安装和设置

NetApp Console local deployment

NetApp
August 10, 2026

目录

安装和设置

设置 NetApp Console 本地部署的快速入门

安装 NetApp Console 本地部署后，设置您的组织，以便合适的团队可以安全地管理合适的存储资源。使用此清单可规划结构、组织资源、添加成员、配置集成以及启用数据服务。

必需的访问角色

超级管理员或组织管理员。"了解访问角色"。

1 安装 NetApp Console 本地部署

- 查看安装工作流程，了解部署流程。"了解 NetApp Console 本地部署的安装工作流"。
- 在您的 vCenter 中安装 NetApp Console 本地部署。"安装 NetApp Console 本地部署"。

2 规划组织

- 了解文件夹和队列如何组织您的资源。"了解文件夹和舰队"。
- 了解基于角色的访问控制 (RBAC) 如何授予成员所需的访问权限。"了解 NetApp Console 本地部署中基于角色的访问控制"。
- 请查看身份和访问管理工作流。"开始使用 IAM 进行队列和资源管理"。

3 设置您的组织

- 将存储系统添加到 NetApp Console 本地部署。"添加存储系统"。
- 创建与业务结构匹配的文件夹和车队层次结构。"创建文件夹和队列"。
- 将资源与正确的文件夹和群组关联。"将资源关联到文件夹和队列"。
- 添加成员并分配其初始角色。"添加成员并分配角色"。

4 配置集成和服务

- 与 Active Directory 集成，以便目录用户可以访问 Console 本地部署。"与 Active Directory 集成"。
- 连接您的大型语言模型（LLM），以启用 Console 助理和人工智能辅助管理。"连接 LLM"。
- 配置控制台本地部署如何传递通知。"配置通知传送"。

5 设置 NetApp Backup and Recovery

- "获取 NetApp Backup and Recovery 许可证".如果不想访问高级备份和恢复服务，则可以跳过此步骤。
- 将 NetApp Backup and Recovery 许可证添加到 NetApp Console 本地部署。"将许可证添加到 NetApp Console 本地部署"。

- "授予用户访问 NetApp Backup and Recovery 的权限"。

安装 NetApp Console

在 vCenter 中使用 OVA 安装 NetApp Console 本地部署

使用 OVA 在 VCenter 中安装 NetApp Console 本地部署。OVA 下载或 URL 可通过 NetApp 支持站点获得。

准备安装 NetApp Console 本地部署

安装前，请确保您的虚拟机主机符合要求，并且 NetApp Console 本地部署可以访问互联网和目标网络。要使用 NetApp Backup and Recovery 等 NetApp 数据服务，请为 NetApp Console 本地部署创建云提供商凭据，以代表您执行操作。

查看 NetApp Console 本地部署主机要求

在安装 NetApp Console 本地部署之前，请确保主机满足安装要求。

- CPU：16 核或 16 个 vCPU
- 内存：64 GB
- 磁盘空间：596 GB（建议使用厚资源调配）
- vSphere 7.0u3 或更高版本，使用虚拟硬件版本 19 或更高版本

在 vCenter 环境中安装 NetApp Console 本地部署，而不是直接在 ESXi 主机上。

设置 NetApp Console 本地部署的网络访问权限

NetApp Console 本地部署使用固定地址空间进行服务间通信。IP 范围 10.42.0.0/16 和 10.43.0.0/16 用于内部网络。在部署 Console 本地部署之前，请确保这些 IP 范围未分配给 Console 本地部署可用的 VLAN 上的其他虚拟机、DHCP 范围、DNS 记录或负载均衡器 VIP 池。

有关如何更改代理接口的 IP 地址的说明，请参阅知识库文章 Agent IP conflict with existing network。

在 VCenter 环境中安装 NetApp Console 本地部署

NetApp 支持在 VCenter 环境中安装 NetApp Console 本地部署。OVA 文件包含一个预配置的虚拟机映像，您可以在 VMware 环境中部署该映像。

下载 OVA 或复制 URL

下载 OVA。

1. 从 NetApp 支持站点下载 Console 本地部署软件。

在 VCenter 中部署 NetApp Console 本地部署

登录到您的 VCenter 环境以部署 Console 本地部署。

步骤

1. 如果您的环境需要，请将自签名证书上传到受信任的证书。您可以在安装后更换此证书。
2. 从内容库或本地系统部署 OVA。

来自本地系统	从内容库
a. 右键单击并选择 **Deploy OVF template……**。b. 从 URL 中选择 OVA 文件或浏览到其位置，然后选择下一步。	a. 转到您的内容库，然后选择 Console OVA。b. 选择 **Actions** > **New VM from this template**

3. 完成 Deploy OVF Template 向导以部署 Console。
4. 选择虚拟机的名称和文件夹，然后选择*下一步*。
5. 选择一个计算资源，然后选择*下一步*。
6. 查看模板详细信息，然后选择*下一步*。
7. 接受许可协议，然后选择*下一步*。
8. 请选择要使用的代理配置类型：显式代理、透明代理或无代理。
9. 选择要在其中部署 VM 的数据存储，然后选择 **Next**。请确保其满足主机要求。
10. 选择要连接虚拟机的网络，然后选择*下一步*。请确保网络为 IPv4，并具有到所需端点的出站 Internet 访问权限。
11. 在*自定义模板*窗口中，填写以下字段：
    - 代理信息
      - 如果选择了显式代理，请输入代理服务器主机名或 IP 地址和端口号，以及用户名和密码。
      - 如果选择了透明代理，请上传相应的证书。
    - 虚拟机配置
      - 跳过配置检查：默认情况下，此复选框未选中，这意味着 NetApp Console 本地部署将运行配置检查以验证网络访问。
        - NetApp 建议不选中此框，以便安装包括对 NetApp Console 本地部署的配置检查。配置检查验证 NetApp Console 本地部署是否具有所需端点的网络访问权限。如果由于连接问题导致部署失败，您可以从 NetApp Console 本地部署主机访问验证报告和日志。在某些情况下，如果您确信 NetApp Console 本地部署具有网络访问权限，则可以选择跳过检查。
      - 维护密码：为 `maint`用户设置密码，该用户可访问 NetApp Console 本地部署维护控制台。
      - **NTP servers**：指定一个或多个用于时间同步的 NTP 服务器。
      - 主机名：设置此虚拟机的主机名。它不能包含搜索域。例如，console10.searchdomain.company.com 的 FQDN 应输入为 console10。
      - 主 **DNS**：指定用于名称解析的主 DNS 服务器。
      - 辅助 **DNS**：指定要用于名称解析的辅助 DNS 服务器。
      - 搜索域：指定解析主机名时要使用的搜索域名。例如，如果 FQDN 是 console10.searchdomain.company.com，则输入 searchdomain.company.com。
      - **IPv4** 地址：映射到主机名的 IP 地址。
      - **IPv4 subnet mask**：IPv4 地址的子网掩码。

