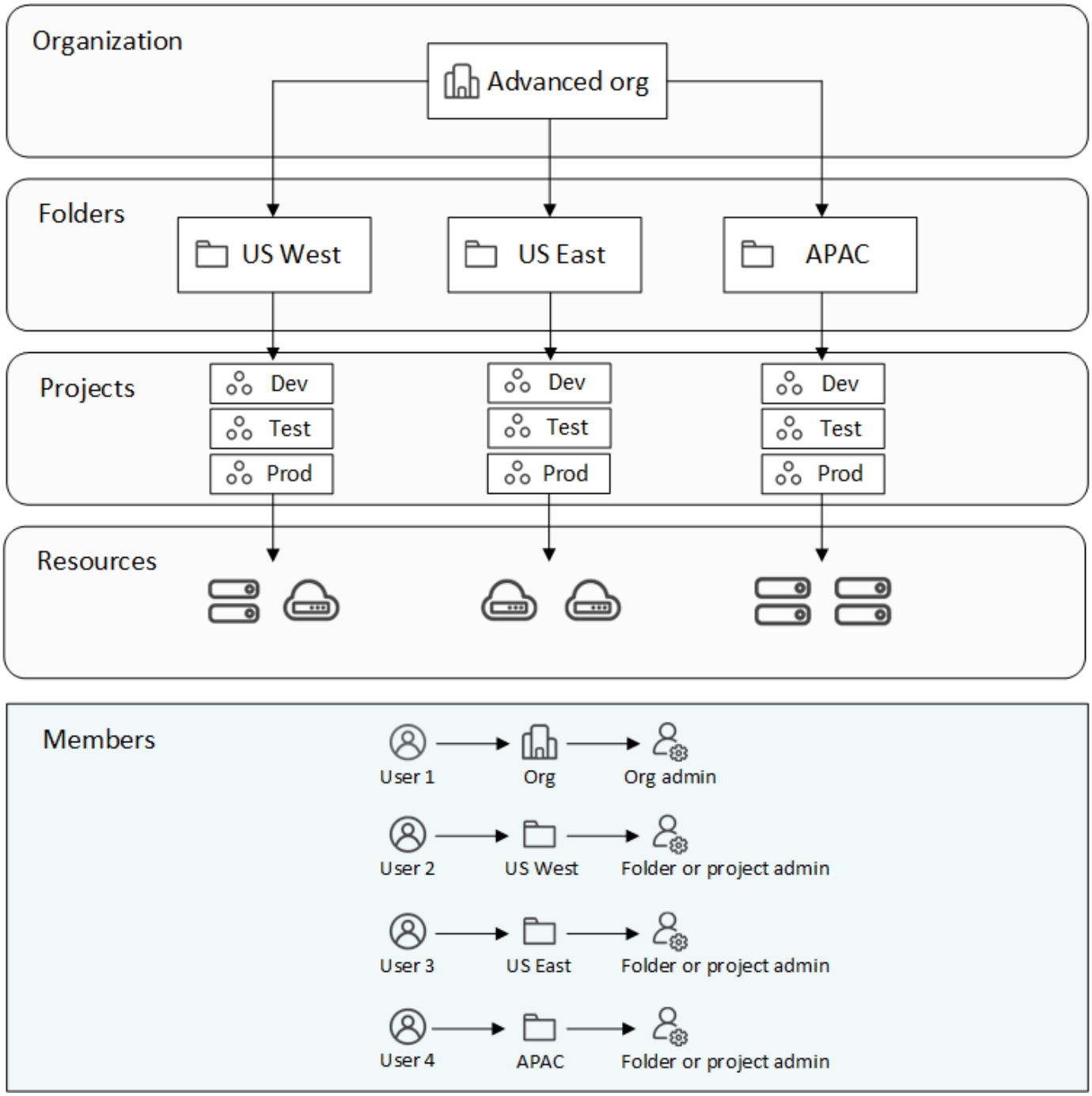
简单的组织

下图显示了使用默认项目且没有文件夹的组织的简单示例。一名成员管理整个组织。



先进组织

下图显示了一个组织使用文件夹来组织业务中每个地理位置的项目。每个项目都有自己的一套相关资源。成员包括组织管理员和组织中每个文件夹的管理员。



IAM 的功能

以下示例描述了如何使用 IAM 来管理控制台组织：

- 授予特定成员特定角色，以便他们只能完成所需的任务。
- 由于成员调动部门或承担额外责任而修改成员权限。
- 删除已离开公司的用户。
- 将文件夹或项目添加到您的层次结构中，因为新的业务部门已添加NetApp存储。
- 将资源与另一个项目关联起来，因为该资源具有另一个团队可以利用的能力。
- 查看成员可以访问的资源。

- 查看与特定项目相关的成员和资源。

下一步

- "开始使用NetApp Console中的 IAM"
- "使用文件夹和项目在NetApp Console中组织您的资源"
- "管理NetApp Console成员及其权限"
- "管理NetApp Console组织中的资源层次结构"
- "将代理与文件夹和项目关联"
- "在NetApp Console项目和组织之间切换"
- "重命名您的NetApp Console组织"
- "监控或审计 IAM 活动"
- "NetApp Console访问角色"
- "了解NetApp Console IAM 的 API"

开始在**NetApp Console**中使用身份和访问权限

当您注册NetApp Console时，系统会提示您创建一个新的组织。该组织包括一名成员（组织管理员）和一个默认项目。要设置身份和访问管理 (IAM) 来满足您的业务需求，您需要自定义组织的层次结构、添加其他成员、添加或发现资源，并在整个层次结构中关联这些资源。

您必须拥有*组织管理员*权限才能管理整个组织的身份和访问权限。如果您具有*文件夹或项目管理员*权限，则您只能管理您有权限的文件夹和项目。

按照以下步骤建立一个新组织。该顺序可能会根据您组织的需求而有所不同。


编辑默认项目或添加到组织的层次结构

使用默认项目或创建与您的业务层次结构相匹配的其他项目和文件夹。

"了解如何使用文件夹和项目来组织资源" 。


将成员与您的组织关联

将用户帐户链接到您的组织并分配权限。您还可以选择向您的组织添加服务帐户。

"了解如何管理成员及其权限" 。


添加或发现资源

向控制台添加或发现资源（系统）。组织成员从项目内部管理系统。

了解如何创建或发现资源：

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "E系列系统"
- "本地ONTAP集群"
- "StorageGRID"

4 将资源与其他项目关联

在控制台中添加或发现系统会自动将资源与当前选定的项目关联。要使该资源可用于组织中的另一个项目，请将其与相应的项目关联。如果使用控制台代理来管理资源，请将控制台代理与相应的项目关联。

- "了解如何管理组织的资源层次结构" 。
- "了解如何将控制台代理与文件夹或项目关联" 。

相关信息

- "了解NetApp Console中的身份和访问管理"
- "了解身份和访问 API"

使用文件夹和项目组织您的NetApp Console资源

在NetApp Console中，您可以使用项目和文件夹来组织您的NetApp资源。 项目_代表控制台中的一个工作区，组织成员可以访问该工作区来管理_资源（例如， Cloud Volumes ONTAP系统）。 _文件夹_将相关项目分组在一起。将资源组织到文件夹和项目中后，您可以通过向组织成员提供特定文件夹和项目的权限来授予对资源的细粒度访问权限。

添加文件夹或项目

当您创建组织时，它包含一个项目。添加项目以管理资源，添加文件夹以将相关项目分组在一起。

您可以在组织的资源结构中创建最多七级的文件夹和项目。在文件夹内创建文件夹，为您的组织构建嵌套结构。

步骤

1. 选择*管理>身份和访问*。
2. 选择*组织*。
3. 从*组织*页面中，选择*添加文件夹或项目*。
4. 选择*文件夹*或*项目*。
5. 请输入文件夹或项目详细信息：
    - 名称和位置：输入名称并选择文件夹或项目的层次结构中的位置。将文件夹或项目放在组织下或另一个文件夹内。
    - 资源：选择您想要与此文件夹或项目关联的资源。

      您可以选择与父文件夹或项目相关的资源。

"了解何时将资源与文件夹关联" 。

- 访问：根据资源层次结构中已定义的现有权限，查看有权访问文件夹或项目的成员。

  选择“添加成员”以分配访问权限和角色。

"了解访问角色" 。

6. 选择“添加”。

重命名文件夹或项目

如果需要，您可以更改文件夹和项目的名称。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，输入新名称并选择*应用*。

删除文件夹或项目

删除不再需要的文件夹和项目。

删除文件夹或项目之前，请确保其中不包含任何资源。了解如何移除资源。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*删除*。
2. 确认您要删除文件夹或项目。

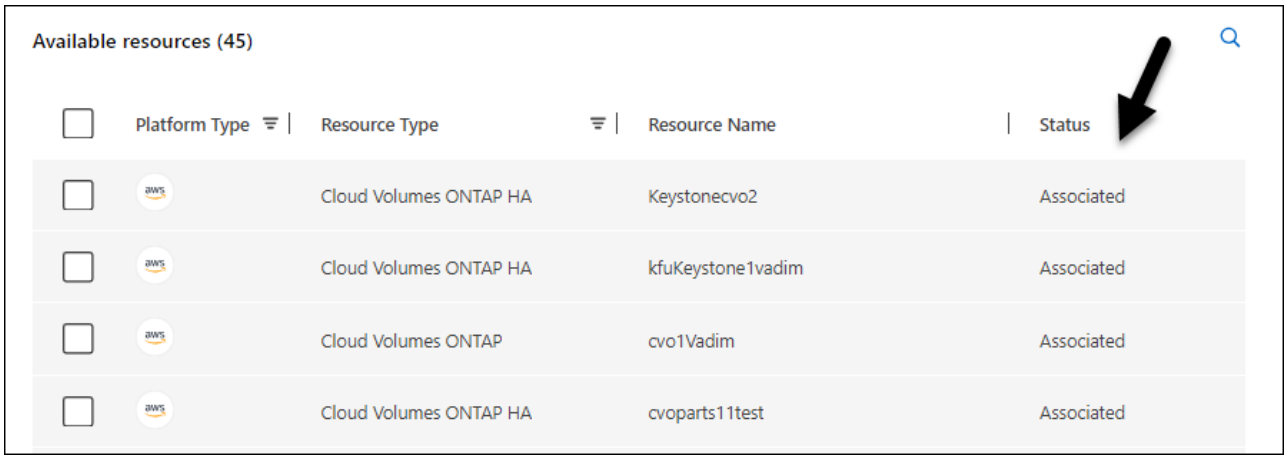
查看与文件夹或项目关联的资源

查看哪些资源和成员与文件夹或项目相关联。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。

2. 在*编辑*页面上，您可以通过展开*资源*或*访问*部分来查看有关所选文件夹或项目的详细信息。
   - 选择“资源”来查看相关资源。在表中，“状态”列标识与文件夹或项目相关的资源。



更改与文件夹或项目关联的资源

拥有文件夹或项目权限的成员可以访问其相关资源。

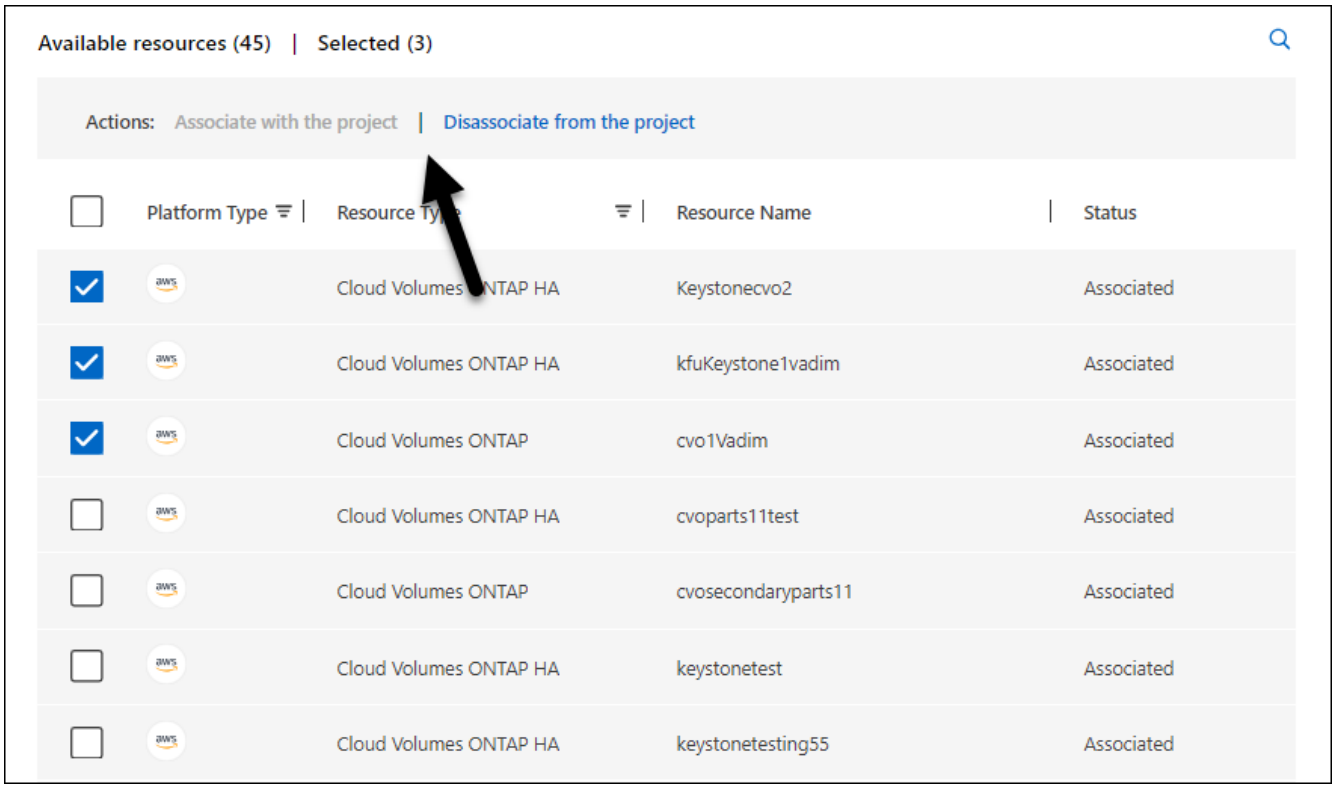
开始之前

"了解何时将资源与文件夹关联" 。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，选择*资源*。

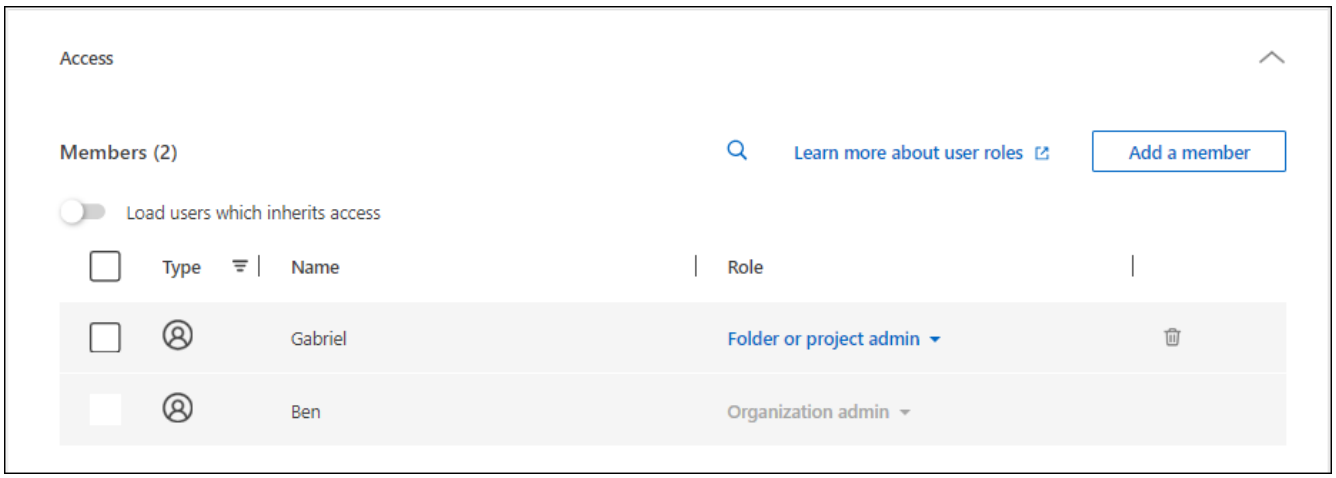
   在表中，“状态”列标识与文件夹或项目相关的资源。
3. 选择您想要关联或取消关联的资源。
4. 根据您选择的资源，选择*与项目关联*或*与项目取消关联*。



5. 选择*应用*。

查看与文件夹或项目关联的成员

- 选择*访问*来查看有权访问该文件夹或项目的成员。



修改成员对文件夹或项目的访问权限

修改成员访问权限以控制资源访问。

如果成員存取權限是從較高階層繼承而來，則無法在較低階層變更成員存取權限。更新更高层次结构级别的成员权限以更改访问权限。或者，您可以 "从“会员”页面管理权限".

"了解有关角色继承的详细信息" 。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，选择*访问*以查看有权访问所选文件夹或项目的成员列表。
3. 修改会员访问权限：
   - 添加成员：选择您想要添加到文件夹或项目的成员并为他们分配角色。
   - 更改成员的角色：对于具有组织管理员以外角色的任何成员，选择其现有角色，然后选择新角色。
   - 删除成员访问权限：对于在您正在查看的文件夹或项目中定义了角色的成员，您可以删除他们的访问权限。
4. 选择*应用*。

相关信息

- "了解NetApp Console中的身份和访问权限"
- "开始使用身份和访问权限"
- "了解身份和访问 API"

将成员和服务帐户添加到NetApp Console

在控制台中，您可以将用户和服务帐户添加到您的组织，并在资源层次结构中为他们分配一个或多个角色。角色包含一组权限，使成员（用户或服务帐户）能够在资源层次结构的特定级别执行特定操作。

您需要以下角色之一来管理用户和权限：

- 组织管理员

  具有此角色的用户可以管理所有成员

- 文件夹或项目管理员

  具有此角色的用户只能管理指定文件夹或项目的成员

  _文件夹或项目管理员_可以在*成员*页面上查看所有成员，但只能管理他们有权访问的文件夹和项目的权限。"详细了解文件夹或项目管理员可以完成的操作" 。

向您的组织添加成员

您可以向您的组织添加两种类型的成员：用户帐户和服务帐户。应用程序使用服务帐户自动执行 API 任务。人们使用用户帐户登录和管理资源。

用户必须先注册NetApp Console，然后您才能将他们添加到组织或为他们分配角色。您可以直接从控制台创建服务帐户。

要管理用户及其权限，您必须具有*组织管理员*角色或*文件夹或项目管理员*角色。请记住，具有“文件夹或项目管理员”角色的用户只能管理他们具有管理员权限的文件夹或项目的成员。

添加用户帐户

尽管用户可以自行注册NetApp Console，但他们需要明确添加到组织或特定文件夹或项目才能访问控制台中的资源。

步骤

1. 引导用户访问 "NetApp Console"进行注册。

   用户注册后，他们会完成*注册*页面，检查电子邮件并登录。如果控制台提示用户创建组织，他们会关闭它并通知您他们的帐户已创建。然后，您可以将该用户添加到您现有的组织。

   "了解如何注册NetApp Console" 。

2. 选择*管理>身份和访问*。
3. 选择*成员*。
4. 选择*添加成员*。
5. 对于*会员类型*，保持选择*用户*。
6. 对于*用户的电子邮件*，输入与其创建的登录相关联的用户的电子邮件地址。
7. 使用“选择组织、文件夹或项目”部分来选择成员应具有权限的资源层次结构级别。

   请注意以下事项：

   - 您只能从您有权限的文件夹和项目中进行选择。
   - 选择一个组织或文件夹将授予成员对其所有内容的权限。
   - 您只能在组织级别分配*组织管理员*角色。

8. 选择一个类别，然后选择一个*角色*，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。

   "了解访问角色" 。

9. 可选：选择其他角色或项目。如果您想提供对组织内其他文件夹或项目的访问权限，或授予用户在所选区域中的其他角色，请选择*添加角色*，指定另一个文件夹或项目或其他角色类别，然后选择一个角色。
10. 选择“添加”。

    控制台向用户发送一封包含说明的电子邮件。

添加服务帐户

您可以使用服务帐户自动执行任务并与控制台 API 安全地集成。创建服务帐户时，请在两种身份验证方法之间进行选择：使用客户端 ID 和密钥，或使用 JWT（JSON Web 令牌）身份验证。客户端 ID 和秘密方法适合简单设置，而 JWT 身份验证为自动化或云原生环境提供更强的安全性。选择最适合您的安全需求以及您计划如何使用控制台的选项。

如果您想使用 JWT 身份验证，请准备好您的公钥或证书。

步骤

1. 选择*管理>身份和访问*。

2. 选择*成员*。
3. 选择*添加成员*。
4. 对于*会员类型*，选择*服务帐户*。
5. 输入服务帐户的名称。
6. 如果您想使用 JWT 身份验证，请选择 使用私钥 **JWT** 身份验证 并上传您的公共 RSA 密钥或证书。如果您想使用客户端 ID 和密钥，请跳过此步骤。

   您的 X.509 证书。它必须是 PEM、CRT 或 CER 格式。

   a. 设置证书到期通知。您可以选择七天或三十天。到期通知将通过电子邮件发送给具有超级管理员或组织管理员角色的用户，并在控制台中显示。
7. 使用“选择组织、文件夹或项目”部分来选择成员应具有权限的资源层次结构级别。

   请注意以下事项：

   - 您只能从您有权限的文件夹和项目中进行选择。
   - 选择一个组织或文件夹将授予成员对其所有内容的权限。
   - 您只能在组织级别分配*组织管理员*角色。
8. 选择一个*类别*，然后选择一个*角色*，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。

   "了解访问角色" 。
9. 可选：选择其他角色或项目。如果您想提供对组织内其他文件夹或项目的访问权限，或授予用户在所选区域中的其他角色，请选择*添加角色*，指定另一个文件夹或项目或其他角色类别，然后选择一个角色。
10. 如果您没有选择使用 JWT 身份验证，请下载或复制客户端 ID 和客户端密钥。 + 控制台仅显示一次客户端密钥。安全地复制它；如果需要，您可以稍后重新创建它。
11. 如果您选择 JWT 身份验证，请下载或复制客户端 ID 和 JWT 受众。此信息仅显示一次，之后无法检索。
12. 选择*关闭*。

查看组织成员

要了解成员可用的资源和权限，您可以查看在组织资源层次结构的不同级别分配给该成员的角色。"了解如何使用角色来控制对控制台资源的访问。"

您可以从“成员”页面查看用户帐户和服务帐户。

您还可以查看与特定文件夹或项目相关的所有成员。"了解更多" 。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。

   *成员*表列出了您组织的成员。

3. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。

从您的组织中移除成员

您可能需要从您的组织中删除某个成员 - 例如，如果他们离开了您的公司。

删除成员时，系统会撤销其权限，但保留其控制台和NetApp支持站点帐户。

步骤

1. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*删除用户*。
2. 确认您要从组织中删除该成员。

重新创建服务帐户的凭据

如果您丢失了凭证或需要更新凭证，请创建新的凭证。

重新创建凭据时，您将删除服务帐户的现有凭据并创建新的凭据。您不能使用以前的凭据。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 在“成员”表中，导航到服务帐户，选择 ••• 然后选择*重新创建秘密*。
4. 选择*重新创建*。
5. 下载或复制客户端 ID 和客户端密钥。+ 控制台只会显示一次客户端密钥。复制或下载并安全存储。

管理用户的多重身份验证 **(MFA)**

如果用户失去对其 MFA 设备的访问权限，您可以删除或禁用其 MFA 配置。

用户移除多因素身份验证后，登录时必须重新设置多因素身份验证。如果用户只是暂时无法访问其 MFA 设备，他们可以使用设置 MFA 时保存的恢复代码登录。

如果他们没有恢复代码，请暂时禁用 MFA 以允许登录。当您为用户禁用 MFA 时，它只会禁用八个小时，然后自动重新启用。在此期间，用户无需 MFA 即可登录一次。八小时后，用户必须使用 MFA 才能登录。

要管理用户的多重身份验证，您必须拥有与受影响用户位于同一域的电子邮件地址。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。

   *成员*表列出了您组织的成员。
3. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*管理多重身份验证*。
4. 选择是否删除或禁用用户的 MFA 配置。

使用角色管理用户对NetApp Console资源的访问

在控制台中，您可以根据用户需要做什么以及在哪里为用户分配角色。

具有*组织管理员*或*文件夹或项目管理员*角色的用户有责任将角色分配给其他用户。您可以根据项目或文件夹分配访问角色。按项目或文件夹分配访问角色。例如，将“勒索软件恢复”管理员角色分配给一个项目的用户，将“SnapCenter”管理员角色分配给另一个项目的用户。要为用户授予文件夹中所有项目的勒索软件恢复管理员角色，请在文件夹级别分配该角色。

使用访问角色根据用户需要执行的特定任务分配对存储资源的访问权限。例如，如果用户需要与 Ransomware Resilience 进行交互，则必须为他们授予访问角色，该角色包括对授予访问角色的项目的 Ransomware Resilience 的查看或管理权限。

根据您的身份和访问管理 (IAM) 策略分配角色，以提高安全性。 IAM角色限制用户访问权限，使其仅限于必要的权限。

请记住，您不能直接授予对资源的访问权限。首先将资源分配给项目。在分配用户访问权限之前，请考虑设置资源层次结构。"了解如何使用文件夹和项目来组织您的资源。"

查看分配给成员的角色

当您向组织添加成员时，系统会提示您为其分配角色。您可以查看他们目前被分配的角色。

如果您具有_文件夹或项目管理员_角色，则该页面将显示组织中的所有成员。但是，您只能查看和管理您拥有权限的文件夹和项目的成员权限。"详细了解文件夹或项目管理员可以完成的操作" 。

1. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
2. 在表格中，展开您想要查看成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”。

为成员添加访问角色

您通常在向组织添加成员时分配角色，但您可以随时通过删除或添加角色来更新它。

您可以为用户分配组织、文件夹或项目的访问角色。

成员可以在同一个项目内以及不同的项目中拥有多个角色。例如，较小的组织可能会将所有可用的访问角色分配给同一个用户，而较大的组织可能会让用户执行更专业的任务。或者，您也可以为一个用户分配组织的勒索软件恢复管理员角色。在该示例中，用户将能够对组织内的所有项目执行勒索软件恢复任务。

您的访问角色策略应与您组织NetApp资源的方式保持一致。

被分配了组织管理员角色的成员不能被分配任何其他角色。他们已经拥有整个组织的权限。具有文件夹或项目角色的成员不能被分配文件夹或项目中他们已经具有该角色的任何其他角色。这两个角色都提供对其被分配范围内的所有服务的访问权限。

步骤

1. 选择*管理>身份和访问*。
2. 选择操作菜单 ••• 在您想要分配角色的成员旁边，选择“添加角色”。
3. 要添加角色，请完成对话框中的步骤：

- 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

  如果您选择组织或文件夹，则该成员将拥有该组织或文件夹内所有内容的权限。

- 选择类别：选择角色类别。"了解访问角色" 。
- 选择*角色*：选择一个角色，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。
- 添加角色：如果您想提供对组织内其他文件夹或项目的访问权限，请选择*添加角色*，指定另一个文件夹或项目或角色类别，然后选择一个角色类别和相应的角色。

4. 选择*添加新角色*。

更改成员的指定角色

更改成员角色以更新其访问权限。

必须为用户分配至少一个角色。您不能删除用户的所有角色。如果您需要删除所有角色，则必须从组织中删除该用户。

步骤

1. 选择*管理>身份和访问*。
2. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
3. 在表格中，展开要更改成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”以查看分配给该成员的角色。
4. 您可以更改成员的现有角色或删除角色。
   a. 要更改成员的角色，请选择要更改的角色旁边的“更改”。您只能将角色更改为同一角色类别内的角色。例如，您可以从一个数据服务角色更改为另一个数据服务角色。确认更改。
   b. 要取消分配成员的角色，请选择 取消为该成员分配相应的角色。系统会要求您确认删除。

管理NetApp Console组织中的资源层次结构

当您将成员与您的组织关联时，您会在组织、文件夹或项目级别提供权限。为了确保这些成员有权访问正确的资源，您需要通过将资源与特定项目和文件夹关联来管理组织的资源层次结构。 _资源_是控制台已经管理或知道的存储系统或控制台代理。

查看组织中的资源

您可以查看与您的组织相关的已发现和未发现的资源。系统会查找存储资源，并将其标记为未发现，直到您将其添加到控制台为止。

资源页面不包含Amazon FSx for NetApp ONTAP资源，因为用户无法将其与角色关联。可以在“系统”页面或“工作负载”中查看。

步骤

1. 选择*管理>身份和访问*。
2. 选择*资源*。

3. 选择*高级搜索和过滤*。
4. 利用现有选项查找资源：
   - 按资源名称搜索：输入文本字符串并选择*添加*。
   - 平台：选择一个或多个平台，例如 Amazon Web Services。
   - 资源：选择一个或多个资源，例如Cloud Volumes ONTAP。
   - 组织、文件夹或项目：选择整个组织、特定文件夹或特定项目。
5. 选择*搜索*。

将资源与文件夹和项目关联

将资源与文件夹或项目关联以使其可用。

开始之前

您应该了解资源关联是如何工作的。"了解资源，包括何时将资源与文件夹关联" 。

步骤

1. 从“资源”页面，导航到表中的资源，选择 ••• 然后选择*关联到文件夹或项目*。
2. 选择一个文件夹或项目，然后选择*接受*。
3. 要关联其他文件夹或项目，请选择*添加文件夹或项目*，然后选择该文件夹或项目。

   请注意，您只能从您拥有管理员权限的文件夹和项目中进行选择。

4. 选择*关联资源*。
   - 如果您将资源与项目关联，则拥有这些项目权限的成员现在可以从控制台访问该资源。
   - 如果您将资源与文件夹关联，则_文件夹或项目管理员_现在可以访问该资源并将其与文件夹内的项目关联。"了解如何将资源与文件夹关联" 。

