事件、性能和运行状况监控
ONTAP 9

NetApp
September 12, 2024

目录

事件、性能和运行状况监控

使用System Manager监控集群性能

使用 System Manager 监控集群性能

本节中的主题介绍如何在 ONTAP 9.7 及更高版本中使用 System Manager 管理集群运行状况和性能。

您可以通过在 System Manager 信息板上查看有关系统的信息来监控集群性能。信息板可显示有关以下内容的信息：重要警报和通知，存储层和卷的效率和容量，集群中可用的节点， HA 对中节点的状态，最活跃的应用程序和对象， 以及集群或节点的性能指标。

通过信息板，您可以确定以下信息：

- * 运行状况 *： 集群的运行状况如何?
- * 容量 *： 集群上有哪些可用容量?
- * 性能 *： 根据延迟， IOPS 和吞吐量，集群的性能如何?
- * 网络 *： 如何为网络配置主机和存储对象，例如端口，接口和 Storage VM ？

在运行状况和容量概述中、您可以单击 → 以查看其他信息并执行任务。

在 " 性能概述 " 中，您可以按小时，天，周，月或年查看指标。

在网络概述中，将显示网络中每个对象的数量（例如， "8 个 NVMe/FC 端口 " ）。 您可以单击这些数字以查看有关每个网络对象的详细信息。

在System Manager信息板上查看集群概述

System Manager信息板可从一个位置快速全面地查看您的ONTAP集群。

使用System Manager信息板、您可以查看有关重要警报和通知、存储层和卷的效率和容量、集群中可用的节点、高可用性(HA)对中节点的状态、最活跃的应用程序和对象、 以及集群或节点的性能指标。

信息板包括四个面板、如下所述：

运行状况

运行状况视图可显示有关集群中所有可发现节点的整体运行状况信息。

此外、运行状况视图还会显示集群级别的错误和警告、例如未配置的节点详细信息、指示可以修改以提高集群性能的特征。

单击 → 以展开"Health"视图、以获取集群概况、例如集群名称、版本、集群创建日期和时间等。您还可以监控与集群关联的节点的运行状况相关的统计信息。您可以管理用于对环境中的资源进行分组和标识的标记。"洞察力"部分可帮助您优化系统的容量、安全合规性和配置。

Capacity

容量视图可显示集群的存储空间。您可以查看已用总逻辑空间、已用总物理空间和可用磁盘空间。

您可以选择向ActiveIQ注册以查看历史集群数据。单击 → 以展开容量视图、以查看与集群关联的层的概述。您可以查看有关每个层的容量信息：总空间、已用空间和可用空间。此时将显示吞吐量、IOPS和延迟的详细信息。"在System Manager中详细了解这些容量测量结果"(英文)

您可以使用容量视图选择添加本地层或云层。有关容量视图的详细信息、请参见 "查看集群的容量"。

网络

网络视图可显示网络中的物理端口、网络接口和Storage VM。

网络视图显示连接到网络的客户端的类型。其中每个网络连接客户端均由一个数字表示(例如、"NVMe/FC 16")。选择该数字可查看有关每个网络元素的特定详细信息。

单击 → 可查看涵盖网络上的端口、网络接口、Storage VM和主机的网络全屏视图。

性能

性能视图可显示性能统计信息、以帮助监控ONTAP集群的运行状况和效率。这些统计信息包括以图形表示的关键集群性能指标、例如延迟、吞吐量和IOPS。

性能视图按天、小时、周或年显示不同时间间隔的性能统计信息。您可以使用各种图形快速分析集群性能、并确定可能需要优化的特征。此快速分析可帮助您确定如何添加或移动工作负载。您还可以查看峰值使用时间以规划潜在的更改。

性能视图显示与延迟、吞吐量和IOPS相关的总性能指标。

从9.15.1开始、性能视图得到了增强、可显示与延迟、吞吐量和IOPS相关的读取、写入、其他和总性能指标的图形。其他指标包括任何不读取或写入的操作。

性能值每 3 秒刷新一次，性能图每 15 秒刷新一次。如果有关集群性能的信息不可用、则不会显示图形。

单击 ↙↗ 可按小时、天、周、月和年查看性能指标的全页视图。您还可以下载本地系统中的性能指标报告。

确定热卷和其他对象

通过识别经常访问的卷（热卷）和数据（热对象）来提高集群性能。

> ⓘ 从ONTAP 9.10.1开始、您可以使用文件系统分析中的活动跟踪功能监控卷中的热对象。

步骤

1. 单击 * 存储 > 卷 * 。
2. 筛选 IOPS ，延迟和吞吐量列以查看经常访问的卷和数据。

修改 **QoS**

从ONTAP 9.8开始、在配置存储时、 服务质量(QoS) 默认情况下处于启用状态。您可以在

配置过程中禁用 QoS 或选择自定义 QoS 策略。您也可以在配置存储后修改 QoS 。

步骤

1. 在System Manager中、依次选择*存储*和*卷*。
2. 在要修改QoS的卷旁边，选择，然后选择 ⋮ **Edit**。

监控风险

从 ONTAP 9.10.0 开始，您可以使用 System Manager 监控 Active IQ Digital Advisor 报告的风险。 从 ONTAP 9.10.1 开始，您还可以使用 System Manager 确认风险。

NetApp Active IQ Digital Advisor 报告了降低风险，提高存储环境性能和效率的机会。 借助 System Manager ，您可以了解 Active IQ 报告的风险，并获得可操作的智能信息，帮助您管理存储并实现更高的可用性，更高的安全性和更好的存储性能。

链接到您的 **Active IQ** 帐户

要从 Active IQ 接收有关风险的信息，您应首先从 System Manager 链接到您的 Active IQ 帐户。

步骤

1. 在 System Manager 中，单击 * 集群 > 设置 * 。
2. 在 * 注册 Active IQ * 下，单击 * 注册 * 。
3. 输入 Active IQ 的凭据。
4. 凭据通过身份验证后，单击 * 确认以将 Active IQ 与 System Manager* 链接起来。

查看风险数量

从 ONTAP 9.10.0 开始，您可以从 System Manager 的信息板查看 Active IQ 报告的风险数。

开始之前

您必须建立从 System Manager 到 Active IQ 帐户的连接。 请参见 链接到您的 Active IQ 帐户。

步骤

1. 在 System Manager 中，单击 * 信息板 * 。
2. 在 * 运行状况 * 部分中，查看报告的风险数量。

> 您可以通过单击显示风险数量的消息来查看有关每个风险的更多详细信息。 请参见 查看风险详细信息。

查看风险详细信息

从 ONTAP 9.10.0 开始，您可以从 System Manager 中查看 Active IQ 报告的风险如何按影响区域进行分类。 此外，您还可以查看有关每个已报告风险，其对系统的潜在影响以及可以采取的更正操作的详细信息。

开始之前

您必须建立从 System Manager 到 Active IQ 帐户的连接。 请参见 链接到您的 Active IQ 帐户。

步骤

1. 单击 * 事件 > 所有事件 * 。
2. 在 * 概述 * 部分的 * Active IQ 建议 * 下，查看每个影响区域类别中的风险数量。 风险类别包括：
   - 性能和效率
   - 可用性和保护
   - Capacity
   - Configuration
   - 安全性
3. 单击 * Active IQ suggestions * 选项卡可查看有关每个风险的信息，包括以下信息：
   - 对系统的影响级别
   - 风险的类别
   - 受影响的节点
   - 所需的缓解类型
   - 您可以采取的更正操作

确认风险

从 ONTAP 9.10.1 开始，您可以使用 System Manager 确认任何未结风险。

步骤

1. 在 System Manager 中，通过在中执行操作步骤来显示风险列表 查看风险详细信息。
2. 单击要确认的未结风险的风险名称。
3. 在以下字段中输入信息：
   - 提醒（日期）
   - 理由
   - 注释
4. 单击 * 确认 * 。

> 确认风险后，需要几分钟的时间才能将更改反映在 Active IQ 建议列表中。

取消确认风险

从 ONTAP 9.10.1 开始，您可以使用 System Manager 取消确认先前确认的任何风险。

步骤

1. 在 System Manager 中，通过在中执行操作步骤来显示风险列表 查看风险详细信息。
2. 单击要取消确认的已确认风险的风险名称。
3. 在以下字段中输入信息：
   - 理由

- 注释

4. 单击 * 取消确认 * 。

取消确认风险后，需要几分钟的时间才能将更改反映在 Active IQ 建议列表中。

System Manager洞察力

从ONTAP 9.11.1开始、System Manager将显示_洞察力_、帮助您优化系统的性能和安全性。

要查看、自定义和响应洞察力、请参见 "获得洞察力，帮助优化您的系统"

容量洞察力

System Manager可以根据系统中的容量状况显示以下见解：

洞察力	severity	条件	修复
本地层缺少空间	修复风险	一个或多个本地层已达到95%以上、并且增长迅速。现有工作负载可能无法增长、或者在极端情况下、现有工作负载可能会用尽空间并发生故障。	建议修复：执行以下选项之一。 • 清除卷恢复队列。 • 在厚配置卷上启用精简配置、以释放陷阱存储。 • 将卷移动到另一本地层。 • 删除不需要的Snapshot副本。 • 删除卷中不需要的目录或文件。 • 启用Fabric Pool以将数据分层到云。
应用程序缺少空间	需要关注	一个或多个卷的容量已超过95%、但未启用自动增长。	建议：启用自动增长、最多可达到当前容量的150%。 其他选项： • 通过删除Snapshot副本回收空间。 • 调整卷大小。 • 删除目录或文件。
FlexGroup卷的容量不平衡	优化存储	一个或多个FlexGroup卷的成分卷大小随着时间的推移增长不平衡、从而导致容量使用不平衡。 如果成分卷已满、则可能会发生写入失败。	建议：重新平衡FlexGroup卷。

Storage VM即将用尽容量	优化存储	一个或多个Storage VM接近其最大容量。 如果Storage VM达到最大容量、您将无法为新卷或现有卷配置更多空间。	建议：如果可能、增加Storage VM的最大容量限制。

安全洞察

System Manager可显示以下见解、以应对可能危及数据或系统安全的情况。

洞察力	severity	条件	修复
卷仍处于反勒索软件学习模式	需要关注	一个或多个卷已处于反勒索软件学习模式90天。	建议：为这些卷启用反勒索软件活动模式。
已在卷上启用Snapshot副本自动删除	需要关注	已在一个或多个卷上启用Snapshot自动删除。	建议：禁用Snapshot副本自动删除功能。否则、在发生勒索软件攻击时、可能无法恢复这些卷的数据。
卷没有Snapshot策略	需要关注	一个或多个卷未附加足够的Snapshot策略。	建议：将Snapshot策略附加到没有此策略的卷。否则、在发生勒索软件攻击时、可能无法恢复这些卷的数据。
未配置本机FPolicy	最佳实践	未在一个或多个NAS Storage VM上配置本机FPolicy。	建议：重要：阻止扩展可能会导致意外结果。从9.11.1开始、您可以为Storage VM启用本机FPolicy、从而阻止已知用于勒索软件攻击的3000多个文件扩展名。"配置本机FPolicy"在NAS Storage VM中、用于控制允许或不允许在环境中的卷上写入的文件扩展名。
已启用Telnet	最佳实践	应使用安全Shell (SSH)进行安全远程访问。	建议：禁用Telnet并使用SSH进行安全远程访问。
配置的NTP服务器太少	最佳实践	为NTP配置的服务器数量小于3。	建议：至少将三个NTP服务器与集群相关联。 否则、集群时间同步可能会出现问题。
已启用远程Shell (RSH)	最佳实践	应使用安全Shell (SSH)进行安全远程访问。	建议：禁用RSH并使用SSH进行安全远程访问。
未配置登录横幅	最佳实践	没有为集群和/或Storage VM配置登录消息。	建议：设置集群和Storage VM的登录横幅并启用其使用。

AutoSupport正在使用非安全协议	最佳实践	AutoSupport未配置为通过HTTPS进行通信。	建议：强烈建议使用HTTPS作为默认传输协议、以便向技术支持发送AutoSupport消息。
默认管理员用户未锁定	最佳实践	没有人使用默认管理帐户(admin或diag)登录、这些帐户不会锁定。	建议：在不使用默认管理帐户时将其锁定。
安全Shell (SSH)正在使用非安全加密	最佳实践	当前配置使用非安全CBC加密。	建议：您应在Web服务器上仅允许使用安全加密来保护与访问者的安全通信。删除名称包含"CBC"的加密、例如"ais128-CBC"、"aes192-CBC"、"AES256-CBC"和"3DES-CBC"。
已禁用全局FIPS 140-2合规性	最佳实践	已在集群上禁用全局FIPS 140-2合规性。	建议：出于安全原因、您应启用符合FIPS 140-2的全局加密法、以确保ONTAP可以安全地与外部客户端或服务器客户端进行通信。
不会监控卷的勒索软件攻击	需要关注	已在一个或多个卷上禁用反勒索软件。	建议：在卷上启用反勒索软件。否则、您可能无法注意到卷何时受到威胁或攻击。
没有为Storage VM配置反勒索软件	最佳实践	一个或多个Storage VM未配置反勒索软件保护。	建议：在Storage VM上启用反勒索软件。否则、您可能无法注意到Storage VM何时受到威胁或攻击。

配置洞察

System Manager可以显示以下见解、以解决有关系统配置的问题。

洞察力	severity	条件	修复
没有为集群配置通知	最佳实践	未将电子邮件、webhook或SNMP陷阱主机配置为接收有关集群问题的通知。	建议：为集群配置通知。
集群未配置自动更新。	最佳实践	集群尚未配置为接收最新磁盘认证包、磁盘固件、磁盘架固件和SP/BMC固件文件(如果有)的自动更新。	建议：启用此功能。

集群固件不是最新版本	最佳实践	您的系统没有最新的固件更新、此更新可能会提供一些改进、安全修补程序或新功能、以帮助保护集群、从而提高性能。	建议：更新ONTAP固件。

获得洞察力，帮助优化您的系统

借助System Manager、您可以查看有助于优化系统的洞察力。

关于此任务

从 ONTAP 9.11.0 开始，您可以在 System Manager 中查看有助于优化系统容量和安全性合规性的见解。

从ONTAP 9.11.1开始、您可以查看更多见解、帮助您优化系统的容量、安全合规性和配置。

> *阻止扩展可能会导致意外结果。*从ONTAP 9.11.1开始、您可以使用System Manager为Storage VM启用本机FPolicy。您可能会收到一条System Manager Insight消息、建议您这样做 "配置本机FPolicy" Storage VM。
>
> 使用FPolicy本机模式、您可以允许或禁止特定的文件扩展名。System Manager建议使用在过去的勒索软件攻击中使用的3000多个不允许的文件扩展名。 其中一些扩展名可能会被环境中的合法文件使用、阻止它们可能会导致意外问题。
>
> 因此、强烈建议您修改扩展名列表以满足环境的需求。请参见 "如何使用System Manager从System Manager创建的本机FPolicy配置中删除文件扩展名以重新创建策略"。
>
> 要了解有关本机FPolicy的更多信息，请参见"Fpolicy配置类型"。

根据最佳实践，这些洞察将显示在一个页面上，您可以从中启动即时操作来优化您的系统。有关每个Insight的更多详细信息、请参见 "System Manager洞察力"。

查看优化洞察

步骤

1. 在 System Manager 中，单击左侧导航列中的 * 见解 * 。

   "* 见解 * " 页面显示了多组见解。 每组见解可能包含一个或多个见解。 此时将显示以下组：

   - 需要您的关注
   - 修复风险
   - 优化存储

2. (可选)单击页面右上角的以下按钮、筛选显示的洞察力：

   - 显示与安全相关的洞察信息。
   - 显示与容量相关的洞察信息。

- 显示与配置相关的洞察信息。
- All 显示所有见解。

响应洞察，优化您的系统

在 System Manager 中，您可以通过以下方式对见解做出响应：将见解弃用，探索修复问题的不同方法或启动修复问题的过程。

步骤

1. 在 System Manager 中，单击左侧导航列中的 * 见解 * 。
2. 将鼠标悬停在某个洞察上可显示用于执行以下操作的按钮：
   - * 取消 * ： 从视图中删除此洞察力。 要 "`取消消除` " 洞察，请参见 [customize-settings-insights]。
   - * 探索 * ： 找到各种方法来修复 Insight 中提到的问题。 只有当存在多种修复方法时，才会显示此按钮。
   - * 修复 * ： 启动修复 Insight 中提及的问题的过程。系统将要求您确认是否要采取应用此修复程序所需的操作。

> 其中一些操作可以从 System Manager 的其他页面启动，但 * 见解 * 页面可通过从该页面启动这些操作来帮助您简化日常任务。

自定义设置以获得洞察力

您可以自定义要在System Manager中通知您的见解。

步骤

1. 在 System Manager 中，单击左侧导航列中的 * 见解 * 。
2. 在页面右上角，单击 ⋮，然后选择*Settings*。
3. 在 * 设置 * 页面上，确保选中要获得通知的见解旁边的复选框。 如果您之前取消了某个 Insight ，则可以 "`undismiss` " ，方法是确保选中其复选框。
4. 单击 * 保存 * 。

将这些洞察导出为**PDF**文件

您可以将所有适用的洞察力导出为PDF文件。

步骤

1. 在 System Manager 中，单击左侧导航列中的 * 见解 * 。
2. 在页面右上角，单击 ⋮，然后选择*Export*。

配置本机**FPolicy**

从ONTAP 9.11.1开始、当您收到System Manager Insight建议实施本机FPolicy时、您可以在Storage VM和卷上对其进行配置。

开始之前

访问System Manager洞察力时、在*应用最佳实践*下、您可能会收到一条消息、指出未配置本机FPolicy。

要了解有关FPolicy配置类型的更多信息，请参见"FPolicy 配置类型"。

步骤

1. 在 System Manager 中，单击左侧导航列中的 * 见解 * 。
2. 在*应用最佳实践*下，找到*未配置本机FPolicy *。
3. 在采取措施之前、请阅读以下消息：

> *阻止扩展可能会导致意外结果。*从ONTAP 9.11.1开始、您可以使用System Manager为Storage VM启用本机FPolicy。
> 使用FPolicy本机模式、您可以允许或禁止特定的文件扩展名。System Manager建议使用在过去的勒索软件攻击中使用的3000多个不允许的文件扩展名。 其中一些扩展名可能会被环境中的合法文件使用、阻止它们可能会导致意外问题。
>
> 因此、强烈建议您修改扩展名列表以满足环境的需求。请参见 "如何使用System Manager从System Manager创建的本机FPolicy配置中删除文件扩展名以重新创建策略"。

4. 单击*Fix*。
5. 选择要应用本机FPolicy的Storage VM。
6. 对于每个Storage VM、选择要接收本机FPolicy的卷。
7. 单击 * 配置 * 。

使用命令行界面监控和管理集群性能

性能监控和管理概述

您可以设置基本的性能监控和管理任务、并确定和解决常见的性能问题。

如果以下假设适用于您的情况、您可以使用以下过程来监控和管理集群性能：

- 您希望使用最佳实践，而不是浏览每个可用选项。
- 除了 ONTAP 命令行界面之外，您还希望使用 Active IQ Unified Manager （以前称为 OnCommand Unified Manager ）显示系统状态和警报，监控集群性能并执行根本原因分析。
- 您正在使用ONTAP命令行界面配置存储服务质量(QoS)。此外、还可以通过以下方式使用QoS：
  - System Manager
  - ONTAP REST API
  - 适用于 VMware vSphere 的 ONTAP 工具
  - NetApp服务级别管理器(NSLM)
  - OnCommand Workflow Automation (WFA)
- 您希望使用虚拟设备安装 Unified Manager ，而不是使用基于 Linux 或 Windows 的安装。
- 您愿意使用静态配置而不是 DHCP 来安装软件。

- 您可以在高级权限级别访问 ONTAP 命令。
- 您是具有 "admin" 角色的集群管理员。

相关信息

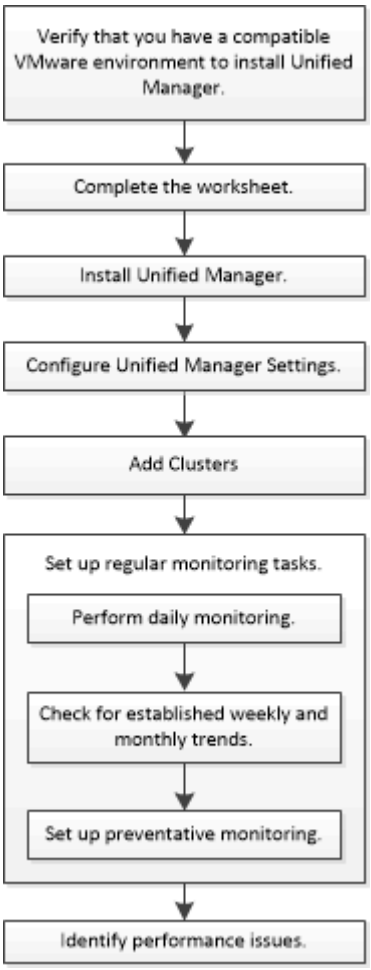
如果这些假设与您的情况不符，您应查看以下资源：

- "Active IQ Unified Manager 9.8 安装"
- "系统管理"

监控性能

性能监控和维护工作流概述

监控和维护集群性能涉及安装Active IQ Unified Manager软件、设置基本监控任务、确定性能问题以及根据需要进行调整。



验证您的 **VMware** 环境是否受支持

要成功安装Active IQ Unified Manager 、您必须验证您的VMware环境是否满足必要的要求。

步骤

1. 验证您的 VMware 基础架构是否满足 Unified Manager 安装的规模估算要求。
2. 转至 "互操作性表" 验证是否支持以下组件的组合：
   - ONTAP 版本
   - ESXi 操作系统版本
   - VMware vCenter Server 版本
   - VMware Tools 版本
   - 浏览器类型和版本

   > http://mysupport.netapp.com/matrix["互操作性表"^]列出了Unified Manager支持的配置。

3. 单击选定配置的配置名称。

   该配置的详细信息将显示在配置详细信息窗口中。

4. 查看以下选项卡中的信息：
   - 注释：

     列出特定于您的配置的重要警报和信息。

   - 策略和准则

     提供所有配置的一般准则。

Active IQ Unified Manager 工作表

在安装，配置和连接 Active IQ Unified Manager 之前，您应准备好有关环境的特定信息。您可以将此信息记录在工作表中。

Unified Manager 安装信息

部署了软件的虚拟机	您的价值
ESXi 服务器 IP 地址	
主机完全限定域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	

主 DNS 地址	
二级 DNS 地址	
搜索域	
维护用户名	
维护用户密码	

Unified Manager 配置信息

正在设置 …	您的价值
维护用户电子邮件地址	
NTP服务器	
SMTP 服务器主机名或 IP 地址	
SMTP用户名	
SMTP密码	
SMTP 默认端口	25 （默认值）
发送警报通知的电子邮件	
LDAP 绑定可分辨名称	
LDAP 绑定密码	
Active Directory 管理员名称	
Active Directory password	
身份验证服务器基本可分辨名称	
身份验证服务器主机名或 IP 地址	

集群信息

捕获 Unified Manager 上每个集群的以下信息。

N 的集群 1	您的价值
主机名或集群管理 IP 地址	
ONTAP 管理员用户名 必须已为管理员分配 "admin" 角色。	
ONTAP 管理员密码	
协议（HTTP 或 HTTPS）	

相关信息

"管理员身份验证和 RBAC"

安装 **Active IQ Unified Manager**

下载并部署 **Active IQ Unified Manager**

要安装此软件，您必须下载虚拟设备（VA）安装文件，然后使用 VMware vSphere Client 将此文件部署到 VMware ESXi 服务器。此 VA 可通过 OVA 文件提供。

步骤

1. 转至 **NetApp** 支持站点软件下载 页面并找到 Active IQ Unified Manager。

   https://mysupport.netapp.com/products/index.html

2. 在 * 选择平台 * 下拉菜单中选择 * VMware vSphere *，然后单击 * 执行！ *
3. 将"`OVA`"文件保存到VMware vSphere Client可访问的本地或网络位置。
4. 在 VMware vSphere Client 中，单击 * 文件 * > * 部署 OVF 模板 *。
5. 找到"`OVA`"文件、然后使用向导在ESXi服务器上部署虚拟设备。

   您可以使用向导中的 * 属性 * 选项卡输入静态配置信息。

6. 启动虚拟机。
7. 单击 * 控制台 * 选项卡以查看初始启动过程。
8. 按照提示在虚拟机上安装 VMware Tools。
9. 配置时区。
10. 输入维护用户名和密码。
11. 转到 VM 控制台显示的 URL。

配置初始 **Active IQ Unified Manager** 设置

首次访问 Web UI 时，将显示 Active IQ Unified Manager 初始设置对话框，您可以通过此

对话框配置一些初始设置并添加集群。

步骤

1. 接受默认的 AutoSupport enabled 设置。
2. 输入 NTP 服务器详细信息，维护用户电子邮件地址， SMTP 服务器主机名和其他 SMTP 选项，然后单击 * 保存 * 。

