管理用户访问权限和安全

NetApp Console setup and administration

NetApp
February 11, 2026

目录

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" 。

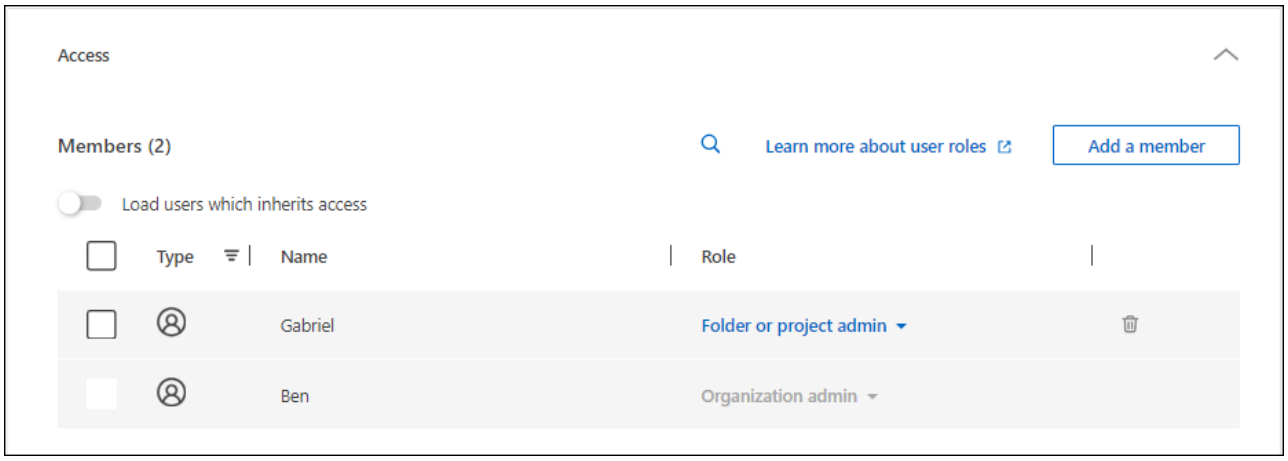
1. 在“成员”页面中，导航至表格中的某个成员，然后选择 ••• 然后选择“查看详情”。
2. 在表格中，展开您想要查看成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”。

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。