- **IPv4** 网关地址：IPv4 地址的网关地址。

12. 选择 **Next**。
13. 查看*准备完成*窗口中的详细信息，选择*完成*。

    vSphere 任务栏显示部署 NetApp Console 本地部署时的进度。

14. 启动此虚拟机。

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"。

设置 NetApp Console 组织

将文件夹和机群添加到 NetApp Console 本地部署组织

创建文件夹和队列以匹配您的业务结构，控制访问权限，并在 NetApp Console 本地部署中组织资源。

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"。

NetApp Console 本地部署在您创建组织时会创建一个默认群组。您可以添加更多群组并将其与文件夹分组。"了解 NetApp Console 中的资源层次结构"。

使用文件夹和队列组织资源

文件夹和 fleet 是您用来将组织塑造成与团队实际工作方式相匹配的两个构建模块。例如，每个区域一个文件夹，每个区域内都有一个生产 fleet 和一个开发 fleet。

- 文件夹对相关队列进行分组，并支持委派管理和角色继承。
- 队列是您关联资源以进行管理以及向用户授予操作访问权限的地方。

您可以先创建文件夹和 fleet，然后再添加资源和成员访问权限。这使您可以在 Console 本地部署中添加用户和资源之前规划资源层次结构。如果您的结构已定义，您可以在创建 fleet 时添加资源并分配访问权限。您可以随时更新 fleet。

例如，将生产集群置于生产舰队中，将测试集群置于测试舰队中，并仅授予每个团队对其所属舰队的访问权限。

文件夹

文件夹按业务结构（例如业务部门、地区或团队）组织机群。您可以嵌套文件夹以映射您的组织结构。

在文件夹级别分配的角色由子文件夹和车队继承。您还可以使用文件夹将车队分配任务委派给该部分层次结构的文件夹或车队管理员。

成员在队列中工作，而不是在文件夹中工作。仅与文件夹关联的资源在与队列关联之前，成员无法对其进行管理。

例如，区域企业可以使用文件夹按业务部门和工作负载组织 ONTAP 存储。它可能会为北美创建顶级文件夹，为生产和开发创建子文件夹，并为托管 SAP、VMware 和备份卷的 ONTAP 集群创建机群。分配给北美文件夹的存储管理员将继承对所有子机群的访问权限，而应用程序团队只能访问他们管理的机群。

车队

将资源与队列关联，以便成员可以对其进行管理。队列可以直接存在于组织下或文件夹中。

例如，一家医疗保健公司在独立的生产和开发集群中使用 ONTAP 存储。生产集群运行临床应用程序和病历数据库，而开发集群支持测试和验证。这种分离可以保护实时数据，实施更严格的生产访问控制，支持可审计性和最小权限控制，并允许开发团队在不影响面向患者的工作负载的情况下开展工作。

用户在*系统*页面上的已分配队列之间导航，以管理与每个队列关联的资源。

添加文件夹或队列

当您需要为资源和成员访问权限设置新边界时，请添加一个舰队；当您想要对相关舰队进行分组并委派其管理时，请添加一个文件夹。例如，添加一个 `Production`文件夹，其中包含一个 `Production-US-East`舰队和一个 `Production-EU-West`舰队，然后仅为其舰队分配区域主管的文件夹或舰队管理员角色。

您最多可以创建七个层次结构级别。

您可以在创建队列或文件夹时添加资源并分配成员访问权限，也可以稍后执行此操作。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*组织*。
3. 在 **Organization** 页面中，选择 **Add folder or fleet**。
4. 选择 **Folder** 或 **Fleet**。
5. 在*名称和位置*中：输入名称并选择文件夹或队列的位置。

1. 可选：展开 **Resources** 部分，将资源与队列或文件夹关联。
   a. 选中要关联的资源旁边的复选框，然后选择 **Associate with the fleet**。如果您尚未将系统添加到 Console 本地部署，可以稍后执行此步骤。

      在将资源分配给队列之前，成员无法访问文件夹中的资源。

2. 可选：展开 **Access** 部分，将访问权限分配给成员。选择 **Add a member** 以分配访问权限和角色。默认情况下，创建队列的用户有权访问该队列。

"了解访问角色"。

3. 选择 **Add**。

重命名文件夹或机群

根据需要重命名文件夹或队列。重命名不会影响关联的资源或成员访问权限。

步骤

1. 在*组织*页面中，导航到表中的车队或文件夹，选择 ⋯，然后选择*编辑文件夹*或*编辑车队*。
2. 在*编辑*页面上，输入一个新名称并选择*应用*。

删除文件夹或舰队

删除不再需要的文件夹和队列，例如在团队重组或队列完成后。

在删除文件夹或机群之前，请完成以下检查：

- 确认此文件夹或车队不包含资源。"了解如何删除资源关联"。
- 审查仍有权访问该文件夹或机群的成员。"查看成员访问权限分配".
- 根据需要删除或更新成员访问权限。"修改成员访问分配"。
- 如果要删除舰队，请先将资源转移到目标舰队。"了解如何在队列之间移动资源"。