完成后

如果您使用控制台代理发现资源，请将控制台代理与项目关联以授予访问权限。否则，没有“组织管理员”角色的成员将无法访问控制台代理及其相关资源。

"了解如何将控制台代理与文件夹或项目关联"。

查看与资源关联的文件夹和项目

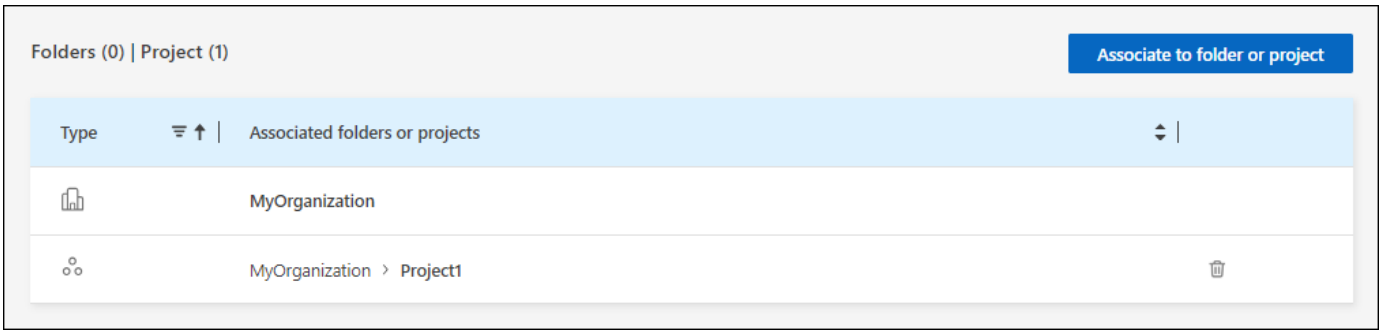
您可以查看与特定资源关联的文件夹和项目。

> 如果您需要了解哪些组织成员有权访问该资源，您可以"查看有权访问与资源关联的文件夹和项目的成员"。

步骤

1. 从“资源”页面，导航到表中的资源，选择 ••• 然后选择*查看详细信息*。

以下示例显示了与一个项目关联的资源。



要查看哪些组织成员有权访问该资源，"查看有权访问关联文件夹和项目的成员"。

从文件夹或项目中删除资源

要从文件夹或项目中删除资源，您需要删除文件夹或项目与资源之间的关联。当您删除关联时，它会阻止成员管理文件夹或项目中的资源。

要从整个组织中删除已发现的资源，请转到“系统”页面并删除该系统。

步骤

1. 从“资源”页面，导航到表中的资源，选择•••然后选择*查看详细信息*。
2. 对于要删除资源的文件夹或项目，选择🗑
3. 通过选择“删除”确认您要删除关联。

相关信息

- "了解NetApp Console中的身份和访问权限"
- "开始在NetApp Console中使用身份和访问权限"
- "了解身份和访问 API"

将控制台代理与其他文件夹和项目关联

当“组织管理员”创建控制台代理时，该控制台代理会自动与组织内当前选定的项目相关联。尽管具有“组织管理员”角色的人可以从组织中的任何地方访问该控制台代理。除非您将该控制台代理与其他项目关联，否则您组织中的其他成员只能从创建该控制台代理的项目访问该控制台代理。

开始之前

回顾控制台代理关联的工作原理。"了解如何将控制台代理与身份和访问结合使用"。

关于此任务

文件夹或项目管理员可以在代理页面上查看所有控制台代理，但只能将控制台代理与他们有权限的文件夹和项目关联。"详细了解文件夹或项目管理员可以完成的操作"。

步骤

1. 选择*管理>身份和访问*>*代理*。

2. 从表中，找到要关联的控制台代理。

   使用表格上方的搜索功能查找特定的控制台代理或按资源层次结构过滤表格。

3. 要查看链接到控制台代理的文件夹和项目，请选择 ••• 然后选择*查看详细信息*。

   该页面显示与控制台代理关联的文件夹和项目的详细信息。

4. 选择*关联到文件夹或项目*。
5. 选择一个文件夹或项目，然后选择*接受*。
6. 要将控制台代理与其他文件夹或项目关联，请选择*添加文件夹或项目*，然后选择该文件夹或项目。
7. 选择*关联代理*。

完成后

将控制台代理的资源与“资源”页面中的相同文件夹和项目关联。

"了解如何将资源与文件夹和项目关联" 。

相关信息

- "了解NetApp Console代理"
- "了解NetApp Console身份和访问管理"
- "开始使用身份和访问权限"
- "了解身份和访问管理的 API"

在控制台组织、项目和代理之间切换

您可能属于多个控制台组织，或者有权访问组织内的多个项目或代理。需要时，您可以轻松地在组织、项目和控制台代理之间切换，以访问与该组织、项目或代理相关的资源。

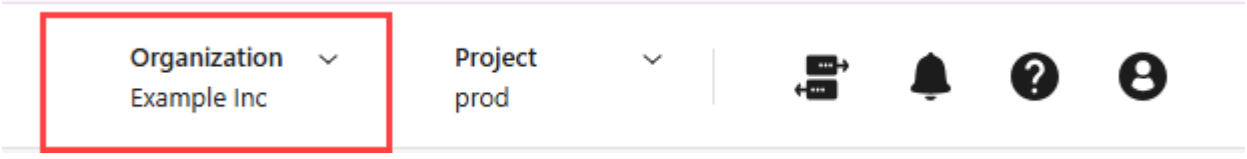
如果其他组织邀请您加入或者您自己创建一个组织，那么您可能属于多个组织。您可以使用 API 创建其他组织。 "了解如何创建新组织"

在组织之间切换

如果您是多个组织的成员，您可以随时在它们之间切换。

步骤

1. 在控制台的顶部标题中，选择*组织*。



2. 如果您有任何合作组织，请选择“合作伙伴关系”选项卡来查看可用的合作伙伴组织。

+ 如果您没有任何合作伙伴组织，则不会显示“合作伙伴关系”选项卡。

1. 选择另一个组织，然后选择*切换*。

+ 如果您有任何合作组织，请选择“合作伙伴关系”选项卡来查看可用的合作伙伴组织。

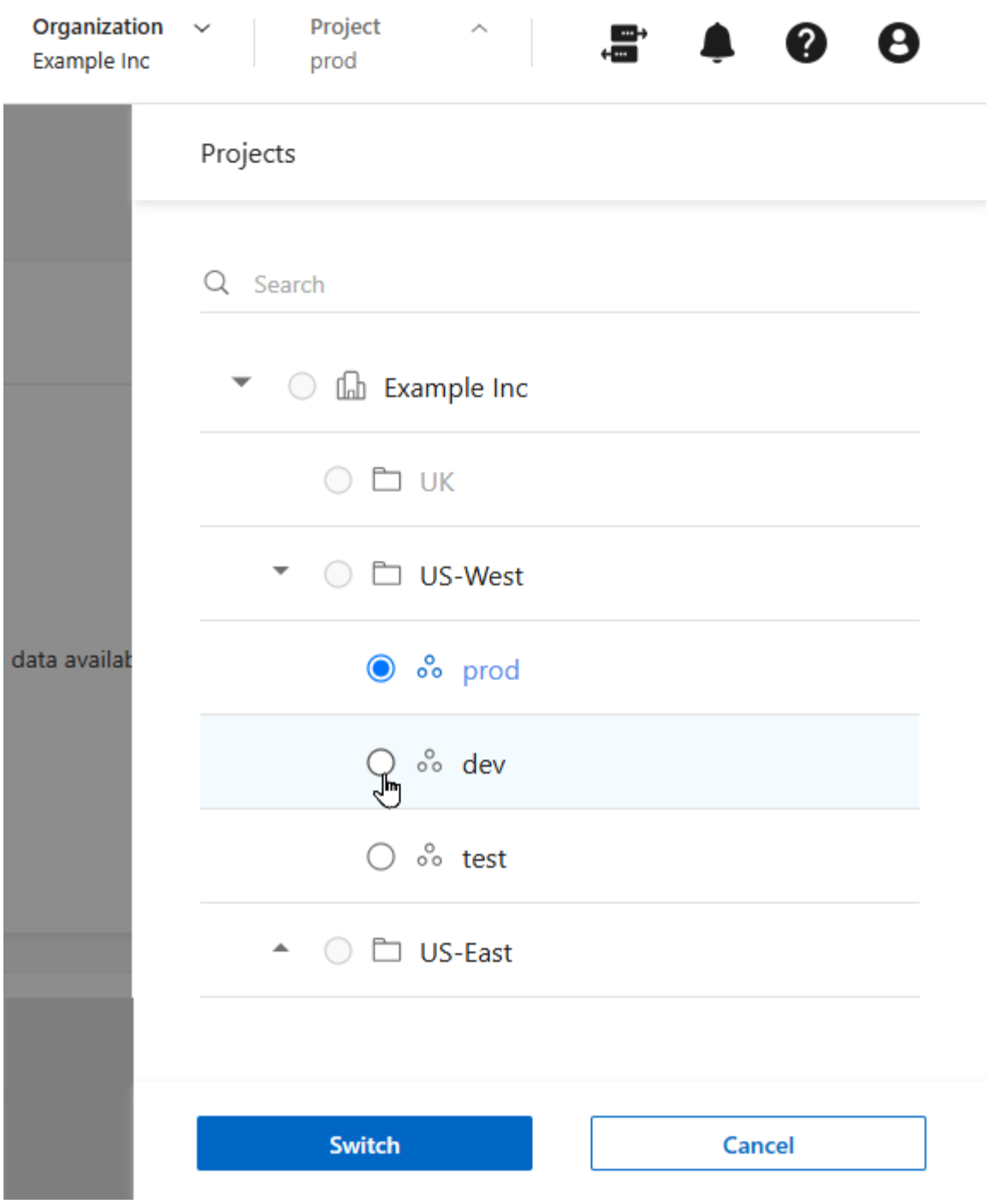
在项目之间切换

如果您的组织包含多个项目并且您有权访问这些项目，则您可以随时在它们之间切换。

在查看任何*身份和访问*页面时，您无法切换到另一个项目。

步骤

1. 在控制台的顶部标题中，选择*项目*。
2. 浏览您组织中的文件夹和项目，选择您想要的项目，然后选择*切换*。



在控制台代理之间切换

如果您有多个控制台代理，您可以在它们之间切换以查看与特定代理关联的系统。

步骤

1. 在控制台的顶部标题中，选择代理图标。
2. 选择另一个代理，然后选择*切换*。

相关信息

"将代理与文件夹和项目关联" 。

相关信息

- "了解NetApp Console中的身份和访问权限"
- "开始使用身份和访问权限"
- "了解身份和访问 API"

组织和项目 ID

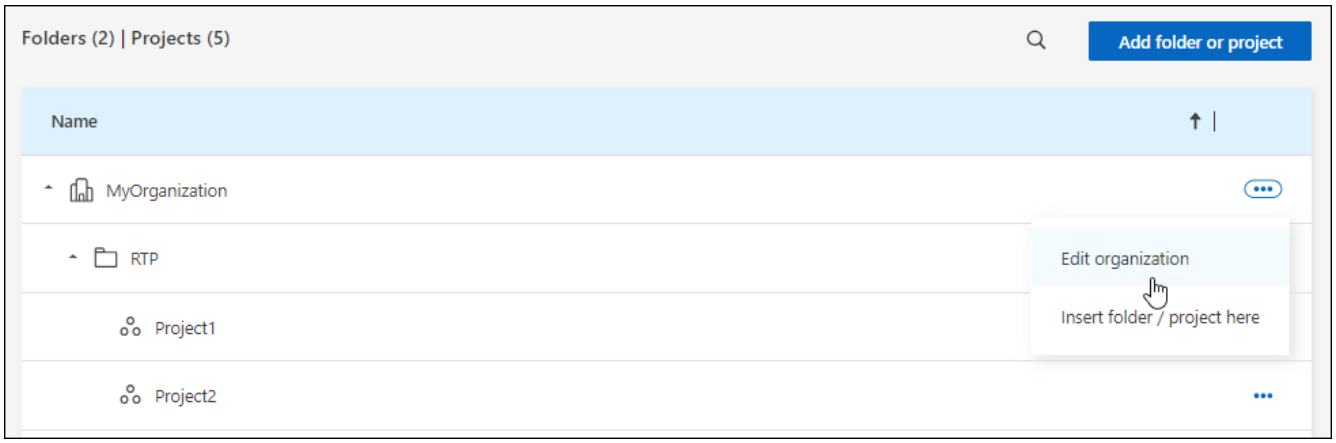
您的NetApp Console组织有一个名称和一个 ID。您可以为您的组织选择一个名称以帮助识别它。您可能还需要检索某些集成的组织 ID。

重命名您的组织

您可以重命名您的组织。如果您支持的不仅仅是组织，这将很有帮助。

步骤

1. 选择*管理>身份和访问*。
2. 选择*组织*。
3. 从“组织”页面，导航到表格的第一行，选择 ••• 然后选择*编辑组织*。



4. 输入新的组织名称并选择*应用*。

获取组织 ID

组织 ID 用于与控制台的某些集成。

您可以从组织页面查看组织 ID，并根据需要将其复制到剪贴板。

步骤

1. 选择*管理>身份和访问*>*组织*。
2. 在*组织*页面上，在摘要栏中查找您的组织 ID 并将其复制到剪贴板。您可以保存它以供以后使用，或者直接将其复制到需要使用它的地方。

获取项目ID

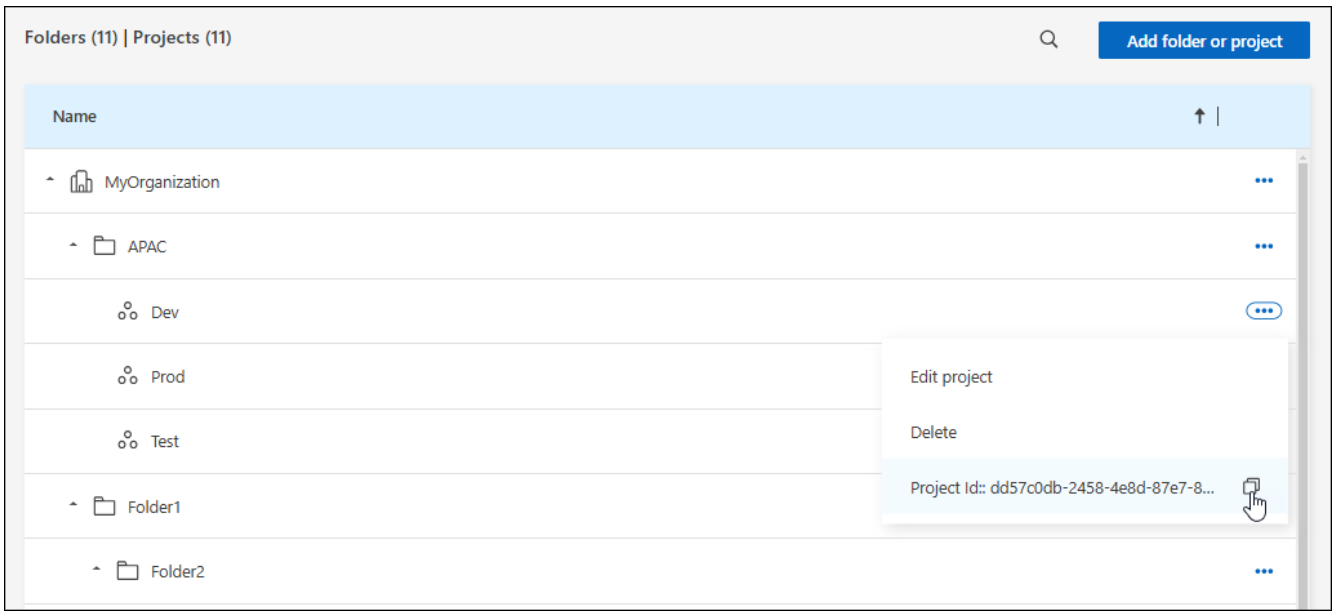
如果您使用 API，则需要获取项目的 ID。例如，创建Cloud Volumes ONTAP系统时。

步骤

1. 从“组织”页面，导航到表中的项目并选择 •••

   显示项目 ID。

2. 要复制 ID，请选择复制按钮。



相关信息

- "了解身份和访问管理"
- "开始使用身份和访问权限"
- "了解身份和访问 API"

监控或审计 IAM 活动

如果您需要监控或审计与身份和访问相关的已完成的操作，您可以从审计页面查看详细信息。例如，您可能想要验证谁向组织添加了成员或者项目是否已成功删除。

步骤

1. 选择“管理”>“审计”。
2. 在*审计*页面上，使用过滤器缩小结果范围。选择*服务*，然后选择*租赁*。
3. 使用任何其他过滤器来更改表中显示的操作。

   例如，您可以使用*用户*过滤器来显示与特定用户帐户相关的操作。

NetApp Console访问角色

了解NetApp Console访问角色

NetApp Console中的身份和访问管理 (IAM) 提供了预定义的角色，您可以将这些角色分配给组织中不同资源层次的成员。在分配这些角色之前，您应该了解每个角色包含的权限。角色分为以下类别：平台、应用程序和数据服务。

平台角色

平台角色授予NetApp Console管理权限，包括角色分配和用户管理。控制台具有多种平台角色。

平台角色	职责
"组织管理员"	允许用户不受限制地访问组织内的所有项目和文件夹，向任何项目或文件夹添加成员，以及执行任何任务和使用任何没有明确关联角色的数据服务。具有此角色的用户可以通过创建文件夹和项目、分配角色、添加用户以及管理系统（如果他们拥有适当的凭据）来管理您的组织。这是唯一可以创建控制台代理的访问角色。
"文件夹或项目管理员"	允许用户不受限制地访问分配的项目和文件夹。可以将成员添加到他们管理的文件夹或项目中，以及执行任何任务并在他们被分配的文件夹或项目内的资源上使用任何数据服务或应用程序。文件夹或项目管理员无法创建控制台代理。
"联盟管理员"	允许用户使用控制台创建和管理联合，从而实现单点登录 (SSO)。
"联邦查看器"	允许用户使用控制台查看现有的联合。无法创建或管理联盟。
"合作伙伴管理员"	允许用户创建和管理合作关系。
"合作伙伴查看器"	允许用户查看现有的合作关系。无法创建或管理合作关系。
"超级管理员"	为用户提供管理员角色的子集。此角色专为可能不需要在多个用户之间分配控制台职责的小型组织而设计。
"超级观众"	为用户提供子集查看者角色。此角色专为可能不需要在多个用户之间分配控制台职责的小型组织而设计。

应用程序角色

以下是应用程序类别中的角色列表。每个角色在其指定范围内授予特定的权限。没有所需应用程序或平台角色的用户无法访问相应的应用程序。

应用程序角色	职责
"Google Cloud NetApp Volumes管理员"	具有Google Cloud NetApp Volumes角色的用户可以发现和管理Google Cloud NetApp Volumes。
"Google Cloud NetApp Volumes查看器"	具有Google Cloud NetApp Volumes用户角色的用户可以查看Google Cloud NetApp Volumes。
"Keystone管理员"	具有Keystone管理员角色的用户可以创建服务请求。允许用户监控和查看他们正在访问的Keystone租户内的使用情况、资源和管理详细信息。
"Keystone查看器"	具有Keystone查看者角色的用户不能创建服务请求。允许用户监控和查看他们正在访问的Keystone租户内的消费、资产和管理信息。

应用程序角色	职责
ONTAP调解器设置角色	具有ONTAP调解器设置角色的服务帐户可以创建服务请求。服务帐户中需要此角色来配置"ONTAP云调解器"。
"运营支持分析师"	提供对警报和监控工具的访问以及输入和管理支持案例的能力。
"存储管理员"	管理存储健康和治理功能，发现存储资源，以及修改和删除现有系统。
"存储查看器"	查看存储健康和治理功能，以及查看以前发现的存储资源。无法发现、修改或删除现有的存储系统。
"系统健康专家"	管理存储和健康和治理功能，存储管理员的所有权限，但不能修改或删除现有系统。

数据服务角色

以下是数据服务类别中的角色列表。每个角色在其指定范围内授予特定的权限。没有所需数据服务角色或平台角色的用户将无法访问数据服务。

数据服务角色	职责
"备份和恢复超级管理员"	在NetApp Backup and Recovery中执行任何操作。
"备份和恢复管理员"	执行本地快照备份、复制到二级存储以及备份到对象存储。
"备份和恢复恢复管理员"	恢复备份和恢复中的工作负载。
"备份和恢复克隆管理员"	在备份和恢复中克隆应用程序和数据。
"备份和恢复查看器"	查看备份和恢复信息。
"灾难恢复管理员"	在NetApp Disaster Recovery服务中执行任何操作。
"灾难恢复故障转移管理员"	执行故障转移和迁移。
"灾难恢复应用程序管理员"	创建复制计划、更改复制计划并启动测试故障转移。
"灾难恢复查看器"	仅查看信息。
分类查看器	允许用户查看NetApp Data Classification扫描结果。具有此角色的用户可以查看合规性信息并生成他们有权访问的资源的报告。这些用户无法启用或禁用卷、存储桶或数据库模式的扫描。分类功能没有管理员角色。
"勒索软件抵御能力管理员"	管理NetApp Ransomware Resilience的“保护”、“警报”、“恢复”、“设置”和“报告”选项卡上的操作。
"勒索软件恢复力查看器"	在 Ransomware Resilience 中查看工作负载数据、查看警报数据、下载恢复数据和下载报告。
"勒索软件恢复用户行为管理员"	在勒索软件恢复中配置、管理和查看可疑用户行为检测、警报和监控。
"勒索软件恢复用户行为查看器"	查看勒索软件恢复中的可疑用户行为警报和见解。
SnapCenter管理员	提供使用NetApp Backup and Recovery从本地ONTAP集群备份应用程序快照的功能。具有此角色的成员可以完成以下操作：* 从“备份和恢复”>“应用程序”完成任何操作* 管理他们具有权限的项目和文件夹中的所有系统* 使用所有NetApp Console服务SnapCenter没有查看者角色。

相关链接

- "了解NetApp Console身份和访问管理"
- "开始使用NetApp Console IAM"
- "管理NetApp Console成员及其权限"
- "了解NetApp Console IAM 的 API"

NetApp Console平台访问角色

为用户分配平台角色，以授予管理NetApp Console、分配角色、添加用户、创建控制台代理和管理联合的权限。

大型跨国组织的组织角色示例

XYZ 公司按地区（北美、欧洲和亚太地区）组织数据存储访问，从而提供区域控制和集中监督。

XYZ 公司控制台中的*组织管理员*为每个区域创建一个初始组织和单独的文件夹。每个区域的*文件夹或项目管理员*在该区域的文件夹中组织项目（及相关资源）。

具有“文件夹或项目管理员”角色的区域管理员通过添加资源和用户来主动管理他们的文件夹。这些区域管理员还可以添加、删除或重命名他们管理的文件夹和项目。*组织管理员*继承任何新资源的权限，保持整个组织的存储使用情况的可见性。

在同一个组织内，一名用户被分配了*联合管理员*角色来管理该组织与其企业 IdP 的联合。该用户可以添加或删除联合组织，但不能管理组织内的用户或资源。*组织管理员*为用户分配*联合查看者*角色，以检查联合状态并查看联合组织。

下表列出了每个控制台平台角色可以执行的操作。

组织管理角色

任务	组织管理员	文件夹或项目管理员
创建代理	是	否
从控制台创建、修改或删除系统（添加或发现系统）	是	是
创建文件夹和项目，包括删除	是	否
重命名现有文件夹和项目	是	是
分配角色并添加用户	是	是
将资源与文件夹和项目关联	是	是
将代理与文件夹和项目关联	是	否
从文件夹和项目中删除代理	是	否
管理代理（编辑证书、设置等）	是	否
从管理 > 凭证管理凭证	是	是
创建、管理和查看联合	是	否
通过控制台注册支持并提交案例	是	是

任务	组织管理员	文件夹或项目管理员
使用与显式访问角色无关的数据服务	是	是
查看审核页面和通知	是	是

联盟角色

任务	联盟管理员	联邦查看器
创建联盟	是	否
验证域名	是	否
将域添加到联合	是	否
禁用和删除联盟	是	否
测试联盟	是	否
查看联盟及其详细信息	是	是

合作伙伴角色

任务	合作伙伴管理员	合作伙伴查看器
可以建立合作关系	是	否
为合作伙伴成员分配角色	是	否
可以向合作关系添加成员	是	否
可以查看组织合作关系详细信息	是	是

超级管理员和查看者角色

*超级管理员*角色提供管理控制台功能、存储和数据服务的完全访问权限。这个角色适合那些监督行政和治理的人。相比之下，“超级查看者”角色提供只读访问权限，非常适合需要查看信息而不进行更改的审计员或利益相关者。

组织应谨慎使用*超级管理员*访问权限，以最大限度地降低安全风险并符合最小特权原则。大多数组织应该分配具有必要权限的细粒度角色，以降低风险并提高可审计性。

超级角色示例

ABC 公司拥有一个由五人组成的小团队，利用NetApp Console进行数据服务和存储管理。他们没有分配多个角色，而是将“超级管理员”角色分配给两名高级团队成员，由他们负责所有管理任务，包括用户管理和资源配置。其余三名团队成员被分配了*超级查看者*角色，允许他们监控存储健康和数据服务状态，但无法修改设置。

角色	继承的角色
超级管理员	• 组织管理员 • 文件夹或项目管理员 • 联盟管理员 • 合作伙伴管理员 • 勒索软件抵御能力管理员 • 灾难恢复管理员 • 备份超级管理员 • 存储管理员 • Keystone管理员 • Google Cloud NetApp Volumes管理员
超级观众	• 组织查看器 • 联邦查看器 • 合作伙伴查看器 • 勒索软件恢复力查看器 • 灾难恢复查看器 • 备份查看器 • 存储查看器 • Keystone查看器 • Google Cloud NetApp Volumes查看器

应用程序角色

NetApp Console中的Google Cloud NetApp Volumes角色

您可以为用户分配以下角色，以便他们能够访问NetApp Console中的Google Cloud NetApp Volumes。

Google Cloud NetApp Volumes使用以下角色：

- * Google Cloud NetApp Volumes管理员*：在控制台中发现和管理Google Cloud NetApp Volumes 。
- * Google Cloud NetApp Volumes查看器*：在控制台中查看Google Cloud NetApp Volumes 。

NetApp Console中的Keystone访问角色

Keystone角色提供对Keystone仪表板的访问权限，并允许用户查看和管理他们的Keystone订阅。 Keystone角色有两种： Keystone管理员和Keystone查看者。这两个角色的主要区

别在于他们在Keystone中可以采取的行动。 Keystone管理员角色是唯一允许创建服务请求或修改订阅的角色。

NetApp Console中的**Keystone**角色示例

XYZ 公司有四名来自不同部门的存储工程师查看Keystone订阅信息。虽然所有这些用户都需要监控Keystone订阅，但只有团队负责人才被允许提出服务请求。团队中的三名成员被赋予 * Keystone查看者* 角色，而团队负责人被赋予 * Keystone管理员* 角色，以便对公司的服务请求进行控制。

下表列出了每个Keystone角色可以执行的操作。

特征和动作	**Keystone**管理员	**Keystone**查看器
查看以下选项卡：订阅、资产、监控和管理	是	是
* Keystone订阅页面*：		
查看订阅	是	是
修改或续订	是	否
* Keystone资产页面*：		
查看资产	是	是
管理资产	是	否
* Keystone警报页面*：		
查看警报	是	是
管理警报	是	否
为自己创建提醒	是	是
Licenses and subscriptions：		
可以查看许可证和订阅	是	是
* Keystone报告页面*：		
下载报告	是	是
管理报告	是	是
为自己创建报告	是	是
服务请求：		
创建服务请求	是	否

特征和动作	**Keystone**管理员	**Keystone**查看器
查看组织内任何用户创建的服务请求	是	是

NetApp Console的运营支持分析师访问角色

您可以将运营支持分析师角色分配给用户，以便他们能够访问警报和监控功能。具有此角色的用户还可以打开支持案例。

运营支持分析师

任务	可以执行
从“设置”>“凭证”管理自己的用户凭证	是
查看发现的资源	是
通过控制台注册支持并提交案例	是
是	查看审核页面和通知
是	查看、下载和配置警报

NetApp Console的存储访问角色

您可以为用户分配以下角色，以便他们访问NetApp Console中的存储管理功能。您可以为用户分配管理角色来管理存储或分配查看者角色来监控。

NetApp Console合作伙伴 API 不提供这些角色。

管理员可以为用户分配以下存储资源和功能的存储角色：

存储资源：

- 本地ONTAP集群
- StorageGRID
- E 系列

控制台服务和功能：

- 数字顾问
- 软件更新
- 生命周期规划
- 可持续性

NetApp Console中的存储角色示例

XYZ 公司是一家跨国公司，拥有庞大的存储工程师和存储管理员团队。它们允许该团队管理其所在地区的存储资产，同时限制对核心控制台任务（如用户管理、代理创建和许可证管理）的访问。

在一个由 12 人组成的团队中，有两名用户被赋予“存储查看者”角色，这使他们能够监控与他们被分配到的控制台项目相关的存储资源。其余九人被赋予*存储管理员*角色，包括管理软件更新、通过控制台访问ONTAP系统管理器以及发现存储资源（添加系统）的能力。团队中的一名成员被赋予*系统健康专家*角色，以便他们可以管理其所在区域的存储资源的健康状况，但不能修改或删除任何系统。此人还可以对其所分配项目的存储资源执行软件更新。

该组织还有两个具有“组织管理员”角色的用户，他们可以管理控制台的所有方面，包括用户管理、代理创建和许可证管理，还有几个具有“文件夹或项目管理员”角色的用户，他们可以对分配到的文件夹和项目执行控制台管理任务。

下表显示了每个存储角色执行的操作。

特征和动作	存储管理员	系统健康专家	存储查看器
存储管理：			
发现新资源（创建系统）	是	是	否
查看发现的系统	是	是	否
从控制台删除系统	是	否	否
修改系统	是	否	否
创建代理	否	否	否
数字顾问			
查看所有页面和功能	是	是	是
Licenses and subscriptions			
查看所有页面和功能	否	否	否
软件更新			
查看登陆页面和建议	是	是	是
审查潜在的版本建议和主要优点	是	是	是
查看集群的更新详细信息	是	是	是
运行更新前检查并下载升级计划	是	是	是
安装软件更新	是	是	否
生命周期规划			
审查容量规划状态	是	是	是

特征和动作	存储管理员	系统健康专家	存储查看器
选择下一步行动（最佳实践、层级）	是	否	否
将冷数据分层到云存储并释放存储空间	是	是	否
设置提醒	是	是	是
可持续性			
查看仪表板和建议	是	是	是
下载报告数据	是	是	是
编辑碳减排百分比	是	是	否
修复建议	是	是	否
推迟建议	是	是	否
系统管理员访问			
可以输入凭证	是	是	否
证书			
用户凭据	是	是	否

数据服务角色

NetApp Console中的NetApp Backup and Recovery角色

您可以为用户分配以下角色，以便他们访问控制台内的NetApp Backup and Recovery 。备份和恢复角色使您可以灵活地为用户分配特定于他们需要在组织内完成的任务的角色。如何分配角色取决于您自己的业务和存储管理实践。

该服务使用特定于NetApp Backup and Recovery 的以下角色。

- 备份和恢复超级管理员：在NetApp Backup and Recovery中执行任何操作。
- 备份和恢复备份管理员：在NetApp Backup and Recovery中执行备份到本地快照、复制到二级存储以及备份到对象存储操作。
- 备份和恢复恢复管理员：使用NetApp Backup and Recovery恢复工作负载。
- 备份和恢复克隆管理：使用NetApp Backup and Recovery克隆应用程序和数据。
- 备份和恢复查看器：查看NetApp Backup and Recovery中的信息，但不执行任何操作。

有关所有NetApp Console访问角色的详细信息，请参阅 "控制台设置和管理文档"。

用于常见操作的角色

下表列出了每个NetApp Backup and Recovery角色可以针对所有工作负载执行的操作。

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复克隆管理员	备份和恢复查看器
添加、编辑或删除主机	是	否	否	否	否
安装插件	是	否	否	否	否
添加凭据（主机、实例、vCenter）	是	否	否	否	否
查看仪表板和所有选项卡	是	是	是	是	是
开始免费试用	是	否	否	否	否
启动工作负载发现	否	是	是	是	否
查看许可证信息	是	是	是	是	是
激活许可证	是	否	否	否	否
查看主机	是	是	是	是	是
时间表：					
激活计划	是	是	是	是	否
暂停时间表	是	是	是	是	否
政策与保护：					
查看保护计划	是	是	是	是	是
创建、修改或删除保护计划	是	是	否	否	否
恢复工作负载	是	否	是	否	否
创建、拆分或删除克隆	是	否	否	是	否
创建、修改或删除策略	是	是	否	否	否
报告：					
查看报告	是	是	是	是	是

