NetApp Console 本地部署文档

NetApp Console local deployment

NetApp
August 10, 2026

目录

NetApp Console 本地部署

发行说明

NetApp Console 本地部署的新增功能

了解最新版本的 NetApp Console 本地部署中的新增功能和增强功能。

介绍 **NetApp Console** 本地部署

"了解 NetApp Console 本地部署"。

NetApp Console 本地部署中的已知限制

已知限制指出本产品版本不支持的平台、设备或功能，或与其无法正常互操作的平台、设备或功能。请仔细查看这些限制。

这些限制特定于 NetApp Console 和管理的设置：代理、软件即服务 (SaaS) 平台等。

Console VM 限制

可能与**10.42.0.0/16**和**10.43.0.0/16**范围内的**IP**地址发生冲突

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。

不支持共享 **Linux** 主机

与其他应用程序共享的 VM 不支持该代理。VM 必须专用于代理软件。

第三方代理和扩展

代理虚拟机不支持第三方代理或虚拟机扩展。

比较 NetApp Console 本地部署和 NetApp Console

未解析的指令，位于 <stdin> - include::https://raw.githubusercontent.com/NetAppDocs/console-all-family/main/intro-family.adoc[lines=15..-1]

开始使用

了解 NetApp Console 本地部署

NetApp Console 本地部署允许您在自己的基础架构中托管和运行 NetApp Console 自主控

制平面。

您可以获得统一的存储管理、策略实施、大规模自动化和 AI 辅助操作。数据、元数据或管理流量均不会离开您的环境。

在自己的基础架构中部署和操作 **Console**

NetApp Console 本地部署在您自己的基础架构中运行，因此您的团队可以控制部署、连接和日常操作。您需要部署 Console 代理、维护 Console 虚拟机，并管理监控和管理流量所需的网络路径。这使企业管理员能够完全控制操作边界，同时将管理数据保留在环境内部。

- "在 vCenter 中使用 OVA 安装 NetApp Console 本地部署"。
- "维护您的 vCenter 或 ESXi 主机以进行 NetApp Console 本地部署"。
- "了解 NetApp Console 本地部署中本地控制台代理的端口"。

通过 **API** 和服务帐户自动执行存储操作

NetApp Console 本地部署支持基于 API 的集成，因此您的组织可以自动执行可重复的存储操作。服务帐户允许应用程序使用分配的角色进行身份验证和操作。适用于交互式用户的基于角色的访问控制和审核控制管理这些操作。这支持企业自动化，同时保持访问范围和责任。

- "将成员添加到 NetApp Console 本地部署组织"。
- "了解用于 NetApp Console IAM 的 API"

使用 **RBAC** 和 **Active Directory** 集成控制访问

NetApp Console 本地部署提供基于零信任的角色访问控制 (RBAC)，限制用户在其管理的机群和资源中可查看和执行的操作。您可以与 Active Directory 集成，以便用户使用其现有的企业凭据登录，本地用户还可以添加多因素身份验证 (MFA) 以实现额外的验证层。访问治理与组织更广泛的身份和访问管理实践保持一致。

- "了解 NetApp Console 本地部署中的身份和访问管理"。
- "了解如何安全访问 NetApp Console 本地部署"。

组织机群并委派存储管理

NetApp Console 本地部署通过将资源组织到文件夹和机群中来扩展管理。您可以将机群映射到环境、业务部门或区域，然后在组织、文件夹或机群范围内委派管理，以保持所有权清晰。这种结构有助于大型存储团队在不影响策略一致性或治理的情况下分配工作。

- "了解 NetApp Console 本地部署中的文件夹和机群"。
- "了解 NetApp Console 本地部署中的存储机群"。

跟踪和导出管理活动以实现合规性

每次管理操作都会生成审计记录。安全和合规团队可以使用这些记录来调查事件、显示控制有效性并满足审计要求。通过 Webhook 将审核日志导出到您的 syslog 服务器，以实现集中监控、更长时间的保留和分析。由于 NetApp Console 本地部署在您自己的环境中运行，因此日志数据永远不会离开您的基础架构。

- "审核 NetApp Console 本地部署活动"。

根据存储类策略一致地调配存储

NetApp Console 本地部署通过存储类（将性能、容量和分层策略捆绑到可重用定义中的模板）强制实施一致的存储行为。管理员定义一次存储标准。管理员和自动化工作流将那些已批准的类用于整个环境中的所有配置活动。这可以防止配置漂移，减少初级管理员在配置决策上花费的时间，并确保每个工作负载立即符合组织的标准。配置完成后，Console 本地部署将继续监控每个工作负载的合规性。

- "了解如何使用 NetApp Console 本地部署管理存储"。

监控存储类合规性并自动补救漂移

NetApp Console 本地部署根据用于配置每个工作负载的存储类对其进行监控。当工作负载因直接集群配置更改或性能降低而发生漂移时，NetApp Console 本地部署会立即标记违规。管理员可以遵循引导式修复步骤或配置自动修复，以解决常见的漂移情况，而无需手动干预。这种持续执行降低了审计风险，并使您的环境在计划审核之间保持合规。

监控存储运行状况并接收跨机群的警报

NetApp Console 本地部署为您提供一个统一位置，用于监控所管理的每个集群的运行状况和性能。全集群控制面板显示需要关注的集群和卷。自定义控制面板允许管理员构建与其职责相匹配的监控视图。Workload Analyzer 将延迟、吞吐量、资源利用率和配置更改随时间进行关联，帮助您在问题影响工作负载之前确定根本原因。

配置电子邮件和 Webhook 交付渠道，以便在条件发生变化时向正确的团队发送警报。组织管理员设置目标，存储管理员在警报规则中应用目标，以便响应路径与您的运营模型相匹配。这有助于企业团队更快地响应容量、性能和保护事件。

- "了解如何在 NetApp Console 本地部署中监控存储运行状况"。
- "在 NetApp Console 本地部署中设置通知传递渠道"。
- "在 NetApp Console 本地部署中配置警报的通知规则"。

使用自然语言配置存储并调查警报

NetApp Console 本地部署可以连接到您自己的大型语言模型 (LLM)，以提供 AI 辅助的存储管理。您可以用简单的语言描述工作负载以获取配置计划，要求 Console 调查活动警报，或获取有关存储环境的上下文答案。每个 AI 操作都会保持在您的存储类以及适用于您的帐户的基于角色的访问控制范围内，您必须确认敏感操作，然后才能继续。Console 本地部署仅向管理员配置的 LLM 端点发送请求。

- "了解 LLM 在 NetApp Console 本地部署中的集成"。

使用 **NetApp Backup and Recovery** 备份和还原存储

除了配置和监控之外，NetApp Console 本地部署还允许您访问 NetApp Backup and Recovery，以便您可以从同一界面保护数据。您可以备份和还原数据，以满足您的保护和恢复要求。将数据保护与存储管理结合在一起，可以保持治理的一致性，并减少团队运营所需的工具数量。

- "了解 NetApp Console 本地部署中的数据服务"。

了解 **NetApp Console** 本地部署身份和访问管理

NetApp Console 本地部署中的身份和访问管理 (IAM) 可控制谁可以登录、如何验证身份、

用户可以访问哪些资源以及他们可以执行哪些操作。在 NetApp Console 本地部署中，IAM 包括基于角色的访问控制 (RBAC)、多因素身份验证 (MFA) 和目录支持的身份验证，以及支持委派管理的层次结构和审计模型。

使用此页面可以从高层次了解 NetApp Console 本地部署 IAM 模型。有关详细的层次结构规划示例，"了解 NetApp Console 本地部署中的文件夹和机群"。

您必须具有 *Super admin*、*Organization admin* 或 *Folder or fleet admin* 角色才能管理 NetApp Console 中的 IAM。

IAM 在 **NetApp Console** 本地部署中的含义

NetApp Console 本地部署 IAM 结合了身份验证、访问控制、委派和可审核性：

- *Authentication* 决定用户登录的方式，无论是使用本地凭据还是通过目录配置。
- *Authorization* 根据预定义的角色和您分配它们的范围，确定成员在登录后可以执行的操作。
- *Hierarchy and scoping* 确定成员可以访问的文件夹、队列和资源。
- _成员和凭据管理_确定如何添加用户、服务帐户以及如何管理 MFA 和服务帐户机密。
- *Audit and compliance tracking* 记录与 IAM 相关的活动，以便您可以查看谁更改了访问权限以及何时更改。

身份验证的工作原理

NetApp Console 本地部署支持本地身份和外部身份集成。

您可以将 NetApp Console 本地部署与 Active Directory 集成，以便用户使用其现有的公司凭据登录。这消除了在 Console 本地部署中使用单独密码的需要，并允许管理员在分配访问权限时查找目录用户。

对于本地用户，MFA 添加了另一个验证步骤，以降低凭据泄露时未经授权访问的风险。

要详细了解身份验证和安全登录选项，"了解 NetApp Console 本地部署中的安全访问"。

授权的工作原理

用户登录后，NetApp Console 本地部署使用 RBAC 来确定该用户可以查看的内容和执行的操作。

Active Directory 或 LDAP 集成处理身份验证。NetApp Console 本地部署授权保持独立：管理员在组织、文件夹或机群级别分配预定义角色，以控制每个成员可以访问的内容。

同一角色授予不同的有效访问权限，具体取决于您分配该角色的范围。此模型允许您向中央管理员授予广泛的访问权限，同时将区域或团队级别的管理员限制在其管理的机群范围内。

您在组织或文件夹级别分配的角色由子作用域继承。此继承模型是 NetApp Console 如何跨文件夹和队列委派访问权限的关键部分。

NetApp 按照最小权限原则设计 NetApp Console 本地部署角色，以便每个角色仅包含其任务所需的权限。

"了解 NetApp Console 本地部署中基于角色的访问控制和角色继承"。

IAM层次结构的工作原理

NetApp Console 本地部署使用层次结构对资源进行分组并限定访问范围。组织位于顶层，其次是文件夹，然后是队列，最后是与这些队列关联的资源（包括可能的子文件夹）。

这种层次结构使委派成为可能。例如，组织管理员可以管理整个组织的访问权限，而 Folder 或 fleet 管理员只能管理其所拥有的层次结构部分中的资源和成员。

NetApp Console IAM 基于三种类型的组件：定义层次结构的组织组件、在该层次结构中分配的资源以及控制谁可以访问什么的成员和角色。

由于角色通过此层次结构继承，因此您的文件夹和队列设计直接影响每个访问分配的适用范围。

"了解如何为贵组织添加队列。"。

成员安全性和凭据

NetApp Console 本地部署中的 IAM 还包括用于在账户存在后确保成员访问安全的操作控制。

对于本地用户，管理员可以通过指导密码重置、删除或暂时禁用 MFA 以及查看本地用户 MFA 行为来帮助用户恢复访问权限。对于服务帐户，管理员可以在机密丢失或轮换时重新创建凭据。

这些控件是 IAM 的一部分，因为它们决定了身份如何随时间保持安全，而不仅仅是最初分配访问权限的方式。

"了解如何管理成员安全"。

审核 **IAM** 活动

NetApp Console 本地部署中的 IAM 包括审查和导出与访问相关活动的能力。

从"审核"页面，您可以查看与管理组织相关的操作，例如添加成员、创建队列以及关联资源。您还可以按 Tenancy 服务筛选审核记录，以专注于与 IAM 相关的更改，或将审核日志导出到外部系统。

可审计性是一项重要的 IAM 原则，因为它允许您验证谁更改了访问权限、何时发生更改以及更改是否成功。

"了解如何审核 NetApp Console 本地部署活动"。

在 **NetApp Console** 中使用 **IAM** 的后续步骤

- "开始在 NetApp Console 中使用身份和访问权限"
- "了解 NetApp Console 本地部署中的安全访问"
- "了解 NetApp Console 本地部署中的 RBAC"
- "监控或审核 Console 本地部署活动"
- "了解用于 NetApp Console IAM 的 API"

了解 **NetApp Console** 本地部署中的机群管理

NetApp Console 本地部署中的群组管理是将存储系统组织成逻辑组的做法，以便您可以在相关集群中应用一致的策略、控制访问并监控运行状况。群组管理无需单独管理每个集群

，而是让您将整个群组视为支持数据存储目标的公共资源池。

随着存储环境的增长，管理单个集群变得不切实际。Fleet management 通过为您提供一种结构化的方式来对相关系统进行分组、委派职责，并确保每个集群按照相同的标准运行，从而解决了这一问题。

为何需要进行机群管理

车队管理解决了三大核心挑战：

- 通过抽象化简化 - Fleet management 将管理单个存储基础架构的复杂性抽象化。您无需逐个集群进行配置，而是将整个存储资产作为统一整体进行管理，从而降低运营开销并减少决策疲劳。
- 一致性和可扩展性 - 如果没有明确的组织结构，不同的团队会对相似的工作负载做出不同的决策，从而导致配置分散。Fleet management 让您可以同时在数十个系统中应用标准，确保新工作负载在各团队和 Fleet 中从相同的基线开始。
- 治理和控制 - 随着团队的成长，需要明确界定谁可以管理什么。Fleet management 通过组织结构和访问控制提供这些边界，确保存储决策始终受到管理且可审计。

队列如何组织您的资源

您组织的资源层次结构由文件夹和队列组成：

有关层次结构和访问模型的详细概述，请参见 "了解 NetApp Console 本地部署中的文件夹和机群"。

- 组织 - 代表贵公司的顶层。
- **Folders** - 帮助您组织相关的 fleet。例如，您可以为每个地区或业务部门创建一个文件夹，然后在每个文件夹中创建 fleet。文件夹可以包含其他文件夹或 fleet。当您在文件夹级别分配角色时，成员将继承该文件夹内所有 fleet 的相应角色。
- **Fleets** - 将您管理的存储系统分组在一起。您将存储系统与 Fleets 关联，并将成员分配给 Fleets 以授予其访问权限。

文件夹是一种组织工具，对于不具备 Organization admin、Folder admin 或 Fleet admin 角色等 IAM 权限的的成员不可见。成员访问的是 Fleet，而不是文件夹。

常见机群组织模式

如何组织队列取决于您的运营模式：

- 按环境 - 为生产、开发和测试工作负载创建单独的队列。这样可以使生产存储受到更严格的策略约束，同时在较低级别的环境中保持更大的灵活性。
- 按业务部门 - 将服务于特定部门（如财务、工程或人力资源）的集群分组为专用队列。然后，您可以将存储管理职责分配给该业务部门内的团队成员，而无需向他们公开其他队列。
- 按位置或数据中心 - 当集群分布在各个站点时，按位置组织可以监控站点级别的运行状况、应用特定于区域的策略，并跟踪每个站点的容量消耗。
- 按应用程序层 - 对托管特定工作负载类别（例如数据库、文件共享或虚拟机）的集群进行分组，以便在整个集群组中应用针对该工作负载类型调整的一致标准。

使用文件夹添加另一个级别的组织。例如，为每个区域创建一个文件夹，然后在每个区域文件夹内创建基于环境的舰队。

车队管理如何实现访问控制

车队和文件夹作为用户访问和管理职责的边界：

- 文件夹级别的访问权限 - 当您在文件夹级别分配角色时，成员将继承该文件夹中所有队列和资源的相应角色。这样，您可以委派管理职责，而无需授予对整个组织的访问权限。
- **Fleet** 级别访问 - 当您在 Fleet 级别分配角色时，成员只能访问该 Fleet 内的存储系统。这使您可以将存储管理委托给团队成员或应用程序所有者，而不会暴露基础架构中不相关的部分。

Console 本地部署提供集群组级运行状况和性能监控，让您可以从单一视图查看集群组中所有集群的状态，尽早识别问题，并在影响工作负载之前采取行动。

存储管理的工作原理

存储管理是定义存储标准、一致地应用这些标准以及操作工作负载以使其长期保持一致的实践。在 Console 本地部署中，这些标准以存储类策略和存储类的形式表示，范围限定于机群，并通过由 RBAC 和审计日志管理的置备工作流加以实施。

控制台本地部署将四个概念连接到一个工作流中：

- **Fleets** 定义您管理存储的范围。Fleet 对系统进行分组，以便您可以控制访问权限、一致地应用标准并作为一个整体管理资源。
- *存储类策略*将标准定义为可重用的构建模块（性能、容量、安全性、数据保护）。
- *存储类*表达了工作负载意图。存储类是由一个或多个策略组合而成的命名模板。
- *配置工作流程*在护栏内创建存储。不同的工作流做出不同的配置决策，但所有工作流都可以强制执行存储类，并保持由 RBAC 和审计日志管理。

配置方法

控制台本地部署支持三种配置方法，均由 RBAC、审核日志记录和存储类标准管理：

- 手动配置 - 您可以选择目标系统并直接指定配置详细信息。当您需要对系统选择和配置进行明确控制时，请使用此选项。
- 自动配置 - 您提供工作负载输入，并可选择存储类。Console 本地部署建议最佳放置方案，并应用类驱动设置以减少手动决策。
- **AI** 辅助（代理）配置 - 您用自然语言描述所需内容。Console 本地部署提出一个受 RBAC 和存储类约束的计划，然后仅在您审核并批准后进行配置。

后续步骤

- 要了解存储标准，请参见 "了解 NetApp Console 本地部署中的存储类和策略"。
- 要创建和管理队列，请参见 "管理文件夹和队列"。
- "手动预配存储"
- "自动配置存储"
- "在 AI 辅助下配置存储"

了解 NetApp Console 本地部署中的存储类和策略

存储类是定义存储行为方式的可重用模板。使用存储类调配存储时，NetApp Console 本地部署会自动强制执行该类中编码的标准，而无需管理员为每个工作负载单独做出配置决策。

存储类是根据存储类策略构建的，这些策略定义了存储行为的各个维度。它们共同使您能够一次性捕获组织的存储标准，并将其一致地应用于各个集群。

什么是存储类策略

存储类策略定义了存储行为的一个维度。策略是可重用的构建基块，可将其组合以创建存储类。

常见的策略类型包括：

- 性能策略 - 定义延迟目标、IOPS 或吞吐量要求。
- 容量策略 - 定义调配模式、阈值警报或增长限制。
- 安全策略 - 定义加密、合规或访问控制要求。
- 数据保护策略 - 定义快照计划、复制目标或保留期。

您可以独立定义策略，然后在构建存储类时组合它们。这使您可以在多个类中重用相同的性能策略，或在一个地方更新容量策略，并将该更改应用于使用该策略的每个类。

什么是存储类

存储类是由一个或多个策略组合而成的命名模板。它体现了组织针对特定类型工作负载的存储标准。

例如，您可以创建一个结合了高性能、高可用性和严格数据保护策略的 **Production Database** 存储类，或者创建一个结合了中等性能、灵活容量和基本数据保护策略的 **Development File Share** 存储类。

存储管理员定义存储类以编码企业要求。所有配置活动，无论是手动完成的、通过引导的工作流完成的，还是通过自动化完成的，都来自管理员已批准的类库。

存储类如何强制执行标准

配置存储时，您需要选择一个存储类，而不是配置单个设置。Console 本地部署使用该类中的策略来确定您的集群中哪些集群具有支持工作负载的容量和性能余量，推荐最佳放置选项，并在配置时自动应用类驱动的设置。

配置完成后，Console 本地部署会根据其存储类标准持续评估每个工作负载。

存储等级漂移和合规性

当工作负载不再与其存储类意图匹配时，NetApp Console 本地部署会标记该工作负载以进行调查和修正。

问题分为两类：

- 配置漂移：受存储类策略管理的存储设置不再与预期配置匹配。当直接在 ONTAP 集群上进行更改或在标准配置工作流之外进行更改时，可能会发生这种情况。
- 性能不合规：工作负载的运行时行为不再符合存储类性能意图（例如，接近 QoS 限制的持续压力或尾部延迟升高）。

分析视图解释了更改的内容及其原因。引导式修正操作（例如，修复它）可能有助于恢复合规性。某些修正措施可以就地应用，而其他修正措施可能需要将工作负载调整到不同的存储类以恢复预期的行为。

调查位置

您通常可以从以下位置之一调查偏差和不合规情况（可用性取决于您的部署和权限）：

- 存储类： 漂移/合规性
- *警报：*分析

有关分步说明，请参见 补救存储类漂移。

端到端工作流

以下步骤描述了如何使用存储类来标准化和管理环境中的存储：

1. 创建存储类策略 - 策略定义存储行为的各个维度（性能目标、容量设置、安全要求、数据保护计划）。在创建存储类之前，请先创建策略。
2. **Create a storage class** - 通过组合每个适用类别的一个策略来组装存储类。您可以使用预定义的存储类或为组织的标准创建自定义存储类。
3. 将存储类与群组关联 - 创建存储类后，将其与将用于配置和合规性监控的群组关联。
4. 使用存储类调配存储 - 调配卷或 LUN 时，请选择存储类，而不是配置单个设置。Console 本地部署使用类来推荐最适合的集群放置，然后使用类中定义的设置进行调配。
5. 监控工作负载的漂移 - Console 本地部署根据其存储类中编码的标准持续评估每个工作负载。如果发生配置偏移或性能不合规，则会标记问题并可能引发警报。
6. 修正漂移以恢复合规性 - 当检测到漂移或性能不合规时，您可以按照指导步骤手动纠正问题，让 Console 本地部署自动解决常见的漂移条件，或者在需要更改其设置时将工作负载与其存储类解除关联。

存储类如何与队列配合使用

存储类与队列相关联。当您将存储类与队列关联时，该类将可用于队列内的所有配置。这可确保在队列中配置的每个工作负载都遵循相同的标准，使队列成为跨相关集群实施一致存储行为的主要方式。

有关如何组织车队的详细信息，请参见 "了解 NetApp Console 本地部署中的机群管理"。

后续步骤

- 要了解车队组织，请参见 "了解 NetApp Console 本地部署中的机群管理"。
- 要创建策略和存储类，请参见 "管理存储类和策略"。
- "手动预配存储"
- "自动配置存储"
- "在 AI 辅助下配置存储"
- 要分析和修复漂移，请参见 "补救存储类漂移"

了解 **LLM** 在 **NetApp Console** 本地部署中的集成

NetApp Console 本地部署连接到大型语言模型 (LLM)，用于 AI 辅助存储管理。设置完成后，用户可以使用自然语言配置存储、调查警报并获取存储指导。

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。

AI 辅助管理让用户能够以简单语言描述请求，同时 Console 本地部署应用您的存储策略。

控制台本地部署仅向您配置的端点发送 LLM 请求。

您可以使用 **AI** 辅助存储管理做什么

当您启用 LLM 集成时，Console 本地部署通过 Console 助手提供三种功能：

- **Storage provisioning** 以通俗易懂的语言描述工作负载要求。Console 本地部署根据您的存储类推荐并运行配置计划。
- **Alert response** 要求 Console 本地部署调查活动警报。它会分析问题，并根据分配的权限建议或运行操作。
- 搜索和指导 询问有关您的存储环境或 ONTAP 管理的问题。Console 本地部署从文档和当前集群状态返回上下文答案。

