身份和访问管理

NetApp Console setup and administration

NetApp
February 11, 2026

目录

身份和访问管理

了解NetApp Console身份和访问管理

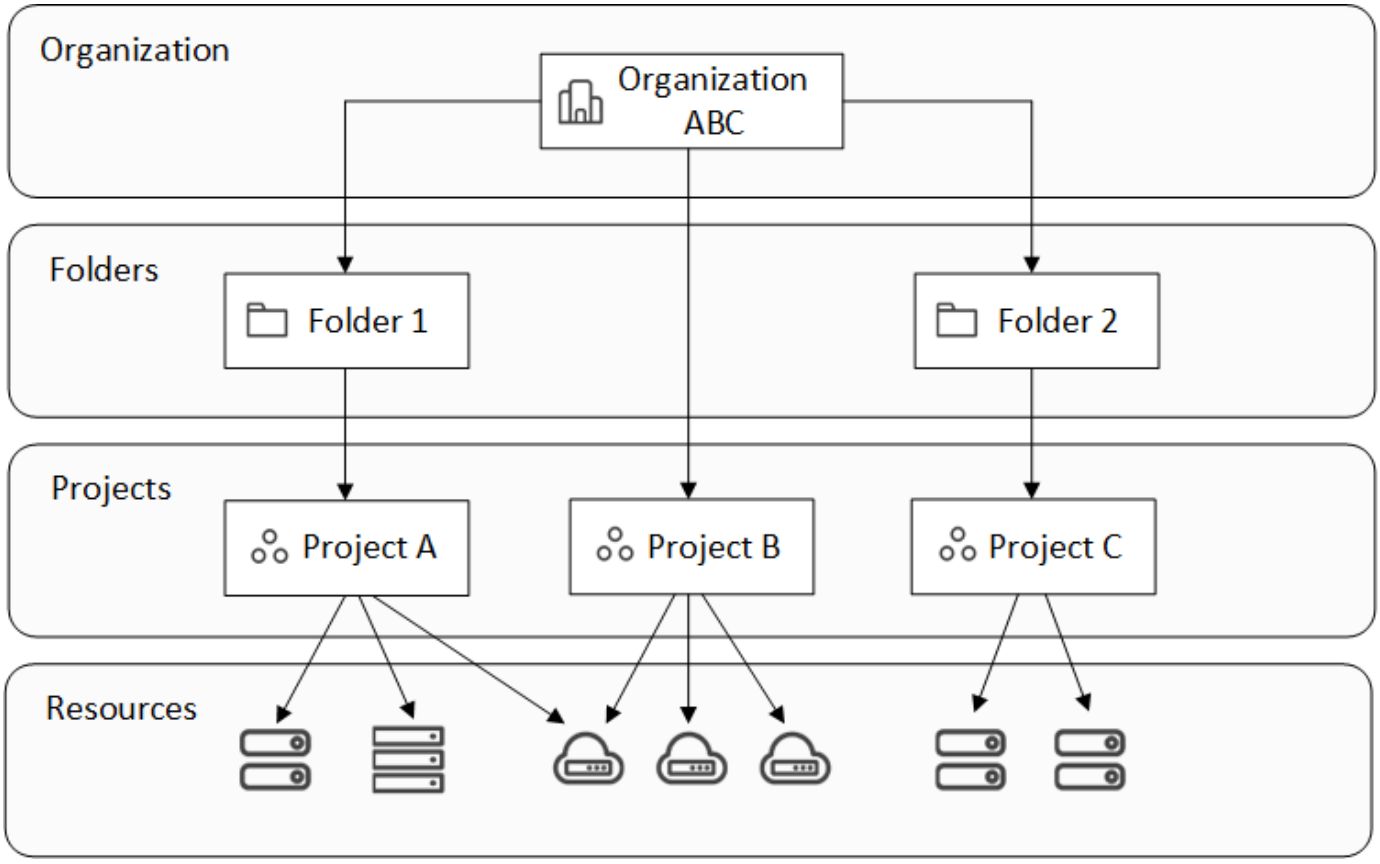
使用NetApp控制台的身份和访问管理 (IAM) 来组织您的NetApp资源，并根据您的业务结构（按位置、部门或项目）控制访问权限。

资源按层级排列：组织位于顶层，其次是文件夹（可以包含其他文件夹或项目），然后是项目，项目包含存储系统、工作负载和代理。

在组织、文件夹或项目级别分配访问角色，以便用户有权访问资源。

您必须拥有_超级管理员_、_组织管理员_或_文件夹或项目管理员_角色才能在NetApp Console中管理 IAM。

下图从基本层面说明了这一层次结构。



]

身份和访问管理组件

在NetApp Console中，您可以使用三个主要组件来组织存储资源：组织组件、资源组件和用户访问组件。

组织内的项目和文件夹

在您的 IAM 结构中，您使用三个组织组件：组织、项目和文件夹。您可以通过为用户分配以下任何级别的角色来授予他们访问权限。

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。

项目

项目用于提供对存储资源的访问。必须先将资源分配给项目，其他人才能访问这些资源。您可以将多个资源分配给一个项目，也可以创建多个项目。然后，您可以为用户分配项目权限，使他们能够访问项目中的资源。

例如，您可以根据需要，将本地ONTAP系统与单个项目或组织中的所有项目关联起来。

"了解如何向您的组织添加项目。"

文件夹

将相关项目分组到_文件夹_中，以便按位置、站点或业务部门进行组织。您无法直接将资源与文件夹关联，但将用户分配到文件夹级别的角色，即可使其访问该文件夹中的所有项目。

"了解如何向您的组织添加文件夹。"