完成后

初始设置完成后，将显示集群数据源页面，您可以在其中添加集群详细信息。

指定要监控的集群

您必须将集群添加到 Active IQ Unified Manager 服务器中，才能监控集群，查看集群发现状态以及监控其性能。

您需要的内容

- 您必须具有以下信息：
  - 主机名或集群管理 IP 地址

    主机名是 Unified Manager 用于连接到集群的完全限定域名 （ FQDN ） 或简称。此主机名必须解析为集群管理 IP 地址。

  集群管理 IP 地址必须是管理 Storage Virtual Machine （ SVM ） 的集群管理 LIF 。如果使用节点管理 LIF ，则操作将失败。

  - ONTAP 管理员用户名和密码
  - 可以在集群上配置的协议类型（ HTTP 或 HTTPS ） 以及集群的端口号
- 您必须具有应用程序管理员或存储管理员角色。
- ONTAP 管理员必须具有 ONTAPI 和 SSH 管理员角色。
- Unified Manager FQDN 必须能够对 ONTAP 执行 ping 操作。

  您可以使用ONTAP命令对此进行验证 `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*。

关于此任务

对于 MetroCluster 配置，必须同时添加本地和远程集群，并且必须正确配置这些集群。

步骤

1. 单击 * 配置 * > * 集群数据源 * 。
2. 在集群页面中，单击 * 添加 * 。
3. 在 * 添加集群 * 对话框中，指定所需的值，例如集群的主机名或 IP 地址（ IPv4 或 IPv6 ），用户名，密码，通信协议和端口号。

   默认情况下， HTTPS 协议处于选中状态。

您可以将集群管理 IP 地址从 IPv6 更改为 IPv4 或从 IPv4 更改为 IPv6 。下一个监控周期完成后，新 IP 地址将反映在集群网格和集群配置页面中。

4. 单击 * 添加 * 。
5. 如果选择 HTTPS ，请执行以下步骤：

   a. 在 * 授权主机 * 对话框中，单击 * 查看证书 * 以查看有关集群的证书信息。
   b. 单击 * 是 * 。

      Unified Manager 仅在首次添加集群时才会检查证书，但不会在每次对 ONTAP 进行 API 调用时检查该证书。

   如果证书已过期，则无法添加集群。您必须续订 SSL 证书，然后添加集群。

6. * 可选 * ：查看集群发现状态：

   a. 从 * 集群设置 * 页面查看集群发现状态。

   集群将在默认监控间隔约为 15 分钟后添加到 Unified Manager 数据库中。

设置基本监控任务

执行每日监控

您可以执行每日监控，以确保没有任何需要关注的即时性能问题。

步骤

1. 从 Active IQ Unified Manager UI 中，转到 * 事件清单 * 页面以查看所有当前事件和已废弃事件。
2. 从*view*选项中，选择 `Active Performance Events` 并确定需要执行的操作。

使用每周和每月性能趋势来确定性能问题

通过分析卷延迟，确定性能趋势有助于确定集群是否过度使用或未充分利用。您可以使用类似的步骤来确定 CPU ，网络或其他系统瓶颈。

步骤

1. 找到您怀疑使用不足或过度使用的卷。
2. 在 * 卷详细信息 * 选项卡上，单击 * 。 30 d* 以显示历史数据。
3. 在 " 细分数据依据 " 下拉菜单中，选择 * 延迟 * ，然后单击 * 提交 * 。
4. 在集群组件比较图表中取消选择 * 聚合 * ，然后将集群延迟与卷延迟图表进行比较。
5. 选择 * 聚合 * 并取消选择集群组件比较图表中的所有其他组件，然后将聚合延迟与卷延迟图表进行比较。
6. 将读取 / 写入延迟图表与卷延迟图表进行比较。
7. 确定客户端应用程序负载是否已导致工作负载争用，并根据需要重新平衡工作负载。
8. 确定聚合是否已过度使用并根据需要引发资源争用和重新平衡工作负载。

使用性能阈值生成事件通知

事件是指发生预定义条件或性能计数器值超过阈值时 Active IQ Unified Manager 自动生成的通知。事件可帮助您确定要监控的集群中的性能问题。您可以将警报配置为在发生某些严重性类型的事件时自动发送电子邮件通知。

设置性能阈值

您可以设置性能阈值以监控关键性能问题。当系统接近或超过定义的阈值时，用户定义的阈值将触发警告或严重事件通知。

步骤

1. 创建警告和严重事件阈值：
   a. 选择 * 配置 * > * 性能阈值 * 。
   b. 单击 * 创建 * 。
   c. 选择对象类型并指定策略的名称和问题描述。
   d. 选择对象计数器条件并指定用于定义警告和严重事件的限制值。
   e. 选择要发送的事件必须违反限制值的持续时间，然后单击 * 保存 * 。
2. 将阈值策略分配给存储对象。
   a. 转至先前选择的同一集群对象类型的 " 清单 " 页面，然后从 " 视图 " 选项中选择 * 性能 * 。
   b. 选择要将阈值策略分配到的对象，然后单击 * 分配阈值策略 * 。
   c. 选择先前创建的策略，然后单击 * 分配策略 * 。

示例

您可以设置用户定义的阈值以了解关键性能问题。例如、如果您使用的是Microsoft Exchange Server、并且您知道如果卷延迟超过20毫秒、它将崩溃、则可以将警告阈值设置为12毫秒、将严重阈值设置为15毫秒。使用此阈值设置，您可以在卷延迟超过限制时收到通知。

添加警报

您可以配置警报，以便在生成特定事件时向您发出通知。您可以为单个资源，一组资源或特定严重性类型的事件配置警报。您可以指定通知频率，并将脚本与警报关联。

您需要的内容

- 您必须已配置通知设置，例如用户电子邮件地址， SMTP 服务器和 SNMP 陷阱主机，以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。
- 您必须了解要触发警报的资源和事件，以及要通知的用户的用户名或电子邮件地址。
- 如果要根据事件执行脚本，则必须已使用脚本页面将脚本添加到 Unified Manager 中。
- 您必须具有应用程序管理员或存储管理员角色。

关于此任务

除了从 "Alert Setup" 页面创建警报之外，您还可以在收到事件后直接从 "Event Details" 页面创建警报，如下所述。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 警报设置 * 。
2. 在 * 警报设置 * 页面中，单击 * 添加 * 。
3. 在 * 添加警报 * 对话框中，单击 * 名称 * ，然后输入警报的名称和问题描述。
4. 单击 * 资源 * ，然后选择要包含在警报中或从警报中排除的资源。

   您可以通过在 * 名称包含 * 字段中指定文本字符串来设置筛选器，以选择一组资源。根据您指定的文本字符串，可用资源列表仅显示与筛选器规则匹配的资源。指定的文本字符串区分大小写。

   如果某个资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除的资源相关的事件生成警报。

5. 单击 * 事件 * ，然后根据要触发警报的事件名称或事件严重性类型选择事件。

   要选择多个事件，请在选择时按 Ctrl 键。

6. 单击 * 操作 * ，然后选择要通知的用户，选择通知频率，选择是否将 SNMP 陷阱发送到陷阱接收方，并分配生成警报时要执行的脚本。

   如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则 " 名称 " 字段将显示为空，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果您从用户页面修改了选定用户的电子邮件地址，则不会为选定用户更新修改后的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 * 保存 * 。

添加警报的示例

此示例显示了如何创建满足以下要求的警报：

- 警报名称： HealthTest
- 资源：包括名称包含 "abc" 的所有卷，并排除名称包含 "xyz" 的所有卷
- 事件：包括所有严重运行状况事件
- 操作：包括 sample@domain.com ，一个 "Test" 脚本，必须每 15 分钟通知一次用户

在添加警报对话框中执行以下步骤：

1. 单击*名称*、然后输入 `HealthTest` 在*警报名称*字段中。
2. 单击 * 资源 * ，然后在包括选项卡中，从下拉列表中选择 * 卷 * 。
   a. 输入 … `abc` 在*名称包含*字段中、以显示名称包含abc的卷。
   b. 选择 * +[All Volumes whose name contains 'abc']从 "Available Resources" 区域中选择 +* ，然后将其移动到 "Selected Resources" 区域。

c. 单击*排除*、然后输入 `xyz` 在*名称包含*字段中、然后单击*添加*。

3. 单击 * 事件 * ，然后从事件严重性字段中选择 * 严重 * 。
4. 从匹配事件区域中选择 * 所有严重事件 * ，然后将其移动到选定事件区域。
5. 单击*操作*、然后输入 `sample@domain.com` 在向这些用户发送警报字段中。
6. 选择 * 每 15 分钟提醒一次 * 以每 15 分钟通知一次用户。

   您可以将警报配置为在指定时间内向收件人重复发送通知。您应确定警报的事件通知处于活动状态的时间。

7. 在 Select Script to Execute 菜单中，选择 * 测试 * 脚本。
8. 单击 * 保存 * 。

配置警报设置

您可以指定 Active IQ Unified Manager 中的哪些事件触发警报，这些警报的电子邮件收件人以及警报频率。

您需要的内容

您必须具有应用程序管理员角色。

关于此任务

您可以为以下类型的性能事件配置唯一的警报设置：

- 违反用户定义的阈值触发的严重事件
- 因违反用户定义的阈值，系统定义的阈值或动态阈值而触发的警告事件

默认情况下，对于所有新事件，系统会向 Unified Manager 管理员用户发送电子邮件警报。您可以通过添加其他用户的电子邮件地址向这些用户发送电子邮件警报。

> 要禁止针对某些类型的事件发送警报，必须清除事件类别中的所有复选框。此操作不会阻止事件显示在用户界面中。

步骤

1. 在左侧导航窗格中，选择 * 存储管理 * > * 警报设置 * 。

   此时将显示 "Alert Setup" 页面。

2. 单击 * 添加 * 并为每个事件类型配置适当的设置。

   要将电子邮件警报发送给多个用户，请在每个电子邮件地址之间输入一个逗号。

3. 单击 * 保存 * 。

确定 **Active IQ Unified Manager** 中的性能问题

如果发生性能事件，您可以在 Active IQ Unified Manager 中找到问题描述的源并使用其他工具进行修复。您可能会收到事件的电子邮件通知，也可能会在日常监控期间注意到事件。

步骤

1. 单击电子邮件通知中的链接，可直接转到发生性能事件的存储对象。

如果您 …	那么 …
接收事件的电子邮件通知	单击此链接可直接转到事件详细信息页面。
在分析 " 事件清单 " 页面时，请注意此事件	选择事件以直接转到事件详细信息页面。

2. 如果事件已超过系统定义的阈值，请按照 UI 中的建议操作对问题描述进行故障排除。
3. 如果事件已超过用户定义的阈值，请分析此事件以确定是否需要采取措施。
4. 如果问题描述仍然存在，请检查以下设置：
   - 存储系统上的协议设置
   - 任何以太网或网络结构交换机上的网络设置
   - 存储系统上的网络设置
   - 存储系统上的磁盘布局和聚合指标
5. 如果此问题描述仍然存在，请联系技术支持以获得帮助。

使用 **Active IQ Digital Advisor** 查看系统性能

对于向NetApp发送AutoSupport 遥测的任何ONTAP 系统、您都可以查看大量性能和容量数据。Active IQ 显示系统性能的时间比您在 System Manager 中看到的时间长。

您可以查看 CPU 利用率，延迟， IOPS ，按协议划分的 IOPS 以及网络吞吐量的图形。您也可以下载 .csv 格式的数据，以便在其他工具中进行分析。

除了这些性能数据之外， Active IQ 还可以按工作负载向您显示存储效率，并将该效率与此类工作负载的预期效率进行比较。您可以查看容量趋势、并查看在给定时间范围内可能需要添加的额外存储量的估计值。

- 存储效率可在主信息板左侧的客户，集群和节点级别使用。
- 主信息板左侧提供集群和节点级别的性能。

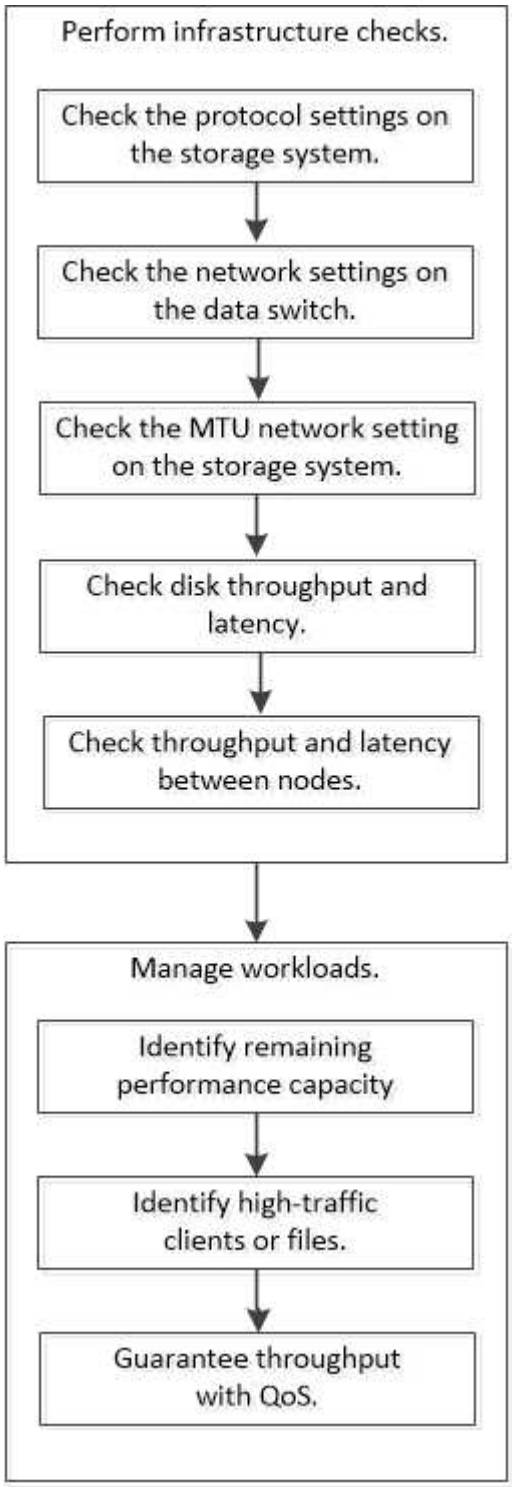
相关信息

- "Active IQ Digital Advisor 文档"
- "Active IQ Digital Advisor 视频播放列表"
- "Active IQ Web 门户"

管理性能问题

性能管理工作流

确定性能问题描述后，您可以对基础架构执行一些基本诊断检查，以排除明显的配置错误。如果这些问题无法确定问题所在，您可以开始查看工作负载管理问题。



执行基本基础架构检查

检查存储系统上的协议设置

检查 **NFS TCP** 最大传输大小

对于 NFS ，您可以检查读取和写入的 TCP 最大传输大小是否可能导致性能问题描述。如果您认为大小正在降低性能，则可以提高性能。

您需要的内容

- 要执行此任务，您必须具有集群管理员权限。
- 您必须对此任务使用高级权限级别命令。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 检查 TCP 最大传输大小：

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. 如果 TCP 最大传输大小太小，请增加大小：

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

以下示例将更改的TCP最大传输大小 `SVM1` 至1048576：

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

检查 **iSCSI TCP** 读 **/** 写大小

对于 iSCSI ，您可以检查 TCP 读 / 写大小以确定大小设置是否正在创建性能问题描述。如果此大小是问题描述的源，则可以更正此大小。

您需要的内容

此任务需要高级权限级别命令。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 检查 TCP 窗口大小设置：

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. 修改 TCP 窗口大小设置：

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. 返回到管理权限：

```
set -privilege admin
```

示例

以下示例将更改的TCP窗口大小 `SVM1` 到131、400字节：

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

检查 **CIFS** 多路传输设置

如果 CIFS 网络性能较慢导致出现性能问题描述，您可以修改多路传输设置以改进和更正它。

步骤

1. 检查 CIFS 多路传输设置：

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. 修改 CIFS 多路传输设置：

   ```
   vserver cifs options modify –vserver -vserver_name –max-mpx integer
   ```

示例

以下示例将更改上的最大传输计数 `SVM1` 到255：

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

检查 **FC** 适配器端口速度

适配器目标端口速度应与所连接设备的速度匹配，以优化性能。如果端口设置为自动协商，则在接管和交还或其他中断后，重新连接可能需要较长时间。

您需要的内容

使用此适配器作为主端口的所有 LIF 都必须脱机。

步骤

1. 使适配器脱机：

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. 检查端口适配器的最大速度：

   ```
   fcp adapter show -instance
   ```

3. 根据需要更改端口速度：

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. 使适配器联机：

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. 使适配器上的所有 LIF 联机：

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

示例

以下示例更改了适配器的端口速度 `0d` 开启 `node1` 至2 Gbps：

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

检查数据交换机上的网络设置

尽管您必须在客户端，服务器和存储系统（即网络端点）上保持相同的 MTU 设置，但 NIC 和交换机等中间网络设备应设置为其最大 MTU 值，以确保性能不会受到影响。

为了获得最佳性能，网络中的所有组件都必须能够转发巨型帧（包括以太网在内的 9000 字节 IP ， 9022 字节）。数据交换机应至少设置为 9022 字节，但对于大多数交换机，典型值可能为 9216 。

操作步骤

对于数据交换机，请检查 MTU 大小是否设置为 9022 或更高。

有关详细信息，请参见交换机供应商文档。

检查存储系统上的 **MTU** 网络设置

如果存储系统上的网络设置与客户端或其他网络端点上的网络设置不同，则可以更改这些设置。管理网络 MTU 设置为 1500 ，而数据网络 MTU 大小应为 9000 。

关于此任务

广播域中的所有端口都具有相同的 MTU 大小，但处理管理流量的 e0M 端口除外。如果端口属于广播域、请使用 `broadcast-domain modify` 命令以更改修改后的广播域中所有端口的MTU。

请注意， NIC 和数据交换机等中间网络设备可以设置为比网络端点更大的 MTU 大小。有关详细信息，请参见 "检查数据交换机上的网络设置"。

步骤

1. 检查存储系统上的 MTU 端口设置：

```
network port show -instance
```

2. 更改端口所使用的广播域上的MTU：

   network port broadcast-domain modify -ipspace *ipspace* -broadcast-domain *broadcast_domain* -mtu *new _mtu*

示例

以下示例将MTU端口设置更改为9000：

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

检查磁盘吞吐量和延迟

您可以检查集群节点的磁盘吞吐量和延迟指标，以帮助您进行故障排除。

关于此任务

此任务需要高级权限级别命令。

步骤

1. 更改为高级权限级别：

   set -privilege advanced

2. 检查磁盘吞吐量和延迟指标：

   statistics disk show -sort-key latency

示例

以下示例显示的每个用户读取或写入操作的总数 `node2` 开启 `cluster1`：

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

您可以使用 `network test-path` 用于确定网络瓶颈或对节点之间的网络路径进行预先资格认定的命令。您可以在集群间节点或集群内节点之间运行命令。

您需要的内容

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限级别命令。
- 对于集群间路径，源集群和目标集群必须建立对等关系。

关于此任务

有时，节点之间的网络性能可能无法满足路径配置的预期。例如，在 SnapMirror 复制操作中，对于这种大型数据传输， 1 Gbps 的传输速率与源集群和目标集群之间的 10 GbE 链路不一致。

您可以使用 `network test-path` 用于测量节点间吞吐量和延迟的命令。您可以在集群间节点或集群内节点之间运行命令。

> 此测试会将网络路径与数据饱和，因此，您应在系统不繁忙以及节点之间的网络流量不大时运行此命令。测试在 10 秒后超时。此命令只能在 ONTAP 9 节点之间运行。

。 `session-type` 选项用于标识您正在通过网络路径运行的操作类型，例如，用于将SnapMirror复制到远程目标的“AsyncMirrorRemote”。类型决定了测试中使用的数据量。下表定义了会话类型：

会话类型	Description
AsyncMirrorLocal	SnapMirror在同一集群中的节点之间使用的设置
AsyncMirrorRemote	SnapMirror在不同集群中的节点之间使用的设置(默认类型)
RemoteDataTransfer	ONTAP 用于在同一集群中的节点之间远程访问数据的设置(例如、向节点发出NFS请求、请求存储在另一节点上的卷中的文件)

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 测量节点之间的吞吐量和延迟：

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   源节点必须位于本地集群中。目标节点可以位于本地集群或对等集群中。的值为"local" `-source-node` 指定要运行命令的节点。

以下命令用于测量之间SnapMirror类型复制操作的吞吐量和延迟 `node1` 在本地集群上、然后 `node3` 开启 `cluster2`：

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
Min latency in ms:  61.14
Max latency in ms:  3056.86
```

3. 返回到管理权限：

   ```
   set -privilege admin
   ```

完成后

如果性能不符合路径配置的预期，则应检查节点性能统计信息，使用可用工具隔离网络中的问题，检查交换机设置等。

管理工作负载

确定剩余性能容量

性能容量（或 _余 量 _ ）用于衡量在资源上的工作负载性能开始受到延迟影响之前，您可以在节点或聚合上执行多少工作。了解集群上的可用性能容量有助于您配置和平衡工作负载。

您需要的内容

此任务需要高级权限级别命令。

关于此任务

您可以对使用以下值 `-object` 用于收集和显示性能余量统计信息的选项：

- 对于CPU、 `resource_headroom_cpu`。
- 对于聚合、 `resource_headroom_aggr`。

您也可以使用 System Manager 和 Active IQ Unified Manager 完成此任务。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 开始实时性能余量统计信息收集：

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

   有关完整的命令语法，请参见手册页。

3. 显示实时性能余量统计信息：

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   有关完整的命令语法，请参见手册页。

4. 返回到管理权限：

   ```
   set -privilege admin
   ```

示例

以下示例显示了集群节点的平均每小时性能余量统计信息。

您可以通过减去来计算节点的可用性能容量 `current_utilization` 中的计数器 `optimal_point_utilization` 计数器。在此示例中、是的利用率容量 `CPU_sti2520-213` 为-14%(72% -86%)、表示CPU在过去一小时的平均利用率过高。

您可以指定 `ewma_daily`， `ewma_weekly``或 `ewma_monthly` 以获取较长时间段内的相同信息的平均值。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                current_utilization                               86
                  optimal_point_ops                             2573
              optimal_point_latency                             3589
           optimal_point_utilization                              72
     optimal_point_confidence_factor                               1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                current_utilization                                 0
                  optimal_point_ops                                 0
              optimal_point_latency                                 0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                               1
2 entries were displayed.
```

确定高流量客户端或文件

您可以使用 ONTAP 活动对象技术来确定造成集群流量过大的客户端或文件。确定这些 " 排名前 " 的客户端或文件后，您可以重新平衡集群工作负载或执行其他步骤来解决问题描述。

您需要的内容

您必须是集群管理员才能执行此任务。

步骤

1. 查看访问集群的前几个客户端：

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   有关完整的命令语法，请参见手册页。

   以下命令显示访问的前几个客户端 `cluster1`：

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                                 *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. 查看在集群上访问的前几个文件：

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   有关完整的命令语法，请参见手册页。

   以下命令显示在上访问的前几个文件 `cluster1`：

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

通过 **QoS** 保证吞吐量

QoS 概述保证吞吐量

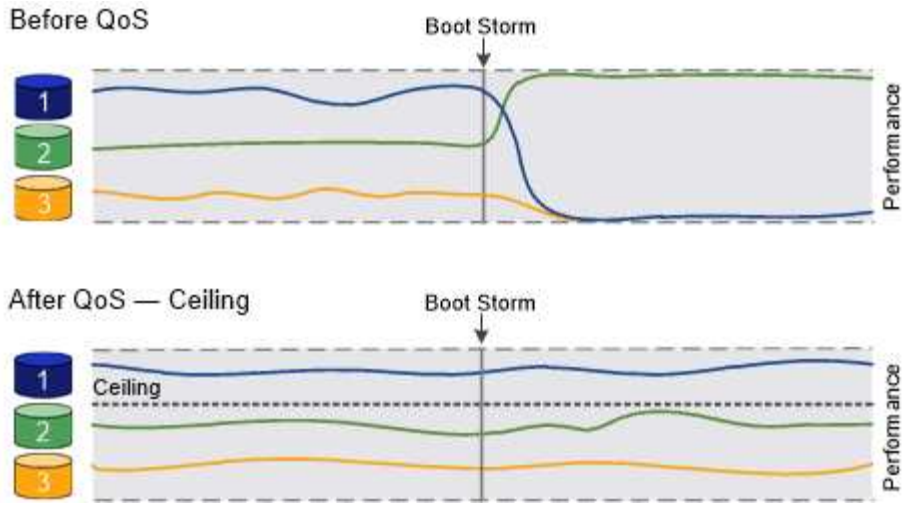
您可以使用存储服务质量（QoS）来保证关键工作负载的性能不会因争用资源的工作负载而降级。您可以为争用资源的工作负载设置吞吐量上限，以限制其对系统资源的影响，也可以为关键工作负载设置吞吐量上限，以确保满足最小吞吐量目标，而不管争用资源的工作负载有何需求。您甚至可以为同一工作负载设置上限和下限。

关于吞吐量上限（**QoS** 最大值）

吞吐量上限会将工作负载的吞吐量限制为最大 IOPS 或 MBps 数，或者 IOPS 和 MBps 数。在下图中，工作负载 2 的吞吐量上限可确保它不会 " 抢占 " 工作负载 1 和 3 。

策略组定义了一个或多个工作负载的吞吐量上限。工作负载表示 _storage 对象： _ 卷，文件， qtree 或 LUN ，或者 SVM 中的所有卷，文件， qtree 或 LUN 的 I/O 操作。您可以在创建策略组时指定上限，也可以等到监控工作负载之后再指定上限。

> 工作负载的吞吐量可能会超出指定上限 10% ，尤其是在工作负载的吞吐量发生快速变化时。要处理突发事件，上限可能会超过 50% 。令牌累积率高达 150% 时，单个节点上发生突发