为 **Console assistant** 选择只读或读/写访问权限

用户根据他们想要的结果选择助手访问模式：

- 用于指导和调查的*只读*模式，无需进行基础架构更改。
- 用于引导执行的*读/写*模式。控制台本地部署显示建议的操作，请求确认，然后运行更改。

了解控制台助理操作的控制因素

Console 本地部署通过平台上使用的相同治理模型控制 Console 助手操作：

- 基于角色的访问控制限制了每个用户可以查看和操作的内容。
- 存储策略限制配置和相关操作。
- Console 助理在运行存储更改操作之前需要确认。

选择 **LLM** 提供商路径

NetApp Console 本地部署支持以下 LLM 提供程序类型：

- **OpenAI** 用于直接访问 OpenAI 模型。
- **OpenAI-compatible** 适用于兼容的端点，例如企业网关或代理服务。
- Anthropic 的 Claude 模型。

模型可用性取决于您配置的端点。在 Console 本地部署的列表中选择一个模型。

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"。

了解 **LLM** 请求的去向

数据流取决于您选择的端点路径：

- 如果配置 OpenAI 端点，Console 本地部署会将提示和上下文发送到 OpenAI 端点。
- 如果配置与 OpenAI 兼容的终结点，则 Console 本地部署会将提示和上下文发送到组织配置的兼容终结点。

保护 **LLM** 凭据并控制管理员访问

保护与这些控件的集成：

- 将 API 密钥视为特权凭据，并根据组织策略进行轮换。
- 查看提供商端的使用情况和警报，以检测意外活动。

连接 **LLM**

做出这些决定后，请继续"连接您的 LLM 并启用 NetApp Console 助理"。

如果连接或运行时检查失败，请参见 "对 LLM 集成进行故障排除"。

了解 NetApp Console 本地部署中的 NetApp Backup and Recovery

NetApp Backup and Recovery 是一种数据服务，可为所有 ONTAP 工作负载（包括卷、数据库、虚拟机和 Kubernetes 工作负载）提供高效、安全且经济高效的数据保护。

工作负载是系统内资源的逻辑分组，作为一个单位管理，用于保护、治理、检测和恢复。在 Backup and Recovery 中，工作负载是您保护的单位。其含义取决于数据源：对于 Kubernetes，工作负载是一个应用程序，对于 VM 环境，它是一个虚拟机，对于数据库环境，它是一个数据库。

所有 ONTAP 系统都内置了对备份和恢复的支持，因此无需额外的硬件或媒体网关。这使得备份操作简单且具有成本效益。NetApp Console 简化了任何备份策略的实施，包括全方位的 3-2-1 备份变体，而无需多个资源管理员或专业人员。

NetApp Backup and Recovery 处于 NetApp Console 本地部署的预览模式。该服务尚未全面推出，特性和功能可能会发生变化。

"详细了解 NetApp Backup and Recovery。"。

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

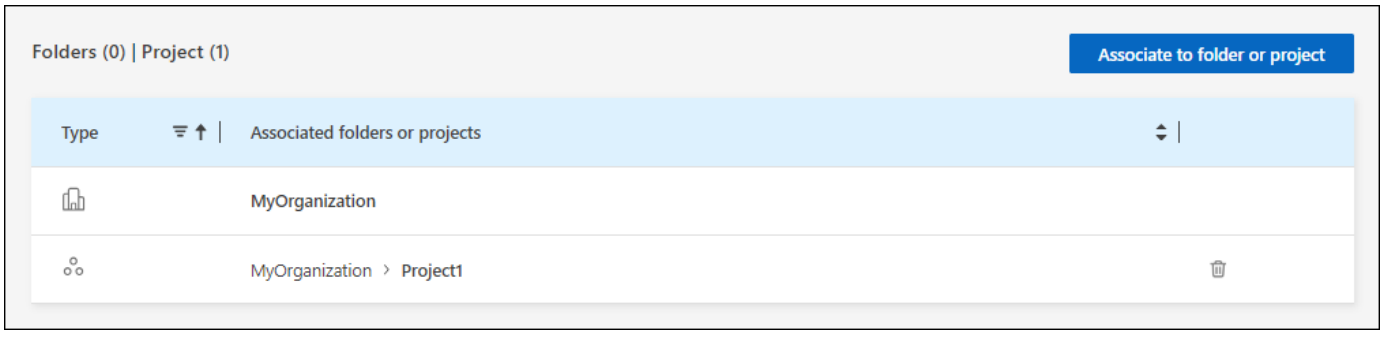
验证资源与哪些队列或文件夹关联。

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。

平台角色	职责
"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。
"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
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
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
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

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
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

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
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
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

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
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。"

使用 NetApp Console

登录 NetApp Console 本地部署

在组织管理员邀请您加入 NetApp Console 本地部署组织用户帐户后，您可以登录 Console 本地部署。要登录，请使用与您的登录关联的电子邮件地址。

如果您已登录但未看到任何资源，请联系您的组织管理员。"请联系您的组织管理员"。

步骤

1. 打开 Web 浏览器，转到安装 Console 本地部署的 IP 地址。
2. 在*登录*页面上，输入与您的登录相关联的电子邮件地址。
3. 系统会提示您输入凭据，具体取决于与您的登录相关的身份验证方法。

   - 使用您的电子邮件地址和密码的 NetApp Console 帐户

   - 如果启用了 MFA：输入密码后，系统会提示您输入 TOTP 代码（来自您的身份验证器应用程序）或使用恢复代码。
   - 如果使用恢复代码登录，请在恢复代码提示期间按 UI 中显示的顺序使用它们。

   +

   - 使用您的电子邮件地址和密码的 Active Directory 帐户

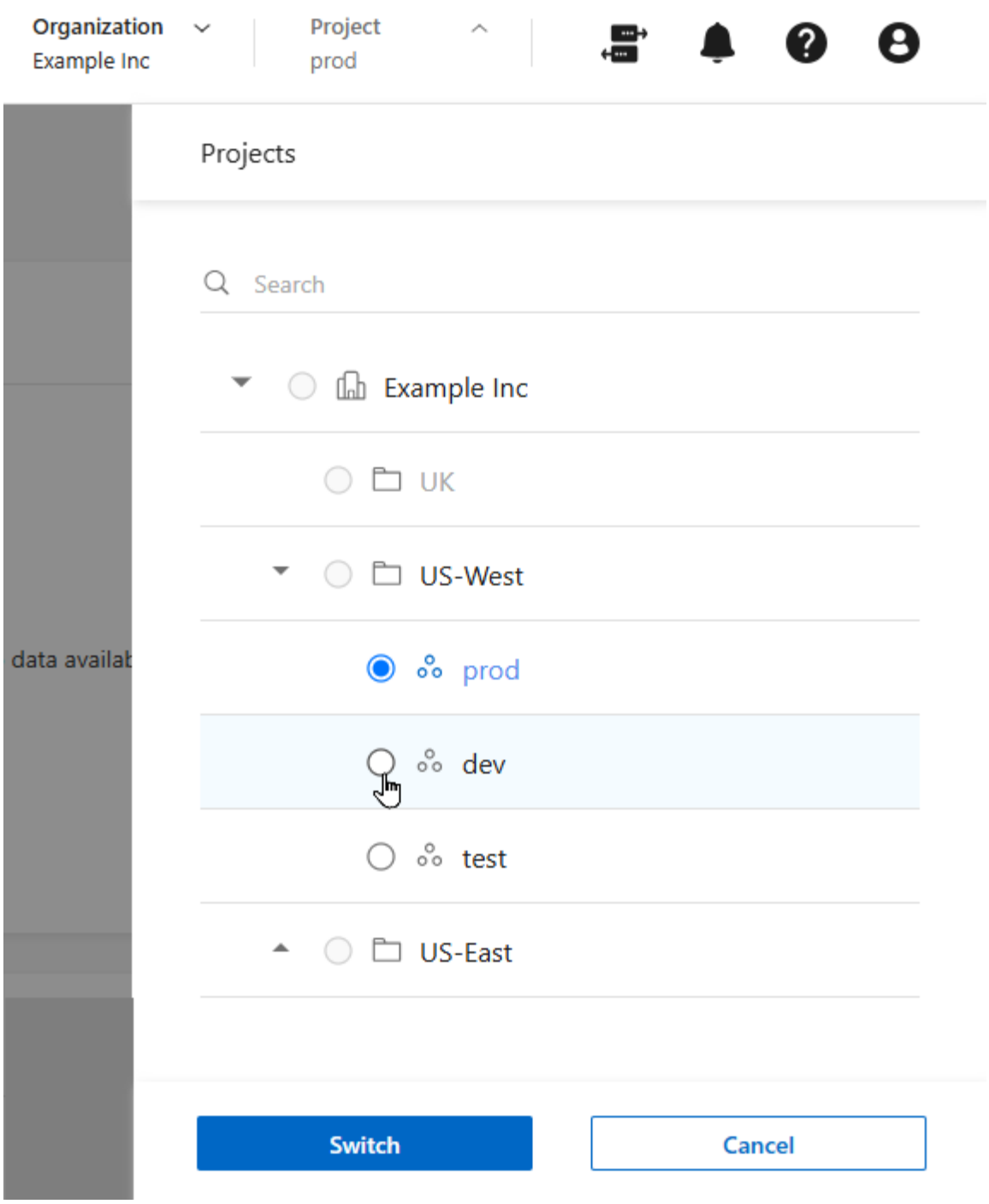
在 NetApp Console 本地部署中切换车队

在 NetApp Console 本地部署中，如果您有权访问多个集群，则可以随时在它们之间进行切换。

查看任何*身份和访问权限*页面时，您无法切换到其他机群。

步骤

1. 在 Console 本地部署的顶部标题中，选择 **Scope**。
2. 浏览组织中的机群，选择所需的机群，然后选择 **Switch**。



管理 NetApp Console 本地部署用户设置

在 NetApp Console 本地部署中，您可以修改 Console 本地部署配置文件，包括更改密码、启用多因素身份验证 (MFA) 以及查看控制台管理员是谁。

更改您的显示名称

您可以更改 Console 本地部署显示名称，该名称会将您标识给其他用户。您无法更改用户名或电子邮件地址。

步骤

1. 选择 Console 本地部署右上角的配置文件图标，以查看用户设置面板。
2. 选择姓名旁边的*编辑*图标。
3. 在 **Name** 字段中输入新的显示名称。

配置多因素身份验证

配置多因素身份验证 (MFA)，以便在登录 NetAppConsole 本地部署时通过要求第二种验证方法来提高安全性。

通过 NetApp 支持站点登录的用户无法启用 MFA。如果您属于这种情况，则在个人资料设置中将看不到启用 MFA 的选项。

如果您的用户帐户用于 API 访问，请勿启用 MFA。为用户帐户启用多重身份验证后，将停止 API 访问。使用服务帐户进行所有 API 访问。

如果您的帐户使用 Active Directory 或其他集成目录服务进行身份验证，则无法通过控制台本地部署为您的帐户配置 MFA。

开始之前

- 您必须已将身份验证应用（例如 Google Authenticator 或 Microsoft Authenticator）下载到您的设备。
- 您需要密码才能设置多重身份验证。

如果无法访问身份验证应用或丢失恢复代码，请与控制台管理员联系以获取帮助。

步骤

1. 选择 Console 右上角的配置文件图标，查看用户设置面板。
2. 选择*多重身份验证*标题旁边的*配置*。
3. 按照提示为您的账号设置 MFA。
4. 完成后，系统会提示您保存恢复代码。选择复制代码或下载包含代码的文本文件。请将这些代码保存在安全的地方。如果您失去对身份验证应用程序的访问权限，则需要恢复代码。

   如果需要使用恢复代码登录，请在恢复代码提示期间按 UI 中显示的顺序使用它们。

   设置 MFA 后，每次登录时，Console 本地部署都会提示您从身份验证应用中输入一次性代码。

重新生成您的 **MFA** 恢复代码

您只能使用一次恢复代码。如果您丢失了，请创建一个新的。

步骤

1. 选择 Console 本地部署右上角的配置文件图标，以查看用户设置面板。
2. 选择*多因素身份验证*标题旁边的 ••• 。
3. 选择*重新生成恢复代码*。
4. 复制生成的恢复代码并将其保存在安全的位置。

删除您的 **MFA** 配置

删除 MFA 会移除下次登录时的第二个验证步骤。若要再次使用 MFA，必须从用户设置中重新配置。

如果无法访问身份验证应用或恢复代码，则需要联系组织管理员以重置 MFA 配置。

步骤

1. 选择 Console 本地部署右上角的配置文件图标，以查看用户设置面板。
2. 选择*多因素身份验证*标题旁边的 ••• 。
3. 选择 **Delete**。

请联系您的组织管理员

如果您需要联系您的组织管理员，可以直接从 Console 向他们发送电子邮件。管理员管理组织内的用户帐户和权限。

要使用*联系管理员*功能，您必须为浏览器配置默认电子邮件应用程序。

步骤

1. 选择 Console 本地部署右上角的配置文件图标，以查看用户设置面板。
2. 选择*Contact admins*以向您的组织管理员发送电子邮件。
3. 选择要使用的电子邮件应用程序。
4. 完成电子邮件并选择*发送*。

配置深色模式（深色主题）

您可以将 Console 本地部署设置为以深色模式显示。

步骤

1. 选择 Console 本地部署右上角的配置文件图标，以查看用户设置面板。
2. 移动*深色主题*滑块以启用它。

在 **NetApp Console** 本地部署中使用 **NetApp Console** 助理

使用 NetApp Console 本地部署中的 NetApp Console 助手来管理存储并通过自然语言获取答案。用简单的语言描述您的需求，NetApp Console 本地部署将在您的存储策略和基于角色的访问权限范围内执行相应操作。

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。

助理的操作受您分配的基于角色的访问权限的限制。"了解访问角色"。

了解您可以使用控制台助理执行的操作

控制台助手是 NetApp Console 本地部署的自然语言界面。提出问题或描述任务，它会返回答案或建议的操作。该助手提供以下功能：

- 调配存储 用通俗易懂的语言描述工作负载。Assistant 会推荐一个存储类和位置，然后在您确认详细信息后创建卷或 LUN。例如，要求其创建具有特定容量的 CIFS 卷。Assistant 标识集群和存储虚拟机 (SVM)，填写所需参数，并预配存储。
- 搜索并获取指导 询问有关存储环境的问题，查找 Console 本地部署功能，并从 NetApp 文档和当前机群状态中获取上下文答案。
- **Investigate alerts** 要求助理查看活动警报。它会分析问题并提出修复建议，或者在您确认的情况下执行补救措施。

助理仅向管理员在 Console 本地部署中配置的 LLM 端点发送请求。它会在执行存储更改操作之前请求确认，所有操作均遵循分配给您帐户的基于角色的访问控制。

确认您可以使用 **Console** 助手

- 组织管理员或超级管理员必须通过将大型语言模型 (LLM) 连接到 Console 本地部署来启用 Console 助理。如果您在仪表板上没有看到 **Console** 助理 按钮，请让您的管理员启用它。有关详细信息，请参见 "连接您的 LLM 并启用 NetApp Console 助理"。
- 确保您具有希望助理执行的操作所需的基于角色的访问控制。

向 **Console** 助理提问或请求操作

打开 Console 助理，选择访问模式，然后输入描述您的请求的提示。

步骤

1. 从 NetApp Console 本地部署仪表板中，选择 **Console assistant** 按钮。
2. 选择访问模式：
   - 选择*只读*即可提出问题并获得指导，无需进行更改。
   - 选择*Read/write*以允许助手对您的存储基础设施进行操作。
3. 输入描述您的问题或任务的提示，然后选择*Send*。

   例如： `Create a 10GiB volume for home directories named home, and share it with Everyone set to FULL_CONTROL.`

4. 请查看该助理的回复：
   - 对于问题，助手会返回一个答案，您可以根据该答案采取行动。
   - 对于操作，助理显示建议的操作，询问缺少的详细信息（如权限级别），然后在继续之前要求确认。
5. 确认操作。对于异步操作，例如卷创建，助手创建作业以完成请求。
6. 要查看请求，请咨询助手。例如，输入 `Let me know when the job completes`，助手将返回当前状态。

管理 NetApp Console 中的存储

了解 NetApp Console 本地部署中的机群管理

NetApp Console 本地部署中的群组管理是将存储系统组织成逻辑组的做法，以便您可以在相关集群中应用一致的策略、控制访问并监控运行状况。群组管理无需单独管理每个集群，而是让您将整个群组视为支持数据存储目标的公共资源池。

随着存储环境的增长，管理单个集群变得不切实际。Fleet management 通过为您提供一种结构化的方式来对相关系统进行分组、委派职责，并确保每个集群按照相同的标准运行，从而解决了这一问题。

为何需要进行机群管理

车队管理解决了三大核心挑战：

- 通过抽象化简化 - Fleet management 将管理单个存储基础架构的复杂性抽象化。您无需逐个集群进行配置，而是将整个存储资产作为统一整体进行管理，从而降低运营开销并减少决策疲劳。
- 一致性和可扩展性 - 如果没有明确的组织结构，不同的团队会对相似的工作负载做出不同的决策，从而导致配置分散。Fleet management 让您可以同时在数十个系统中应用标准，确保新工作负载在各团队和 Fleet 中从相同的基线开始。
- 治理和控制 - 随着团队的成长，需要明确界定谁可以管理什么。Fleet management 通过组织结构和访问控制提供这些边界，确保存储决策始终受到管理且可审计。

队列如何组织您的资源

您组织的资源层次结构由文件夹和队列组成：

有关层次结构和访问模型的详细概述，请参见 "了解 NetApp Console 本地部署中的文件夹和机群"。

- 组织 - 代表贵公司的顶层。
- **Folders** - 帮助您组织相关的 fleet。例如，您可以为每个地区或业务部门创建一个文件夹，然后在每个文件夹中创建 fleet。文件夹可以包含其他文件夹或 fleet。当您在文件夹级别分配角色时，成员将继承该文件夹内所有 fleet 的相应角色。
- **Fleets** - 将您管理的存储系统分组在一起。您将存储系统与 Fleets 关联，并将成员分配给 Fleets 以授予其访问权限。

> ⓘ 文件夹是一种组织工具，对于不具备 Organization admin、Folder admin 或 Fleet admin 角色等 IAM 权限的的成员不可见。成员访问的是 Fleet，而不是文件夹。

常见机群组织模式

如何组织队列取决于您的运营模式：

- 按环境 - 为生产、开发和测试工作负载创建单独的队列。这样可以使生产存储受到更严格的策略约束，同时在较低级别的环境中保持更大的灵活性。
- 按业务部门 - 将服务于特定部门（如财务、工程或人力资源）的集群分组为专用队列。然后，您可以将存储管理职责分配给该业务部门内的团队成员，而无需向他们公开其他队列。

- 按位置或数据中心 - 当集群分布在各个站点时，按位置组织可以监控站点级别的运行状况、应用特定于区域的策略，并跟踪每个站点的容量消耗。
- 按应用程序层 - 对托管特定工作负载类别（例如数据库、文件共享或虚拟机）的集群进行分组，以便在整个集群组中应用针对该工作负载类型调整的一致标准。

使用文件夹添加另一个级别的组织。例如，为每个区域创建一个文件夹，然后在每个区域文件夹内创建基于环境的舰队。

车队管理如何实现访问控制

车队和文件夹作为用户访问和管理职责的边界：

- 文件夹级别的访问权限 - 当您在文件夹级别分配角色时，成员将继承该文件夹中所有队列和资源的相应角色。这样，您可以委派管理职责，而无需授予对整个组织的访问权限。
- **Fleet** 级别访问 - 当您在 Fleet 级别分配角色时，成员只能访问该 Fleet 内的存储系统。这使您可以将存储管理委托给团队成员或应用程序所有者，而不会暴露基础架构中不相关的部分。

Console 本地部署提供集群组级运行状况和性能监控，让您可以从单一视图查看集群组中所有集群的状态，尽早识别问题，并在影响工作负载之前采取行动。

存储管理的工作原理

存储管理是定义存储标准、一致地应用这些标准以及操作工作负载以使其长期保持一致的实践。在 Console 本地部署中，这些标准以存储类策略和存储类的形式表示，范围限定于机群，并通过由 RBAC 和审计日志管理的置备工作流加以实施。

控制台本地部署将四个概念连接到一个工作流中：

- **Fleets** 定义您管理存储的范围。Fleet 对系统进行分组，以便您可以控制访问权限、一致地应用标准并作为一个整体管理资源。
- *存储类策略*将标准定义为可重用的构建模块（性能、容量、安全性、数据保护）。
- *存储类*表达了工作负载意图。存储类是由一个或多个策略组合而成的命名模板。
- *配置工作流程*在护栏内创建存储。不同的工作流做出不同的配置决策，但所有工作流都可以强制执行存储类，并保持由 RBAC 和审计日志管理。

配置方法

控制台本地部署支持三种配置方法，均由 RBAC、审核日志记录和存储类标准管理：

- 手动配置 - 您可以选择目标系统并直接指定配置详细信息。当您需要对系统选择和配置进行明确控制时，请使用此选项。
- 自动配置 - 您提供工作负载输入，并可选择存储类。Console 本地部署建议最佳放置方案，并应用类驱动设置以减少手动决策。
- **AI** 辅助（代理）配置 - 您用自然语言描述所需内容。Console 本地部署提出一个受 RBAC 和存储类约束的计划，然后仅在您审核并批准后进行配置。

后续步骤

- 要了解存储标准，请参见 "了解 NetApp Console 本地部署中的存储类和策略"。
- 要创建和管理队列，请参见 "管理文件夹和队列"。
- "手动预配存储"
- "自动配置存储"
- "在 AI 辅助下配置存储"

标准化存储行为

了解 **NetApp Console** 本地部署中的存储类和策略

存储类是定义存储行为方式的可重用模板。使用存储类调配存储时，NetApp Console 本地部署会自动强制执行该类中编码的标准，而无需管理员为每个工作负载单独做出配置决策。

存储类是根据存储类策略构建的，这些策略定义了存储行为的各个维度。它们共同使您能够一次性捕获组织的存储标准，并将其一致地应用于各个集群。

什么是存储类策略

存储类策略定义了存储行为的一个维度。策略是可重用的构建基块，可将其组合以创建存储类。

常见的策略类型包括：

- 性能策略 - 定义延迟目标、IOPS 或吞吐量要求。
- 容量策略 - 定义调配模式、阈值警报或增长限制。
- 安全策略 - 定义加密、合规或访问控制要求。
- 数据保护策略 - 定义快照计划、复制目标或保留期。