资源

resource 是 NetApp Console 知道并可以分配给项目的实体。*Resources* 包括存储系统、Keystone 订阅、某些 NetApp Backup and Recovery 工作负载以及 NetApp Console 代理。

+ 必须先将资源与项目关联，其他人才能访问该资源。

+

例如，您可以将Cloud Volumes ONTAP系统与一个项目或组织中的所有项目关联起来。资源的分配方式取决于贵组织的需求。

+

"了解如何将资源关联到项目。"

存储系统和**Keystone**订阅

存储系统是您在 NetApp Console 中管理的主要资源。NetApp Console 支持本地和云存储系统的管理。必须将存储系统添加到项目中，以便分配给项目的人员可以访问它。

存储系统

存储系统会自动与添加它们的项目关联，但您可以从*资源*页面将其与其他项目或文件夹关联。您无法将 FSx for NetApp ONTAP 存储系统与项目或文件夹关联，但您可以在*系统*页面或从工作负载中查看它们。

Keystone订阅

Keystone订阅也是您可以与项目关联的资源，以便授予用户在NetApp Console中访问订阅的权限。

备份和恢复工作负载（**Oracle** 和 **Microsoft SQL Server**）

一些 Backup and Recovery 工作负载也被视为资源。您可以分配用户权限来访问 Backup and

控制台代理

组织管理员创建控制台代理来管理存储系统并启用NetApp数据服务。代理最初与创建它们的项目关联，但管理员可以从“代理”页面将它们添加到其他项目或文件夹。

将代理与项目关联起来，可以管理该项目中的资源；而将代理与文件夹关联起来，可以让文件夹或项目管理员决定哪些项目应该使用该代理。代理人必须与特定项目关联才能提供管理能力。

"了解如何将代理商与项目关联起来。"

成员及角色

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。

成员注册NetApp Console后，您需要将他们添加到您的组织中。添加完成后，您可以为他们分配角色，以便授予他们访问资源的权限。您可以手动从控制台添加服务帐户，也可以通过NetApp ConsoleIAM API 自动创建和管理服务帐户。

"了解如何向您的组织添加成员。"

访问角色

控制台提供您可以分配给组织成员的访问角色。

将成员与角色关联时，您可以为整个组织、特定文件夹或特定项目授予该角色。您选择的角色赋予成员对层次结构中选定部分的资源的权限。

NetApp Console提供细粒度的角色控制，遵循“最小权限”原则，这意味着访问角色旨在仅向用户授予其所需的权限。

这意味着随着用户职责的增加，他们可能会被分配多个角色。

"了解访问角色" 。

IAM 策略示例

小型组织战略

对于用户少于 50 人且采用集中式存储管理的组织，可以考虑使用超级管理员和超级查看者角色的简化方法。

示例：**ABC**公司（**5**人团队）

- 组织结构： 单一组织，下设 3 个项目（生产、开发、备份）
- 角色：
  - 2 位高级成员：拥有*超级管理员*角色，可获得完整的管理权限
  - 3 名团队成员：*超级查看者*角色，拥有监控权限但无修改权限
- 代理策略：所有项目都关联一个代理，以实现资源共享访问。

- 优势：简化管理，降低角色复杂性，适合需要广泛访问权限的团队

多区域企业战略

对于拥有区域运营和专业团队的大型组织，应采用层级式方法，用文件夹表示地理或业务单元边界。

例如：**XYZ**公司（跨国公司）

- 结构： 组织结构 > 区域文件夹（北美、欧洲、亚太） > 每个区域的项目文件夹
- 平台角色：
  - 1 组织管理：全球监督和政策管理
  - 3 文件夹或项目管理员：区域控制（每个区域一个）
  - 1 联盟管理员：企业身份提供商集成
- 按区域划分的存储角色：
  - 9 存储管理员：发现和管理指定区域中的存储系统
  - 2 存储查看器：监控跨区域的存储资源
  - 1 系统健康专家：无需修改系统即可管理存储健康状况
- 数据服务角色：
  - 备份和恢复管理员：按项目根据备份职责而定
  - 勒索软件恢复管理员：负责跨项目的安全团队监控
- 代理策略：与相应地理项目相关的区域代理
- 优势： 通过角色分离、区域自主权和遵守当地法规来增强安全性

部门专业化战略

对于拥有需要特定数据服务访问权限的专业团队的组织，应根据职能职责进行有针对性的角色分配。

例如：**TechCorp**（一家中型科技公司）

- 结构： 组织 > 部门文件夹（IT、安全、开发） > 项目特定资源
- 专业岗位：
  - 安全团队：*勒索软件恢复管理员*和*分类查看器*角色
  - 备份团队：备份和恢复超级管理员，负责全面的备份操作
  - 开发团队：测试环境管理存储管理员
  - 合规团队：运营支持分析师，负责监控和支持案例管理
- 代理策略： 根据资源所有权将代理与部门项目关联起来
- 优势： 可定制的访问控制、更高的运营效率以及明确的专项任务责任划分

NetApp Console中 IAM 的后续步骤

- "开始使用NetApp Console中的 IAM"

- "监控或审计 IAM 活动"
- "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。

您需要拥有*组织管理员*或*超级管理员*权限才能管理组织的身份和访问权限。拥有*文件夹或项目管理员*权限，您只能管理您有权访问的文件夹和项目。

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

用户注册NetApp Console后，您必须明确地将他们添加到您的 Console 组织中。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"

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"