关于吞吐量下限（ **QoS** 最小值）

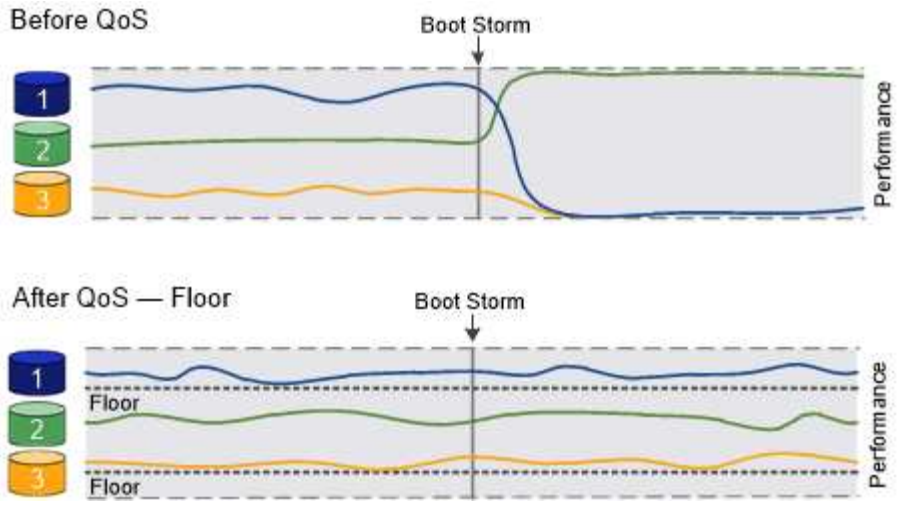
吞吐量下限可确保工作负载的吞吐量不会低于最小IOPS或MBps数或IOPS和MBps数。在下图中，工作负载 1 和工作负载 3 的吞吐量下限可确保满足最小吞吐量目标，而不管工作负载 2 的需求如何。

> 如示例所示，吞吐量上限会直接限制吞吐量。吞吐量下限会优先考虑设置了下限的工作负载，从而间接限制吞吐量。

您可以在创建策略组时指定下限，也可以等到监控工作负载之后再指定下限。

从ONTAP 9.13.1开始、您可以使用在SVM范围设置吞吐量下限 [adaptive-qos-templates]。在9.13.1之前的ONTAP 版本中、定义吞吐量下限的策略组不能应用于SVM。

> 在 ONTAP 9.7 之前的版本中，如果有足够的可用性能容量，则可以保证吞吐量下限。
>
> 在 ONTAP 9.7 及更高版本中，即使可用性能容量不足，也可以保证吞吐量下限。这种新的楼层行为称为 Floor v2 。为了满足保证要求，对于没有吞吐量下限的工作负载或超出下限设置的工作负载， Floor v2 可能会导致延迟更高。第 2 层适用场景 QoS 和自适应 QoS 。
>
> ONTAP 9.7P6及更高版本提供了启用/禁用楼层v2新行为的选项。在执行关键操作(如)期间、工作负载可能会低于指定的下限 `volume move trigger-cutover`。即使有足够的可用容量且未执行关键操作，工作负载的吞吐量也可能会低于指定下限 5% 。如果楼层配置过度，并且没有性能容量，则某些工作负载可能会低于指定的楼层。



关于共享和非共享 **QoS** 策略组

从 ONTAP 9.4 开始，您可以使用 *non-shared* QoS 策略组分别指定每个成员工作负载的已定义吞吐量上限或下限适用场景。*shared* 策略组的行为取决于策略类型：

- 对于吞吐量上限，分配给共享策略组的工作负载的总吞吐量不能超过指定的上限。
- 对于吞吐量下限，共享策略组只能应用于单个工作负载。

关于自适应 **QoS**

通常，分配给存储对象的策略组值是固定的。当存储对象的大小发生变化时，您需要手动更改此值。例如，增加卷上的已用空间量通常需要相应地增加为卷指定的吞吐量上限。

Adaptive QoS 会自动将策略组值扩展到工作负载大小，并在工作负载大小发生变化时保持 IOPS 与 TBSGB 的比率。如果您要在大型部署中管理数百或数千个工作负载，则这是一项显著优势。

通常，您可以使用自适应 QoS 来调整吞吐量上限，但也可以使用它来管理吞吐量下限（当工作负载大小增加时）。工作负载大小表示为存储对象分配的空间或存储对象使用的空间。

> 在 ONTAP 9.5 及更高版本中，已用空间可用于吞吐量下限。在 ONTAP 9.4 及更早版本中，吞吐量下限不支持此功能。

- 已分配空间策略会根据存储对象的标称大小保持 IOPS/TBGB 比率。如果此比率为 100 IOPS/GB ，则只要 150 GB 卷保持此大小，其吞吐量上限将为 15 ， 000 IOPS 。如果将卷大小调整为 300 GB ，则自适应 QoS 会将吞吐量上限调整为 30 ， 000 IOPS 。
- 已用空间策略（默认值）会根据存储效率之前存储的实际数据量保持 IOPS/TBGB 比率。如果此比率为 100 IOPS/GB ，则存储了 100 GB 数据的 150 GB 卷的吞吐量上限为 10 ， 000 IOPS 。随着已用空间量的变化，自适应 QoS 会根据比率调整吞吐量上限。

从 ONTAP 9.5 开始，您可以为应用程序指定 I/O 块大小，以便以 IOPS 和 MBps 为单位表示吞吐量限制。MBps 限制是通过块大小乘以 IOPS 限制计算得出的。例如，如果 I/O 块大小为 32 K ，而 IOPS 限制为 6144IOPS/TB ，则 MBps 限制为 192 MBps 。

吞吐量上限和下限均会出现以下行为：

- 将工作负载分配给自适应 QoS 策略组后，上限或下限将立即更新。

- 调整自适应 QoS 策略组中的工作负载大小后，上限或下限大约会在五分钟内更新。

在进行更新之前，吞吐量必须至少增加 10 IOPS 。

自适应 QoS 策略组始终为非共享组：定义的吞吐量上限或每个成员工作负载的下限适用场景。

从ONTAP 9.6开始、采用SSD的ONTAP Select 高级版支持吞吐量下限。

自适应策略组模板

从ONTAP 9.13.1开始、您可以在SVM上设置自适应QoS模板。通过自适应策略组模板、您可以为SVM中的所有卷设置吞吐量下限和上限。

只有在创建SVM之后、才能设置自适应策略组模板。使用 `vserver modify` 命令 `-qos-adaptive-policy-group-template` 参数以设置策略。

设置自适应策略组模板时、在设置策略后创建或迁移的卷会自动继承策略。分配策略模板时、SVM上现有的任何卷不受影响。如果在SVM上禁用此策略、则此后迁移到SVM或在此SVM上创建的任何卷都不会收到此策略。禁用自适应策略组模板不会影响继承策略模板的卷、因为它们会保留策略模板。

有关详细信息，请参见 设置自适应策略组模板。

常规支持

下表显示了在支持吞吐量上限，吞吐量下限和自适应 QoS 方面的差异。

资源或功能	吞吐量上限	吞吐量下限	吞吐量下限 **v2**	自适应 **QoS**
ONTAP 9 版本	全部	9.2及更高版本	9.7及更高版本	9.3及更高版本
平台	全部	• AFF • C190 * • 采用 SSD * 的 ONTAP Select 高级版	• AFF • C190 • 采用 SSD 的 ONTAP Select 高级版	全部
协议	全部	全部	全部	全部
FabricPool	是的。	是，如果分层策略设置为 " 无 " 且云中没有块。	是，如果分层策略设置为 " 无 " 且云中没有块。	否
SnapMirror 同步	是的。	否	否	是的。

从ONTAP 9.6版开始支持C190和ONTAP Select。

支持的工作负载达到吞吐量上限

下表按 ONTAP 9 版本显示了工作负载对吞吐量上限的支持。不支持根卷，负载共享镜像和数据保护镜像。

工作负载支持—上限	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8及更高版本
Volume	是的。	是的。	是的。	是的。	是的。	是的。
文件	是的。	是的。	是的。	是的。	是的。	是的。
LUN	是的。	是的。	是的。	是的。	是的。	是的。
SVM	是的。	是的。	是的。	是的。	是的。	是的。
FlexGroup 卷	否	否	否	是的。	是的。	是的。
qtree*	否	否	否	否	否	是的。
每个策略组具有多个工作负载	是的。	是的。	是的。	是的。	是的。	是的。
非共享策略组	否	否	否	否	是的。	是的。

从ONTAP 9.8开始、在启用了NFS的FlexVol和FlexGroup卷中的qtrees支持NFS访问。从 ONTAP 9.1.1 开始，启用了 SMB 的 FlexVol 和 FlexGroup 卷的 qtree 也支持 SMB 访问。

支持吞吐量下限的工作负载

下表按 ONTAP 9 版本显示了吞吐量下限的工作负载支持。不支持根卷，负载共享镜像和数据保护镜像。

工作负载支持—楼层	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 - 9.13.0	ONTAP 9.13.1及更高版本
Volume	是的。	是的。	是的。	是的。	是的。
文件	否	是的。	是的。	是的。	是的。
LUN	是的。	是的。	是的。	是的。	是的。
SVM	否	否	否	否	是的。
FlexGroup 卷	否	否	是的。	是的。	是的。
qtree *	否	否	否	是的。	是的。
每个策略组具有多个工作负载	否	否	是的。	是的。	是的。
非共享策略组	否	否	是的。	是的。	是的。

*从ONTAP 9.8开始、在启用了NFS的FlexVol 和FlexGroup 卷中的qtrees支持NFS访问。从 ONTAP 9.1.1 开始，启用了 SMB 的 FlexVol 和 FlexGroup 卷的 qtree 也支持 SMB 访问。

自适应 **QoS** 支持的工作负载

下表显示了 ONTAP 9 版本对自适应 QoS 的工作负载支持。不支持根卷，负载共享镜像和数据保护镜像。

工作负载支持—自适应 **QoS**	**ONTAP 9.3**	**ONTAP 9.4 - 9.13.0**	**ONTAP 9.13.1**及更高版本
Volume	是的。	是的。	是的。
文件	否	是的。	是的。
LUN	否	是的。	是的。
SVM	否	否	是的。
FlexGroup 卷	否	是的。	是的。
每个策略组具有多个工作负载	是的。	是的。	是的。
非共享策略组	是的。	是的。	是的。

工作负载和策略组的最大数量

下表按 ONTAP 9 版本显示了工作负载和策略组的最大数量。

工作负载支持	**ONTAP 9.3**及更早版本	**ONTAP 9.4**及更高版本
每个集群的最大工作负载数	12、000	40、000
每个节点的最大工作负载数	12、000	40、000
最大策略组数	12、000	12、000

启用或禁用吞吐量下限 **v2**

您可以在 AFF 上启用或禁用吞吐量下限 v2 。默认值为 enabled 。如果启用了楼层 v2 ，则在控制器大量使用时，以其他工作负载更高的延迟为代价，可以满足吞吐量下限。第 2 层适用场景 QoS 和自适应 QoS 。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 输入以下命令之一：

如果您要 ...	使用以下命令：
禁用楼层 v2	`qos settings throughput-floors-v2 -enable false`

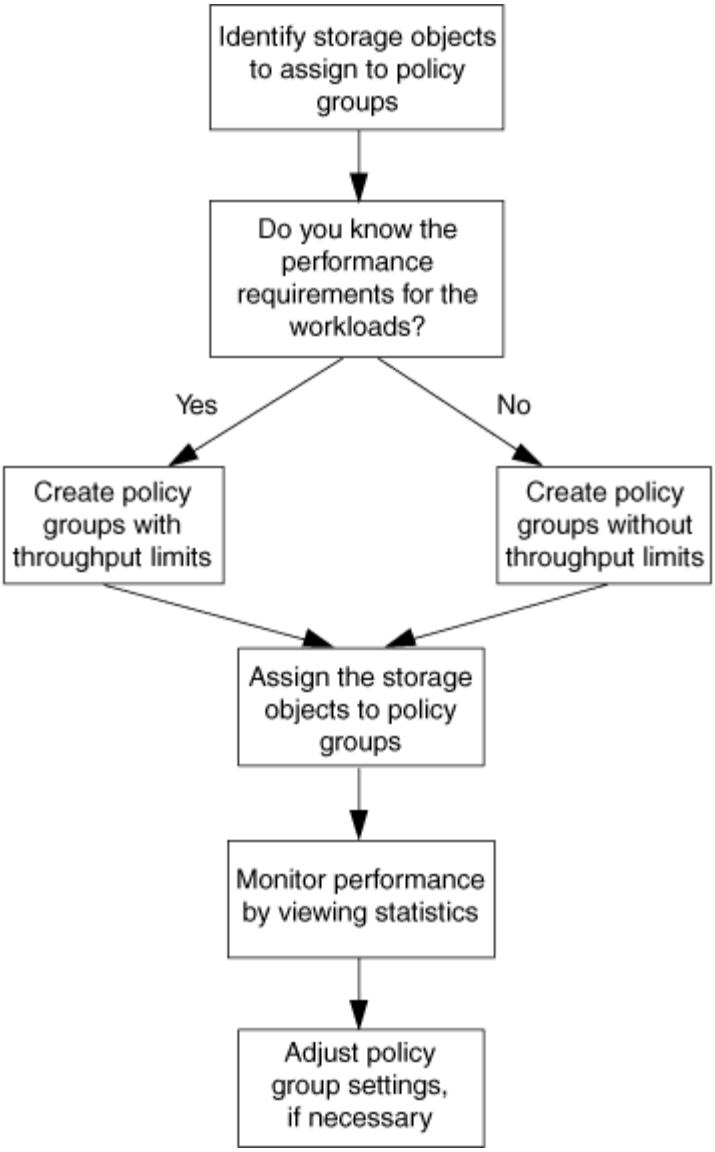
如果您要 ...	使用以下命令：
启用楼层 v2	`qos settings throughput-floors-v2 -enable true`

> 要在 MetroCluster 集群中禁用吞吐量下限 v2 ，必须运行
>
> `qos settings throughput-floors-v2 -enable false`
>
> 命令。

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

存储 **QoS** 工作流

如果您已经知道要使用 QoS 管理的工作负载的性能要求，则可以在创建策略组时指定吞吐量限制。否则，您可以等到监控工作负载之后再指定限制。



使用 **QoS** 设置吞吐量上限

您可以使用 `max-throughput` 用于定义存储对象工作负载吞吐量上限(QoS最大值)的策略组字段。您可以在创建或修改存储对象时应用策略组。

您需要的内容

- 您必须是集群管理员才能创建策略组。
- 要将策略组应用于 SVM ，您必须是集群管理员。

关于此任务

- 从 ONTAP 9.4 开始，您可以使用 *non-shared* QoS 策略组来指定定义的吞吐量上限适用场景每个成员工作负载。否则，策略组为 _shared： _ 分配给策略组的工作负载的总吞吐量不能超过指定的上限。

  设置 `-is-shared=false` 。 `qos policy-group create` 用于指定非共享策略组的命令。

- 您可以指定 IOPS ， MB/ 秒或 IOPS ， MB/ 秒上限的吞吐量限制如果同时指定 IOPS 和 MB/ 秒，则会强制执行首先达到的限制。

> 如果为同一工作负载设置了上限和下限，则只能以 IOPS 为单位指定上限的吞吐量限制。

- 受 QoS 限制的存储对象必须包含在策略组所属的 SVM 中。多个策略组可以属于同一个 SVM 。
- 如果某个存储对象的包含对象或子对象属于某个策略组，则不能将该存储对象分配给该策略组。
- QoS 最佳实践是将策略组应用于相同类型的存储对象。

步骤

1. 创建策略组。

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   有关完整的命令语法，请参见手册页。您可以使用 `qos policy-group modify` 用于调整吞吐量上限的命令。

   以下命令将创建共享策略组 `pg-vs1` 最大吞吐量为5、000次IOPS：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   以下命令将创建非共享策略组 `pg-vs3` 最大吞吐量为100 IOPS和400 KB/秒：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   以下命令将创建非共享策略组 `pg-vs4` 无吞吐量限制：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. 将策略组应用于 SVM ，文件，卷或 LUN ：

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   有关完整的命令语法，请参见手册页。您可以使用 *`storage_object`* `modify` 命令将不同的策略组应用于存储对象。

   以下命令将应用策略组 `pg-vs1` 到SVM `vs1`：

   ```
   cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
   ```

   以下命令将应用策略组 `pg-app` 到卷 `app1` 和 `app2`：

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. 监控策略组性能：

   `qos statistics performance show`

   有关完整的命令语法，请参见手册页。

   > 从集群监控性能。请勿使用主机上的工具监控性能。

   以下命令显示策略组性能：

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. 监控工作负载性能：

   `qos statistics workload performance show`

   有关完整的命令语法，请参见手册页。

   > 从集群监控性能。请勿使用主机上的工具监控性能。

   以下命令显示工作负载性能：

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

您可以使用 `qos statistics workload latency show` 命令以查看QoS工作负载的详细延迟统计信息。

使用 **QoS** 设置吞吐量下限

您可以使用 `min-throughput` 用于为存储对象工作负载定义吞吐量下限(QoS最小值)的策略组字段。您可以在创建或修改存储对象时应用策略组。从 ONTAP 9.8 开始，您可以以 IOPS 或 MBps 或 IOPS 和 MBps 为单位指定吞吐量下限。

开始之前

- 您必须运行 ONTAP 9.2 或更高版本。从 ONTAP 9.2 开始，吞吐量下限可用。
- 您必须是集群管理员才能创建策略组。
- 从ONTAP 9.13.1开始、您可以使用在SVM级别强制实施吞吐量下限 自适应策略组模板。您不能在具有QoS策略组的SVM上设置自适应策略组模板。

关于此任务

- 从 ONTAP 9.4 开始，您可以使用 *non-shared* QoS 策略组来指定将定义的吞吐量下限分别应用于每个成员工作负载。只有在这种情况下，吞吐量下限的策略组才能应用于多个工作负载。

  设置 `-is-shared=false` 。 `qos policy-group create` 命令以指定非共享策略组。

- 如果节点或聚合上的性能容量（余量）不足，则工作负载的吞吐量可能会低于指定的下限。
- 受 QoS 限制的存储对象必须包含在策略组所属的 SVM 中。多个策略组可以属于同一个 SVM 。
- QoS 最佳实践是将策略组应用于相同类型的存储对象。
- 定义吞吐量下限的策略组不能应用于 SVM 。

步骤

1. 检查节点或聚合上是否具有足够的性能容量，如中所述 "确定剩余性能容量"。
2. 创建策略组。

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   有关完整的命令语法，请参见适用于您的 ONTAP 版本的手册页。您可以使用 `qos policy-group modify` 命令以调整吞吐量下限。

   以下命令将创建共享策略组 `pg-vs2` 最小吞吐量为1、000 IOPS：

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   以下命令将创建非共享策略组 `pg-vs4` 无吞吐量限制：