您可以独立定义策略，然后在构建存储类时组合它们。这使您可以在多个类中重用相同的性能策略，或在一个地方更新容量策略，并将该更改应用于使用该策略的每个类。

什么是存储类

存储类是由一个或多个策略组合而成的命名模板。它体现了组织针对特定类型工作负载的存储标准。

例如，您可以创建一个结合了高性能、高可用性和严格数据保护策略的 **Production Database** 存储类，或者创建一个结合了中等性能、灵活容量和基本数据保护策略的 **Development File Share** 存储类。

存储管理员定义存储类以编码企业要求。所有配置活动，无论是手动完成的、通过引导的工作流完成的，还是通过自动化完成的，都来自管理员已批准的类库。

存储类如何强制执行标准

配置存储时，您需要选择一个存储类，而不是配置单个设置。Console 本地部署使用该类中的策略来确定您的集群中哪些集群具有支持工作负载的容量和性能余量，推荐最佳放置选项，并在配置时自动应用类驱动的设置。

配置完成后，Console 本地部署会根据其存储类标准持续评估每个工作负载。

存储等级漂移和合规性

当工作负载不再与其存储类意图匹配时，NetApp Console 本地部署会标记该工作负载以进行调查和修正。

问题分为两类：

- 配置漂移：受存储类策略管理的存储设置不再与预期配置匹配。当直接在 ONTAP 集群上进行更改或在标准配置工作流之外进行更改时，可能会发生这种情况。
- 性能不合规：工作负载的运行时行为不再符合存储类性能意图（例如，接近 QoS 限制的持续压力或尾部延迟升高）。

分析视图解释了更改的内容及其原因。引导式修正操作（例如，修复它）可能有助于恢复合规性。某些修正措施可以就地应用，而其他修正措施可能需要将工作负载调整到不同的存储类以恢复预期的行为。

调查位置

您通常可以从以下位置之一调查偏差和不合规情况（可用性取决于您的部署和权限）：

- 存储类： 漂移/合规性
- *警报：*分析

有关分步说明，请参见 补救存储类漂移。

端到端工作流

以下步骤描述了如何使用存储类来标准化和管理环境中的存储：

1. 创建存储类策略 - 策略定义存储行为的各个维度（性能目标、容量设置、安全要求、数据保护计划）。在创建存储类之前，请先创建策略。
2. **Create a storage class** - 通过组合每个适用类别的一个策略来组装存储类。您可以使用预定义的存储类或为组织的标准创建自定义存储类。
3. 将存储类与群组关联 - 创建存储类后，将其与将用于配置和合规性监控的群组关联。
4. 使用存储类调配存储 - 调配卷或 LUN 时，请选择存储类，而不是配置单个设置。Console 本地部署使用类来推荐最适合的集群放置，然后使用类中定义的设置进行调配。
5. 监控工作负载的漂移 - Console 本地部署根据其存储类中编码的标准持续评估每个工作负载。如果发生配置偏移或性能不合规，则会标记问题并可能引发警报。
6. 修正漂移以恢复合规性 - 当检测到漂移或性能不合规时，您可以按照指导步骤手动纠正问题，让 Console 本地部署自动解决常见的漂移条件，或者在需要更改其设置时将工作负载与其存储类解除关联。

存储类如何与队列配合使用

存储类与队列相关联。当您将存储类与队列关联时，该类将可用于队列内的所有配置。这可确保在队列中配置的每个工作负载都遵循相同的标准，使队列成为跨相关集群实施一致存储行为的主要方式。

有关如何组织车队的详细信息，请参见 "了解 NetApp Console 本地部署中的机群管理"。

后续步骤

- 要了解车队组织，请参见 "了解 NetApp Console 本地部署中的机群管理"。
- 要创建策略和存储类，请参见 "管理存储类和策略"。
- "手动预配存储"
- "自动配置存储"
- "在 AI 辅助下配置存储"
- 要分析和修复漂移，请参见 "补救存储类漂移"

了解 **NetApp Console** 本地部署中的存储类策略

存储类策略是用于构建存储类的构建基块。每个策略都控制存储行为的特定方面。将策略组合到存储类中时，可以创建一个可重用的模板，NetApp Console 本地部署在配置时自动实施该模板，并在工作负载的整个生命周期中持续监视该模板。

策略作为构建块

存储类由一个或多个策略组成，每个策略管理不同的存储行为维度。存储管理员定义策略以编码企业标准——性能预期、容量阈值、数据放置规则——然后将这些策略组合到存储类模板中。当使用存储类调配工作负载时，它将继承该类中的所有策略。此设计将定义标准的责任与调配行为分开，因此可以通过自动化工作流程一致地调配存储，而无需做出单独的配置决策。

存储类策略类型

NetApp Console 本地部署包括四种类型的策略，可用于构建存储类：

性能策略

性能策略设置工作负载的预期 IOPS/TB、峰值 IOPS/TB、绝对最小 IOPS 和预期延迟目标。Console 本地部署使用这些值在配置时推荐具有足够余量的集群，并在配置后检测 IOPS 或延迟漂移。

容量策略

容量策略控制卷如何消耗和管理空间。它设置空间保留（厚置备、精简置备或系统默认）、自动增长行为、FabricPool 分层以及是否将 NAS 工作负载置备为 FlexVol 或 FlexGroup 卷。

安全策略

安全策略为工作负载设置加密、勒索软件保护和 FIPS 要求。每个属性可以设置为必需值，也可以保留为"any"以接受系统默认值。

数据保护策略

数据保护策略设置在每个时间间隔保留的快照数量，以确保使用该策略的工作负载获得一致的备份计划。

默认策略

Console 本地部署包括跨所有四种策略类型的系统定义策略。您可以在创建存储类时按原样使用这些策略，也可以将其复制作为根据组织要求定制的自定义策略的起点。

性能策略

名称	类型	预期 **IOPS/TB**	峰值 **IOPS/TB**	绝对最小 **IOPS**	预期延迟（毫秒）	摘要
数据库数据的 Extreme	系统定义	12,288	24,576	2,000	1	用于需要持续高 IOPS 和亚毫秒延迟的事务性数据库数据卷。
数据库日志的 Extreme	系统定义	22,528	45,056	4,000	1	用于需要最高 IOPS 基准的数据库事务日志卷，以防止写入瓶颈。
Extreme for Database Shared Data	系统定义	16,384	32,768	2,000	1	用于需要高吞吐量和一致延迟的多个主机访问的共享数据库卷。
至高性能	系统定义	6,144	12,288	1,000	1	用于需要高突发 IOPS 和可预测的低延迟的 HPC、AI/ML 和分析工作负载。
性能	系统定义	2,048	4,096	500	2	适用于需要可靠性能但无极高 IOPS 要求的虚拟化和企业应用程序。
值	系统定义	128	512	75	17	用于对成本敏感的工作负载，如主目录、文件共享和存档。

容量策略

名称	类型	空间预留	自动增长模式	分层策略	卷类型 **(NAS)**	摘要
默认	系统定义	系统默认值	系统默认值	无	系统默认值	用于平台默认容量行为可以接受的一般工作负载。
投入使用	系统定义	系统默认值	增长	无	系统默认值	用于必须自动扩展以防止空间不足故障的生产工作负载。

安全策略

名称	类型	加密	勒索软件防护	**FIPS**	摘要
默认	系统定义	任意	任意	任意	用于平台默认安全行为可接受的工作负载。
反勒索软件	系统定义	任意	on	任意	用于包含需要主动勒索软件保护的敏感或关键业务数据的工作负载。
投入使用	系统定义	启用	任意	任意	用于需要加密以实现合规性的生产工作负载。

数据保护策略

名称	类型	每小时快照	每日快照	每周快照	每月快照	摘要
默认	系统定义	6	2	2	0	用于需要短期恢复点的标准工作负载，而无需长期保留开销。
3 个月-每小时	系统定义	23	6	4	3	用于需要精细化日内恢复点和三个月历史记录保留的受监管或业务关键型工作负载。

查看 **NetApp Console** 本地部署中的预定义存储类策略

NetApp Console 本地部署包括跨所有四种策略类型的系统定义策略。使用此参考信息确定创建或自定义存储类时最适合工作负载要求的策略。

性能策略

至高性能
: 用于需要高突发 IOPS 和可预测的低延迟的 HPC、AI/ML 和分析工作负载。

数据库数据的 **Extreme**
: 用于需要持续高 IOPS 和亚毫秒延迟的事务性数据库数据卷。

数据库日志的 **Extreme**
: 用于需要最高 IOPS 基准的数据库事务日志卷，以防止写入瓶颈。

Extreme for Database Shared Data
: 用于需要高吞吐量和一致延迟的多个主机访问的共享数据库卷。

性能
: 适用于需要可靠性能但无极高 IOPS 要求的虚拟化和企业应用程序。

值
: 用于对成本敏感的工作负载，如主目录、文件共享和存档。

容量策略

自动扩展容量
: 用于必须自动扩展以防止空间不足故障的生产工作负载。

安全策略

静态加密
: 用于需要加密以实现合规性的生产工作负载。

勒索软件防护
: 用于包含需要主动勒索软件保护的敏感或关键业务数据的工作负载。

标准安全

用于平台默认安全行为可接受的工作负载。

数据保护策略

默认

用于需要短期恢复点的标准工作负载，而无需长期保留开销。

3 个月**-**每小时

用于需要精细化全天内恢复点和三个月历史保留的受监管或业务关键型工作负载。

30 天恢复

用于需要短期恢复点的标准工作负载，而无需长期保留开销。

90 天恢复

用于需要精细化全天内恢复点和三个月历史保留的受监管或业务关键型工作负载。

在 **NetApp Console** 本地部署中创建存储类

在 NetApp Console 本地部署中创建存储类，以标准化跨机群配置和管理存储的方式。存储类是一种可重用的模板，它将存储类策略（如性能目标、容量行为、安全要求和数据保护计划）捆绑到单个命名定义中。

当用户（或自动化）使用存储类配置卷或 LUN 时，NetApp Console 本地部署会自动应用该类的策略。配置完成后，Console 本地部署会根据存储类持续监控工作负载以检测偏差，并可指导或自动执行修复操作以恢复合规性。

开始之前

- 请至少发现一个 ONTAP 集群，以便 Console 本地部署具有放置建议的目标。
- 请确保您具有组织管理员角色（或在环境中授予存储类管理权限的角色）。
- 创建（或识别）您计划使用的存储类策略——性能、容量、安全性和数据保护——因为存储类是由策略组合而成的。

创建存储类

您必须具有组织管理员或文件夹或队列管理员角色才能添加存储类。

步骤

1. 选择 **Storage > Management**。
2. 选择 **Storage classes**。
3. 选择 **Add**。
4. 在*基本信息*下，输入以下信息：
   - 存储类名称：输入存储类的唯一名称。
   - 说明：（可选）输入存储类的说明。
   - 推荐的应用程序：（可选）输入存储类的推荐应用程序列表。

5. 在*存储策略*下，选择一个或多个要与存储类关联的策略。
6. 选择 **Add**。

自定义现有存储类

您必须具有组织管理员或文件夹或队列管理员角色才能自定义现有存储类。

步骤

1. 选择 **Storage > Management**。
2. 选择 **Storage classes**。
3. 对于要自定义的存储类，选择 **……**，然后选择*复制*。
4. 在*基本信息*下，根据需要更新以下内容：
   - 存储类名称：输入存储类的唯一名称。
   - 说明：（可选）输入存储类的说明。
   - 推荐的应用程序：（可选）输入存储类的推荐应用程序列表。
5. 在*存储策略*下，选择一个或多个要与存储类关联的策略。
6. 选择 **Add**。

编辑用户定义的存储类

您必须具有组织管理员或文件夹或队列管理员角色才能编辑用户定义的存储类。

步骤

1. 选择 **Storage > Management**。
2. 选择 **Storage classes**。
3. 对于要编辑的存储类，选择 **……**，然后选择 编辑。
4. 在*基本信息*下，根据需要编辑以下内容：
   - 存储类名称：输入存储类的唯一名称。
   - 说明：（可选）输入存储类的说明。
   - 推荐的应用程序：（可选）输入存储类的推荐应用程序列表。
5. 在*存储策略*下，选择一个或多个要与存储类关联的策略。
6. 选择*编辑*。

删除用户定义的存储类

要删除用户定义的存储类，您必须具有组织管理员或文件夹或舰队管理员角色。

步骤

1. 选择 **Storage > Management**。
2. 选择 **Storage classes**。
3. 对于要删除的存储类，选择 **……**，然后选择 **Delete**。

4. 选择 **Delete**。

   请注意，此操作无法撤消。如果删除当前正在使用的存储类，则使用该类设置的任何卷或 LUN 都将继续运行，但不再与已删除的类关联。

在 NetApp Console 本地部署中设置存储

在 NetApp Console 本地部署中预置卷和 LUN，使存储资源可用于您的工作负载。在预置期间，您可以选择存储类以应用预定义的存储策略和组织标准。

必需的访问角色

超级管理员、组织管理员、文件夹或舰队管理员或存储管理员。"了解访问角色"。

预配卷

步骤

1. 选择 **Storage > Management**。
2. 选择 **Fleets**。
3. 选择要预置的机群。
4. 选择 **Add**。
5. 从菜单中，选择 **Volume**。
6. 在*卷详细信息*下：
   a. 输入卷名称。
   b. 输入容量（如果需要，请选择单位）。
   c. （可选）选择要应用存储类策略的存储类。如果不选择，则在没有存储类策略的情况下配置卷。
7. 在*系统详细信息*下：
   a. 从适用于选定车队的符合条件的系统中选择一个系统。
   b. 选择 Storage VM。
8. 在*主机(NAS)详细信息*下，选择主机访问卷的方式：
   a. 通过 NFS 导出（导出策略控制哪些 NFS 主机可以访问卷）
   b. 通过 SMB/CIFS 共享
9. 选择 **Add**。

配置 **LUN**

步骤

1. 选择 **Storage > Management**。
2. 选择 **Fleets**。
3. 选择要预置的机群。
4. 选择 **Add**。

5. 从菜单中，选择 **LUNs**。
6. 在 **LUN** 存储详细信息 下：
   a. 请输入前缀名称。
   b. 输入要使用该前缀创建的 LUN 数。
   c. 输入每个 LUN 的容量（如果需要，请选择单位）。
   d. （可选）选择要应用存储类策略的存储类。如果不选择，则在没有存储类策略的情况下调配 LUN。
7. 在*系统详细信息*下：
   a. 选择一个系统（如果出现提示）。
   b. 选择 Storage VM。
8. 在*主机(SAN)详细信息*下，选择主机访问卷的方式：
   a. 选择主机操作系统（例如，Windows 或 Linux）以设置 LUN 对齐和块大小的建议默认值。
   b. 选择主机映射组以控制哪些启动器可以访问 LUN。
9. 选择 **Add**。

监控存储运行状况

NetApp Console 本地部署中的存储监控

NetApp Console 本地部署可帮助您通过仪表板、警报、深入分析和补救措施监控整个机群的存储，以便在问题影响工作负载之前发现并解决问题。

使用控制面板监控整个机群的运行状况

从仪表板开始，快速查看存储运行状况和性能。使用主页查看一目了然的指标，打开预定义和自定义仪表板的仪表板表格，并在需要更多详细信息时进入警报、调查和修正。

- "在 NetApp Console 本地部署中查看主页指标"
- "在 NetApp Console 本地部署中保持仪表板处于最新状态"
- "了解 NetApp Console 本地部署中的自定义仪表板"

调查性能问题

使用 Workload Analyzer 调查单个卷上的性能问题。它将延迟、吞吐量、IOPS 和配置更改相关联，以便查明根本原因。

- "了解 NetApp Console 本地部署 Workload Analyzer"
- "在 NetApp Console 本地部署中调查卷上的高延迟"
- "调查 NetApp Console 本地部署中卷的高吞吐量需求"
- "了解 NetApp Console 本地部署中的 Workload Analyzer 指标"

配置警报和通知

配置警报策略和通知渠道，以便合适的人员了解需要注意的存储条件。例如，将容量警告发送给存储团队，将保护警报发送给可以对其执行操作的备份管理员。

"在 NetApp Console 本地部署中配置通知和警报策略"。"在 NetApp Console 本地部署中查看存储警报"。

补救问题

当您检测到问题时，请直接从 NetApp Console 本地部署进行修复：

- 自动修正 — NetApp Console 本地部署根据预定义的规则自动应用纠正措施。
- 指导性补救措施 — 遵循分步建议，在完全控制每个操作的情况下解决问题。

使用信息板监控

在 **NetApp Console** 本地部署中查看主页指标

将 NetApp Console 本地部署中的主页面板用作监视存储运行状况和性能的默认起点。它提供了集群运行状况、警报、安全性、容量使用率、延迟、吞吐量和 IOPS 的高级指标。

主页仪表板会自动限定范围，仅显示您有权查看的机群和系统。您还可以将自定义仪表板添加到主页，以进行特定角色的监控。

将卡片用作分层分流工作流程。从 **Fleet health** 和 **Alerts** 开始，查找风险热点。使用 **System health status** 和 **Recommended remediations** 来识别受影响的资源。使用 **Capacity usage**、**Latency**、**Throughput** 和 **IOPS** 来调查根本原因。

集群运行状况

Fleet health 卡显示前五个机群的高级状态摘要，包括系统计数、已用容量、安全合规性和关键警报。使用此卡确定哪些机群需要立即关注。选择机群名称，以查看选定机群的专属仪表板。

建议的补救措施

*推荐补救措施*卡片列出了活动问题和建议措施。该卡片根据容量压力、离线资源和保护相关风险确定补救措施的优先级。

警报

*警报*卡汇总选定时间范围内的警报量，并按严重程度对其进行分组。使用此卡了解当前的事件负载，并发现关键、警告或信息警报的近期变化。

安全性

Security 卡汇总了合规性和保护指标，例如系统合规性和与勒索软件相关的控制措施。使用此视图可监控整个资源的安全趋势。

容量使用情况

*容量使用*卡显示所选机群或系统的预测和历史使用趋势。使用此卡识别增长模式并规划额外容量。

延迟

*延迟*卡跟踪所选系统随时间的响应时间行为。使用此趋势来检测新出现的性能延迟，并比较不同资源的相对延迟。

吞吐量

*吞吐量*卡显示选定系统随时间的数据传输速率。使用此卡可了解工作负载强度并监控吞吐量需求变化。

IOPS

IOPS 卡显示一段时间内的输入/输出操作速率。使用此卡可比较系统之间的活动水平，并确定持续或间歇性的 I/O 需求。

控制面板卡（指标卡示例）

较低的*仪表板*区域可以包含用户选择的自定义仪表板，例如所选生产范围的平均延迟。使用这些卡片按团队、工作负载或目标进行重点监控。

系统运行状况

*系统健康状态*卡片列出了各个系统及其当前健康状态。使用此卡可以快速识别运行异常的系统，并将状态变化与警报和性能信号相关联。

相关信息

- "了解 NetApp Console 本地部署中的自定义仪表板"
- "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"

使用自定义仪表板

了解 **NetApp Console** 本地部署中的自定义仪表板

在 NetApp Console 本地部署中使用自定义仪表板，为特定团队、机群、工作负载和运营目标创建重点监控视图。自定义仪表板通过为广泛、始终可用的监控添加有针对性的可见性，从而对主页仪表板进行补充。

控制面板类型如何协同工作

主页控制面板

用于容量、警报、性能容量、许可证和数据保护状态的即用型监控窗格。视图已预配置并自动更新。"在 NetApp Console 本地部署中查看主页指标"。

自定义信息板

根据预定义卡片生成的特定角色监控视图，包括可选范围、指标、目标资源和时间窗口。

同时使用两者：* 从主页开始进行每日基线监控。* 使用自定义仪表板按团队、机群、工作负载或运营问题进行重点调查。

一次可以将一个自定义控制面板添加到主页。

了解自定义信息板

自定义仪表板是您在网格上排列的已保存卡片集合。每张卡片都基于预定义的卡片模板，其中包含指标和图表类型。添加卡片时，需要配置作用域、目标对象、聚合和时间窗口。

自定义控制面板和卡片仅供您使用。每张卡片仅显示您有权查看的存储资源的数据。

您可以从主页中删除自定义控制面板，并在监控优先级发生变化时添加其他控制面板。

监控重要事项

卡片模板按指标类型组织，因此您可以将控制面板的重点放在特定的运营区域。例如，使用容量卡观察增长速度超过预期的卷，或使用警报卡跟踪繁忙集群上的重复故障：

性能
: 整个集群、系统、SVM、卷和 LUN 的延迟、IOPS、吞吐量、利用率和性能容量。

容量
: 跨机群、系统、SVM、卷、LUN 和本地层的已用容量、可用容量、已用容量百分比和快照容量。

运行状况
: 运行状况状态、降级或关键对象计数、故障磁盘、网络接口错误和热对象。

警报
: 关键警报计数、按严重程度划分的警报、按受影响区域划分的警报、最近的警报以及一段时间内的警报趋势。

有关预定义卡片和指标的完整目录，请参见 "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"。

资源类型

您可以将卡片范围扩展到 ONTAP 存储层次结构的任何级别：舰队、群集、系统（节点）、SVM、卷、LUN 和本地层（聚合）。可用的资源类型取决于您选择的卡片模板。

计划信息板视图

围绕存储管理目标（如工作负载性能分类、容量规划、健康风险检测和警报优先级排序）组织自定义仪表板。

相关信息

- "开始在 NetApp Console 本地部署中使用仪表板"
- "在 NetApp Console 本地部署中查看主页指标"
- "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"

开始在 **NetApp Console** 本地部署中使用仪表板

在 NetApp Console 本地部署中，按照此工作流程从宏观到微观监控视图：查看主页仪表板、查看预定义仪表板、创建自定义仪表板，并保持仪表板为最新状态。

必需的访问角色

所有角色。仪表板仅显示您有权查看的资源。如果在可用资源列表中未看到资源，则表示您没有查看该资源的权限。

在主页上查看基线运行状况

使用主页仪表板查看组织级容量、警报、性能和数据保护状态。

- "在 NetApp Console 本地部署中查看主页指标"
- "了解 NetApp Console 本地部署中的存储监控"

查看其他预定义的仪表板

打开 存储 > 仪表板，查看预定义的仪表板以获取其他特定于角色的视图。

- "在 NetApp Console 本地部署中管理仪表板"

构建用于重点监控的自定义仪表板

当您需要所选资源、指标和时间窗口的目标视图时，请创建自定义仪表板。

- "创建自定义仪表板"
- "在 NetApp Console 本地部署中自定义仪表板卡"

保持信息板的最新状态

通过编辑、复制或删除自定义仪表板，在优先级发生变化时更新仪表板。

- "在 NetApp Console 本地部署中管理仪表板"
- "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"

相关信息

- "了解 NetApp Console 本地部署中的自定义仪表板"
- "在 NetApp Console 本地部署中查看主页指标"

