



常见 **Unified Manager** 运行状况工作流程和任务

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

目录

常见 Unified Manager 运行状况工作流程和任务	1
监控数据可用性并对其进行故障排除	2
解决容量问题	8
管理运行状况阈值	9
管理集群安全目标	14
管理备份和还原操作	23
管理脚本	38
管理和监控组	41
使用标注确定存储对象事件的优先级	50
管理 SAML 身份验证设置	58
通过 Web UI 和维护控制台发送支持包	64
与多个工作流相关的任务和信息	71

常见 Unified Manager 运行状况工作流程和任务

与 Unified Manager 关联的一些常见管理工作流程和任务包括：选择要监控的存储集群；诊断对数据可用性，容量和保护产生不利影响的情况；还原丢失的数据；配置和管理卷；根据需要捆绑诊断数据并将其发送给技术支持。

通过 Unified Manager，存储管理员可以查看信息板，评估受管存储集群的整体容量，可用性和保护运行状况，然后快速确定，找到，诊断和分配可能出现的任何特定问题以解决问题。

与集群，Storage Virtual Machine（SVM），卷或 FlexGroup 卷相关的影响受管存储对象存储容量或数据可用性的最重要问题会显示在信息板页面上的系统运行状况图和事件中。确定严重问题后，此页面将提供相应的故障排除工作流程支持链接。

Unified Manager 还可以包含在包含相关易管理性工具（例如 OnCommand Workflow Automation（WFA））的工作流中，以支持直接配置存储资源。

本文档介绍了与以下管理任务相关的常见工作流：

- 诊断和管理可用性问题

如果硬件故障或存储资源配置问题发生原因在信息板页面中显示数据可用性事件，存储管理员可以通过嵌入的链接查看有关受影响存储资源的连接信息，查看故障排除建议以及将问题描述解决方案分配给其他管理员。

- 配置和监控性能意外事件

管理员可以监控和管理所监控存储系统资源的性能。请参见 ["Active IQ Unified Manager 性能监控简介"](#) 有关详细信息 ...

- 诊断和管理卷容量问题

如果 "信息板" 页面中显示卷存储容量问题，则存储管理员可以通过嵌入的链接查看与受影响卷的存储容量相关的当前和历史趋势，查看故障排除建议并将问题描述解决方案分配给其他管理员。

- 配置，监控和诊断保护关系问题

创建和配置保护关系后，存储管理员可以查看与保护关系相关的潜在问题，保护关系的当前状态，有关受影响关系的当前和历史保护作业成功信息以及故障排除建议。请参见 ["创建，监控保护关系并对其进行故障排除"](#) 有关详细信息 ...

- 创建备份文件并从备份文件还原数据。

- 将存储对象与标注关联

通过将存储对象与标注关联，存储管理员可以筛选和查看与存储对象相关的事件，从而使存储管理员能够确定与事件相关的问题的优先级并解决这些问题。

- 使用 REST API 通过查看 Unified Manager 捕获的运行状况，容量和性能信息来帮助管理集群。请参见 ["Active IQ Unified Manager 入门"](#) 有关详细信息 ...

- 向技术支持发送支持包

存储管理员可以使用维护控制台检索支持包并将其发送给技术支持。如果问题描述需要比 AutoSupport 消息

更详细的诊断和故障排除信息，则必须将支持包发送给技术支持。

监控数据可用性并对其进行故障排除

Unified Manager 可监控授权用户访问存储数据的可靠性，在出现阻止或阻碍访问的情况时向您发出警报，并可用于诊断这些情况并分配和跟踪其解决方法。

本节中的可用性 workflow 主题介绍了一些示例，说明存储管理员如何使用 Unified Manager Web UI 发现，诊断和分配对数据可用性产生不利影响的硬件和软件状况以解决问题。

扫描并解决存储故障转移互连链路断开情况

此 workflow 举例说明如何扫描，评估和解决已关闭的存储故障转移互连链路情况。在这种情况下，您是一名管理员，使用 Unified Manager 在节点上开始 ONTAP 版本升级之前扫描存储故障转移风险。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

如果在无中断升级尝试期间 HA 对节点之间的存储故障转移互连失败，则升级将失败。因此，管理员通常会在开始升级之前监控和确认要升级的集群节点上的存储故障转移可靠性。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。
2. 在 * 事件管理 * 清单页面中，选择 * 活动可用性事件 *。
3. 在 * 事件管理 * 清单页面 * 名称 * 列顶部、单击  然后输入 * failover 在文本框中、将要显示的事件限制为与存储故障转移相关的事件。

