修正警报

NetApp Console local deployment

NetApp
August 10, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/console-local/concept-console-alerts.html on August 10, 2026. Always check docs.netapp.com for the latest.

目录

修正警报 1
了解 NetApp Console 本地部署中的警报 1
警报严重程度和影响区域 1
警报来源和范围 1
警报通知规则 1
监控和调查 NetApp Console 本地部署中的警报 2
可用警报 2
查看警报控制面板 2
查看所有提醒 3
按系统查看警报 3
调查警报 4
修正警报 4
分析警报 5
将警报导出为CSV 6
在 NetApp Console 本地部署中配置警报的通知规则 6
开始之前 7
查看通知规则 7
创建通知规则 7
启用或禁用通知规则 8
将通知规则静音 9
删除通知规则 9
相关信息 9
修正 NetApp Console 本地部署中的存储类偏移 10
补救漂移 10
相关信息 10
NetApp Console 本地部署中的警报修复操作 11
修复操作 11

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

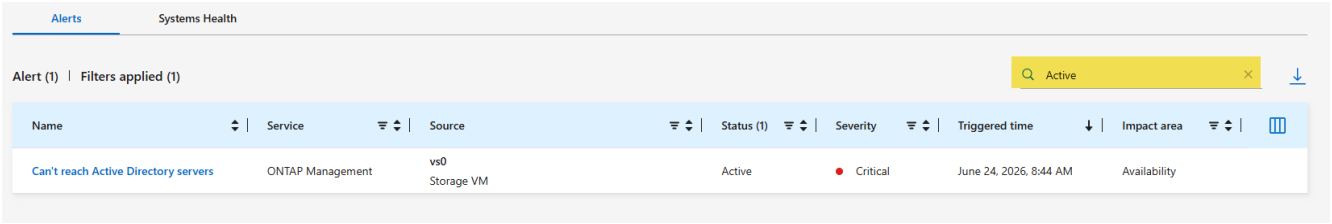
1. 选择 **Health > Alerts > Overview**。
2. 从范围选择器中，选择以下选项之一：
   - 全部（默认）以查看您有权访问的所有队列的警报
   - 仅可查看该队列警报的特定队列
3. 根据您需要查看的警报筛选仪表板，包括：
   - 严重程度（严重、警告或信息）
   - 按影响区域分组的关键警报
   - 影响区域（安全性、保护、可用性、性能、容量或配置）

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。

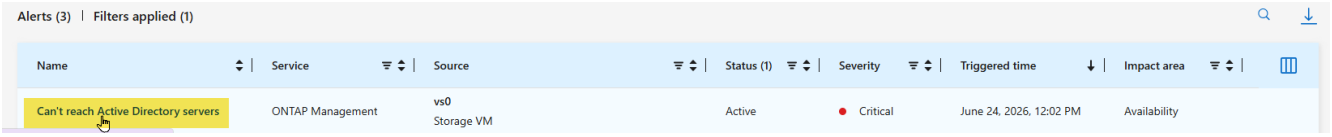
调查警报

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。

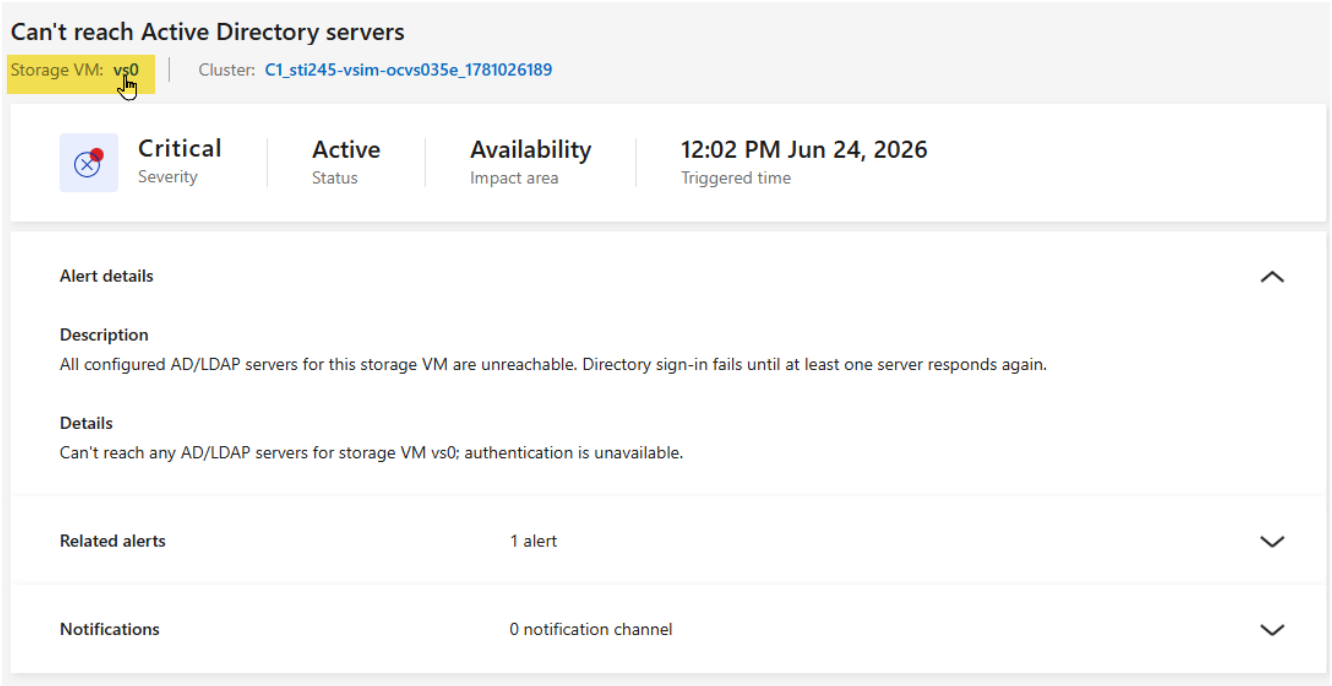
在调查 ONTAP 警报时，您还可以直接转到生成警报的系统的 System Manager 界面，以查看其他详细信息并采取相应措施。