设置您的控制台组织

将文件夹和项目添加到NetApp Console组织

添加文件夹和项目，以匹配您的业务结构。创建文件夹和项目后，您可以将资源与它们关联起来，并管理成员对这些项目的访问权限。

创建新组织时，控制台会自动为您创建一个项目。大多数组织都需要多个项目，以及文件夹来保持井然有序。"了解NetApp Console中的资源层次结构"。

使用文件夹和项目来组织资源

在NetApp Console中，组织包含文件夹和项目，可帮助您组织资源。文件夹可以帮助您对相关项目进行分组，项目可以帮助您管理资源和成员访问权限。

文件夹

文件夹可以帮助您整理相关项目。您可以创建嵌套文件夹来表示组织结构的不同层级。例如，您可以为每个业务部门创建一个顶级文件夹，然后在该业务部门内为不同的团队创建子文件夹。然后，您可以在文件夹内创建项目。

文件夹还可以通过角色继承更有效地管理成员访问权限。在文件夹级别为成员分配角色时，他们将继承所有子项目和文件夹的权限。

文件夹是一种组织工具，对于没有 IAM 权限的成员（例如组织管理员、文件夹或项目管理员或超级管理员角色）是不可见的。成员访问的是项目，而不是文件夹。

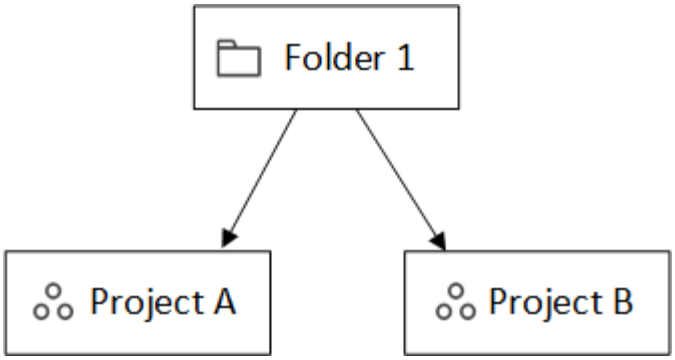
组织管理员可以通过创建文件夹来委派管理职责。创建文件夹后，组织管理员可以为特定文件夹分配文件夹管理员或项目管理员角色。这些成员无需访问整个组织即可管理该文件夹内的所有项目。

文件夹可以包含其他文件夹或项目作为子文件夹，但不能直接关联资源。资源必须与项目关联。

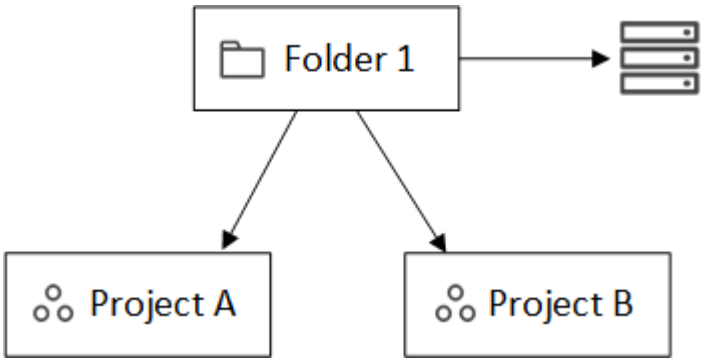
何时将资源与文件夹关联

_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：

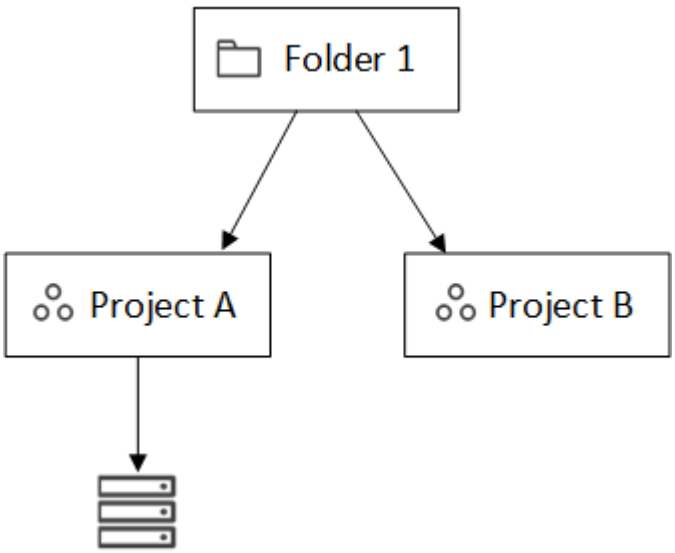


_组织管理员_可以将资源与文件夹关联：



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。

项目

将资源与项目关联起来，以便成员进行管理。资源必须与项目关联才能进行管理和用户访问。

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，也可以位于文件夹内。如果使用代理来发现项目中

的资源，则还必须将该代理与该项目关联起来。

用户可在“系统”页面上浏览已分配的项目，以管理与每个项目相关的资源。

添加文件夹或项目

添加项目以管理资源，添加文件夹以对相关项目进行分组。创建新组织时，控制台会包含一个项目。

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。根据需要创建嵌套文件夹来整理资源。

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：输入文件夹或项目的名称并选择其位置。您可以将文件夹或项目放置在组织下，也可以放置在其他文件夹内。
   - 资源：选择要与此文件夹或项目关联的资源。如果您尚未向主机添加存储系统，您可以稍后执行此步骤。

     只有当文件夹中的资源被分配给某个项目后，成员才能访问这些资源。使用文件夹临时存放资源，直到创建必要的项目为止。这可以帮助组织管理员将资源分配委派给文件夹或项目管理员，然后由该管理员将资源分配给文件夹内的项目。