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复克隆管理员	备份和恢复查看器
创建报告	是	是	是	是	否
删除报告	是	否	否	否	否
从**SnapCenter**导入并管理主机：					
查看导入的SnapCenter数据	是	是	是	是	是
从SnapCenter导入数据	是	是	否	否	否
管理（迁移）主机	是	是	否	否	否
配置设置：					
配置日志目录	是	是	是	否	否
关联或删除实例凭证	是	是	是	否	否
桶：					
查看存储桶	是	是	是	是	是
创建、编辑或删除存储桶	是	是	否	否	否

用于特定于工作负载的操作的角色

下表列出了每个NetApp Backup and Recovery角色可以针对特定工作负载执行的操作。

Kubernetes 工作负载

该表显示了每个NetApp Backup and Recovery角色可以针对特定于 Kubernetes 工作负载的操作执行的操作。

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
查看集群、命名空间、存储类别和 API 资源	是	是	是	是
添加新的 Kubernetes 集群	是	是	否	否
更新集群配置	是	否	否	否
从管理中删除集群	是	否	否	否
查看应用程序	是	是	是	是

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
创建和定义新的应用程序	是	是	否	否
更新应用程序配置	是	是	否	否
从管理中删除应用程序	是	是	否	否
查看受保护的资源和备份状态	是	是	是	是
创建备份并使用策略保护应用程序	是	是	否	否
取消保护应用程序并删除备份	是	是	否	否
查看恢复点和资源查看器结果	是	是	是	是
从恢复点还原应用程序	是	否	是	否
查看 Kubernetes 备份策略	是	是	是	是
创建 Kubernetes 备份策略	是	是	是	否
更新备份策略	是	是	是	否
删除备份策略	是	是	是	否
查看执行钩子和钩子源	是	是	是	是
创建执行钩子和钩子源	是	是	是	否
更新执行钩子和钩子源	是	是	是	否
删除执行钩子和钩子源	是	是	是	否
查看执行钩子模板	是	是	是	是
创建执行钩子模板	是	是	是	否
更新执行钩子模板	是	是	是	否
删除执行钩子模板	是	是	是	否

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
查看工作负载摘要和分析仪表板	是	是	是	是
查看StorageGRID存储桶和存储目标	是	是	是	是

NetApp Console中的NetApp Disaster Recovery角色

您可以为用户分配以下角色，以便他们访问控制台内的NetApp Disaster Recovery。灾难恢复角色使您可以灵活地为用户分配特定于他们需要在组织内完成的任务的角色。如何分配角色取决于您自己的业务和存储管理实践。

灾难恢复使用以下角色：

- 灾难恢复管理员：执行任何操作。
- 灾难恢复故障转移管理：执行故障转移和迁移。
- 灾难恢复应用程序管理员：创建复制计划。修改复制计划。开始测试故障转移。
- 灾难恢复查看器：仅查看信息。

下表列出了每个角色可以执行的操作。

特征和动作	灾难恢复管理员	灾难恢复故障转移管理员	灾难恢复应用程序管理员	灾难恢复查看器
查看仪表板和所有选项卡	是	是	是	是
开始免费试用	是	否	否	否
启动工作负载发现	是	否	否	否
查看许可证信息	是	是	是	是
激活许可证	是	否	是	否
在“站点”选项卡上：				
查看网站	是	是	是	是
添加、修改或删除站点	是	否	否	否
在复制计划选项卡上：				
查看复制计划	是	是	是	是
查看复制计划详细信息	是	是	是	是

特征和动作	灾难恢复管理员	灾难恢复故障转移管理员	灾难恢复应用程序管理员	灾难恢复查看器
创建或修改复制计划	是	是	是	否
创建报告	是	否	否	否
查看快照	是	是	是	是
执行故障转移测试	是	是	是	否
执行故障转移	是	是	否	否
执行故障回复	是	是	否	否
执行迁移	是	是	否	否
在资源组选项卡上：				
查看资源组	是	是	是	是
创建、修改或删除资源组	是	否	是	否
在“作业监控”选项卡上：				
查看职位	是	否	是	是
取消作业	是	是	是	否

NetApp Console的勒索软件恢复访问角色

勒索软件恢复角色为用户提供对NetApp Ransomware Resilience的访问权限。勒索软件恢复能力支持以下角色：

基线角色

- 勒索软件恢复管理员 - 配置勒索软件恢复设置；调查并响应加密警报
- 勒索软件恢复力查看器 - 查看加密事件、报告和发现设置

用户行为活动角色"可疑用户活动检测"警报提供对文件活动事件等数据的可见性；这些警报包括文件名和用户执行的文件操作（例如读取、写入、删除、重命名）。为了限制这些数据的可见性，只有具有这些角色的用户才能管理或查看这些警报。

- 勒索软件恢复用户行为管理员 - 激活可疑用户活动检测，调查并响应可疑用户活动警报
- 勒索软件恢复用户行为查看器 - 查看可疑用户活动警报

用户行为角色不是独立角色；它们旨在添加到勒索软件恢复管理员或查看者角色中。有关详细信息，请参阅 [用户行为角色]。

有关每个角色的详细描述，请参阅下表。

基线角色

下表描述了勒索软件恢复管理员和查看者角色可执行的操作。

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
查看仪表板和所有选项卡	是	是
在仪表板上更新推荐状态	是	否
开始免费试用	是	否
启动工作负载发现	是	否
启动工作负载的重新发现	是	否
在“保护”选项卡上：		
添加、修改或删除加密策略的保护计划	是	否
保护工作负载	是	否
通过数据分类识别敏感数据的暴露	是	否
列出保护计划和细节	是	是
列出保护组	是	是
查看保护组详细信息	是	是
创建、编辑或删除保护组	是	否
下载数据	是	是
在“警报”选项卡上：		
查看加密警报和警报详细信息	是	是
编辑加密事件状态	是	否

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
标记加密警报以供恢复	是	否
查看加密事件详细信息	是	是
解除或解决加密事件	是	否
获取加密事件中受影响文件的完整列表	是	否
下载加密事件警报数据	是	是
阻止用户（使用工作负载安全代理配置）	是	否
在“恢复”选项卡上：		
下载加密事件中受影响的文件	是	否
从加密事件中恢复工作负载	是	否
从加密事件下载恢复数据	是	是
下载加密事件报告	是	是
在“设置”选项卡上：		
添加或修改备份目标	是	否
列出备份目的地	是	是
查看已连接的 SIEM 目标	是	是
添加或修改 SIEM 目标	是	否
配置准备演练	是	否
开始、重置或编辑准备情况演练	是	否
审查准备演习状态	是	是
更新发现配置	是	否
查看发现配置	是	是
在“报告”选项卡上：		

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
下载报告	是	是

用户行为角色

要配置可疑用户行为设置并响应警报，用户必须具有勒索软件恢复用户行为管理员角色。要仅查看可疑用户行为警报，用户应具有勒索软件恢复用户行为查看者角色。

应将用户行为角色授予具有现有勒索软件恢复管理员或查看者权限且需要访问"可疑用户活动设置和警报"。例如，具有勒索软件恢复管理员角色的用户应该获得勒索软件恢复用户行为管理员角色来配置用户活动代理并阻止或解除阻止用户。不应将勒索软件恢复用户行为管理员角色授予勒索软件恢复查看者。

要激活可疑用户活动检测，您必须具有控制台组织管理员角色。

下表描述了勒索软件恢复用户行为管理员和查看者角色可执行的操作。

特征和动作	勒索软件恢复用户行为管理员	勒索软件恢复用户行为查看器
在“设置”选项卡上：		
创建、修改或删除用户活动代理	是	否
创建或删除用户目录连接器	是	否
暂停或恢复数据收集器	是	否
进行数据泄露准备演习	是	否
在“保护”选项卡上：		
添加、修改或删除可疑用户行为策略的保护计划	是	否
在“警报”选项卡上：		
查看用户活动警报和警报详细信息	是	是
编辑用户活动事件状态	是	否
标记用户活动警报以供恢复	是	否
查看用户活动事件详细信息	是	是
解除或解决用户活动事件	是	否
获取可疑用户受影响文件的完整列表	是	是

特征和动作	勒索软件恢复用户行为管理员	勒索软件恢复用户行为查看器
下载用户活动事件警报数据	是	是
阻止或取消阻止用户	是	否
在“恢复”选项卡上：		
下载用户活动事件受影响的文件	是	否
从用户活动事件恢复工作负载	是	否
从用户活动事件下载恢复数据	是	是
从用户活动事件下载报告	是	是

合作组织

NetApp Console中的合作伙伴关系

在NetApp Console中创建组织间的合作伙伴关系，可以让合作伙伴安全地跨组织边界管理NetApp资源，从而简化协作并增强安全性。

必需角色

合作伙伴管理员"了解有关访问角色的更多信息。"

合作伙伴关系允许使用控制台中的角色驱动关系跨组织安全地管理NetApp资源。发起组织授予对其资源的访问权限，而接受组织提供被授予访问权限的用户或服务帐户。合作伙伴关系是通过自助服务工作流程建立的，使发起组织能够完全控制共享的资源、分配的角色以及根据需要加入、管理或撤销合作伙伴访问权限的能力。

客户可以授权 MSP 或经销商来管理NetApp环境，而无需复杂的设置。客户可以控制合作伙伴可以访问哪些集群以及他们拥有哪些角色，并且可以随时撤销访问权限以维护安全性和合规性。

作为合作伙伴，您可以获得跨客户环境的集中可见性和控制力。您可以轻松切换到客户的组织来管理资源、运行数据服务并在定义的边界内监控健康状况，从而减少自定义工具并确保与每个客户的政策保持一致。

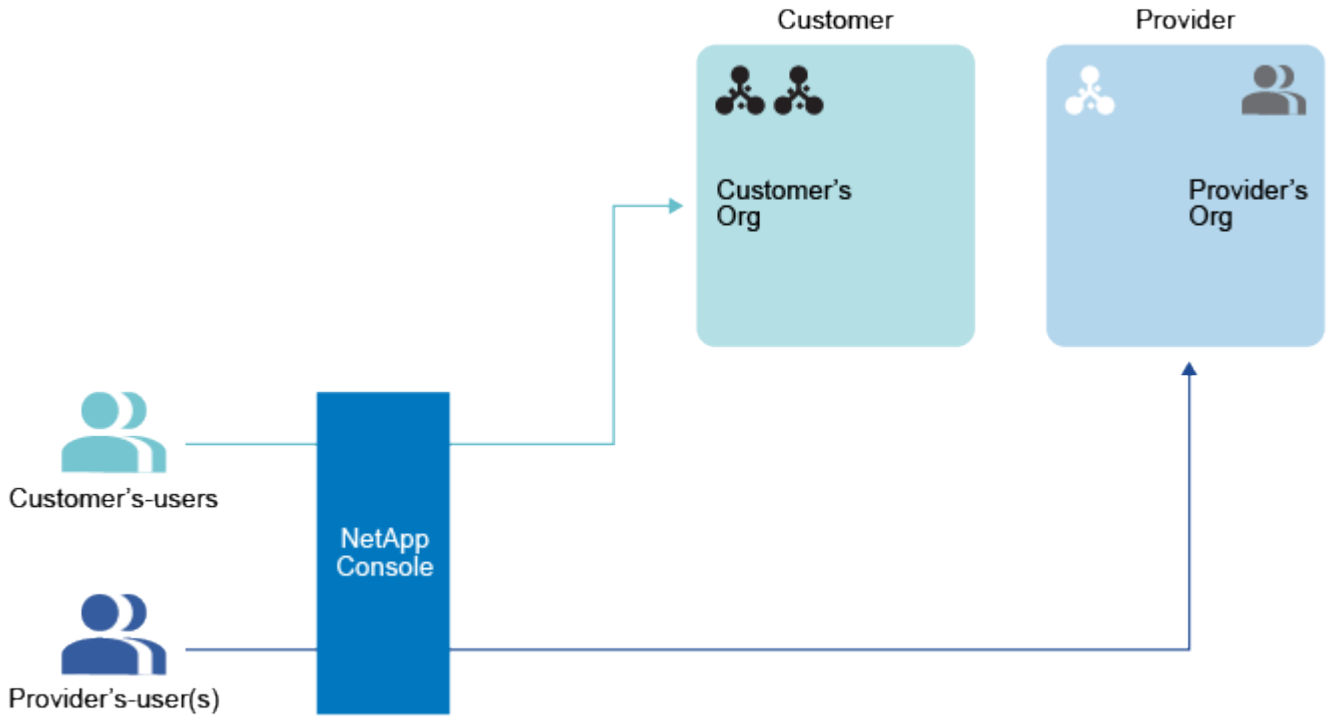
1. 为一个或多个用户分配合作伙伴管理员角色

为发起组织和接收组织中的一个或多个用户分配合作伙伴管理员角色来创建和管理合作伙伴关系。您可以将合作伙伴查看器角色分配给只需要查看合作伙伴关系而不需要管理的用户。

2. 与发起组织共享您的组织 **ID**

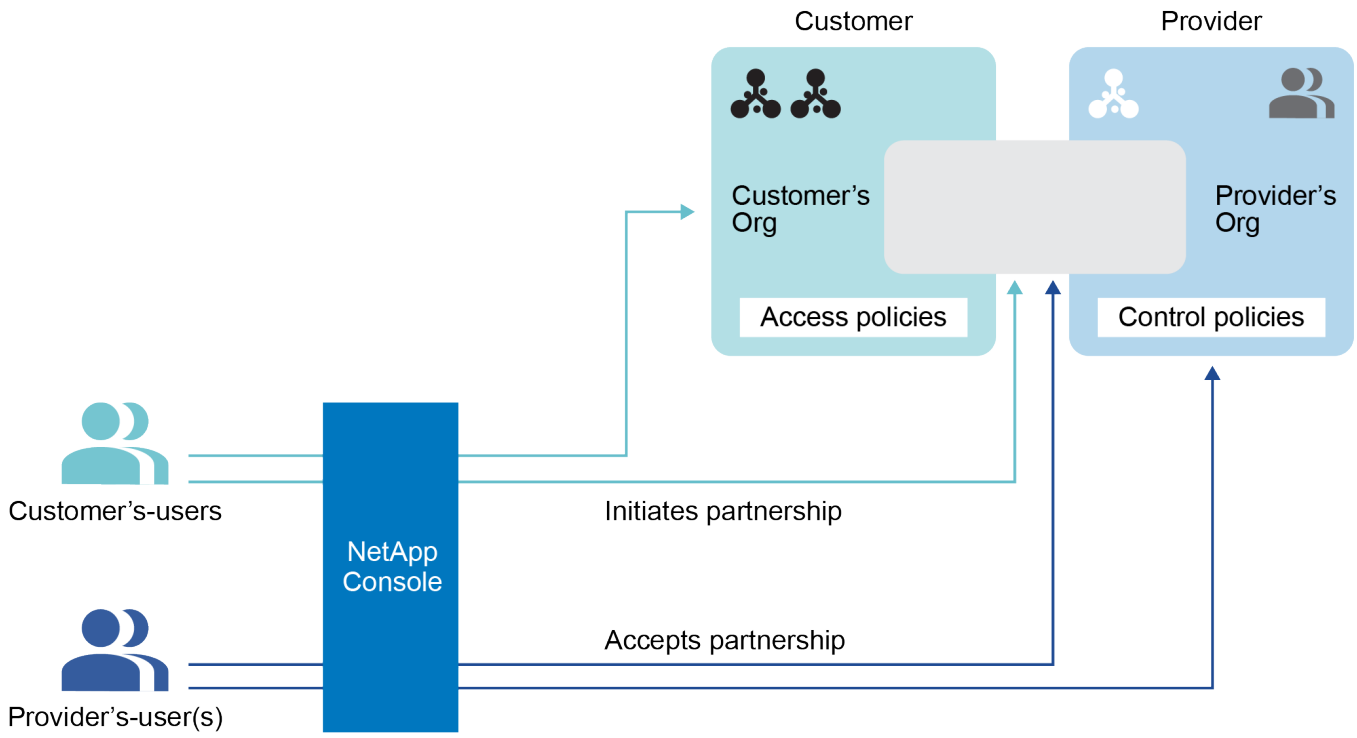
要发起合作关系，发起者必须知道目标组织的组织 ID。只有相应的组织可以访问此组织 ID。通过电子邮件或其他方式直接与NetApp Console之外的发起组织共享。

发起组织是授予其资源访问权限的组织。



3 在**NetApp Console**内建立合作关系

发起合作关系的组织通过从NetApp Console发送合作关系请求来发起合作关系。



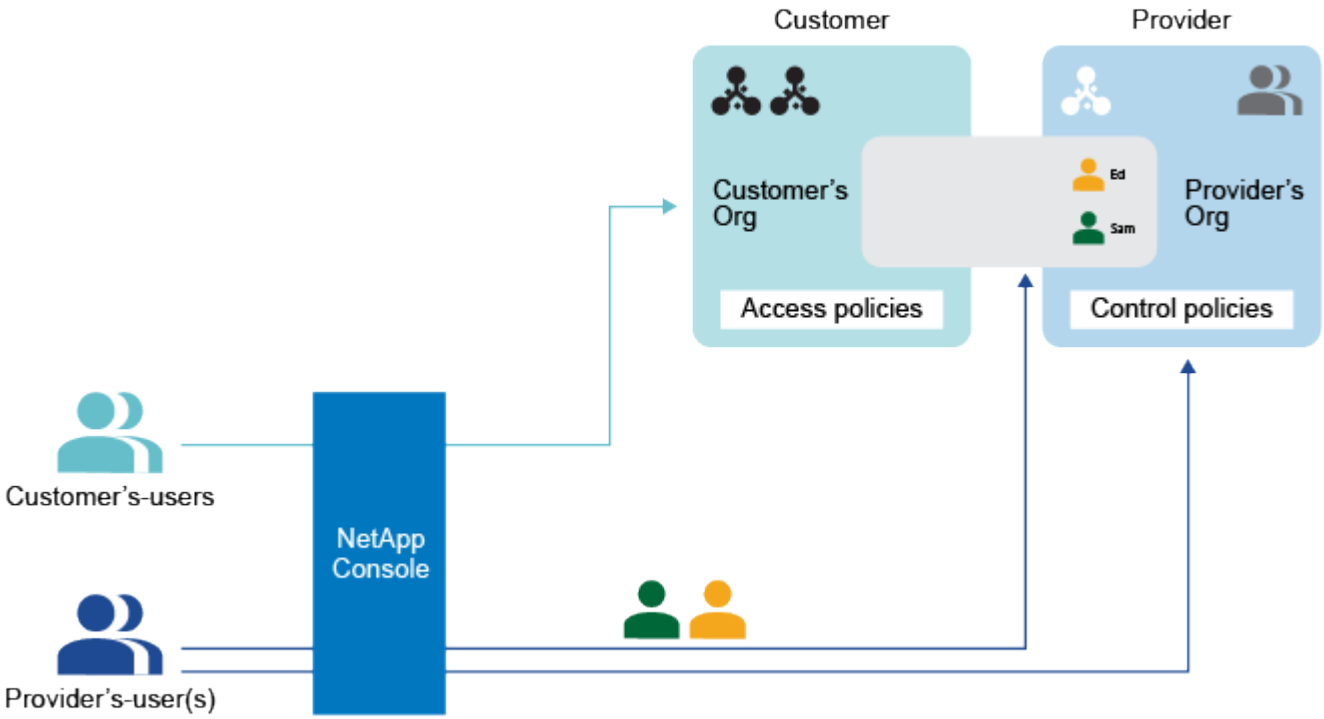
4 批准合作

接收组织必须接受该请求。

接收组织是被授予资源访问权限的组织。

5 将用户分配到合作关系

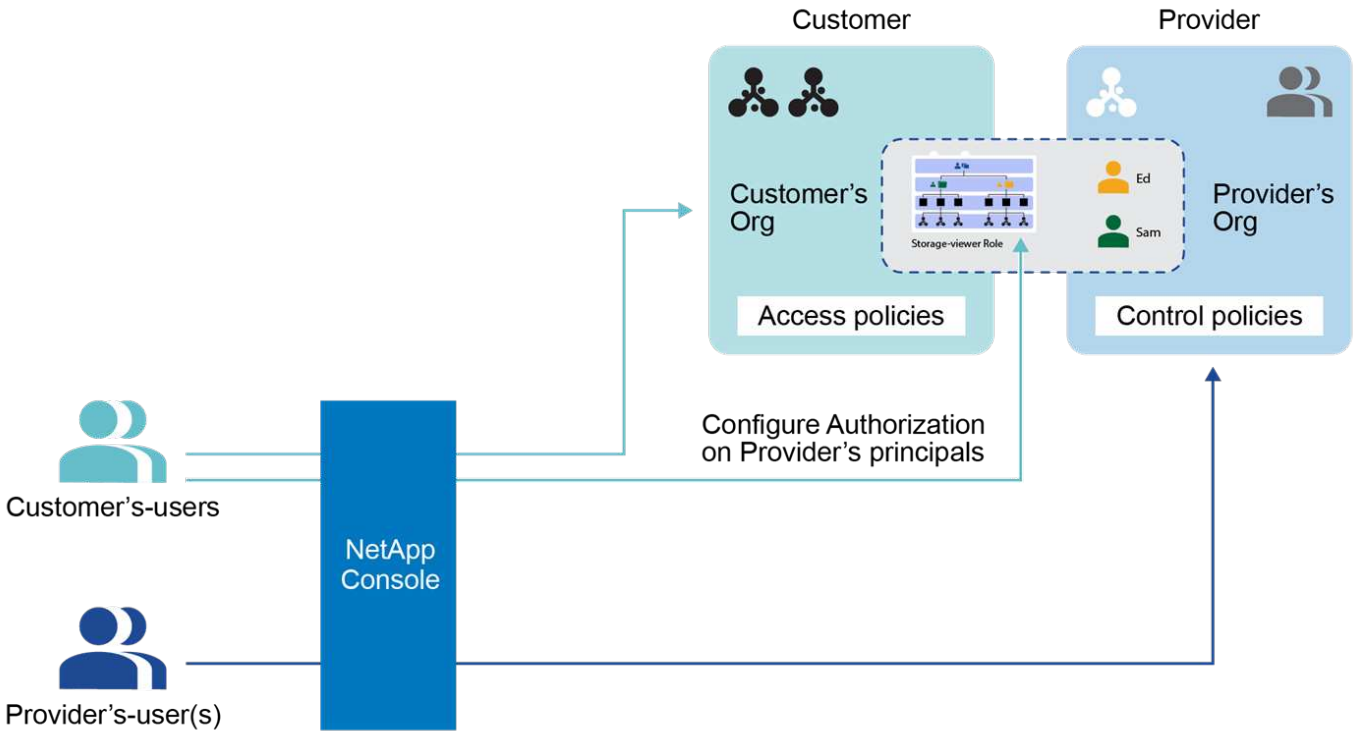
接收组织将您组织中的特定用户或服务帐户分配给合作伙伴关系。发起组织为这些用户分配角色。



6 授予指定用户对资源的访问权限

如果您是发起组织，您可以向分配给合作关系的用户授予特定资源的访问权限。您可以随时撤销访问权限。

您可以通过为组织内的特定项目或文件夹分配角色来实现此目的。



在NetApp Console中管理合作伙伴关系

建立合作伙伴关系，在您的组织和值得信赖的合作伙伴之间建立安全、可管理的连接，以实现协作式NetApp资源管理。

通过合作伙伴关系，您可以通过控制台中的角色驱动关系安全地跨边界管理NetApp资源。发起组织授予对其资源的访问权限，而接受组织提供被授予访问权限的用户或服务帐户。合作伙伴关系是通过自助服务工作流程建立的，使发起组织能够完全控制共享的资源、分配的角色以及根据需要加入、管理或撤销合作伙伴访问权限的能力。

必需角色

需要“合作伙伴关系管理员”角色来创建和管理合作伙伴关系。 *合作伙伴查看者*可以查看合作伙伴页面。"了解有关访问角色的更多信息。"

建立组织伙伴关系

如果您知道其他组织的组织 ID，您可以请求与其建立合作关系。接收组织必须批准该请求，合作关系才能继续进行。

在开始之前，请确保您拥有合作伙伴组织的组织 ID，并且已被分配 合作伙伴管理员 角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择“合作伙伴关系”选项卡。
3. 选择*添加合作伙伴关系*。
4. 在*创建合作伙伴关系*对话框中，输入请求合作伙伴的合作伙伴组织 ID，然后选择*添加*。

合作请求被发送给合作伙伴组织以供批准。您可以在*合作伙伴关系*页面上查看合作请求的状态。

批准组织合作关系

接收组织必须接受组织合作请求，合作才能继续进行。您必须具有*合作伙伴关系管理员*角色才能批准和管理合作伙伴关系。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 导航到您想要批准的合作关系并选择 ••• 然后选择*批准*。
5. 查看合作关系的详细信息，包括请求合作关系的组织的名称和组织 ID，然后选择“下一步”。
6. 可选，将组织成员添加到合作伙伴关系并选择*应用*。

   您可以随时通过*合作伙伴*页面添加其他成员。

   您添加的任何成员都会在合作伙伴的组织中可见，合作伙伴可以在其中将他们分配给资源。

结果

您批准的合作关系现在显示状态为*已建立*。任一组织中具有 **Partnership admim** 或 **Partnership viewer** 角色的用户都可以查看合作关系。

查看合作关系状态

查看您的合作关系状态。

所需角色

合作伙伴关系管理员、合作伙伴关系查看者。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已发起的合作关系”或“已接收的合作关系”选项卡。
4. 查看显示合作关系及其状态的相应表格。

禁用组织合作关系

您必须是发起组织的成员才能禁用合作关系。禁用合作关系将立即撤销您组织中与合作伙伴组织共享的任何资源的访问权限。

所需角色

合伙管理员。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已启动的合作伙伴关系”选项卡。
4. 查看显示合作关系及其状态的相应表格。
5. 导航到您想要禁用的已启动合作关系并选择 ••• 然后选择*禁用*。

管理合作组织的成员

您可以通过将用户添加到合作伙伴组织来将用户添加到合作伙伴关系。添加用户后，合作伙伴组织负责为他们分配组织中特定资源的角色。

必需角色

需要“合作伙伴关系管理员”角色来创建和管理合作伙伴关系。 *合作伙伴查看者*可以查看合作伙伴页面。"了解有关访问角色的更多信息。"

您可以随时从合作关系中移除用户。从合作关系中移除用户会立即撤销其对合作伙伴组织中任何资源的访问权限。

向合作关系添加成员

当您向合作伙伴关系添加成员时，合作伙伴组织的*合作伙伴关系管理员*必须为他们分配组织中特定资源的角色，然后他们才能访问这些资源。

将成员添加到合作伙伴关系后，这些成员将显示为合作伙伴组织中的成员，合作伙伴可以在其中为他们分配资源。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 选择操作菜单 ••• 在您想要添加成员的已建立的合作关系旁边，选择“添加成员”。
5. 选择一个或多个要添加到合作关系中的成员，然后选择*添加*。

从合作关系中移除成员

您可以随时从合作关系中移除成员。从合作关系中移除用户会立即撤销其对合作伙伴组织中任何资源的访问权限。

如果您想调整成员拥有的角色或他们可以访问的资源，合作伙伴组织的合作伙伴管理员必须进行这些更改。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 选择操作菜单 ••• 在您想要删除的成员旁边，选择“删除关联”。

5. 通过在对话框中选择“删除”来确认该操作。

查看用户的角色信息

您可以查看已分配给用户的角色以及相关资源。

您不能更改与用户关联的角色。如果您对所提供的资源或角色有任何疑问，请联系合作伙伴组织的管理员。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
5. 在表格中，展开您想要查看成员分配角色的组织、文件夹或项目的相应行，然后选择“角色”列中的数字。

为合作伙伴用户提供资源访问

您可以通过为合作伙伴用户分配组织内文件夹和项目的特定角色来授予他们访问权限。

必需角色

合伙管理员。"了解有关访问角色的更多信息。"

合作伙伴组织必须先将成员添加到合作伙伴关系中，然后您才能为他们分配组织中资源的角色。"了解如何向合作关系添加成员。"

了解合作伙伴用户的角色

您可以按照管理自己的角色的方式来管理合作伙伴组织成员的角色。然而，并非所有角色都适合合作伙伴用户。特别是，您不能授予合作伙伴用户允许软件更新的角色。更新ONTAP软件通常需要直接网络访问。

您可以为合作伙伴用户分配以下角色：

- "组织管理员"
- "文件夹或项目管理员"
- "联盟管理员"
- "联邦查看器"
- "备份和恢复管理员"
- "备份查看器"
- "恢复管理员"
- "克隆管理员"
- "灾难恢复管理员"
- "灾难恢复故障转移管理员"
- "灾难恢复应用程序管理员"

- "灾难恢复查看器"
- "运营支持分析师"
- "分类查看器"

"了解有关预定义角色的更多信息"

向合作伙伴用户添加角色

您可以通过向成员添加角色来提供对组织资源的访问权限。分配角色时，您指定一个资源和一个角色。您可以为一个用户分配多个角色。

例如，如果您有两个项目，并且希望同一个用户同时拥有这两个项目的备份和恢复管理员角色，则您需要为每个项目的用户提供该角色。同样，如果您想为同一个项目的用户提供两个不同的角色，则需要分别分配每个角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择*合作伙伴关系已启动*选项卡。
4. 选择操作菜单 ••• 在您想要查看的已建立的合作关系旁边，选择“查看详细信息”。

   *成员*列表显示合作伙伴组织已添加到合作伙伴关系的成员。

5. 选择操作菜单 ••• 在您想要分配角色的成员旁边，选择“添加角色”。
6. 要添加角色，请完成对话框中的步骤：
   - 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

     如果您选择组织或文件夹，则该成员将拥有该组织或文件夹内所有内容的权限。

   - 选择类别：选择角色类别。"了解访问角色" 。
   - 选择*角色*：选择一个角色，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。
   - 添加角色：如果您想提供对组织内其他文件夹或项目的访问权限，请选择*添加角色*，指定另一个文件夹或项目或角色类别，然后选择一个角色类别和相应的角色。
7. 选择*添加新角色*。

更改或删除合作伙伴用户的角色

您可以更改或删除分配给合作伙伴组织成员的角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择*合作伙伴关系已启动*选项卡。
4. 选择操作菜单 ••• 在您想要查看的已建立的合作关系旁边，选择“查看详细信息”。

   *成员*列表显示合作伙伴组织已添加到合作伙伴关系的成员。

5. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
6. 在表格中，展开要更改成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”以查看分配给该成员的角色。
7. 您可以更改成员的现有角色或删除角色。
   a. 要更改成员的角色，请选择要更改的角色旁边的“更改”。您只能将角色更改为同一角色类别内的角色。例如，您可以从一个数据服务角色更改为另一个数据服务角色。确认更改。
   b. 要取消分配成员的角色，请选择 🗑 取消为该成员分配相应的角色。系统会要求您确认删除。

在合作组织工作

一旦您在合作伙伴组织中被赋予角色，您就可以切换到该组织并执行您有权执行的操作。

使用组织菜单在您的组织和您有权访问的任何合作伙伴组织之间切换。"了解有关切换组织和项目的更多信息。"