此时将显示与存储故障转移条件相关的所有过去事件。

在这种情况下，Unified Manager 会在其可用性意外事件部分显示事件 " 存储故障转移互连的一个或多个链路断开 "。

4. 如果与存储故障转移相关的一个或多个事件显示在 * 事件管理 * 清单页面上，请执行以下步骤：
 - a. 单击事件标题链接可显示该事件的事件详细信息。

在此示例中，您单击事件标题 Storage Failover Interconnect one or more links down。

此时将显示该事件的 " 事件 " 详细信息页面。

- a. 在 * 事件 * 详细信息页面上、您可以执行以下一项或多项任务：
 - 查看发生原因字段中的错误消息并评估问题描述。 [对存储故障转移互连链路断开执行更正操作](#)

- 将事件分配给管理员。 [分配事件](#)
- 确认事件。 [确认并解决事件](#)

对存储故障转移互连链路断开执行更正操作

显示存储故障转移相关事件的事件详细信息页面时，您可以查看页面的摘要信息，以确定事件的紧急性，问题描述的可能发生原因以及问题描述的可能解决方案。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

在此示例场景中，“事件”详细信息页面上提供的事件摘要包含有关存储故障转移互连链路断开情况的以下信息：

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

示例事件信息表示 HA 对节点 aardvark 和 bonobo 之间的存储故障转移互连链路 Link1 已关闭，但 Apple 和 Boy 之间的 Link0 处于活动状态。由于一个链路处于活动状态，因此远程动态内存访问（RDMA）仍在运行，存储故障转移作业仍可成功完成。

但是，为了确保两个链路均发生故障且存储故障转移保护完全禁用，您决定进一步诊断 Link1 发生故障的原因。

步骤

1. 在 * 事件 * 详细信息页面中，您可以单击源字段中指定的事件的链接，以获取可能与存储故障转移互连链路断开情况相关的其他事件的详细信息。

在此示例中，事件源是名为 aardvark 的节点。单击该节点名称将在集群 / 运行状况详细信息页面的节点选项卡上显示受影响 HA 对 aardvark 和 bonobo 的 HA 详细信息，并显示最近在受影响 HA 对上发生的其他事件。

2. 有关此事件的详细信息，请查看 * HA 详细信息 *。

在此示例中，相关信息位于 Events 表中。该表显示了 " s 存储故障转移连接一个或多个链路断开 " 事件，事件的生成时间，以及此事件的源节点。

完成后

使用 HA 详细信息中的节点位置信息，请求或亲自完成受影响 HA 对节点上的存储故障转移问题描述的物理检查和修复。

解决卷脱机问题

此 workflow 举例说明了如何评估和解决 Unified Manager 可能在事件管理清单页面中显示的卷脱机事件。在这种情况下，您是使用 Unified Manager 对一个或多个卷脱机事件进行故障排除的管理员。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

报告卷脱机的原因可能有多种：

- SVM 管理员故意使卷脱机。
- 卷的托管集群节点已关闭，存储故障转移到其 HA 对配对节点也失败。
- 卷的托管 Storage Virtual Machine (SVM) 已停止，因为托管该 SVM 根卷的节点已关闭。
- 由于两个 RAID 磁盘同时发生故障，卷的托管聚合已关闭。

您可以使用事件管理清单页面以及集群 / 运行状况， Storage VM/ 运行状况和卷 / 运行状况详细信息页面来确认或消除其中一种或多种可能性。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。
2. 在 * 事件管理 * 清单页面中，选择 * 活动可用性事件 *。
3. 单击为卷脱机事件显示的超文本链接。

此时将显示可用性意外事件的事件详细信息页面。

4. 在该页面上，查看注释以了解是否有迹象表明 SVM 管理员已使相关卷脱机。
5. 在 * 事件 * 详细信息页面上，您可以查看以下一项或多项任务的信息：

- 查看发生原因字段中显示的信息，以获取可能的诊断指导。

在此示例中，发生原因字段中的信息仅通知您卷已脱机。

- 检查 "Notes and Updates" 区域，查看是否有迹象表明 SVM 管理员故意使相关卷脱机。

- 单击事件源（此处为报告脱机的卷）以获取有关该卷的详细信息。 [针对卷脱机情况执行更正操作](#)
- 将事件分配给管理员。 [分配事件](#)
- 确认此事件，或在适当情况下将其标记为已解决。 [确认并解决事件](#)

