管理用户和访问权限

NetApp Console local deployment

NetApp
August 10, 2026

目录

管理用户和访问权限

在 NetApp Console 本地部署中管理成员访问权限

在 NetApp Console 本地部署中，跨多个文件夹或组查看或更改用户的角色，例如检查存储工程师可以访问的所有内容、在另一个区域添加新角色，或在职责发生变化时撤销该用户的访问权限。

必需的访问角色

超级管理员、组织管理员或文件夹或车队管理员（针对他们管理的文件夹和车队）。"了解访问角色"。

您可以根据需要通过两种方式查看和管理访问权限。如果要查看特定用户在组织中所有资产中的角色，请使用 **Members** 页面。

如果要确认谁可以访问特定车队，请查看分配给该车队的成员。"管理机群访问分配".

要添加新成员、服务帐户或目录用户并分配其第一个角色，请改用入职任务。"添加成员并分配角色"。

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) 来管理成员权限。您可以在组织、文件夹或机群级别分配预定义的角色，具体视成员所需的访问权限范围而定。

使用角色继承

在组织或文件夹级别分配的角色由其下方的子作用域继承，因此请在您最初授予该角色的更高作用域中更改继承的分配。

"了解 NetApp Console 本地部署中的角色继承"。

查看分配给成员的角色

在进行更改之前，请准确确认成员担任的角色及其范围。例如，检查团队成员是否已在 `Production-EU-West` fleet 中拥有 Storage admin 角色。

如果您有_文件夹或车队管理员_角色，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所管理的文件夹和车队的权限。"了解 NetApp Console 本地部署中的文件夹或群组管理员操作"。

1. 在*成员*页面中，导航到表中的成员，选择 ⋯，然后选择*查看详细信息*。
2. 在表中，展开希望查看成员所分配角色的组织、文件夹或队列的相应行，然后在 **Role** 列中选择 **View**。

分配或修改成员访问权限

每当职责发生变化时，您都可以调整成员的访问权限。例如，当团队成员承担第二个区域的备份职责时，请在该区域的机群中添加 Backup and Recovery 管理员角色，而无需更改其现有的存储角色。

如果需要添加新成员并分配其第一个角色，请参阅 "添加成员并分配角色"。

向现有成员添加访问角色

当成员的职责范围扩大时，为其授予组织、文件夹或 fleet 级别的额外角色。例如，为 Storage admin 指定组织级别的 Backup and recovery admin 角色，以便他们可以跨每个 fleet 管理备份和恢复任务，而不会失去其现有存储权限。

您可以为成员分配组织、文件夹或队列的访问角色。

成员可以在同一 fleet 和不同 fleet 中担任多个角色。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级别的 Ransomware resilience admin 角色。在该示例中，用户将能够对组织内的所有 fleet 执行 Ransomware resilience 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 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择一个成员选项卡：用户、目录用户*或*服务帐户。
4. 选择要分配角色的成员旁边的操作菜单 ⋯，然后选择*添加角色*。
5. 要添加角色，请完成对话框中的步骤：
   - 选择一个组织、文件夹或队列：选择成员应具有权限的资源层次结构级别。

     如果选择组织或文件夹，则成员将对组织或文件夹中的所有内容拥有权限。
   - **Select a category**：选择一个角色类别。"了解访问角色"。
   - 选择一个*角色*：选择一个角色，为成员提供与您选择的组织、文件夹或舰队关联的资源的权限。
   - **Add role**：如果要提供对组织内其他文件夹或队列的访问权限，请选择 **Add role**，指定其他文件夹或队列或角色类别，然后选择角色类别和相应的角色。
6. 选择*添加新角色*。

更改成员的分配角色

当成员的职责发生变化时，将成员的现有角色替换为其他角色。例如，当 `Production-US-East`队列中的 Storage viewer 需要 Storage admin 角色时。

> ⓘ 每个用户必须至少有一个角色。您无法从用户中删除所有角色。如果需要删除所有角色，请从组织中删除该用户。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择一个成员选项卡：用户、目录用户*或*服务帐户。
4. 在*成员*页面中，导航到表中的成员，选择 ⋯，然后选择*查看详细信息*。
5. 在表中，展开要更改成员分配角色的组织、文件夹或队列的相应行，然后在*角色*列中选择*查看*，以查看

分配给此成员的角色。

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，请选择您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中的角色。例如，您可以从一个数据服务角色更改为另一个。确认更改。
   b. 要取消分配成员的角色，请选择角色旁边的 以取消分配成员的相应角色。系统将提示您确认删除。

从组织中删除成员

当成员离开组织或以某种方式更改角色，不再需要访问 Console 时，请删除该成员。例如，当承包商的合同结束或员工转移到 Console 组织以外的团队时。

目录用户

从目录中删除用户会阻止该用户进行身份验证。您还应从 Console 组织中删除该用户，以保持成员列表的准确性，并删除在 Console 本地部署中分配的任何角色。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择一个成员选项卡：用户、目录用户*或*服务帐户。
4. 在*成员*页面中，导航到表中的成员，选择 ••• 然后选择*删除用户*。
5. 请确认您要从组织中删除此成员。