您将能够看到合作伙伴组织中与您共享的资源，并根据分配给您的角色执行操作。与您的合作伙伴管理员合作，确保您拥有需要访问的资源的适当角色。

身份联合

使用NetApp Console的身份联合实现单点登录

单点登录（联合）允许用户使用其公司凭证登录NetApp Console，从而简化了登录过程并增强了安全性。您可以使用身份提供商 (IdP) 或NetApp支持站点启用单点登录 (SSO)。

所需角色

组织管理员、联盟管理员、联盟查看器。"了解有关访问角色的更多信息。"

与NetApp支持站点的身份联合

与NetApp支持站点联合允许用户使用相同的凭据登录控制台、 Active IQ Digital Advisor和其他相关应用程序。

ⓘ 如果您与NetApp支持站点联合，则您不能与您的企业身份管理提供商联合。选择最适合您组织的一种。

步骤

1. 下载并完成 "NetApp联合申请表"。
2. 将表格提交至表格中指定的电子邮件地址。

   NetApp支持团队将审核并处理您的请求。

与您的身份提供商建立联合连接

您可以与身份提供商建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的身份提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

如果您之前使用NetApp Cloud Central（控制台的外部应用程序）配置了联合，则需要使用联合页面导入联合以在控制台内进行管理。"了解如何导入您的联盟。"

支持的身份提供者

NetApp支持以下联合协议和身份提供程序：

协议

- 安全断言标记语言 (SAML) 身份提供者
- Active Directory 联合身份验证服务 (AD FS)

身份提供者

- 微软Entra ID
- Ping联邦

与**NetApp Console**联合工作流程

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与您的电子邮件域或您拥有的其他域联合。要与不同于您的电子邮件域的域联合，请首先验证您拥有该域。

1 验证您的域名（如果不使用您的电子邮件域名）

要与不同于您的电子邮件域的域联合，请验证您拥有该域。您无需任何额外步骤即可联合您的电子邮件域。

2 配置您的 **IdP** 以信任**NetApp**作为服务提供商

通过创建新应用程序并提供 ACS URL、实体 ID 或其他凭证信息等详细信息，将您的身份提供商配置为信任NetApp 。服务提供商信息因身份提供商而异，因此请参阅特定身份提供商的文档以了解详细信息。您需要与您的 IdP 管理员合作来完成此步骤。

3 在控制台中创建联合连接

提供来自身份提供商的 SAML 元数据 URL 或文件以创建连接。此信息用于建立控制台和您的身份提供者之间的信任关系。您提供的信息取决于您使用的 IdP。例如，如果您使用 Microsoft Entra ID，则需要提供客户端 ID、密钥和域。

4 在控制台中测试您的联盟

在启用联合连接之前对其进行测试。使用控制台中联合页面上的测试选项来验证您的测试用户是否可以成功进行身份验证。如果测试成功，则可以启用连接。

5 在控制台中启用您的连接

启用连接后，用户可以使用其公司凭证登录控制台。

查看相应协议或 IdP 的主题以开始：

- "与 AD FS 设置联合连接"
- "与 Microsoft Entra ID 建立联合连接"
- "使用 PingFederate 设置联合连接"
- "与 SAML 身份提供商建立联合连接"

域验证

验证联合连接的电子邮件域

如果您想要与不同于您的电子邮件域的域联合，您必须首先验证您拥有该域。您只能使用已验证的域进行联合。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

验证您的域名涉及向您的域名的 DNS 设置添加 TXT 记录。此记录用于证明您拥有该域并允许NetApp Console信任该域进行联合。您可能需要与您的 IT 或网络管理员协调来完成此步骤。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 选择*验证域名所有权*。
5. 输入您要验证的域名并选择*继续*。
6. 复制提供的 TXT 记录。
7. 转到您域的 DNS 设置并配置作为您域的 TXT 记录提供的 TXT 值。如果需要，请与您的 IT 或网络管理员合作。
8. 添加TXT记录后，返回控制台并选择*验证*。

配置联合

将**NetApp Console**与 **Active Directory** 联合服务 **(AD FS)** 联合起来

将您的 Active Directory 联合身份验证服务 (AD FS) 与NetApp Console联合起来，以便为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录控制台。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。首先，配置身份提供者以信任NetApp Console作为服务提供者。然后，使用您的身份提供商的配置在控制台中创建连接。

您可以与 AD FS 服务器建立联合，以启用NetApp Console的单点登录 (SSO)。该过程涉及配置您的 AD FS 以信任控制台作为服务提供商，然后在NetApp Console中创建连接。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp Console中验证您的域"话题。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*Active Directory 联合身份验证服务 (AD FS)*。
7. 选择“下一步”。
8. 在您的 AD FS 服务器中创建依赖方信任。您可以使用 PowerShell 或在 AD FS 服务器上手动配置它。有关如何创建信赖方信任的详细信息，请参阅 AD FS 文档。
   a. 使用以下脚本通过 PowerShell 创建信任：

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. 或者，您可以在 AD FS 管理控制台中手动创建信任。创建信任时使用以下NetApp Console值：
      - 创建依赖信任标识符时，使用 **YOUR_TENANT** 值： `netapp-cloud-account`
      - 当您选择 启用对 **WS-Federation** 的支持 时，请使用 **YOUR_AUTH0_DOMAIN** 值： `netapp-cloud-account.auth0.com`
   c. 创建信任后，从 AD FS 服务器复制元数据 URL 或下载联合元数据文件。您需要此 URL 或文件来完成控制台中的连接。

NetApp建议使用元数据 URL 让NetApp Console自动检索最新的 AD FS 配置。如果您下载联合元数据文件，则每当 AD FS 配置发生更改时，都需要在NetApp Console中手动更新它。

9. 返回控制台，然后选择“下一步”来创建连接。
10. 创建与 AD FS 的连接。
    a. 输入您在上一步中从 AD FS 服务器复制的 **AD FS URL** 或上传您从 AD FS 服务器下载的联合元数据文件。
11. 选择*创建连接*。建立连接可能需要几秒钟。
12. 选择“下一步”。
13. 。选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。
14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

将**NetApp Console**与 **Microsoft Entra ID** 联合起来

与您的 Microsoft Entra ID IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 Microsoft Entra ID 建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 Microsoft Entra ID 以信任控制台作为服务提供商，然后在控制台中创建连接。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp Console中验证您的域"话题。

步骤

1. 选择*管理>身份和访问*。

2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。

域名详细信息

1. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
2. 选择“下一步”。

连接方法

1. 对于您的连接方法，选择*提供商*，然后选择*Microsoft Entra ID*。
2. 选择“下一步”。

配置说明

1. 配置您的 Microsoft Entra ID 以信任NetApp作为服务提供商。您需要在 Microsoft Entra ID 服务器上执行此步骤。
   a. 注册 Microsoft Entra ID 应用程序以信任控制台时，请使用以下值：
      - 对于 重定向 **URL** ，使用 `https://services.cloud.netapp.com`
      - 对于 回复 **URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   b. 为您的 Microsoft Entra ID 应用创建客户端机密。您需要提供客户端 ID、客户端密钥和 Entra ID 域名来完成联合。
2. 返回控制台，然后选择“下一步”来创建连接。

创建连接

1. 使用 Microsoft Entra ID 创建连接
   a. 输入您在上一步中创建的客户端 ID 和客户端密钥。
   b. 输入 Microsoft Entra ID 域名。
2. 选择*创建连接*。系统在几秒钟内建立连接。

测试并启用连接

1. 选择“下一步”。
2. 。选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。
3. 在控制台中，选择“下一步”以查看摘要页面。
4. 设置通知。

   您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显

示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

5. 查看联盟详细信息，然后选择“启用联盟”。
6. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

使用 **PingFederate** 联合**NetApp Console**

与您的 PingFederate IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以使用 PingFederate 设置联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 PingFederate 服务器以信任控制台作为服务提供商，然后在控制台中创建连接。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp Console中验证您的域"话题。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*提供商*，然后选择*PingFederate*。
7. 选择“下一步”。
8. 配置您的 PingFederate 服务器以信任NetApp作为服务提供商。您需要在 PingFederate 服务器上执行此步骤。
   a. 配置 PingFederate 以信任NetApp Console时，请使用以下值：

- 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
- 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
- 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-pingfederate>` 是联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。

b. 复制 PingFederate 服务器 URL。在控制台中创建连接时，您将需要此 URL。

c. 从您的 PingFederate 服务器下载 X.509 证书。它需要采用 Base64 编码的 PEM 格式（.pem、.crt、.cer）。

9. 返回控制台，然后选择“下一步”来创建连接。
10. 使用 PingFederate 创建连接
    a. 输入您在上一步中复制的 PingFederate 服务器 URL。
    b. 上传 X.509 签名证书。证书必须采用 PEM、CER 或 CRT 格式。
11. 选择*创建连接*。系统在几秒钟内建立连接。
12. 选择“下一步”。
13. 。选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。
14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

与 **SAML** 身份提供商联合

与您的 SAML 2.0 IdP 提供商联合，为 NEtApp 控制台启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

所需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。你不能与两者结成联盟。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 SAML 2.0 提供商建立联合连接，以便为控制台启用单点登录 (SSO)。该过程涉及配置您的提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp Console中验证您的域"话题。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*SAML 身份提供者*。
7. 选择“下一步”。
8. 配置您的 SAML 身份提供商以信任NetApp作为服务提供商。您需要在 SAML 提供商服务器上执行此步骤。
   a. 确保您的 IdP 具有属性 `email`设置为用户的电子邮件地址。这是控制台正确识别用户所必需的：

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中注册 SAML 应用程序时，请使用以下值：
   - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
   - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-saml>` 是您想要用于联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 创建信任后，从 SAML 提供商服务器复制以下值：
   - 登录网址

- 退出 URL（可选）

3. 从您的 SAML 提供商服务器下载 X.509 证书。它需要采用 PEM、CER 或 CRT 格式。
   a. 返回控制台，然后选择“下一步”来创建连接。
   b. 使用 SAML 创建连接。
4. 输入您的 SAML 服务器的 登录 **URL**。
5. 上传从 SAML 提供商服务器下载的 X.509 证书。
6. 或者，输入您的 SAML 服务器的 退出 **URL**。
   a. 选择*创建连接*。系统在几秒钟内建立连接。
   b. 选择“下一步”。
   c. 。选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。
   d. 在控制台中，选择“下一步”以查看摘要页面。
   e. 设置通知。

      您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

   f. 查看联盟详细信息，然后选择“启用联盟”。
   g. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

在NetApp Console中管理联合

您可以在NetApp Console中管理您的联合。您可以禁用它，更新过期的凭据，以及在不再需要它时禁用它。

如果您使用NetApp Cloud Central 配置了联合，请通过 **Federation** 页面导入它以在控制台中进行管理。"了解如何导入您的联盟"

您还可以将已验证的域添加到现有联合中，这允许您使用多个域进行联合连接。

联合管理事件（例如启用、禁用和更新联合）显示在时间轴中。"了解有关在NetApp Console中监控操作的更多信息。"

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

启用联盟

如果您已经创建了联盟但尚未启用，您可以通过*联盟*页面启用它。启用联合允许与联合关联的用户使用其公司凭据登录控制台。在启用联合之前，请先成功创建并测试联合。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ••• 旁边的您想要启用的联盟并选择*启用*。

将已验证的域添加到现有联合

您可以在控制台中将已验证的域添加到现有联合，以便使用具有相同身份提供商 (IdP) 的多个域。

您必须先在控制台中验证该域，然后才能将其添加到联合中。如果您尚未验证域名，可以按照以下步骤进行验证"在控制台中验证您的域"。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ⋮ 在您要添加已验证域的联盟旁边，然后选择*更新域*。 *更新域*对话框显示已与此联合关联的域。
4. 从可用域列表中选择一个已验证的域。
5. 选择*更新*。新域用户可以在 30 秒内获得联合控制台访问权限。

更新即将到期的联合连接

您可以在控制台中更新联合的详细信息。例如，如果证书或客户端机密等凭证过期，则需要更新联合。在需要时，更新通知日期以提醒您在连接到期之前更新连接。

> ⓘ 在更新您的 IdP 之前，请先更新控制台以避免登录问题。在此过程中保持登录控制台。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择要更新的联合旁边的操作菜单（三个垂直点），然后选择*更新联合*。
4. 根据需要更新联盟的详细信息。
5. 选择*更新*。

测试现有的联盟

测试现有联合的连接以验证其是否正常工作。这可以帮助您识别联盟中的任何问题并进行故障排除。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ⋮ 旁边的您想要添加已验证域的联盟，然后选择*测试连接*。
4. 选择*测试*。系统提示您使用公司凭证登录。如果连接成功，您将被重定向到NetApp Console。如果连接失败，您会看到一条错误消息，表明联合存在问题。

5. 选择“完成”返回“联合”选项卡。

禁用联合

如果您不再需要联合，您可以禁用它。这可以防止与联盟关联的用户使用其公司凭证登录控制台。如果需要，您可以稍后重新启用联合。

在删除联合之前，请先禁用它，例如在停用 IdP 或停止联合时。如果需要的话，您可以稍后重新启用它。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单:在您要添加已验证域的联盟旁边，然后选择*禁用*。

删除联盟

如果您不再需要联盟，您可以将其删除。这将删除联合并阻止与联合关联的任何用户使用其公司凭据登录控制台。例如，如果 IdP 被停用或者不再需要联合。

删除联合后，您将无法恢复它。您必须创建一个新的联盟。

您必须先禁用联合，然后才能删除它。一旦删除联盟，就无法恢复删除。

步骤

1. 选择“管理”>“身份和访问”。
2. 选择“**Federations**”以查看“**Federations**”页面。
3. 选择操作菜单:在您要添加已验证域的联盟旁边，然后选择*删除*。

将您的联合导入**NetApp Console**

如果您之前已通过NetApp Cloud Central（ NetApp Console的外部应用程序）设置联合，则联合页面会提示您将现有的联合连接导入控制台，以便您可以在新界面中对其进行管理。然后，您可以利用最新的增强功能，而无需重新创建联合连接。

导入现有联盟后，您可以从“联盟”页面管理该联盟。"了解有关管理联盟的更多信息。"

所需角色

组织管理员或联盟管理员。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择*导入联合*。

控制台代理

维护控制台代理虚拟机和操作系统

维护控制台代理主机上的操作系统是您（客户）的责任。例如，您（客户）应按照贵公司的操作系统分发标准程序对代理主机上的操作系统应用安全更新。

如果您有现成的代理，您应该注意"受支持的 Linux 操作系统的变更"。

操作系统补丁和代理

无需停止代理主机服务即可应用操作系统安全补丁。

VM 或实例类型

如果您从控制台创建控制台代理，它会使用默认配置在您的云提供商中部署 VM 实例。创建代理后，不要切换到具有较少 CPU 或 RAM 的较小 VM 实例。

下表列出了 CPU 和 RAM 要求：

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

"了解代理的默认配置" 。

监控代理

当代理虚拟机不健康时，控制台会通知您，包括磁盘空间、RAM 和 CPU 问题。在控制台内的通知中心监控这些通知或配置电子邮件通知。磁盘空间、内存或 CPU 使用率偶尔增加是正常现象，但如果经常发生，则应采取措施解决。

例如，当代理资源（CPU、RAM 或磁盘空间）连续 30 分钟超过其总容量的 90% 时，控制台会通知您。之后，如果资源使用率低于该阈值，则通知中心将显示通知已解决（绿色）。

如果您对修改代理 VM 有任何疑问，请联系NetApp支持。

"了解更多信息。"

通知	需要采取行动
磁盘空间过高	"查看NetApp知识库文章" 。
CPU 使用率过高	根据安装位置，增加云提供商或本地代理 VM 的 CPU 大小。或者，创建额外的代理并将工作负载分配给多个代理。 RAM 利用率可能因您的环境、 ONTAP工作负载、 Cloud Volumes ONTAP系统的数量以及您正在使用的数据服务而异。

通知	需要采取行动
RAM 使用率过高	根据安装位置，增加云提供商或本地代理虚拟机的 RAM。或者，创建额外的代理并将工作负载分配给多个代理。 RAM 利用率可能因您的环境、 ONTAP工作负载、 Cloud Volumes ONTAP系统的数量以及您正在使用的数据服务而异。

停止和启动代理虚拟机

如果需要，请使用云提供商的控制台或标准内部部署程序停止并启动代理虚拟机。

"请注意，控制台代理必须始终处于运行状态" 。

连接到 **Linux VM**

如果您需要连接到代理运行的 Linux VM，请使用云提供商提供的连接选项。

AWS

在 AWS 中创建代理实例时，请提供 AWS 访问密钥和密钥。您可以使用此密钥对通过 SSH 连接到实例。对 EC2 Linux 实例使用用户名“ubuntu”。对于 2023 年 5 月之前创建的代理，请使用用户名“ec2-user”。

"AWS 文档：连接到您的 Linux 实例"

Azure

在 Azure 中创建代理 VM 时，您可以指定用户名并选择使用密码或 SSH 公钥进行身份验证。使用您选择的身份验证方法连接到虚拟机。

"Azure 文档：通过 SSH 进入您的 VM"

Google Cloud

在 Google Cloud 中创建代理时，您无法指定身份验证方法。但是，您可以使用 Google Cloud Console 或 Google Cloud CLI (gcloud) 连接到 Linux VM 实例。

"Google Cloud Docs：连接到 Linux 虚拟机"

更改代理的 **IP** 地址

如果需要，您可以更改云提供商分配的代理实例的内部和公共 IP 地址。

步骤

1. 按照云提供商的说明更改代理实例的本地 IP 地址或公共 IP 地址（或两者）。
2. 重新启动代理实例以向控制台注册新的公共 IP 地址。
3. 如果您更改了私有 IP 地址，请更新Cloud Volumes ONTAP配置文件的备份位置，以便将备份发送到代理上的新私有 IP 地址。

   更新每个Cloud Volumes ONTAP系统的备份位置。

   a. 从Cloud Volumes ONTAP CLI，将权限级别设置为高级：

```
set -privilege advanced
```

1. 运行以下命令显示当前备份目标：

```
system configuration backup settings show
```

1. 运行以下命令来更新备份目标的 IP 地址：

```
system configuration backup settings modify -destination <target-location>
```

编辑代理的 **URI**

您可以添加和删除代理的统一资源标识符 (URI)。

步骤

1. 选择“管理 **>** 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

   控制台代理必须处于活动状态才能对其进行编辑。

3. 展开*代理 URI* 栏以查看代理 URI。
4. 添加和删除 URI，然后选择*应用*。

为控制台代理维护 **VCenter** 或 **ESXi** 主机

部署控制台代理后，您可以对现有的 VCenter 或 ESXi 主机进行更改。例如，您可以增加托管控制台代理的 VM 实例的 CPU 或 RAM。

使用 VM Web 控制台执行以下维护任务：

- 增加磁盘大小
- 重启代理
- 更新静态路由
- 更新搜索域

限制

尚不支持通过控制台升级代理。此外，您只能查看有关 IP 地址、DNS 和网关的信息。

访问虚拟机维护控制台

您可以从 VSphere 客户端访问维护控制台。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。

修改主用户密码

您可以更改 `maint`用户。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `1`查看 `System Configuration`菜单。
6. 进入 `1`更改维护用户密码并按照屏幕上的提示进行操作。

增加虚拟机实例的 **CPU** 或 **RAM**

您可以增加托管控制台代理的 VM 实例的 CPU 或 RAM。

在您的 VCenter 或 ESXi 主机中编辑 VM 实例设置，然后使用维护控制台应用更改。

VSphere 客户端中的步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 右键单击 VM 实例并选择*编辑设置*。
4. 增加用于 /opt 或 /var 分区的硬盘空间。
   a. 选择“硬盘 **2**”以增加用于 /opt 的硬盘空间。
   b. 选择*硬盘 3* 来增加 /var 使用的硬盘空间。
5. 保存更改。

维护控制台中的步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `1 to view the `System Configuration`菜单。

6. 进入 `2`并按照屏幕上的提示进行操作。控制台扫描新设置并增加分区的大小。

查看代理虚拟机的网络设置

查看 VSphere 客户端中代理 VM 的网络设置以确认或排除网络问题。您只能查看（不能更新）以下网络设置：IP 地址和 DNS 详细信息。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `2`查看 `Network Configuration`菜单。
6. 输入 1 到 6 之间的数字来查看相应的网络设置。

更新代理虚拟机的静态路由

根据需要添加、更新或删除代理虚拟机的静态路由。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `2`查看 `Network Configuration`菜单。
6. 进入 `7`更新静态路由并按照屏幕上的提示进行操作。
7. 按 Enter。
8. 或者，进行其他更改。
9. 进入 `9`提交您的更改。

更新代理虚拟机的域搜索设置

您可以更新代理虚拟机的搜索域设置。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。

5. 进入 `2``查看 `Network Configuration`菜单。
6. 进入 `8`更新域搜索设置并按照屏幕上的提示进行操作。
7. 按 Enter。
8. 或者，进行其他更改。
9. 进入 `9`提交您的更改。

访问代理诊断工具

访问诊断工具来解决控制台代理的问题。 NetApp支持可能会在解决问题时要求您执行此操作。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `3`查看支持和诊断菜单。
6. 进入 `1`访问诊断工具并按照屏幕上的提示进行操作。 + 例如，您可以验证所有代理服务是否正在运行。"检查控制台代理状态" 。

远程访问代理诊断工具

您可以使用 Putty 等工具远程访问诊断工具。通过分配一次性密码启用对代理 VM 的 SSH 访问。

SSH 访问支持复制和粘贴等高级终端功能。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint`密码是您在创建 VM 实例时指定的密码。
5. 进入 `3`查看 `Support and Diagnostics`菜单。
6. 进入 `2`访问诊断工具并按照屏幕上的提示配置 24 小时后过期的一次性密码。
7. 使用 SSH 工具（例如 Putty）通过用户名连接到代理虚拟机 `diag`以及您配置的一次性密码。

安装 **CA** 签名的证书以进行基于 **Web** 的控制台访问

当您在受限模式下使用NetApp Console时，可以从部署在云区域或本地的控制台代理虚拟机访问用户界面。默认情况下，控制台使用自签名 SSL 证书为控制台代理上运行的基于 Web 的控制台提供安全的 HTTPS 访问。

如果您的业务需要，您可以安装由证书颁发机构 (CA) 签名的证书，它比自签名证书提供更好的安全保护。安装

证书后，当用户访问基于 Web 的控制台时，控制台将使用 CA 签名的证书。

安装 **HTTPS** 证书

安装由 CA 签名的证书，以便安全访问在控制台代理上运行的基于 Web 的控制台。

关于此任务

您可以使用以下选项之一安装证书：

- 从控制台生成证书签名请求 (CSR)，将证书请求提交给 CA，然后在控制台代理上安装 CA 签名的证书。

  控制台用于生成 CSR 的密钥对存储在控制台代理内部。当您在控制台代理上安装证书时，控制台会自动检索相同的密钥对（私钥）。

- 安装您已有的 CA 签名证书。

  使用此选项，CSR 不会通过控制台生成。您单独生成 CSR 并将私钥存储在外部。安装证书时，您需要向控制台提供私钥。

步骤

1. 选择“管理 **>** 代理”。
2. 在*概述*页面上，选择控制台代理的操作菜单并选择*HTTPS 设置*。

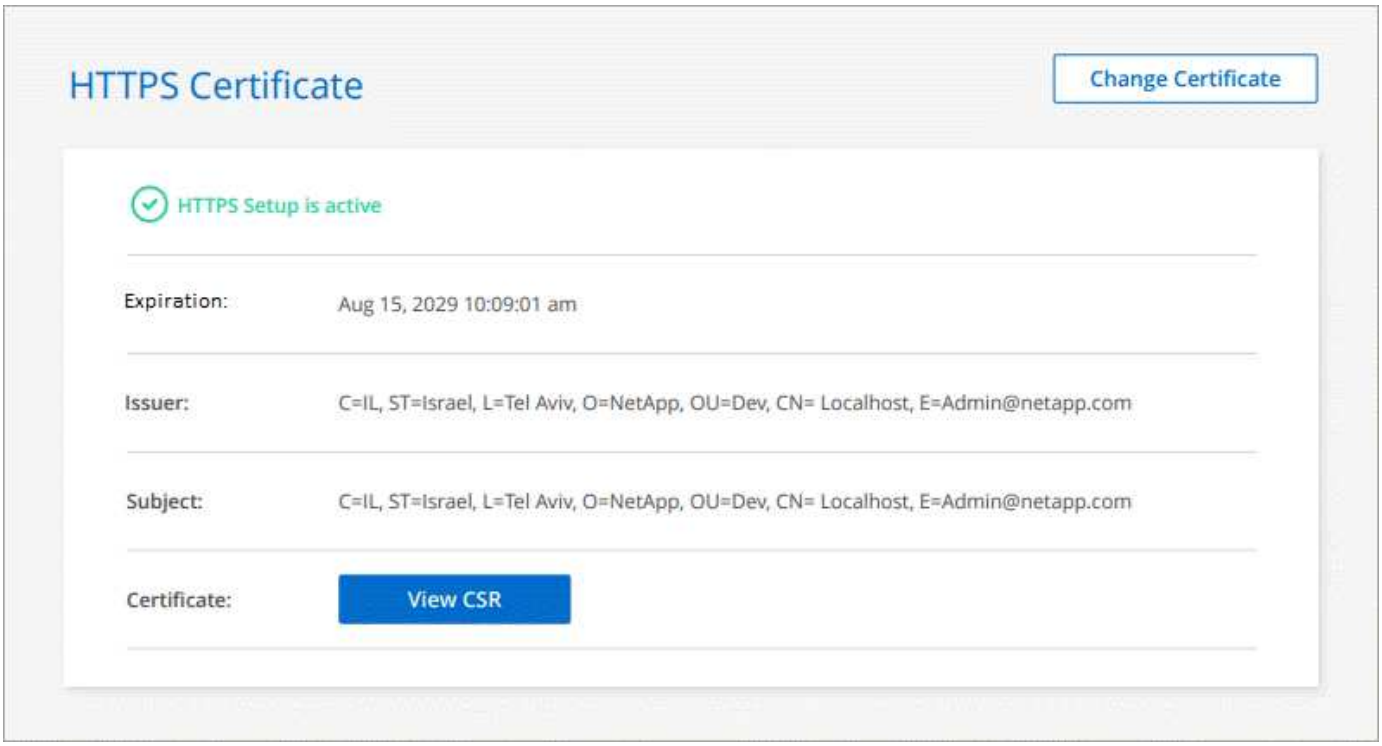
   必须连接控制台代理才能进行编辑。

3. 在 HTTPS 设置页面中，通过生成证书签名请求 (CSR) 或安装您自己的 CA 签名证书来安装证书：

选项	描述
生成 CSR	a. 输入控制台代理主机的主机名或 DNS（其通用名称），然后选择 生成 **CSR**。 控制台显示证书签名请求。 b. 使用 CSR 向 CA 提交 SSL 证书请求。 证书必须使用隐私增强邮件 (PEM) Base-64 编码的 X.509 格式。 c. 上传证书文件，然后选择*安装*。
安装您自己的 CA 签名证书	a. 选择*安装 CA 签名证书*。 b. 加载证书文件和私钥，然后选择*安装*。 证书必须使用隐私增强邮件 (PEM) Base-64 编码的 X.509 格式。

结果

控制台代理现在使用 CA 签名的证书来提供安全的 HTTPS 访问。下图显示了配置为安全访问的代理：



续订控制台 **HTTPS** 证书

您应该在代理的 HTTPS 证书到期之前更新它，以确保安全访问。如果您未在证书到期前续订，则当用户使用 HTTPS 访问 Web 控制台时会出现警告。

步骤

1. 选择“管理 **>** 代理”。
2. 在*概述*页面上，选择控制台代理的操作菜单并选择*HTTPS 设置*。

   显示有关证书的详细信息，包括到期日期。

3. 选择*更改证书*并按照步骤生成 CSR 或安装您自己的 CA 签名证书。

配置控制台代理以使用代理服务器

如果您的公司政策要求您使用代理服务器进行所有与互联网的通信，那么您需要配置您的代理以使用该代理服务器。如果您在安装期间没有将控制台代理配置为使用代理服务器，那么您可以随时将控制台代理配置为使用该代理服务器。

代理的代理服务器无需公共 IP 或 NAT 网关即可实现出站互联网访问。代理服务器仅为控制台代理提供出站连接，而不为Cloud Volumes ONTAP系统提供出站连接。

如果Cloud Volumes ONTAP系统缺少出站互联网访问，控制台会将其配置为使用控制台代理的代理服务器。您必须确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后打开此端口。

如果控制台代理本身没有出站互联网连接， Cloud Volumes ONTAP系统将无法使用配置的代理服务器。

支持的配置

- 为Cloud Volumes ONTAP系统提供服务的代理支持透明代理服务器。如果您将NetApp数据服务与Cloud Volumes ONTAP一起使用，请为Cloud Volumes ONTAP创建专用代理，您可以在其中使用透明代理服务器。
- 所有代理都支持显式代理服务器，包括管理Cloud Volumes ONTAP系统的代理和管理NetApp数据服务的代理。
- HTTP 和 HTTPS。
- 代理服务器可以位于云端或您的网络中。

一旦配置了代理，您就无法更改代理类型。如果需要更改代理类型，请删除控制台代理并添加具有新代理类型的新代理。

在控制台代理上启用显式代理

当您将控制台代理配置为使用代理服务器时，该代理及其管理的Cloud Volumes ONTAP系统（包括任何 HA 中介）都会使用代理服务器。

此操作重新启动控制台代理。在继续之前，请验证控制台代理是否空闲。

步骤

1. 选择“管理 **>** 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

   控制台代理必须处于活动状态才能对其进行编辑。

3. 选择*HTTP 代理配置*。
4. 在配置类型字段中选择*显式代理*。
5. 选择*启用代理*。
6. 使用语法指定服务器 http://address:port或者 https://address:port
7. 如果服务器需要基本身份验证，请指定用户名和密码。

   请注意以下事项：

   - 用户可以是本地用户或域用户。
   - 对于域用户，您必须输入 \ 的 ASCII 代码，如下所示：domain-name%92user-name

     例如：netapp%92proxy

   - 控制台不支持包含 @ 字符的密码。
8. 选择*保存*。

为控制台代理启用透明代理

仅Cloud Volumes ONTAP支持在控制台代理上使用透明代理。如果您除了Cloud Volumes ONTAP之外还使用NetApp数据服务，则应创建一个单独的代理来用于数据服务或用于Cloud Volumes ONTAP。

启用透明代理前，请确保满足以下要求：

- 代理与透明代理服务器安装在同一网络上。
- 代理服务器上启用了 TLS 检查。
- 您有一个 PEM 格式的证书，与透明代理服务器上使用的证书相匹配。
- 您不要将控制台代理用于除Cloud Volumes ONTAP之外的任何NetApp数据服务。

要配置现有代理以使用透明代理服务器，您可以使用控制台代理维护工具，该工具可通过控制台代理主机上的命令行获取。

当您配置代理服务器时，控制台代理将重新启动。在继续之前，请验证控制台代理是否空闲。

步骤

确保您拥有代理服务器的 PEM 格式的证书文件。如果您没有证书，请联系您的网络管理员获取证书。

1. 在控制台代理主机上打开命令行界面。
2. 导航到控制台代理维护工具目录： `/opt/application/netapp/service-manager-2/agent-maint-console`
3. 运行以下命令启用透明代理，其中 `/home/ubuntu/<certificate-file>.pem`是您拥有的代理服务器证书文件的目录和名称：