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
-is-shared false
```

3. 将策略组应用于卷或 LUN：

   storage_object create -vserver *SVM* -qos-policy-group *policy_group*

   有关完整的命令语法，请参见手册页。您可以使用 _storage_object_modify 命令将不同的策略组应用于存储对象。

   以下命令将应用策略组 pg-app2 卷 app2：

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

4. 监控策略组性能：

   qos statistics performance show

   有关完整的命令语法，请参见手册页。

   > 从集群监控性能。请勿使用主机上的工具监控性能。

   以下命令显示策略组性能：

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. 监控工作负载性能：

   qos statistics workload performance show

   有关完整的命令语法，请参见手册页。

   > 从集群监控性能。请勿使用主机上的工具监控性能。

   以下命令显示工作负载性能：

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

> 您可以使用 `qos statistics workload latency show` 命令以查看QoS工作负载的详细延迟统计信息。

使用自适应 **QoS** 策略组

您可以使用 *adaptive QoS* 策略组自动将吞吐量上限或下限扩展到卷大小，从而在卷大小发生变化时保持 IOPS 与 TBSGB 的比率。如果您要在大型部署中管理数百或数千个工作负载，则这是一项显著优势。

开始之前

- 您必须运行ONTAP 9.3或更高版本。自 ONTAP 9.3 起，可使用自适应 QoS 策略组。
- 您必须是集群管理员才能创建策略组。

关于此任务

存储对象可以是自适应策略组或非自适应策略组的成员，但不能同时是这两者。存储对象的 SVM 和策略必须相同。存储对象必须处于联机状态。

自适应 QoS 策略组始终为非共享组：定义的吞吐量上限或每个成员工作负载的下限适用场景。

吞吐量限制与存储对象大小的比率取决于以下字段的交互：

- `expected-iops` 是每分配的TB|GB的最小预期IOPS。

> `expected-iops`仅在AFF平台上提供担保。 `expected-iops`只有当层策略设置为"无"且云中没有任何块时、才保证适用于FabricPool。 `expected-iops`保证适用于非SnapMirror同步关系中的卷。

- `peak-iops` 是已分配或已使用的每TB|GB可能的最大IOPS。
- `expected-iops-allocation` 指定是将已分配空间(默认值)还是已用空间用于预期IOPS。

> `expected-iops-allocation` 适用于ONTAP 9.5及更高版本。ONTAP 9.4 及更早版本不支持此功能。

- `peak-iops-allocation` 指定是将已分配空间用于还是将已用空间(默认值)用于 `peak-iops`。

- `absolute-min-iops` 是绝对最小IOPS数。您可以对非常小的存储对象使用此字段。它会同时覆盖这两者 `peak-iops` 和 / 或 `expected-iops` 时间 `absolute-min-iops` 大于计算得出的 `expected-iops`。

  例如、如果您设置了 `expected-iops` 计算得出的值为1、000 IOS/TB、并且卷大小小于1 GB `expected-iops` 将是部分IOP。计算的 `peak-iops` 将是一个更小的比例。您可以通过设置来避免此问题 `absolute-min-iops` 以获得实际价值。

- `block-size` 指定应用程序I/O块大小。默认值为 32 K 。有效值为 8K ， 16K ， 32K ， 64K ，任意。any 表示不强制实施块大小。

可用的三个默认自适应 QoS 策略组如下表所示。您可以将这些策略组直接应用于卷。

默认策略组	预期 IOPS/TB	峰值 IOPS/TB	绝对最小 IOPS
`extreme`	6、144	12、288	1000
`performance`	2 ， 048	4、096	500
`value`	128.	512	75

如果某个存储对象的包含对象或子对象属于某个策略组，则不能将该存储对象分配给该策略组。下表列出了这些限制。

如果您分配 ...	则不能分配 ...
SVM 到策略组	将 SVM 包含的任何存储对象分配给策略组
卷到策略组	包含 SVM 的卷或策略组的任何子 LUN
将LUN分配给策略组	将包含 LUN 的卷或 SVM 分配给策略组
文件到策略组	将文件包含的卷或 SVM 分配给策略组

步骤

1. 创建自适应 QoS 策略组：

   ```
   qos adaptive-policy-group create -policy group policy_group -vserver SVM
   -expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
   -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
   space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
   ```

   有关完整的命令语法，请参见手册页。

   > `-expected-iops-allocation` 和 `-block-size` 适用于ONTAP 9.5及更高版本。ONTAP 9.4 及更早版本不支持这些选项。

   以下命令将创建自适应QoS策略组 `adpg-app1` 使用 `-expected-iops` 设置为300 IOS/TB、 `-peak-iops` 设置为1、000 IOS/TB、 `-peak-iops-allocation` 设置为 `used-space`，和 `-absolute-min`

`-iops` 设置为50 IOPS：

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. 将自适应 QoS 策略组应用于卷：

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

   有关完整的命令语法，请参见手册页。

   以下命令将应用自适应QoS策略组 `adpg-app1` 到卷 `app1`：

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

   以下命令将应用默认自适应QoS策略组 `extreme` 到新卷 `app4` 和到现有卷 `app5`。为策略组适用场景卷定义的吞吐量上限 `app4` 和 `app5` 单独：

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

设置自适应策略组模板

从ONTAP 9.13.1开始、您可以使用自适应策略组模板在SVM级别强制实施吞吐量下限和上限。

关于此任务

- 自适应策略组模板是默认策略 `apg1`。可以随时修改此策略。它只能通过命令行界面或ONTAP REST API进行设置、并且只能应用于现有SVM。
- 自适应策略组模板仅会影响在SVM上创建或迁移到该SVM的卷。SVM上的现有卷将保留其现有状态。

  如果禁用自适应策略组模板、SVM上的卷将保留其现有策略。只有随后在SVM上创建或迁移到SVM的卷才会受此功能的影响。

- 您不能在具有QoS策略组的SVM上设置自适应策略组模板。
- 自适应策略组模板专为AFF 平台而设计。可以在其他平台上设置自适应策略组模板、但该策略可能不会强制实施最小吞吐量。同样、您可以向FabricPool聚合或不支持最小吞吐量的聚合中的SVM添加自适应策略组模

板、但不会强制实施吞吐量下限。

- 如果SVM采用MetroCluster 配置或SnapMirror关系、则会在镜像的SVM上强制实施自适应策略组模板。

步骤

1. 修改SVM以应用自适应策略组模板：
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. 确认已设置策略：
   `vserver show -fields qos-adaptive-policy-group`

使用 Unified Manager 监控集群性能

借助 Active IQ Unified Manager ，您可以最大限度地提高 NetApp AFF 和 FAS 存储基础架构的可用性并保持对其的控制，从而提高可扩展性，可支持性，性能和安全性。

Active IQ Unified Manager 会持续监控系统运行状况并发送警报，以便您的组织腾出 IT 人员资源。您可以从一个信息板即时查看存储状态，并通过建议的操作快速解决问题。

数据管理之所以简化，是因为您可以发现，监控和接收通知，从而主动管理存储并快速解决问题。 管理效率得到了提高，因为您可以从一个信息板监控数 PB 的数据，并大规模管理数据。

借助 Active IQ Unified Manager ，您可以跟上不断变化的业务需求，利用性能数据和高级分析优化性能。 通过报告功能，您可以访问标准报告或创建自定义运营报告，以满足您的特定业务需求。

相关链接：

- "详细了解Active IQ Unified Manager"
- "开始使用适用于VMware的Active IQ Unified Manager"
- "开始使用Active IQ Unified Manager for Linus"
- "开始使用Active IQ Unified Manager for Windows"

使用 Cloud Insights 监控集群性能

NetApp Cloud Insights 是一款监控工具，可让您深入了解整个基础架构。借助 Cloud Insights ，您可以监控，故障排除和优化所有资源，包括公有云和私有数据中心。

Cloud Insights 提供两个版本

Cloud Insights 基本版专为监控和优化您的 NetApp Data Fabric 资产而设计。它可以免费为环境中的所有 NetApp 资源（包括 HCI 和全闪存 FAS （ AFF ））之间的连接提供高级分析。

Cloud Insights 标准版不仅关注支持 NetApp Data Fabric 的基础架构组件，还关注多供应商和多云环境。凭借丰富的功能，您可以获得对 100 多项服务和资源的支持。

在当今世界中，随着资源从内部数据中心到多个公有云的发挥，从应用程序本身到存储阵列后端磁盘的全面了解至关重要。应用程序监控（如 Kafka ， MongoDB 和 Nginx ）的额外支持为您提供了以最佳利用率运行所需的信息和知识，同时还提供了完美的风险缓冲区。

这两个版本（基本版和标准版）均可与 NetApp Active IQ Unified Manager 集成。使用Active IQ Unified Manager的客户可以在Cloud Insights用户界面中查看联接信息。在Active IQ Unified Manager上发布的通知不会被忽略、并且可以与Cloud Insights中的事件相关联。换言之，您可以充分利用这两种环境。

监控，故障排除和优化所有资源

Cloud Insights 可帮助您显著缩短解决问题的时间，并防止问题影响最终用户。 它还可以帮助您降低云基础架构成本。 通过利用可操作的智能来保护数据，可以减少您遭受内部威胁的风险。

从公有云到数据中心， Cloud Insights 让您可以在一个位置查看整个混合基础架构。 您可以即时创建相关信息板，以便根据您的特定需求进行自定义。您还可以根据组织的需求创建有针对性的有条件警报。

高级异常检测功能可帮助您在问题出现之前主动修复问题。 您可以自动查看资源争用和降级情况，以快速还原受影响的工作负载。 通过堆栈中不同组件之间自动构建的关系层次结构，故障排除速度更快。

您可以确定整个环境中未使用或已废弃的资源，从而帮助您发现调整基础架构规模并优化整个支出的机会。

Cloud Insights 可将您的系统拓扑可视化，以了解您的 Kubernetes 架构。您可以监控 Kubernetes 集群的运行状况，包括出现故障的节点，并在发现问题时放大。

Cloud Insights 通过高级机器学习和异常检测功能帮助您保护组织数据，防止被恶意用户或被泄露的用户滥用，从而为您提供有关内部威胁的可操作情报。

Cloud Insights 可帮助您直观地显示 Kubernetes 指标，以便您能够全面了解 Pod ，节点和集群之间的关系。您可以评估集群或工作 Pod 的运行状况及其当前正在处理的负载，从而对 K8S 集群执行命令并控制部署的运行状况和成本。

相关链接

- "详细了解Cloud Insights"
- "开始使用Cloud Insights"

审核日志记录

ONTAP 如何实施审核日志记录

审核日志中记录的管理活动包括在标准 AutoSupport 报告中，某些日志记录活动包括在 EMS 消息中。此外，您还可以将审核日志转发到指定的目标，并可使用命令行界面或 Web 浏览器显示审核日志文件。

从ONTAP 9.11.1开始、您可以使用System Manager显示审核日志内容。

从ONTAP 9.12.1开始、ONTAP可为审核日志提供篡改警报。ONTAP会运行每日后台作业来检查audit.log文件是否被篡改、如果发现任何已更改或篡改的日志文件、则会发送EMS警报。

ONTAP 会记录在集群上执行的管理活动，例如发出了什么请求，触发了该请求的用户，用户的访问方法以及发出请求的时间。

管理活动可以是以下类型之一：

- 设置请求、通常适用于非显示命令或操作：

- 运行时会发出这些请求 `create`， `modify`或 `delete` 命令、例如。
- 默认情况下，系统会记录设置请求。

- 获取请求、用于检索信息并将其显示在管理界面中：
  - 运行时会发出这些请求 `show` 命令、例如。
  - 默认情况下、不会记录获取请求、但您可以控制是否从ONTAP命令行界面发送获取请求 (`-cliget`ONTAP) （-ontapiget`)或REST API (`-httpget`)将记录在文件中。

ONTAP会在中记录管理活动 `/mroot/etc/log/mlog/audit.log` 节点的文件。此处会记录三个 shell 中用于 CLI 命令的命令— clustershell ， nodeshell 和非交互式 systemshell （交互式 systemshell 命令不会记录）—以及 API 命令。审核日志包含时间戳，用于显示集群中的所有节点是否都进行了时间同步。

。 `audit.log` AutoSupport工具会将文件发送给指定的收件人。您还可以将内容安全地转发到指定的外部目标，例如 Splunk 或系统日志服务器。

。 `audit.log` 文件每天轮换。当大小达到 100 MB 时，也会进行轮换，并保留前 48 个副本（最多总共 49 个文件）。当审核文件执行每日轮换时，不会生成 EMS 消息。如果审核文件因超过其文件大小限制而发生轮换，则会生成一条 EMS 消息。

对 **ONTAP 9** 中的审核日志记录进行的更改

从ONTAP 9开始、 `command-history.log` 文件将替换为 `audit.log`和 `mgwd.log` 文件不再包含审核信息。如果要升级到 ONTAP 9 ，则应查看引用旧文件及其内容的任何脚本或工具。

升级到ONTAP 9后、现有 `command-history.log` 文件将保留。它们将作为新的旋转(删除) `audit.log` 文件将进行轮换(创建)。

用于检查的工具和脚本 `command-history.log` 文件可能会继续工作、因为中有一个软链接 `command-history.log` to `audit.log` 在升级时创建。但是、用于检查的工具和脚本 `mgwd.log` 文件将失败、因为该文件不再包含审核信息。

此外， ONTAP 9 及更高版本中的审核日志不再包含以下条目，因为它们不会被视为有用，并且发生原因不必要的日志记录活动：

- ONTAP 运行的内部命令（即 username=root ）
- 命令别名（与其所指向的命令不同）

从 ONTAP 9 开始，您可以使用 TCP 和 TLS 协议将审核日志安全地传输到外部目标。

显示审核日志内容

您可以显示集群的内容 `/mroot/etc/log/mlog/audit.log` 使用ONTAP命令行界面、系统管理器或Web浏览器访问文件。

集群的日志文件条目包括以下内容：

时间

日志条目时间戳。

应用程序

用于连接到集群的应用程序。可能值的示例包括 `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, 和 `service-processor`。

用户

远程用户的用户名。

State

审核请求的当前状态、可能为 `success`, `pending`, 或 `error`。

message

一个可选字段、其中可能包含有关命令状态的错误或追加信息。

会话**ID**

接收请求时使用的会话ID。每个SSH _session_都分配有一个会话ID、而每个HTTP、ONTAPI或SNMP _request_都分配有一个唯一的会话ID。

Storage VM

用户连接到的SVM。

范围

显示 `svm` 请求位于数据Storage VM上时；否则显示 `cluster`。

命令**ID**

在CLI会话上收到的每个命令的ID。这样、您就可以关联请求和响应。ZAPI、HTTP和SNMP请求没有命令ID。

您可以从ONTAP 命令行界面、Web浏览器以及从ONTAP 9.11.1开始的System Manager中显示集群的日志条目。

System Manager

- 要显示清单、请选择*事件和作业>审核日志*。+
  每列都有用于筛选、排序、搜索、显示和清单类别的控件。清单详细信息可作为Excel工作簿下载。
- 要设置过滤器，请单击右上角的*Filter*按钮，然后选择所需的字段。+
  您还可以通过单击会话ID链接来查看在发生故障的会话中执行的所有命令。

命令行界面

要显示从集群中的多个节点合并的审核条目、请输入：+
`security audit log show [parameters]`

您可以使用 `security audit log show` 命令以显示集群中单个节点或多个节点合并的节点的审核条目。您还可以显示的内容 `/mroot/etc/log/mlog` 目录。
有关详细信息，请参见手册页。

Web 浏览器

您可以显示的内容 `/mroot/etc/log/mlog` 目录。 "了解如何使用Web浏览器访问节点的日志、核心转储和MIB文件"。

管理审核获取请求设置

虽然默认情况下会记录设置请求、但不会记录获取请求。但是、您可以控制是否从ONTAP HTML发送GET请求 (`-httpget`)、ONTAP命令行界面 (`-cliget`)或ONTAP API (`-ontapiget`)将记录在文件中。

您可以从ONTAP 命令行界面修改审核日志记录设置、并从ONTAP 9.11.1开始从System Manager修改。

System Manager

1. 选择*事件和作业>审核日志*。
2. 单击 ⚙ 右上角的，然后选择要添加或删除的请求。

命令行界面

- 要指定应将来自ONTAP命令行界面或API的获取请求记录在审核日志(audit.log文件)中、除了默认设置请求之外、还应输入：+
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 要显示当前设置、请输入：+
  `security audit show`

有关详细信息、请参见手册页。

管理审核日志目标

您最多可以将审核日志转发到10个目标。例如，您可以将日志转发到 Splunk 或系统日志服务器，以便进行监控，分析或备份。

关于此任务

要配置转发、您必须提供系统日志或Splunk主机的IP地址、其端口号、传输协议以及用于转发日志的系统日志工具。 "了解系统日志工具"。

您可以选择以下传输值之一：

UDP未加密

无安全性的用户数据报协议(默认)

TCP未加密

传输控制协议无安全性

TCP已加密

传输控制协议与传输层安全(Transport Layer Security、TLS)+
选择TCP加密协议后，可使用*Verify server*选项。

您可以从ONTAP 命令行界面转发审核日志、并从ONTAP 9.11.1开始从System Manager转发审核日志。

System Manager

- 要显示审核日志目标、请选择*集群>设置*。+日志目标计数显示在*通知管理区块*中。单击 ⋮ 以显示详细信息。
- 要添加、修改或删除审核日志目标、请选择*事件和作业>审核日志*、然后单击屏幕右上角的*管理审核目标*。+单击 + Add ，或单击 ⋮ *主机地址*列以编辑或删除条目。

命令行界面

1. 对于要将审核日志转发到的每个目标，请指定目标 IP 地址或主机名以及任何安全选项。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - 如果 `cluster log-forwarding create` 命令无法对目标主机执行ping操作以验证连接、命令失败并显示错误。尽管不建议使用 `-force` 参数并使用命令可绕过连接验证。
   - 设置时 `-verify-server` 参数设置为 `true`、日志转发目标的标识通过验证其证书进行验证。您可以将此值设置为 `true` 仅当您选择时 `tcp-encrypted` 中的值 `-protocol` 字段。

2. 使用验证目标记录是否正确 `cluster log-forwarding show` 命令：

```
cluster1::> cluster log-forwarding show

                                                    Verify Syslog
Destination Host           Port   Protocol         Server Facility
-------------------------- ------ --------         ------ --------
192.168.123.96             514    udp-unencrypted false  user
192.168.123.98             514    tcp-encrypted   true   user
2 entries were displayed.
```

有关详细信息、请参见手册页。

AutoSupport

了解AutoSupport

关于AutoSupport

AutoSupport 是一种主动监控系统运行状况并自动向 NetApp 技术支持，您的内部支持组

织和支持合作伙伴发送消息的机制。尽管默认情况下会启用发送给技术支持的 AutoSupport 消息，但您必须设置正确的选项并具有有效的邮件主机，才能将消息发送到内部支持组织。

只有集群管理员才能执行 AutoSupport 管理。Storage Virtual Machine （ SVM ）管理员无法访问 AutoSupport 。

首次配置存储系统时， AutoSupport 默认处于启用状态。启用 AutoSupport 24 小时后， AutoSupport 开始向技术支持发送消息。您可以通过升级或还原系统，修改 AutoSupport 配置或将系统时间更改为 24 小时以外的时间来缩短 24 小时时间段。

> 您可以随时禁用 AutoSupport ，但应保持启用状态。如果存储系统出现问题，启用 AutoSupport 可以显著加快问题的确定和解决速度。默认情况下，系统会收集 AutoSupport 信息并将其存储在本地，即使您禁用了 AutoSupport 也是如此。

有关 AutoSupport 的详细信息，请参见 NetApp 支持站点。

相关信息

- "NetApp 支持"
- "ONTAP 命令参考"

关于**Active IQ**数字顾问和**AutoSupport**

ONTAP 的 AutoSupport 组件会收集遥测数据并将其发送以供分析。Active IQ Digital Advisor 可分析 AutoSupport 中的数据，并提供主动式维护和优化。利用人工智能，Active IQ 可以识别潜在问题并帮助您在问题影响业务之前解决这些问题。

Active IQ 通过基于云的门户和移动应用程序提供可操作的预测性分析和主动式支持，帮助您优化全球混合云中的数据基础架构。Active IQ 提供的数据驱动型洞察力和建议可供具有有效 SupportEdge 合同的所有 NetApp 客户使用（功能因产品和支持层而异）。

以下是您可以使用 Active IQ 执行的一些操作：

- 计划升级。Active IQ 可确定环境中可通过升级到较新版本的 ONTAP 来解决的问题， Upgrade Advisor 组件可帮助您规划成功升级。
- 查看系统运行状况。您的 Active IQ 信息板可报告任何健康问题，并帮助您更正这些问题。监控系统容量，确保存储空间不会用尽。查看您的系统的支持案例。
- 管理性能。Active IQ 显示系统性能的时间比您在 System Manager 中看到的时间长。确定影响性能的配置和系统问题。
- 最大限度地提高效率。查看存储效率指标并确定如何在更少的空间中存储更多数据。
- 查看清单和配置。Active IQ 将显示完整的清单以及软件和硬件配置信息。查看服务合同何时到期并续订，以确保您始终获得支持。

相关信息

"NetApp 文档： Active IQ Digital Advisor"

"启动 Active IQ"

"SupportEdge 服务"

AutoSupport 消息的发送时间和位置

AutoSupport 会根据消息类型将消息发送给不同的收件人。了解 AutoSupport 发送消息的时间和位置有助于您了解通过电子邮件接收的消息或在 Active IQ （以前称为 My AutoSupport ）网站上查看的消息。

除非另有说明、否则下表中的设置是的参数 `system node autosupport modify` 命令：

事件触发的消息

当系统上发生需要采取更正操作的事件时， AutoSupport 会自动发送事件触发的消息。

发送消息时	消息的发送位置
AutoSupport 对 EMS 中的触发事件做出响应	中指定的地址 `-to` 和 `-noteto`。（仅发送影响服务的严重事件。） 中指定的地址 `-partner-address` 技术支持、IF `-support` 设置为 `enable`

已计划消息

AutoSupport 会定期自动发送多条消息。

发送消息时	消息的发送位置
每天（默认情况下，在午夜 12： 00 之间发送和凌晨 1： 00作为日志消息）	中指定的地址 `-partner-address` 技术支持、IF `-support` 设置为 `enable`
每天（默认情况下，在午夜 12： 00 之间发送和凌晨 1： 00作为性能消息) `-perf` 参数设置为 `true`	在 -partner-address` 中指定的地址  技术支持、IF `-support` 设置为 `enable`
每周（默认情况下，在星期日中午 12： 00 之间发送和凌晨 1： 00 ）	中指定的地址 `-partner-address` 技术支持、IF `-support` 设置为 `enable`

手动触发的消息

您可以手动启动或重新发送 AutoSupport 消息。

发送消息时	消息的发送位置
您可以使用手动启动消息 `system node autosupport invoke` 命令	如果使用指定了URI `-uri` 中的参数 `system node autosupport invoke` 命令、则会将消息发送到该URI。 条件 `-uri` 如果省略、则会将消息发送到中指定的地址 `-to` 和 `-partner-address`。如果出现这种情况、此消息还会发送给技术支持 `-support` 设置为 `enable`。
您可以使用手动启动消息 `system node autosupport invoke-core-upload` 命令	如果使用指定了URI `-uri` 中的参数 `system node autosupport invoke-core-upload` 命令时、消息将发送到此URI、而核心转储文件将上传到此URI。 条件 `-uri` 在中省略 `system node autosupport invoke-core-upload` 命令中、消息将发送到技术支持、核心转储文件将上传到技术支持站点。 这两种情况都需要这样做 `-support` 设置为 `enable` 和 `-transport` 设置为 `https` 或 `http`。 由于核心转储文件非常大、因此不会将消息发送到中指定的地址 `-to` 和 `-partner-addresses` parameters
您可以使用手动启动消息 `system node autosupport invoke-performance-archive` 命令	如果使用指定了URI `-uri` 中的参数 `system node autosupport invoke-performance-archive` 命令时、消息将发送到此URI、性能归档文件将上传到此URI。 条件 `-uri` 在中省略 `system node autosupport invoke-performance-archive`，消息将发送至技术支持，性能归档文件将上传到技术支持站点。 这两种情况都需要这样做 `-support` 设置为 `enable` 和 `-transport` 设置为 `https` 或 `http`。 由于性能归档文件非常大、因此不会将消息发送到中指定的地址 `-to` 和 `-partner-addresses` parameters
您可以使用手动重新发送过去的消息 `system node autosupport history retransmit` 命令	仅限您在中指定的URI `-uri` 的参数 `system node autosupport history retransmit` 命令

技术支持触发的消息

技术支持可以使用 AutoSupport 按需功能从 AutoSupport 请求消息。

发送消息时	消息的发送位置
AutoSupport 获取生成新 AutoSupport 消息的传送指令时	中指定的地址 `-partner-address` 技术支持、IF `-support` 设置为 `enable` 和 `-transport` 设置为 `https`
AutoSupport 获取重新发送过去 AutoSupport 消息的传送指令时	技术支持、IF `-support` 设置为 `enable` 和 `-transport` 设置为 `https`
当 AutoSupport 获取生成新 AutoSupport 消息以上传核心转储或性能归档文件的传送指令时	技术支持、IF `-support` 设置为 `enable` 和 `-transport` 设置为 `https`。核心转储或性能归档文件将上传到技术支持站点。

AutoSupport 如何创建和发送事件触发的消息

AutoSupport 会在 EMS 处理触发事件时创建事件触发的 AutoSupport 消息。事件触发的 AutoSupport 消息会提醒收件人需要采取更正操作的问题，并且仅包含与问题相关的信息。您可以自定义要包含的内容以及接收消息的人员。

AutoSupport 使用以下过程创建和发送事件触发的 AutoSupport 消息：

1. 当 EMS 处理触发事件时， EMS 会向 AutoSupport 发送一个请求。

   触发器事件是指具有AutoSupport目标且名称以开头的EMS事件 `callhome.` 前缀。

2. AutoSupport 会创建事件触发的 AutoSupport 消息。

   AutoSupport 从与触发器关联的子系统收集基本信息和故障排除信息，以创建一条仅包含与触发器事件相关信息的消息。

   每个触发器都会关联一组默认子系统。但是、您可以选择使用将其他子系统与触发器关联 `system node autosupport trigger modify` 命令：

3. AutoSupport会将事件触发的AutoSupport消息发送给定义的收件人 `system node autosupport modify` 命令 `-to`， `-noteto`， `-partner-address`，和 `-support` parameters

   您可以使用启用和禁用特定触发器的AutoSupport消息传送 `system node autosupport trigger modify` 命令 `-to` 和 `-noteto` parameters

为特定事件发送的数据示例

。 `storage shelf PSU failed` EMS事件触发一条消息、其中包含Mandatory、Log Files、Storage、RAID、HA、 平台和网络子系统以及来自强制、日志文件和存储子系统的故障排除数据。

您决定在为响应未来的请求而发送的任何AutoSupport消息中包含有关NFS的数据 `storage shelf PSU failed` 事件。输入以下命令可为启用NFS故障排除级别的数据 `callhome.shlf.ps.fault` 事件：

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

请注意、 `callhome.` 前缀将从中删除 `callhome.shlf.ps.fault` 事件 `system node autosupport trigger` 命令、或者在命令行界面中由AutoSupport和EMS事件引用时。

AutoSupport 消息的类型及其内容

AutoSupport 消息包含有关受支持子系统的状态信息。了解 AutoSupport 消息包含哪些内容有助于您解读或响应通过电子邮件接收的消息或在 Active IQ （以前称为 My AutoSupport ）网站上查看的消息。

消息类型	消息包含的数据类型
事件触发	包含有关发生事件的特定子系统的上下文相关数据的文件
每天	日志文件
性能	在过去 24 小时内采样的性能数据
每周	配置和状态数据
由触发 `system node autosupport invoke` 命令	取决于中指定的值 `-type` 参数： • `test` 发送用户触发的消息、其中包含一些基本数据。 此外、此消息还会使用触发从技术支持到任何指定电子邮件地址的自动电子邮件响应 `-to` 选项、以便您可以确认正在接收AutoSupport消息。 • `performance` 发送性能数据。 • `all` 发送一条用户触发的消息、其中包含一组与每周消息类似的完整数据、包括每个子系统的故障排除数据。 技术支持通常会请求此消息。
由触发 `system node autosupport invoke-core-upload` 命令	节点的核心转储文件
由触发 `system node autosupport invoke-performance-archive` 命令	指定时间段内的性能归档文件

消息类型	消息包含的数据类型
由 AutoSupport OnDemand 触发	AutoSupport OnDemand 可以请求新消息或过去的消息： • 根据AutoSupport收集的类型、新消息可以是 `test` ， `all`或 `performance`。 • 过去的消息取决于重新发送的消息类型。 AutoSupport OnDemand可以请求新消息，并将以下文件上传到NetApp支持站点 "mysupport.netapp.com"： • 核心转储 • 性能归档

查看**AutoSupport**子系统

每个子系统都提供 AutoSupport 用于其消息的基本信息和故障排除信息。每个子系统还会与触发事件关联，从而使 AutoSupport 能够仅从子系统收集与触发事件相关的信息。

AutoSupport 收集上下文相关内容。

步骤

1. 查看有关子系统和触发器事件的信息：