   - 访问权限：选择*添加成员*以分配访问权限和角色。您可以随时向项目或文件夹中添加或删除成员。

     "了解访问角色" 。
6. 选择“添加”。

重命名文件夹或项目

根据需要重命名文件夹或项目。重命名不会影响相关资源或成员访问权限。

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，例如团队重组或项目完成后。

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。

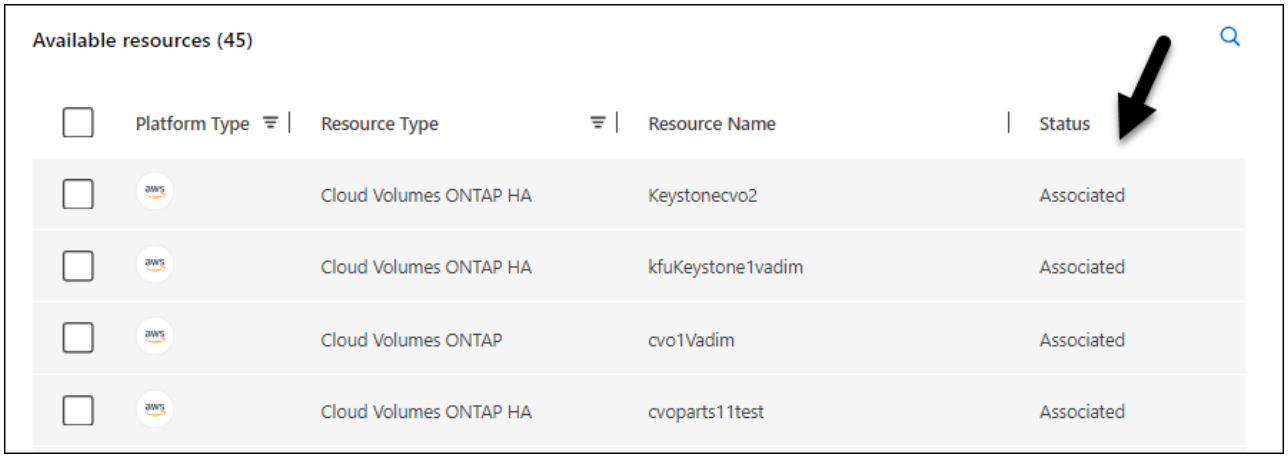
查看与文件夹或项目关联的资源

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

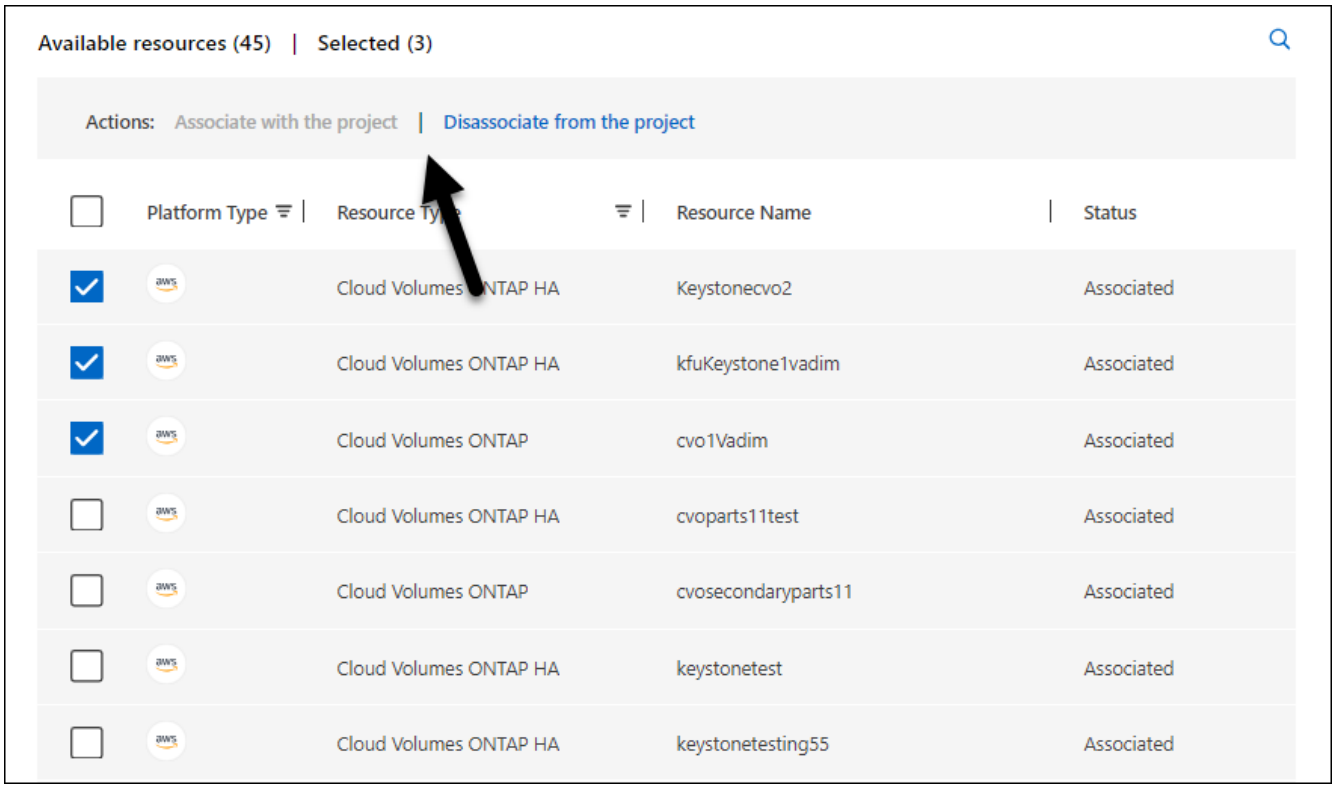
您可以根据组织的需求变化更改与文件夹或项目关联的资源。

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*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”。