步骤

1. 在*组织*页面中，导航到表中的机群或文件夹，选择 ⋯，然后选择*删除*。
2. 确认要删除此文件夹或舰队。

在 **NetApp Console** 本地部署中管理机群和文件夹

初始设置后，您可以执行以下操作：

- 管理文件夹和队列的资源关联："了解如何将资源与队列和文件夹关联"。
- 查看或更新一个文件夹或车队的访问权限："了解如何授予用户对队列的访问权限"。
- 跨多个文件夹和队列管理一个成员："了解如何管理成员访问权限"。
- 添加其他成员并分配启动权限："了解如何管理成员和权限"。

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"
- "管理机群访问分配"
- "了解身份和访问 API"

将存储系统添加到 NetApp Console 本地部署

将存储系统添加到 NetApp Console 本地部署，以实现对存储基础架构的监控、清单管理和管理。添加存储系统后，Console 本地部署将发现该系统并开始收集可用于监控和管理任务的信息。

开始之前，请确保您具有添加存储系统所需的权限，并且可以从 Console 本地部署访问存储系统。

步骤

1. 选择 **Storage > Management**。
2. 从 Scope 下拉列表中，选择要将存储系统添加到的群组。
3. 选择*添加系统*。
4. 请输入所需的存储系统详细信息，包括连接信息和凭据。
5. 查看您输入的信息并选择*添加*。

   已将存储系统添加至所选群组。Console 本地部署开始发现和监控系统。根据环境和网络连接，系统可能需要几分钟才能显示为完全受管。

您还可以通过选择 **Add system** 并提供所需的系统信息，从 **Administration > Identity and access** 页面添加存储系统。

管理 NetApp Console 本地部署中的文件夹和队列中的资源

通过将资源与正确的文件夹或群组关联来管理 NetApp Console 本地部署中的资源访问，这些文件夹或群组控制哪些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"。

将资源放置在合适的团队可以管理的位置，在所有权发生变更时进行移动，并在不再需要时删除关联。

resource 是 Console 本地部署识别的实体，例如存储资源或备份和恢复工作负载。

控制台资源类型

控制台本地部署同时支持存储资源和备份与恢复工作负载。将任一资源类型与机群关联，以控制访问和管理。

存储资源

存储资源是组织中最常见的资源类型。将存储系统添加到 Console 本地部署时，请将其与机群关联，以便相应的团队可以访问和管理它。例如，添加 ONTAP 集群后，将其与 `Production-US-East`机群关联。

备份和恢复工作负载

备份和恢复工作负载也被视为资源。您可以通过将工作负载与机群关联来分配成员访问备份和恢复工作负载的权限。例如，通过将备份和恢复工作负载与成员可以访问的机群关联并授予相应的备份和恢复角色，为成员分配对该工作负载的访问权限。

查看组织中的资源

查看组织中的资源以查找特定资源，并查看其关联的队列或文件夹。如果您尚未创建任何文件夹或队列，则所有资源都与组织下的默认队列直接关联。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*资源*。
3. 选择*高级搜索和过滤*。
4. 使用可用选项查找资源：
   - 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、文件夹或队列：选择整个组织、特定文件夹或特定队列。
5. 选择*搜索*。

将资源与文件夹或群组关联

将资源与队列或文件夹关联，以便相应的团队可以对其进行管理。例如，添加 ONTAP 集群后，将其与 `Production-US-East`队列关联，以便该队列的区域存储管理员可以对其进行管理。

具有组织管理员角色的用户可以将资源添加到文件夹，以将队列关联任务委托给该文件夹的文件夹或队列管理员。"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*关联到文件夹或群组*。
2. 选择一个文件夹或队列，然后选择 **Accept**。
3. 要关联其他文件夹或队列，请选择 **Add folder or fleet**，然后选择相应的文件夹或队列。

   请注意，您只能从具有管理员权限的文件夹和队列中进行选择。

4. 选择*关联资源*。
   - 如果将资源与队列关联，则拥有这些队列权限的成员现在可以从 Console 访问资源。
   - 如果您将资源与文件夹关联，*Folder or fleet admin* 现在可以访问该资源，并将其与文件夹中的舰队关联。"将资源与文件夹关联".

查看与资源关联的文件夹和群组

验证资源与哪些队列或文件夹关联。

要查看哪些成员具有对资源的访问权限，请查看分配给关联文件夹或舰队的成员。"管理机群访问分配".

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队列关联的资源。

要查看哪些成员有权访问资源，请查看关联的文件夹或舰队。

"管理机群访问分配"。"管理成员访问权限"。

从文件夹或队列中删除资源

删除资源与文件夹或机群的关联，以防止成员在该处管理该资源。

要从整个组织中删除存储系统，请转到*系统*页面并删除系统。

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. 要从文件夹或队列中删除资源，请选择文件夹或队列旁边的 🗑 。
3. 选择*删除*以删除关联。

在机群之间移动资源

通过删除资源与当前队列的关联，然后将其与目标队列关联，从而将资源从一个队列移动到另一个队列。

关联更改后，对资源的访问权限立即更改。如果可能，请在一个维护窗口内完成这两个步骤。

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. 选择当前队列旁边的 🗑 ，然后选择*删除*。
3. 选择*添加文件夹或 fleet*。
4. 选择目标队列并选择 **Accept**。
5. 选择*关联资源*。

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"

- "移动资源后管理队列访问分配"
- "了解用于身份和访问的 API"

将成员添加到 NetApp Console 本地部署组织

将成员添加到 NetApp Console 本地部署组织并分配角色，以授予用户、服务帐户和目录用户在组织、文件夹或群组级别的访问权限。

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"。

开始之前

- 创建与贵组织匹配的文件夹和车队层次结构。"了解如何使用文件夹和队列组织资源"。
- 在分配成员访问权限之前，请将资源与正确的队列关联。"了解如何管理文件夹和队列中的资源"。
- 如果要添加目录用户，请先集成目录服务。"了解如何与您的目录服务集成"。