```
system node autosupport trigger show
```

AutoSupport 大小和时间预算

AutoSupport 按子系统收集信息，并对每个子系统的内容实施大小和时间预算。随着存储系统的增长， AutoSupport 预算可以控制 AutoSupport 有效负载，进而可扩展 AutoSupport 数据的交付。

如果子系统内容超过其大小或时间预算， AutoSupport 将停止收集信息并截断 AutoSupport 内容。如果无法轻松截断内容（例如二进制文件）， AutoSupport 将省略该内容。

只有在NetApp支持部门要求您修改默认大小和时间预算时、才应进行修改。您还可以使用查看子系统的默认大小和时间预算 `autosupport manifest show` 命令：

在事件触发的 **AutoSupport** 消息中发送的文件

事件触发的 AutoSupport 消息仅包含与导致 AutoSupport 生成消息的事件相关的子系统的基本信息和故障排除信息。具体数据有助于 NetApp 支持和支持合作伙伴解决问题。

AutoSupport 使用以下标准控制事件触发的 AutoSupport 消息中的内容：

- 包括哪些子系统

  数据分为多个子系统，包括日志文件等通用子系统和 RAID 等特定子系统。每个事件都会触发一条仅包含特定子系统数据的消息。

- 所包含的每个子系统的详细信息级别

  所包含的每个子系统的数据都是在基本级别或故障排除级别提供的。

您可以使用查看所有可能的事件、并确定在有关每个事件的消息中包含哪些子系统 `system node autosupport trigger show` 命令 `-instance` 参数。

除了默认情况下每个事件包含的子系统之外、您还可以使用在基本级别或故障排除级别添加其他子系统 `system node autosupport trigger modify` 命令：

在 **AutoSupport** 消息中发送的日志文件

AutoSupport 消息可以包含多个关键日志文件，使技术支持人员能够查看最近的系统活动。

启用日志文件子系统后，所有类型的 AutoSupport 消息都可能包含以下日志文件：

日志文件	文件中包含的数据量
• 中的日志文件 `/mroot/etc/log/mlog/` 目录 • 消息日志文件	仅自上次 AutoSupport 消息以来添加到日志中的新行数，最多不超过指定的最大值。这样可以确保 AutoSupport 消息具有唯一的相关数据，而不是重叠数据。 （来自合作伙伴的日志文件除外；对于合作伙伴，将包括允许的最大数据。）
• 中的日志文件 `/mroot/etc/log/shelflog/` 目录 • 中的日志文件 `/mroot/etc/log/acp/` 目录 • 事件管理系统（ EMS ）日志数据	最新的数据行数，最高可达指定的最大值。

AutoSupport 消息的内容可能会在 ONTAP 版本之间发生变化。

每周 **AutoSupport** 消息中发送的文件

每周 AutoSupport 消息包含其他配置和状态数据，这些数据可用于跟踪系统随时间发生的更改。

以下信息将以每周 AutoSupport 消息的形式发送：

- 有关每个子系统的基本信息
- 选定内容 `/mroot/etc` 目录文件

- 日志文件
- 提供系统信息的命令的输出
- 追加信息，包括复制的数据库（RDB）信息，服务统计信息等

AutoSupport OnDemand 如何从技术支持获取交付指令

AutoSupport OnDemand 会定期与技术支持进行通信，以获取有关发送，重新发送和拒绝 AutoSupport 消息以及将大型文件上传到 NetApp 支持站点的交付说明。通过 AutoSupport OnDemand ，可以按需发送 AutoSupport 消息，而无需等待每周 AutoSupport 作业运行。

AutoSupport OnDemand 包含以下组件：

- 在每个节点上运行的 AutoSupport OnDemand 客户端
- 驻留在技术支持中的 AutoSupport OnDemand 服务

AutoSupport OnDemand 客户端会定期轮询 AutoSupport OnDemand 服务，以从技术支持获取传送指令。例如，技术支持可以使用 AutoSupport OnDemand 服务请求生成新的 AutoSupport 消息。当 AutoSupport OnDemand 客户端轮询 AutoSupport OnDemand 服务时，客户端将获取传送指令，并根据请求按需发送新的 AutoSupport 消息。

默认情况下， AutoSupport OnDemand 处于启用状态。但是， AutoSupport OnDemand 依靠某些 AutoSupport 设置来继续与技术支持进行通信。满足以下要求时， AutoSupport OnDemand 会自动与技术支持通信：

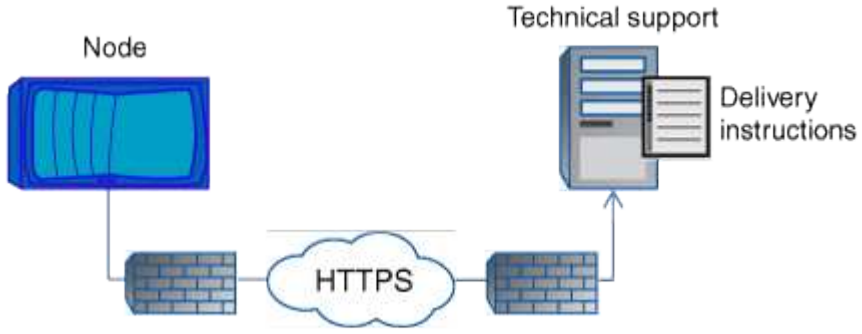
- AutoSupport 已启用
- AutoSupport 已配置为向技术支持发送消息。
- AutoSupport 已配置为使用 HTTPS 传输协议。

AutoSupport OnDemand 客户端会将 HTTPS 请求发送到 AutoSupport 消息所发送到的同一技术支持位置。AutoSupport OnDemand 客户端不接受传入连接。

> AutoSupport OnDemand 使用 "`AutoSupport` " 用户帐户与技术支持进行通信。ONTAP 会阻止您删除此帐户。

如果要禁用AutoSupport OnDemand但保持启用AutoSupport、请使用命令：link：https://docs.netapp.com/us-en/ontap-cli/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`]。

下图显示了 AutoSupport OnDemand 如何向技术支持发送 HTTPS 请求以获取传送指令。



传送指令可以包括请求 AutoSupport 执行以下操作：

- 生成新的 AutoSupport 消息。

  技术支持可能会请求新的 AutoSupport 消息来帮助鉴别问题。

- 生成新的 AutoSupport 消息，将核心转储文件或性能归档文件上传到 NetApp 支持站点。

  技术支持可能会请求核心转储或性能归档文件来帮助鉴别问题。

- 重新传输先前生成的 AutoSupport 消息。

  如果由于传送失败而未收到消息，则会自动发出此请求。

- 禁止传送特定触发事件的 AutoSupport 消息。

  技术支持可能会禁止传送未使用的数据。

通过电子邮件发送的 **AutoSupport** 消息的结构

通过电子邮件发送 AutoSupport 消息时，该消息具有一个标准主题，一个简短的正文以及一个 7z 文件格式的大附件，其中包含数据。

> 如果将 AutoSupport 配置为隐藏私有数据，则某些信息（例如主机名）会在标题，主题，正文和附件中被省略或屏蔽。

主题

AutoSupport 机制发送的消息的主题行包含一个文本字符串，用于标识通知的原因。主题行的格式如下：

来自 *System_Name* （ *Message* ） *Severity* 的 HA 组通知

- *System_Name* 是主机名或系统 ID ，具体取决于 AutoSupport 配置

body

AutoSupport 消息的正文包含以下信息：

- 消息的日期和时间戳
- 生成消息的节点上的 ONTAP 版本
- 生成消息的节点的系统 ID ，序列号和主机名
- AutoSupport 序列号
- SNMP 联系人姓名和位置（如果指定）
- HA 配对节点的系统 ID 和主机名

附加文件

AutoSupport消息中的关键信息包含在压缩为一个名为的7z文件的文件中 `body.7z` 并附加到消息。

附件中包含的文件特定于 AutoSupport 消息的类型。

AutoSupport 严重性类型

AutoSupport 消息的严重性类型可帮助您了解每条消息的用途，例如，用于立即引起对紧急问题的注意，或者仅用于提供信息。

消息具有以下严重性之一：

- * 警报 *： 警报消息表示，如果不采取某些操作，可能会发生更高级别的事件。

  您必须在 24 小时内对警报消息采取措施。

- * 紧急 *： 发生中断时会显示紧急消息。

  您必须立即对紧急消息采取措施。

- * 错误 *： 错误条件表示忽略后可能发生的情况。
- * 注意事项 *： 正常但重要的情况。
- * 信息 *： 信息性消息提供了有关问题描述的详细信息，您可以忽略这些信息。
- * 调试 *： 调试级别的消息提供了应执行的说明。

如果您的内部支持组织通过电子邮件接收 AutoSupport 消息，则严重性将显示在电子邮件消息的主题行中。

获取 AutoSupport 消息说明

您可以通过ONTAP 系统日志翻译器查看所收到的AutoSupport 消息的说明。

步骤

1. 转至 "系统日志翻译器"。
2. 在"版本"*字段中、输入所使用的ONTAP 版本。在"*搜索字符串"字段中、输入"CallHome"。选择*转换。
3. 系统日志翻译器将按字母顺序列出与您输入的消息字符串匹配的所有事件。

用于管理 AutoSupport 的命令

您可以使用 `system node autosupport` 用于更改或查看AutoSupport配置、显示有关先前AutoSupport消息的信息以及发送、重新发送或取消AutoSupport消息的命令。

配置 AutoSupport

如果您要 ...	使用此命令 ...
控制是否发送任何 AutoSupport 消息	`system node autosupport modify` 使用 `-state` 参数
控制是否将 AutoSupport 消息发送给技术支持	`system node autosupport modify` 使用 `-support` 参数

如果您要 ...	使用此命令 ...
设置 AutoSupport 或修改 AutoSupport 的配置	`system node autosupport modify`
启用和禁用针对单个触发事件向内部支持组织发送 AutoSupport 消息的功能，并指定要包含在针对单个触发事件发送的消息中的其他子系统报告	`system node autosupport trigger modify`

显示有关 **AutoSupport** 配置的信息

如果您要 ...	使用此命令 ...
显示 AutoSupport 配置	`system node autosupport show` 使用 `-node` 参数
查看接收 AutoSupport 消息的所有地址和 URL 的摘要	`system node autosupport destinations show`
显示针对单个触发事件向内部支持组织发送的 AutoSupport 消息	`system node autosupport trigger show`
显示 AutoSupport 配置的状态以及向各种目标的传输	`system node autosupport check show`
显示 AutoSupport 配置的详细状态以及向各种目标的传输	`system node autosupport check show-details`

显示有关以往 **AutoSupport** 消息的信息

如果您要 ...	使用此命令 ...
显示有关 50 个最新 AutoSupport 消息中一个或多个消息的信息	`system node autosupport history show`
显示有关为将核心转储或性能归档文件上传到技术支持站点或指定 URI 而生成的最新 AutoSupport 消息的信息	`system node autosupport history show-upload-details`
查看 AutoSupport 消息中的信息，包括为此消息收集的每个文件的名称和大小以及任何错误	`system node autosupport manifest show`

发送，重新发送或取消 **AutoSupport** 消息

如果您要 ...	使用此命令 ...
重新传输本地存储的 AutoSupport 消息，此消息由其 AutoSupport 序列号标识 如果您重新传输 AutoSupport 消息，并且支持部门已收到该消息，则支持系统不会创建重复的案例。另一方面，如果支持人员未收到此消息，则 AutoSupport 系统将分析此消息并在必要时创建案例。	`system node autosupport history retransmit`
生成并发送 AutoSupport 消息，例如，用于测试目的	`system node autosupport invoke` 使用 `-force` 用于在禁用AutoSupport 的情况下发送消息的参数。使用 `-uri` 参数、用于将消息发送到您指定的目标、而不是配置的目标。
取消 AutoSupport 消息	`system node autosupport history cancel`

相关信息

"ONTAP 命令参考"

AutoSupport 清单中包含的信息

AutoSupport 清单为您提供了为每个 AutoSupport 消息收集的文件的详细视图。AutoSupport 清单还包含有关 AutoSupport 无法收集所需文件时的收集错误的信息。

AutoSupport 清单包含以下信息：

- AutoSupport 消息的序列号
- AutoSupport 消息中包含哪些文件 AutoSupport
- 每个文件的大小，以字节为单位
- AutoSupport 清单收集的状态
- 如果 AutoSupport 无法收集一个或多个文件，则出现错误问题描述

您可以使用查看AutoSupport清单 `system node autosupport manifest show` 命令：

AutoSupport 清单随每个 AutoSupport 消息一起提供，并以 XML 格式显示，这意味着您可以使用通用 XML 查看器来读取它，也可以使用 Active IQ （以前称为 My AutoSupport ）门户来查看它。

规划

准备使用AutoSupport

您可以将ONTAP集群配置为向NetApp传送AutoSupport消息。在此过程中、您还可以将消息副本发送到本地电子邮件地址、通常是在您的组织内。您应通过查看可用选项来准备配置AutoSupport。

向NetApp传送AutoSupport消息

可以使用HTTP或SMTP协议将AutoSupport消息传送到NetApp。为了提高安全性、您可以将TLS与HTTP结合使用。从ONTAP 9.15.1开始、您还可以将TLS与SMTP结合使用。

> 尽可能对TLS (HTTPS)使用HTTP。

另请注意以下事项：

- 只能为NetApp AutoSupport消息配置一个传送通道。您不能使用两种协议向NetApp传送AutoSupport消息。
- AutoSupport 会限制每个协议的最大文件大小。如果AutoSupport消息的大小超过配置的限制、则AutoSupport会尽可能多地发送消息、但会发生消息被删除。
- 您可以根据需要更改最大文件大小。请参见命令 `system node autosupport modify` 有关详细信息 ...
- 这两种协议都可以根据名称解析到的地址系列通过IPv4或IPv6进行传输。
- ONTAP为发送AutoSupport消息而建立的TCP连接是临时的、短暂的。

HTTP

这提供了最强大的功能。请注意以下事项：

- 支持AutoSupport OnDemand和大型文件传输。
- 首先尝试HTTP放置请求。如果此请求在传输期间失败、则此请求将从停止位置重新启动。
- 如果服务器不支持Put、则改用HTTP POST方法。
- HTTP传输的默认限制为50 MB。
- 不安全的HTTP协议使用端口80。

SMTP

一般情况下、只有在出于某种原因不允许或不支持HTTPS/HTTP时、才应使用SMTP。请注意以下事项：

- 不支持AutoSupport OnDemand和传输大型文件。
- 如果配置了SMTP登录凭据、则会以未加密的方式以明文形式发送这些凭据。
- HTTP传输的默认限制为5 MB。
- 不安全的SMTP协议使用端口25。

利用TLS提高安全性

使用HTTP或SMTP时、所有流量均未加密、并且可以轻松截获和读取。使用HTTP时、您应始终将协议配置为同时使用TLS (HTTPS)。

> 从ONTAP 9.15.1开始、您还可以将TLS与SMTP (SMTPS)结合使用。在这种情况下、会使用_explicit tls_、以便在建立TCP连接后激活安全通道。

用于安全协议的端口

以下端口通常用于这些协议的安全版本：

- HTTPS—端口443
- SMTPS—端口587

证书验证

对于TLS、ONTAP会根据根CA证书验证从服务器下载的证书。在使用HTTPS或SMTPS之前、您需要确保根证书已安装在ONTAP中。请参见 [安装服务器证书] 有关详细信息 …

其他配置注意事项

配置AutoSupport时、还需要考虑一些其他注意事项。

使用电子邮件发送本地副本

无论使用哪种协议将AutoSupport消息传送到NetApp、您都可以将每条消息的副本发送到一个或多个本地电子邮件地址。例如、您可以向内部支持组织或合作伙伴组织发送消息。

> 如果您使用SMTP (或SMTPS)将消息传送到NetApp、同时还发送了这些消息的本地电子邮件副本、则会使用相同的电子邮件服务器配置。

HTTP 代理

根据您的网络配置、HTTPS协议可能需要对代理URL进行额外配置。如果使用HTTPS向技术支持发送AutoSupport消息、并且您有代理、则必须标识此代理的URL。如果代理使用的端口不是默认端口(端口3128)、则可以为该代理指定端口。您也可以选择为代理身份验证指定用户名和密码。

安装服务器证书

如果使用TLS (HTTPS或SMTPS)、则需要确保ONTAP可以验证服务器证书。此验证将根据签署服务器证书的CA来执行。

ONTAP包含大量预安装的根CA证书。因此、在许多情况下、ONTAP将立即识别服务器的证书、而无需进行额外配置。但是、根据服务器证书的签名方式、您可能需要安装根CA证书和任何中间证书。

如果需要、请按照下面提供的说明安装证书。您应在集群级别安装所有必需的证书。

示例 **1.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 选择 → *Certificates*旁边的。
4. 在“可信证书颁发机构”选项卡下，单击“添加”。
5. 单击*Import*并选择证书文件。
6. 完成环境的配置参数。
7. 单击 * 添加 * 。

命令行界面

1. 开始安装：

   ```
   security certificate install -type server-ca
   ```

2. 查找以下控制台消息：

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 使用文本编辑器打开证书文件。
4. 复制整个证书、包括以下行：

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. 在命令提示符后、将证书粘贴到终端中。
6. 按*Enter*键完成安装。
7. 使用以下方法之一确认已安装证书：

   ```
   security certificate show-user-installed

   security certificate show
   ```

设置 **AutoSupport**

您可以配置ONTAP集群、以便向NetApp技术支持传送AutoSupport消息、并向内部支持组织发送电子邮件副本。在此过程中、您还可以先对配置进行测试、然后再在生产环境中使用它。

关于此任务

从ONTAP 9.5开始、您可以同时为集群中的所有节点启用和配置AutoSupport。当新节点加入集群时、该节点会自动继承相同的AutoSupport配置。为此、请查看CLI命令的范围 `system node autosupport modify` 是集

群级别的。。 `-node` 为了向后兼容、保留了命令选项、但会将其忽略。

> 在ONTAP 9.4及更早版本中、命令 `system node autosupport modify` 特定于每个节点。如果集群运行的是ONTAP 9.4或更早版本、则需要在集群中的每个节点上启用和配置AutoSupport。

开始之前

将AutoSupport消息传送到NetApp时、建议使用HTTPS (HTTP与TLS)传输配置。此选项可提供最强大的功能和最佳的安全性。

请查看 "准备使用AutoSupport" 了解有关配置ONTAP集群之前的详细信息。

步骤

1. 确保已启用 AutoSupport：

```
system node autosupport modify -state enable
```

2. 如果您希望NetApp技术支持接收AutoSupport消息、请使用以下命令：

```
system node autosupport modify -support enable
```

   如果要使 AutoSupport 能够与 AutoSupport OnDemand 配合使用，或者要将核心转储和性能归档文件等大型文件上传到技术支持或指定 URL ，则必须启用此选项。

3. 如果已启用NetApp技术支持来接收AutoSupport消息、请指定要用于这些消息的传输协议。

   您可以从以下选项中进行选择：

如果您要 ...	然后设置的以下参数 `system node autosupport modify` 命令...
使用默认 HTTPS 协议	a. 设置 `-transport` to `https`。 b. 如果使用代理、请设置 `-proxy-url` 代理的URL。 此配置支持与 AutoSupport OnDemand 通信以及上传大型文件。
使用 SMTP	设置 `-transport` to `smtp`。 此配置不支持 AutoSupport OnDemand 或上传大型文件。

4. 如果您希望内部支持组织或支持合作伙伴接收 AutoSupport 消息，请执行以下操作：

   a. 通过设置的以下参数、确定组织中的收件人 `system node autosupport modify` 命令：

设置此参数 ...	目标位置 ...

`-to`	您的内部支持组织中最多五个将接收关键 AutoSupport 消息的电子邮件地址或分发列表，以逗号分隔
`-noteto`	您的内部支持组织中最多有五个以逗号分隔的单个电子邮件地址或分发列表，这些地址或分发列表将接收专为手机和其他移动设备设计的关键 AutoSupport 消息的简略版本
`-partner-address`	您的支持合作伙伴组织中最多五个以逗号分隔的单个电子邮件地址或分发列表，这些电子邮件地址或分发列表将接收所有 AutoSupport 消息

b. 通过使用列出目标来检查是否已正确配置地址 `system node autosupport destinations show` 命令：

5. 如果您要向内部支持组织发送消息、或者为发送给技术支持的消息选择了SMTP传输、请通过设置的以下参数来配置SMTP `system node autosupport modify` 命令：

   - 设置 `-mail-hosts` 发送到一个或多个邮件主机、以逗号分隔。

     最多可以设置五个。

   您可以通过在邮件主机名后面指定冒号和端口号来为每个邮件主机配置端口值：例如、`mymailhost.example.com:5678`，其中5678是邮件主机的端口。

   - 设置 `-from` 发送AutoSupport消息的电子邮件地址。

6. 配置 DNS 。

7. (可选)如果要更改特定设置、请添加命令选项：

如果要执行此操作 ...	然后设置的以下参数 `system node autosupport modify` 命令...
通过删除，屏蔽或对消息中的敏感数据进行编码来隐藏私有数据	设置 `-remove-private-data` to `true`。如果您从进行了更改 `false` to `true`，所有AutoSupport历史记录和所有关联文件都将被删除。
停止在定期 AutoSupport 消息中发送性能数据	设置 `-perf` to `false`。

8. 如果您使用SMTP向NetApp传送AutoSupport消息、则可以选择启用TLS以提高安全性。

   a. 显示可用于新参数的值：

   ```
   cluster1::> system node autosupport modify -smtp-encryption ?
   ```

   b. 为SMTP消息传送启用TLS：

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

c. 显示当前配置：

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. 使用检查整体配置 `system node autosupport show` 命令 `-node` 参数。
10. 使用验证AutoSupport操作 `system node autosupport check show` 命令：

    如果报告任何问题、请使用 `system node autosupport check show-details` 命令以查看详细信息。

11. 测试是否正在发送和接收 AutoSupport 消息：

    a. 使用 `system node autosupport invoke` 命令 `-type` 参数设置为 `test`：

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. 确认 NetApp 正在接收您的 AutoSupport 消息：

    ```
    system node autosupport history show -node local
    ```

    最新传出AutoSupport消息的状态最终应更改为 `sent-successful` 所有适当的协议目标。

    c. (可选)通过检查为配置的任何地址的电子邮件来确认AutoSupport消息正在发送到您的内部支持组织或您的支持合作伙伴 `-to`， `-noteto`或 `-partner-address` 的参数 `system node autosupport modify` 命令：

配置

管理**AutoSupport**设置

您可以使用System Manager管理AutoSupport帐户的设置。

您可以执行以下过程：

查看 **AutoSupport** 设置

您可以使用 System Manager 查看 AutoSupport 帐户的设置。

步骤

1. 在 System Manager 中，单击 * 集群 > 设置 * 。

   在 * AutoSupport * 部分中，将显示以下信息：

- Status
- 传输协议
- 代理服务器
- 发件人电子邮件地址

2. 在* AutoSupport选项*部分中，选择，然后选择 ⋮ 更多选项。

   此时将显示有关 AutoSupport 连接和电子邮件设置的追加信息。此外，还会列出消息的传输历史记录。

生成并发送 **AutoSupport** 数据

在 System Manager 中，您可以启动 AutoSupport 消息的生成，并选择从哪个或哪些集群节点收集数据。

步骤

1. 在System Manager中、选择*集群>设置*。
2. 在*Generate AutoSupport and Send*部分中，选择 ⋮，然后选择*Generate and Send*。
3. 输入主题。
4. 选中*收集数据来源*下的复选框，指定要从中收集数据的节点。

测试与 **AutoSupport** 的连接

在 System Manager 中，您可以发送测试消息以验证与 AutoSupport 的连接。

步骤

1. 在 System Manager 中，单击 * 集群 > 设置 * 。
2. 在*Test Connectivity (测试连接)*部分，选择，然后选择***Test AutoSupport** ⋮ **(***测试连接**)**。
3. 输入消息的主题。

启用或禁用 **AutoSupport**

AutoSupport为NetApp客户提供经验证的业务优势、包括主动识别可能的配置问题并加快解决支持案例的速度。默认情况下、AutoSupport在新系统中处于启用状态。如果需要、您可以使用System Manager禁用AutoSupport监控存储系统运行状况并向您发送通知消息的功能。 禁用 AutoSupport 后，您可以重新启用它。

关于此任务

禁用AutoSupport之前、您应注意关闭NetApp自动通报系统、将失去以下优势：

- 运行状况监控：AutoSupport可监控存储系统的运行状况并向技术支持和内部支持组织发送通知。
- 自动化：AutoSupport自动报告支持案例。大多数支持案例都是在客户意识到存在问题之前自动创建的。
- 解决速度更快：与不发送AutoSupport数据的系统相比，发送AutoSupport数据的系统解决支持案例的时间缩短一半。
- 加快升级速度：AutoSupport为客户自助服务工作流提供支持，例如System Manager中的版本升级、附加项、续订和固件更新自动化。
- 更多功能：其他工具中的某些功能仅在启用AutoSupport时才起作用，例如BlueXP中的某些工作流。

步骤

1. 选择*集群>设置*。
2. 在* AutoSupport禁用*部分，选择，然后选择 ⋮禁用。
3. 如果要重新启用AutoSupport，请在*Enable* AutoSupport部分中选择，然后选择 ⋮**Enable**。

禁止生成支持案例

从 ONTAP 9.10.1 开始，您可以使用 System Manager 向 AutoSupport 发送请求，以禁止生成支持案例。

关于此任务

要禁止生成支持案例，请指定要进行禁止的节点和小时数。

如果您不希望 AutoSupport 在对系统执行维护时自动创建支持案例，则禁止支持案例尤其有用。

步骤

1. 选择*集群>设置*。
2. 在*Suppress (禁止支持案例生成)部分，选择，然后选择***Suppress AutoSupport** ⋮**Case Generation**(禁止支持案例生成)。
3. 输入要进行禁止的小时数。
4. 选择要对其执行禁止的节点。

继续生成支持案例

从 ONTAP 9.10.1 开始，如果已禁止生成支持案例，您可以使用 System Manager 从 AutoSupport 恢复生成支持案例。

步骤

1. 选择*集群>设置*。
2. 在*Resume*部分中，选择，然后选择*恢复AutoSupport ⋮支持案例生成*。
3. 选择要恢复生成的节点。

编辑 **AutoSupport** 设置

您可以使用 System Manager 修改 AutoSupport 帐户的连接和电子邮件设置。

步骤

1. 选择*集群>设置*。
2. 在* AutoSupport选项*部分中，选择，然后选择 ⋮更多选项。
3. 在*连接*部分或*电子邮件*部分中，选择 Edit 以修改任一部分的设置。

禁止在计划的维护时段创建**AutoSupport**案例

通过 AutoSupport 案例禁止，您可以阻止在计划维护时段触发的 AutoSupport 消息创建不必要的案例。

步骤

1. 手动调用带有文本字符串的AutoSupport消息 `MAINT=xh`，其中 `x` 是维护窗口的持续时间(以小时为单位)。将<node>替换为要从中发送AutoSupport消息的节点的名称：