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。

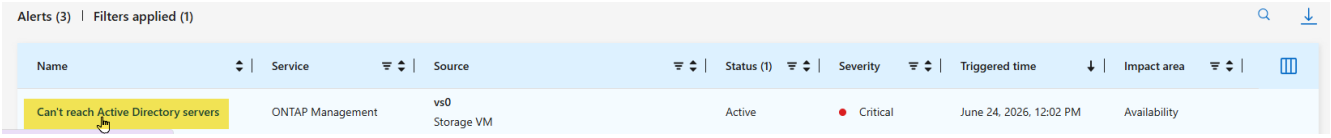
分析警报

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

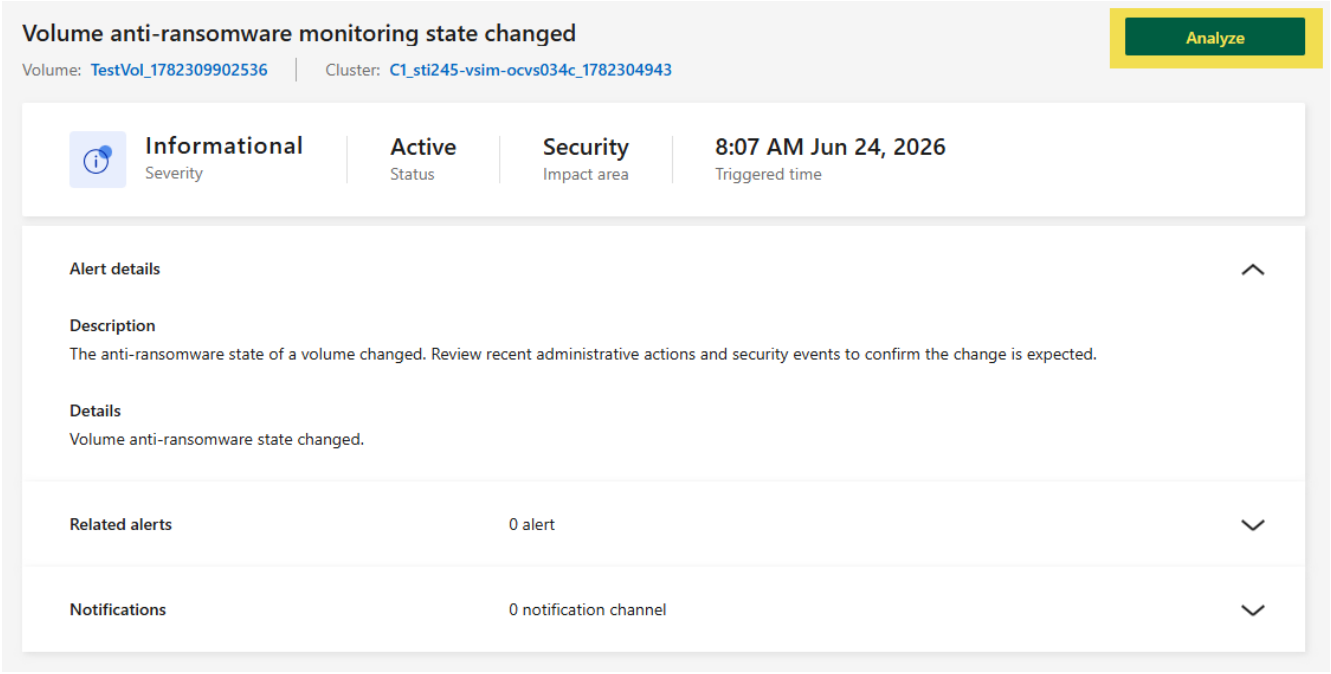
在调查 ONTAP 警报时，您还可以直接转到生成警报的系统的 System Manager 界面，以查看其他详细信息并采取相应措施。

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。

修正操作	警报名称	警报说明	影响区域	修正摘要
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。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 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。