针对卷脱机情况执行诊断操作

导航到报告为脱机的卷的 "Volume/Health" 详细信息页面后，您可以搜索追加信息以帮助诊断卷脱机情况。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

如果报告脱机的卷未被有意脱机，则该卷可能会因为多种原因脱机。

从脱机卷的卷 / 运行状况详细信息页面开始，您可以导航到其他页面和窗格以确认或消除可能的原因：

选项

- 单击 * 卷 / 运行状况 * 详细信息页面链接，确定卷是否因其主机节点已关闭以及存储故障转移到其 HA 对配对节点也失败而脱机。

请参见 [确定卷脱机情况是否是由已关闭的节点引起的](#)。

- 单击 * 卷 / 运行状况 * 详细信息页面链接，确定卷是否已脱机，其主机 Storage Virtual Machine （SVM）是否因托管此 SVM 根卷的节点已关闭而停止。

请参见 [确定卷是否因节点关闭而脱机以及 SVM 是否已停止](#)。

- 单击 * 卷 / 运行状况 * 详细信息页面链接，确定卷是否因主机聚合中的磁盘损坏而脱机。

请参见 [确定卷是否因聚合中的磁盘损坏而脱机](#)。

确定卷是否因其主机节点已关闭而脱机

您可以使用 Unified Manager Web UI 确认或消除卷因主机节点关闭而脱机以及存储故障转移到其 HA 对配对节点失败的可能性。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

要确定卷脱机情况是否是由于托管节点故障以及后续存储故障转移失败而导致的，请执行以下操作：

步骤

1. 在脱机卷的 * 卷 / 运行状况 * 详细信息页面的 * 相关设备 * 窗格中，找到并单击 SVM 下显示的超文本链接。
Storage VM/ 运行状况详细信息页面显示有关脱机卷的托管 Storage Virtual Machine (SVM) 的信息。
2. 在 * Storage VM / Health* 详细信息页面的 * 相关设备 * 窗格中，找到并单击卷下显示的超文本链接。
"运行状况：所有卷" 视图显示一个表，其中包含有关 SVM 托管的所有卷的信息。
3. 在 * 运行状况：所有卷 * 查看状态列标题上，单击筛选器符号 ，然后选择 * 脱机 * 选项。
仅会列出处于脱机状态的 SVM 卷。
4. 在*运行状况：所有卷*视图中、单击网格符号 ，然后选择 * 集群节点 * 选项。
您可能需要滚动网格选择框以找到 * 集群节点 * 选项。
集群节点列将添加到卷清单中，并显示托管每个脱机卷的节点的名称。
5. 在 * 运行状况：所有卷 * 视图中，找到脱机卷的列表，然后在其集群节点列中单击其托管节点的名称。
集群 / 运行状况详细信息页面上的节点选项卡显示托管节点所属的 HA 节点对的状态。托管节点的状态以及任何集群故障转移操作是否成功将显示在屏幕中。

完成后

确认由于主机节点已关闭且存储故障转移到 HA 对配对节点失败而导致卷脱机情况存在后，请联系相应的管理员或操作员以手动重新启动已关闭的节点并修复存储故障转移问题。

确定卷是否因节点关闭而脱机及其 SVM 是否已停止

您可以使用 Unified Manager Web UI 确认或消除卷脱机的可能性，因为托管该 SVM 根卷的节点已关闭，导致其主机 Storage Virtual Machine (SVM) 停止。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

要确定卷脱机情况是否是由于托管此 SVM 根卷的节点已关闭而导致其主机 SVM 停止的，请执行以下操作：

步骤

1. 在脱机卷的 * 卷 / 运行状况 * 详细信息页面的 * 相关设备 * 窗格中，找到并单击 SVM 下显示的超文本链接。
Storage VM/ 运行状况详细信息页面会显示托管 SVM 的 "Running" 或 "s已加注" 状态。如果 SVM 状态为 running，则卷脱机情况不是由托管此 SVM 根卷的节点关闭所致。
2. 如果 SVM 状态为 stopped，则单击 * 查看 SVM* 以进一步确定要停止的托管 SVM 的发生原因。