```
system node autosupport invoke -node <node> -message MAINT=xh
```

相关信息

- "ONTAP 命令参考"
- "如何在计划的维护时段禁止自动创建案例"

使用AutoSupport上传文件

上传核心转储文件

保存核心转储文件时，系统会生成一条事件消息。如果 AutoSupport 服务已启用并配置为向 NetApp 支持发送消息，则会传输 AutoSupport 消息，并自动向您发送电子邮件确认。

您需要的内容

- 您必须已使用以下设置设置 AutoSupport：
  - 已在节点上启用 AutoSupport 。
  - AutoSupport 已配置为向技术支持发送消息。
  - AutoSupport 已配置为使用 HTTP 或 HTTPS 传输协议。

    发送包含核心转储文件等大型文件的消息时，不支持 SMTP 传输协议。

关于此任务

您还可以使用通过AutoSupport服务通过HTTPS上传核心转储文件 `system node autosupport invoke-core-upload` 命令(如果NetApp支持部门要求)。

"如何将文件上传到 NetApp"

步骤

1. 使用查看节点的核心转储文件 `system node coredump show` 命令：

   在以下示例中，将显示本地节点的核心转储文件：

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------- -----
-----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. 使用生成AutoSupport消息并上传核心转储文件 `system node autosupport invoke-core-upload` 命

令：

在以下示例中，系统会生成一条 AutoSupport 消息并将其发送到默认位置（即技术支持），并且核心转储文件会上传到默认位置（即 NetApp 支持站点）：

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

在以下示例中，将生成一条 AutoSupport 消息并发送到 URI 中指定的位置，并且核心转储文件将上传到 URI：

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

上传性能归档文件

您可以生成并发送包含性能归档的 AutoSupport 消息。默认情况下， NetApp 技术支持会收到 AutoSupport 消息，而性能归档会上传到 NetApp 支持站点。您可以为消息指定备用目标并上传。

您需要的内容

- 您必须已使用以下设置设置 AutoSupport：
  - 已在节点上启用 AutoSupport 。
  - AutoSupport 已配置为向技术支持发送消息。
  - AutoSupport 已配置为使用 HTTP 或 HTTPS 传输协议。

    发送包含性能归档文件等大型文件的消息时，不支持 SMTP 传输协议。

关于此任务

您必须指定要上传的性能归档数据的开始日期。大多数存储系统会将性能归档保留两周，使您可以指定最长两周前的开始日期。例如，如果今天是 1 月 15 日，则可以指定开始日期 1 月 2 日。

步骤

1. 使用生成AutoSupport消息并上传性能归档文件 `system node autosupport invoke-performance-archive` 命令：

   在以下示例中，将从 2015 年 1 月 12 日起 4 小时的性能归档文件添加到 AutoSupport 消息中并上传到默认位置，即 NetApp 支持站点：

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

在以下示例中，将从 2015 年 1 月 12 日起 4 小时的性能归档文件添加到 AutoSupport 消息中并上传到 URI 指定的位置：

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

故障排除

在未收到消息时对 **AutoSupport** 进行故障排除

如果系统未发送 AutoSupport 消息，您可以确定这是因为 AutoSupport 无法生成消息还是无法传送消息。

步骤

1. 使用检查消息的传送状态 `system node autosupport history show` 命令：
2. 读取状态。

此状态	表示
正在初始化	收集过程正在启动。如果此状态为临时状态，则一切正常。但是，如果此状态仍然存在，则会显示问题描述。
收集失败	AutoSupport 无法在 spool 目录中创建 AutoSupport 内容。您可以输入来查看AutoSupport尝试收集的内容 `system node autosupport history show -detail` 命令：
正在收集	AutoSupport 正在收集 AutoSupport 内容。您可以输入来查看AutoSupport收集的内容 `system node autosupport manifest show` 命令：
已排队	AutoSupport 消息已排队等待传送，但尚未传送。
正在传输	AutoSupport 当前正在传送消息。
已成功发送	AutoSupport 已成功传送消息。您可以输入来了解AutoSupport将消息传送到何处 `system node autosupport history show -delivery` 命令：
忽略	AutoSupport 没有消息的目标。您可以输入来查看交付详细信息 `system node autosupport history show -delivery` 命令：
已重新排队	AutoSupport 尝试传送消息，但尝试失败。因此， AutoSupport 会将消息重新置于传送队列中，以便再次尝试发送。您可以输入来查看此错误 `system node autosupport history show` 命令：

此状态	表示
传输失败	AutoSupport 无法传送消息达到指定次数，并停止尝试传送消息。您可以输入来查看此错误 `system node autosupport history show` 命令：
OnDemand —忽略	已成功处理此 AutoSupport 消息，但 AutoSupport OnDemand 服务选择忽略此消息。

3. 执行以下操作之一：

的状态	执行此操作 ...
初始化或收集失败	请联系NetApp支持部门、因为AutoSupport 无法生成消息。请参阅以下知识库文章： "AutoSupport is failing to deliver：状态停留在initializing状态"
忽略，重新排队或传输失败	检查是否已为目标正确配置 SMTP ， HTTP 或 HTTPS ，因为 AutoSupport 无法传送消息。

对通过 **HTTP** 或 **HTTPS** 传送 **AutoSupport** 消息进行故障排除

如果系统未发送预期的 AutoSupport 消息，并且您使用的是 HTTP 或 HTTPS ，或者自动更新功能不起作用，则可以检查多项设置来解决此问题。

您需要的内容

您应已确认基本网络连接和 DNS 查找：

- 您的节点管理 LIF 必须处于运行和管理状态。
- 您必须能够从集群管理 LIF （而不是任何节点上的 LIF ）对同一子网上运行正常的主机执行 ping 操作。
- 您必须能够从集群管理 LIF 对子网以外正在运行的主机执行 ping 操作。
- 您必须能够使用主机的名称（而不是 IP 地址）从集群管理 LIF 对子网外正常运行的主机执行 ping 操作。

关于此任务

如果您已确定 AutoSupport 可以生成消息，但无法通过 HTTP 或 HTTPS 传送消息，请执行以下步骤。

如果您遇到错误或无法完成此操作步骤中的某个步骤，请先确定并解决此问题，然后再继续执行下一步。

步骤

1. 显示 AutoSupport 子系统的详细状态：

   ```
   system node autosupport check show-details
   ```

   其中包括通过发送测试消息来验证与 AutoSupport 目标的连接，并提供 AutoSupport 配置设置中可能出现的错误列表。

2. 验证节点管理 LIF 的状态：

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   。 `status-oper` 和 `status-admin` 字段应返回"`up`"。

3. 记录 SVM 名称， LIF 名称和 LIF IP 地址，以供日后使用。
4. 确保已启用并正确配置 DNS ：

   ```
   vserver services name-service dns show
   ```

5. 解决 AutoSupport 消息返回的任何错误：

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   有关对任何返回的错误进行故障排除的帮助、请参见 "《ONTAP AutoSupport (传输HTTPS和HTTP)解决指南》"。

6. 确认集群可以成功访问所需的服务器和 Internet ：

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > 地址 `support.netapp.com` 自身不响应ping/traceroute、但每跳信息非常重要。

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   如果其中任何一条路由无法正常运行，请尝试使用大多数第三方网络客户端上的 "`traceroute` " 或 "`tracert` " 实用程序从与集群位于同一子网上且正常运行的主机执行相同的路由。这有助于您确定问题描述是位于网络配置还是集群配置中。

7. 如果您对 AutoSupport 传输协议使用 HTTPS ，请确保 HTTPS 流量可以退出您的网络：

   a. 在与集群管理 LIF 相同的子网上配置 Web 客户端。

      确保所有配置参数的值与 AutoSupport 配置的值相同，包括使用相同的代理服务器，用户名，密码和端口。

   b. 访问 `https://support.netapp.com` 使用Web客户端。

      访问应成功。如果没有，请确保已正确配置所有防火墙以允许 HTTPS 和 DNS 流量，并且已正确配置代理服务器。有关为support.netapp.com配置静态名称解析的详细信息、请参见知识库文章 "如何在 ONTAP for support.netapp.com? 中添加主机条目"

8. 从 ONTAP 9.10.1 开始，如果您启用了自动更新功能，请确保与以下其他 URL 建立 HTTPS 连接：
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com

- https://support-sg-nawest.netapp.com

对通过 **SMTP** 传送 **AutoSupport** 消息进行故障排除

如果系统无法通过 SMTP 传送 AutoSupport 消息，您可以检查多项设置来解决此问题。

您需要的内容

您应已确认基本网络连接和 DNS 查找：

- 您的节点管理 LIF 必须处于运行和管理状态。
- 您必须能够从集群管理 LIF （而不是任何节点上的 LIF ）对同一子网上运行正常的主机执行 ping 操作。
- 您必须能够从集群管理 LIF 对子网以外正在运行的主机执行 ping 操作。
- 您必须能够使用主机的名称（而不是 IP 地址）从集群管理 LIF 对子网外正常运行的主机执行 ping 操作。

关于此任务

如果您已确定 AutoSupport 可以生成消息，但无法通过 SMTP 传送消息，则可以执行以下步骤。

如果您遇到错误或无法完成此操作步骤中的某个步骤，请先确定并解决此问题，然后再继续执行下一步。

除非另有说明，否则所有命令均在 ONTAP 命令行界面中输入。

步骤

1. 验证节点管理 LIF 的状态：

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   。 `status-oper` 和 `status-admin` 字段应返回 `up`。

2. 记录 SVM 名称， LIF 名称和 LIF IP 地址，以供日后使用。
3. 确保已启用并正确配置 DNS ：

   ```
   vserver services name-service dns show
   ```

4. 显示配置为由 AutoSupport 使用的所有服务器：

   ```
   system node autosupport show -fields mail-hosts
   ```

   记录显示的所有服务器名称。

5. 对于上一步显示的每个服务器、和 `support.netapp.com`下，确保节点可以访问服务器或URL：

   ```
   network traceroute -node local -destination server_name
   ```

   如果其中任何一条路由无法正常运行，请使用大多数第三方网络客户端上的 "`traceroute` " 或 "`tracert` " 实用程序，尝试从与集群位于同一子网上且正常运行的主机执行相同的路由。这有助于您确定问题描述是位于网络配置还是集群配置中。

6. 登录到指定为邮件主机的主机，并确保它可以处理 SMTP 请求：

netstat -aAn|grep 25

25 是侦听器SMTP端口号。

此时将显示类似于以下文本的消息：

```
ff64878c tcp        0      0  *.25    *.*    LISTEN.
```

7. 从其他某个主机上，使用邮件主机的 SMTP 端口打开 Telnet 会话：

   telnet *mailhost* 25

   此时将显示类似于以下文本的消息：

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. 在 telnet 提示符处，确保可以从邮件主机中继消息：

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   domain_name 是网络的域名。

   如果返回一个错误，指出中继被拒绝，则邮件主机上不会启用中继。请与系统管理员联系。

9. 在 telnet 提示符处，发送一条测试消息：

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   > 请确保在一行中单独输入最后一个句点（.）。句点向邮件主机指示消息已完成。

   如果返回错误，则表示未正确配置邮件主机。请与系统管理员联系。

10. 从 ONTAP 命令行界面，将 AutoSupport 测试消息发送到您有权访问的可信电子邮件地址：

    system node autosupport invoke -node local -type test

11. 查找尝试的序列号：

```
system node autosupport history show -node local -destination smtp
```

根据时间戳查找尝试的序列号。这可能是最近一次尝试。

12. 显示测试消息尝试的错误：

```
system node autosupport history show -node local -seq-num seq_num -fields
error
```

如果显示的错误为 `Login denied`，则SMTP服务器不接受来自集群管理LIF的发送请求。如果您不想更改为使用 HTTPS 作为传输协议，请与站点网络管理员联系，以配置 SMTP 网关以处理此问题描述。

如果此测试成功，但发送到 mailto： autosupport@netapp.com 的同一消息未成功，请确保在所有 SMTP 邮件主机上启用 SMTP 中继，或者使用 HTTPS 作为传输协议。

如果即使将消息发送到本地管理的电子邮件帐户也不成功，请确认 SMTP 服务器已配置为转发具有以下两个特征的附件：

- "`7z` " 后缀
- "`application/x-7x-compressed` " MIME 类型。

对 **AutoSupport** 子系统进行故障排除

。 `system node check show` 可以使用命令验证与AutoSupport配置和交付相关的任何问题并对其进行故障排除。

步骤

1. 使用以下命令显示 AutoSupport 子系统的状态。

使用此命令 ...	要执行此操作 ...
`system node autosupport check show`	显示 AutoSupport 子系统的整体状态，例如 AutoSupport HTTP 或 HTTPS 目标， AutoSupport SMTP 目标， AutoSupport OnDemand 服务器和 AutoSupport 配置的状态
`system node autosupport check show-details`	显示 AutoSupport 子系统的详细状态，例如错误的详细说明和更正操作

运行状况监控

监控系统运行状况概述

运行状况监控器会主动监控集群中的某些严重情况，并在检测到故障或风险时发出警报。如果存在活动警报，则系统运行状况状态将报告集群的已降级状态。警报包含响应降级的系统运行状况所需的信息。

如果状态为 degraded ，则可以查看有关问题的详细信息，包括可能的发生原因和建议的恢复操作。解决此问题

后，系统运行状况将自动恢复为 OK 。

系统运行状况反映了多个单独的运行状况监控器。单个运行状况监控器中的降级状态会导致整个系统运行状况处于降级状态。

有关 ONTAP 如何支持集群交换机在集群中监控系统运行状况的详细信息，请参见 *cluster* Hardware Universe 。

"Hardware Universe 中支持的交换机"

有关集群交换机运行状况监控器（ Cluster Switch Health Monitor ， CSHM ） AutoSupport 消息的原因以及解决这些警报所需采取的必要操作的详细信息，您可以参阅知识库文章。

"AutoSupport 消息：运行状况监控器进程 CSHM"

运行状况监控的工作原理

各个运行状况监控器都有一组策略，可在发生特定情况时触发警报。了解运行状况监控的工作原理有助于您对问题做出响应并控制未来的警报。

运行状况监控包括以下组件：

- 单独监控特定子系统的运行状况，每个子系统都有自己的运行状况

  例如，存储子系统具有一个节点连接运行状况监控器。

- 一个整体系统运行状况监控器，用于整合各个运行状况监控器的运行状况

  任何一个子系统中的降级状态都会导致整个系统处于降级状态。如果没有子系统出现警报，则整体系统状态为 OK 。

每个运行状况监控器都由以下关键要素组成：

- 运行状况监控器可能会发出的警报

  每个警报都有一个定义，其中包括警报严重性及其可能的发生原因等详细信息。

- 用于确定何时触发每个警报的运行状况策略

  每个运行状况策略都有一个规则表达式，这是触发警报的确切条件或更改。

运行状况监控器会持续监控并验证其子系统中的资源，以查看其状况或状态是否发生变化。如果条件或状态更改与运行状况策略中的规则表达式匹配，则运行状况监控器将发出警报。警报会导致子系统的运行状况和整体系统运行状况降级。

响应系统运行状况警报的方式

发生系统运行状况警报时，您可以确认该警报，了解其详细信息，修复基本状况并防止其再次发生。

当运行状况监控器发出警报时，您可以通过以下任一方式做出响应：

- 获取有关警报的信息，其中包括受影响的资源，警报严重性，可能的发生原因，可能的影响以及更正操作。
- 获取有关警报的详细信息，例如发出警报的时间以及是否有任何其他人已确认警报。
- 获取有关受影响资源或子系统的状态的运行状况信息，例如特定磁盘架或磁盘。
- 确认警报以指示有人正在处理此问题，并将您自己标识为 "`确认者。`
- 通过采取警报中提供的更正操作解决问题，例如修复布线以解决连接问题。
- 如果系统未自动清除警报，请将其删除。
- 禁止警报以防止其影响子系统的运行状况。

  当您了解问题时，禁止非常有用。禁止警报后，警报可能仍会发生，但在出现禁止的警报时，子系统运行状况显示为 "`ok-on-suppressed 。` " 。

系统运行状况警报自定义

您可以通过启用和禁用定义何时触发警报的系统运行状况策略来控制运行状况监控器生成的警报。这样，您就可以根据特定环境自定义运行状况监控系统。

您可以通过显示有关生成的警报的详细信息或显示特定运行状况监控器，节点或警报 ID 的策略定义来了解策略名称。

禁用运行状况策略与禁止警报不同。禁止警报时，它不会影响子系统的运行状况，但警报仍可能发生。

如果禁用某个策略，则在其策略规则表达式中定义的条件或状态将不再触发警报。

要禁用的警报示例

例如，假设出现对您不有用的警报。您可以使用 `system health alert show -instance` 命令以获取警报的策略ID。您可以在中使用策略ID `system health policy definition show` 命令以查看有关策略的信息。查看规则表达式以及有关策略的其他信息后，您决定禁用此策略。您可以使用 `system health policy definition modify` 命令以禁用策略。

运行状况警报如何触发 **AutoSupport** 消息和事件

系统运行状况警报会在事件管理系统（ EMS ）中触发 AutoSupport 消息和事件，使您不仅可以直接使用运行状况监控系统，还可以使用 AutoSupport 消息和 EMS 监控系统的运行状况。

您的系统会在收到警报后五分钟内发送 AutoSupport 消息。AutoSupport 消息包括自上次 AutoSupport 消息以来生成的所有警报，但在前一周内为同一资源和可能的发生原因复制警报的警报除外。

某些警报不会触发 AutoSupport 消息。如果警报的运行状况策略禁止发送 AutoSupport 消息，则该警报不会触发 AutoSupport 消息。例如，默认情况下，运行状况策略可能会禁用 AutoSupport 消息，因为在发生问题时，AutoSupport 已生成消息。您可以使用将策略配置为不触发AutoSupport消息 `system health policy definition modify` 命令：

您可以使用查看前一周发送的所有警报触发的AutoSupport消息的列表 `system health autosupport trigger history show` 命令：

警报还会触发 EMS 事件的生成。每次创建警报以及清除警报时都会生成事件。

可用的集群运行状况监控器

有多个运行状况监控器可监控集群的不同部分。运行状况监控器可以检测事件，向您发送警报以及在清除事件后删除事件，从而帮助您从 ONTAP 系统中的错误中恢复。

运行状况监控器名称（标识符）	子系统名称（标识符）	目的
集群交换机（集群交换机）	交换机（交换机运行状况）	监控集群网络交换机和管理网络交换机的温度，利用率，接口配置，冗余（仅限集群网络交换机）以及风扇和电源运行情况。集群交换机运行状况监控器通过 SNMP 与交换机通信。SNMPv2c 是默认设置。 从 ONTAP 9.2 开始，此监控器可以检测并报告自上次轮询期间以来集群交换机重新启动的时间。
MetroCluster 网络结构	交换机	监控 MetroCluster 配置后端网络结构拓扑并检测错误配置，例如布线和分区不正确以及 ISL 故障。
MetroCluster 运行状况	互连， RAID 和存储	监控 FC-VI 适配器， FC 启动程序适配器，左后聚合和磁盘以及集群间端口
节点连接（节点连接）	CIFS 无中断运行（ CIFS-NDO ）	监控 SMB 连接，确保 Hyper-V 应用程序无中断运行。
存储（ SAS 连接）	监控节点级别的磁盘架，磁盘和适配器，以查看适当的路径和连接。	系统
不适用	聚合来自其他运行状况监控器的信息。	系统连接（ system-connect ）

自动接收系统运行状况警报

您可以使用手动查看系统运行状况警报 `system health alert show` 命令：但是，您应订阅特定事件管理系统（ EMS ）消息，以便在运行状况监控器生成警报时自动接收通知。

关于此任务

以下操作步骤介绍了如何为所有 hm.alert.raised 消息和所有 hm.alert.cleared 消息设置通知。

所有 hm.alert.raised 消息和所有 hm.alert.cleared 消息均包含 SNMP 陷阱。SNMP陷阱的名称是 `HealthMonitorAlertRaised` 和 `HealthMonitorAlertCleared`。有关 SNMP 陷阱的信息，请参见

Network Management Guide 。

步骤

1. 使用 `event destination create` 命令以定义要将EMS消息发送到的目标。

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. 使用 `event route add-destinations` 用于路由的命令 `hm.alert.raised` 消息和 `hm.alert.cleared` 发送到目标的消息。

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

相关信息

"网络管理"

响应降级的系统运行状况

当系统的运行状况处于降级状态时，您可以显示警报，阅读可能的发生原因和更正操作，显示有关降级子系统的信息并解决问题。此外，还会显示禁止的警报，以便您可以修改这些警报并查看它们是否已确认。

关于此任务

您可以通过查看AutoSupport消息或EMS事件或使用来发现已生成警报 `system health` 命令

步骤

1. 使用 `system health alert show` 命令以查看影响系统运行状况的警报。
2. 阅读警报的可能发生原因，可能影响和更正操作，确定您是可以解决问题还是需要更多信息。
3. 如果需要详细信息、请使用 `system health alert show -instance` 命令以查看可用于警报的追加信息。
4. 使用 `system health alert modify` 命令 `-acknowledge` 参数表示您正在处理特定警报。
5. 按照中所述、采取更正操作以解决问题 `Corrective Actions` 字段。

   更正操作可能包括重新启动系统。

   解决问题后，系统将自动清除警报。如果此子系统没有其他警报、则此子系统的运行状况将更改为 `OK`。如果所有子系统的运行状况均正常、则整体系统运行状况将更改为 `OK`。

6. 使用 `system health status show` 命令以确认系统运行状况是否为 `OK`。

   如果系统运行状况不是 `OK`，重复此操作步骤。

响应降级的系统运行状况的示例

通过查看因磁盘架缺少节点的两个路径而导致系统运行状况降级的具体示例，您可以查看在响应警报时命令行界面显示的内容。

启动 ONTAP 后，您将检查系统运行状况并发现状态为 degraded：