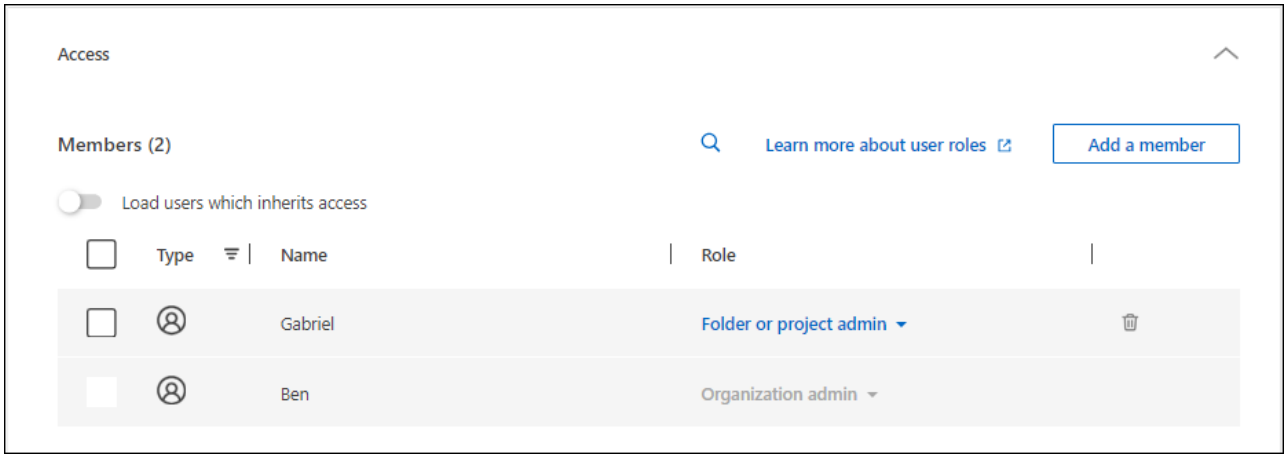
5. 选择*应用*。

查看与文件夹或项目关联的成员

您可以从“组织”页面查看与文件夹或项目关联的成员。

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。
   - 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。请记住，在文件夹级别分配的角色将被所有子项目和文件夹继承。

如果成员访问权限是从文件夹或组织级别继承的，则无法在较低级别更改成员访问权限。更改更高层级成员的权限以更改访问权限。或者，您可以 "从“会员”页面管理权限"。

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"

在NetApp Console中向文件夹和项目添加资源

通过将用户添加到NetApp Console组织中的项目和文件夹来控制用户对资源的访问权限。授予项目级用户访问权限。

资源是指控制台所感知到的实体，例如存储资源、控制台代理或备份和恢复工作负载。

您可以在控制台的“资源”页面中查看和管理资源。

控制台资源类型

您可以将多种类型的资源关联到NetApp Console组织中的项目：

存储资源

存储资源是组织中最常见的资源类型，包括本地存储系统和云存储系统。在控制台中添加存储系统时，您可以将其添加到文件夹或项目中。在此之前，控制台会将其标记为未发现，并且不会在“资源”页面上显示它。

控制台代理

如果您使用控制台代理来发现存储系统，请将该代理添加到同一文件夹或项目中。这允许用户执行代理启用的功能，例如数据服务或控制台原生存储管理。您可以从控制台的“代理”页面向文件夹或项目中添加代理。"了解如何将控制台代理与文件夹或项目关联"。

Keystone订阅

如果您的组织拥有Keystone订阅，您可以在“资源”页面上查看它们。您可以将Keystone订阅与文件夹或项目关联起来，以便向拥有这些文件夹或项目权限的成员提供访问权限。

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。

> 控制台会将Amazon FSx for NetApp ONTAP资源从“资源”页面中排除，因为用户无法将其与角色关联。您可以在“系统”页面或“工作负载”中查看这些资源。

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

将资源关联到文件夹或项目，使其可供具有该文件夹或项目权限的成员使用。

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，请删除其关联。这样可以防止成员管理该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. 要从文件夹或项目中移除资源，请选择 在文件夹或项目旁边。
3. 选择“删除”以移除关联。

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

将控制台代理与特定项目关联起来，以实现资源管理和数据服务访问。通过控制台代理发现的资源需要资源和代理都与同一个项目关联，才能实现团队访问。

超级管理员和组织管理员可以创建代理，并将任何代理与任何项目或文件夹关联起来。文件夹或项目管理员只能将现有代理与他们拥有权限的文件夹和项目关联起来。"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"

将用户添加到您的控制台组织

将用户添加到**NetApp Console**组织

在控制台中，您可以根据访问角色授予用户对项目或文件夹的访问权限。_访问角色_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指定级别执行特定操作。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。"了解访问角色"。

了解如何在**NetApp Console**中授予访问权限

NetApp Console使用基于角色的访问控制 (RBAC) 来管理权限。可以单独为用户分配角色，也可以通过联合组为用户分配角色。每个角色都定义了对特定资源允许的操作。

请注意以下关于在NetApp Console中授予访问权限的事项：

- 所有用户必须先注册NetApp Console，然后才能获得资源访问权限。
- 即使用户是已分配角色的联合组的成员，也必须在控制台中明确地为每个用户分配角色，然后他们才能访问资源。

- 您可以直接从控制台添加服务帐户并为其分配角色。

向您的组织添加成员

NetApp Console支持三种类型的成员：用户帐户、服务帐户和联合组。

即使用户属于联合组，也必须先注册NetApp Console，然后才能添加他们并分配角色。直接在控制台中创建服务帐户。

所有成员必须至少被明确分配一个角色才能访问资源。

添加成员时，选择资源级别（组织、文件夹或项目），并分配一个或多个具有所需权限的角色。

添加用户

用户注册NetApp Console，但组织管理员、文件夹管理员或项目管理员必须将他们添加到组织、文件夹或项目中，以便他们能够访问资源。

开始之前：

用户必须已经注册了NetApp Console。如果他们还没有注册，请引导他们…… "注册NetApp Console。"