了解如何在 **NetApp Console** 本地部署中授予访问权限

NetApp Console 使用基于角色的访问控制 (RBAC) 来管理权限。为成员分配角色以提供所需的访问权限。每个角色都定义了特定资源的允许操作。

请注意以下有关在 NetApp Console 本地部署中授予访问权限的信息：

- 必须将每个用户显式添加到您的组织，并至少分配一个角色，该用户才能访问资源。
- 在组织或文件夹级别分配的角色由子作用域继承，因此请仔细选择分配作用域，仅在需要时授予成员访问权限。"了解 NetApp Console 本地部署中的角色继承"。

将成员添加到您的组织

NetApp Console 支持三种类型的成员：用户帐户、目录用户和服务帐户。

> 在添加用户之前，必须首先配置电子邮件服务器以与 Console 本地部署配合使用。"了解如何配置电子邮件服务器。"

目录用户通过您的集成目录服务进行身份验证，但您仍然必须单独添加每个目录用户并在 Console 本地部署中分配角色。直接在 Console 中创建服务帐户。

要访问 Console 本地部署，所有成员必须至少明确分配一个角色。

添加成员时，请选择成员需要访问的组织、文件夹或舰队，并分配他们所需的起始角色。

添加用户帐户

要将用户添加到组织、文件夹或队列，以便他们可以访问资源，您必须具有组织管理员或文件夹或队列管理员角色。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择*添加成员*。
4. 对于*成员类型*，请保持选择*用户*。
5. 对于*用户的电子邮件*，输入与他们创建的登录名关联的用户的电子邮件地址。
6. 请使用*选择组织、文件夹或 Fleet* 部分，选择成员需要访问的位置。

   请注意以下事项：

   - 您只能选择您有权限的文件夹和车队。
   - 选择组织或文件夹时，您将授予成员对其所有内容的权限。
   - 您只能在组织级别分配*Organization admin*角色。
7. 选择一个类别，然后选择一个*角色*，为成员提供所选组织、文件夹或队列所需的起始权限。

   "了解访问角色"。
8. 要允许访问更多文件夹、队列或角色，请选择 **Add role**，选择文件夹、队列或角色类别，然后选择一个角色。
9. 选择 **Add**。

   Console 通过电子邮件将说明发送给用户。

添加服务帐户

需要自动执行任务或安全连接到 Console API 时，请添加服务帐户。创建帐户后，复制其客户端 ID 和客户端密钥，以供将使用该帐户的集成使用。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择*添加成员*。
4. 对于 **Member Type**，选择 **Service account**。
5. 输入服务帐户的名称。
6. 使用*选择组织、文件夹或队列*部分，选择服务账号需要访问的位置。

   请注意以下事项：

   - 您只能从您有权限的文件夹和队列中进行选择。
   - 选择一个组织或文件夹将授予成员访问其所有内容的权限。
   - 您只能在组织级别分配*Organization admin*角色。
7. 选择一个 **Category**，然后选择一个 **Role**，为服务帐户提供所选组织、文件夹或 fleet 所需的起始权限。

   "了解访问角色"。

8. 要允许访问更多文件夹、队列或角色，请选择 **Add role**，选择文件夹、队列或角色类别，然后选择一个角色。
9. 下载或复制客户端 ID 和客户端密钥。

   Console 仅显示一次客户端密码。请安全地复制它；如果丢失，您可以稍后重新创建。

10. 选择*Close*。

将目录用户添加到您的组织

从集成目录服务中添加用户并授予其第一个角色。例如，从 Active Directory 中添加新的存储工程师，并在 `Production-US-East`机群中分配 Storage admin 角色，以便他们可以在该机群中工作。

添加目录用户之前，必须先配置目录服务。"了解如何与您的目录服务集成".

步骤

1. 选择 **Administration > Identity and access**。
2. 选择 **Members**。
3. 选择*添加成员*。
4. 对于*成员类型*，选择*目录用户*。
5. 对于*用户的电子邮件*，请输入要添加的目录用户的电子邮件地址。此电子邮件地址必须与用户在您的目录中登录时关联的电子邮件地址匹配。
6. 使用*选择组织、文件夹或舰队*部分选择目录用户需要访问的位置。

   请注意以下事项：

   - 您只能从您有权限的文件夹和队列中进行选择。
   - 选择一个组织或文件夹将授予成员访问其所有内容的权限。
   - 您只能在组织级别分配*Organization admin*角色。
7. 选择一个*Category*，然后选择一个*Role*，为目录用户提供所选组织、文件夹或队列所需的起始权限。

   "了解访问角色"。

8. 要授予用户对其他文件夹、队列或角色的额外访问权限，请选择 **Add role**，选择文件夹或队列、角色类别，然后选择一个角色。

访问角色

NetApp Console 本地部署访问角色

NetApp Console 本地部署中的标识和访问管理 (IAM) 提供预定义的角色，可将这些角色分配给资源层次结构不同级别的组织成员。在分配这些角色之前，您应了解每个角色所包含的权限。角色分为以下几类：平台、应用程序和数据服务。

平台角色

平台角色授予 NetApp Console 本地部署管理权限，包括角色分配和用户管理。Console 本地部署有多个平台角色。

平台角色	职责
"组织管理员"	允许用户无限制地访问组织内的所有 fleet 和文件夹，将成员添加到任何 fleet 或文件夹，以及执行任何任务和使用任何未关联明确角色的数据服务。具有此角色的用户通过创建文件夹和 fleet、分配角色、添加用户以及在拥有适当凭据的情况下管理系统来管理您的组织。
"文件夹或舰队管理员"	允许用户不受限制地访问指定的队列和文件夹。可以将成员添加到其管理的文件夹或队列，以及在分配给他们的文件夹或队列内的资源上执行任何任务并使用任何数据服务或应用程序。
"联盟管理员"	允许用户使用控制台创建和管理目录服务联盟，以便用户可以使用其现有目录凭据进行身份验证。
"联盟查看器"	允许用户使用 Console 查看现有目录服务联盟。无法创建或管理联盟。
"超级管理员"	为用户提供所有管理员角色。此角色专为不需要跨多个用户分配 Console 职责的小型组织设计。
"超级查看器"	为用户提供所有查看者角色。此角色专为不需要跨多个用户分配 Console 职责的小型组织设计。