3. 在*运行状况：所有Storage VM* viewSVM列标题上、单击筛选器符号  然后键入已停止的 SVM 的名称。
该 SVM 的信息显示在一个表中。
4. 在 * 运行状况：所有 Storage VM* 视图中，单击  然后选择 * 根卷 * 选项。
根卷列将添加到 SVM 清单中，并显示已停止 SVM 的根卷的名称。
5. 在根卷列中，单击根卷的名称以显示该卷的 * 存储 VM / 运行状况 * 详细信息页面。
如果 SVM 根卷的状态为（联机），则不会因为托管该 SVM 根卷的节点已关闭而导致原始卷脱机。
6. 如果SVM根卷的状态为(脱机)、则在SVM根卷的*卷/运行状况*详细信息页面的*相关设备*窗格中、找到并单击聚合下显示的超文本链接。
7. 在聚合的 * 聚合 / 运行状况 * 详细信息页面的 * 相关设备 * 窗格中，找到并单击节点下显示的超文本链接。
集群 / 运行状况详细信息页面上的节点选项卡显示 SVM 根卷的托管节点所属的 HA 节点对的状态。节点的状态将显示在屏幕中。

完成后

确认卷脱机情况是由该卷的主机 SVM 脱机状况引起的，而该状况本身是由托管该 SVM 根卷的节点关闭引起的，然后，请与相应的管理员或操作员联系以手动重新启动已关闭的节点。

确定卷是否因聚合中的磁盘损坏而脱机

您可以使用 Unified Manager Web UI 确认或消除卷脱机的可能性，因为 RAID 磁盘问题已使其主机聚合脱机。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

要确定卷脱机情况是否是由使托管聚合脱机的 RAID 磁盘问题引起的，请执行以下操作：

步骤

1. 在 * 卷 / 运行状况 * 详细信息页面的 * 相关设备 * 窗格中，找到并单击聚合下显示的超文本链接。
聚合 / 运行状况详细信息页面显示托管聚合的联机或脱机状态。如果聚合状态为联机，则 RAID 磁盘问题不是要脱机的卷的发生原因。
2. 如果聚合状态为脱机，则单击 * 磁盘信息 *，并在 * 磁盘信息 * 选项卡上的 * 事件 * 列表中查找损坏的磁盘事件。
3. 要进一步确定损坏的磁盘，请单击 * 相关设备 * 窗格中节点下显示的超文本链接。

此时将显示集群 / 运行状况详细信息页面。

4. 单击 * 磁盘 * ，然后在 * 筛选器 * 窗格中选择 * 已断开 * 以列出处于断开状态的所有磁盘。

如果处于断开状态的磁盘导致主机聚合处于脱机状态，则聚合的名称将显示在受影响的聚合列中。

完成后

确认卷脱机情况是由损坏的 RAID 磁盘以及由此导致的主机聚合脱机引起的，请联系相应的管理员或操作员，手动更换损坏的磁盘并将聚合重新联机。

解决容量问题

此工作流程举例说明了如何解决容量问题描述。在这种情况下，您是管理员或操作员，可以访问 Unified Manager 信息板页面以查看任何受监控存储对象是否存在容量问题。您希望确定可能发生的原因并解决此问题。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

在信息板页面上，您会在容量面板的事件下拉列表下查找 "Volume Space Full" 错误事件。

步骤

1. 在 * 信息板 * 页面的 * 容量 * 面板中，单击卷空间已满错误事件的名称。

此时将显示此错误的事件详细信息页面。

2. 在 * 事件 * 详细信息页面中，您可以执行以下一项或多项任务：

- 查看发生原因字段中的错误消息，然后单击建议的补救措施下的建议以查看可能的补救措施的说明。 [对已满的卷执行建议的补救措施](#)
- 在源字段中单击对象名称（此处为卷）以获取有关此对象的详细信息。 [卷详细信息页面](#)
- 查找可能已添加的有关此事件的注释。 [添加和查看与事件关联的注释](#)
- 向事件添加注释。 [添加和查看与事件关联的注释](#)
- 将事件分配给其他用户。 [分配事件](#)
- 确认事件。 [确认并解决事件](#)
- 将事件标记为已解决。 [确认并解决事件](#)