如果要添加属于联合组的用户，请确保该用户已注册NetApp Console，并在控制台中明确分配了角色。NetApp建议分配最低访问权限角色，例如组织查看者。

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*，保持选择*用户*。
5. 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。
6. 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：

   - 您只能选择您拥有权限的文件夹和项目。
   - 选择组织或文件夹时，即授予该成员对其所有内容的访问权限。
   - 您只能在组织级别分配*组织管理员*角色。
7. 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" 。
8. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。
9. 选择“添加”。

   控制台会通过电子邮件向用户发送操作说明。

添加服务帐户

服务帐户允许您自动执行任务并安全地连接到控制台 API。对于简单的设置，可以选择客户端 ID 和密钥；对于自动化或云原生环境，可以选择 JWT（JSON Web Token）以获得更强的安全性。选择符合您安全要求的方法。

开始之前：

对于 JWT 身份验证，请准备您的公钥或证书。

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. 要使用 JWT 身份验证，请选择“使用私钥 JWT 身份验证”，然后上传您的 RSA 公钥或证书。如果使用客户端 ID 和密钥，则跳过此步骤。

   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*，授予成员对所选组织、文件夹或项目中的资源的权限。

   "了解访问角色" 。
9. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。
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。

    控制台只会显示一次客户端密钥。请妥善备份；如果丢失，您可以稍后重新创建。
11. 如果您选择 JWT 身份验证，请下载或复制客户端 ID 和 JWT 受众群体。控制台只会显示此信息一次，之后无法再检索。
12. 选择*关闭*。

向您的组织添加联合组

您可以将身份提供商 (IdP) 中的联合组添加到您的组织，并为其分配一个或多个角色。联合组的成员将继承您在控制台中分配给该组的角色。

在为联合组分配角色之前，请确保以下事项：

- 在身份提供商 (IdP) 和控制台之间建立联盟。 "了解如何建立联邦。"
- 该组必须已存在于您的身份提供商 (IdP) 中，并且已被分配对控制台的应用程序访问权限。
- 属于该组的用户必须已经注册了NetApp Console，并且已被明确分配了控制台中的角色。NetApp建议分配最低访问权限角色，例如组织查看者。

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“成员类型”，请选择“联合组”。
5. 选择该团体所属的联邦。
6. 对于“组名称”，请输入您身份提供商 (IdP) 中组的确切名称。
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*，授予成员对所选组织、文件夹或项目中的资源的权限。

   "了解访问角色" 。
9. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。

相关信息

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

管理用户访问权限和安全

了解NetApp Console基于角色的访问控制 (RBAC)

使用基于角色的访问控制 (RBAC) 管理用户对NetApp Console的访问，在组织、文件夹或项目级别分配预定义角色。每个角色都授予特定的权限，定义用户在其分配的权限范围内可以执行哪些操作。

NetApp在设计控制台角色时遵循最小权限原则，因此每个角色仅包含其任务所需的权限。这种方法通过限制每个成员所需的访问权限来增强安全性。

将资源整理成文件夹和项目后，为组织成员分配特定文件夹或项目的角色，使他们只能履行自己的职责。

例如，您可以为特定项目级别的成员分配勒索软件恢复管理员角色，允许他们对该项目内的资源执行勒索软件恢复操作，而无需授予他们对整个组织的更广泛访问权限。同一用户可以被授予组织内多个项目的角色。

您可以根据用户的职责，为同一范围或不同范围的用户分配多个角色。例如，规模较小的组织可能会让同一用户在组织层面管理勒索软件恢复和备份与恢复任务，而规模较大的组织可能会在项目层面为每个角色分配不同的用户。

控制台组织成员的类型

NetApp Console组织中有三种类型的成员：* 用户帐户：登录到NetApp Console以管理资源的个人用户。用户必须先注册NetApp Console，然后才能被添加到组织中。* 服务帐户：应用程序或服务通过 API 与NetApp Console交互时使用的非人类帐户。您可以将服务帐户直接添加到您的控制台组织中。* 联合组：从您的身份提供商 (IdP) 同步的组，允许您集中管理多个用户的访问权限。联合组中的每个用户都必须先注册NetApp Console，并被添加到您的组织中，且拥有相应的访问角色，然后才能访问授予该组的资源。

"了解如何向您的组织添加成员。"

NetApp Console中的预定义角色

NetApp Console包含预定义角色，您可以将其分配给组织成员。每个角色都包含权限，用于指定成员在其分配的范围（组织、文件夹或项目）内可以执行哪些操作。

NetApp Console角色采用最小权限原则，确保成员仅拥有完成任务所需的权限，并按角色提供的访问权限类型对其进行分类：

- 平台角色：提供控制台管理权限
- 数据服务角色：提供管理特定数据服务的权限，例如勒索软件恢复和备份与恢复。
- 应用程序角色：提供管理存储以及审核控制台事件和警报的权限

您可以根据成员的职责为其分配多个角色。例如，您可以为特定项目为一名成员分配勒索软件恢复管理员角色和备份与恢复管理员角色。

"了解NetApp Console中可用的预定义角色"。

在NetApp Console中管理成员访问权限

管理您在控制台组织中的成员访问权限。分配角色以设置权限。成员离开时将其移除。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。链接：reference-iam-predefined-roles.html[了解访问角色]。