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
"运营支持分析师"	提供对警报和监控工具（如"审核"页面）的访问。
"存储管理员"	管理存储运行状况和治理功能，发现存储资源，以及修改和删除现有系统。
"存储查看器"	查看存储运行状况和治理功能，以及查看以前发现的存储资源。无法发现、修改或删除现有存储系统。
"系统运行状况专家"	管理存储、运行状况和治理功能，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"	执行对本地快照的备份，复制到辅助存储，并备份到对象存储。
"备份和恢复还原管理员"	在 Backup and Recovery 中还原工作负载。
"备份和恢复克隆管理"	在 Backup and Recovery 中克隆应用程序和数据。

数据服务角色	职责
"备份和恢复查看器"	查看 Backup and Recovery 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为其有权访问的资源生成报告。这些用户无法启用或禁用卷、存储桶或数据库架构的扫描。Data Classification 没有管理员角色。
SnapCenter 管理员	提供使用 NetApp Backup and Recovery 针对应用程序从本地 ONTAP 集群备份快照的功能。拥有此角色的成员可以执行以下操作：* 执行 Backup and Recovery > Applications 中的任何操作 * 管理其拥有权限的队列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"
- "开始在 NetApp Console 中使用身份和访问权限"
- "在 NetApp Console 组织中添加成员并分配角色"
- "了解用于 NetApp Console IAM 的 API"

NetApp Console 本地部署平台访问角色

将平台角色分配给用户，以授予管理 NetApp Console 本地部署、分配角色、添加用户、创建车队和管理用户身份验证的权限。

大型跨国组织的组织角色示例

XYZ Corporation 按区域（北美、欧洲和亚太地区）组织数据存储访问，通过集中监督提供区域控制。

XYZ Corporation 的 Console 本地部署中的*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*文件夹或队列管理员*在该区域的文件夹中组织队列（以及相关资源）。

具有 **Folder or fleet admin** 角色的区域管理员通过添加资源和用户来主动管理其文件夹。这些区域管理员还可以添加、删除或重命名其管理的文件夹和 fleet。**Organization admin** 继承任何新资源的权限，从而保持对整个组织存储使用情况的可见性。

在同一组织内，一个用户被分配了 **Federation admin** 角色，以管理组织与其公司 IdP 的联合。此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。**Organization admin** 为用户分配 **Federation viewer** 角色，以检查联合状态并查看联合组织。

下表显示了每个 Console 本地部署平台角色可以执行的操作。

组织管理角色

任务	组织管理员	文件夹或舰队管理员
在控制台本地部署中创建、修改或删除系统（添加或发现系统）	是	是
创建文件夹和舰队，包括删除	是	否

任务	组织管理员	文件夹或舰队管理员
重命名现有文件夹和机群	是	是
分配角色并添加用户	是	是
将资源与文件夹和队列关联	是	是
注册支持并通过 Console 提交案例	是	是
使用未与显式访问角色关联的数据服务	是	是
查看审核页面和通知	是	是

联合身份验证角色

任务	联盟管理员	联盟查看器
创建和更新目录服务集成	是	否
查看联盟及其详细信息	是	是

超级管理员和查看者角色

*超级管理员*角色提供管理 Console 功能、存储和数据服务的完全访问权限。此角色适合负责管理和治理的人员。相比之下，*超级查看器*角色提供只读访问权限，非常适合需要了解情况但不进行更改的审核员或利益相关者。

组织应谨慎使用 **Super admin** 访问权限，以最大限度地降低安全风险，并遵循最低权限原则。大多数组织应分配只具有必要权限的细粒度角色，以降低风险并提高可审核性。

超级角色示例

ABC Corporation 拥有一个五人的小团队，他们利用 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 **Super admin** 角色分配给两名资深团队成员，由其处理所有管理任务，包括用户管理和资源配置。其余三名团队成员被分配了 **Super viewer** 角色，使他们能够监控存储运行状况和数据服务状态，但无法修改设置。

角色	继承的角色
超级管理员	• 组织管理员 • 文件夹或舰队管理员 • 备份和恢复超级管理员 • 存储管理员
超级查看器	• 组织查看器 • 备份查看器 • 存储查看器

NetApp Console 本地部署中的运维支持分析师访问角色

在 NetApp Console 本地部署中，您可以将操作支持分析师角色分配给用户，以便为他们

提供对警报和监控的访问权限。

运营支持分析师

任务	可执行
查看存储系统	是
查看审核页面和通知	是
查看、下载和配置警报	是

适用于 **NetApp Console** 本地部署的存储访问角色

您可以将以下角色分配给用户，以便为他们提供对 NetApp Console 本地部署中存储管理功能的访问权限。您可以为用户分配用于管理存储的管理角色或用于监控的查看器角色。

管理员可以将以下存储资源和功能的存储角色分配给用户：

存储资源：

- 本地 ONTAP 集群

控制台服务和功能：

- 存储健康功能

NetApp Console 本地部署中的存储角色示例

XYZ Corporation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。他们允许该团队管理其区域的存储资产，同时限制对用户管理和许可证管理等核心 Console 本地部署任务的访问。

在一个由 12 人组成的团队中，两个用户被赋予 **Storage viewer** 角色，允许他们监控与分配给他们的 Console 本地部署队列相关联的存储资源。其余九个用户被赋予 **Storage admin** 角色，该角色包括管理软件更新、通过 Console 本地部署访问 ONTAP System Manager 以及发现存储资源（添加系统）的能力。团队中的一个人被赋予 **System health specialist** 角色，以便他们可以管理其所在区域中存储资源的运行状况，但不能修改或删除任何系统。此人还可以对分配给他们的队列的存储资源执行软件更新。