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

   确保证书文件为 PEM 格式并与命令位于同一目录中，或者指定证书文件的完整路径。

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

修改控制台代理的透明代理

您可以使用以下方法更新控制台代理现有的透明代理服务器： `proxy update`通过使用命令来移除透明代理服务器 `proxy remove`命令。更多信息，请查阅相关文档。"代理维护控制台" 。

> 一旦配置了代理，您就无法更改代理类型。如果需要更改代理类型，请删除控制台代理并添加具有新代理类型的新代理。

如果控制台代理无法访问互联网，请更新它

如果您的网络代理配置发生变化，您的代理可能会失去对互联网的访问权限。例如，如果有人更改了代理服务器的密码或更新了证书。在这种情况下，您需要直接从控制台代理主机访问 UI 并更新设置。确保您可以通过网络访问控制台代理主机，并且可以登录控制台。

启用直接 **API** 流量

如果您已将控制台代理配置为使用代理服务器，则可以在控制台代理上启用直接 API 流量，以便直接向云提供商服务发送 API 调用，而无需通过代理。在 AWS、Azure 或 Google Cloud 中运行的代理支持此选项。

如果您禁用带有Cloud Volumes ONTAP 的Azure Private Links 并使用服务端点，请启用直接 API 流量。否则，流量将无法正确路由。

"了解有关将 Azure Private Link 或服务端点与Cloud Volumes ONTAP结合使用的更多信息"

步骤

1. 选择“管理 > 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

   控制台代理必须处于活动状态才能对其进行编辑。

3. 选择*支持直接 API 流量*。
4. 选中复选框以启用该选项，然后选择*保存*。

要求在 **Amazon EC2** 实例上使用 **IMDSv2**

NetApp Console通过控制台代理和Cloud Volumes ONTAP （包括 HA 部署的中介）支持 Amazon EC2 实例元数据服务版本 2 (IMDSv2)。大多数情况下，IMDSv2 会在新的 EC2 实例上自动配置。 IMDSv1 于 2024 年 3 月之前启用。如果您的安全策略需要，您可能需要在 EC2 实例上手动配置 IMDSv2。

开始之前

- 控制台代理版本必须为 3.9.38 或更高版本。
- Cloud Volumes ONTAP必须运行以下版本之一：
  - 9.12.1 P2（或任何后续补丁）
  - 9.13.0 P4（或任何后续补丁）
  - 9.13.1 或此版本之后的任何版本
- 此更改要求您重新启动Cloud Volumes ONTAP实例。
- 这些步骤需要使用 AWS CLI，因为您必须将响应跳数限制更改为 3。

关于此任务

IMDSv2 提供了增强的针对漏洞的保护。 "从 AWS 安全博客了解有关 IMDSv2 的更多信息"

实例元数据服务 (IMDS) 在 EC2 实例上启用如下：

- 对于从控制台或使用 "Terraform 脚本"，IMDSv2 在 EC2 实例上默认启用。
- 如果您在 AWS 中启动新的 EC2 实例，然后手动安装控制台代理软件，则 IMDSv2 也会默认启用。
- 如果您从 AWS Marketplace 启动控制台代理，则默认启用 IMDSv1。您可以在 EC2 实例上手动配置 IMDSv2。
- 对于现有的控制台代理，仍然支持 IMDSv1，但如果您愿意，可以在 EC2 实例上手动配置 IMDSv2。
- 对于Cloud Volumes ONTAP，IMDSv1 在新实例和现有实例上默认启用。如果愿意，您可以在 EC2 实例上手动配置 IMDSv2。

步骤

1. 要求在控制台代理实例上使用 IMDSv2：

   a. 连接到控制台代理的 Linux VM。

      当您在 AWS 中创建控制台代理实例时，您提供了 AWS 访问密钥和密钥。您可以使用此密钥对通过 SSH 连接到实例。 EC2 Linux 实例的用户名是 ubuntu（对于 2023 年 5 月之前创建的控制台代理，用户名是 ec2-user）。

      "AWS 文档：连接到您的 Linux 实例"

   b. 安装 AWS CLI。

      "AWS 文档：安装或更新到最新版本的 AWS CLI"

   c. 使用 `aws ec2 modify-instance-metadata-options`命令要求使用 IMDSv2 并将 PUT 响应跳数限制更改为 3。

      例子

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

+

> 这 `http-tokens`参数将 IMDSv2 设置为必需。什么时候 `http-tokens`是必需的，您还必须设置 `http-endpoint`启用。

2. 要求在Cloud Volumes ONTAP实例上使用 IMDSv2：

   a. 前往 "Amazon EC2 控制台"

   b. 从导航窗格中，选择*实例*。

   c. 选择一个Cloud Volumes ONTAP实例。

   d. 选择*操作>实例设置>修改实例元数据选项*。

   e. 在“修改实例元数据选项”对话框中，选择以下内容：

      - 对于*实例元数据服务*，选择*启用*。
      - 对于 **IMDSv2**，选择 必需。
      - 选择*保存*。

   f. 对其他Cloud Volumes ONTAP实例（包括 HA 中介）重复这些步骤。

   g. "停止并启动Cloud Volumes ONTAP实例"

结果

控制台代理实例和Cloud Volumes ONTAP实例现已配置为使用 IMDSv2。

使用多个控制台代理

如果您使用多个控制台代理，则可以直接从控制台在这些控制台代理之间切换以查看相关系统。

在控制台代理之间切换

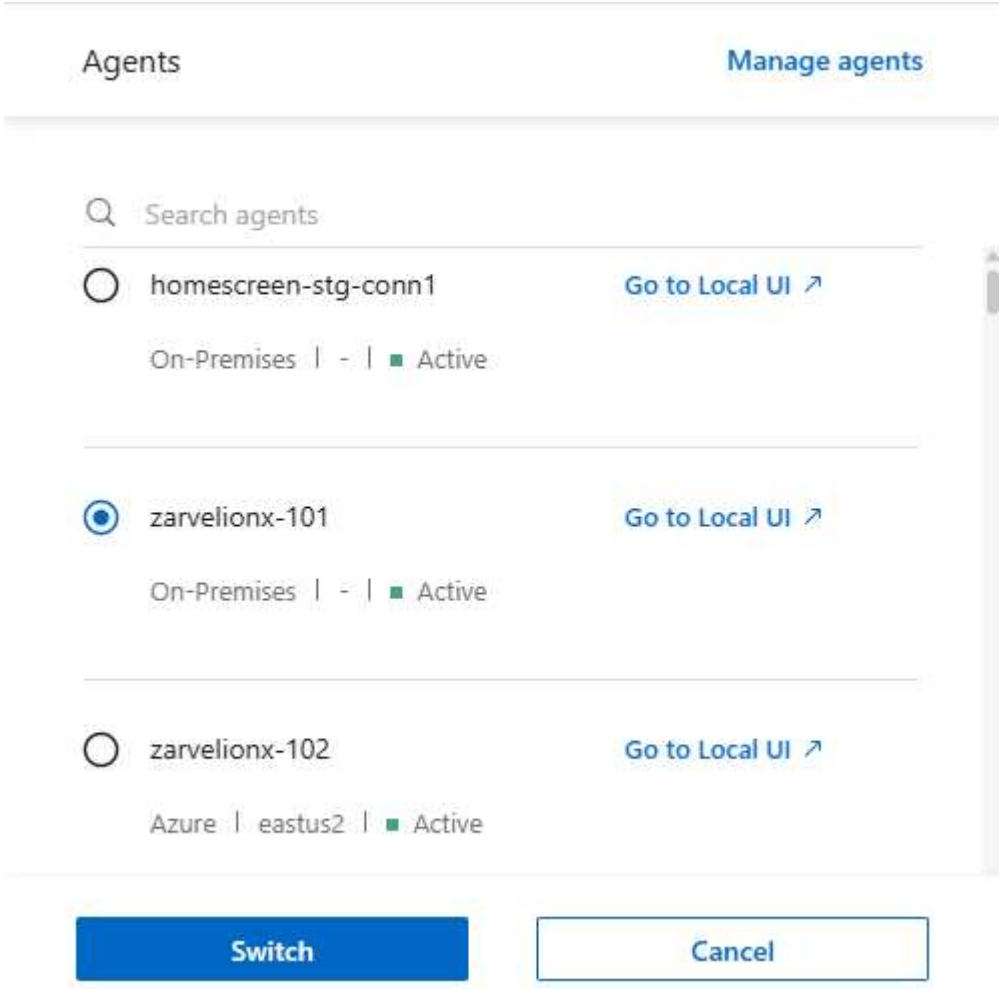
如果您有多个控制台代理，您可以在它们之间切换以查看与特定代理关联的系统。

例如，在多云环境中，您可能在 AWS 中有一个代理，在 Google Cloud 中有一个代理。在这些代理之间切换以管理各自云环境中的Cloud Volumes ONTAP系统。

从代理的本地 UI 查看NetApp Console时，此选项不可用

步骤

1. 选择控制台代理图标 ( ) 查看可用代理的列表。



结果

控制台刷新并显示与所选代理关联的系统。

控制台代理故障排除

要解决控制台代理的问题，您可以自行验证问题或与NetApp支持人员合作，他们可能会询问您的系统 ID、代理版本或最新的AutoSupport消息。

如果您有NetApp支持站点帐户，您还可以查看"NetApp知识库。"

常见错误消息和解决方法

此表列出了常见的错误信息以及解决方法：

错误消息	说明	该怎么办
无法加载控制台代理 UI	代理安装失败	• 验证服务管理器服务是否处于活动状态。 • 验证所有容器是否正在运行。 • 确保您的防火墙允许访问端口 8888 的服务。 • 如果仍有问题，请联系客服。
无法访问NetApp代理 UI	尝试访问代理的 IP 地址时会出现此消息。如果代理没有正确的网络访问权限或不稳定，则代理可能无法初始化。	• 连接到控制台代理。 • 验证 Service Manager 服务 • 验证代理是否具有所需的网络访问权限。"了解有关所需网络访问端点的更多信息。"
无法加载代理设置	当您尝试访问代理设置页面时，控制台会显示此消息。	• 检查 OCCM 容器是否正在运行并正常工作。 • 如果问题仍然存在，请联系支持人员。
无法加载代理的支持信息。	如果代理无法访问您的支持帐户，则会显示此消息。	• 确认代理程序拥有对所需端点的出站访问权限。"了解有关所需网络访问端点的更多信息。"

检查控制台代理状态

使用以下命令之一来验证您的控制台代理。所有服务的状态都应为“正在运行”。如果不是这种情况，请联系NetApp支持。

有关访问控制台代理诊断的详细信息，请参阅以下主题：

- "检查控制台代理状态（适用于 Linux 主机部署）"
- "检查控制台代理状态（针对 VCenter 部署）"

Docker（用于 **Ubuntu** 和 **VCenter** 部署）

```
docker ps -a
```

Podman（用于 **RedHat Enterprise Linux** 部署）

```
podman ps -a
```

查看控制台代理版本

查看控制台代理版本以确认升级或与您的NetApp代表共享。

步骤

1. 选择*管理>支持>代理*。

   控制台在页面顶部显示版本。

验证网络访问

确保控制台代理具有所需的网络访问权限。"了解有关所需网络接入点的更多信息。"

对控制台代理运行配置检查

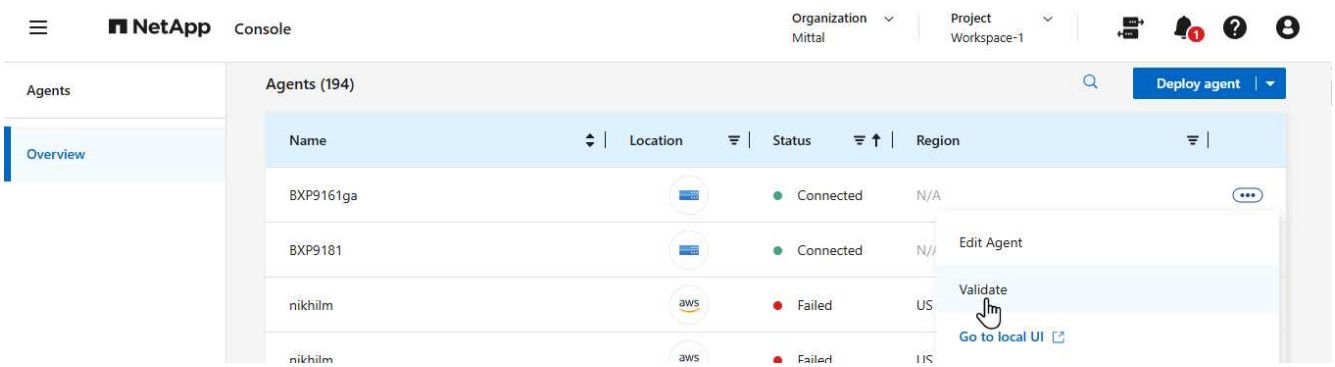
从控制台或代理维护控制台对控制台代理运行配置检查，以确保它们已连接。

您还可以使用代理维护控制台运行配置检查。"了解更多关于使用 config-checker validate 命令的信息。"

您只能验证状态为“已连接”的代理。

控制台操作步骤

1. 选择“管理 > 代理”。
2. 选择要检查的控制台代理的操作菜单，然后选择“验证”。



验证过程最多可能需要 15 分钟。结果会在完成后显示。

控制台代理安装问题

如果安装失败，请查看报告和日志以解决问题。

您还可以直接从以下目录中的控制台代理主机访问 JSON 格式的验证报告和配置日志：

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- 对于新代理部署， NetApp会检查以下端点："此处列出" 。如果您使用之前用于升级的端点，则此配置检查将失败并出现错误，"此处列出" 。 NetApp建议您尽快更新防火墙规则，以允许访问当前端点并阻止访问以前的端点"了解如何更新您的网络"。
- 如果您更新防火墙中的端点，您现有的代理将继续工作。

禁用手动安装的配置检查

有时您可能需要禁用在安装期间验证出站连接的配置检查。例如，在政府云环境中手动安装代理时，需要禁用配置检查，否则安装将失败。

步骤

您可以通过在 *com/opt/application/netapp/service-manager-2/config.json* 文件中设置 *skipConfigCheck* 标志来禁用配置检查。默认情况下，此标志设置为 false，并且配置检查会验证代理的出站访问。将此标志设置为 true 以禁用检查。在完成此步骤之前，请先熟悉 JSON 语法。

要重新启用配置检查，请使用以下步骤并将_skipConfigCheck_标志设置为false。

步骤

1. 以 root 身份或使用 sudo 权限访问控制台代理主机。
2. 创建 */opt/application/netapp/service-manager-2/config.json* 文件的备份副本，以确保您可以恢复更改。
3. 通过运行以下命令停止服务管理器 2 服务：

```
systemctl stop netapp-service-manager.service
```

1. 编辑 */opt/application/netapp/service-manager-2/config.json* 文件并将 *skipConfigCheck* 标志的值更改为 true。

```
  "skipConfigCheck": true
```

2. 保存您的文件。
3. 通过运行以下命令重新启动服务管理器 2 服务：

```
systemctl restart netapp-service-manager.service
```

与NetApp支持部门合作

如果您无法解决控制台代理的问题，您可能需要联系NetApp支持。 NetApp支持人员可能会要求您提供控制台代理 ID，或者如果他们还没有控制台代理日志，则要求您将控制台代理日志发送给他们。

查找控制台代理 ID

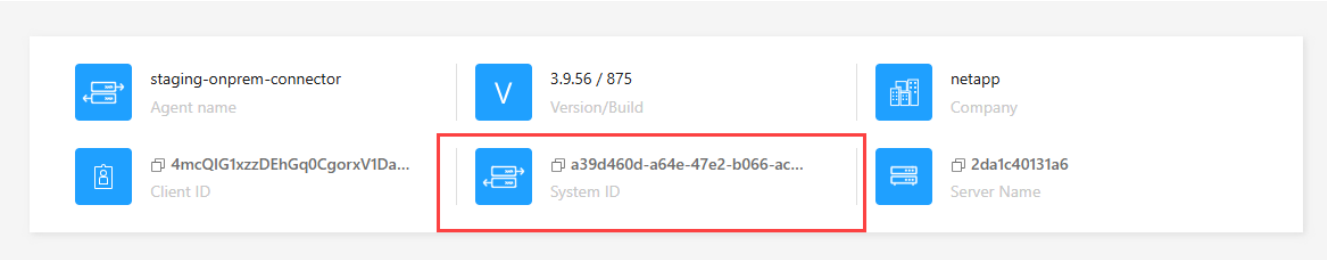
为了帮助您入门，您可能需要控制台代理的系统 ID。该 ID 通常用于许可和故障排除目的。

步骤

1. 选择*管理>支持>代理*。

   您可以在页面顶部找到系统 ID。

   例子



2. 将鼠标悬停在 ID 上并单击即可复制它。

下载或发送AutoSupport消息

如果您遇到问题， NetApp可能会要求您向NetApp支持发送AutoSupport消息以进行故障排除。

由于负载平衡， NetApp Console最多需要五个小时才能发送AutoSupport消息。对于紧急通信，请下载文件并手动发送。

步骤

1. 选择*管理>支持>代理*。
2. 根据您需要向NetApp支持发送信息的方式，选择以下选项之一：
   a. 选择将AutoSupport消息下载到本地计算机的选项。然后，您可以使用首选方法将其发送给NetApp支持。
   b. 选择“发送AutoSupport”以将消息直接发送给NetApp支持。

修复使用 Google Cloud NAT 网关时下载失败的问题

控制台代理会自动下载Cloud Volumes ONTAP 的软件更新。如果您的配置使用 Google Cloud NAT 网关，则可能导致下载失败。您可以通过限制软件映像划分的部分数来解决此问题。此步骤必须使用 API 完成。

步骤

1. 向 /occm/config 提交 PUT 请求，并将以下 JSON 作为正文：

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions 的值可以是 1 或任何大于 1 的整数。如果值为1，则下载的图像不会被分割。

请注意，32 是一个示例值。该值取决于您的 NAT 配置和同时会话的数量。

"了解有关 /occm/config API 调用的更多信息"

从**NetApp**知识库获取帮助

"查看NetApp支持团队创建的故障排除信息" 。

卸载并删除控制台代理

卸载控制台代理以解决问题或将其从主机中永久删除。您需要使用的步骤取决于您使用的部署模式。从环境中删除控制台代理后，您可以将其从控制台中删除。

"了解NetApp Console部署模式" 。

使用标准或受限模式时卸载代理

如果您使用的是标准模式或受限模式（换句话说，代理主机具有出站连接），那么您应该按照以下步骤卸载代理。

步骤

1. 连接到代理的 Linux VM。
2. 从 Linux 主机运行卸载脚本：

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent 运行脚本而不提示您确认。

从控制台中删除控制台代理

如果您删除了代理虚拟机或卸载了代理，则应将其从控制台的代理列表中删除。删除代理虚拟机或卸载代理软件后，代理在控制台中会显示“已断开连接”的状态。

删除控制台代理时请注意以下事项：

- 此操作不会删除虚拟机。
- 此操作无法恢复 - 一旦删除控制台代理，就无法将其添加回来。

步骤

1. 选择“管理 **>** 代理”。

2. 在“概览”页面上，选择已断开连接的代理的操作菜单，然后选择“移除代理”。
3. 输入代理人的姓名进行确认，然后选择*删除*。

控制台代理的默认配置

了解 AWS、Azure 和 Google Cloud 上标准部署（可访问互联网）的控制台代理默认配置，以及本地环境受限部署（不可访问互联网）的控制台代理默认配置。

可访问互联网的默认配置

如果您从NetApp Console、云提供商的市场部署了控制台代理，或者在具有 Internet 访问权限的本地 Linux 主机上手动安装了控制台代理，则以下配置详细信息适用。

AWS 控制台代理 **VM** 详细信息

如果您从控制台或云提供商的市场部署了控制台代理，请注意以下事项：

- EC2 实例类型为 t3.2xlarge。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。
- EC2 Linux 实例的用户名是 ubuntu（对于 2023 年 5 月之前创建的代理，用户名是 ec2-user）。
- 默认系统磁盘是 100 GiB gp2 磁盘。

Azure 控制台代理 **VM** 详细信息

如果您从控制台或云提供商的市场部署了控制台代理，请注意以下事项：

- VM 类型为 Standard_D8s_v3。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。
- 默认系统盘为100GiB高级SSD盘。

Google Cloud 控制台代理 **VM** 详细信息

如果您从控制台部署了控制台代理，请注意以下事项：

- VM 实例是 n2-standard-8。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。

- 默认系统磁盘是 100 GiB SSD 持久磁盘。

安装文件夹

代理程序安装文件夹位于以下位置：

```
/opt/application/netapp/cloudmanager
```

日志文件

日志文件包含在以下文件夹中：

- `/opt/application/netapp/cloudmanager/log` 或者
- `/opt/application/netapp/service-manager-2/logs` （从新安装的 3.9.23 版本开始）

  这些文件夹中的日志提供了有关控制台代理的详细信息。

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

  此文件夹中的日志提供有关云服务和在控制台代理上运行的控制台服务的详细信息。

控制台代理服务

- 控制台代理服务名为 occm。
- occm 服务依赖于 MySQL 服务。

  如果 MySQL 服务关闭，那么 occm 服务也会关闭。

端口

代理在 Linux 主机上使用以下端口：

- 80 用于 HTTP 访问
- 443 用于 HTTPS 访问

无需互联网访问的默认配置

如果您在没有互联网访问权限的本地 Linux 主机上手动安装了控制台代理，则适用以下配置。"了解有关此安装选项的更多信息" 。

- 代理程序安装文件夹位于以下位置：

  ```
  /opt/application/netapp/ds
  ```

- 日志文件包含在以下文件夹中：

  ```
  /var/lib/docker/volumes/ds_occmdata/_data/log
  ```

  此文件夹中的日志提供有关控制台代理和 Docker 映像的详细信息。

- 所有服务都在docker容器内运行

  这些服务依赖于docker运行时服务的运行

- 代理在 Linux 主机上使用以下端口：
  - 80 用于 HTTP 访问
  - 443 用于 HTTPS 访问

强制实施**ONTAP Advanced View**（**ONTAP**系统管理器）的**ONTAP**权限

默认情况下，控制台代理凭据允许用户访问高级视图（ONTAP系统管理器）。您可以提示用户输入他们的ONTAP凭据。这可确保用户在Cloud Volumes ONTAP和ONTAP本地集群中使用ONTAP集群时应用其ONTAP权限。

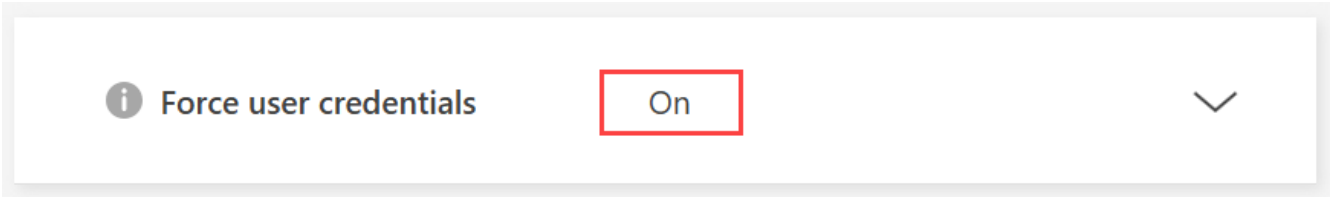
您必须具有组织管理员角色才能编辑控制台代理设置。

步骤

1. 选择“管理 > 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

   控制台代理必须处于活动状态才能对其进行编辑。

3. 展开*强制凭证*选项。
4. 选中复选框以启用*强制凭证*选项，然后选择*保存*。
5. 验证“强制凭证”选项是否已启用。



凭证和订阅

AWS

了解**NetApp Console**中的 **AWS** 凭证和权限

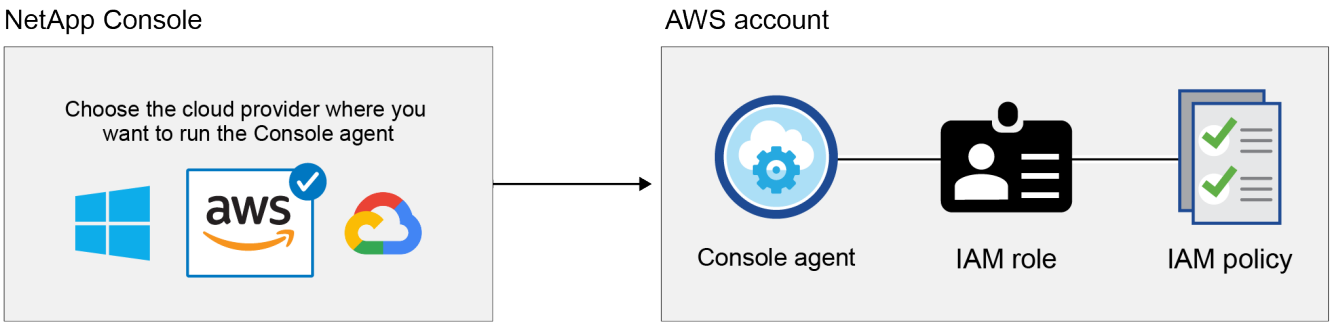
您可以通过NetApp Console直接管理 AWS 凭证和市场订阅，通过在控制台代理部署期间提供适当的 IAM 凭证并将其与 AWS Marketplace 订阅关联以进行计费，来确保Cloud Volumes ONTAP和其他数据服务的安全部署。

初始 **AWS** 凭证

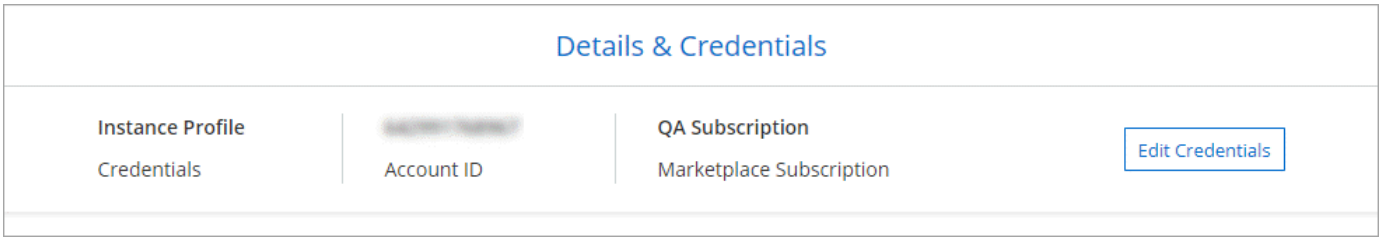
从控制台部署控制台代理时，您需要提供 IAM 角色的 ARN 或 IAM 用户的访问密钥。身份验证方法必须具有在

AWS 中部署控制台代理的权限。所需权限列于表中"AWS代理部署策略"。

当控制台在 AWS 中启动控制台代理时，它会为代理创建一个 IAM 角色和一个配置文件。它还附加了一项策略，为控制台代理提供管理该 AWS 账户内的资源和流程的权限。"查看代理如何使用权限"。



如果您添加新的Cloud Volumes ONTAP系统，控制台将默认选择以下 AWS 凭证：



使用初始 AWS 凭证部署所有Cloud Volumes ONTAP系统，或者您可以添加其他凭证。

额外的 **AWS** 凭证

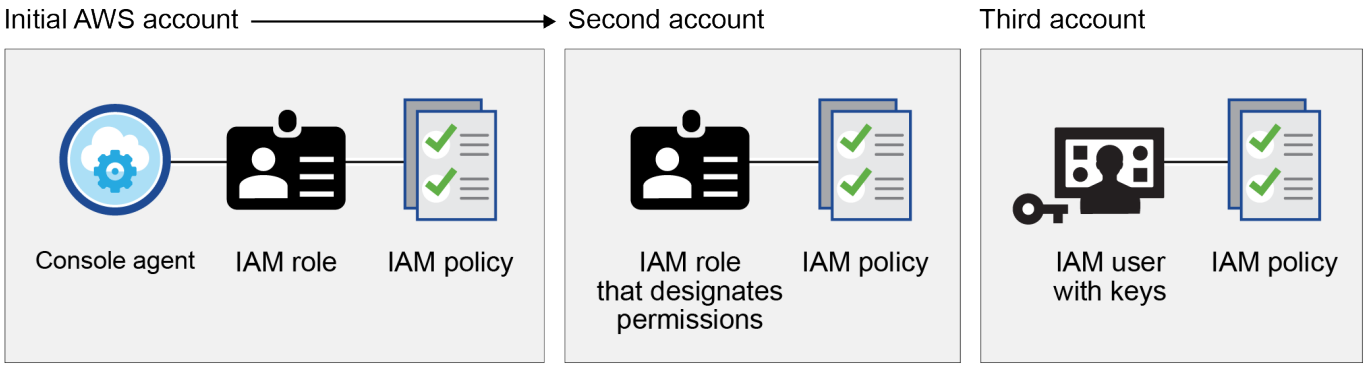
在以下情况下，您可能会向控制台添加其他 AWS 凭证：

- 要将您现有的控制台代理与额外的 AWS 账户一起使用，请执行以下操作：
- 在特定 AWS 账户中创建新代理
- 创建和管理 FSx for ONTAP文件系统

请参阅以下部分以了解更多详细信息。

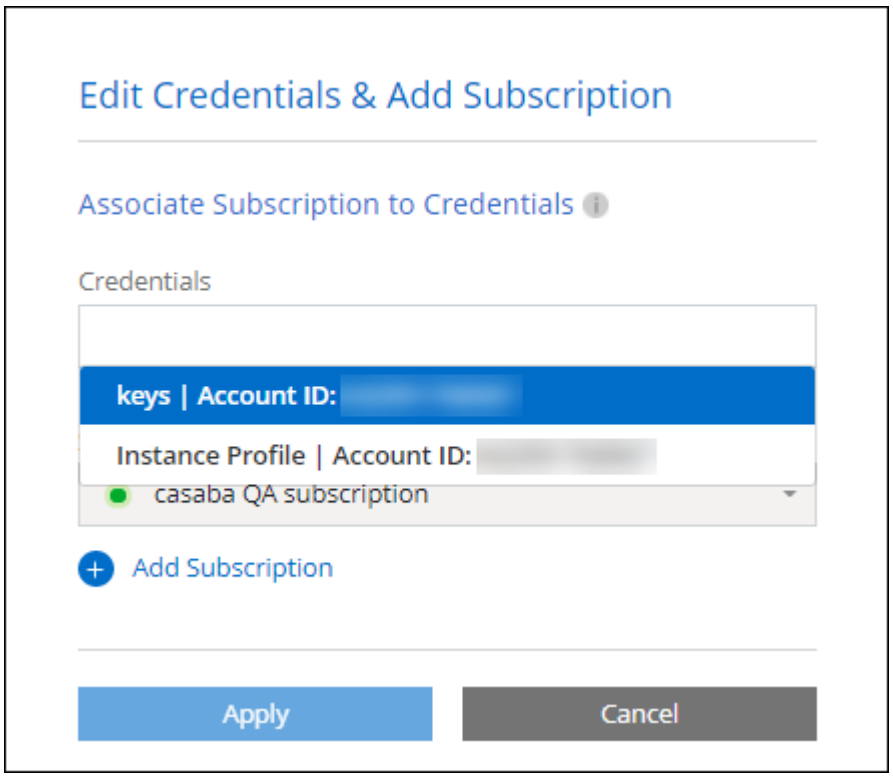
添加 **AWS** 凭证以将控制台代理与另一个 **AWS** 账户一起使用

要将控制台与额外的 AWS 账户一起使用，请提供 AWS 密钥或受信任账户中角色的 ARN。下图显示了两个附加账户，一个通过受信任账户中的 IAM 角色提供权限，另一个通过 IAM 用户的 AWS 密钥提供权限：



