# 规划您的 **Console** 组织

## NetApp Console local deployment

NetApp
August 10, 2026

# 目录

# 规划您的 Console 组织

## 开始使用 NetApp Console 本地部署中的身份和访问权限

在 NetApp Console 本地部署中，设置文件夹和队列层次结构，添加成员和起始权限，并将资源添加到正确的队列中并进行放置，以便合适的团队可以访问和管理它们。

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"。

您需要*组织管理员*或*超级管理员*角色才能完成初始设置。设置完成后，您可以根据组织的变化管理资源、成员访问权限和舰队访问权限。


添加或发现资源

将系统添加到 Console 本地部署。在初始设置过程中，通常在选择默认机群的同时添加系统。

了解如何创建或发现资源：

- "本地 ONTAP 集群"


创建您的文件夹和车队层次结构

创建与业务层次结构匹配的其他队列和文件夹。

"了解如何使用文件夹和队列组织资源"。


将资源与正确的队列关联

在 Console 本地部署中添加或发现系统会自动将资源与当前选定的机群相关联。要使系统可供正确的团队使用，请将其与层次结构中的相应机群相关联。

- "了解如何管理文件夹和队列中的资源"。


添加成员并分配起始权限

根据管理内容，在组织、文件夹或队列级别添加成员并为其分配角色。

"了解如何管理成员及其权限"。

### 初始设置后

初始设置完成后，根据组织变化管理访问权限和资源放置：

- "管理文件夹和队列中的资源"
- "管理跨机群和文件夹的成员访问权限（以成员为中心）"

- "管理谁可以访问特定机群或文件夹（以机群为中心）"
- "不再需要时删除文件夹和车队"

相关信息

- "了解 NetApp Console 中的身份和访问管理"
- "了解用于身份和访问的 API"

# 了解 NetApp Console 本地部署中的文件夹和机群

在 NetApp Console 本地部署中，使用文件夹和存储舰队根据您的业务结构（按位置、部门或工作负载类型）来组织 NetApp 资源并控制访问。

此页面用于层次结构策略和机群设计模式。有关成员、角色和资源范围的完整 IAM 模型，"了解 NetApp Console 本地部署中的身份和访问管理"。

您可以按层次结构组织资源：组织位于顶部，然后是文件夹（可能包含其他文件夹或舰队），然后是包含存储系统的舰队。在组织、文件夹或舰队级别分配访问角色，以便用户拥有对资源的正确访问权限。

要管理 NetApp Console 本地部署中的文件夹和队列，您必须具有组织管理员或文件夹或队列管理员角色。

## 组织组成部分

组织组件——组织、文件夹和队列——形成一个层次结构，确定资源的分组方式以及访问权限的委派方式。

组织

组织是 NetApp Console 本地部署层次结构的顶层，通常代表您的公司。您的组织由文件夹、舰队、成员、角色和资源组成。资源与舰队相关联，成员在组织、文件夹或舰队级别被分配角色。

文件夹

文件夹对相关舰队进行分组，按位置、站点或业务部门对其进行组织。无法将存储系统直接与文件夹关联，但在文件夹级别为成员分配角色可使其访问该文件夹中的所有舰队。

组织管理员可以将资源添加到文件夹，以将资源与队列关联的任务委派给文件夹或队列管理员。"将资源与文件夹和队列关联"。

车队

Fleet 对存储系统进行分组。将资源分配给 Fleet，并在 Fleet 级别授予成员访问权限。资源可以属于多个 Fleet。拥有 Fleet 访问权限的成员可以管理该 Fleet 中的资源。

例如，根据您的需求，您可以将本地 ONTAP 系统与单个机群或组织中的所有机群相关联。

"了解如何创建文件夹和存储舰队"。

## 资源

资源是 Console 本地部署已识别并可分配给群组的存储系统。将资源与群组关联，以便有权访问该群组的用户

可以管理该资源。

例如，您可以将 ONTAP 集群与一个机群或组织中的所有机群相关联。如何关联资源取决于您组织的需求。

"了解如何将资源与队列关联"。

## 成员和角色

成员是组织中的用户和服务帐户。角色定义他们可以执行的操作以及在层次结构的哪个级别执行（组织、文件夹或群组）。

成员

组织的成员是用户帐户或服务帐户。服务帐户通常由应用程序使用，以在无需人工干预的情况下完成指定任务。

具有组织管理员角色的用户可以向贵组织添加新成员。必须显式添加所有用户（包括服务帐户和 Active Directory 用户）并授予至少一个角色，才能访问 Console 本地部署。

"了解如何向组织中添加成员"。

访问角色

Console 本地部署提供可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、特定文件夹或特定队列授予该角色。您选择的角色将授予成员对层次结构选定部分中资源的访问权限。

NetApp Console 本地部署提供了符合最小特权原则的细粒度角色，这意味着访问角色的设计旨在仅向成员授予其所需的访问权限。

随着职责的扩展，用户可以拥有多个角色。

角色继承

在组织或文件夹级别分配角色时，其下的子文件夹、队列和资源将继承该角色，因此文件夹和队列设计决定了每个分配的适用范围。

"了解 NetApp Console 本地部署中的角色继承"。

## 组织设计示例

正确的组织结构取决于组织的规模和团队的组织方式。以下示例演示了不同的组织如何使用文件夹和舰队层次结构来有效管理访问权限。

小型组织策略

对于用户数少于 50 且集中式存储管理的组织，请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 Corporation**（**5** 人团队）