查看或更改 NetApp Console 本地部署中的机群访问分配

审核或更改 NetApp Console 本地部署中文件夹和存储设备的成员访问分配。文件夹和存储设备管理员通常从此视图工作，因为它仅显示他们管理的范围。

必需的访问角色

超级管理员、组织管理员或文件夹或车队管理员。"了解访问角色"。

或者，您可以跨多个文件夹或队列管理特定成员的所有角色。"管理成员访问权限"。

文件夹和队列访问权限的工作原理

控制台本地部署使用基于角色的访问控制 (RBAC)。在文件夹级别分配的角色适用于该文件夹中的所有队列和子文件夹；在队列级别分配的角色仅适用于该队列的资源。"了解 NetApp Console 本地部署中的角色继承"。

如果成员从文件夹或组织继承了角色，则无法在队列级别更改该角色。要更改继承的访问权限，请在较高范围内更改角色。

查看分配给文件夹或队列的成员

准确查看谁可以管理特定的文件夹或队列。例如，在将新的生产 ONTAP 集群与 `Production-US-East`队列关联之前，请打开队列的"访问权限"选项卡以确认谁有权访问。

步骤

1. 选择*管理* > 身份和访问。
2. 选择*组织*。
3. 在"组织"页面中，导航到表中的文件夹或队列，选择 ••• ，然后选择 **Edit folder** 或 **Edit fleet**。
4. 选择*访问权限*以查看有权访问该文件夹或舰队的成员。

从文件夹或队列修改成员访问权限

调整已属于您的组织的成员角色，范围限定为单个文件夹或舰队。例如，当团队成员从开发舰队迁移到生产舰队时，将其在生产舰队中的角色从 Storage viewer 提升为 Storage admin，而不影响其在其他位置的访问权限。

要添加新成员并分配其第一个角色，请改用入职任务。"添加成员并分配角色"。

步骤

1. 在"组织"页面中，导航到表中的文件夹或队列，选择 ••• ，然后选择 **Edit folder** 或 **Edit fleet**。
2. 选择*访问权限*以查看具有访问权限的成员列表。
3. 修改成员访问权限：
   - 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，选择其现有角色并选择新角色。更改仅适用于此范围；从更高范围继承的角色不会显示在此处。
   - 删除此范围内的成员访问权限：对于在此文件夹或舰队中直接定义角色的成员，请删除该角色以撤销其在此范围内的访问权限。这不会从您的组织中删除成员，也不会影响他们在其他范围内的角色。

     "从组织中删除成员"。
4. 选择*应用*。

在 NetApp Console 本地部署中管理成员安全性

通过管理成员安全设置，保护用户对 NetApp Console 本地部署组织的访问权限。您可以指导本地用户更改自己的密码、管理本地用户的多因素身份验证 (MFA) 以及重新创建服务帐户凭据。

必需的访问角色

超级管理员、组织管理员或文件夹或车队管理员。"了解访问角色"。

重置用户密码（仅限本地用户）

管理员不能直接重置本地用户密码。

通过选择 **Forgot password?** ，引导本地用户从 Console 本地部署登录页面重置密码。

此选项不适用于目录用户。

管理本地用户的多因素身份验证(MFA)

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

多重身份验证仅适用于本地用户。目录用户无法通过 Console 本地部署启用 MFA。

请使用以下指南选择正确的操作：

- 当用户暂时无法访问其 MFA 设备时，选择*禁用*。禁用 MFA 后，用户可在八小时内无需 MFA 登录一次，之后系统将自动重新启用 MFA。
- 当用户必须完全重置 MFA 时，选择*移除*。删除 MFA 后，用户在未配置 MFA 的情况下登录，直到他们再次配置 MFA。

如果用户已保存恢复代码，则可以使用此代码登录。如果用户没有恢复代码，请禁用 MFA，以便用户可以登录并重新获得访问权限。

要管理本地用户的多因素身份验证，您必须拥有与受影响用户相同域中的电子邮件地址。

步骤

1. 选择*管理* > 身份和访问。
2. 选择 **Members**。
3. 在"成员"页面中，导航到表中的成员，选择 ••• 然后选择"管理多因素身份验证"。
4. 选择是删除还是禁用用户的 MFA 配置。

完成后

查看审核日志，以确认谁更改了 MFA 访问权限、何时更改以及操作是否成功。"了解如何审核 NetApp Console 本地部署活动"。

重新创建服务帐户的凭据

如果丢失或需要更新，您可以为服务帐户创建新凭据。

创建新凭据会删除旧凭据。不能使用旧的凭据。

步骤

1. 选择*管理* > 身份和访问。
2. 选择 **Members**。
3. 在 Members 表中，导航到服务帐户，选择 •••，然后选择 **Recreate secrets**。
4. 选择*重新创建*。
5. 下载或复制客户端 ID 和客户端密钥。

   Console 本地部署仅显示一次客户端密码。请务必复制或下载并安全存储。