您可以通过指定 IAM 角色的 Amazon 资源名称 (ARN) 或 IAM 用户的 AWS 密钥，将帐户凭证添加到控制台。

例如，您可以在创建新的Cloud Volumes ONTAP系统时在凭据之间切换：



"了解如何将 AWS 凭证添加到现有代理。"

添加 **AWS** 凭证以创建控制台代理

添加 AWS 凭证即可获得创建控制台代理的权限。

"了解如何将 AWS 凭证添加到控制台以创建控制台代理"

为 **FSx for ONTAP**添加 **AWS** 凭证

将 AWS 凭证添加到控制台以提供创建和管理 FSx for ONTAP系统所需的权限。

"了解如何将 AWS 凭证添加到Amazon FSx for ONTAP控制台"

凭证和市场订阅

您必须将添加到控制台代理的凭证与 AWS Marketplace 订阅关联起来，才能按小时费率 (PAYGO) 支付Cloud Volumes ONTAP费用，并通过年度合同支付其他NetApp数据服务费用。"了解如何关联 AWS 订阅"。

请注意以下有关 AWS 凭证和市场订阅的事项：

- 您只能将一个 AWS Marketplace 订阅与一组 AWS 凭证关联
- 您可以使用新的订阅替换现有的市场订阅

常见问题解答

以下问题与凭证和订阅有关。

如何安全地轮换我的 **AWS** 凭证？

如上文所述，控制台允许您通过几种方式提供 AWS 凭证：与控制台代理关联的 IAM 角色、在受信任的账户中承担 IAM 角色或提供 AWS 访问密钥。

对于前两个选项，控制台使用 AWS 安全令牌服务来获取不断轮换的临时凭证。这个流程是最佳实践——它既自动化又安全。

如果您向控制台提供 AWS 访问密钥，则应通过定期在控制台中更新密钥来轮换密钥。这是一个完全手动的过程。

我可以更改**Cloud Volumes ONTAP**系统的 **AWS Marketplace** 订阅吗？

是的，你可以。当您更改与一组凭证关联的 AWS Marketplace 订阅时，所有现有和新的Cloud Volumes ONTAP系统都将根据新订阅收费。

"了解如何关联 AWS 订阅" 。

我可以添加多个 **AWS** 凭证，每个凭证都有不同的市场订阅吗？

属于同一 AWS 账户的所有 AWS 凭证都将与同一个 AWS Marketplace 订阅相关联。

如果您有属于不同 AWS 账户的多个 AWS 凭证，则这些凭证可以与同一个 AWS Marketplace 订阅或不同的订阅相关联。

我可以将现有的**Cloud Volumes ONTAP**系统移动到不同的 **AWS** 账户吗？

不可以，无法将与您的Cloud Volumes ONTAP系统关联的 AWS 资源移动到其他 AWS 账户。

凭证如何用于市场部署和本地部署？

以上部分描述了控制台代理的推荐部署方法，即从控制台部署。您还可以从 AWS Marketplace 在 AWS 中部署代理，也可以在您自己的 Linux 主机或 VCenter 中手动安装控制台代理软件。

如果您使用市场，则权限以相同的方式提供。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。

对于本地部署，您无法为控制台设置 IAM 角色，但可以使用 AWS 访问密钥提供权限。

要了解如何设置权限，请参阅以下页面：

- 标准模式
  - "设置 AWS Marketplace 部署的权限"
  - "设置本地部署的权限"
- 限制模式
  - "设置限制模式的权限"

管理**NetApp Console**的 **AWS** 凭证和市场订阅

添加和管理 AWS 凭证，以便您从NetApp Console部署和管理 AWS 帐户中的云资源。如果您管理多个 AWS Marketplace 订阅，则可以从“凭证”页面将每个订阅分配给不同的 AWS 凭证。

概述

您可以将 AWS 凭证添加到现有的控制台代理或直接添加到控制台：

- 向现有代理添加额外的 AWS 凭证

  将 AWS 凭证添加到控制台代理以管理云资源。了解如何将 AWS 凭证添加到控制台代理 。

- 将 AWS 凭证添加到控制台以创建控制台代理

  向控制台添加新的 AWS 凭证可提供创建控制台代理所需的权限。了解如何将 AWS 凭证添加到NetApp Console 。

- 将 AWS 凭证添加到 FSx for ONTAP控制台

  将新的 AWS 凭证添加到控制台以创建和管理 FSx for ONTAP。 "了解如何设置 FSx for ONTAP 的权限"

如何轮换凭证

NetApp Console允许您通过几种方式提供 AWS 凭证：与代理实例关联的 IAM 角色、在受信任的帐户中承担 IAM 角色或提供 AWS 访问密钥。"了解有关 AWS 凭证和权限的更多信息" 。

对于前两个选项，控制台使用 AWS 安全令牌服务来获取不断轮换的临时凭证。这个过程是最佳实践，因为它是自动的并且是安全的。

通过在控制台中更新来手动轮换 AWS 访问密钥。

向控制台代理添加附加凭据

向控制台代理添加额外的 AWS 凭证，以便它具有管理公共云环境中的资源和流程所需的权限。您可以提供另一个账户中的 IAM 角色的 ARN，也可以提供 AWS 访问密钥。

"了解NetApp Console如何使用 AWS 凭证和权限"。

授予权限

在将 AWS 凭证添加到控制台代理之前授予权限。这些权限允许控制台代理管理该 AWS 账户内的资源和流程。您可以使用受信任账户或 AWS 密钥中角色的 ARN 来提供权限。

如果您从控制台部署了控制台代理，它会自动为您部署控制台代理的账户添加 AWS 凭证。这确保了管理资源所需的必要权限。

选择

- 通过承担另一个账户中的 IAM 角色来授予权限
- 通过提供 AWS 密钥授予权限

通过承担另一个账户中的 **IAM** 角色来授予权限

您可以使用 IAM 角色在部署控制台代理的源 AWS 账户与其他 AWS 账户之间建立信任关系。然后，您将向控制台提供来自受信任账户的 IAM 角色的 ARN。

如果控制台代理安装在本地，则无法使用此身份验证方法。您必须使用 AWS 密钥。

步骤

1. 转到您想要为控制台代理提供权限的目标账户中的 IAM 控制台。
2. 在访问管理下，选择*角色>创建角色*并按照步骤创建角色。

   请务必执行以下操作：

   - 在 受信任实体类型 下，选择 **AWS** 账户。
   - 选择“其他 AWS 账户”，并输入控制台代理实例所在账户的 ID。
   - 通过复制并粘贴以下内容来创建所需的策略"控制台代理的 IAM 策略"。
3. 复制 IAM 角色的角色 ARN，以便稍后将其粘贴到控制台中。

结果

该帐户具有所需的权限。您现在可以将凭证添加到控制台代理 。

通过提供 **AWS** 密钥授予权限

如果您想为 IAM 用户提供带有 AWS 密钥的控制台，则需要向该用户授予所需的权限。控制台 IAM 策略定义了控制台允许使用的 AWS 操作和资源。

如果本地安装了控制台代理，则必须使用此身份验证方法。您不能使用 IAM 角色。

步骤

1. 从 IAM 控制台，通过复制并粘贴以下内容来创建策略"控制台代理的 IAM 策略"。

   "AWS 文档：创建 IAM 策略"
2. 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"

将凭证添加到现有代理

为 AWS 账户提供所需权限后，您可以将该账户的凭证添加到现有代理。这使您可以使用相同的代理在该帐户中启动Cloud Volumes ONTAP系统。

您的云提供商中的新凭证可能需要几分钟才能生效。

步骤

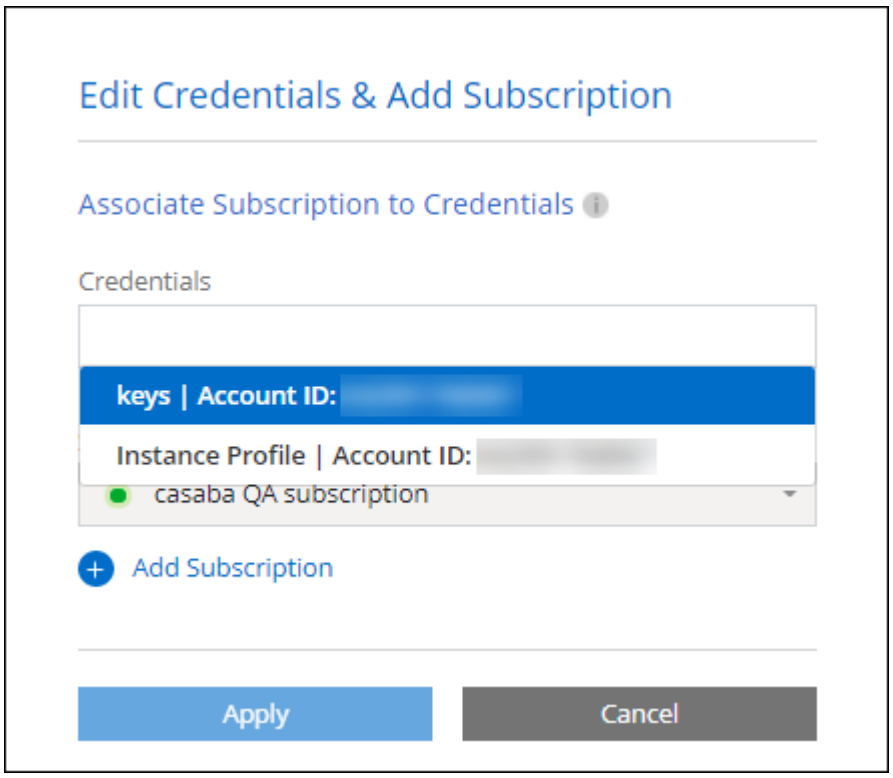
1. 使用顶部导航栏选择要添加凭据的控制台代理。
2. 在左侧导航栏中，选择“管理”>“凭据”。
3. 在*组织凭据*页面上，选择*添加凭据*并按照向导中的步骤进行操作。
   a. 凭证位置：选择*Amazon Web Services > 代理*。
   b. 定义凭证：提供受信任的 IAM 角色的 ARN（Amazon 资源名称），或输入 AWS 访问密钥和密钥。
   c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。

      要按小时费率（PAYGO）或年度合同支付服务费用，您必须将 AWS 凭证与您的 AWS Marketplace 订阅关联起来。

   d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

现在，您可以在向控制台添加订阅时从“详细信息和凭据”页面切换到不同的凭据集。



通过提供 IAM 角色的 ARN 来添加 AWS 凭证，该角色授予创建控制台代理所需的权限。您可以在创建新代理时选择这些凭据。

设置 IAM 角色

设置一个 IAM 角色，使NetApp Console软件即服务 (SaaS) 层能够承担该角色。

步骤

1. 转到目标账户中的 IAM 控制台。
2. 在访问管理下，选择*角色>创建角色*并按照步骤创建角色。

   请务必执行以下操作：

   - 在 受信任实体类型 下，选择 **AWS** 账户。
   - 选择“另一个 AWS 账户”并输入NetApp Console SaaS 的 ID：952013314444
   - 具体来说，对于Amazon FSx for NetApp ONTAP ，编辑 信任关系 策略以包含“AWS”：“arn:aws:iam::952013314444:root”。

     例如，该策略应如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
参考"AWS 身份和访问管理 (IAM) 文档"有关 IAM 中跨账户资源访问的更多信息。

   - 创建一个包含创建控制台代理所需权限的策略。
     - "查看 FSx for ONTAP所需的权限"
     - "查看代理部署策略"
3. 复制 IAM 角色的角色 ARN，以便您可以在下一步中将其粘贴到控制台中。

结果

IAM 角色现在具有所需的权限。您现在可以将其添加到控制台。

添加凭据

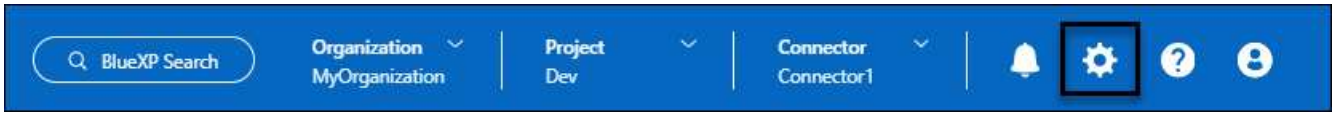
为 IAM 角色提供所需的权限后，将角色 ARN 添加到控制台。

开始之前

如果您刚刚创建了 IAM 角色，则可能需要几分钟才能使用它们。等待几分钟，然后将凭据添加到控制台。

步骤

1. 选择“管理 > 凭证”。



2. 在*组织凭据*页面上，选择*添加凭据*并按照向导中的步骤进行操作。
   a. 凭证位置：选择*Amazon Web Services > 控制台*。
   b. 定义凭证：提供 IAM 角色的 ARN（Amazon 资源名称）。
   c. 审核：确认有关新凭证的详细信息并选择*添加*。

向**Amazon FSx for ONTAP**控制台添加凭证

有关详细信息，请参阅 "Amazon FSx for ONTAP 的控制台文档"

配置 **AWS** 订阅

添加 AWS 凭证后，您可以使用这些凭证配置 AWS Marketplace 订阅。通过订阅，您可以按小时费率（PAYGO）或使用年度合同支付NetApp数据服务和Cloud Volumes ONTAP 的费用。

在添加凭证后，您可以在两种情况下配置 AWS Marketplace 订阅：

- 最初添加凭据时您没有配置订阅。
- 您想要更改配置为 AWS 凭证的 AWS Marketplace 订阅。

  用新的订阅替换当前的市场订阅会更改任何现有Cloud Volumes ONTAP系统和所有新系统的市场订阅。

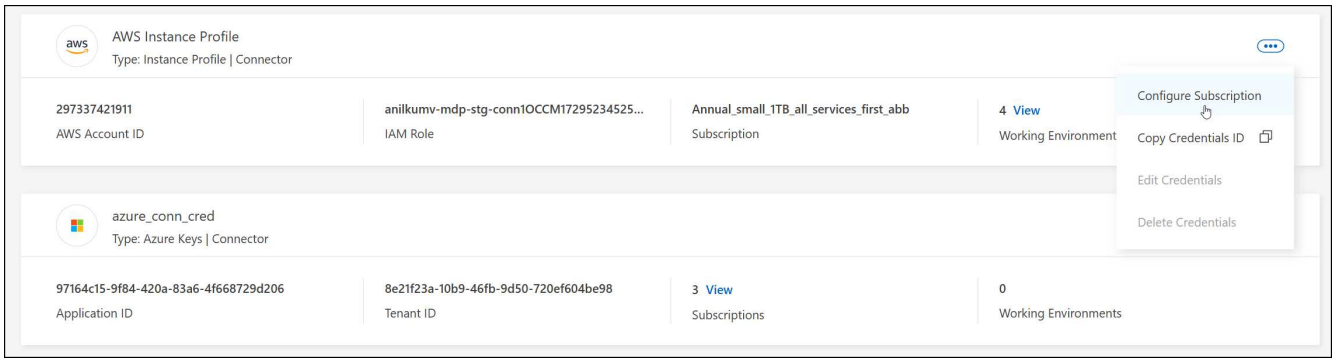
开始之前

您需要先创建控制台代理，然后才能配置订阅。"了解如何创建控制台代理" 。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择与控制台代理关联的一组凭据的操作菜单，然后选择*配置订阅*。

   您必须选择与控制台代理关联的凭据。您无法将市场订阅与与NetApp Console关联的凭据关联。



4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭证与新订阅关联，请选择“添加订阅”>“继续”*，然后按照 AWS Marketplace 中的步骤操作：

    a. 选择“查看购买选项”。

    b. 选择*订阅*。

    c. 选择*设置您的帐户*。

    您将被重定向到NetApp Console。

    d. 从“订阅分配”页面：

    - 选择您想要与此订阅关联的控制台组织或帐户。
    - 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

    控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

将现有订阅与您的组织关联

当您从 AWS Marketplace 订阅时，流程的最后一步是将订阅与您的组织关联。如果您没有完成此步骤，那么您就无法在您的组织中使用该订阅。

- "了解控制台部署模式"
- "了解控制台身份和访问管理"

如果您从 AWS Marketplace 订阅了NetApp Intelligent Services，但错过了将订阅与您的帐户关联的步骤，请按照以下步骤操作。

步骤

1. 确认您没有将您的订阅与您的控制台组织关联。

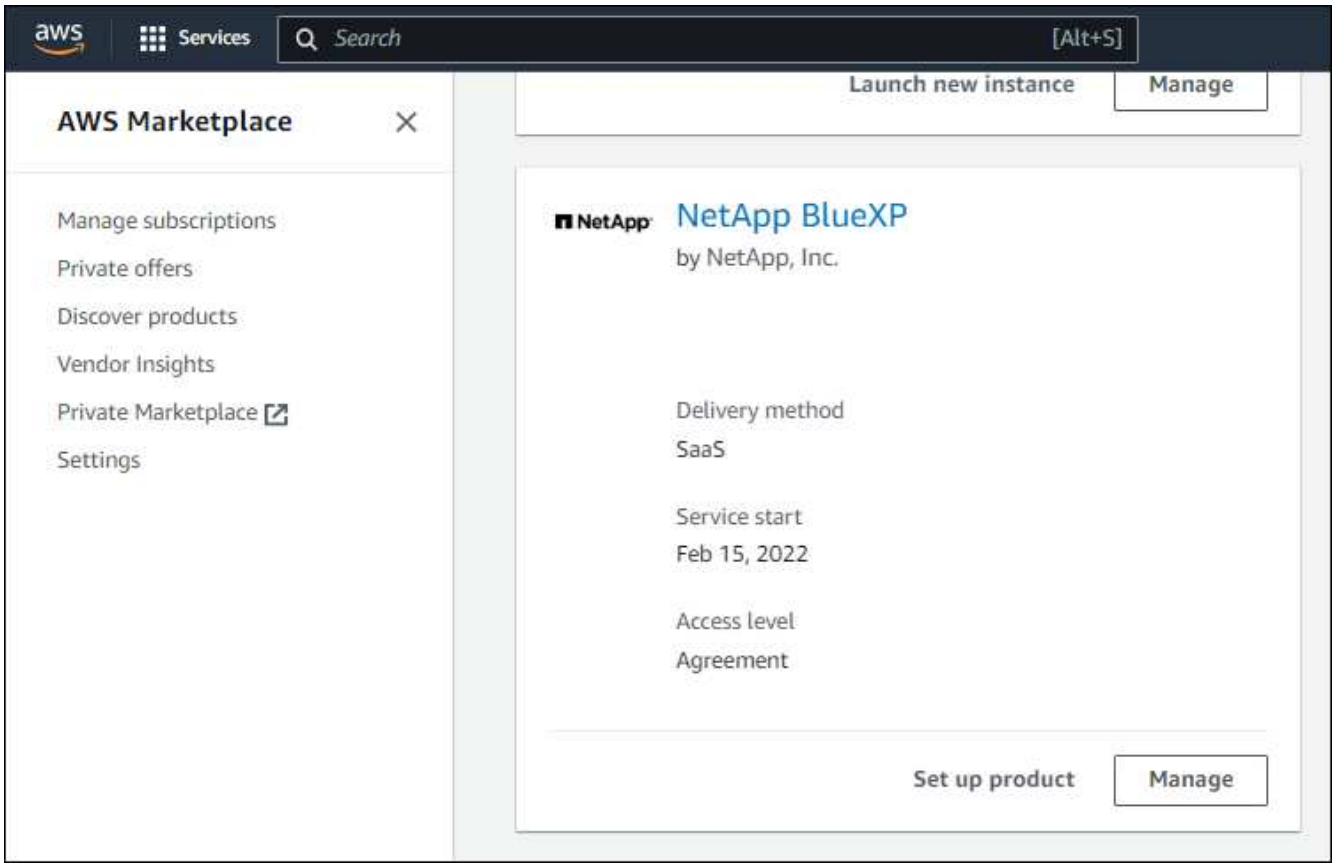
    a. 从导航菜单中，选择*管理>Licenses and subscriptions*。

    b. 选择*订阅*。

    c. 确认您的订阅没有出现。

您只会看到与您当前正在查看的组织或帐户相关的订阅。如果您没有看到您的订阅，请继续执行以下步骤。

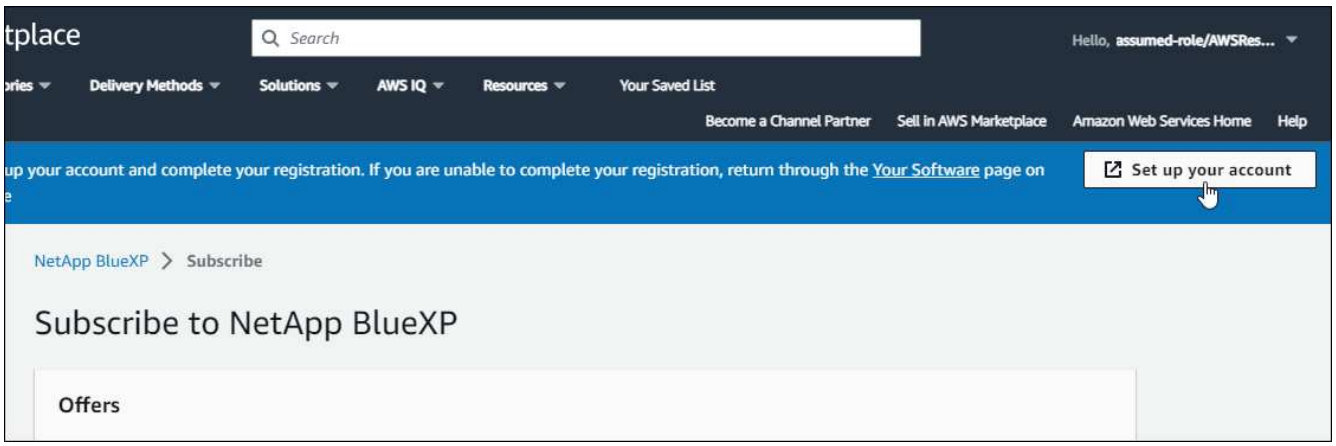
2. 登录 AWS 控制台并导航到 **AWS Marketplace** 订阅。
3. 查找订阅。



4. 选择*设置产品*。

订阅优惠页面应在新的浏览器选项卡或窗口中加载。

5. 选择*设置您的帐户*。



netapp.com 上的 **Subscription Assignment** 页面应在新浏览器选项卡或窗口中加载。

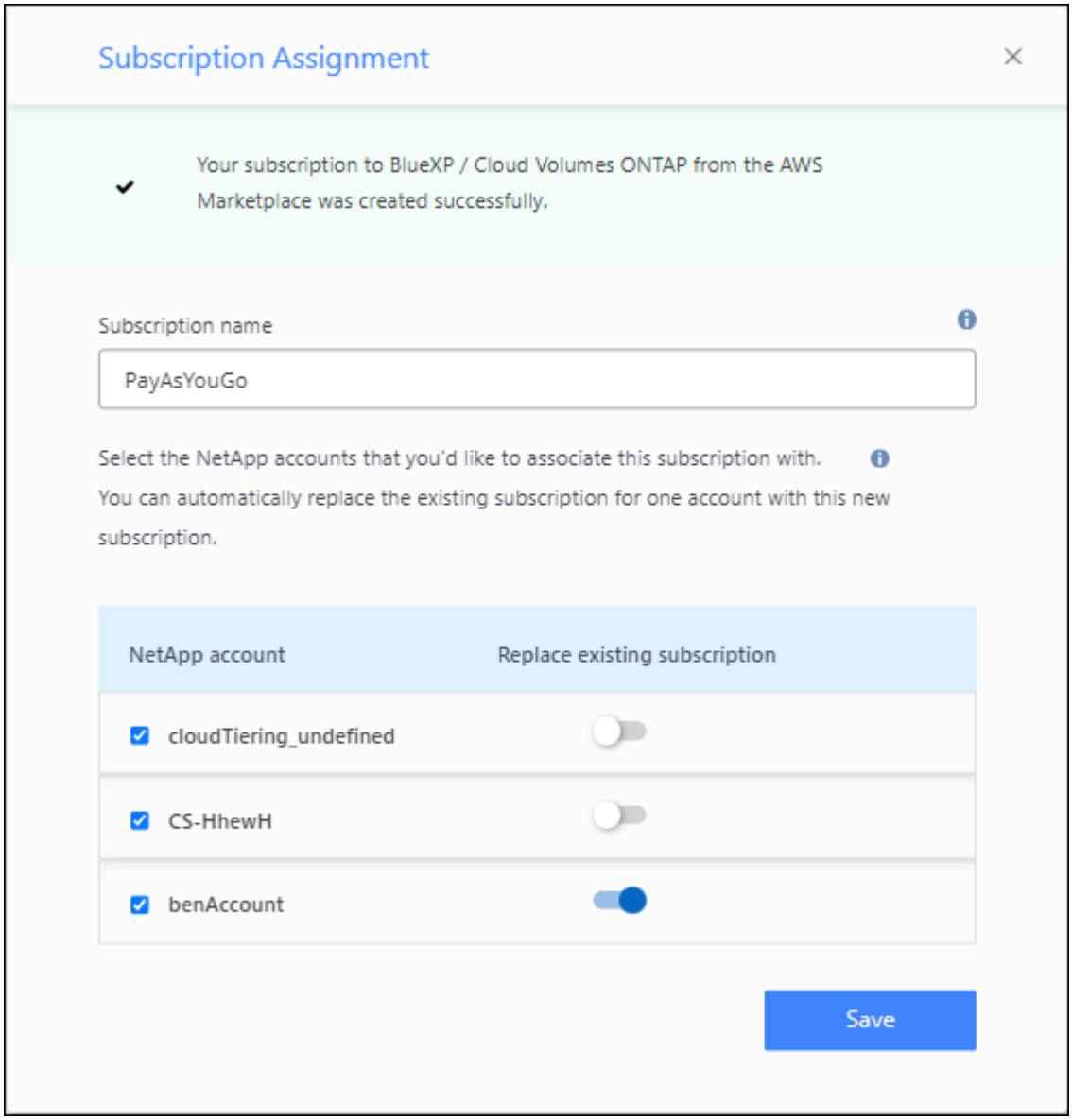
请注意，系统可能会提示您先登录控制台。

6. 从“订阅分配”页面：

   - 选择您想要与此订阅关联的控制台组织或帐户。
   - 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

     控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

     对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。



7. 确认订阅与您的组织相关联。

   a. 从导航菜单中，选择*管理>许可证和订阅*。

   b. 选择*订阅*。

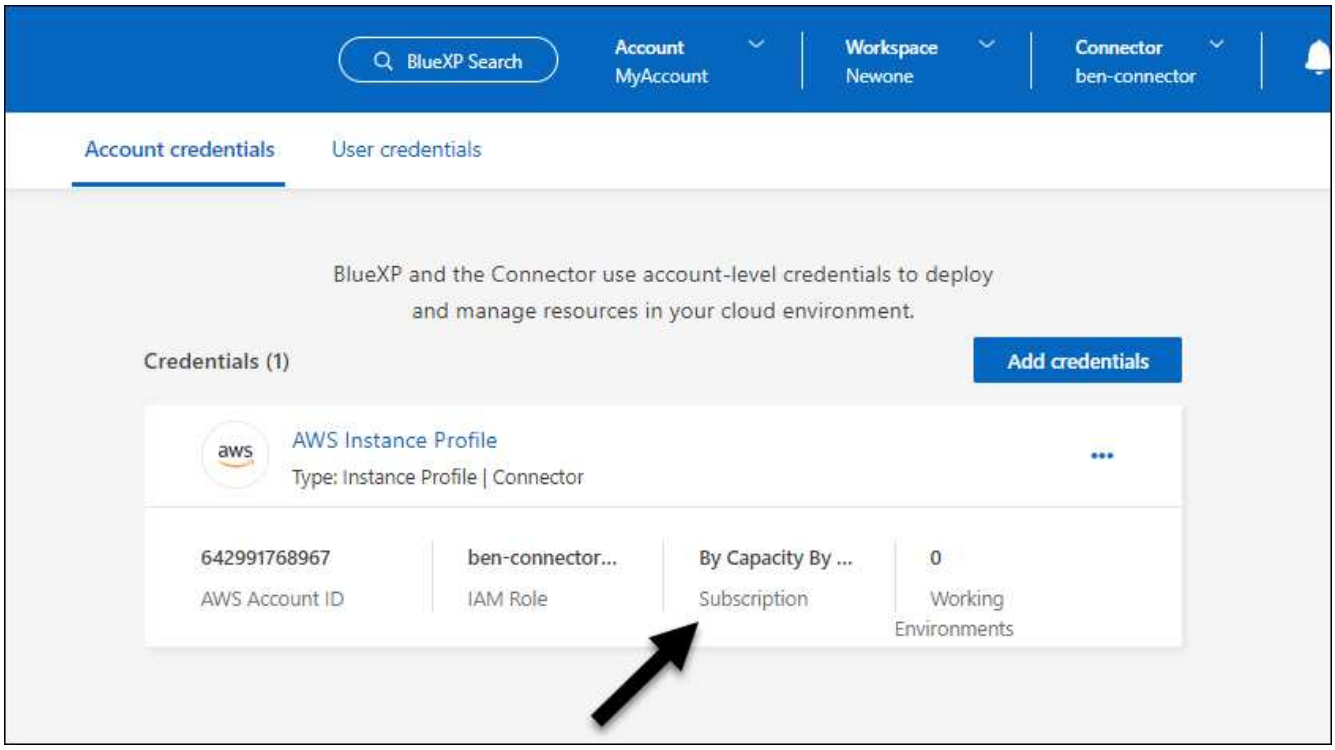
   c. 验证您的订阅是否出现。

8. 确认订阅与您的 AWS 凭证相关联。

   a. 选择“管理 > 凭证”。

   b. 在“组织凭证”页面上，验证订阅是否与您的 AWS 凭证关联。

      这是一个例子。



编辑凭据

通过更改帐户类型（AWS 密钥或承担角色）、编辑名称或更新凭证本身（密钥或角色 ARN）来编辑您的 AWS 凭证。

您无法编辑与控制台代理实例或Amazon FSx for ONTAP实例关联的实例配置文件的凭证。您只能重命名 FSx for ONTAP实例的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 在*组织凭证*页面上，选择一组凭证的操作菜单，然后选择*编辑凭证*。
3. 进行所需的更改，然后选择*应用*。

删除凭据

如果您不再需要一组凭证，您可以删除它们。您只能删除与系统无关的凭据。

您无法删除与控制台代理关联的实例配置文件的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 在*组织凭据*或*帐户凭据*页面上，选择一组凭据的操作菜单，然后选择*删除凭据*。
3. 选择*删除*进行确认。