在 **NetApp Console** 本地部署中构建用于监控目标的仪表板

在 NetApp Console 本地部署中创建自定义仪表板，添加卡片，并为日常操作保存监控视图。

如果您只需要可以直接使用的组织级监控，请从预定义的主页仪表板开始。在需要特定于角色的视图、资源级别定位或定制卡片布局时，请创建自定义仪表板。

Console 本地部署仪表板指南

- 只有创建仪表板的用户才能查看它。即使将其添加到控制台主页，也不能与其他用户共享仪表板。
- 您只能查看您有权查看的资源。如果在可用资源列表中未看到资源，则表示您没有查看该资源的权限。

- 在开始之前，请确定您希望仪表板跟踪的指标类型和资源。 "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"

为您的监控目标构建仪表板

当您需要一个地方来监控与您的角色相关的指标时，请创建一个控制面板，例如机群健康状况、性能热点和警报趋势。

步骤

1. 选择 **Storage > Dashboards**。
2. 选择*添加控制面板*。

   控制台本地部署将创建一个具有默认名称且无描述的新仪表板。

3. 选择 **Add Card**。
4. 选择卡片的*资源类型*，例如机群、系统或卷，然后从可用资源列表中选择资源。
5. 选择*下一步*以继续选择指标和卡片类型。
6. 选择要显示的指标。您可以按类型筛选可用指标：指标类型：性能、容量、运行状况*或*警报，或按名称搜索特定指标。可用指标取决于您选择的资源类型。

   "了解可用的指标。"

7. 选择要包含在管理面板中的卡片，然后选择*下一步*。

   一次只能选择一张卡。卡片预览显示所选指标和资源类型的实时数据。

8. 为您的卡片命名。该名称在控制面板中必须是唯一的。
9. 查看卡片预览，输入卡片名称和描述，然后选择*添加*。
10. 对其他卡片重复这些步骤。
11. 选择铅笔图标以编辑仪表板名称和描述，以说明其用途。
12. 选择"添加卡片"按钮右侧的操作菜单，然后选择*保存仪表板*。

    已保存的仪表板可在*存储 > 仪表板*下找到。

13. 也可以从操作菜单中选择 添加至主页，将此控制面板添加至您的主页。控制面板已添加至主页。只有您可以查看您创建的自定义仪表板。不与他人共享。

相关信息

- "在 NetApp Console 本地部署中查看主页指标"
- "了解 NetApp Console 本地部署中的自定义仪表板"
- "在 NetApp Console 本地部署中自定义仪表板卡"
- "在 NetApp Console 本地部署中管理仪表板"

在 **NetApp Console** 本地部署中自定义卡片

在 NetApp Console 本地部署中，当您需要将操作员的关注点集中在最重要的信号上时，请自定义仪表板卡，例如 SLA 风险、容量压力或反复出现的警报噪声。使用本主题可围绕团队需要做出的运营决策来定制仪表板视图。

开始之前

- 创建或打开希望将卡片放置到的控制面板。
- 查看 "了解 NetApp Console 本地部署中的自定义仪表板卡和指标" 中的可用模板和指标。

在优化现有仪表板的同时添加卡片

当您正在优化现有仪表板并需要快速添加回答特定操作问题的卡片时，请使用此选项。

步骤

1. 打开要添加卡片的控制面板。
2. 选择 **Add Card**。
3. 选择卡片的*资源类型*，例如机群、系统或卷，然后从可用资源列表中选择资源。
4. 选择*下一步*以继续选择指标和卡片类型。
5. 选择要显示的指标。您可以按类型筛选可用指标：指标类型：性能、容量、运行状况*或*警报，或按名称搜索特定指标。可用指标取决于您选择的资源类型。

   "了解可用的指标。"

6. 选择要包含在管理面板中的卡片，然后选择*下一步*。

   一次只能选择一张卡。卡片预览显示所选指标和资源类型的实时数据。

7. 为您的卡片命名。该名称在控制面板中必须是唯一的。
8. 查看卡片预览，输入卡片名称和描述，然后选择*添加*。
9. 对其他卡片重复这些步骤。
10. 保存仪表板。

相关信息

- "在 NetApp Console 本地部署中查看主页指标"
- "了解 NetApp Console 本地部署中的自定义仪表板"
- "创建自定义仪表板"
- "管理自定义仪表板"
- "了解 NetApp Console 本地部署中的自定义仪表板卡和指标"

NetApp Console 本地部署中的预定义仪表板和自定义仪表板卡参考

在 NetApp Console 本地部署中，预定义的仪表板和自定义仪表板卡模板为 ONTAP 性

能、容量、运行状况和警报操作提供监控覆盖。

预定义信息板

以下是开箱即用的预定义仪表板。

名称	问题描述
卷	卷性能、容量、QoS、FabricPool、增长率和预测指标。
到满为止的时间	ONTAP 集群、卷和聚合的预计存满时间。
安全性	安全合规性、加密、自主勒索软件保护和身份验证概述。
SVM	ONTAP SVM 性能、容量、卷、LIF、协议（CIFS、FCP、iSCSI、NFS、NVMe/FC）、QoS 和延迟热图监控。
电源	监控节点、磁盘架和聚合的 ONTAP 集群功耗、温度和风扇速度。
节点	ONTAP 节点性能、CPU、网络和后端监控。
网络	网络性能指标包括以太网、FibreChannel、NVMe/FC、链路聚合组和路由。
LUN 数	ONTAP LUN 性能、容量和效率监控。
运行状况	ONTAP 集群运行状况监控包括错误、警告、EMS 警报、HA 问题、节点/磁盘/盘架运行状况、卷、许可证和网络端口。
聚合	ONTAP 聚合容量、效率比和增长率监控。

仪表板级别的时间窗口和聚合

可用的时间窗为 30 分钟、1 小时、24 小时、48 小时、7 天和 30 天。聚合选项因模板而异，包括全队汇总或 top-N 样式结果等视图。时间窗口和聚合在仪表板级别配置，并应用于仪表板中的所有卡片。

仪表板卡片模板和指标

卡片是自定义控制面板的基石。每张卡都使用带有指标和图表类型的预定义模板，然后将该视图映射到特定的 ONTAP 对象和监控目标。

卡片模板是预定义的，不是用户创建的。

存储操作指标索引（一目了然）

指标类型与常见的存储管理结果一致，包括性能瓶颈、容量压力、健康风险和警报量。

指标类型	支持的指标	存储管理员用例	详细模板
性能	平均延迟、峰值延迟、IOPS、吞吐量(MB/s)、利用率、性能容量	识别瓶颈、持续压力和性能余量	转至模板
容量	已用容量、可用容量、已用容量（%）、已用快照容量	跟踪增长、识别低可用容量区域并监控快照影响	转至模板
运行状况	健康状态、降级/关键对象、故障磁盘、网络接口错误、热对象（按延迟）	检测健康退化并确定运营分诊的优先级	转至模板

指标类型	支持的指标	存储管理员用例	详细模板
警报	警报（严重），按严重程度划分的警报，按受影响区域划分的警报，最近的警报，警报趋势	随着时间的推移，监控活动事件和趋势警报量	转至模板

支持的 **ONTAP** 对象层次结构（资源类型）

卡片数据可以在多个 ONTAP 对象级别表示，从集群级别的可见性到对象级别的故障排除。

*资源类型*设置映射到以下一个或多个资源级别：

- 车队
- 集群
- 系统 (节点)
- SVM
- 卷
- LUN
- 本地层（聚合）

可用的资源级别取决于您选择的模板和指标。

用于运营分析的图表类型

图表类型会影响您解读趋势、比较、分布和时间点值的速度。

图表类型	最适合
折线图	时间序列趋势，如延迟、IOPS、吞吐量、利用率和一段时间内的警报趋势。
条形图	分类比较和分布，例如按严重程度或影响区域列出的警报。
饼图或环形图	比例分布，例如容量使用百分比。
表	详细的多列数据，例如已使用的容量、运行状况和最近的警报。
单个数字（stat）	一目了然的单个键值，例如关键警报计数或故障磁盘。

用于工作负载分类的性能模板

性能模板侧重于指示工作负载压力的延迟、吞吐量和利用率信号。

模板	图表类型	问题描述
平均延迟	行	选定时间窗口内选定目标的平均延迟。
峰值延迟	行	在所选时间窗口内，在所选目标上观察到的最大延迟。
IOPS	行	跨选定目标的每秒 I/O 操作总数。
吞吐量 (MB/秒)	行	跨选定目标的数据吞吐量总和。
利用率	行	所选目标的平均 CPU 或磁盘利用率。

模板	图表类型	问题描述
性能容量	表	将当前利用率与最佳点进行比较的净空分析。

用于增长和净空的容量模板

容量模板侧重于已消耗空间和可用空间，以支持增长规划和风险检测。

模板	图表类型	问题描述
已用容量	表	跨选定目标的已用容量总和。
空闲容量	表	选定目标的可用容量总和。
已用容量(%)	饼图或环形图	选定目标的平均使用/总比率。
已用快照容量	表	跨选定目标消耗的快照空间总和。

用于风险检测的健康模板

运行状况模板侧重于对象状态和故障指标，以支持运营分流。

模板	图表类型	问题描述
运行状况状态	表	每个选定目标对象的最新健康状态。
已降级/关键对象	单个号码	运行状况状态不正常的对象计数。
故障磁盘	单个号码	所选系统中故障磁盘的总数。
网络接口错误	饼图或环形图	所选目标的网络接口错误计数器总和。
热对象（按延迟）	表	按峰值延迟降序排列的资源。

用于事件优先级排序的警报模板

警报模板侧重于事件数量、严重程度和影响区域，以支持监控和优先级排序。

模板	图表类型	问题描述
警报（严重）	单个号码	时间窗口内严重级别警报的计数。
警报（按严重程度）	栏	按严重程度级别分组的警报。
警报（按影响区域）	栏	按影响区域（例如容量、性能或安全性）分组的警报。
近期警报	表	最新提醒，按时间降序排列。
警报趋势	行	在所选时间窗口内每个时间段的警报计数。

相关信息

- "在 NetApp Console 本地部署中查看主页指标"
- "了解 NetApp Console 本地部署中的自定义仪表板"
- "创建自定义仪表板"
- "在 NetApp Console 本地部署中自定义仪表板卡"

- "管理自定义仪表板"

管理自定义仪表板

在 **NetApp Console** 本地部署中管理仪表板

在 NetApp Console 本地部署中管理自定义仪表板，使视图与操作保持一致。随着团队、机群和优先级的变化，您可以编辑、复制和删除仪表板。

此任务仅适用于*存储 > 仪表板*下的自定义仪表板。预定义的主页仪表板无法以相同的方式编辑。

查看控制面板

查看自定义和预定义的仪表板，以查找要打开、编辑、复制或删除的仪表板。

您可以复制预定义的仪表板以创建可编辑的自定义版本。

步骤

1. 选择 **Storage > Dashboards**。
2. 查看仪表板表格，找到要打开的仪表板。
3. 选择仪表板名称以打开它并查看其指标。
4. 如果需要，请使用可用操作编辑、复制或删除自定义控制面板。

随着优先级的变化更新控制面板

在运营优先级发生变化时编辑控制面板，以调整可见的卡片和指标。

步骤

1. 选择 **Storage > Dashboards**。
2. 打开要编辑的控制面板。
3. 通过从卡片的操作菜单中选择"编辑"，修改控制面板上的现有卡片。
4. 选择 **Add Card**，将新卡添加至仪表板。

   "在 NetApp Console 本地部署中自定义卡片"。

5. 选择*保存更改*以保存控制面板。
   - 您也可以从操作菜单中选择 **Save as new dashboard**，将更改另存为新控制面板。如果要为其他团队或车队保留原始控制面板，同时根据当前监控需求创建新版本，则此选项非常有用。
   - 您还可以通过从操作菜单中选择*放弃更改*来选择放弃更改。如果要恢复到仪表板的上次保存版本，此选项非常有用。

为其他资源或机群重复使用自定义仪表板

如果要将经过验证的布局重用于其他团队、车队或监控场景，而无需从头开始重建，请复制仪表板。

您可以复制预定义的仪表板以创建可编辑的自定义版本。

步骤

1. 选择 **Storage > Dashboards**。
2. 对于要复制的控制面板，请从操作菜单中选择*复制*。

   控制台本地部署会创建一个副本，其中包括来自原始仪表板的所有卡片。

3. 为复制的仪表板提供名称和描述。
4. 选择您刚刚创建的重复控制面板。更改指标、资源和卡片类型，以适应新的监控场景。

   "在 NetApp Console 本地部署中自定义卡片"。

删除不再使用的控制面板

如果仪表板不再支持当前操作，并且要将仪表板列表的重点放在活动用例上，请将其删除。

步骤

1. 选择 **Storage > Dashboards**。
2. 对于要删除的仪表板，选择*删除*。
3. 确认删除。

相关信息

- "在 NetApp Console 本地部署中查看主页指标"
- "开始在 NetApp Console 本地部署中使用仪表板"
- "了解 NetApp Console 本地部署中的自定义仪表板"
- "创建自定义仪表板"
- "在 NetApp Console 本地部署中自定义仪表板卡"

在 NetApp Console 本地部署中使用清单监控机群

在 NetApp Console 本地部署中，使用清单监控机群运行状况并调查整个环境中的存储资源。清单提供容量、安全性和性能视图，可帮助您识别问题、了解资源利用率并跟踪受管存储系统。

库存主要是一个信息和诊断工作区。从库存中，您可以查看整个机群的系统、卷和其他存储对象，并执行常见操作，例如调配存储资源。对于高级存储管理操作，NetApp Console 本地部署会将您重定向到 System Manager。

访问清单

您可以从 Console 本地部署的几个区域访问*清单*，包括：

- 主页

- 机群概述页面
- 机群运行状况卡和相关清单视图

根据您进入*Inventory*的位置，显示的范围可以是组织级别或机群级别。

清单视图

Inventory 提供多个视图，可帮助您分析存储环境的不同方面。

容量
: 查看容量利用率并识别占用存储资源的系统、卷和其他存储对象。

安全性
: 查看托管存储资源中与安全相关的信息和合规性状态。

性能
: 分析与性能相关的指标，并确定可能需要进一步调查的资源。

显示的信息因选定视图和对象类型而异。

调查存储资源

使用 **Inventory** 以：

- 监控机群运行状况
- 查看存储容量使用情况
- 跟踪托管存储系统
- 确定卷和其他占用容量的对象
- 调查潜在的安全或性能问题
- 查找需要管理关注的资源

*清单*可帮助您从对环境的高级可见性转向对特定存储资源的更详细调查。

预配存储资源

清单包括允许您调配存储资源（如卷和 LUN）的工作流。

调配资源时，请选择现有托管存储系统并提供工作负载所需的配置设置。

库存和警报

系统会针对您环境中的特定存储对象和条件生成警报。

当您选择警报时，Console 本地部署可能会将您引导到 System Manager 以进行其他调查或管理操作。*清单*通过提供对存储环境和托管资源整体状态的更广泛可见性来补充警报。

高级管理任务

Inventory 可帮助您识别需要操作的资源，但一些高级存储管理操作在 System Manager 中执行。

示例包括：

- 高级工作负载管理
- 资源重新定位和优化任务
- 详细的系统管理活动

使用 **Inventory** 识别和调查问题，然后在需要更深入的管理功能时使用 System Manager。

修正警报

了解 **NetApp Console** 本地部署中的警报

NetApp Console 本地部署会生成警报，用于识别本地 ONTAP 集群上的运行状况问题以及 NetApp Backup and Recovery 操作。

Console 本地部署将来自 ONTAP 集群以及备份和恢复操作的警报整合到单个视图中。Alerts 页面包括仪表板、警报列表和系统视图，以便您可以查看整个组织的警报，或将其范围缩小到特定的机群或系统。每个警报都会标识受影响的系统、其严重程度及其影响区域。

在 Console 本地部署中使用警报，以便：

- 检测容量、连接性、数据保护、性能和安全问题。
- 按严重程度和影响区域排列警报的优先级。
- 在 System Manager 或 Workload Analyzer 中打开警报，然后在页面提供时运行引导式或自动化的 Fix-It 操作。
- 通过电子邮件将通知路由到具有指定访问角色的用户，或通过 webhook 将警报数据发送到外部系统。
- 将警报列表导出到 CSV 文件以进行离线分析。

警报严重程度和影响区域

每个警报都包括严重程度和影响区域：

- *严重程度*表示从最高到最低的紧急程度：严重、重大、轻微、警告和信息。
- *影响区域*确定受影响的域：容量、连接性、数据保护、性能和安全性。

警报来源和范围

- *ONTAP 警报*源自 NetApp Console 本地部署发现的本地集群上的 ONTAP 事件管理系统 (EMS)。 "详细了解 ONTAP EMS 和可用警报。"
- **NetApp Backup and Recovery alerts** 源自备份和恢复操作。 "详细了解 NetApp Backup and Recovery 警报。"
- 您的权限决定您可以查看哪些机群。将视图范围扩展到整个组织、特定机群或单个系统。*系统运行状况*选项卡显示每个系统的状态，*警报*选项卡显示选定范围的当前警报列表。

- CSV 导出反映当前范围、搜索文本和筛选器。

警报通知规则

创建通知规则，以确定哪些警报生成通知以及由谁接收通知。通知规则具有以下特征：

- 它匹配服务（例如 ONTAP 管理或 Backup and Recovery）、严重程度、影响区域和目标系统上的警报。
- 对于电子邮件传递，它向具有指定访问角色的用户发送通知。对于 Webhook 传递，它将警报数据发送到配置的端点——对该数据的访问由接收应用程序控制，而非由 Console 本地部署控制。
- 它适用于特定系统，而非整个集群。
- 它可以在计划的维护窗口期间静音，以抑制预期的警报。

控制台本地部署包括安装后立即激活的默认通知规则。默认规则监控所有服务和系统的关键严重性警报，并仅向控制台通知中心发送通知——在您设置之前，不会配置电子邮件或 Webhook 传递。您可以查看和调整此规则，并创建与您的环境相匹配的自定义规则。

信息级别的警报在警报页面中可见，但不会通过通知发送，除非您明确创建包含信息严重级别的规则。

相关信息

- "监控和调查警报"
- "创建和管理警报通知规则"
- "了解 NetApp Console 本地部署中的 ONTAP 警报"

监控和调查 **NetApp Console** 本地部署中的警报

监控和调查 NetApp Console 本地部署中的警报，以保持存储正常运行并最大限度地减少中断。

查看整个组织或特定机群的活动警报，按严重程度和影响区域排定优先级，并调查根本原因，以便在问题升级前解决问题。当警报包含建议的操作或 Fix It 选项时，您可以直接从调查转入补救。

必需的访问角色

除 Federation admin 和 Federation viewer 之外的所有角色。具有 Federation admin 或 Federation viewer 角色的用户无法查看警报。"了解访问角色"。

对于 ONTAP 警报，您可以直接从警报页面访问 System Manager 和 Workload Analyzer 等工具以调查和解决问题。

对于外部报告，您可以将警报列表导出为 CSV 文件进行离线分析。

您还可以设置通知规则，以通过电子邮件或 Webhook 接收警报。"了解如何设置警报通知"。

可用警报

NetApp Console 本地部署支持 ONTAP 和 NetApp Backup and Recovery 的警报。

- "了解 NetApp Console 本地部署中的 ONTAP 警报"
- "详细了解 NetApp Backup and Recovery 警报。"

查看警报控制面板

使用警报仪表板可快速查看所选范围的当前警报活动。控制面板按严重程度和影响区域汇总活动警报，并包含一个图表，显示过去 24 小时内的警报分布情况，以便您快速发现趋势。

您可以筛选控制面板，以专注于关键警报或特定影响区域的警报。

步骤

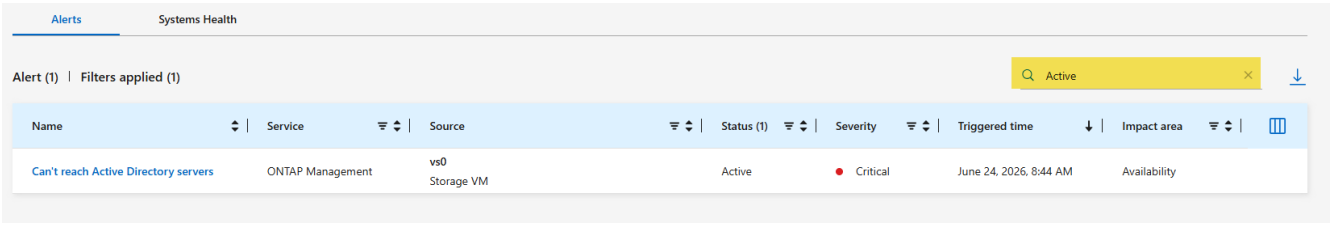
1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 根据您需要查看的警报筛选仪表板，包括：
   - 严重程度（严重、警告或信息）
   - 按影响区域分组的关键警报
   - 影响区域（安全性、保护、可用性、性能、容量或配置）

查看所有提醒

使用"警报"选项卡可查看所选范围的活动警报的完整列表。列表将更新以反映当前组织或机群范围，您可以按名称或描述搜索列表中的特定警报。

步骤

1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 选择*Alerts*选项卡以查看选定范围的活动警报的完整列表。
4. （可选）按名称或描述搜索列表中的特定警报。



按系统查看警报

您可以查看特定系统在机群或组织内的警报。

步骤

1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：

- 全部（默认）以查看您有权访问的所有队列的警报
- 仅可查看该队列警报的特定队列

3. 选择 **Systems health** 选项卡以查看与所选范围内的系统关联的警报摘要。
4. 在相应系统的行上选择*查看警报*，以查看与该系统关联的活动警报的完整列表。