该组织还有另外两个具有 **Organization admin** 角色的用户，他们可以管理 Console 本地部署的所有方面，包括用户管理和许可证管理，以及几个具有 **Folder or fleet admin** 角色的用户，他们可以为分配给他们的文件夹和机群执行 Console 本地部署管理任务。

下表显示了每个存储角色执行的操作。

功能和操作	存储管理员	系统运行状况专家	存储查看器
存储管理：			
发现新资源（添加系统）	是	是	否
查看已添加的系统	是	是	否
从 Console 中删除系统	是	否	否

功能和操作	存储管理员	系统运行状况专家	存储查看器
修改系统	是	否	否
System Manager 访问			
可以输入凭据	是	是	否

NetApp Backup and Recovery 在 **NetApp Console** 本地部署中的角色

在 NetApp Console 本地部署中，您可以将以下角色分配给用户，以便为他们提供对 Console 内 NetApp Backup and Recovery 的访问权限。Backup and Recovery 角色使您能够灵活地为用户分配特定于其在组织内需要完成的任务的角色。如何分配角色取决于您自己的业务和存储管理实践。

该服务使用以下特定于 NetApp Backup and Recovery 的角色。

- 备份和恢复超级管理员：在 NetApp Backup and Recovery 中执行任何操作。
- **Backup and recovery backup admin**：在 NetApp Backup and Recovery 中执行备份到本地快照、复制到辅助存储以及备份到对象存储操作。
- 备份和恢复还原管理：使用 NetApp Backup and Recovery 还原工作负载。
- 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，请参见 "Console 设置和管理文档"。

用于常见操作的角色

下表显示了每个 NetApp Backup and Recovery 角色可以为所有工作负载执行的操作。

功能和操作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复还原管理员	备份和恢复克隆管理	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
查看控制面板和所有选项卡	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

功能和操作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复还原管理员	备份和恢复克隆管理	备份和恢复查看器
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
计划：					
激活计划	是	是	是	是	否
暂停计划	是	是	是	是	否
策略和保护：					
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
还原工作负载	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

功能和操作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复还原管理员	备份和恢复克隆管理	备份和恢复查看器
关联或删除实例凭据	是	是	是	否	否
Buckets：					
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

下表显示了每个 NetApp Backup and Recovery 角色可以对特定工作负载执行的操作。

Kubernetes 工作负载

下表显示了每个 NetApp Backup and Recovery 角色可以为特定于 Kubernetes 工作负载的操作执行的操作。

功能和操作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复还原管理员	备份和恢复查看器
查看群集、命名空间、存储类和 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
使用策略创建备份并保护应用程序	是	是	否	否
取消对应用程序的保护并删除备份	是	是	否	否
查看恢复点和资源查看器结果	是	是	是	是

功能和操作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复还原管理员	备份和恢复查看器
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
查看执行挂钩和挂钩源	是	是	是	是
创建执行挂钩和挂钩源	是	是	是	否
更新执行挂钩和挂钩源	是	是	是	否
删除执行挂钩和挂钩源	是	是	是	否
查看执行挂钩模板	是	是	是	是
创建执行挂钩模板	是	是	是	否
更新执行挂钩模板	是	是	是	否
删除执行挂钩模板	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 桶和存储目标	是	是	是	是

配置 Console 集成和服务

将 NetApp Console 本地部署与 Active Directory 集成

将 NetApp Console 本地部署与 Active Directory 集成，以进行目录支持的登录和用户查找。使用目录服务对用户进行身份验证，然后在 NetApp Console 本地部署中将访问权限分配给这些用户。

必需的访问角色

超级管理员或组织管理员。"了解访问角色"。

与 Active Directory 集成时，Console 本地部署将通过现有目录对用户进行身份验证。添加目录用户后，分配 Console 访问角色以控制该用户可以访问的内容。

Active Directory 集成还可以通过将现有控件、审计跟踪和策略应用于 Console 本地部署访问，帮助您满足合规性要求。

- Active Directory 集成不会创建联合组，不会同步目录组分配，也不会自动授予访问权限。管理员仍会将目录用户添加到组织并在 Console 本地部署中分配角色。
- 一次仅支持一个 Active Directory 集成。配置集成后，添加集成 按钮将被禁用。要切换到其他目录，请先禁用或删除现有集成。
- 目录用户不配置或使用多重身份验证 (MFA)。Console 本地部署仅为本地用户支持 MFA。"了解如何管理成员安全设置"。

开始之前

在与 Active Directory 集成之前，请确认您已：

- 可以查询目录的Active Directory域和凭据
- LDAP 服务器地址和目录树的基本可分辨名称 (DN)
- 从 Console 本地部署到 LDAP 服务器的端口 389（LDAP）或 636（LDAPS）的网络访问
- SSL/TLS 证书（如果您计划使用 LDAPS）

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 选择*添加集成*。
4. 输入 Active Directory 服务器的连接详细信息：
   - 集成的描述性名称。
   - **LDAP** 主机：您的 LDAP 服务器的主机名或 IP 地址。对于多台服务器，请输入主服务器。
   - 端口：LDAP 为 389，LDAPS 为 636。
   - *连接超时*以毫秒为单位。默认值为 1000 毫秒。
5. 选择 **Use SSL/TLS** 以使用 LDAPS。确认您的 LDAP 服务器支持 LDAPS，并且控制台可以访问所需的证书。
6. 测试连接。如果失败，请检查 LDAP 主机、端口、网络连接和 SSL/TLS 证书。
7. 测试成功后，输入目录和用户详细信息：
   - **Base DN binding**：输入此应用程序将用于连接到目录的 LDAP/AD 帐户的绑定 DN，并输入该帐户的绑定凭据（密码）。Console 使用这些详细信息绑定到 LDAP 并验证连接。
   - 用户 **DN**：有权查询目录的用户帐户。例如， `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`。
8. 选择*添加*以保存此集成。