您可以按项目或文件夹分配访问角色。例如，可以为用户分配两个特定项目的角色，或者在文件夹级别分配角色，从而授予用户对文件夹中所有项目的勒索软件恢复管理员角色。

请先添加文件夹和项目，然后再分配用户访问权限。 "了解如何添加文件夹和项目。"

了解如何在**NetApp Console**中授予访问权限

NetApp Console使用基于角色的访问控制 (RBAC) 模型来管理用户权限。您可以单独或通过联合组为成员分配预定义的角色。您可以向服务帐户以及联合组添加和分配角色。每个角色都定义了成员可以在相关资源上执行哪些操作。

请注意以下关于在NetApp Console中授予访问权限的事项：

- 所有用户必须先注册NetApp Console，然后才能获得资源访问权限。
- 即使用户是已分配角色的联合组的成员，也必须在控制台中明确地为每个用户分配角色，然后他们才能访问资源。
- 您可以直接从控制台添加服务帐户并为其分配角色。

使用角色继承

在NetApp Console中，当您在组织、文件夹或项目级别分配角色时，所选范围内的所有资源都会自动继承该角色。例如，文件夹级角色适用于所有包含的项目，而项目级角色适用于该项目内的所有资源。

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。"

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*。

查看分配给成员的角色

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. 在“成员”页面中，导航至表格中的某个成员，然后选择 ••• 然后选择“查看详情”。
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”。

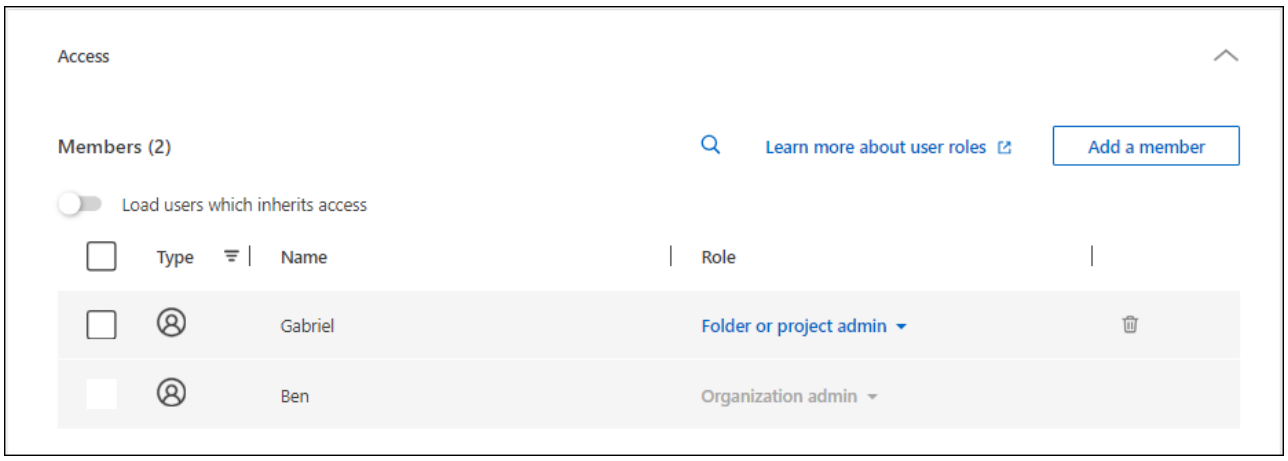
查看与文件夹或项目关联的成员

您可以查看哪些成员有权访问特定文件夹或项目。

步骤

1. 选择*管理>身份和访问*。

2. 选择*组织*。
3. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
    - 选择*访问*来查看有权访问该文件夹或项目的成员。



分配或修改成员访问权限

用户注册NetApp Console后，您可以将他们添加到您的组织并分配角色，以便向他们提供资源访问权限。 "了解如何向您的组织添加成员。"

您可以根据需要添加或删除角色来调整成员的访问权限。

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或不同的项目中担任多个角色。例如，规模较小的组织可能会将所有可用的访问角色分配给同一用户，而规模较大的组织可能会让用户执行更专业的任务。或者，您也可以在组织级别为一名用户分配勒索软件恢复管理员角色。在这个例子中，用户可以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。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。
4. 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”。
5. 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。

6. 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. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。
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。
6. 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 🗑 在角色旁边，点击即可从成员中移除相应的角色。您将被要求确认删除操作。

从您的组织中移除成员

如果成员离开您的组织，则将其从组织中移除。

删除成员时，系统会撤销其控制台权限，但保留其控制台和NetApp支持站点帐户。

联邦成员

- 当联合用户从您的身份提供商 (IdP) 中移除时，他们将自动失去对NetApp Console的访问权限。但您仍然应该将它们从您的控制台组织中删除，以保持您的成员列表是最新的。
- 如果您从身份提供商 (IdP) 中的联合组中移除用户，他们将失去与该组关联的控制台访问权限。但是，他们仍然保留在控制台中分配给他们的明确角色所关联的任何访问权限。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。
4. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*删除用户*。
5. 确认您要从组织中删除该成员。

用户安全

通过管理成员安全设置，确保用户对NetApp Console组织的访问权限。您可以重置用户密码、管理多因素身份验证 (MFA) 以及重新创建服务帐户凭据。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。链接：reference-iam-predefined-roles.html[了解访问角色]。

重置用户密码（仅限本地用户）

组织管理员无法重置本地用户的用户密码。但是，他们可以指导用户重置自己的密码。

指示用户通过选择“忘记密码？”从控制台登录页面重置密码。

此选项不适用于联合组织中的用户。

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。

多因素身份验证仅适用于本地用户。联合身份验证用户无法启用多因素身份验证 (MFA)。

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。如果用户暂时无法访问其 MFA 设备，他们可以使用已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。