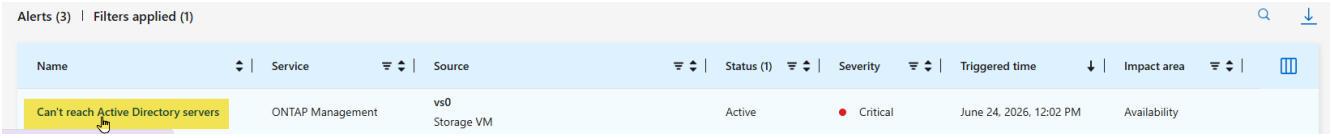
调查警报

您可以调查警报，查看是什么触发了警报，以及谁收到了通知。

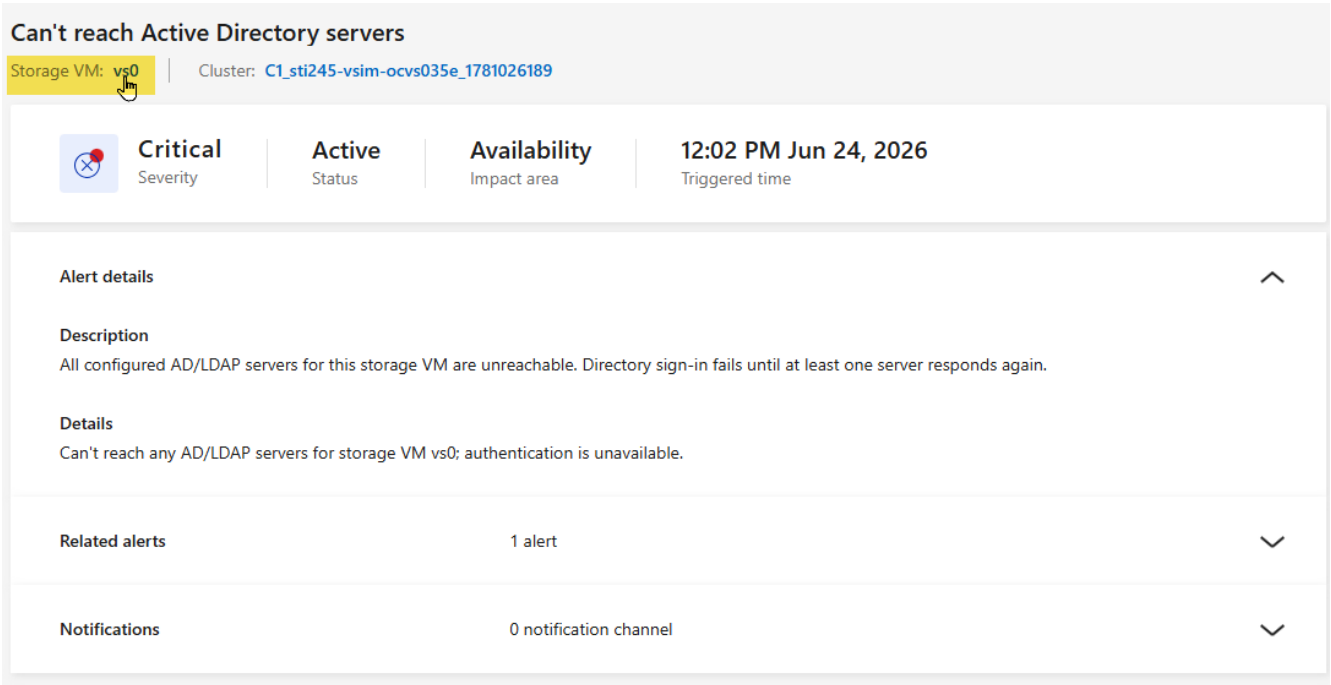
在调查 ONTAP 警报时，您还可以直接转到生成警报的系统的 System Manager 界面，以查看其他详细信息并采取相应措施。

步骤

1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 在任一选项卡中，选择要调查的警报的名称以查看其详细信息。



4. 如果适用，请选择 VM 或集群名称，以打开生成警报的系统的 System Manager 界面。



修正警报

当警报包含建议的操作或"修复"选项时，可使用它从调查转入补救，而无需离开警报详细信息。

步骤

1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 选择要修正的警报。
4. 查看警报详细信息，然后选择建议的操作或 **Fix It** 选项（如果可用）。
5. 按照指导步骤应用补救措施，然后返回警报详细信息以确认警报状态。

如果该操作解决了问题，警报将不再显示为该范围的活动警报。如果警报仍处于活动状态，请再次查看警报详细信息并继续调查。

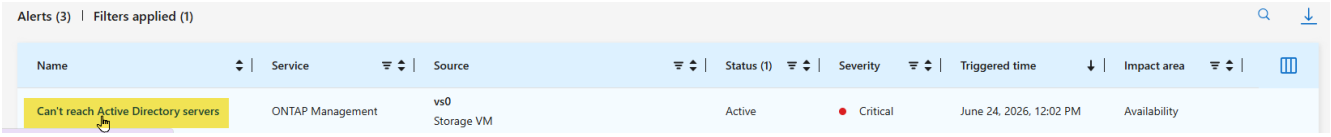
分析警报

您可以在 Workload Analyzer 中分析 ONTAP 警报，以了解触发它的原因。

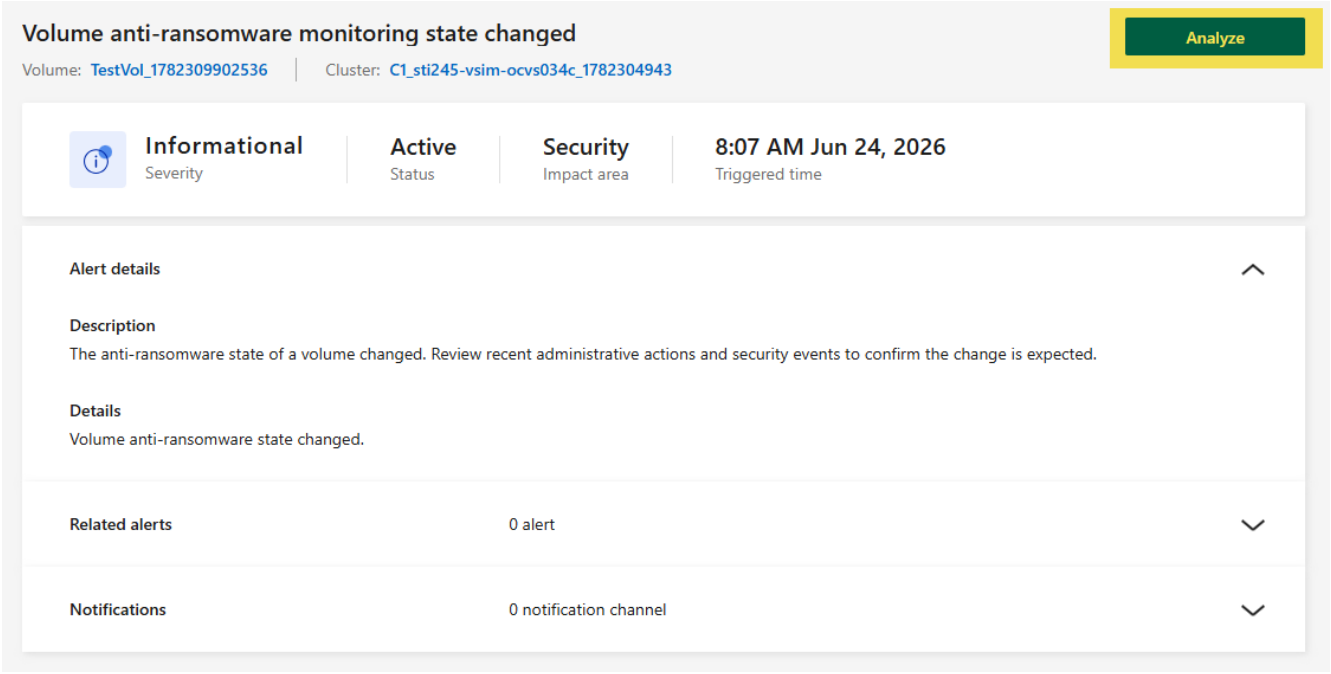
在调查 ONTAP 警报时，您还可以直接转到生成警报的系统的 System Manager 界面，以查看其他详细信息并采取相应措施。

步骤

1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 选择 **Systems health** 选项卡以查看选定范围的活动警报的完整列表。
4. 在任一选项卡中，选择要调查的警报的名称以查看其详细信息。



5. 如果适用，选择 **Analyze** 以打开生成警报的系统的工作负载分析器界面。



6. 输入触发警报期间的时间范围，然后选择 **Analyze** 以查看分析结果。 "了解 Workload Analyzer。"

将警报导出为**CSV**

将 NetApp Console 本地部署中的警报列表导出到 CSV 文件以进行离线分析或报告。导出反映当前范围（组织或机群）、搜索文本和筛选器。

步骤

1. 选择 **Health > Alerts**，然后选择 **Alerts** 选项卡。
2. 设置范围（组织或机群）并应用您希望包含在导出中的任何过滤器或搜索文本。
3. 选择下载图标，将警报列表导出为 CSV 文件。

在 **NetApp Console** 本地部署中配置警报的通知规则

在 NetApp Console 本地部署中配置通知规则，以控制哪些警报会触发通知、谁接收通知以及如何发送通知。

必需的访问角色

超级管理员、组织管理员、存储管理员、运营支持分析员或 NetApp Backup and Recovery 的任何管理员角色。"了解访问角色"。

使用通知规则，通过适合您环境的渠道将正确的警报发送给正确的人，同时减少与您无关的警报带来的噪音。通知规则是对"警报"页面的补充：您可以在"警报"工作流程中调查或修复警报，然后使用规则来控制将来发送类似警报的方式。

通知规则根据您定义的条件（例如服务、严重程度和影响区域）匹配警报，然后通过您选择的渠道发送通知。Console 本地部署包括您可以查看和调整的默认通知规则，您也可以创建自己的自定义规则。您还可以将规则静音，以便在计划事件（如维护窗口）期间暂时禁止通知。

- "详细了解 ONTAP EMS 和可用警报。"

开始之前

- 若要通过电子邮件发送通知，您的组织管理员必须在 Console 本地部署中配置电子邮件服务器。要向外部系统发送通知，您的组织管理员必须配置 webhook。有关步骤，请参见 "配置通知传送"。
- 默认情况下，Console 本地部署通知中心会显示通知，因此无需对控制台内通知进行其他设置。

查看通知规则

通知规则页面是查看和管理适用于贵组织的每个规则的中心位置。每个规则都会显示其关键属性，以便您可以快速评估和调整警报行为。

步骤

1. 从左侧导航栏中，选择 **Health > Alerts**。
2. 选择*通知设置*。
3. 查看列表中的规则。每个规则显示其活动状态、名称、其监视的服务和严重性级别、授权接收通知的角色、启用的传递通道、上次修改的时间以及任何计划的静音时间段。
4. 要查找特定规则，请使用筛选器和搜索控件按活动状态、服务、严重程度、角色、频道或静音状态进行筛选。

创建通知规则

创建通知规则以定义触发通知的条件以及通知的传递方式。

> 您无法为机群设置通知规则。您只能为特定系统设置通知规则。在包含多个系统的大型环境中，建议按严重性创建更广泛的规则，而不是为每个系统重复创建规则——例如，一条涵盖所有系统的"严重"规则可作为通用规则，同时为需要不同路由或收件人的系统添加额外的针对性规则。

适用于所有系统的严重警报的通知规则示例

假设您希望确保不会忽视任何关键警报，无论其来自哪个系统。您可以创建一个广泛的规则，将所有关键警报路由到存储管理员的 Console Notification Center。

在此示例中，您创建的规则具有以下设置：

- 服务：全部
- **Severity**：严重
- **IAM role**：存储管理员
- **System**：（留空以应用于所有系统）
- 交付方式：Console Notification Center

通过此规则，存储管理员可以在 Console 中看到所有系统上每个关键警报的通知。此规则用作基准，您可以用更有针对性的规则进行补充。

存储管理员容量警报的目标通知规则示例

假设您的存储管理员需要立即响应特定生产系统上的关键容量问题，但您不希望严重程度较低的警报淹没其收件箱。您可以创建一个有针对性的规则，仅在系统触发关键容量警报时向存储管理员发送电子邮件。

在此示例中，您创建的规则具有以下设置：

- 服务：ONTAP 管理
- **Severity**：严重
- 影响区域：容量
- **IAM role**：存储管理员
- 系统：<system_name>
- 交付方式：电子邮件

设置此规则后，当发生关键容量警报时，Console 本地部署会向指定系统的所有存储管理员发送电子邮件。严重程度较低的警报（例如警告或信息）不会生成电子邮件，因此团队可以专注于需要紧急关注的问题。

步骤

1. 从左侧导航栏中，选择 **Health > Alerts**。
2. 选择*通知设置*，然后选择*添加规则*。
3. 定义规则匹配的条件：
   - 规则名称：输入一个简洁、描述性的名称。此字段为必填项。
   - **Rule description**：可选择输入有关规则目的的其他上下文。
   - 服务：选择规则适用的一个或多个 ONTAP 或平台服务。
   - 角色：选择触发规则时用户必须具备的访问角色，以便接收通知。
   - 严重级别：选择规则监控的严重级别，例如严重、警告、错误或信息。
   - 影响区域：选择要匹配的运营区域，例如容量或性能。
   - **Alert name**：选择触发规则的特定警报类型。
   - 系统：选择规则适用的系统上下文。
4. 选择通知的传送渠道：
   - **Email**：向具有选定角色的用户发送警报电子邮件。需要配置的电子邮件服务器。
   - **Webhook**：将警报数据发送到外部系统。需要选择已配置的 Webhook 集成。
   - **Console Notification Center**：为具有选定角色的用户显示实时警报。
5. 可选地，要在计划期间（例如维护窗口）抑制来自此规则的通知，请设置 **Mute notifications** 计划，如果希望静音期间重复，请选择重复周期。您可以为每个规则添加多个静音窗口，这对于每周修补等定期维护周期非常有用。
6. 选择 **Create**。

启用或禁用通知规则

启用或禁用单个通知规则以控制哪些条件引发通知。禁用与您的环境无关的规则以减少干扰，并启用规则以重新开始接收相关通知。

步骤

1. 从左侧导航栏中，选择 **Health > Alerts**。
2. 选择*通知设置*。
3. 找到要更改的规则。

4. 打开或关闭规则的*Active*开关。更改立即生效。

将通知规则静音

将通知规则静音，以在计划事件（如维护窗口）期间抑制警报传递，而不禁用该规则。在静音期间，警报会继续显示在"警报"页面中，只有电子邮件、webhook 和控制台内通知会被抑制。当静音窗口到期时，通知会自动恢复。

可以将多个静音窗口添加到一个规则中，并将每个窗口配置为按计划重复出现。

静音窗口示例

- 一次性维护时段：您正在星期六晚上对存储系统运行固件升级，并希望在该时段内抑制预期的警报。将静音窗口设置为周六晚上 10 点至周日凌晨 2 点，不重复出现。窗口到期后，通知将自动恢复。
- 每周定期修补窗口：您的团队每周日午夜至凌晨 4:00 对系统进行修补。添加每周重复的静音窗口，以便每周自动抑制通知，而无需手动干预。如果第二个系统在不同时间有其自己的修补计划，请将第二个静音窗口添加到同一规则中，并为其设置各自的开始时间和重复周期。

步骤

1. 从左侧导航栏中，选择 **Health > Alerts**。
2. 选择*通知规则*。
3. 在规则列表中，找到要静音的规则，然后选择该规则的操作菜单。
4. 选择*编辑*。
5. 在*静音通知*部分，设置静音窗口的开始和结束日期和时间。
6. （可选）选择重复周期，以按计划重复该窗口。
7. 要添加其他静音窗口，请选择*Add mute window*并重复前面的步骤。
8. 选择 * 保存 *。

删除通知规则

如果您不再需要通知规则，请将其删除。删除规则会将其永久移除，因此无法恢复。

步骤

1. 从左侧导航栏中，选择 **Health > Alerts**。
2. 选择*通知设置*。
3. 在规则列表中，找到要删除的规则，然后选择该规则的操作菜单。
4. 从操作菜单中选择*删除*。

相关信息

- "配置通知传送"
- "了解控制台警报"
- "查看提醒"

修正 **NetApp Console** 本地部署中的存储类偏移

在 NetApp Console 本地部署中，查找与漂移相关的警报，分析漂移发现，并修复不再符合其存储类意图的工作负载。

必需角色

存储管理员

您只能在拥有权限的队列中查看和修复工作负载。

补救漂移

当工作负载不再与其存储类意图匹配时，NetApp Console 本地部署会引发警报。使用警报分析漂移并应用推荐的补救措施。

您可以直接从警报中应用一些修正。对于其他问题，请更新工作负载配置或分配其他存储类以恢复合规性。修正工作流程在应用更改之前显示预期的影响。

步骤

1. 选择 **Storage > Storage classes**。

   存储类漂移摘要显示在*按存储类划分的漂移*区域中。完整列表显示在表格中。

2. 在*漂移*列中，选择相关存储类的*查看*。

   此时会打开*提醒>概览*页面，其中应用了筛选器。

3. 选择一个警报以打开警报详细信息页面。
4. 选择*分析*。
5. 请查看 **Workload analyzer** 中的结果。

   有关配置漂移结果，请比较预期设置和实际设置，以确定更改的内容。

6. 选择建议的修正操作，例如 **Fix it**。
7. 查看建议的更改并应用修复措施。
8. 返回 **Storage > Storage classes**，确认工作负载不再显示为已漂移。

   合规性评估可能需要几分钟才能反映最近的配置更改。如果工作负载仍列为"漂移"，请返回警报详细信息页面并选择*分析*以查看任何剩余结果。

相关信息

- "了解 NetApp Console 本地部署中的存储类漂移和合规性"
- "了解有关存储警报的信息"
- "查看提醒"

NetApp Console 本地部署中的警报修复操作

使用此参考了解 NetApp Console 本地部署中*修复*可用的修复操作。对于每个操作，表格描述了操作的功能和相关警报。在运行之前，请查看确认对话框中的操作详细信息。

修复操作

修正操作	警报名称	警报说明	影响区域	修正摘要
启用自动卷增长	卷已满	此卷的空间不足，已接近满容量。	容量	自动增加卷的大小（最高可达配置的限制），以降低空间耗尽的风险。
调整卷大小	卷已满	此卷的空间不足，已接近满容量。	容量	增加卷的大小以立即提供更多空间。
使卷联机	卷脱机	此卷已脱机，不提供数据。	可用性	使脱机卷联机，以便它可以恢复提供数据。
使聚合联机	聚合脱机	此聚合未联机，其上托管的卷可能不可用。	可用性	使脱机聚合联机以恢复对其托管卷的访问。
使 **LUN** 联机	LUN 脱机	此 LUN 已脱机，主机访问不可用。	可用性	使脱机 LUN 联机，以便主机可以恢复访问和 I/O。
取消限制卷	卷受限	此卷处于受限状态，可能无法正常提供 I/O。	可用性	将受限卷恢复到联机状态，以便客户端可以再次访问它。
使 **NVMe** 命名空间联机	NVMe 命名空间处于脱机状态	NVMe 命名空间脱机，主机访问不可用。	可用性	使脱机 NVMe 命名空间联机以恢复主机访问。
启动集群间 **LIF**	集群间 LIF 已关闭	集群间 LIF 已关闭，集群到集群的通信可能会受到影响。	连接	启动集群间 LIF 以恢复用于复制的集群间连接。
重新启用 **MetroCluster AUSO**	MetroCluster 自动计划外切换已禁用	此集群上的自动计划外切换已禁用。	可用性	重新启用自动计划外切换（AUSO），以便 MetroCluster 保护按预期工作。
配置 **Service Processor** 网络	未配置 Service Processor	未配置服务处理器(SP)网络。	易管理性	配置 Service Processor (SP) 网络设置以启用带外管理访问。
分配未分配的磁盘	检测到未分配的磁盘	存在未分配的磁盘，并且可能未使用可用容量。将磁盘分配给节点，以便它们可用于存储。	可用性	将当前未分配的磁盘分配给节点，以便它们可用于存储。
根卷空间恢复	节点根卷空间不足	节点根卷上的可用空间不足，可能会影响正常的系统运行。	系统运行状况	通过删除最大的快照或最大的核心转储文件来释放节点根卷上的空间。删除是永久性的。

调查性能问题

了解 NetApp Console 本地部署 Workload Analyzer

使用 NetApp Console 本地部署 Workload Analyzer 查看单个卷在一段时间内的行为。您可以从卷本身、警报或清单中调查性能降级、容量趋势和资源争用问题。

Workload Analyzer 如何识别根本原因

使用 Workload Analyzer 跨六个部分关联单个卷的指标，以便快速识别根本原因。选择一个卷和一个时间范围，以便在同一窗口中同时查看事件、性能和容量。此视图可以帮助您确定存储是否是应用程序问题的可能来源，或者其他层（如网络）是否导致了问题。

当您已经知道哪个卷受到影响时，分析器最为有用。如果您从警报或卷清单中打开它，NetApp Console 本地部署会在选定卷的情况下打开分析器，以便您可以专注于分析窗口和图表。

分析器一次跟踪一个卷，因此使用它来调查特定问题，而不是比较多个卷。

作为此评估的一部分，请查看容量部分。当 ONTAP 系统使用率超过 85% 时，高利用率本身就会导致性能问题，因此可用容量不足可以解释性能图表本身无法说明的延迟。

确定根本原因后，您可以直接从分析器中操作。当自动选项可用时，Console 本地部署提供带有引导步骤或一键修正的 Fix-It 建议。

> LUN 的工作负载图表不能提供与卷的图表相同级别的详细信息，因此在分析 LUN 时，您将看到较少的统计信息。

访问工作负载分析器

可以通过以下几种方式打开 Workload Analyzer：

- 从 **Health** 菜单中，选择 **Workload Analyzer**，然后在 **Volume** 字段中搜索并选择要调查的卷。
- 从 **Storage > Fleets > Inventory** 页面，导航到要分析的卷，然后从操作菜单中选择 **Analyze**。
- 从 **Alerts > Overview** 页面中，为要调查的卷选择一个警报，然后从警报详细信息中选择 **Analyze**。

您还可以分析 LUN，但它们显示的统计信息少于卷。

分析延迟、吞吐量和存储容量

使用以下六个部分调查卷：

卷选择
: 选择要调查的卷和时间范围，以便所有图表和事件都与相同的工作负载和分析窗口保持一致。

事件时间轴
: 查看分析窗口期间选定卷的当前和历史配置更改、警告警报和关键警报。使用此部分将"发生了什么变化"与性能或容量行为的变化相关联。

延迟分析

查看随时间推移的卷延迟，可以作为总计查看，也可以按延迟中心细分——网络、数据处理、聚合操作、集群互连等。如果卷使用 QoS 策略，则分析器将策略的最大和最小延迟限制显示为参考线，以便您可以查看工作负载与限制阈值的接近程度。切换预测以预测延迟是否趋向警告阈值或临界阈值。

吞吐量分析

查看一段时间内的 IOPS 和 MB/s，以及可选的读/写/其他细分。如果卷使用 QoS 策略，分析器将显示 IOPS 和吞吐量限制线。切换预测以预测需求是否趋向于 QoS 限制。

资源利用率

查看在分析窗口期间为卷提供服务的节点和聚合的繁忙程度。分析器将每个资源绘制为独立的行，而不是堆叠值，因此您可以识别特定节点或聚合是否为争用源。切换预测以预测是否有任何资源正朝着高利用率阈值发展。

容量分析

查看卷中的物理空间和可用空间随时间的变化情况。悬停以查看存储效率明细，包括重复数据删除、压缩和数据缩减节省情况。切换预测以预测卷何时达到警告或临界容量阈值。切换到快照视图，查看快照空间如何根据配置的快照预留进行跟踪。