完成后

保存集成后，向组织添加目录用户并分配角色。添加目录用户之前，必须配置并启用至少一个 Active Directory 集成。"了解如何添加目录用户并分配角色"。

禁用或启用 **Active Directory** 集成

禁用集成以暂时挂起目录支持的身份验证，而不删除配置。禁用目录服务时，目录用户无法通过目录登录。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 在集成列表中，找到该集成，然后选择该行的操作菜单。
4. 选择*禁用*以暂停集成，或选择*启用*以恢复集成。

删除 **Active Directory** 集成

删除集成以永久删除目录服务配置。在删除之前，请查看有关链接到集成的目录用户的任何警告，因为他们的访问权限将受到影响。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 在集成列表中，找到该集成，然后选择该行的操作菜单。
4. 选择 **Delete** 并确认删除。

连接您的 **LLM** 并在 **NetApp Console** 本地部署中启用 **NetApp Console** 助手

将您的大型语言模型 (LLM) 连接到 NetApp Console 本地部署，以启用 Console 助理和 AI 辅助存储管理。

本文档以技术预览形式提供有关将 LLM 连接到 Console 助理以启用 AI 功能的文档。通过此预览产品，NetApp 保留在正式发布之前修改产品详情、内容和时间表的权利。

必需的访问角色

超级管理员或组织管理员。"了解访问角色"。

设置完成后，用户从控制面板打开 Console 助理并选择访问模式：

- 在*只读*模式下，助手回答问题并提供指导，而不进行任何更改。
- 在"读/写"模式下，助手可以对存储基础设施进行操作。它会在每次更改前显示详细信息以供审核和确认。对于异步操作（例如创建卷），它会创建一个作业，用户可以从助手检查该作业。

要连接您的 LLM，请选择提供程序路径，输入端点详细信息和 API 密钥，然后在 **Administration > AI Tools** 中选择一个模型。助手操作在您的存储策略和基于角色的访问控制范围内执行。

在连接 **LLM** 之前，请先收集所需信息

在连接 LLM 之前，请收集以下信息：

- 您的提供程序类型决定：OpenAI 或 OpenAI 兼容。 "了解提供者的选择。"
- 您选择的提供程序路径的有效 API 密钥。
- 提供程序路径的端点 URL。
- 您的代理或网关 URL（如果您的组织需要）。
- LLM 提供商帐户的用户名或单点登录 (SSO) ID（如果需要）。
- 从 Console 本地部署到选定端点的网络访问。
- 计划允许的助理操作的存储类和基于角色的访问控制。

有关支持的型号详细信息，请参见 "了解 NetApp Console 本地部署中受支持的 LLM 提供程序和模型"。

将 **LLM** 连接到 **NetApp Console** 本地部署

输入提供程序设置、API 密钥和模型，将 LLM 连接到 Console 本地部署。

步骤

1. 登录到 NetApp Console 本地部署。
2. 选择 **Administration > AI Tools**。
3. 选择菜单，然后选择 **Edit**。
4. 在*提供程序类型*中，选择一个提供程序类型。

   "了解 LLM 在 NetApp Console 本地部署中的集成"。
5. 如果提示输入提供程序端点，请输入所选提供程序路径的端点 URL。
6. 输入代理或网关 URL 和凭据。
7. 在*用户名*字段中，输入您的用户名或 SSO ID（如果您的提供商路径需要）。
8. 在 **API key** 字段中，粘贴您所选提供商路径中的 API 密钥。
9. 从列表中选择一个模型。
10. 查看配置，然后选择 **Save**。

    如果保存或测试失败，请验证提供程序类型、端点 URL、API 密钥和所选模型，然后重试。

"排查 LLM 集成故障"。

验证 **LLM** 集成是否有效

保存配置后，请验证助手的可用性和行为。

步骤

1. 确认 **Console assistant** 按钮出现在 NetApp Console 本地部署仪表板上。

2. 在*只读*模式下打开助手并运行基本查询。
3. 在*读/写*模式下打开助手，确认存储更改操作需要用户确认后才能执行。
4. 验证需要操作工作流的用户是否具有所需的基于角色的访问控制。

完成验证后，用户可以从仪表板打开 Console 助理，并以简单的语言描述任务。有关使用示例和最终用户工作流，请参见 "使用 NetApp Console 助手"。

保护凭据并监控 **LLM** 使用情况

- 尽可能使用专用 API 密钥进行 Console 本地部署集成。
- 根据您的组织策略轮换 API 密钥。
- 将可以编辑 AI Tools 设置的人员限制为仅所需的管理员角色。
- 监控提供商端 API 使用情况和警报，以跟踪异常活动或成本峰值。

排除 NetApp Console 本地部署中的 LLM 集成故障

使用此快速分流流程来诊断和解决 NetApp Console 本地部署中的常见 LLM 集成问题。

本文档以技术预览形式提供有关将 LLM 连接到 Console 助理以启用 AI 功能的文档。通过此预览产品，NetApp 保留在正式发布之前修改产品详情、内容和时间表的权利。

如果您尚未完成设置，请参见 "连接您的 LLM 并启用 NetApp Console 助理"。

快速分类 **LLM** 集成问题

1. 在*管理 > AI Tools*中验证 AI Tools 配置。

   确认提供程序类型、端点 URL、API 密钥、所选模型和出站网络访问。

2. 在控制面板上验证助手可用性。

   确认预期用户和组织的 **Console assistant** 按钮是否显示。

3. 验证运行时行为。

   运行一个简单的只读请求，并确认提供程序端点可访问性、模型可用性和提供程序服务运行状况。

按症状排查故障

症状	可能的原因	需要检查的内容	下一步操作
在 AI Tools 中保存或测试失败	配置或连接不匹配	提供程序类型、端点 URL、API 密钥格式、所选模型和出站访问	请更正验证失败的值，然后再次保存
Console assistant 按钮缺失	不正常的集成状态、组织不匹配或 RBAC 不匹配	成功的 AI Tools 保存、集成状态、当前组织和预期访问角色	刷新会话并使用已知良好的管理员账号进行验证