Azure

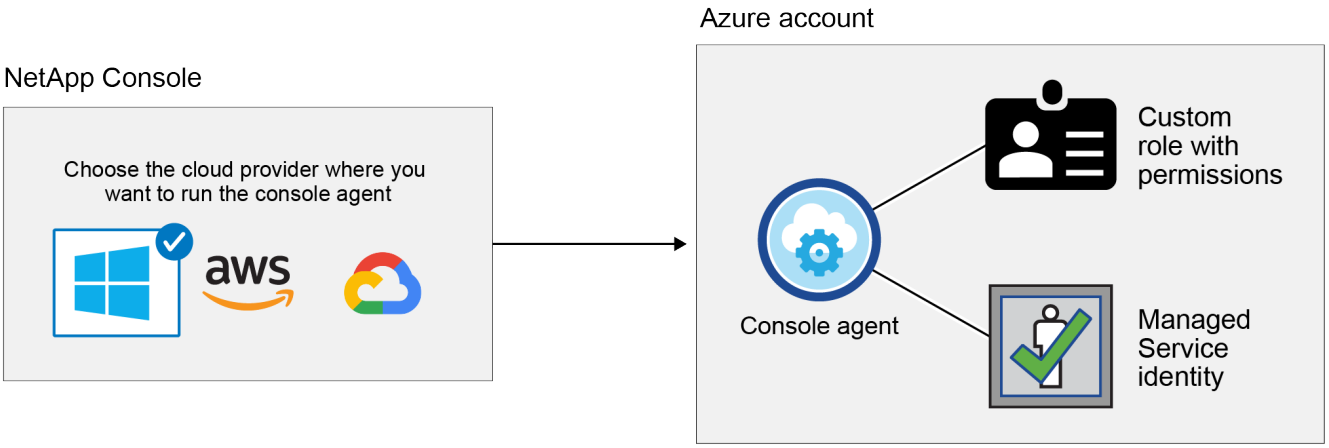
了解NetApp Console中的 Azure 凭据和权限

了解NetApp Console如何使用 Azure 凭据代表您执行操作以及这些凭据如何与市场订阅相关联。了解这些详细信息有助于您管理一个或多个 Azure 订阅的凭据。例如，您可能想了解何时向控制台添加其他 Azure 凭据。

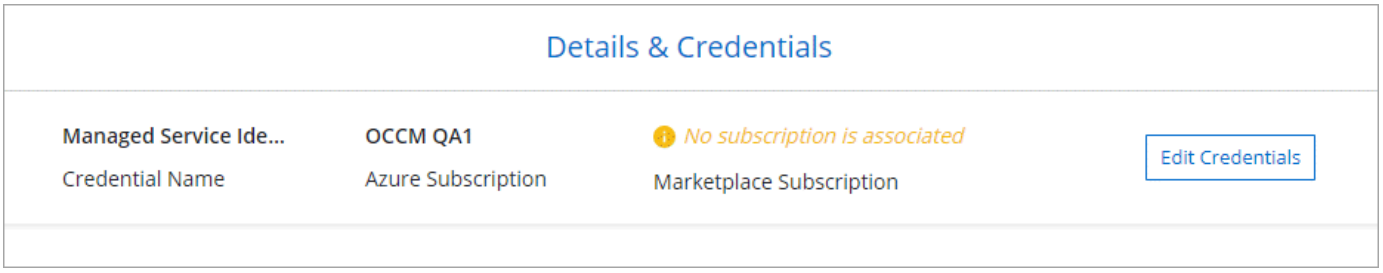
初始 Azure 凭据

从控制台部署控制台代理时，您需要使用具有部署控制台代理虚拟机权限的 Azure 帐户或服务主体。所需权限列于"Azure 的代理部署策略"。

当控制台在 Azure 中部署控制台代理虚拟机时，它会启用 "系统分配的托管标识"在虚拟机上，创建自定义角色，并将其分配给虚拟机。该角色为控制台提供管理该 Azure 订阅内的资源和流程所需的权限。"查看控制台如何使用权限" 。



如果您为Cloud Volumes ONTAP创建新系统，控制台将默认选择以下 Azure 凭据：



您可以使用初始 Azure 凭据部署所有Cloud Volumes ONTAP系统，也可以添加其他凭据。

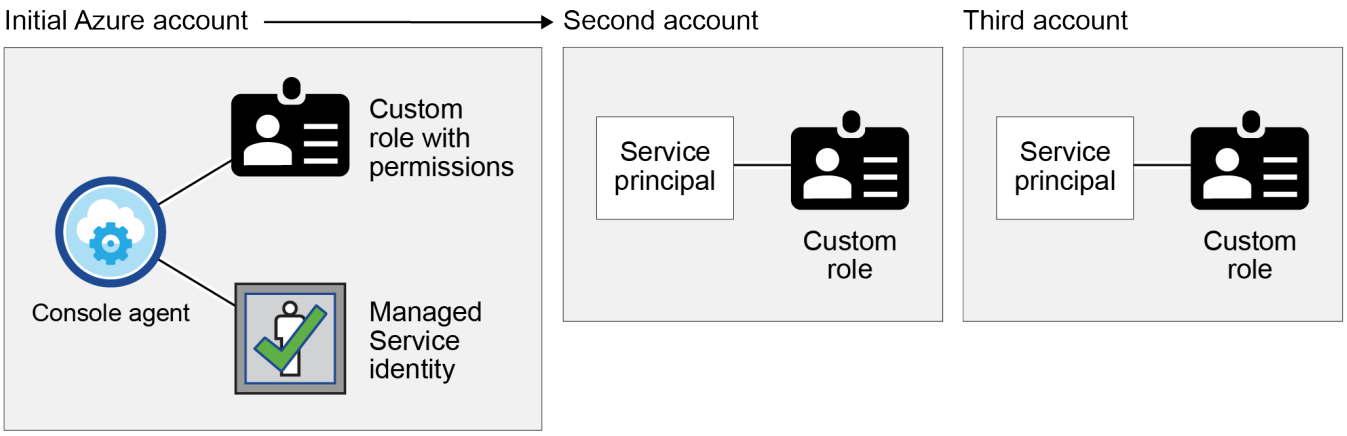
托管标识的其他 Azure 订阅

分配给控制台代理 VM 的系统分配托管标识与您启动控制台代理的订阅相关联。如果您想选择不同的 Azure 订

阅，则需要"将托管标识与这些订阅关联"。

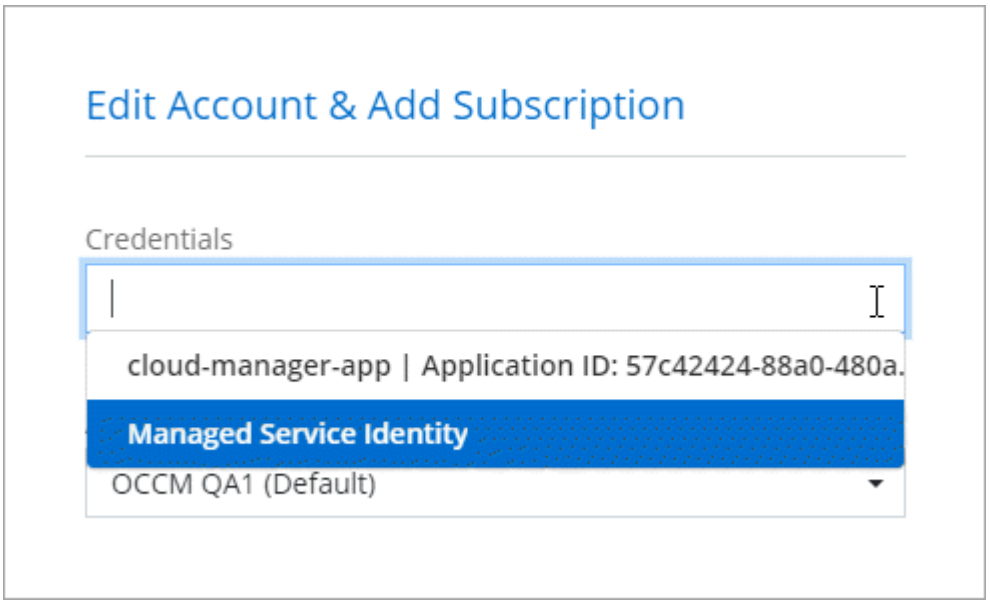
其他 **Azure** 凭据

如果要在控制台中使用不同的 Azure 凭据，则必须通过以下方式授予所需的权限"在 Microsoft Entra ID 中创建和设置服务主体"对于每个 Azure 帐户。下图显示了另外两个帐户，每个帐户都设置了服务主体和提供权限的自定义角色：



那么你会"将帐户凭据添加到控制台"通过提供有关 AD 服务主体的详细信息。

例如，您可以在创建新的Cloud Volumes ONTAP系统时在凭据之间切换：



凭证和市场订阅

您添加到控制台代理的凭据必须与 Azure Marketplace 订阅相关联，以便您可以按小时费率（PAYGO）或NetApp数据服务或通过年度合同支付Cloud Volumes ONTAP费用。

"了解如何关联 Azure 订阅" 。

请注意有关 Azure 凭据和市场订阅的以下事项：

- 只能将一个 Azure 市场订阅与一组 Azure 凭据关联
- 您可以使用新的订阅替换现有的市场订阅

常见问题解答

以下问题与凭证和订阅有关。

我可以更改**Cloud Volumes ONTAP**系统的 **Azure Marketplace** 订阅吗？

是的，你可以。当您更改与一组 Azure 凭据关联的 Azure 市场订阅时，所有现有和新的Cloud Volumes ONTAP系统都将根据新订阅收费。

"了解如何关联 Azure 订阅" 。

我可以添加多个 **Azure** 凭据，每个凭据都有不同的市场订阅吗？

属于同一 Azure 订阅的所有 Azure 凭据都将与同一 Azure 市场订阅相关联。

如果您有属于不同 Azure 订阅的多个 Azure 凭据，则这些凭据可以与同一个 Azure 市场订阅或不同的市场订阅相关联。

我可以将现有的**Cloud Volumes ONTAP**系统移动到不同的 **Azure** 订阅吗？

不可以，无法将与您的Cloud Volumes ONTAP系统关联的 Azure 资源移动到其他 Azure 订阅。

凭证如何用于市场部署和本地部署？

以上部分描述了控制台代理的推荐部署方法，即从控制台部署。您还可以从 Azure 市场在 Azure 中部署控制台代理，并且可以在自己的 Linux 主机上安装控制台代理软件。

如果您使用 Marketplace，您可以通过向控制台代理 VM 和系统分配的托管身份分配自定义角色来提供权限，或者您可以使用 Microsoft Entra 服务主体。

对于本地部署，您无法为控制台代理设置托管标识，但可以使用服务主体提供权限。

要了解如何设置权限，请参阅以下页面：

- 标准模式
  - "设置 Azure 市场部署的权限"
  - "设置本地部署的权限"
- 限制模式
  - "设置限制模式的权限"

管理**NetApp Console**的 **Azure** 凭据和市场订阅

添加和管理 Azure 凭据，以便NetApp Console具有在 Azure 订阅中部署和管理云资源所需的权限。如果您管理多个 Azure 市场订阅，则可以从“凭据”页面将每个订阅分配给不同的 Azure 凭据。

概述

有两种方法可以在控制台中添加额外的 Azure 订阅和凭据。

1. 将其他 Azure 订阅与 Azure 托管标识关联。
2. 要使用不同的 Azure 凭据部署Cloud Volumes ONTAP ，请使用服务主体授予 Azure 权限并将其凭据添加到控制台。

将其他 **Azure** 订阅与托管标识关联**Associate additional Azure subscriptions with a managed identity**

控制台使您能够选择要部署Cloud Volumes ONTAP 的Azure 凭据和 Azure 订阅。除非关联 "托管标识"通过这些订阅。

关于此任务

托管身份"初始 Azure 帐户"当您从控制台部署控制台代理时。部署控制台代理时，控制台会将控制台操作员角色分配给控制台代理虚拟机。

步骤

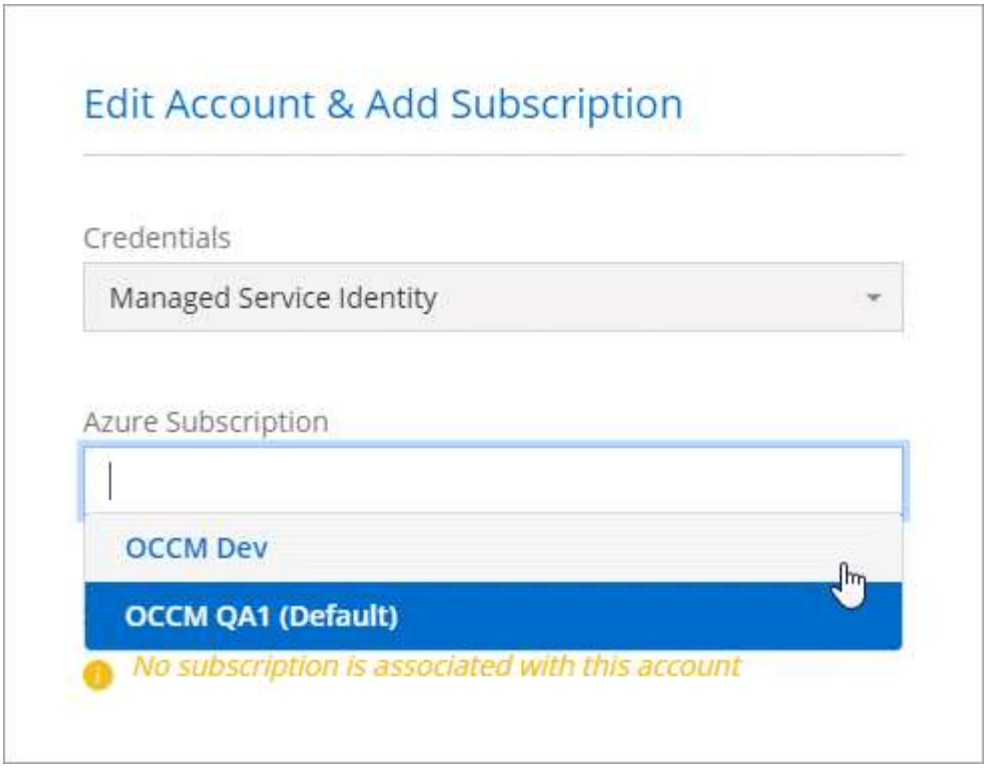
1. 登录 Azure 门户。
2. 打开*订阅*服务，然后选择要部署Cloud Volumes ONTAP 的订阅。
3. 选择*访问控制（IAM）*。
   a. 选择 添加 > 添加角色分配，然后添加权限：
      - 选择*控制台操作员*角色。

        控制台操作员是控制台代理策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

      - 分配对*虚拟机*的访问权限。
      - 选择创建控制台代理虚拟机的订阅。
      - 选择一个控制台代理虚拟机。
      - 选择*保存*。
4. 重复这些步骤以获得更多订阅。

结果

创建新系统时，您现在可以从多个 Azure 订阅中选择托管标识配置文件。



向**NetApp Console**添加其他 **Azure** 凭据

从控制台部署控制台代理时，控制台会在具有所需权限的虚拟机上启用系统分配的托管标识。当您为Cloud Volumes ONTAP创建新系统时，控制台会默认选择这些 Azure 凭据。

如果您在现有系统上手动安装了控制台代理软件，则不会添加初始凭据集。"了解 Azure 凭据和权限" 。

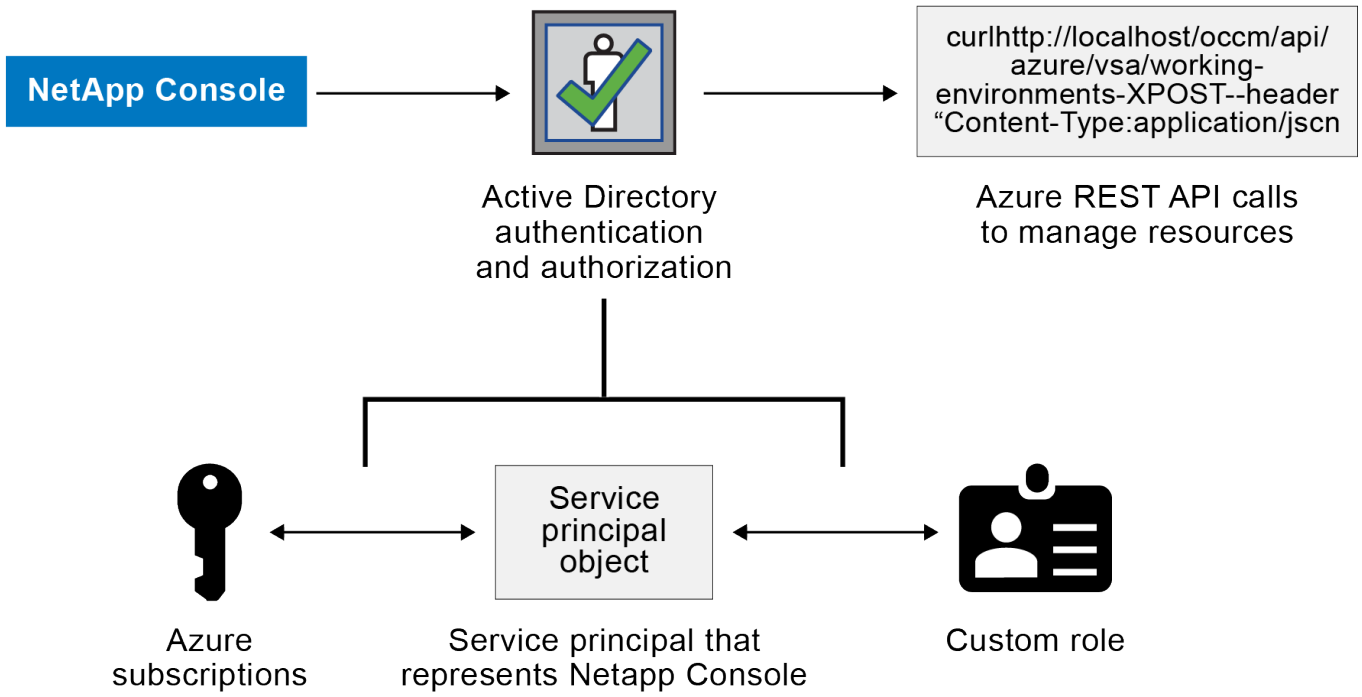
如果您想使用不同的 Azure 凭据部署Cloud Volumes ONTAP ，则必须通过在 Microsoft Entra ID 中为每个 Azure 帐户创建和设置服务主体来授予所需的权限。然后，您可以将新凭据添加到控制台。

使用服务主体授予 **Azure** 权限

控制台需要权限才能在 Azure 中执行操作。您可以通过在 Microsoft Entra ID 中创建和设置服务主体并获取控制台所需的 Azure 凭据来向 Azure 帐户授予所需的权限。

关于此任务

下图描述了控制台如何获取在 Azure 中执行操作的权限。服务主体对象与一个或多个 Azure 订阅绑定，代表 Microsoft Entra ID 中的控制台，并分配给允许所需权限的自定义角色。



步骤

1. 创建 Microsoft Entra 应用程序 。
2. [将应用程序分配给角色] 。
3. 添加 Windows Azure 服务管理 API 权限 。
4. 获取应用程序ID和目录ID 。
5. [创建客户端机密] 。

创建 **Microsoft Entra** 应用程序

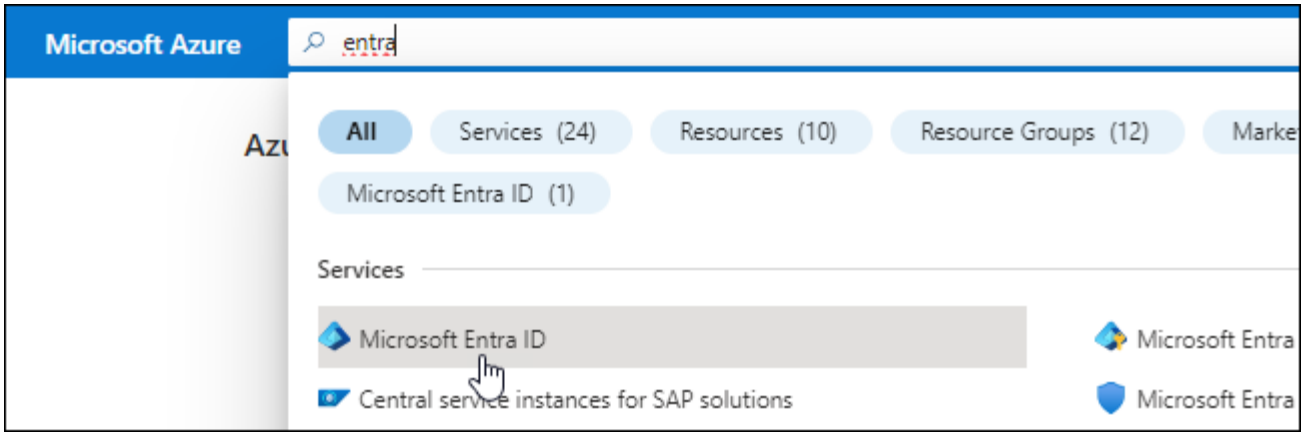
创建控制台可用于基于角色的访问控制的 Microsoft Entra 应用程序和服务主体。

步骤

1. 确保您在 Azure 中拥有创建 Active Directory 应用程序并将该应用程序分配给角色的权限。

   有关详细信息，请参阅 "Microsoft Azure 文档：所需权限"

2. 从 Azure 门户打开 **Microsoft Entra ID** 服务。



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
   - 名称：输入应用程序的名称。
   - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

   您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

您必须将服务主体绑定到一个或多个 Azure 订阅，并为其分配自定义“控制台操作员”角色，以便控制台在 Azure 中拥有权限。

步骤

1. 创建自定义角色：

   请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

   a. 复制"控制台代理的自定义角色权限"并将它们保存在 JSON 文件中。
   b. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

      您应该为用户将从中创建Cloud Volumes ONTAP系统的每个 Azure 订阅添加 ID。

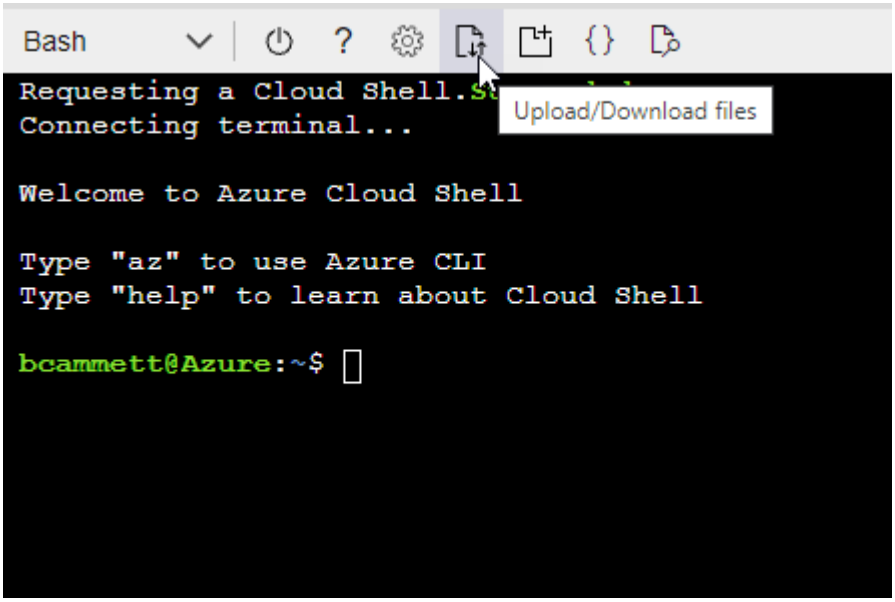
      例子

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]
```

c. 使用 JSON 文件在 Azure 中创建自定义角色。

以下步骤介绍如何使用 Azure Cloud Shell 中的 Bash 创建角色。

- 开始 "Azure 云外壳"并选择 Bash 环境。
- 上传 JSON 文件。



- 使用 Azure CLI 创建自定义角色：