预测容量和性能趋势

使用每个分析部分中的预测切换可将图表时间线扩展到当前时间之外，并根据观察到的趋势预测未来值。虚线将预测值与实际数据区分开来。当预测表明可能发生阈值违规时，分析器还会显示洞察消息，以及预计的违规时间。

相关信息

"调查卷上的高延迟"。"调查卷上的高吞吐量需求"。"调查卷的容量增长情况"。"了解 NetApp Console 本地部署中的 Workload Analyzer 指标"。

在 **NetApp Console** 本地部署中调查卷上的高延迟

在 NetApp Console 本地部署中使用 Workload Analyzer 查找卷响应时间缓慢的根源。

如果您从警报或卷清单中打开分析器，则已选择卷，您可以专注于时间范围和图表细分。

当应用程序性能下降时，请确定 I/O 路径的哪一部分导致了速度下降。延迟分析部分按延迟中心分解响应时间，以便您可以区分网络问题、数据处理开销、聚合争用和其他影响因素。

步骤

1. 使用以下方法之一打开 Workload Analyzer：
   - 从 **Health** 菜单中，选择 **Workload Analyzer**，然后在 **Volume** 字段中搜索并选择要调查的卷。
   - 从 **Storage > Fleets > Inventory** 页面，导航到要分析的卷，然后从操作菜单中选择 **Analyze**。
   - 在*警报 > 概览*页面中，为要调查的卷选择与容量相关的警报，然后从警报详细信息中选择*分析*。
2. 将*时间范围*设置为涵盖性能问题发生的时间段，然后选择*分析*。
3. 查看*事件时间轴*部分，了解与延迟增加相关的配置更改和警报。

   分析器沿着与延迟图表相同的时间轴绘制配置更改事件（扳手图标）和警报事件（警告和关键图标），以便于查看更改是否先于降级。

4. 在*延迟*部分，打开*视图*下拉列表，然后选择*按延迟中心细分*。该图表显示了每个延迟中心在一段时间内对总延迟的贡献。延迟中心包括：
   - 读取延迟
   - 写入延迟
   - 其他延迟
5. 将鼠标悬停在图表中延迟最高的点上，以查看每个延迟中心的值及其占总延迟的百分比。

   最大的延迟中心通常指向争用的资源。当共享资源无法满足需求时，使用它的卷会等待更长时间的 I/O。通过移动工作负载或调整 QoS 限制等方式减少该资源的负载，从而降低延迟。

6. 确定主要贡献者，并使用该值确定后续步骤：
   - 高*读取延迟*可能表示磁盘争用。请检查*资源利用率*部分以确认聚合繁忙百分比。
   - 高*写入延迟*可能表示集群外的 NIC 饱和度或网络路径问题。
   - 高*其他延迟*可能表明内联效率设置消耗的 CPU 超出了工作负载的容忍范围。请考虑调整效率设置或 QoS。
   - 高*云延迟*可能表示工作负载正在频繁访问容量层上的冷数据。请考虑调整分层策略。
7. 如果延迟中心未能解释性能下降的原因，请查看*容量分析*部分。当 ONTAP 系统使用率超过 85% 时，无论延迟中心细分情况如何，高利用率都可能导致性能问题。
8. 如果延迟在更改事件后立即增加，请同时使用事件详细信息和相关图表来验证可能的原因：
   - 对于 QoS 更改，将延迟线与 QoS 限制线进行比较，并查看吞吐量图表，以确认需求是否达到策略上限。
   - 对于聚合或卷移动，请将延迟峰值与相同时间范围内显示的节点和聚合利用率值进行比较。
   - 对于分层策略更改，请查看云延迟贡献，以确定更改后冷数据访问是否增加。

完成后

如果配置或放置问题导致此问题，并且 Console 本地部署可以解决此问题，则卷上的警报可能会提供 Fix-It 选项。

"了解 NetApp Console 本地部署中的 Workload Analyzer 指标"。

调查 **NetApp Console** 本地部署中卷上的高吞吐量

在 NetApp Console 本地部署中使用 Workload Analyzer 检查卷随时间变化的 IOPS 和吞吐量需求。

当卷的工作负载消耗的 IOPS 或吞吐量超过预期时，请确定是什么推动了需求。吞吐量分析部分显示 IOPS 和 MB/s，以及可选的读取、写入和其他细分，以便您可以确定哪种类型的 I/O 推动了高需求，以及该需求是否趋向于 QoS 限制。

如果您从警报或卷清单中打开分析器，则已选择卷，您可以专注于时间范围和吞吐量图表。

步骤

1. 使用以下方法之一打开 Workload Analyzer：
   - 从 **Health** 菜单中，选择 **Workload Analyzer**，然后在 **Volume** 字段中搜索并选择要调查的卷。

- 从 **Storage > Fleets > Inventory** 页面，导航到要分析的卷，然后从操作菜单中选择 **Analyze**。
- 从 **Alerts > Overview** 页面中，为要调查的卷选择一个警报，然后从警报详细信息中选择 **Analyze**。

2. 设置*时间范围*以覆盖高需求时期，然后选择*分析*。
3. 滚动到*吞吐量分析*部分。
4. 打开 **View** 下拉菜单并选择 **Breakdown (RWO)**。

   对于 IOPS 和 MB/s，图表分为读取、写入和其他组件。这使您可以确定是读取密集型访问模式、写入密集型模式还是两者的组合在推动需求。

5. 使用组件选取器启用或禁用要检查的指标：
   - **Read IOPS** 和 **Write IOPS** — 按 I/O 方向的每秒操作数
   - 读取 **MB/s** 和 写入 **MB/s** — 按 I/O 方向以 MB/s 表示的吞吐量
   - 其他 **IOPS** 和 其他 **MB/s** — 元数据和其他非数据操作
   - **QoS IOPS Limit** 和 **QoS MB/s Limit** — 仅在卷使用 QoS 策略时显示的策略上限
   - 云吞吐量 — 向云写入和从云读取的 MB/s，仅针对通过 FabricPool 将容量分层到云的工作负载显示
6. 将鼠标悬停在图表中的峰值上，可查看该时间点每个组件的确切值和百分比明细。

   悬停工具提示还显示每个类别的平均 I/O 大小（吞吐量除以 IOPS），这可以指示工作负载是执行大型顺序 I/O 还是执行小型随机 I/O。

7. 启用 **Show Forecast** 以预测当前吞吐量趋势是否将达到 QoS IOPS 或 MB/s 限制。

   如果预测线接近 QoS 限制线，ONTAP 可能会很快限制工作负载。

8. 如果希望在不显示明细的情况下查看总需求，请打开*查看*下拉列表并选择*总计*。

   总计视图显示单个 IOPS 行和单个 MB/s 行，这对于快速了解总体需求摘要非常有用。

完成后

使用您观察到的吞吐量模式来决定接下来要做什么：

- 如果读取 IOPS 相对于写入 IOPS 非常高，请考虑预读设置或缓存是否可以减少卷上的负载。
- 如果工作负载接近或已达到 QoS IOPS 或 MB/s 限制，请使用 QoS 限制线和相关指标定义来确认限制并决定是否需要调整限制。
- 如果吞吐量高且延迟也升高，请检查*资源利用率*部分以确定底层节点或聚合是否处于争用状态。比较同期的吞吐量峰值、延迟峰值和资源利用率。
- 如果分析器在需求增加的同时显示快速容量或快照增长，请查看容量和快照指标，以了解这种增长可能会如何影响卷。

"调查卷上的高延迟"。"了解 NetApp Console 本地部署中的 Workload Analyzer 指标"。

调查 **NetApp Console** 本地部署中卷的容量增长

使用 NetApp Console 本地部署中的 Workload Analyzer 来调查卷空间不足的原因。

当卷正在填充或快照副本占用的空间超过预期时，请检查一段时间内的容量和快照趋势。容量分析部分显示物理空间和可用空间的变化情况、存储效率节省的细分，以及卷何时将达到容量阈值的预测。

如果您从警报或卷清单中打开分析器，则该卷已被选中，您可以专注于容量趋势和预测窗口。

步骤

1. 使用以下方法之一打开 Workload Analyzer：
   - 从 **Health** 菜单中，选择 **Workload Analyzer**，然后在 **Volume** 字段中搜索并选择要调查的卷。
   - 从 **Storage > Fleets > Inventory** 页面，导航到要分析的卷，然后从操作菜单中选择 **Analyze**。
   - 从 **Alerts > Overview** 页面中，为要调查的卷选择一个警报，然后从警报详细信息中选择 **Analyze**。
2. 设置*时间范围*以覆盖容量增长期间，然后选择*分析*。
3. 滚动到*容量分析*部分。
4. 从*视图*下拉列表中选择*容量视图*。

   图表显示物理容量为底部堆叠区域，可用容量为顶部堆叠区域。两者之和等于总卷大小，因此您可以看到可用空间减少的速度有多快。

5. 将鼠标悬停在图表上的某个点，可查看存储效率明细，包括重复数据删除、压缩和数据缩减节省量，以及总体存储效率比率。

   在物理容量增加的同时，效率比率下降可能表明新写入的数据的重复数据删除或压缩效果不如现有数据。

6. 要调查快照消耗情况，请从*View*下拉列表中选择*Snapshot View*。

   图表将快照预留空间显示为水平参考线，快照已用容量作为其下方的区域。悬停可查看已使用的快照空间及其占预留空间的百分比、快照总数以及最旧快照的时间。

   当快照消耗量超过预留空间时，快照开始占用卷数据区域中的空间，这会减少可用于新写入的空间。

7. 如果卷将数据分层到云，请从*视图*下拉列表中选择*云层视图*，以比较本地性能层与云容量层的容量。
8. 启用*显示预测*以预测卷何时将达到警告或临界容量阈值。

   容量预测至少需要 10 天的历史数据。当卷满之前剩余容量不足 30 天时，分析器会将存储标识为接近已满。预测会显示一条包含预计突破时间的洞察消息。

完成后

使用您观察到的容量趋势来决定接下来要做什么：

- 如果可用容量正趋向于满，请考虑增加卷大小、启用自动增长或将数据从卷移出。
- 如果快照已用容量超出保留容量，请查看您的快照策略和保留以回收空间。
- 如果存储效率比率正在下降，请检查工作负载的数据类型或内联效率设置是否正在减少节省。使用 "了解 NetApp Console 本地部署中的 Workload Analyzer 指标" 获取容量、快照和效率指标的详细描述。

NetApp Console 本地部署中的 **Workload Analyzer** 指标

在 NetApp Console 本地部署中，Workload Analyzer 显示六个部分的指标。每个指标描述都解释了分析器如何在图表上呈现指标，以及它对卷行为的指示。

延迟图表中的 **QoS** 参考线

如果所选卷使用 QoS 策略，您可以在指标选择器中使用两条额外的参考线：

参考线	问题描述
服务质量 (QoS) 上限	QoS 策略定义的最大延迟上限。当延迟线接近或触及此线时，ONTAP 将对工作负载进行限速，QoS 限制（而非物理资源）是延迟的主要来源。
服务质量 (QoS) 下限	由 QoS 策略定义的保证最小延迟下限。此行指示针对工作负载实施的响应时间下限。当其他工作负载使用 QoS 最小值来保证其吞吐量时，ONTAP 可以限制此工作负载，从而显示更高的延迟。

这些水平线不会出现在悬停时的延迟中心细目中。它们用作参考阈值，而非延迟的贡献因素。

按 **I/O** 类型划分的延迟细分

从视图下拉列表中选择*按延迟中心分类*后，请使用*延迟分析*部分中的 I/O 类型分类。该图表根据 I/O 操作的方向将总延迟分为三类。使用这些指标来确定性能问题是否影响读取、写入或元数据操作。

延迟类型	问题描述	值升高的常见原因
读取延迟	在卷上完成客户端读取请求的平均时间，从收到请求到返回数据。读取请求必须遍历完整的 I/O 路径，从网络协议层通过数据处理堆栈到达数据所在的聚合。	聚合或磁盘争用；将读取提升到物理磁盘的缓存未命中；通过 FabricPool 从云容量层检索的冷数据；当数据驻留在与处理请求的节点不同的节点上时，跨节点读取。
写入延迟	确认卷上的客户端写入请求的平均时间。ONTAP 在将写入提交到 NVRAM 写入日志后确认写入；数据随后刷新到聚合。	NIC 饱和或客户端与存储节点之间的高往返延迟；同步 SnapMirror 在写入确认之前等待目标集群确认接收；写入负载过重时的 NVRAM 压力；写入 I/O 路径中运行的内联重复数据删除、压缩或压缩所产生的 CPU 开销。
其他延迟	在卷上完成非读、非写操作的平均时间，包括文件打开、属性查找、目录遍历、文件创建和锁定。即使读写延迟看起来正常，其他延迟的增加也会影响应用程序的响应能力。	内联效率操作与元数据处理竞争产生的 CPU 压力；产生大量文件创建、删除或目录扫描的工作负载引发的高命名空间活动；限制总 IOPS 的 QoS 限制，导致可用于元数据操作的 IOPS 减少；多个卷同时处于活动状态时产生的卷激活开销。

吞吐量组件

从视图下拉列表中选择*细分（RWO）*后，请使用*吞吐量分析*部分中的吞吐量组件。分析器同时显示 IOPS 和 MB/s。

组件	问题描述	呈现为
读取 IOPS	每秒读取操作数。	IOPS 图表上的堆积区域。
写入 IOPS	每秒写入操作数。	IOPS 图表上的堆积区域。
其他 IOPS	每秒的元数据和其他非数据操作。	IOPS 图表上的堆积区域。
读取 MB/s	读取吞吐量，以MB/秒表示。	MB/s 图表上的堆积面积图。
写入 MB/s	写入吞吐量，以MB/秒表示。	MB/s 图表上的堆积面积图。

组件	问题描述	呈现为
云吞吐量	卷和云容量层之间的吞吐量，以 MB/秒表示。此指标仅显示通过 FabricPool 将容量分层到云的工作负载。	MB/s 图表上的堆积面积图。

读取、写入和其他组件的总和为总 IOPS 或 MB/s 值。将鼠标悬停在图表上可查看每个组件的值、其占总数的百分比以及每个类别的平均 I/O 大小（MB/s ÷ IOPS）。

资源利用率指标

使用*资源利用率*部分查看资源利用率指标。分析器将为卷提供服务的每个资源显示为独立行。资源不堆叠。

节点指标

指标	问题描述
节点利用率	节点的复合利用率百分比。悬停以查看每个节点的 CPU 利用率、网络利用率和可用余量。
CPU 利用率	正在使用的节点 CPU 容量百分比。悬停工具提示显示此值。
网络利用率	使用中的节点网络容量百分比。悬停工具提示显示此值。
性能余量	可用于额外工作负载的剩余节点容量。悬停工具提示显示此值。

聚合指标

指标	问题描述
聚合利用率	聚合的磁盘忙率百分比。悬停以查看磁盘忙碌值、聚合上的卷数和可用余量。
磁盘繁忙	聚合磁盘主动服务 I/O 的时间百分比。悬停工具提示显示此值。
卷计数	当前在聚合上托管的卷数。悬停工具提示显示此值。
性能余量	可用于额外工作负载的剩余聚合容量。悬停工具提示显示此值。

当节点或聚合利用率线超过图表用虚线标记的高利用率警告阈值时，该资源上的其他工作负载可能会与所选卷竞争 I/O 容量。

容量指标

容量视图

从视图下拉列表中选择*容量视图*后，使用*容量分析*部分查看容量视图指标。

指标	问题描述
物理容量	存储效率操作后磁盘上消耗的空间。这是图表中的底部堆叠区域。物理 + 可用始终等于总卷大小。
可用容量	卷中剩余的可用空间。这是图表中最顶部的堆叠区域。它会随着物理容量的增加而减少。

指标	问题描述
存储效率比	总效率比（逻辑数据 ÷ 物理数据）。悬停工具提示显示此值。它反映了重复数据删除、压缩和数据缩减的综合节省。
重复数据删除节省量	通过删除重复数据块节省的空间。悬停工具提示显示此值。
压缩节省	通过内联压缩数据节省的空间。悬停工具提示显示此值。
数据压缩节省	将多个小块打包到单个物理块中所节省的空间。悬停工具提示显示此值。

Snapshot 视图

当要查看特定于快照的指标时，请使用"快照视图"。

指标	问题描述	呈现为
可用快照	为快照预留的预分配空间，配置为卷大小的百分比。	水平参考线。
已用 Snapshot	Snapshot 副本占用的实际空间。	储备线下方的面积图。

将鼠标悬停在图表上可查看快照保留大小、使用的快照空间及其在保留中的百分比、快照总数以及最旧快照的使用时间。当快照消耗量超过保留时，快照开始占用卷数据区域的空间。

预测行为

如果要根据观察到的趋势预测当前时间之后的未来值，请在任何分析部分中使用*显示预测*切换。以下行为适用于所有部分：

方面	行为
投影窗口	根据选定时间范围向前预测。对于 2 小时视图，预测窗口约为 1 小时。对于 7 天视图，预测窗口可延伸数天。
视觉风格	分析器将预测值呈现为虚线。垂直分隔符标记实际数据与预测值之间的边界。
阈值警报	当预测表明卷将突破警告或严重阈值时，分析器会显示洞察消息，以及预计的突破时间。
趋势基础	预测使用选定时间范围最近部分的变化率。近期数据的高波动性会降低预测置信度。
所需最少数据	容量预测需要至少 10 天的历史数据。当卷满之前剩余容量不足 30 天时，分析器会将该存储标识为接近已满。

相关信息

- "了解 NetApp Console 本地部署 Workload Analyzer"
- "调查卷上的高延迟"
- "调查卷上的高吞吐量需求"
- "调查卷的容量增长情况"

管理和监控 NetApp Console 本地部署

了解 NetApp Console 本地部署中的管理和监控

部署 NetApp Console 本地部署后，使用管理和监控工具查看活动、维护 VM 和管理成员访问。

审核活动

查看用户和 API 活动，跟踪 Console 操作的状态，下载审核日志，并在需要更长保留期或进行其他分析时将日志导出到外部工具。

- "审核 NetApp Console 本地部署活动"
- "在 NetApp Console 本地部署中设置通知传递渠道"

Licenses and subscriptions

使用 Licenses and subscriptions 信息了解 NetApp Console 环境的服务授权和订阅状态。

"了解许可证和订阅"。

维护控制台本地部署虚拟机并排除故障

维护托管 Console 本地部署的虚拟机，检查网络和系统设置，访问诊断工具，并在服务或代理不按预期运行时排除问题。

"维护您的 vCenter 或 ESXi 主机以进行控制台本地部署"。

管理用户和访问权限

查看整个组织的成员访问权限，在机群级别调整访问权限，并管理安全设置，例如 MFA 恢复和服务帐户凭据。

- "在 NetApp Console 中管理成员访问权限"
- "查看或更改 NetApp Console 本地部署中的机群访问分配"
- "在 NetApp Console 本地部署中管理成员安全性"

审核 NetApp Console 本地部署活动

您可以从"审核"页面审核从UI和API启动的用户活动，还可以监视NetApp Console本地部署中的操作状态以及启动这些操作的用户。

必需角色

超级管理员、组织管理员、文件夹和车队管理员、运营支持分析师、超级查看者、组织查看者或文件夹和车队查看者。"了解访问角色"。

您可以在 Console 本地部署中查看审核活动，下载审核日志的 CSV，或通过使用 webhook 将审核日志配置为发送到您自己的 syslog 服务器。

从"审核"页面审核用户活动

使用"审核"页面可识别执行操作的人员或其状态。

"审核"页面显示用户在组织内完成的操作。例如，您可以验证是谁向组织添加了成员或已成功删除了舰队，以及查看用户在组织中执行的其他存储管理操作。

审核日志显示以下服务的活动：

- 租用：与管理组织相关的操作，例如添加用户、创建队列以及关联资源。
- 存储管理：与管理存储资源相关的操作。
- 联合身份验证：与管理联合身份验证相关的操作，例如创建联合身份验证以及添加或删除联合身份验证组织。

步骤

1. 选择 **Administration > Audit**。
2. 使用表格上方的筛选器更改表格中显示的操作。

   例如，您可以使用*服务*筛选器显示与特定服务相关的操作，也可以使用*用户*筛选器显示与特定用户帐户相关的操作。

筛选身份和访问管理操作的审核日志

要仅查看与管理组织相关的操作（例如添加成员、创建队列或删除资源），请按 Tenancy 服务筛选审核日志。

步骤

1. 选择 **Administration > Audit**。
2. 使用筛选器缩小结果范围。选择 **Service**，然后选择 **Tenancy**。
3. 使用任何其他筛选器进一步细化结果。

   例如，使用 **User** 筛选器显示特定用户帐户执行的 IAM 操作。

从审核页面下载审核日志

您可以将审核日志从"审核"页面下载到 CSV 文件中。这使您能够记录用户在组织中执行的操作。下载的 CSV 文件包括所有审核日志列，无论"审核"页面上的过滤器或显示的列如何。

步骤

1. 在*审核*页面中，选择表格右上角的下载图标。

维护 NetApp Console

维护您的 **vCenter** 或 **ESXi** 主机以进行 **NetApp Console** 本地部署

在 NetApp Console 本地部署中，您可以在部署 Console 本地部署后对现有 VCenter 或 ESXi 主机进行更改。例如，您可以增加托管 Console 本地部署的虚拟机实例的 CPU 或 RAM。

使用 VM Web 控制台执行以下维护任务：

- 增加磁盘大小
- 重新启动控制台本地部署
- 更新静态路由
- 更新搜索域

限制

您只能通过维护控制台查看（不更新）有关 IP 地址、DNS 和网关的信息。

访问**VM**维护控制台

您可以从 vSphere 客户端访问维护控制台。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。

更改维护用户密码

您可以更改 `maint`用户的密码。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `1`以查看 `System Configuration`菜单。
6. 输入 `1`以更改维护用户密码，然后按照屏幕上的提示操作。

增加**VM**实例的**CPU**或**RAM**

您可以增加托管 Console 本地部署的 VM 实例的 CPU 或 RAM。

编辑 VCenter 或 ESXi 主机中的 VM 实例设置，然后使用维护控制台应用更改。

VSphere 客户端中的步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 右键单击 VM 实例并选择*编辑设置*。

4. 增加用于 /opt 或 /var 分区的硬盘空间。
    a. 选择 **Hard Disk 2** 以增加用于 /opt 的硬盘空间。
    b. 选择 **Hard Disk 3** 以增加用于 /var 的硬盘空间。
5. 保存更改。

维护控制台中的步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `1 to view the `System Configuration`菜单。
6. 输入 `2`并按照屏幕提示操作。控制台扫描新设置并增加分区大小。