症状	可能的原因	需要检查的内容	下一步操作
助手已打开但请求失败	提供程序或运行时路径问题	端点可达性、该端点上的模型可用性、提供程序限制和临时提供程序状态	修复端点/模型不匹配或提供方端限制问题后重试
助理响应缓慢或不一致	提示大小、端点性能或网络/代理不稳定性	短提示测试、提供商服务健康状况和网络/代理稳定性	使用较短的提示，尝试其他支持的模型，并稳定网络或代理路由

应对 **LLM** 凭据泄露或滥用

如果怀疑 API 密钥泄露或未经授权使用：

1. 撤销提供程序系统中的现有 API 密钥。
2. 创建新的 API 密钥。
3. 更新 **Administration > AI Tools** 中的密钥。
4. 使用只读助手测试验证重新连接是否成功。

在 **NetApp Console** 本地部署中设置通知传递渠道

在 NetApp Console 本地部署中，您可以为警报通知设置多个通道，包括电子邮件和 Webhook。

必需的访问角色

超级管理员或组织管理员。"了解访问角色"。

默认情况下，Console 本地部署通过其内置通知系统显示通知。配置其他交付渠道可让您以最适合工作流程的方式接收通知。

您可以通过相同的渠道发送所有通知，也可以针对不同的通知类型使用不同的渠道。例如，您可以通过电子邮件发送紧急存储警报，同时通过 webhook 将其他警报流量路由到第三方监控工具。

设置通知投递通道后，您可以配置通知规则并将其分配给不同的通道。"了解如何配置通知规则"。

配置电子邮件服务器

配置电子邮件服务器时，Console 本地部署会通过它发送通知、警报和用户邀请。Console 本地部署支持 SMTP 电子邮件服务器，该服务器可以是您现有的企业电子邮件服务器或第三方电子邮件服务。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在*电子邮件服务器*部分，选择*配置*。
4. 输入电子邮件服务器的连接详细信息：
   - 添加发件人姓名和发件人电子邮件地址。
   - **SMTP** 主机：SMTP 服务器的主机名或 IP 地址。对于多台服务器，请输入主服务器。

- 从*连接安全*下拉列表中选择连接协议。该端口已为您配置，且为只读：25 用于 SMTP with STARTTLS，或 465 用于 SMTPS。

  SMTPS（端口 465）立即建立加密连接，建议用于安全敏感的环境。STARTTLS（端口 25）从未加密的连接升级，如果加密协商失败，可能会回退到未加密的传输。

5. 选择*测试电子邮件*以向您指定的收件人发送测试电子邮件。
6. 测试成功后，选择 **Save** 保存配置。

   如果测试失败，请重新验证您输入的设置，并仔细检查 Console 本地部署是否具有对电子邮件服务器的网络访问权限。

更新电子邮件服务器配置

如果要使用其他电子邮件服务器，可以更新现有的电子邮件服务器配置。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在*电子邮件服务器*部分，选择*配置*。
4. 选择*Clear fields*以清除现有配置。
5. 输入电子邮件服务器的新连接详细信息。
6. 选择*测试电子邮件*以向您指定的收件人发送测试电子邮件。
7. 测试成功后，选择 **Save** 保存新配置。

   如果测试失败，请重新验证您输入的设置，并仔细检查 Console 本地部署是否具有对电子邮件服务器的网络访问权限。

删除电子邮件服务器配置

如果您不再希望 Console 本地部署发送电子邮件，则可以删除电子邮件服务器配置。

步骤

1. 选择 **Administration > Console**。
2. 选择*配置*以打开系统配置页面。
3. 在*电子邮件服务器*部分，选择*配置*。
4. 选择*Clear fields*以清除现有配置。
5. 选择 **Save** 保存已清除的配置，这将从 Console 本地部署中删除电子邮件服务器配置。

配置 **Webhook**

设置 Webhook，以便从 Console 本地部署向其他工具或服务发送通知。您可以配置多个 Webhook，每个 Webhook 指向不同的端点。例如，一个用于 SIEM，另一个用于值班寻呼服务。

创建 webhook 后，具有 Storage admin 角色的用户可以将其分配给特定的警报规则。例如，他们可以将关键警

报发送到电子邮件，同时通过 webhook 将所有警报发送到第三方监控工具。

> Console 本地部署不会在 Webhook 端点上实施访问控制。任何可以访问端点 URL 的用户或系统都会收到警报数据。确保通过应用程序自己的访问控制，将对接收应用程序的访问权限限制为授权用户。

开始之前

确认 Console 本地部署可以通过网络到达接收应用程序，并收集端点 URL、HTTP 方法以及该应用程序所需的任何身份验证或证书详细信息。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在 **Webhook** 集成 部分，选择 配置。
4. 输入 Webhook 所需的详细信息：
   - Webhook 的描述性名称。
   - 接收应用程序提供的端点 URL。
   - HTTP 方法
   - 可选：PEM 格式的自签名证书。
   - 任何必需的标头或机密（身份验证凭据）。
   - 发送 Webhook 时使用的格式。支持 JSON 和 OTEL (OpenTelemetry)。

     将 JSON 用于通用 Webhook 和自定义 REST 端点。将 OTEL 用于本机使用 OpenTelemetry 信号的可观测性平台，例如 Grafana 或其他 OpenTelemetry 兼容的收集器。
5. 选择 **Test webhook** 以测试 webhook 连接，并确保 Console 本地部署可以成功将消息发送到接收应用程序。
6. 测试成功后，选择*保存*以创建 Webhook。

   保存 Webhook 后，用户可以在支持 Webhook 的位置选择它，例如警报传递选项。 "了解如何创建警报规则并分配用于警报传递的 Webhook。"

版权信息

商标信息