```
az role definition create --role-definition agent_Policy.json
```

现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

2. 将应用程序分配给角色：

a. 从 Azure 门户打开 **Subscriptions** 服务。

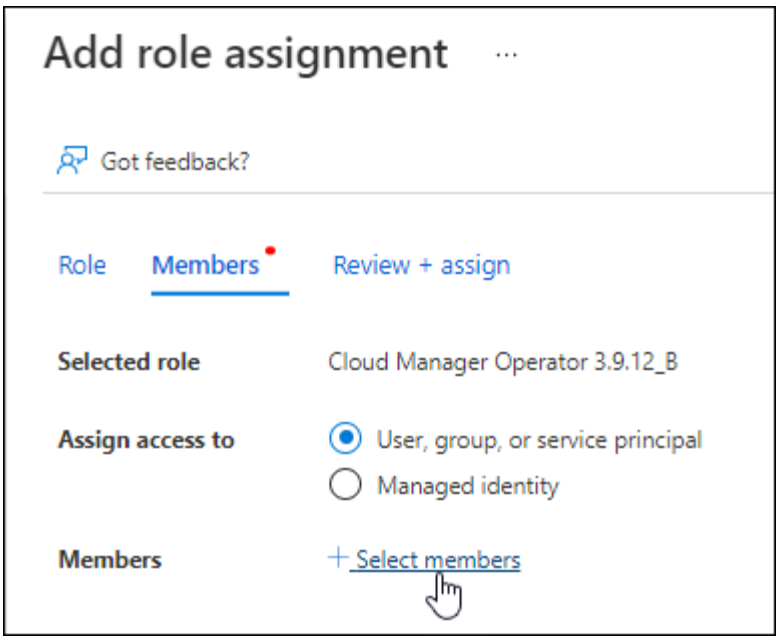
b. 选择订阅。

c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。

d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

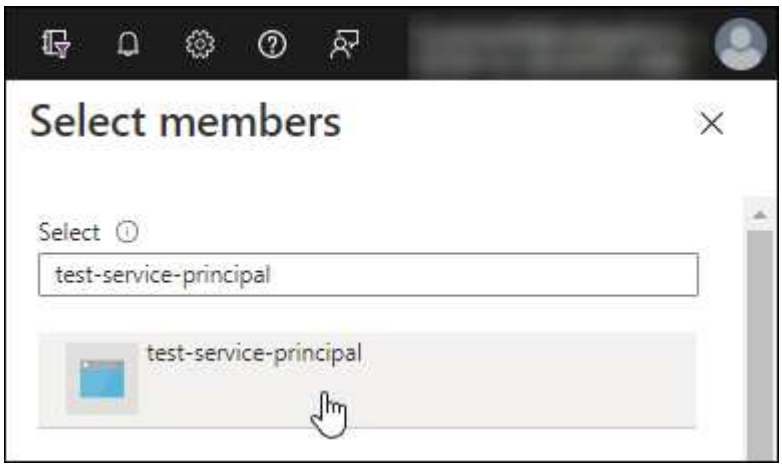
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

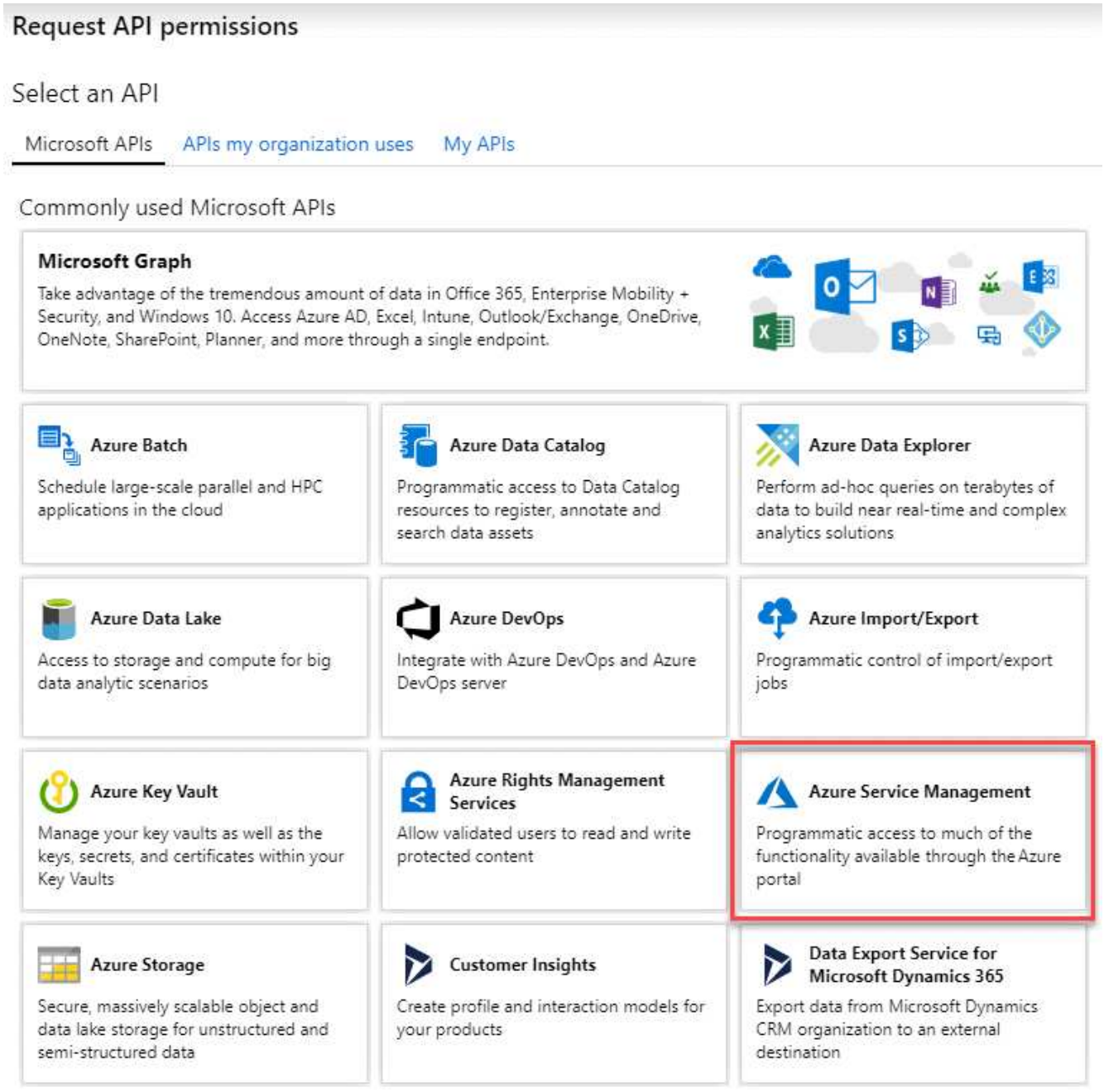
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

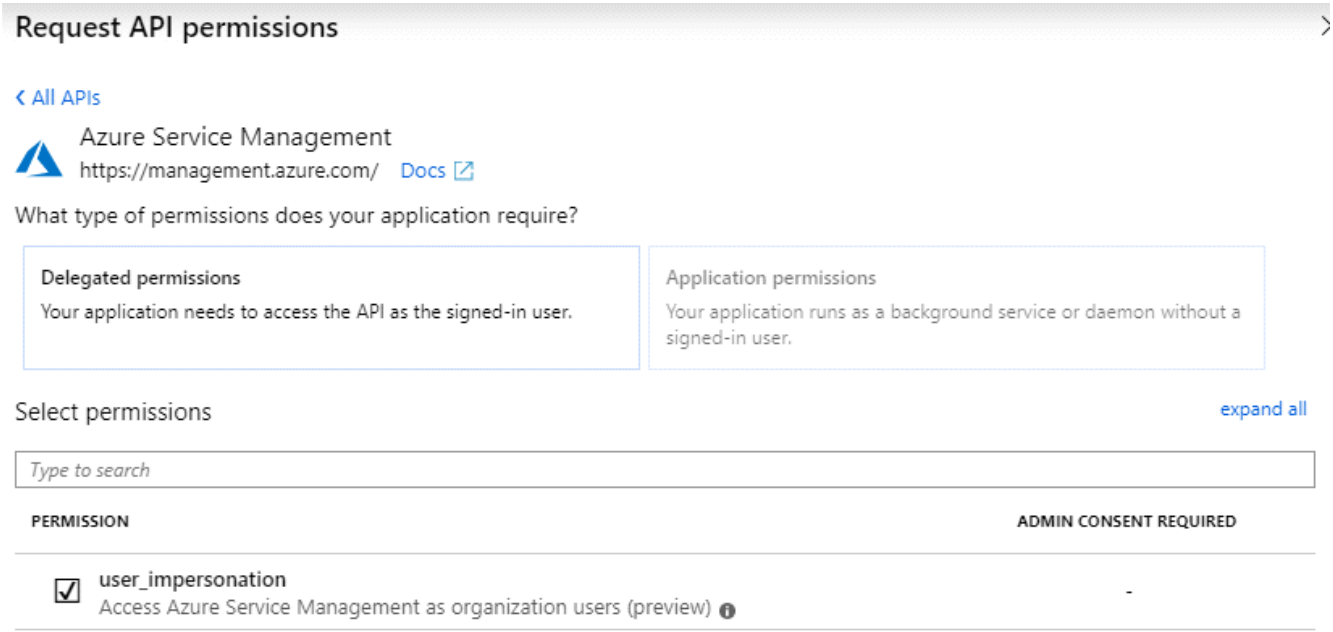
您必须为服务主体分配“Windows Azure 服务管理 API”权限。

步骤

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。



4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。

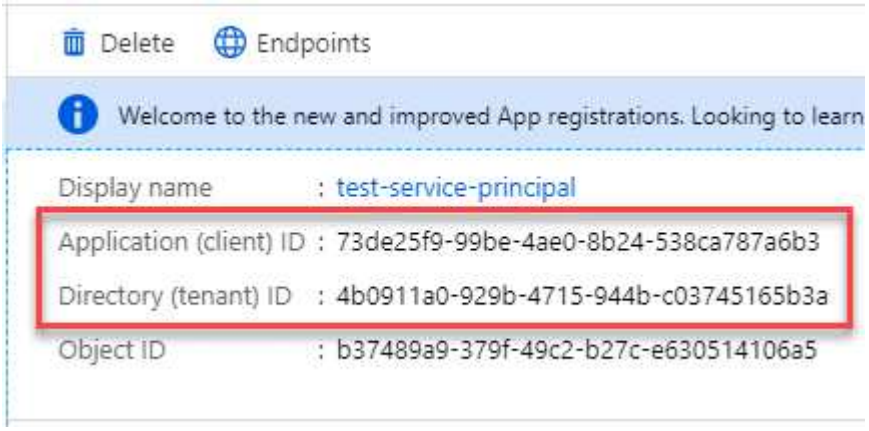


获取应用程序**ID**和目录**ID**

将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

步骤

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

创建客户端机密

创建客户端密钥并将其值提供给控制台以使用 Microsoft Entra ID 进行身份验证。

步骤

1. 开启*Microsoft Entra ID*服务。

2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。

结果

您的服务主体现已设置，您应该已经复制了应用程序（客户端）ID、目录（租户）ID 和客户端机密的值。添加 Azure 帐户时，您需要在控制台中输入此信息。

将凭据添加到控制台

为 Azure 帐户提供所需权限后，您可以将该帐户的凭据添加到控制台。完成此步骤后，您可以使用不同的 Azure 凭据启动Cloud Volumes ONTAP 。

开始之前

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟才能使用它们。等待几分钟，然后将凭据添加到控制台。

开始之前

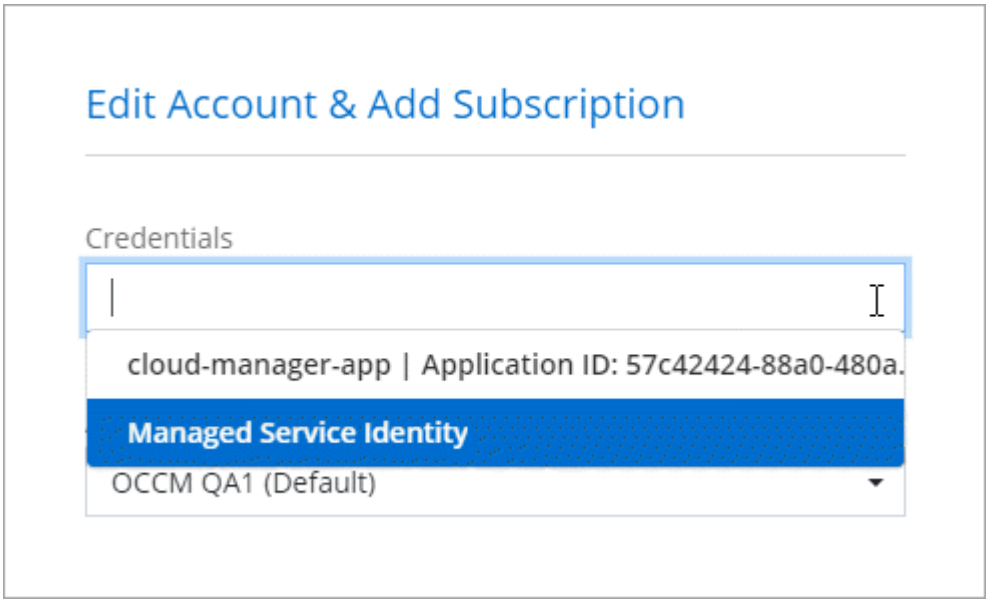
您需要先创建控制台代理，然后才能更改控制台设置。"了解如何创建控制台代理" 。

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
   a. 凭证位置：选择*Microsoft Azure > 代理*。
   b. 定义凭据：输入有关授予所需权限的 Microsoft Entra 服务主体的信息：
      - 应用程序（客户端）ID
      - 目录（租户）ID
      - 客户端密钥
   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证关联。
   d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

您可以从“详细信息和凭证”页面切换到另一组凭证 "将系统添加到控制台时"



管理现有凭证

通过关联 Marketplace 订阅、编辑凭据和删除凭据来管理已添加到控制台的 Azure 凭据。

将 **Azure** 市场订阅关联到凭据

将 Azure 凭据添加到控制台后，您可以将 Azure 市场订阅与这些凭据关联。您可以使用订阅来创建按使用量付费的Cloud Volumes ONTAP系统并访问NetApp数据服务。

在将凭据添加到控制台后，可以在两种情况下关联 Azure 市场订阅：

- 当您最初将凭据添加到控制台时，您没有关联订阅。
- 您想要更改与 Azure 凭据关联的 Azure 市场订阅。

  替换当前的市场订阅会针对现有和新的Cloud Volumes ONTAP系统进行更新。

步骤

1. 选择“管理 **>** 凭证”。
2. 选择*组织凭证*。
3. 选择与控制台代理关联的一组凭据的操作菜单，然后选择*配置订阅*。

   您必须选择与控制台代理关联的凭据。您无法将市场订阅与与NetApp Console关联的凭据关联。

4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭据与新订阅关联，请选择“添加订阅”>“继续”*，然后按照 Azure 市场中的步骤操作：

   a. 如果出现提示，请登录您的 Azure 帐户。

   b. 选择*订阅*。

   c. 填写表格并选择*订阅*。

d. 订阅过程完成后，选择*立即配置帐户*。

您将被重定向到NetApp Console。

e. 从“订阅分配”页面：

- 选择您想要与此订阅关联的控制台组织或帐户。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

编辑凭据

在控制台中编辑您的 Azure 凭据。例如，如果为服务主体应用程序创建了新的密钥，您可以更新客户端密钥。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择一组凭证的操作菜单，然后选择*编辑凭证*。
4. 进行所需的更改，然后选择*应用*。

删除凭据

如果您不再需要一组凭证，您可以删除它们。您只能删除与系统无关的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 在*组织凭证*页面上，选择一组凭证的操作菜单，然后选择*删除凭证*。
4. 选择*删除*进行确认。

Google Cloud

了解 **Google Cloud** 项目和权限

了解NetApp Console如何使用 Google Cloud 凭证代表您执行操作以及这些凭证如何与市场订阅相关联。了解这些详细信息有助于您管理一个或多个 Google Cloud 项目的凭据。例如，您可能想要了解与控制台代理 VM 关联的服务帐户。

NetApp Console的项目和权限

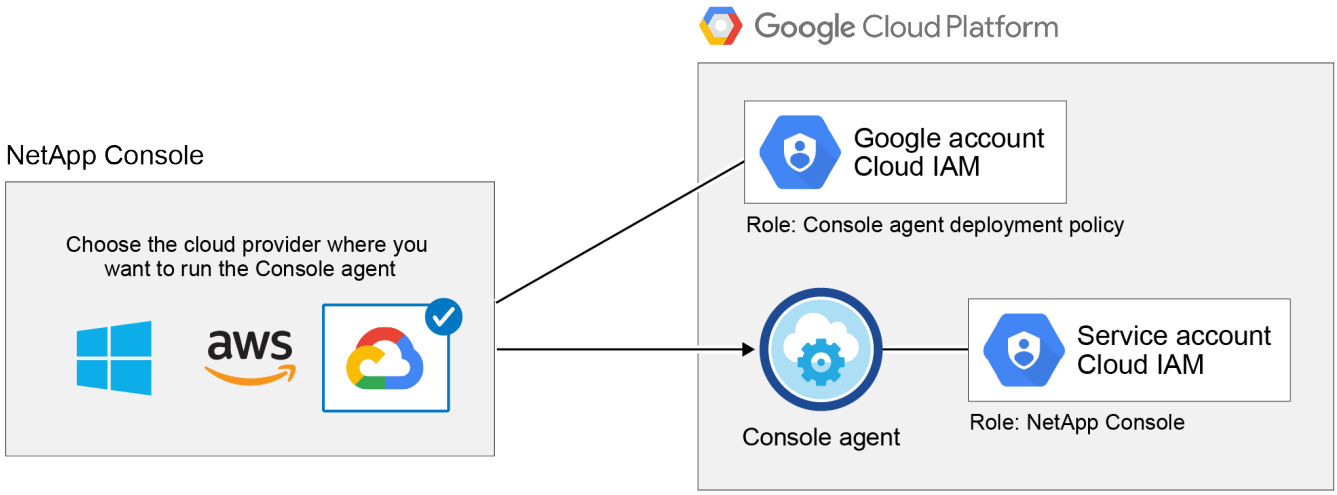
您必须先部署控制台代理，然后才能使用控制台管理 Google Cloud 项目中的资源。代理不能在您的场所或不同

的云提供商中运行。

直接从控制台部署控制台代理之前，必须具备两组权限：

1. 您需要使用具有从控制台启动控制台代理权限的 Google 帐户部署控制台代理。
2. 部署控制台代理时，系统会提示您选择 "服务帐户"对于代理控制台从服务帐户获取权限来创建和管理Cloud Volumes ONTAP系统、使用NetApp备份和恢复管理备份等等。通过将自定义角色附加到服务帐户来提供权限。

下图描述了上面第 1 项和第 2 项中描述的权限要求：



要了解如何设置权限，请参阅以下页面：

- "设置标准模式的 Google Cloud 权限"
- "设置限制模式的权限"

凭证和市场订阅

当您在 Google Cloud 中部署控制台代理时，控制台会为控制台代理所在项目中的 Google Cloud 服务帐号创建一组默认凭据。这些凭证必须与 Google Cloud Marketplace 订阅相关联，以便您可以支付Cloud Volumes ONTAP和NetApp数据服务的费用。

"了解如何关联 Google Cloud Marketplace 订阅" 。

请注意以下有关 Google Cloud 凭据和市场订阅的事项：

- 一个控制台代理只能关联一组 Google Cloud 凭据
- 您只能将一个 Google Cloud Marketplace 订阅与凭据关联
- 您可以使用新的订阅替换现有的市场订阅

Cloud Volumes ONTAP项目

Cloud Volumes ONTAP可以与控制台代理位于同一项目中，也可以位于不同的项目中。要在不同的项目中部署Cloud Volumes ONTAP ，您需要首先将控制台代理服务帐户和角色添加到该项目。

- "了解如何设置服务帐户"
- "了解如何在 Google Cloud 中部署Cloud Volumes ONTAP并选择项目"

管理 **Google Cloud** 部署的控制台代理权限

NetApp有时会在将控制台代理部署到 Google Cloud 时更新用于该代理的服务帐户所需的权限。

"核实所需的 Google 权限列表"。

使用 Google Cloud 控制台更新分配给服务帐号的 IAM 角色，使其与新的权限集匹配。

"Google Cloud 文档：编辑自定义角色"

管理与**NetApp Console**关联的 **NSS** 凭据

将NetApp支持站点帐户与您的控制台组织关联，以启用存储管理的关键工作流程。这些 NSS 凭证与整个组织相关。

控制台还支持每个用户帐户关联一个 NSS 帐户。"了解如何管理用户级凭证" 。

概述

需要将NetApp支持站点凭据与您的特定控制台帐户序列号关联才能启用以下任务：

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

  需要提供您的 NSS 帐户，以便控制台可以上传您的许可证密钥并启用您购买的期限的订阅。这包括期限续订的自动更新。

- 注册即用即付Cloud Volumes ONTAP系统

  需要提供您的 NSS 帐户才能激活对您的系统的支持并获得对NetApp技术支持资源的访问权限。

- 将Cloud Volumes ONTAP软件升级到最新版本

这些凭证与您的特定控制台帐户序列号相关联。用户可以从*支持 > NSS 管理*访问这些凭据。

添加 **NSS** 帐户

您可以从控制台中的支持信息板添加和管理用于控制台的NetApp支持站点帐户。

当您添加了 NSS 帐户后，控制台会使用此信息进行许可证下载、软件升级验证和未来支持注册等。

您可以将多个 NSS 帐户与您的组织关联；但是，您不能在同一个组织内拥有客户帐户和合作伙伴帐户。

NetApp使用 Microsoft Entra ID 作为特定于支持和许可的身份验证服务的身份提供者。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 选择*添加 NSS 帐户*。
4. 选择“继续”以重定向到 Microsoft 登录页面。
5. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码。

   成功登录后， NetApp将存储 NSS 用户名。

   这是系统生成的映射到您的电子邮件的 ID。在*NSS 管理*页面上，您可以显示来自 ••• 菜单。

   - 如果您需要刷新登录凭证令牌，还有一个*更新凭证*选项 ••• 菜单。

     使用此选项会提示您再次登录。请注意，这些帐户的令牌将在 90 天后过期。我们将发布通知来提醒您此事。

下一步是什么?

用户现在可以在创建新的Cloud Volumes ONTAP系统和注册现有Cloud Volumes ONTAP系统时选择帐户。

- "在 AWS 中启动Cloud Volumes ONTAP"
- "在 Azure 中启动Cloud Volumes ONTAP"
- "在 Google Cloud 中启动Cloud Volumes ONTAP"
- "注册现收现付系统"

更新 **NSS** 凭证

出于安全原因，您必须每 90 天更新一次您的 NSS 凭据。如果您的 NSS 凭证已过期，您将在控制台通知中心收到通知。"了解通知中心" 。

过期的凭证可能会影响以下情况，但不限于：

- 许可证更新，这意味着您将无法利用新购买的容量。
- 能够提交和跟踪支持案例。

此外，如果您想更改与您的组织关联的 NSS 帐户，您可以更新与您的组织关联的 NSS 凭据。例如，如果与您的 NSS 帐户关联的人员已离开您的公司。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要更新的 NSS 帐户，选择 ••• 然后选择*更新凭证*。
4. 当出现提示时，选择“继续”以重定向到 Microsoft 登录页面。

   NetApp使用 Microsoft Entra ID 作为与支持和许可相关的身份验证服务的身份提供者。

5. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码。

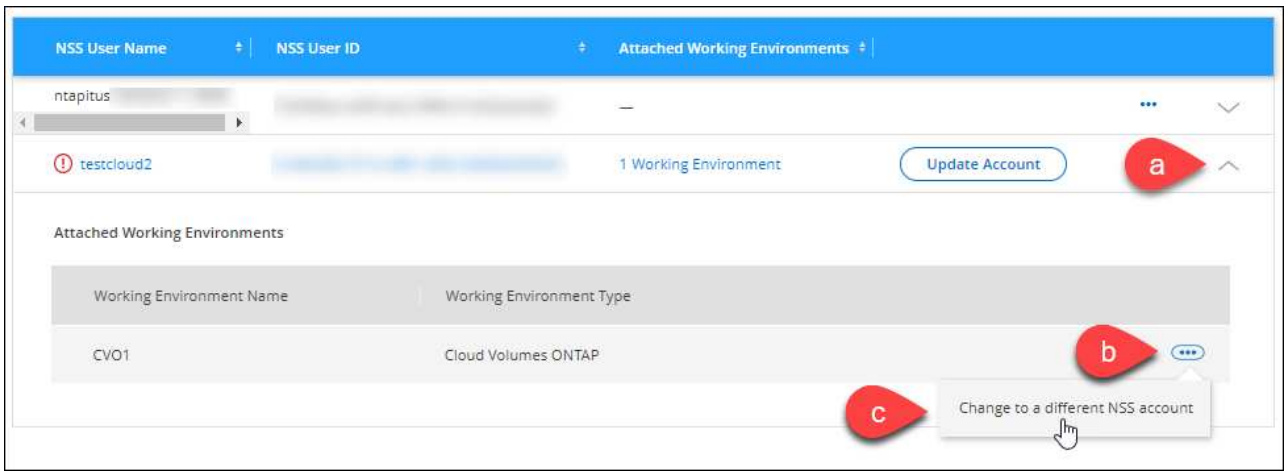
将系统附加到不同的 NSS 帐户

如果您的组织有多个NetApp支持站点帐户，您可以更改与Cloud Volumes ONTAP系统关联的帐户。

您必须首先将帐户与控制台关联。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 完成以下步骤来更改 NSS 帐户：
   a. 展开系统当前关联的NetApp支持站点帐户的行。
   b. 对于要更改关联的系统，选择 •••
   c. 选择*更改为不同的 NSS 帐户*。



   d. 选择帐户，然后选择*保存*。

显示 NSS 帐户的电子邮件地址

为了安全起见，默认情况下不显示与 NSS 帐户关联的电子邮件地址。您可以查看 NSS 帐户的电子邮件地址和关联的用户名。

当您转到 NSS 管理页面时，控制台会为表中的每个帐户生成一个令牌。该令牌包含有关关联电子邮件地址的信息。当您离开页面时，令牌将被删除。信息永远不会被缓存，这有助于保护您的隐私。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要更新的 NSS 帐户，选择 ••• 然后选择*显示电子邮件地址*。您可以使用复制按钮复制电子邮件地址。

删除 NSS 帐户

删除不再想在控制台中使用的所有 NSS 帐户。

您无法删除当前与Cloud Volumes ONTAP系统关联的帐户。你首先需要将这些系统附加到不同的 NSS 帐户。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要删除的 NSS 帐户，选择 ••• 然后选择*删除*。
4. 选择*删除*进行确认。

管理与您的NetApp Console登录关联的凭据

根据您在控制台中执行的操作，您可能已将ONTAP凭据和NetApp支持站点 (NSS) 凭据与您的用户登录关联。关联这些凭证后，您可以查看和管理它们。例如，如果您更改这些凭据的密码，则需要在控制台中更新密码。

ONTAP凭据

用户需要ONTAP管理员凭据才能在控制台中发现ONTAP集群。但是， ONTAP系统管理器访问取决于您是否使用控制台代理。

无需控制台代理

系统会提示用户输入其ONTAP凭据以访问集群的ONTAP系统管理器。用户可以选择将这些凭据保存在控制台中，这意味着他们不必每次都输入这些凭据。用户凭证仅对相应用户可见，并且可以从用户凭证页面进行管理。

使用控制台代理

默认情况下，不会提示用户输入其ONTAP凭据来访问ONTAP系统管理器。但是，控制台管理员（具有组织管理员角色）可以配置控制台以提示用户输入其ONTAP凭据。启用此设置后，用户每次都需要输入其ONTAP凭据。

"了解更多信息。"

NSS 凭证

与您的NetApp Console登录关联的 NSS 凭据可支持注册、案例管理和访问Digital Advisor。

- 当您访问*支持>资源*并注册支持时，系统会提示您将 NSS 凭据与您的登录名关联。

  这将注册您的组织或帐户以获得支持并激活支持权利。您的组织中只有一个用户必须将NetApp支持站点帐户与其登录名关联，以注册支持并激活支持权利。完成后，“资源”页面将显示您的帐户已注册支持。

  "了解如何注册以获得支持"

- 当您访问*管理 > 支持 > 案例管理*时，如果您还没有输入 NSS 凭证，系统会提示您输入。此页面使您能够创建和管理与您的 NSS 帐户和公司相关的支持案例。
- 当您在控制台中访问Digital Advisor时，系统会提示您输入 NSS 凭据登录Digital Advisor 。

请注意与您的登录名关联的 NSS 帐户的以下事项：

- 该帐户在用户级别进行管理，这意味着其他登录的用户无法查看该帐户。
- 每个用户只能有一个与Digital Advisor和支持案例管理关联的 NSS 帐户。

- 如果您尝试将NetApp支持站点帐户与Cloud Volumes ONTAP系统关联，则只能从添加到您所属组织的 NSS 帐户中进行选择。

  NSS 帐户级凭据与与您的登录关联的 NSS 帐户不同。 NSS 帐户级凭证使您能够使用 BYOL 部署Cloud Volumes ONTAP 、注册 PAYGO 系统并升级其软件。

  "了解有关将 NSS 凭据与您的NetApp Console组织或帐户结合使用的更多信息" 。

管理您的用户凭证

通过更新用户名和密码或删除凭证来管理您的用户凭证。

步骤

1. 选择“管理 > 凭证”。
2. 选择*用户凭证*。
3. 如果您还没有任何用户凭证，您可以选择*添加 NSS 凭证*来添加您的NetApp支持站点帐户。
4. 通过从“操作”菜单中选择以下选项来管理现有凭据：
   - 更新凭据：更新帐户的用户名和密码。
   - 删除凭据：删除与您的控制台登录关联的 NSS 帐户。

监控NetApp Console操作

您可以监视控制台正在执行的操作的状态，以查看是否存在需要解决的问题。您可以从审核页面、通知中心查看状态，或将通知发送到您的电子邮件。

该表通过比较突出了审计页面和通知中心的功能。

通知中心	审计页面
显示事件和动作的高级状态	提供每个事件或行动的详细信息以供进一步调查
显示当前登录会话的状态（注销后，该信息不会出现在通知中心）	保留上个月的状态
仅显示在用户界面中发起的操作	显示来自 UI 或 API 的所有操作
显示用户发起的操作	显示所有操作，无论是用户发起的还是系统发起的
按重要性过滤结果	按服务、操作、用户、状态等进行过滤
提供向用户和其他人发送电子邮件通知的功能	没有电子邮件功能

从审核页面审核用户活动

审计页面显示用户为管理您的组织或帐户而完成的操作。这包括关联用户、创建系统、创建代理等管理操作。

使用审计页面来识别谁执行了操作或其状态。

步骤

1. 选择“管理”>“审计”。
2. 使用表格上方的过滤器来更改表格中显示的操作。

   例如，您可以使用*服务*过滤器显示与特定服务相关的操作，或者可以使用*用户*过滤器显示与特定用户帐户相关的操作。

从审计页面下载审计日志

您可以将审计日志从审计页面下载到 CSV 文件中。这使您能够记录用户在您的组织中执行的操作。 CSV 文件包含下载的 CSV 文件中的所有列，无论审计页面上的过滤器或显示的列如何。

步骤

1. 在*审计*页面中，选择表格右上角的下载图标。

使用通知中心监控活动

通知跟踪控制台操作以确认成功。它们使您能够查看在当前登录会话期间启动的许多控制台操作的状态。并非所有控制台服务都会将信息报告到通知中心。

您可以通过选择通知铃来显示通知（  ）在菜单栏中。铃铛中小气泡的颜色表示处于活动状态的最高级别严重性通知。因此，如果您看到红色气泡，则表示有重要的通知需要您查看。

您还可以配置控制台通过电子邮件发送某些类型的通知，这样即使您未登录系统也可以了解重要的系统活动。电子邮件可以发送给您组织中的任何用户，或任何其他需要了解某些类型的系统活动的收件人。了解如何设置电子邮件通知设置。

比较通知中心和警报

通知中心使您能够查看已启动的操作的状态并为某些类型的系统活动设置警报通知。同时，警报使您能够查看ONTAP存储环境中与容量、可用性、性能、保护和安全性相关的问题或潜在风险。

"了解有关NetApp Console警报的更多信息"

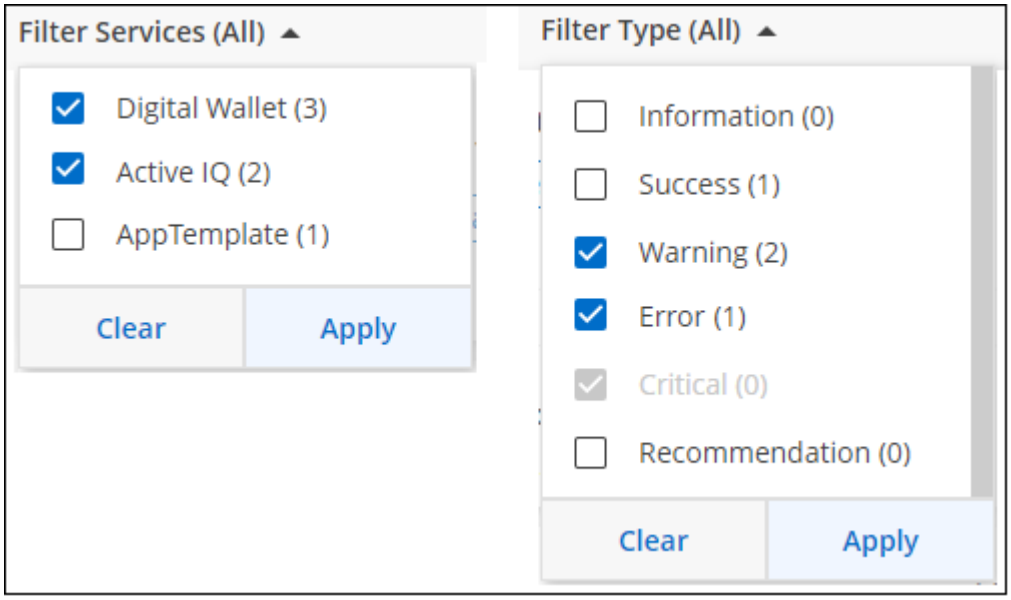
通知类型

控制台将通知分为以下类别：

通知类型	描述
批判的	出现问题，如果不立即采取纠正措施，可能会导致服务中断。
错误	一项行动或过程以失败告终，或者如果不采取纠正措施则可能导致失败。
警告	您应该注意这个问题，以确保其不会达到严重程度。这种严重程度的通知不会导致服务中断，并且可能不需要立即采取纠正措施。
建议	系统建议您采取行动来改进系统或某项服务；例如：节省成本、新服务建议、推荐安全配置等。
信息	提供有关操作或过程的附加信息的消息。
成功	动作或过程成功完成。

过滤通知

默认情况下，您会在通知中心看到所有活动通知。您可以过滤看到的通知，以仅显示对您重要的通知。您可以按“服务”和通知“类型”进行过滤。



例如，如果您只想查看控制台操作的“错误”和“警告”通知，请选择这些条目，您将只看到这些类型的通知。

关闭通知

如果您不再需要查看通知，可以从页面中删除它们。您可以单独或一次性关闭所有通知。

要关闭所有通知，请在通知中心选择:并选择*全部关闭*。

要关闭单个通知，请将光标悬停在通知上并选择*关闭*。

设置电子邮件通知设置

您可以通过电子邮件发送特定类型的通知，这样即使您未登录也可以获知重要的系统活动。电子邮件可以发送给您组织或帐户中的任何用户，或任何其他需要了解某些类型的系统活动的收件人。

- 控制台发送代理、许可证和订阅、 NetApp Copy and Sync以及NetApp Backup and Recovery的电子邮件通知。
- 当控制台代理安装在没有互联网访问的站点时，不支持发送电子邮件通知。

您在通知中心设置的过滤器不会决定您通过电子邮件收到的通知类型。默认情况下，任何组织管理员都会收到所有“关键”和“建议”通知的电子邮件。这些通知涵盖所有服务 - 您不能选择仅接收某些服务的通知，例如代理或NetApp Backup and Recovery。

所有其他用户和收件人都配置为不接收任何通知电子邮件 - 因此您需要为任何其他用户配置通知设置。

您必须具有组织管理员角色才能自定义通知设置。

步骤

1. 选择*管理>通知设置*。
2. 选择*组织用户*或*其他收件人*。

   *其他收件人*页面允许您配置控制台以通知控制台组织的成员。

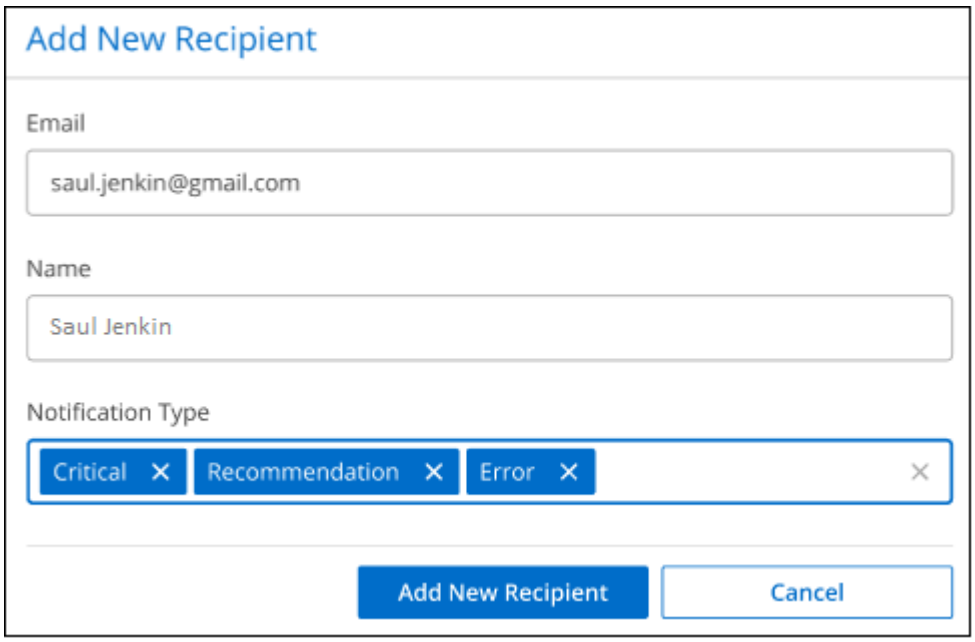
3. 从“组织用户”页面或“其他收件人”页面中选择一个或多个用户，然后选择要发送的通知类型：
   - 要对单个用户进行更改，请选择该用户的通知列中的菜单，检查要发送的通知类型，然后选择*应用*。
   - 要对多个用户进行更改，请选中每个用户的复选框，选择*管理电子邮件通知*，检查要发送的通知类型，然后选择*应用*。

添加其他电子邮件收件人

_组织用户_页面中显示的用户是从您的组织或帐户中的用户自动填充的。您可以在“其他收件人”页面中为其他无权访问控制台但需要收到某些类型的警报和通知的个人或团体添加电子邮件地址。

步骤

1. 从*通知设置*页面中，选择*添加新收件人*。



2. 输入姓名、电子邮件地址，选择收件人将收到的通知类型，然后选择*添加新收件人*。