- 结构：拥有 3 个舰队的单一组织（生产、开发、备份）
- 角色：

- 2名高级成员：具有完全管理权限的超级管理员角色
- 3 名团队成员：超级查看者角色，用于在没有修改权限的情况下进行监控

- 优势：简化管理，降低角色复杂性，适用于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，使用代表地理或业务部门边界的文件夹实施分层方法。

示例：**XYZ Corporation**（跨国公司）

- 结构：组织 > 区域文件夹（北美、欧洲、亚太地区）> 每个地区的车队
- 平台角色：
  - 1 组织管理员：全局监督和策略管理
  - 3 个文件夹或机群管理员：区域控制（每个区域一个）
  - 1 Federation admin：公司目录服务集成
- 按地区划分的存储角色：
  - 存储管理员：发现和管理指定区域中的存储系统
  - 存储查看器：监控跨区域的存储资源
  - 系统健康专员：无需修改系统即可管理存储健康
- 好处：通过角色隔离、区域自治和遵守当地法规来增强安全性

部门专业化策略

对于拥有需要特定访问权限的专业团队的组织，请根据职能职责使用有针对性的角色分配。

示例：**TechCorp**（中型科技公司）

- 结构：组织 > 部门文件夹（IT、安全、开发）> 车队特定资源
- 专业角色：
  - 安全团队：Ransomware resilience admin 和 Classification viewer 角色
  - 备份团队：用于全面备份操作的备份和恢复超级管理员
  - 开发团队：测试环境管理的存储管理员
  - 合规团队：负责监控和支持案例管理的运营支持分析师
- 优势：量身定制的访问控制、提高运营效率以及明确的专业任务问责制

## 后续步骤

- "创建文件夹和存储舰队"
- "将资源与文件夹和队列关联"
- "管理机群访问分配"
- "监控或审核控制台本地部署操作"

# 了解 NetApp Console 本地部署中基于角色的访问控制

使用基于角色的访问控制 (RBAC) 管理用户对 NetApp Console 本地部署的访问，在组织、文件夹或群组级别分配预定义角色。每个角色都授予特定权限，用于定义用户可以在其分配的范围内执行的操作。

NetApp 在设计 Console 本地部署角色时遵循最小权限原则，因此每个角色仅包含执行其任务所需的权限。这种方法通过将访问权限限制为每个成员所需的内容来增强安全性。

将资源整理到文件夹和队列后，为组织成员分配特定文件夹或队列的一个或多个角色，使他们只能执行其职责。

例如，您可以为成员分配特定舰队级别的 Backup and Recovery 管理员角色，允许他们对该舰队内的资源执行备份和恢复操作，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您组织内多个舰队的角色。

您可以为同一范围或不同范围的成员分配多个角色，具体取决于他们的职责。例如，较小的组织可能会在组织级别为同一成员同时分配 Storage admin 和 Backup and Recovery admin 角色，而较大的组织可能在机群级别为每个角色分配不同的成员。

## Console 组织成员类型

NetApp Console 本地部署支持以下类型的成员：

- *Users*：单个用户可以是您添加到 NetApp Console 本地部署中使用本地凭据的本地用户，也可以是通过您的集成 Active Directory 或 LDAP 服务进行身份验证的目录用户。两种类型的用户都可以在 NetApp Console 本地部署中分配角色以访问资源。
- *Service accounts*：应用程序或服务用于通过 API 与 NetApp Console 本地部署交互的非人工帐户。您可以将服务帐户直接添加到您的 Console 本地部署组织。

"了解如何向贵组织添加成员。"

## NetApp Console 本地部署中的预定义角色

NetApp Console 本地部署包括可分配给组织成员的预定义角色。每个角色都包含权限，用于指定成员可在其分配的范围（组织、文件夹或舰队）内执行的操作。

NetApp Console 本地部署角色使用最小权限原则，确保成员仅拥有其任务所需的权限，并按其提供的访问类型对角色进行分类：

- 平台角色：提供 Console 本地部署管理权限
- 数据服务角色：提供管理特定数据服务的权限，例如 Ransomware Resilience 和 Backup and Recovery
- 应用程序角色：提供用于管理存储以及审核 Console 本地部署事件和警报的权限

您可以根据成员的职责为其分配多个角色。例如，您可以为成员分配特定机群的 Storage admin 角色和 Backup and Recovery admin 角色。

要为成员选择访问权限，请将角色类别与成员的职责相匹配，然后在与成员应具有该访问权限的范围相匹配的范围（组织、文件夹或舰队）中分配角色。"了解不同组织如何在 NetApp Console 本地部署中构建角色和范围".

"了解可分配给 NetApp Console 本地部署中的成员的预定义角色"。

## 角色继承的工作原理

在组织或文件夹级别分配角色时，该角色将由层次结构中该部分的子作用域继承。这意味着组织级角色适用于整个组织，文件夹级角色适用于该文件夹中的所有子文件夹和舰队，舰队级角色仅适用于该舰队中的资源。

使用与您希望成员保留的访问权限匹配的范围。例如，当成员需要在一个区域中跨多个队列拥有相同访问权限时，请在文件夹级别分配角色。当成员只需访问一个队列时，请在队列级别分配角色。

您不能在较低的作用域覆盖继承的访问权限。如果成员从组织或文件夹继承角色，请在最初授予该角色的更高作用域更改该分配。

"了解 NetApp Console 本地部署中的文件夹和机群"。"管理成员访问权限"。"管理机群访问分配"。