```
      cluster1::>system health status show
        Status
        ---------------
        degraded
```

您将显示警报以查明问题所在，并看到磁盘架 2 没有两个指向 node1 的路径：

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

您可以显示有关警报的详细信息以获取更多信息，包括警报 ID：

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

您确认警报以指示您正在处理该警报。

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

修复磁盘架 2 和节点 1 之间的布线，然后重新启动系统。然后、您再次检查系统运行状况、发现其状态为 `OK`：

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

配置集群和管理网络交换机的发现

集群交换机运行状况监控器会自动尝试使用 Cisco 发现协议（ CDP ）发现集群和管理网络交换机。如果运行状况监控器无法自动发现交换机，或者您不想使用 CDP 进行自动发现，则必须对其进行配置。

关于此任务

。 `system cluster-switch show` 命令可列出运行状况监控器发现的交换机。如果未在该列表中看到预期显示的交换机，则运行状况监控器将无法自动发现它。

步骤

1. 如果要使用CDP进行自动发现、请执行以下操作：

   a. 确保已在交换机上启用 Cisco 发现协议（ CDP ）。

      有关说明，请参见交换机文档。

   b. 在集群中的每个节点上运行以下命令，以验证是否已启用 CDP ：

      run -node *node_name* -command options cdpd.enable

      如果启用了 CDP ，请转至步骤 d如果 CDP 已禁用，请转至步骤 C

   c. 运行以下命令以启用 CDP ：

      run -node *node_name* -command options cdpd.enable on

   请等待五分钟，然后再执行下一步。

   a. 使用 `system cluster-switch show` 命令以验证ONTAP现在是否可以自动发现交换机。

2. 如果运行状况监控器无法自动发现交换机、请使用 `system cluster-switch create` 用于配置交换机发现的命令：

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   请等待五分钟，然后再执行下一步。

3. 使用 `system cluster-switch show` 命令以验证ONTAP是否可以发现您为其添加了信息的交换机。

完成后

验证运行状况监控器是否可以监控您的交换机。

验证对集群和管理网络交换机的监控

集群交换机运行状况监控器会自动尝试监控其发现的交换机；但是，如果交换机配置不正确，监控可能不会自动进行。您应验证是否已正确配置运行状况监控器以监控交换机。

步骤

1. 要确定集群交换机运行状况监控器发现的交换机、请输入以下命令：

   ONTAP 9.8及更高版本

   ```
   system switch ethernet show
   ```

   ONTAP 9.7及更早版本

   ```
   system cluster-switch show
   ```

   如果 `Model` 列显示值 `OTHER`，则ONTAP无法监控交换机。ONTAP会将此值设置为 `OTHER` 如果自动发现的交换机不支持运行状况监控。

   > 如果命令输出中未显示交换机、则必须配置交换机发现。

2. 升级到支持的最新交换机软件，并参考 NetApp 支持站点上的配置文件 (RCF)。

   "NetApp支持下载页面"

   交换机 RCF 中的社区字符串必须与配置为运行状况监控器使用的社区字符串匹配。默认情况下、运行状况监控器使用社区字符串 `cshm1!`。

   > 目前、运行状况监控器仅支持SNMPv2。

   如果需要更改有关集群监控的交换机的信息、可以使用以下命令修改运行状况监控器使用的社区字符串：

   ONTAP 9.8及更高版本

   ```
   system switch ethernet modify
   ```

   ONTAP 9.7及更早版本

   ```
   system cluster-switch modify
   ```

3. 验证交换机的管理端口是否已连接到管理网络。

   要执行 SNMP 查询，需要此连接。

用于监控系统运行状况的命令

您可以使用 `system health` 用于显示系统资源运行状况信息、响应警报以及配置未来警报的命令。使用命令行界面命令，您可以深入查看有关如何配置运行状况监控的信息。这些命令的手册页包含更多信息。

显示系统运行状况的状态

如果您要 ...	使用此命令 ...
显示系统的运行状况，其中反映了各个运行状况监控器的整体状态	`system health status show`
显示运行状况监控可用的子系统的运行状况	`system health subsystem show`

显示节点连接的状态

如果您要 ...	使用此命令 ...
显示有关从节点到存储架的连接的详细信息，包括端口信息， HBA 端口速度， I/O 吞吐量以及每秒 I/O 操作速率	`storage shelf show -connectivity` 使用 `-instance` 用于显示每个磁盘架详细信息的参数。
显示有关驱动器和阵列 LUN 的信息，包括可用空间，磁盘架和托架编号以及所属节点名称	`storage disk show` 使用 `-instance` 用于显示每个驱动器的详细信息的参数。
显示有关存储架端口的详细信息，包括端口类型，速度和状态	`storage port show` 使用 `-instance` 用于显示每个适配器详细信息的参数。

管理集群、存储和管理网络交换机的发现

如果您要 ...	使用此命令。**(ONTAP 9.8**及更高版本**)**	使用此命令。**(ONTAP 9.7**及更早版本**)**
显示集群监控的交换机	`system switch ethernet show`	`system cluster-switch show`

如果您要 ...	使用此命令。(ONTAP 9.8及更高版本)	使用此命令。(ONTAP 9.7及更早版本)
显示集群当前监控的交换机，包括您删除的交换机（显示在命令输出的原因列中）以及通过网络访问集群和管理网络交换机所需的配置信息。 此命令可在高级权限级别下使用。	`system switch ethernet show-all`	`system cluster-switch show-all`
配置发现未发现的交换机	`system switch ethernet create`	`system cluster-switch create`
修改有关集群监控的交换机的信息（例如，设备名称， IP 地址，SNMP 版本和社区字符串）	`system switch ethernet modify`	`system cluster-switch modify`
禁用对交换机的监控	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
禁用对交换机的发现和监控，并删除交换机配置信息	`system switch ethernet delete`	`system cluster-switch delete`
永久删除存储在数据库中的交换机配置信息（这样做会重新启用交换机的自动发现）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
启用自动日志记录以随 AutoSupport 消息一起发送。	`system switch ethernet log`	`system cluster-switch log`

响应生成的警报

如果您要 ...	使用此命令 ...
显示有关生成的警报的信息，例如触发警报的资源和节点，警报的严重性和可能的发生原因	`system health alert show`
显示有关生成的每个警报的信息	`system health alert show -instance`
指示有人正在处理警报	`system health alert modify`
确认警报	`system health alert modify -acknowledge`
禁止后续警报，使其不会影响子系统的运行状况	`system health alert modify -suppress`

如果您要 ...	使用此命令 ...
删除未自动清除的警报	`system health alert delete`
显示有关上周触发警报的 AutoSupport 消息的信息，例如，确定警报是否触发 AutoSupport 消息	`system health autosupport trigger history show`

配置未来警报

如果您要 ...	使用此命令 ...
启用或禁用控制特定资源状态是否引发特定警报的策略	`system health policy definition modify`

显示有关如何配置运行状况监控的信息

如果您要 ...	使用此命令 ...
显示有关运行状况监控器的信息，例如其节点，名称，子系统和状态	`system health config show` 使用 `-instance` 参数、用于显示有关每个运行状况监控器的详细信息。
显示有关运行状况监控器可能生成的警报的信息	`system health alert definition show` 使用 `-instance` 用于显示有关每个警报定义的详细信息的参数。
显示有关运行状况监控策略的信息，这些策略可确定何时发出警报	`system health policy definition show` 使用 `-instance` 参数以显示有关每个策略的详细信息。使用其他参数筛选警报列表，例如，按策略状态（是否已启用），运行状况监控器，警报等进行筛选。

显示环境信息

传感器可帮助您监控系统的环境组件。您可以显示的环境传感器信息包括其类型，名称，状态，值和阈值警告。

步骤

1. 要显示有关环境传感器的信息、请使用 `system node environment sensors show` 命令：

文件系统分析

文件系统分析概述

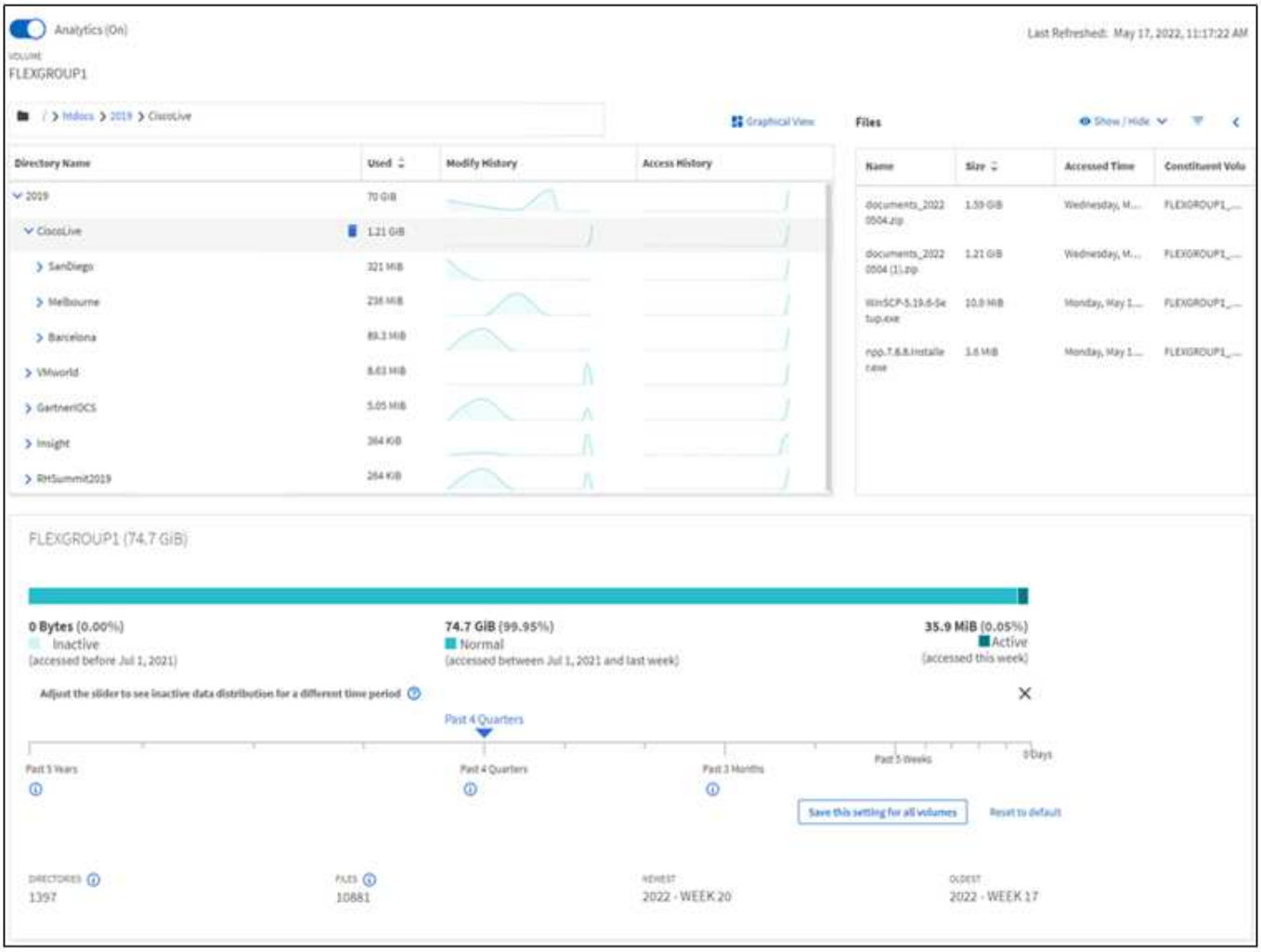
文件系统分析(File System Analytics、FSA)是在ONTAP 9.8中首次推出的、用于实时查看ONTAP FlexGroup 或FlexVol 卷中的文件使用情况和存储容量趋势。此原生 功能无需使用外部工具、并可提供有关如何利用存储以及是否有机会根据业务需求优化存储的重要见解。

借助FSA、您可以在NAS中查看卷文件系统层次结构的所有级别。例如、您可以了解Storage VM (SVM)、卷、目录和文件级别的使用情况和容量。您可以使用FSA问题解答 解决以下问题：

- 什么是填满我的存储？是否有任何大文件可以移动到其他存储位置？
- 哪些是我最活跃的卷、目录和文件？我的存储性能是否针对用户需求进行了优化？
- 上个月添加了多少数据？
- 谁是我最活跃或最不活跃的存储用户？
- 主存储上有多少非活动或休眠数据？我是否可以将这些数据移至成本较低的冷层？
- 我计划内的服务质量变更是否会对访问经常访问的关键文件产生负面影响？

文件系统分析已集成到ONTAP System Manager中。System Manager中的视图提供：

- 实时可见性、可实现有效的数据管理和操作
- 实时数据收集和聚合
- 子目录以及文件大小和计数以及关联的性能配置文件
- 用于修改和访问历史记录的文件期限直方图



支持的卷类型

文件系统分析旨在提供对包含活动 NAS 数据的卷的可见性，但 FlexCache 缓存和 SnapMirror 目标卷除外。

文件系统分析功能的可用性

每个ONTAP版本都扩展了文件系统分析的范围。

	ONTAP 9.15.1.	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
System Manager 中的可视化	✓	✓	✓	✓	✓	✓	✓	✓
容量分析	✓	✓	✓	✓	✓	✓	✓	✓
非活动数据信息	✓	✓	✓	✓	✓	✓	✓	✓
支持从Data ONTAP 7-模式过渡的卷	✓	✓	✓	✓	✓	✓	✓	
可以在System Manager中自定义非活动期限	✓	✓	✓	✓	✓	✓	✓	
卷级别活动跟踪	✓	✓	✓	✓	✓	✓		

	ONTAP 9.15.1.	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
将活动跟踪数据下载到CSV	✓	✓	✓	✓	✓	✓		
SVM级别的活动跟踪	✓	✓	✓	✓	✓			
时间线	✓	✓	✓	✓	✓			
使用情况分析	✓	✓	✓	✓				
选项以默认启用文件系统分析	✓	✓	✓					
初始化扫描进度监控器	✓	✓						

了解有关文件系统分析的更多信息

进一步阅读

- "TR 4687：《 ONTAP 文件系统分析最佳实践准则》"
- "知识库：启用NetApp ONTAP 文件系统分析后的高延迟或波动延迟"

启用文件系统分析

要收集和显示容量分析等使用情况数据、您需要在卷上启用文件系统分析。

关于此任务

- 从ONTAP 9.8开始、您可以对新卷或现有卷启用文件系统分析。如果要将系统升级到ONTAP 9.8或更高版本、请确保在启用文件系统分析之前已完成所有升级过程。
- 启用分析所需的时间取决于卷的大小和内容。System Manager 将显示进度并在完成后提供分析数据。如果

需要有关初始化扫描进度的更精确信息、可以使用ONTAP命令行界面命令 `volume analytics show`。

- 从ONTAP 9.14.1开始、ONTAP除了提供有关影响扫描进度的限制事件的通知之外、还提供初始化扫描的进度跟踪。
- 从ONTAP 9.15.1开始、您只能在一个节点上同时执行四次初始化扫描。您必须等待扫描完成、然后才能启动新扫描。ONTAP还会强制要求卷上有足够的可用空间、如果没有、则会显示错误消息。确保卷的可用空间至少有5%到8%可用。如果卷已启用自动调整大小、请根据最大自动增长大小计算可用大小。
- 有关初始化扫描的更多注意事项、请参见 扫描注意事项。

在现有卷上启用文件系统分析

您可以使用ONTAP System Manager或命令行界面启用文件系统分析。

示例 **2.** 步骤

System Manager

在 **ONTAP 9.8** 和 **9.9.1** 中	从 **ONTAP 9.10.1** 开始
1. 选择 * 存储 > 卷 * 。 2. 选择所需的卷，然后选择 * 资源管理器 * 。 3. 选择 * 启用分析 * 或 * 禁用分析 * 。	1. 选择 * 存储 > 卷 * 。 2. 选择所需的卷。从单个卷菜单中，选择 * 文件系统 > 资源管理器 * 。 3. 选择 * 启用分析 * 或 * 禁用分析 * 。

命令行界面

使用 **CLI** 启用文件系统分析

1. 运行以下命令：
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`
   默认情况下，命令在前台运行； ONTAP 将显示进度并在完成后提供分析数据。如果您需要更精确的信息、可以使用在后台运行命令 `-foreground false` 选项、然后使用 `volume analytics show` 命令以在命令行界面中显示初始化进度。
2. 成功启用文件系统分析后、请使用System Manager或ONTAP REST API显示分析数据。

修改默认的文件系统分析设置

从ONTAP 9.13.1开始、您可以修改SVM或集群设置、以便在新卷上默认启用文件系统分析。

示例 **3.** 步骤

System Manager

如果您使用的是System Manager、则可以修改Storage VM或集群设置、以便默认在创建卷时启用容量分析和活动跟踪。默认启用仅在修改设置后创建的适用场景卷、而不是现有卷。

修改集群上的文件系统分析设置

1. 在System Manager中、导航到集群设置。
2. 在群集设置中，查看文件系统设置选项卡。要修改设置、请选择图标。
3. 默认情况下，在“活动跟踪”字段中，输入要启用活动跟踪的SVM的名称。将此字段留空将使所有SVM上的活动跟踪处于禁用状态。

   取消选中在新**Storage VM**上启用复选框，默认情况下在新Storage VM上禁用活动跟踪。

4. 在分析字段中，输入默认情况下要启用容量分析的Storage VM的名称。将此字段留空将使所有SVM上的容量分析处于禁用状态。

   取消选中在新**Storage VM**上启用复选框可在默认情况下在新Storage VM上禁用容量分析。

5. 选择保存。

修改**SVM**上的文件系统分析设置

1. 选择要修改的SVM，然后选择 **Storage VM**设置。
2. 在文件系统分析卡中，使用切换为Storage VM上的所有新卷启用或禁用活动跟踪和容量分析。

命令行界面

您可以使用ONTAP命令行界面将Storage VM配置为在新卷上默认启用文件系统分析。

默认情况下、在**SVM**上启用文件系统分析

1. 修改SVM、以便在所有新创建的卷上默认启用容量分析和活动跟踪：
   ```
   vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto
   -enable-analytics true
   ```

查看文件系统活动

启用文件系统分析(File System Analytics、FSA)后、您可以按每个子树中使用的空间排序、查看选定卷的根目录内容。

选择任何文件系统对象以浏览文件系统并显示有关目录中每个对象的详细信息。有关目录的信息也可以以图形方式显示。随着时间的推移，会显示每个子树的历史数据。如果目录数超过 3000 个，则不会对已用空间进行排序。

资源管理器

文件系统分析 * 资源管理器 * 屏幕包含三个区域：

- 目录和子目录的树视图；显示名称，大小，修改历史记录和访问历史记录的可扩展列表。

- 文件；显示目录列表中选定对象的名称，大小和访问时间。
- 目录列表中选定对象的活动和非活动数据比较。

  从 ONTAP 9.1.1 开始，您可以自定义要报告的范围。默认值为一年。根据这些自定义设置，您可以采取更正操作，例如移动卷和修改分层策略。

默认情况下，会显示访问时间。但是、如果已通过命令行界面(通过设置 `-atime-update` 选项 `false` 使用 `volume modify` 命令)、则仅显示上次修改时间。例如：

- 树视图不会显示 * 访问历史记录 * 。
- 文件视图将被更改。
- 活动/非活动数据视图将基于修改后的时间 (`mtime`）。

使用这些显示，您可以检查以下内容：

- 文件系统位置占用的空间最多
- 有关目录树的详细信息，包括目录和子目录中的文件和子目录计数
- 包含旧数据的文件系统位置（例如， Scratch ， temp 或日志树）

解释 FSA 输出时，请记住以下几点：

- FSA 将显示数据在何处以及何时使用，而不是显示正在处理的数据量。例如，最近访问或修改的文件占用的空间较大并不一定表示系统处理负载较高。
- * 卷资源管理器 * 选项卡计算 FSA 空间消耗的方式可能与其他工具不同。特别是，如果卷启用了存储效率功能，则与 * 卷概述 * 中报告的使用量可能会有显著差异。这是因为 * 卷资源管理器 * 选项卡不包括效率节省。
- 由于目录显示中的空间限制，无法在 *List View* 中查看超过 8 个级别的目录深度。要查看深度超过 8 个级别的目录，必须切换到 *Graphical View* ，找到所需的目录，然后切换回 *List View* 。这样可以在显示中留出更多的屏幕空间。

步骤

1. 查看选定卷的根目录内容：

在 **ONTAP 9.8** 和 **9.9.1** 中	从 **ONTAP 9.10.1** 开始
单击 * 存储 > 卷 * ，选择所需的卷，然后单击 * 资源管理器 * 。	选择 * 存储 > 卷 * ，然后选择所需的卷。从单个卷菜单中，选择 * 文件系统 > 资源管理器 * 。

启用活动跟踪

从ONTAP 9.10.1开始、文件系统分析包括一项活动跟踪功能、可用于识别热对象并将数据下载为CSV文件。从ONTAP 9.11.1开始、活动跟踪已扩展到SVM范围。此外、从ONTAP 9.11.1开始、System Manager还提供了活动跟踪时间表、您可以查看长达五分钟的活动跟踪数据。

通过活动跟踪，可以监控以下四个类别：

- 目录
- 文件
- 客户端
- 用户

对于监控的每个类别，活动跟踪将显示读取 IOPS ，写入 IOPS ，读取吞吐量和写入吞吐量。有关活动跟踪的查询，每 10 到 15 秒刷新一次与系统中在前五秒间隔内发现的热点相关的信息。

活动跟踪信息为近似信息，数据的准确性取决于传入 I/O 流量的分布情况。

在System Manager中查看卷级别的活动跟踪时、只有扩展卷的菜单才会主动刷新。如果任何卷的视图已折叠，则只有在卷显示展开后，这些卷才会刷新。您可以使用 * 暂停刷新 * 按钮停止刷新。可以下载 CSV 格式的活动数据，此格式将显示为选定卷捕获的所有时间点数据。

从ONTAP 9.11.1开始提供时间线功能、您可以记录卷或SVM上的热点活动、大约每五秒持续更新一次、并保留前五分钟的数据。只有页面的可见区域字段才会保留时间线数据。如果折叠跟踪类别或滚动以使时间线无法显示、则时间线将停止收集数据。默认情况下、时间线处于禁用状态、当您离开活动选项卡时、时间线将自动禁用。

为单个卷启用活动跟踪

您可以使用ONTAP系统管理器或命令行界面启用活动跟踪。

关于此任务

如果将 RBAC 与 ONTAP REST API 或 System Manager 结合使用，则需要创建自定义角色来管理对活动跟踪的访问。请参见 基于角色的访问控制 。

System Manager

步骤

1. 选择 * 存储 > 卷 * 。选择所需的卷。从单个卷菜单中，选择文件系统，然后选择活动选项卡。
2. 确保已启用 * 活动跟踪 * ，以查看有关顶层目录，文件，客户端和用户的各个报告。
3. 要在不刷新的情况下更深入地分析数据，请选择 * 暂停刷新 * 。您也可以下载数据以获取报告的 CSV 记录。

命令行界面

步骤

1. 启用活动跟踪：

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 使用命令检查卷的活动跟踪状态是打开还是关闭：

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 启用后，使用 ONTAP 系统管理器或 ONTAP REST API 显示活动跟踪数据。

为多个卷启用活动跟踪

您可以使用System Manager或命令行界面为多个卷启用活动跟踪。

关于此任务

如果将 RBAC 与 ONTAP REST API 或 System Manager 结合使用，则需要创建自定义角色来管理对活动跟踪的访问。请参见 基于角色的访问控制 。

System Manager

为特定卷启用

1. 选择 * 存储 > 卷 * 。选择所需的卷。从单个卷菜单中，选择文件系统，然后选择活动选项卡。
2. 选择要启用活动跟踪的卷。在卷列表顶部、选择*更多选项*按钮。选择*启用活动跟踪*。
3. 要在SVM级别查看活动跟踪、请从*存储>卷*中选择要查看的特定SVM。导航到文件系统选项卡、然后导航到活动、您将看到已启用活动跟踪的卷的数据。

为所有卷启用

1. 选择 * 存储 > 卷 * 。从菜单中选择一个SVM。
2. 导航到*文件系统*选项卡、选择*更多*选项卡以对SVM中的所有卷启用活动跟踪。

命令行界面

从ONTAP 9.13.1开始、您可以使用ONTAP命令行界面为多个卷启用活动跟踪。

步骤

1. 启用活动跟踪：

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   使用 … * 为指定Storage VM上的所有卷启用活动跟踪。

   使用 … ！后跟卷名称、以便为SVM上的所有卷(命名卷除外)启用活动跟踪。

2. 确认操作成功：

   ```
   volume show -fields activity-tracking-state
   ```

3. 启用后，使用 ONTAP 系统管理器或 ONTAP REST API 显示活动跟踪数据。

启用使用情况分析

从ONTAP 9.12.1开始、您可以启用使用情况分析来查看卷中哪些目录使用的空间最多。您可以查看卷中的目录总数或卷中的文件总数。报告仅限于使用最多空间的25个目录。

大型目录的分析每15分钟刷新一次。您可以通过在页面顶部检查上次刷新的时间戳来监控最近的刷新。您也可以单击"下载"按钮将数据下载到Excel工作簿。下载操作在后台运行、并显示选定卷的最新报告信息。如果扫描返回时未显示任何结果、请确保卷处于联机状态。SnapRestore 等事件将通过发生原因 文件系统分析功能重建其大型目录列表。

步骤

1. 选择 * 存储 > 卷 * 。选择所需的卷。
2. 从单个卷菜单中、选择*文件系统*。然后选择*使用情况*选项卡。
3. 切换*分析*开关以启用使用情况分析。
4. System Manager将显示一个条形图、以降序标识大小最大的目录。

> 在收集顶层目录列表时、ONTAP 可能会显示部分数据或根本不显示任何数据。扫描进度可以位于扫描期间显示的*使用情况*选项卡中。

要深入了解特定目录、您可以执行以下操作 查看文件系统上的活动。

根据分析结果采取更正操作

从ONTAP 9.1.1开始、您可以直接从文件系统分析显示中根据当前数据和所需结果采取更正操作。

删除目录和文件

在资源管理器显示中，您可以选择要删除的目录或单个文件。使用低延迟快速目录删除功能删除目录。（从 ONTAP 9.9.1 开始，也可以快速删除目录，而不会启用分析。）

步骤

1. 单击 * 存储 > 卷 * ，然后单击 * 资源管理器 * 。

   将鼠标悬停在文件或文件夹上时，将显示删除选项。一次只能删除一个对象。

> 删除目录和文件后，不会立即显示新的存储容量值。

在存储层中分配介质成本，以比较非活动数据存储位置的成本

介质成本是根据存储成本评估结果分配的一个值，表示为您选择的每 GB 货币。设置后， System Manager 将使用分配的介质成本预测移动卷时的预计节省量。

您设置的介质成本不是永久性的；只能为单个浏览器会话设置。

步骤

1. 单击*存储>层*，然后在所需本地层(聚合)磁贴中单击*设置媒体成本*。

   请务必选择活动层和非活动层以进行比较。

2. 输入货币类型和金额。

   输入或更改介质成本时，所有介质类型都会进行更改。

移动卷以降低存储成本

根据分析结果和介质成本比较、您可以将卷移至本地层中成本较低的存储。

一次只能比较和移动一个卷。

步骤

1. 启用介质成本显示后，单击 * 存储 > 层 * ，然后单击 * 卷 * 。
2. 要比较某个卷的目标选项，请单击该卷的，然后单击 ⋮ **move**。
3. 在 * 选择目标本地层 * 显示中，选择目标层以显示估计成本差异。
4. 比较选项后，选择所需层并单击 * 移动 * 。

通过文件系统分析实现基于角色的访问控制

从ONTAP 9.12.1开始、ONTAP 包括一个预定义的基于角色的访问控制(Role-Based Access Control、RBAC)角色、称为 `admin-no-fsa`。。 `admin-no-fsa` 角色授予管理员级别的权限、但会阻止用户执行与相关的操作 `files` ONTAP 命令行界面、REST API和System Manager中的端点(即文件系统分析)。

有关的详细信息、请参见 `admin-no-fsa` 角色、请参见 集群管理员的预定义角色。

如果您使用的是ONTAP 9.12.1之前发布的ONTAP 版本、则需要创建一个专用角色来控制对文件系统分析的访问。在ONTAP 9.12.1之前的ONTAP 版本中、您必须通过ONTAP 命令行界面或ONTAP REST API配置RBAC权限。

System Manager

从ONTAP 9.12.1开始、您可以使用System Manager为文件系统分析配置RBAC权限。

步骤

1. 选择*集群>设置*。在*安全性*下，导航至*用户和角色*，然后选择 →。
2. 在*roles*下，选择 + Add 。
3. 请为此角色提供一个名称。在角色属性下、通过提供相应的来配置用户角色的访问或限制 "API端点"。请参见下表、了解用于配置文件系统分析访问或限制的主路径和二级路径。

限制	主路径	二级路径
卷上的活动跟踪	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVM上的活动跟踪	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
所有文件系统分析操作	`/api/storage/volumes`	`/:uuid/files`

您可以使用 `/*/` 而不是使用UUID为端点的所有卷或SVM设置策略。

选择每个端点的访问权限。

4. 选择 * 保存 * 。
5. 要将角色分配给一个或多个用户、请参见 控制管理员访问。

命令行界面

如果您使用的是ONTAP 9.12.1之前发布的ONTAP 版本、请使用ONTAP 命令行界面创建自定义角色。

步骤

1. 创建一个默认角色以访问所有功能。

   在创建限制性角色之前需要执行此操作，以确保此角色仅对活动跟踪具有限制性：

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

2. 创建限制性角色：

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

3. 授权角色访问 SVM 的 Web 服务：

   - `rest` 用于REST API调用
   - `security` 用于密码保护
   - `sysmgr` 用于访问System Manager