查看 **Console** 本地部署虚拟机的网络设置

查看 vSphere 客户端中 Console 本地部署虚拟机的网络设置，以确认或排除网络问题。您只能查看（不能更新）以下网络设置：IP 地址和 DNS 详细信息。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `2`以查看 `Network Configuration`菜单。
6. 输入介于 1 到 6 之间的数字以查看相应的网络设置。

更新 **Console** 本地部署虚拟机的静态路由

根据需要添加、更新或删除控制台本地部署虚拟机的静态路由。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `2`以查看 `Network Configuration`菜单。
6. 输入 `7`以更新静态路由，然后按照屏幕提示操作。
7. 按 Enter。

8. （可选）进行其他更改。
9. 按 9 提交更改。

更新 **Console** 本地部署虚拟机的域搜索设置

您可以更新 Console 本地部署虚拟机的搜索域设置。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `2``以查看 `Network Configuration`菜单。
6. 输入 `8`以更新域搜索设置，然后按照屏幕上的提示操作。
7. 按 Enter。
8. （可选）进行其他更改。
9. 按 9 提交更改。

访问 **Console** 本地部署诊断工具

访问诊断工具以对 Console 本地部署的问题进行故障排除。NetApp 支持人员在排查问题时可能会要求您执行此操作。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。
3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `3`以查看支持和诊断菜单。
6. 进入 `1`以访问诊断工具，然后按照屏幕上的提示操作。

远程访问 **Console** 本地部署诊断工具

您可以使用 Putty 等工具远程访问诊断工具。通过分配一次性密码，启用对 Console 本地部署虚拟机的 SSH 访问。

SSH 访问启用了复制和粘贴等高级终端功能。

步骤

1. 打开 VSphere 客户端并登录到 VCenter。
2. 选择托管 Console 本地部署的 VM 实例。

3. 选择 **Launch Web Console**。
4. 使用创建 VM 实例时指定的用户名和密码登录到 VM 实例。用户名是 `maint`，密码是您在创建 VM 实例时指定的密码。
5. 输入 `3`以查看 `Support and Diagnostics`菜单。
6. 进入 `2`以访问诊断工具，并按照屏幕提示配置一个 24 小时后到期的一次性密码。
7. 请使用 SSH 工具（如 Putty），使用您配置的用户名 `diag`和一次性密码连接到 Console 本地部署虚拟机。

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**。

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。

参考

NetApp Console 本地部署 API

管理您的 NetApp Console 本地部署组织和机群 ID

在 NetApp Console 本地部署中，您的 NetApp Console 组织具有名称和 ID。您可以为组织选择一个名称以便于识别。您可能还需要检索某些集成的组织 ID。

必需的访问角色

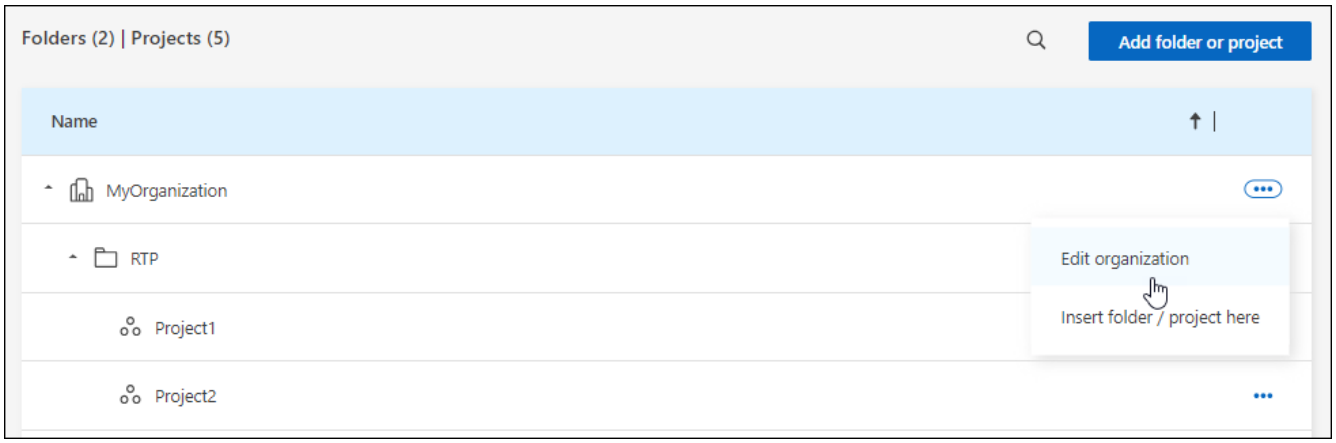
超级管理员或组织管理员。"了解访问角色"。

重命名您的组织

您可以重命名组织。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*组织*。
3. 从*组织*页面，导航到表中的第一行，选择 ••• ，然后选择*编辑组织*。



4. 输入新的组织名称，然后选择*Apply*。

获取组织 ID

组织 ID 用于与 Console 进行某些集成。

您可以从组织页面查看组织 ID，并将其复制到剪贴板以满足您的需求。

步骤

1. 选择 **Administration > Identity and access > Organization**。
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。您可以保存此内容供日后使用，也可以将其直接复制到需要使用的地方。

获取机群的 ID

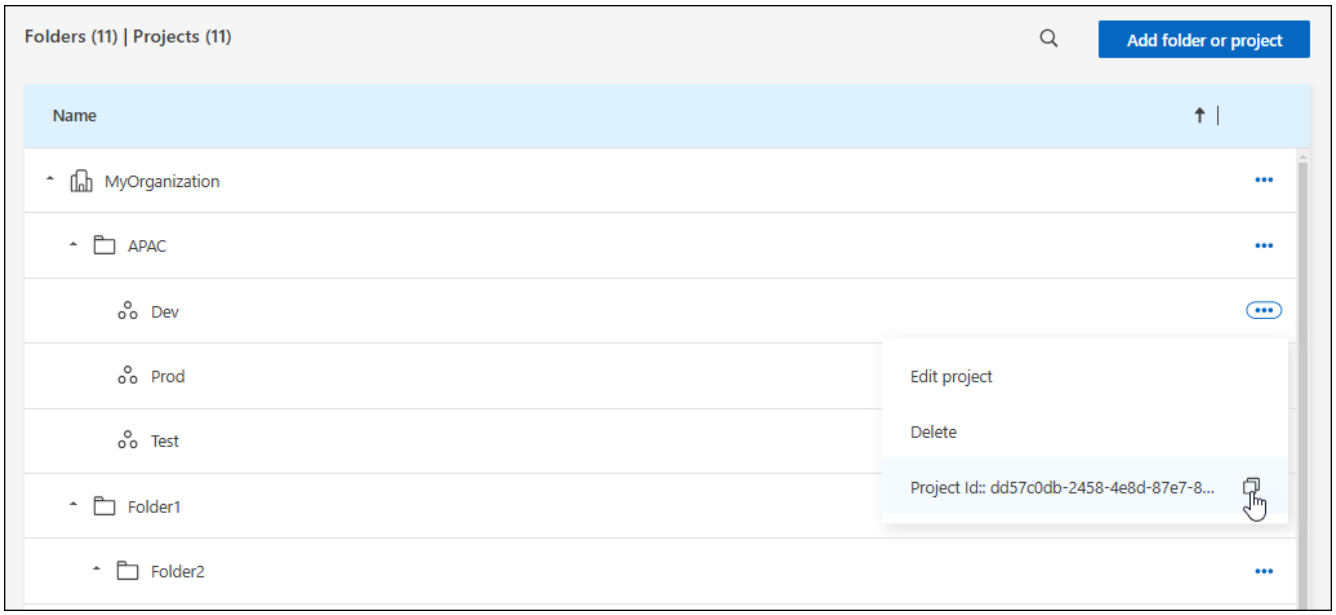
如果使用 API，则需要获取队列的 ID。

步骤

1. 在*组织*页面中，导航到表中的机群并选择 •••

   将显示机群 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"
- "开始在 NetApp Console 中使用身份和访问权限"
- "了解用于身份和访问的 API"

在 NetApp Console 本地部署中支持的 LLM 提供程序和模型

NetApp Console 本地部署支持 OpenAI、OpenAI 兼容和 Anthropic LLM 提供程序类型。您可以选择的模型取决于您配置的提供程序类型和端点。

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。

选择与您的性能、成本和治理要求相匹配的型号。

了解提供程序类型如何影响模型可用性

您选择的提供程序类型决定了哪些模型显示在 Console 本地部署模型列表中：

- **OpenAI** — 提供直接 OpenAI 集成的模型。

- **OpenAI-compatible** — 提供企业兼容端点公开的模型。
- **Anthropic** — 提供用于直接 Anthropic 集成的模型。

根据端点配置、代理或网关行为以及组织策略，您看到的模型可能会有所不同。提供程序类型因连接的端点和端点公开的模型而不同，而非传输协议。

支持的 **OpenAI** 模型

- GPT-5.4
- GPT-5.5

支持的 **Anthropic** 模型

- Claude Sonnet 4.6
- Claude Opus 4.6、4.7 & 4.8

相关信息

- "连接您的 LLM 并启用 NetApp Console 助理"。
- "了解 LLM 在 NetApp Console 本地部署中的集成"。

ONTAP 警报参考（NetApp Console 本地部署）

此参考文档按影响类别列出 NetApp Console 本地部署可以监控的 ONTAP 警报。

严重程度映射

相同的 EMS 警报可能显示为"严重"、"警告"或"信息"，具体视引起警报的 ONTAP 事件而定：

- **Critical**：映射自 ONTAP 严重性 `alert`， `emergency`
- **Warning**: 来自 ONTAP 严重程度的映射 `error`
- **Info**：来自 ONTAP 严重程度的映射 `notice`， `informational`
- 其他：按原样传递

动态映射允许单个警报规则根据 EMS 事件的运行时上下文发出不同严重性的告警。

以下部分按影响类别对警报进行分组，并按警报名称的字母顺序对每个表进行排序。

可用性警报

这些警报可能会影响系统、服务或数据的可用性。

警报名称	严重性	类型	问题描述
Active Directory 服务器连接断开	关键	EMS	此 SVM 的所有已配置 AD/LDAP 服务器均无法访问。
聚合未联机	关键	指标	一些聚合已脱机。卷创建可能导致重复的 FSID。

警报名称	严重性	类型	问题描述
防病毒服务器繁忙	严重、警告、信息	EMS	防病毒服务器已过载，无法接受其他扫描请求。
AWS 凭据未初始化	严重、警告、信息	EMS	模块在初始化之前尝试访问基于 AWS IAM 角色的凭据。
云层无法访问	严重、警告、信息	EMS	存储节点无法连接到 Cloud Tier 对象存储 API。某些数据将无法访问。
磁盘故障	关键	指标	磁盘出现故障、正在清理或处于维护模式。
磁盘已停用	严重、警告、信息	EMS	磁盘因故障、清理或维护而停止服务。
磁盘架电源已移除	严重、警告、信息	EMS	从磁盘架上取下了一个电源装置。
FC 目标端口命令超出限制	严重、警告、信息	EMS	物理 FC 目标端口上的未完成命令数超出支持的限制。
存储池交还失败	严重、警告、信息	EMS	此事件发生在存储池（聚合）重定位期间，作为存储故障转移 (SFO) 回馈的一部分，此时目标节点无法访问对象存储。
HA 互连已关闭	严重、警告、信息	EMS	高可用性 (HA) 互连断开。故障转移不可用时存在服务中断的风险。
InstanceDown	关键	指标	被监控的实例无法访问，可能已关闭或遇到网络问题。
LUN已销毁	严重、警告、信息	EMS	LUN 已被销毁，无法再访问。
LUN 脱机	严重、警告、信息	EMS	已手动使 LUN 脱机。
主机风扇出现故障	严重、警告、信息	EMS	一个或多个主机风扇出现故障。该系统仍在运行。
主机风扇处于警告状态	严重、警告、信息	EMS	一个或多个主机组件冷却风扇处于警告状态。
已超过每个用户的最大会话数	严重、警告、信息	EMS	已超过 TCP 连接上每个用户允许的最大会话数。
超过每个文件的最大打开次数	严重、警告、信息	EMS	已超过可通过 TCP 连接打开文件的最大次数。
MetroCluster 自动计划外切换已禁用	严重、警告、信息	EMS	此集群上的自动计划外切换功能已禁用。
MetroCluster 监控	严重、警告、信息	EMS	检测到系统运行状况监视器警报。
NFSv4 存储池已用尽	严重、警告、信息	EMS	NFSv4 存储池已用尽。
NetBIOS 名称冲突	严重、警告、信息	EMS	NetBIOS 名称服务收到来自远程计算机的名称注册请求的否定响应。

警报名称	严重性	类型	问题描述
无注册扫描引擎	严重、警告、信息	EMS	防病毒连接器通知 ONTAP 它没有已注册的扫描引擎。
无 Vscan 连接	严重、警告、信息	EMS	ONTAP 没有用于处理病毒扫描请求的 Vscan 连接。如果启用了 scan-mandatory 选项，这可能会导致数据不可用。
无响应的防病毒服务器	严重、警告、信息	EMS	ONTAP 检测到无响应的防病毒服务器并强制关闭其 Vscan 连接。
不存在的管理员共享	严重、警告、信息	EMS	Vscan 问题：客户端试图连接到不存在的 ONTAP_ADMIN$ 共享。
NVRAM 电池电量低	严重、警告、信息	EMS	NVRAM 电池容量极低。如果电池电量耗尽，可能会出现数据丢失。
NVMe 命名空间已销毁	严重、警告、信息	EMS	NVMe 命名空间已被销毁，无法再访问。
NVMe 命名空间脱机	严重、警告、信息	EMS	已手动使 NVMe 命名空间脱机。
NVMe 命名空间联机	严重、警告、信息	EMS	NVMe 命名空间已恢复联机。
NVMe-oF 许可证宽限期有效	严重、警告、信息	EMS	当使用 NVMe over Fabrics (NVMe-oF) 协议且许可证的宽限期处于活动状态时，此事件每天都会发生。
NVMe-oF 许可证宽限期已过	严重、警告、信息	EMS	NVMe over Fabrics (NVMe-oF) 许可证宽限期已结束，NVMe-oF 功能已禁用。
NVMe-oF 许可证宽限期开始	严重、警告、信息	EMS	在升级到 ONTAP 9.5 软件期间检测到 NVMe over Fabrics (NVMe-oF) 配置。
对象存储主机无法解析	严重、警告、信息	EMS	对象存储服务器主机名无法解析为 IP 地址。
对象存储集群间 LIF 关闭	严重、警告、信息	EMS	对象存储客户端找不到可与对象存储服务器通信的操作 LIF。
对象存储签名不匹配	严重、警告、信息	EMS	发送到对象存储服务器的请求签名与客户端计算的签名不匹配。
端口状态为已关闭	关键	EMS	此以太网端口已关闭。该链路上的流量可能会受到影响。
READDIR 超时	严重、警告、信息	EMS	READDIR 文件操作已超过允许在 WAFL 中运行的超时时间。
重新定位存储池失败	严重、警告、信息	EMS	当目标节点无法访问对象存储时，在存储池（聚合）的重定位期间发生此事件。
SAN "active-active" 状态已更改	严重、警告、信息	EMS	SAN 路径不再对称。
Service Processor 心跳丢失	严重、警告、信息	EMS	ONTAP 未收到来自服务处理器 (SP) 的预期心跳信号。

警报名称	严重性	类型	问题描述
Service Processor 心跳停止	严重、警告、信息	EMS	ONTAP 不再接收来自服务处理器 (SP) 的心跳。
未配置 Service Processor	严重、警告、信息	EMS	此事件每周发生一次，以提醒您配置服务处理器 (SP)。
Service Processor 离线	严重、警告、信息	EMS	此服务处理器(SP)处于脱机状态。
FC 目标适配器中的 SFP 接收功率不足	严重、警告、信息	EMS	当小型可插拔收发器（FC 目标中的 SFP）的接收功率（RX）低于定义的阈值时，会出现此警报。
FC 目标适配器中的 SFP 传输低功率	严重、警告、信息	EMS	当小型可插拔收发器（FC 目标中的 SFP）传输的功率（TX）低于定义的阈值时，会出现此警报。
卷影复制失败	严重、警告、信息	EMS	卷影复制服务 (VSS)，即 Microsoft Server 备份和还原服务操作失败。
磁盘架风扇发生故障	严重、警告、信息	EMS	磁盘架上指示的冷却风扇或风扇模块出现故障。
SnapMirror 滞后时间较长	关键	指标	该 SnapMirror 关系比其预期的更新计划晚了一个多小时。
存储故障转移互连一个或多个链路已关闭	警告	EMS	到合作伙伴节点的一个或多个 HA 互连链路已关闭。故障转移冗余已降低。
存储交换机电源出现故障	严重、警告、信息	EMS	集群交换机中缺少电源。冗余已降低。
Storage VM 停止成功	严重、警告、信息	EMS	已成功停止此Storage VM。
SVM 配置复制许可证无效	警告	EMS	SVM-DR 配置复制许可证缺失、已过期或未应用
由于主机风扇故障，系统无法运行	严重、警告、信息	EMS	一个或多个主机风扇出现故障，中断了系统运行。这可能导致潜在的数据丢失。
CIFS 身份验证过多	严重、警告、信息	EMS	许多身份验证协商同时进行。来自此客户端的 256 个未完成的新会话请求。
未分配的磁盘	严重、警告、信息	EMS	系统有未分配的磁盘 - 容量正在被浪费。
卷状态脱机	信息	指标	此卷已脱机。
卷受限	严重、警告、信息	EMS	此事件指示弹性卷受到限制。
检测到病毒	严重、警告、信息	EMS	Vscan 服务器报告文件可能感染了病毒。

容量警报

这些警报表示存储消耗或容量压力。

警报名称	严重性	类型	问题描述
FabricPool 镜像复制重新同步已完成	严重、警告、信息	EMS	FabricPool 镜像重新同步过程已成功从主对象存储完成到镜像对象存储。
FabricPool 空间使用量已接近上限	严重、警告、信息	EMS	来自容量许可提供商的对象存储的总集群范围 FabricPool 空间使用量已接近许可限制。
FabricPool 空间使用量限制已达到	严重、警告、信息	EMS	来自容量许可提供商的对象存储的总集群范围 FabricPool 空间使用量已达到许可证限制。
节点根卷空间不足	严重、警告、信息	EMS	系统检测到根卷空间严重不足。
QoS监视器内存已达上限	严重、警告、信息	EMS	QoS子系统的动态内存已达到当前平台硬件的极限。
卷自动调整大小成功	严重、警告、信息	EMS	由于启用了自动卷增长，因此已自动调整卷的大小。
卷已满	关键	指标	此卷已满90%以上。释放空间或增加容量以防止写入失败。

配置警报

这些警报指向配置更改或库存更新。

警报名称	严重性	类型	问题描述
发现磁盘架电源	严重、警告、信息	EMS	磁盘架上增加了一个电源装置。
已创建卷	信息	指标	已创建卷。
卷已删除	警告	指标	已删除一个卷。
已修改卷	信息	指标	已修改卷。
WAFL 一致性检查已过期	警告	EMS	此聚合的 WAFL 一致性检查超过了每小时限制。

性能警报

这些警报指向延迟或节点性能问题。

警报名称	严重性	类型	问题描述
节点 NFS 延迟较高	关键	指标	此节点上的 NFS 操作遇到高延迟（>5000 us ）。
节点崩溃	严重、警告、信息	EMS	节点崩溃并重新启动。

保护警报

这些警报会影响复制、故障转移或恢复。

警报名称	严重性	类型	问题描述
扇出 SnapMirror 关系通用快照已删除	严重、警告、信息	EMS	作为 SnapMirror 同步重新同步或更新操作的一部分，较旧的 Snapshot 副本将被删除。
已添加 ONTAP Mediator	严重、警告、信息	EMS	ONTAP Mediator 已成功添加到此集群。
ONTAP Mediator CA 证书已过期	严重、警告、信息	EMS	ONTAP Mediator 证书颁发机构 (CA) 证书已过期。
ONTAP Mediator CA 证书即将过期	严重、警告、信息	EMS	ONTAP Mediator 证书颁发机构 (CA) 证书将在未来 30 天内过期。
ONTAP Mediator 客户端证书已过期	严重、警告、信息	EMS	ONTAP Mediator 客户端证书已过期。
ONTAP Mediator 客户端证书即将过期	严重、警告、信息	EMS	ONTAP Mediator 客户端证书将在未来 30 天内过期。
ONTAP Mediator 不可访问	严重、警告、信息	EMS	无法访问 ONTAP Mediator，原因是它已被重新调整用途，或者 Mediator 软件包不再安装。
ONTAP Mediator 已移除	严重、警告、信息	EMS	已成功从此集群中删除 ONTAP Mediator。
ONTAP Mediator 无法访问	严重、警告、信息	EMS	无法访问 ONTAP Mediator，这意味着在恢复连接之前无法执行 SnapMirror 故障转移。
ONTAP Mediator 服务器证书已过期	严重、警告、信息	EMS	ONTAP Mediator 服务器证书已过期。
ONTAP Mediator 服务器证书即将过期	严重、警告、信息	EMS	ONTAP Mediator 服务器证书将在未来 30 天内过期。
SnapMirror 活动同步关系不同步	严重、警告、信息	EMS	The SnapMirror 同步关系从同步变为不同步。数据保护受到影响。
SnapMirror 主动同步自动计划外故障转移已完成	严重、警告、信息	EMS	已完成 SnapMirror 业务连续性 (SMBC) 自动计划外故障转移操作。
SnapMirror active sync 自动计划外故障转移失败	严重、警告、信息	EMS	SnapMirror 业务连续性 (SMBC) 自动计划外故障转移操作失败。
SnapMirror 活动同步计划故障转移已完成	严重、警告、信息	EMS	已完成 SnapMirror 业务连续性 (SMBC) 计划的故障转移操作。
SnapMirror 活动同步计划故障转移失败	严重、警告、信息	EMS	SnapMirror 业务连续性 (SMBC) 计划的故障转移操作失败。
SnapMirror 关系公共 Snapshot 失败	严重、警告、信息	EMS	创建通用 Snapshot 副本失败。
SnapMirror 关系初始化失败	严重、警告、信息	EMS	SnapMirror initialize 命令失败，将不再尝试重试。
SnapMirror 关系不同步	严重、警告、信息	EMS	The SnapMirror 同步关系从同步变为不同步。数据保护受到影响。

警报名称	严重性	类型	问题描述
SnapMirror 关系重新同步尝试失败	严重、警告、信息	EMS	源卷和目标卷之间的 SnapMirror 同步尝试失败。
SnapMirror 关系快照未复制	严重、警告、信息	EMS	SnapMirror 同步关系的 Snapshot 副本未成功复制。