重新创建服务帐户的凭据

如果您丢失或需要更新服务凭证，可以创建新的凭证。

创建新凭证会删除旧凭证。您不能使用旧的凭据。

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。请务必复制或下载并妥善保存。

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。
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。

数据服务角色	职责
"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

任务	组织管理员	文件夹或项目管理员
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
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

特征和动作	**Keystone**管理员	**Keystone**查看器
为自己创建报告	是	是
服务请求：		
创建服务请求	是	否
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
查看审核页面和通知	是
查看、下载和配置警报	是

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

特征和动作	存储管理员	系统健康专家	存储查看器
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
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

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
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
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
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

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
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
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

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
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
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

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
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

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
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：		
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

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
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
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

身份和访问 API

组织和项目 ID

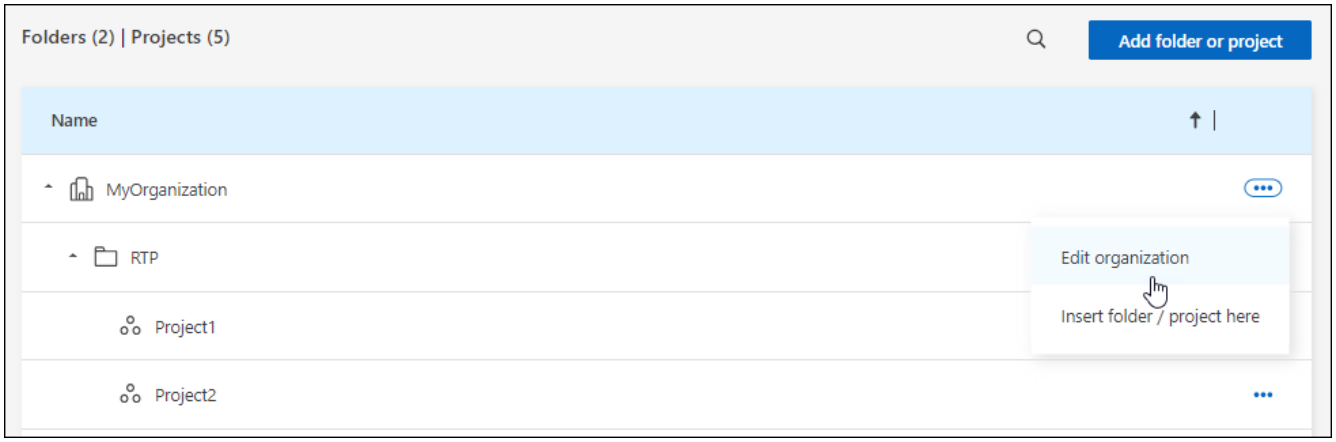
您的NetApp Console组织有一个名称和一个 ID。您可以为您的组织选择一个名称以帮助识别它。您可能还需要检索某些集成的组织 ID。

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

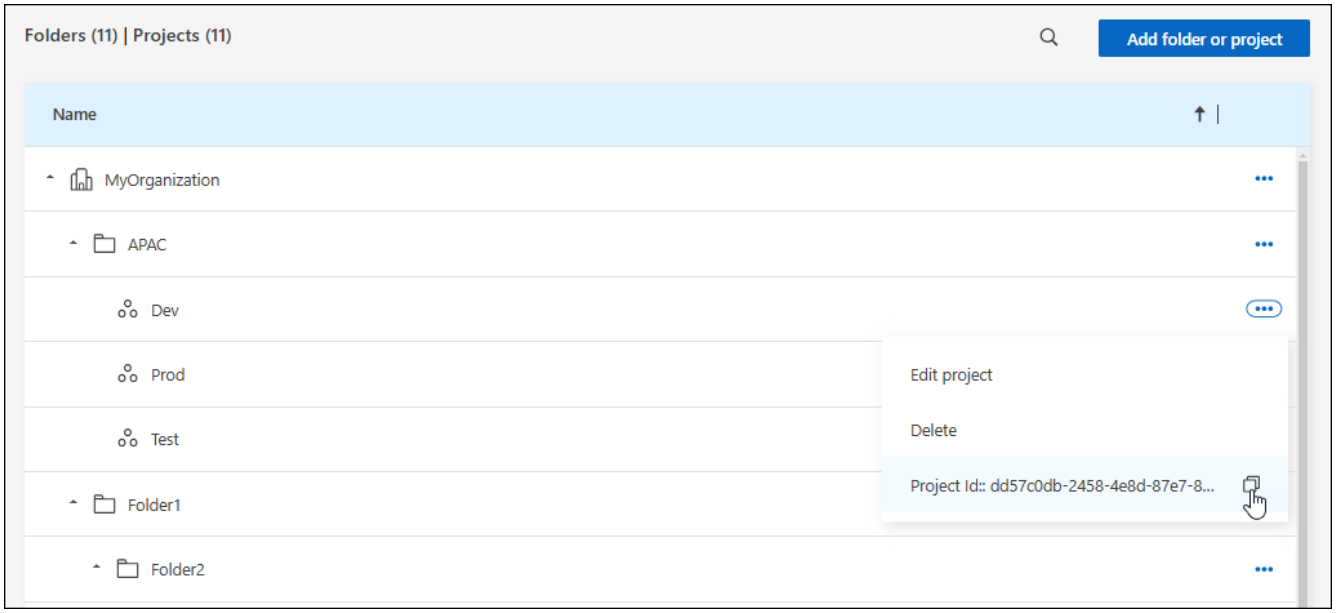
如果您使用 API，则需要获取项目的 ID。例如，创建Cloud Volumes ONTAP系统时。

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"