```
vserver services web access create -vserver svm-name -name_ -name rest
-role storageAdmin

vserver services web access create -vserver svm-name -name security
-role storageAdmin

vserver services web access create -vserver svm-name -name sysmgr -role
storageAdmin
```

4. 创建用户。

   您必须为要应用于用户的每个应用程序问题描述 一个不同的 create 命令。在同一用户上多次调用 create 只会将所有应用程序应用于该用户，而不会每次创建新用户。。 `http` 应用程序类型的参数适用于ONTAP REST API和System Manager。

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

5. 现在、您可以使用新的用户凭据登录到System Manager或使用ONTAP REST API访问文件系统分析数据。

更多信息

- 集群管理员的预定义角色
- 使用System Manager控制管理员访问
- "详细了解RBAC角色和ONTAP REST API"

文件系统分析注意事项

您应了解与实施文件系统分析相关的特定使用限制和潜在性能影响。

受SVM保护的关系

如果已对包含 SVM 的卷处于保护关系中的卷启用文件系统分析，则分析数据不会复制到目标 SVM 。如果必须在恢复操作中重新同步源 SVM ，则必须在恢复后手动重新启用对所需卷的分析。

性能注意事项

在某些情况下、启用文件系统分析可能会对初始元数据收集期间的性能产生负面影响。在利用率达到最大的系统上、这种情况最常见。为了避免在此类系统上启用分析、您可以使用ONTAP System Manager性能监控工具。

如果延迟显著增加、请参阅知识库文章 "启用NetApp ONTAP 文件系统分析后延迟较高或波动较大"。

扫描注意事项

启用容量分析后、ONTAP将执行容量分析初始化扫描。扫描将访问已启用容量分析的卷中所有文件的元数据。扫描期间不读取任何文件数据。从ONTAP 9.14.1开始、您可以使用REST API、System Manager的资源管理器选项卡或跟踪扫描进度 `volume analytics show` CLI命令。如果发生限制事件、ONTAP将提供通知。

在卷上启用文件系统分析时、请确保卷的可用空间至少有5%到8%可用。如果卷已启用自动调整大小、请根据最大自动增长大小计算可用大小。从ONTAP 9.15.1开始、如果在卷上启用文件系统分析时可用空间不足、则ONTAP会显示错误消息。

扫描完成后、文件系统分析会随着文件系统的更改不断实时更新。

扫描所需时间与卷上的目录和文件数量成比例。由于扫描会收集元数据、因此文件大小不会影响扫描时间。

有关初始化扫描的详细信息、请参见 "TR-4867：《文件系统分析最佳实践准则》"。

最佳实践

您应对不共享聚合的卷启动扫描。您可以使用命令查看哪些聚合当前托管哪些卷：

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

在扫描运行期间、卷将继续为客户端流量提供服务。建议您在预期客户端流量较低的时段开始扫描。

如果客户端流量增加、则会占用系统资源、并通过发生原因 扫描所需时间更长。

从ONTAP 9.12.1开始、您可以在System Manager和ONTAP 命令行界面中暂停数据收集。

- 如果使用的是ONTAP 命令行界面：
  - 您可以使用命令暂停数据收集： `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - 客户端流量降低后、您可以使用以下命令恢复数据收集： `volume analytics initialization resume -vserver svm_name -volume volume_name`
- 如果您使用的是System Manager、则在卷菜单的*资源管理器*视图中、可以使用*暂停数据收集*和*恢复数据收集*按钮来管理扫描。

EMS配置

EMS配置概述

您可以将ONTAP 9配置为将重要的EMS (事件管理系统)事件通知直接发送到电子邮件地址、系统日志服务器、简单管理网络协议(SNMP)陷阱主机或webhook应用程序、以便您可

以立即收到需要立即引起关注的系统问题的通知。

由于默认情况下不会启用重要事件通知、因此您需要将EMS配置为向电子邮件地址、系统日志服务器、SNMP陷阱主机或webhook应用程序发送通知。

查看特定于版本的 "《ONTAP 9 EMS参考》"。

如果EMS事件映射使用已弃用的ONTAP 命令集(例如事件目标、事件路由)、则建议您更新映射。"了解如何使用已弃用的ONTAP 命令更新EMS映射"(英文)

使用 System Manager 配置 EMS 事件通知和筛选器

您可以使用 System Manager 配置事件管理系统（ Event Management System， EMS ）发送事件通知的方式，以便在出现需要及时关注的系统问题时收到通知。

ONTAP 版本	使用 System Manager，您可以 …
ONTAP 9.12.1及更高版本	将事件发送到远程系统日志服务器时、请指定传输层安全(TLS)协议。
ONTAP 9.10.1 及更高版本	配置电子邮件地址、系统日志服务器和webhook应用程序以及SNMP陷阱主机。
ONTAP 9.7 到 9.10.0	仅配置 SNMP 陷阱主机。 您可以使用 ONTAP 命令行界面配置其他 EMS 目标。 请参见 "EMS配置概述"。

您可以执行以下过程：

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

相关信息

- "《ONTAP EMS参考》"
- "使用 CLI 配置 SNMP 陷阱主机以接收事件通知"

添加 EMS 事件通知目标

您可以使用 System Manager 指定 EMS 消息要发送到的位置。

从ONTAP 9.12.1开始、可以通过传输层安全(Transport Layer Security、TLS)协议将EMS事件发送到远程系统日志服务器上的指定端口。有关详细信息，请参见 `event notification destination create` 手册页。

步骤

1. 单击 * 集群 > 设置 * 。

2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。
4. 单击 + Add 。
5. 指定名称， EMS 目标类型和筛选器。

> 如果需要，您可以添加新筛选器。 单击 * 添加新事件筛选器 * 。

6. 根据您选择的 EMS 目标类型，指定以下内容：

配置…	指定或选择…
SNMP 陷阱主机	• TrapHost 名称
email （从 9.10.1 开始）	• 目标电子邮件地址 • 邮件服务器 • 发件人电子邮件地址
系统日志服务器 （从 9.10.1 开始）	• 服务器的主机名或 IP 地址 • 系统日志端口(从9.12.1开始) • 系统日志传输(从9.12.1开始) 选择* TCP加密*将启用传输层安全(TLS)协议。如果没有为*系统日志端口*输入任何值、则会根据*系统日志传输*选项使用默认值。
网络钩 （从 9.10.1 开始）	• webhook URL • 客户端身份验证（选择此选项可指定客户端证书）

创建新的 **EMS** 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 定义新的自定义筛选器，以指定处理 EMS 通知的规则。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 单击 + Add 。
5. 指定一个名称，然后选择是要从现有事件筛选器复制规则还是添加新规则。
6. 根据您的选择，执行以下步骤：

如果选择… 。	然后，执行以下步骤…

• 从现有事件筛选器复制规则 *	1. 选择现有事件筛选器。 2. 修改现有规则。 3. 如果需要，可通过单击来添加其他规则 + Add 。
• 添加新规则 *	为每个新规则指定类型，名称模式，严重性和 SNMP 陷阱类型。

编辑 **EMS** 事件通知目标

从 ONTAP 9.10.1 开始，您可以使用 System Manager 更改事件通知目标信息。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。
4. 在事件目标的名称旁边，单击，然后单击 ⋮**Edit**。
5. 修改事件目标信息，然后单击 * 保存 * 。

编辑 **EMS** 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 修改自定义筛选器以更改事件通知的处理方式。

> 您不能修改系统定义的筛选器。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 在事件过滤器的名称旁边，单击，然后单击 ⋮**Edit**。
5. 修改事件筛选器信息，然后单击 * 保存 * 。

删除 **EMS** 事件通知目标

从 ONTAP 9.10.1 开始，您可以使用 System Manager 删除 EMS 事件通知目标。

> 您不能删除 SNMP 目标。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。
4. 在事件目标的名称旁边，单击，然后单击 ⋮**Delete**。

删除 **EMS** 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 删除自定义筛选器。

> 您不能删除系统定义的筛选器。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 在事件过滤器的名称旁边，单击，然后单击 ⋮**Delete**。

使用 **CLI** 配置 **EMS** 事件通知

EMS配置工作流

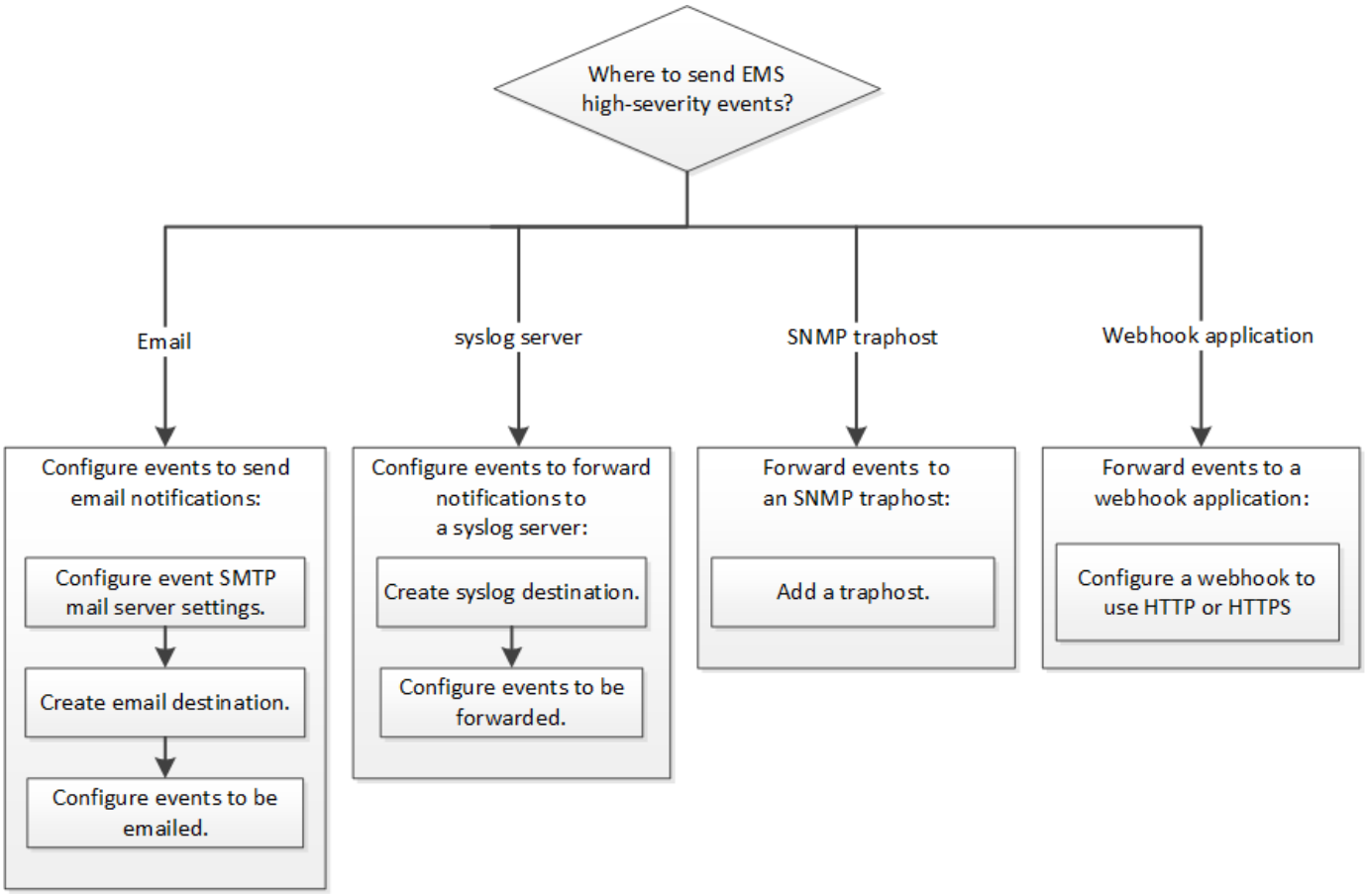
您必须将重要的EMS事件通知配置为以电子邮件形式发送、转发到系统日志服务器、转发到SNMP陷阱主机或转发到webhook应用程序。这有助于您及时采取更正操作，避免系统中断。

关于此任务

如果您的环境已包含用于聚合其他系统（例如服务器和应用程序）中记录的事件的系统日志服务器，则使用该系统日志服务器也可以更方便地从存储系统发出重要事件通知。

如果您的环境尚未包含系统日志服务器，则使用电子邮件发送重要事件通知会更方便。

如果您已将事件通知转发到 SNMP 陷阱主机，则可能需要监控该陷阱主机以查看重要事件。



选项

- 设置 EMS 以发送事件通知。

如果您希望 …	请参见 …
用于向电子邮件地址发送重要事件通知的 EMS	配置重要的 EMS 事件以发送电子邮件通知
用于将重要事件通知转发到系统日志服务器的 EMS	配置重要的 EMS 事件以将通知转发到系统日志服务器
希望 EMS 将事件通知转发到 SNMP 陷阱主机	配置 SNMP 陷阱主机以接收事件通知
希望EMS将事件通知转发到webhook应用程序	配置重要的EMS事件以将通知转发到webhook应用程序

配置重要的 **EMS** 事件以发送电子邮件通知

要接收最重要事件的电子邮件通知，您必须将 EMS 配置为针对表示重要活动的事件发送电子邮件消息。

您需要的内容

要解析电子邮件地址，必须在集群上配置 DNS 。

关于此任务

您可以在集群运行时随时通过在 ONTAP 命令行上输入命令来执行此任务。

步骤

1. 配置事件 SMTP 邮件服务器设置：

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. 为事件通知创建电子邮件目标：

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. 配置重要事件以发送电子邮件通知：

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

配置重要的 **EMS** 事件以将通知转发到系统日志服务器

要在系统日志服务器上记录最严重事件的通知，您必须配置 EMS 以转发用于表示重要活动的事件的通知。

您需要的内容

要解析系统日志服务器名称，必须在集群上配置 DNS 。

关于此任务

如果您的环境尚未包含用于发送事件通知的系统日志服务器，则必须先创建一个。如果您的环境已包含一个用于记录其他系统中的事件的系统日志服务器，则您可能需要使用该服务器来发送重要事件通知。

您可以在集群运行时随时在ONTAP 命令行界面上输入命令来执行此任务。

从ONTAP 9.12.1开始、可以通过传输层安全(Transport Layer Security、TLS)协议将EMS事件发送到远程系统日志服务器上的指定端口。有两个新参数可用：

`tcp-encrypted`

时间 `tcp-encrypted` 已为指定 `syslog-transport`、ONTAP 通过验证目标主机的证书来验证其身份。默认值为 `udp-unencrypted`。

`syslog-port`

默认值 `syslog-port` 参数取决于的设置 `syslog-transport` 参数。条件 `syslog-transport` 设置为 `tcp-encrypted`， `syslog-port` 具有默认值6514。

有关详细信息，请参见 `event notification destination create` 手册页。

步骤

1. 为重要事件创建系统日志服务器目标：

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

从ONTAP 9.12.1开始、可以为指定以下值 `syslog-transport`：

- `udp-unencrypted` —无安全性的用户数据报协议
- `tcp-unencrypted` —传输控制协议无安全性
- `tcp-encrypted` —传输层安全传输控制协议(TLS)

默认协议为 `udp-unencrypted`。

2. 配置重要事件以将通知转发到系统日志服务器：

```
event notification create -filter-name important-events -destinations syslog-ems
```

配置 **SNMP** 陷阱主机以接收事件通知

要在 SNMP 陷阱主机上接收事件通知，必须配置陷阱主机。

您需要的内容

- 必须在集群上启用 SNMP 和 SNMP 陷阱。

> 默认情况下， SNMP 和 SNMP 陷阱处于启用状态。

- 要解析陷阱主机名称，必须在集群上配置 DNS 。

关于此任务

如果尚未将 SNMP 陷阱主机配置为接收事件通知（ SNMP 陷阱），则必须添加一个。

您可以在集群运行时随时通过在 ONTAP 命令行上输入命令来执行此任务。

步骤

1. 如果您的环境尚未配置 SNMP 陷阱主机以接收事件通知，请添加一个：

```
system snmp traphost add -peer-address snmp_traphost_name
```

默认情况下， SNMP 支持的所有事件通知都会转发到 SNMP 陷阱主机。

配置重要的**EMS**事件以将通知转发到**webhook**应用程序

您可以将ONTAP 配置为将重要事件通知转发到webhook应用程序。所需的配置步骤取决于您选择的安全性级别。

准备配置**EMS**事件转发

在配置ONTAP 将事件通知转发到webhook应用程序之前、您应考虑几个概念和要求。

webhook应用程序

您需要一个能够接收ONTAP 事件通知的webhook应用程序。webhook是用户定义的回调例程、用于扩展运行它的远程应用程序或服务器的功能。客户端(在本例中为ONTAP)通过向目标URL发送HTTP请求来调用或激活webhooks。具体而言、ONTAP 会向托管webhook应用程序的服务器发送HTTP POST请求以及XML格式的事件通知详细信息。

安全选项

根据传输层安全(Transport Layer Security、TLS)协议的使用方式、有多个安全选项可用。您选择的选项将确定所需的ONTAP 配置。

> TLS是一种加密协议、在互联网上广泛使用。它使用一个或多个公有 密钥证书提供隐私以及数据完整性和身份验证。证书由可信证书颁发机构颁发。

HTTP

您可以使用HTTP传输事件通知。使用此配置时、连接不安全。不会验证ONTAP 客户端和webhook应用程序的身份。此外、网络流量不会加密或受到保护。请参见 "配置webhook目标以使用HTTP" 以获取配置详细信息。

HTTPS

为了提高安全性、您可以在托管webhook例程的服务器上安装证书。ONTAP 使用HTTPS协议来验证webhook应用程序服务器的身份、双方也使用此协议来确保网络流量的隐私和完整性。请参见 "将网络挂机目标配置为使用HTTPS" 以获取配置详细信息。

使用**HTTPS**进行相互身份验证

您可以通过在发出webbook请求的ONTAP 系统上安装客户端证书来进一步增强HTTPS安全性。除了ONTAP 验证webhook应用程序服务器的身份并保护网络流量之外、webhook应用程序还会验证ONTAP 客户端的身份。这种双向对等身份验证称为_mutual tls_.请参见 "配置一个webhook目标以使用HTTPS进行相互身份验证" 以获取配置详细信息。

相关信息

- "传输层安全(TLS)协议版本1.3"

配置**webhook**目标以使用**HTTP**

您可以将ONTAP 配置为使用HTTP将事件通知转发到webhook应用程序。这是最不安全的选项、但设置最简单。

步骤

1. 创建新目标 `restapi-ems` 要接收事件、请执行以下操作：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   在上述命令中、必须对目标使用* HTTP *方案。

2. 创建一个通知以链接 `important-events` 使用进行筛选 `restapi-ems` 目标：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

将网络挂机目标配置为使用HTTPS

您可以将ONTAP配置为使用HTTPS将事件通知转发到webhook应用程序。ONTAP 使用服务器证书来确认webhook应用程序的身份并保护网络流量。

开始之前

- 为webhook应用程序服务器生成专用密钥和证书
- 准备好可在ONTAP 中安装的根证书

步骤

1. 在托管webhook应用程序的服务器上安装相应的服务器专用密钥和证书。具体的配置步骤取决于服务器。
2. 在ONTAP 中安装服务器根证书：

   ```
   security certificate install -type server-ca
   ```

   命令将要求提供证书。

3. 创建 `restapi-ems` 接收事件的目标：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   在上述命令中，必须对目标使用*HTTPS*方案。

4. 创建用于链接的通知 `important-events` 使用新进行筛选 `restapi-ems` 目标：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

配置一个webhook目标以使用HTTPS进行相互身份验证

您可以将ONTAP 配置为使用HTTPS并通过相互身份验证将事件通知转发到webhook应用程序。在此配置中、有两个证书。ONTAP 使用服务器证书确认webhook应用程序的身份并保护网络流量。此外、托管webhook的应用程序使用客户端证书来确认ONTAP 客户端的身份。

开始之前

在配置ONTAP 之前、必须执行以下操作：

- 为webhook应用程序服务器生成专用密钥和证书
- 准备好可在ONTAP 中安装的根证书
- 为ONTAP 客户端生成专用密钥和证书

步骤

1. 执行任务中的前两个步骤 "将网络挂机目标配置为使用HTTPS" 安装服务器证书、以便ONTAP 可以验证服务器的身份。
2. 在webhook应用程序中安装相应的根证书和中间证书以验证客户端证书。
3. 在ONTAP 中安装客户端证书：

```
security certificate install -type client
```

命令将要求提供私钥和证书。

4. 创建 `restapi-ems` 接收事件的目标：

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

在上述命令中、必须对目标使用* HTTPS *方案。

5. 创建用于链接的通知 `important-events` 使用新进行筛选 `restapi-ems` 目标：

```
event notification create -filter-name important-events -destinations restapi-
ems
```

更新已弃用的 EMS 事件映射

EMS 事件映射模型

在 ONTAP 9.0 之前的版本中，只能根据事件名称模式匹配将 EMS 事件映射到事件目标。ONTAP命令集 (`event destination`， `event route`)使用此模型的版本在最新版本的ONTAP中仍然可用、但从ONTAP 9.0开始已弃用。

从ONTAP 9.0开始、ONTAP EMS事件目标映射的最佳实践是使用可扩展性更强的事件筛选器模型、在该模型中、可以使用对多个字段执行模式匹配 `event filter`， `event notification`，和 `event notification destination` 命令集。

如果使用弃用的命令配置EMS映射、则应更新映射以使用 `event filter`， `event notification`，和 `event notification destination` 命令集。

事件目标有两种类型：

1. * 系统生成的目标 * ：系统生成的事件目标有五个（默认为创建）
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     系统生成的某些目标用于特殊目的。例如， asup 目标会将 CallHome.* 事件路由到 ONTAP 中的 AutoSupport 模块，以生成 AutoSupport 消息。

2. 用户创建的目标：这些目标是使用手动创建的 `event destination create` 命令：

```
cluster-1::event*> destination show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

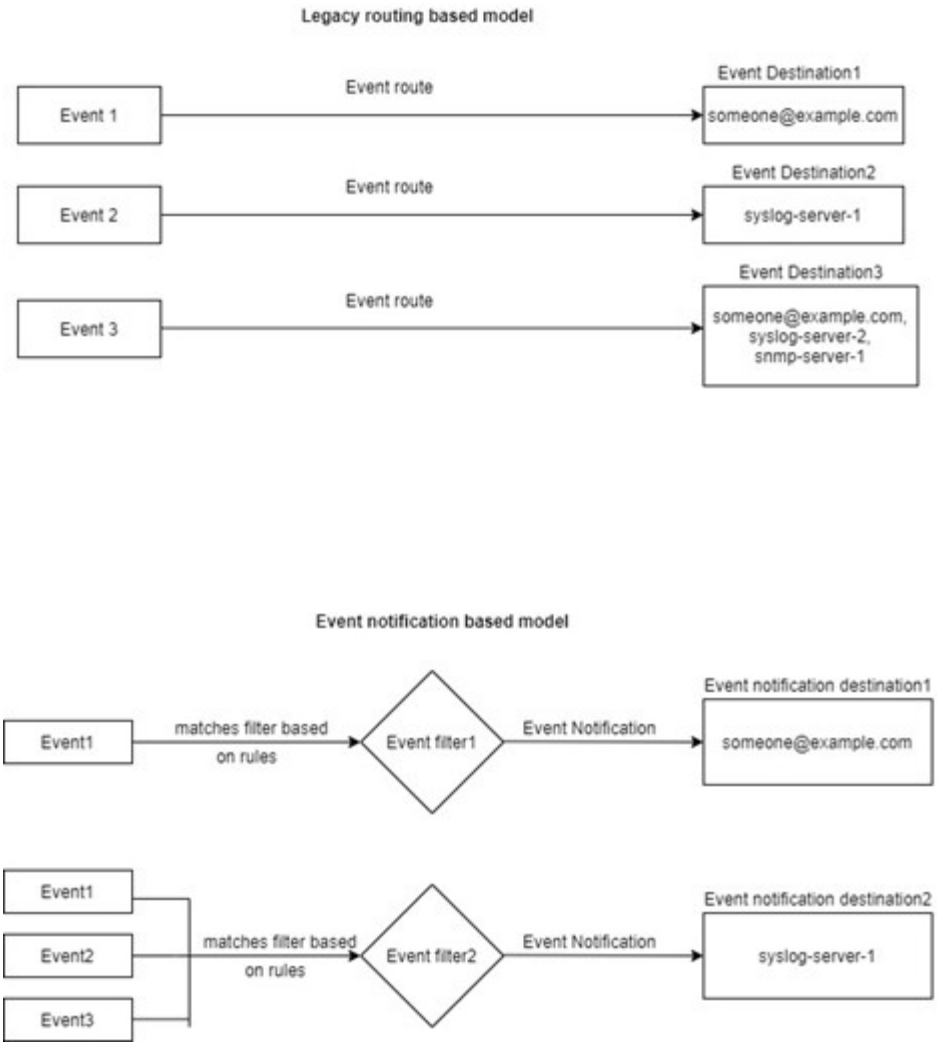
在已弃用的模型中、EMS事件会使用单独映射到目标 `event route add-destinations` 命令：

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
--------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

更具可扩展性的新 EMS 事件通知机制基于事件筛选器和事件通知目标。有关新事件通知机制的详细信息，请参见以下知识库文章：

- "ONTAP 9 事件管理系统概述"



使用已弃用的 **ONTAP** 命令更新 **EMS** 事件映射

当前使用已弃用的ONTAP命令集配置EMS事件映射时 (`event destination`， `event route`)、则应按照此操作步骤更新映射以使用 `event filter`， `event notification`，和 `event notification destination` 命令集。

步骤

1. 使用列出系统中的所有事件目标 `event destination show` 命令：

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. 对于每个目标、使用列出要映射到它的事件 `event route show -destinations <destination name>` 命令：

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. 创建相应的 `event filter` 其中包括所有这些事件子集。
例如、如果要仅包含 `raid.aggr.*`事件、请使用通配符作为 `message-name` 参数。您还可以为单个事件创建筛选器。

> 您最多可以创建 50 个事件筛选器。

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 创建 `event notification destination` 对于每个 `event destination` 端点(即SMP/SNMP/系统日志)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. 通过将事件筛选器映射到事件通知目标来创建事件通知。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                      Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. 对每个重复步骤1-5 `event destination` 具有 `event route` 映射。

路由到SNMP目标的事件应映射到 `snmp-traphost` 事件通知目标。SNMP 陷阱主机目标使用系统配置的 SNMP 陷阱主机。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```