安全警报

这些警报指向威胁或未经授权的访问。

警报名称	严重性	类型	问题描述
检测到勒索软件活动	严重、警告、信息	EMS	为了保护数据免受检测到的勒索软件的侵害，已获取可用于还原原始数据的快照副本。
Storage VM 反勒索软件监控	严重、警告、信息	EMS	Storage VM 的反勒索软件状态已更改。
未经授权的用户访问管理员共享	严重、警告、信息	EMS	客户端尝试连接到特权 ONTAP_ADMIN$ 共享，但登录用户不属于此 SVM 上的任何活动 Vscan 扫描程序池。
卷反勒索软件监控	严重、警告、信息	EMS	卷的反勒索软件状态已更改。

NetApp Console 本地部署中的集群安全合规性类别

使用此参考可查看 NetApp Console 本地部署中显示的集群安全合规性类别，包括建议值以及每个类别是否影响整体合规性状态。

这些类别基于 ONTAP 安全态势检查。

类别	该类别检查的内容	建议值	影响整体合规性
全局 FIPS	是否启用 FIPS 140-2 模式。启用后，TLSv1 和 SSLv3 将被禁用，只允许 TLSv1.1 和 TLSv1.2。	已启用	是
Telnet	是否启用 Telnet 访问。SSH 是推荐的安全远程访问方法。	已禁用	是
不安全的 SSH 设置	SSH 是否配置了不安全的密码，例如以 `cbc` 开头的密码。	否	是
登录横幅	是否为系统访问配置登录横幅。	已启用	是
集群对等	对等集群之间的通信是否已加密。必须在源集群和目标集群上都启用加密。	已加密	是
网络时间协议	是否为集群配置了一个或多个 NTP 服务器。NetApp 建议至少配置三个 NTP 服务器以实现弹性。	已配置	是
OCSP	是否已为 SSL/TLS 证书验证启用在线证书状态协议验证。	已启用	否
远程审核日志记录	日志转发 (syslog) 是否已加密。	已加密	是

类别	该类别检查的内容	建议值	影响整体合规性
AutoSupport HTTPS 传输	是否将 HTTPS 用作 AutoSupport 消息的默认传输协议。	已启用	是
默认管理员用户	是否禁用内置默认admin帐户。	已禁用	是
SAML 用户	是否已将 SAML 配置为单点登录和支持 MFA 的身份验证。	否	否
Active Directory 用户	是否已为集群访问配置 Active Directory 身份验证。	否	否
LDAP 用户	是否为集群访问配置了 LDAP 身份验证。	否	否
证书用户	是否已为基于证书的用户配置集群登录。	否	否
本地用户	是否为集群登录配置了本地用户。	否	否
远程 shell	是否启用 RSH。SSH 是安全远程访问的首选方式。	已禁用	是
MD5 正在使用	ONTAP 用户帐户是否仍使用 MD5 哈希，而非更强的哈希（例如 SHA-512）。	否	是
证书颁发者类型	集群使用的证书颁发者类型。	CA 签名	否

Storage VM 安全合规性类别（NetApp Console 本地部署）

使用此参考可查看 NetApp Console 本地部署中显示的 Storage VM (SVM) 安全合规性类别，包括建议值以及每个类别是否影响整体合规性状态。

这些类别基于 ONTAP 安全态势检查。

类别	该类别检查的内容	建议值	影响整体合规性
审核日志	是否启用 SVM 审核日志记录。	已启用	是
不安全的 SSH 设置	SSH 是否配置了不安全的密码，例如以 `cbc` 开头的密码。	否	是
登录横幅	是否为访问 SVM 的用户配置登录横幅。	已启用	是
LDAP 加密	是否启用 LDAP 加密。	已启用	否
NTLM 身份验证	是否启用 NTLM 身份验证。	已启用	否
LDAP 负载签名	是否启用 LDAP 负载签名。	已启用	否
CHAP 设置	是否启用 CHAP。	已启用	否
Kerberos V5	是否启用 Kerberos V5 身份验证。	已启用	否
NIS 身份验证	是否配置了 NIS 身份验证。	已禁用	否
FPolicy 状态激活	FPolicy是否已创建并处于活动状态。	是	否
SMB 加密已启用	是否已启用 SMB 签名和密封。	是	否
SMB 签名已启用	是否启用 SMB 签名。	是	否

知识和支持

在 **NetApp Console** 本地部署中注册支持

此任务的 NetApp Console 本地部署信息。要获得特定于 NetApp Console 及其存储解决方案和数据服务的技术支持，需要进行支持注册。此外，还需要进行支持注册才能为 Cloud Volumes ONTAP 系统启用关键工作流程。

注册支持不会为云提供商文件服务启用 NetApp 支持。有关云提供商文件服务、其基础架构或使用该服务的任何解决方案的技术支持，请参阅该产品文档中的"获取帮助"。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

支持注册概述

激活支持权限有两种注册形式：

- 注册您的 NetApp Console 帐户序列号（您的 20 位 960xxxxxxxx 序列号位于 Console 的"支持资源"页面）。

  这可作为控制台内任何服务的单个支持订阅 ID。每个 Console 帐户都必须注册。

- 在云提供商的市场中注册与订阅关联的 Cloud Volumes ONTAP 序列号（这些是 20 位 909201xxxxxxxx 序列号）。

  这些序列号通常称为 *PAYGO* 序列号，在 Cloud Volumes ONTAP 部署时由 NetApp Console 生成。

注册这两种类型的序列号可以启用打开支持工单和自动生成案例等功能。通过将 NetApp 支持站点 (NSS) 帐户添加到 Console 来完成注册，如下所述。

注册 **NetApp Console** 以获得 **NetApp** 支持

要注册支持并激活支持授权，您的 NetApp Console 帐户中的一个用户必须将 NetApp Support Site 帐户与其 Console 登录相关联。如何注册 NetApp 支持取决于您是否已经拥有 NetApp Support Site (NSS) 帐户。

拥有 **NSS** 账号的现有客户

如果您是拥有 NSS 帐户的 NetApp 客户，只需通过 Console 注册即可获得支持。

步骤

1. 选择*管理* > 凭据。
2. 选择*用户凭据*。
3. 选择*添加 NSS 凭据*，然后按照 NetApp 支持站点 (NSS) 身份验证提示操作。
4. 要确认注册过程是否成功，请选择"帮助"图标，然后选择 **Support**。

   *资源*页面应显示您的 Console 帐户已注册以获得支持。

请注意，如果其他 Console 用户未将 NetApp 支持站点帐户与其登录名关联，则不会看到相同的支持注册状态。但是，这并不意味着您的帐户未注册支持。只要组织中有一个用户执行了这些步骤，您的帐户即已注册。

现有客户，但没有 **NSS** 帐户

如果您是拥有现有许可证和序列号但_no_ NSS 帐户的现有 NetApp 客户，则需要创建 NSS 帐户并将其与 Console 登录相关联。

步骤

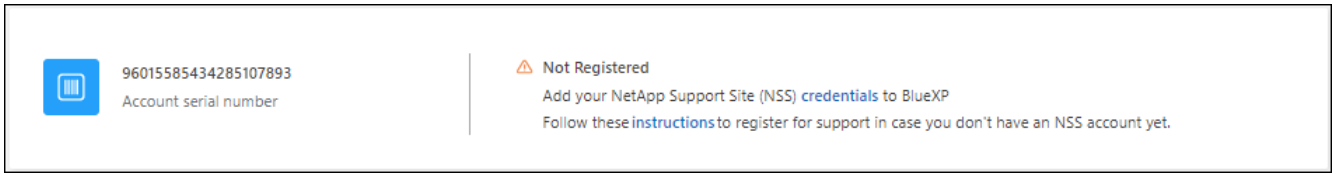
1. 通过完成以下步骤创建 NetApp 支持站点帐户： "NetApp 支持站点用户注册表单"
   a. 请务必选择适当的用户级别，通常为 **NetApp** 客户/最终用户。
   b. 请务必复制上面用于序列号字段的 Console 帐户序列号 (960xxxx)。这将加快账号处理速度。
2. 完成 拥有 NSS 账号的现有客户 下的步骤，将您的新 NSS 帐户与 Console 登录相关联。

全新接触 **NetApp**

如果您是首次接触 NetApp 且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在控制台右上角，选择帮助图标，然后选择*支持*。
2. 从支持注册页面找到您的帐户 ID 序列号。



3. 导航到 "NetApp 的支持注册站点"并选择 我不是注册 **NetApp** 客户。
4. 填写必填字段（带红色星号的字段）。
5. 在*产品线*字段中，选择 **Cloud Manager**，然后选择适用的计费提供商。
6. 复制上述第 2 步中的账号序列号，完成安全检查，然后确认您已阅读 NetApp 的《全球数据隐私政策》。

   电子邮件将立即发送到所提供的邮箱，以完成此安全交易。如果验证电子邮件未在几分钟内到达，请务必检查垃圾邮件文件夹。

7. 从电子邮件中确认操作。

   确认将您的请求提交到 NetApp，并建议您创建 NetApp 支持站点帐户。

8. 通过完成以下步骤创建 NetApp 支持站点帐户： "NetApp 支持站点用户注册表单"
   a. 请务必选择适当的用户级别，通常为 **NetApp** 客户/最终用户。
   b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这样可以加快处理速度。

完成后

NetApp 应在此过程中与您联系。这是针对新用户的一次性引导练习。

拥有 NetApp 支持站点帐户后，请完成 拥有 NSS 账号的现有客户 下的步骤，将该帐户与您的 Console 登录相关联。

将 **NSS** 凭据关联到 **Cloud Volumes ONTAP** 支持

将 NetApp 支持站点凭据与您的 Console 账户相关联，是启用以下 Cloud Volumes ONTAP 关键工作流所必需的：

- 注册按需付费的 Cloud Volumes ONTAP 系统以获得支持

  要激活对系统的支持并获得 NetApp 技术支持资源，需要提供您的 NSS 帐户。

- 自带许可证 (BYOL) 时部署 Cloud Volumes ONTAP

  需要提供您的 NSS 帐户，以便 Console 可以上传您的许可证密钥并启用您购买期限的订阅。这包括定期续订的自动更新。

- 将 Cloud Volumes ONTAP 软件升级到最新版本

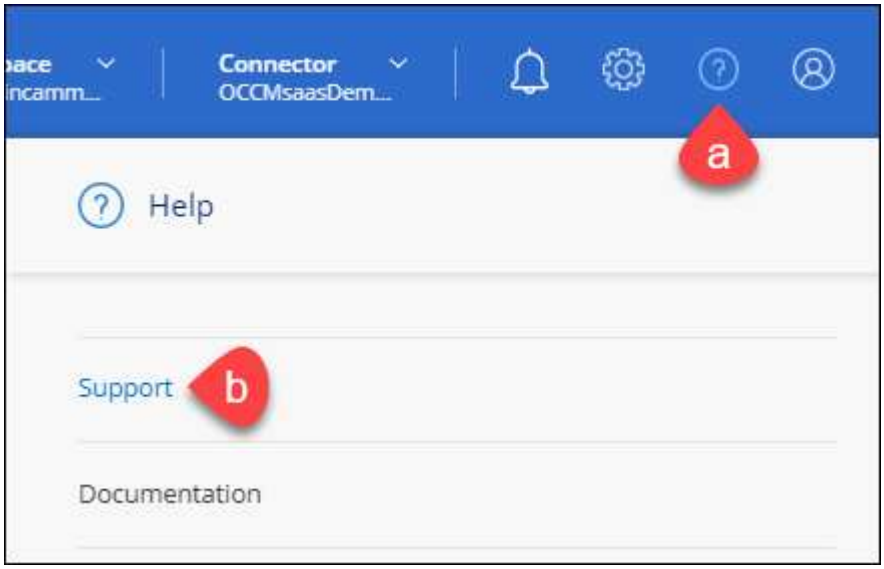
将 NSS 凭据与您的 NetApp Console 帐户关联不同于与 Console 用户登录关联的 NSS 帐户。

这些 NSS 凭据与您的特定 Console 帐户 ID 相关联。属于 Console 组织的用户可以从*支持 > NSS 管理*访问这些凭据。

- 如果您有客户级别的帐户，则可以添加一个或多个 NSS 帐户。
- 如果您有合作伙伴或经销商帐户，则可以添加一个或多个 NSS 帐户，但不能将其与客户级别的帐户一起添加。

步骤

1. 在控制台右上角，选择帮助图标，然后选择*支持*。



2. 选择 **NSS Management > Add NSS Account**。
3. 出现提示时，选择*继续*将重定向至 Microsoft 登录页面。

   NetApp 使用 Microsoft Entra ID 作为特定于支持和许可的身份验证服务的身份提供程序。

4. 在登录页面，提供您的 NetApp 支持站点注册的电子邮件地址和密码以执行身份验证过程。

   这些操作使 Console 能够使用您的 NSS 帐户进行许可证下载、软件升级验证和未来的支持注册。

   请注意以下事项：

   - NSS 账号必须为客户级账号（非访客或临时账号）。您可以拥有多个客户级别的 NSS 帐户。
   - 如果 NSS 账号是合作伙伴级别的账号，则只能有一个该账号。如果您尝试添加客户级别的 NSS 账号，并且存在合作伙伴级别的账号，则会收到以下错误消息：

     "此帐户不允许使用 NSS 客户类型，因为已存在不同类型的 NSS 用户。"

   如果您已有客户级别的 NSS 帐户，并尝试添加合作伙伴级别的帐户，情况也是如此。

   - 登录成功后，NetApp 将存储 NSS 用户名。

     这是一个系统生成的 ID，映射到您的电子邮件。在 **NSS Management** 页面上，您可以从 ••• 菜单中显示您的电子邮件。

   - 如果您需要刷新登录凭据令牌，••• 菜单中还有 **Update Credentials** 选项。

     使用此选项会提示您重新登录。请注意，这些帐户的令牌将在 90 天后过期。系统将发布通知以提醒您注意此事。

获取有关 **NetApp Console** 本地部署的帮助

NetApp Console 本地部署此任务的相关信息。NetApp 以多种方式为 NetApp Console 及其云服务提供支持。全天候 24x7 提供广泛的免费自助服务选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包括通过网络票务提供远程技术支持。

获取对云提供商文件服务的支持

有关云提供商文件服务、其基础架构或使用该服务的任何解决方案的技术支持，请参见该产品的文档。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

要获得特定于 NetApp 及其存储解决方案和数据服务的技术支持，请使用下面描述的支持选项。

使用自助服务选项

这些选项每周7天、每天24小时免费提供：

- 文档

  当前正在查看的 NetApp Console 文档。

- "知识库"

搜索 NetApp 知识库，查找解决问题的有用文章。

- "社区"

  加入 NetApp Console 社区，关注正在进行的讨论或创建新的讨论。

创建 **NetApp** 支持案例

除了上述自助服务选项之外，您还可以在激活支持后与 NetApp 支持专家合作解决任何问题。

在开始之前

- 要使用 创建案例 功能，您必须首先将您的 NetApp Support Site 凭据与您的 Console 登录相关联 "了解如何管理与 Console 登录关联的凭据"。
- 如果您要为具有序列号的 ONTAP 系统创建案例，则您的 NSS 帐户必须与该系统的序列号关联。

步骤

1. 在 NetApp Console 中，选择*帮助 > 支持*。
2. 在*资源*页面上，在"技术支持"下选择一个可用选项：

   a. 如果您想与他人通话，请选择*致电我们*。您将被引导到 netapp.com/cn 上的一个页面，其中列出了您可以拨打的电话号码。

   b. 选择 创建个案 以向 NetApp 支持专员提交工单：

      - 服务：选择问题关联的服务。例如，当特定于 Console 内工作流程或功能的技术支持问题时，请使用 **NetApp Console**。
      - 系统：如果适用于存储，请选择 **Cloud Volumes ONTAP** 或 **On-Prem**，然后选择相关的工作环境。

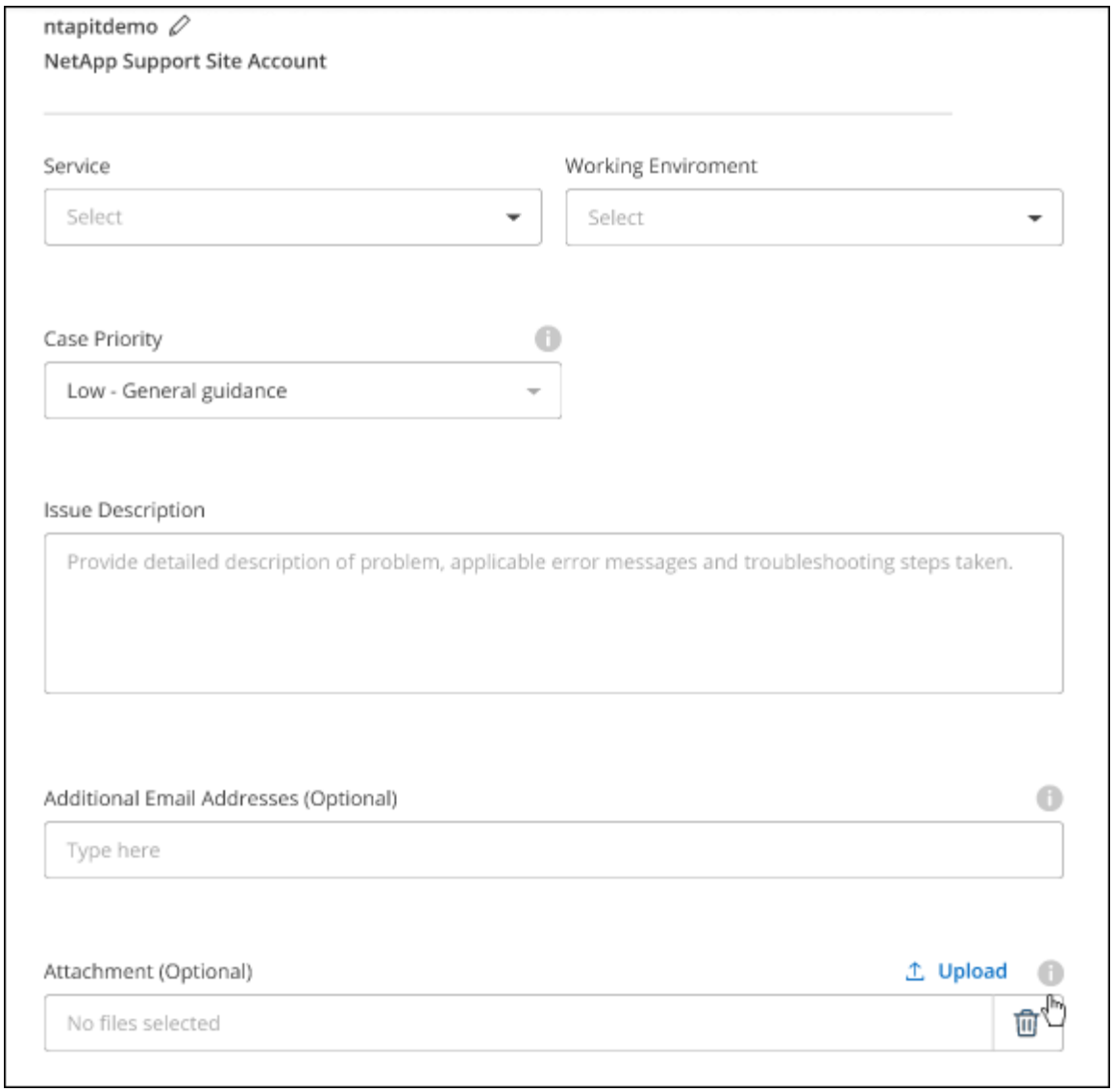
        系统列表在 Console 组织的范围内，以及您在顶部横幅中选择的 Console 代理。

      - **Case Priority**：选择案例的优先级，可以是低、中、高或严重。

        要了解有关这些优先级的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

      - 问题描述：请详细说明您的问题，包括任何适用的错误消息或您执行的故障排除步骤。
      - **Additional Email Addresses**：如果您想告知其他人此问题，请输入其他电子邮件地址。
      - 附件（可选）：上传最多五个附件，一次一个。

        每个文件的附件限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成后

此时会弹出一个窗口，其中包含您的支持案例编号。NetApp 支持专家将审查您的案例并尽快与您联系。

有关支持案例的历史记录，您可以选择*设置 > 时间轴*并查找名为"创建支持案例"的操作。通过最右侧的按钮，您可以展开操作以查看详细信息。

尝试创建个案时，您可能会遇到以下错误消息：

"您无权针对所选服务创建案例"

此错误可能意味着 NSS 帐户及其关联的记录公司与 NetApp Console 帐户序列号（即960xxxx）或工作环境序列号的记录公司不同。您可以使用以下选项之一寻求帮助：

- 在 https://mysupport.netapp.com/site/help提交非技术案例

管理您的支持案例

您可以直接从 Console 查看和管理进行中和已解决的支持个案。您可以管理与您的 NSS 帐户和公司相关的个案。

请注意以下事项：

- 页面顶端的个案管理控制面板提供两种视图：
  - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案例总数。
  - 右侧视图根据您的用户 NSS 帐户显示了贵公司在过去 3 个月内打开的案例总数。

  表格中的结果反映了与所选视图相关的案例。
- 您可以添加或删除感兴趣的列，也可以筛选优先级和状态等列的内容。其他列仅提供排序功能。

  有关更多信息，请查看以下步骤。
- 在个案级别，我们提供更新个案备注或关闭尚未处于"已关闭"或"待关闭"状态的个案的功能。

步骤

1. 在 NetApp Console 中，选择*帮助 > 支持*。
2. 选择 **Case Management**，如果出现提示，请将您的 NSS 账户添加到 Console。

   *个案管理*页面显示与您的 Console 用户账号关联的 NSS 账号相关的未结个案。这与 *NSS 管理*页面顶端显示的 NSS 账号相同。
3. （可选）修改此表中显示的信息：
   - 在*组织的案例*下，选择*查看*以查看与贵公司相关的所有案例。
   - 通过选择确切的日期范围或选择其他时间范围来修改日期范围。
   - 筛选列的内容。
   - 通过选择 然后选择要显示的列来更改表格中显示的列。
4. 通过选择 并选择一个可用选项来管理现有个案：
   - 查看个案：查看有关特定个案的完整详细信息。
   - 更新案例备注：提供有关您问题的其他详细信息，或选择*上传文件*以附加最多五个文件。

     每个文件的附件限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。
   - 关闭个案：请详细说明您关闭个案的原因，然后选择*关闭个案*。

NetApp Console 本地部署法律声明

NetApp Console 本地部署文档，适用于此页面。

法律声明提供对版权声明、商标、专利等信息的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 标识和 NetApp 商标页面上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

当前 NetApp 拥有的专利列表可以在以下网址找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关 NetApp 软件中使用的第三方版权和许可的信息。

"NetApp Console 通知"。