对已满的卷执行建议的补救措施

收到 "Volume Space Full" 错误事件后，您可以在 "Event Details" 页面上查看建议的补救措施，并决定执行建议的操作之一。

开始之前

您必须具有应用程序管理员或存储管理员角色。

具有任何角色的用户均可执行此工作流程中使用 Unified Manager 的所有任务。

关于此任务

在此示例中，您在 Unified Manager Event Management 清单页面上看到卷空间已满错误事件，并单击事件名称。

对于已满的卷，您可能会执行以下补救措施：

- 在卷上启用自动增长，重复数据删除或数据压缩
- 调整卷大小或移动卷
- 从卷中删除或移动数据

虽然所有这些操作都必须从 ONTAP 系统管理器或 ONTAP 命令行界面执行，但您可以使用 Unified Manager 查找确定要执行的操作可能需要的信息。

步骤

1. 在 * 事件 * 详细信息页面中，单击源字段中的卷名称可查看有关受影响卷的详细信息。
2. 在 * 卷 / 运行状况 * 详细信息页面上，单击 * 配置 *，发现卷上已启用重复数据删除和数据压缩。

您决定调整卷大小。

3. 在 * 相关设备 * 窗格中，单击托管聚合的名称以查看该聚合是否可容纳更大的卷。
4. 在 * 聚合 / 运行状况 * 详细信息页面上，您会看到托管完整卷的聚合确实具有足够的未提交容量，因此您可以使用 ONTAP 系统管理器调整卷大小，从而为其提供更多容量。

管理运行状况阈值

您可以为所有聚合，卷和 qtree 配置全局运行状况阈值，以跟踪任何违反运行状况阈值的情况。

什么是存储容量运行状况阈值

存储容量运行状况阈值是指 Unified Manager 服务器生成事件以报告存储对象的任何容量问题的时间点。您可以将警报配置为在发生此类事件时发送通知。

所有聚合，卷和 qtree 的存储容量运行状况阈值均设置为默认值。您可以根据需要更改一个对象或一组对象的设置。

配置全局运行状况阈值设置

您可以为容量，增长，Snapshot 预留，配额和索引节点配置全局运行状况阈值条件，以有效监控聚合，卷和 qtree 大小。您还可以编辑用于生成超过滞后阈值的事件的设置。

关于此任务

全局运行状况阈值设置适用于与其关联的所有对象，例如聚合，卷等。超过阈值后，系统将生成事件，如果配置了警报，则会发送警报通知。阈值默认值设置为建议值，但您可以对其进行修改，以便按一定间隔生成事件，以满足您的特定需求。更改阈值后，将在下一个监控周期生成或废弃事件。

全局运行状况阈值设置可从左侧导航菜单的事件阈值部分访问。您还可以从各个对象的清单页面或详细信息页面修改这些对象的阈值设置。

选项

- [配置全局聚合运行状况阈值](#)

您可以为所有聚合的容量，增长和 Snapshot 副本配置运行状况阈值设置，以跟踪任何违反阈值的情况。

- [配置全局卷运行状况阈值](#)

您可以编辑容量，Snapshot 副本，qtree 配额，卷增长，覆盖预留空间的运行状况阈值设置。和索引节点以跟踪任何违反阈值的情况。

- [配置全局 qtree 运行状况阈值](#)

您可以编辑所有 qtree 的容量的运行状况阈值设置，以跟踪任何违反阈值的情况。

- [编辑非受管保护关系的滞后运行状况阈值设置](#)

您可以增加或减少警告或错误滞后时间百分比，以便按更适合您需求的间隔生成事件。

配置全局聚合运行状况阈值

您可以为所有聚合配置全局运行状况阈值，以跟踪任何违反阈值的情况。系统会针对违反阈值的情况生成相应的事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控聚合的阈值最佳实践设置来配置全局值。

开始之前

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

全局配置选项时，对象的默认值将被修改。但是，如果在对象级别更改了默认值，则不会修改全局值。

阈值选项具有默认值，以便更好地进行监控，但是，您可以根据环境要求更改这些值。

如果对位于聚合上的卷启用自动增长，则根据自动增长设置的最大卷大小，而不是原始卷大小，聚合容量阈值将视为已违反。



运行状况阈值不适用于节点的根聚合。

步骤

1. 在左侧导航窗格中，单击 * 事件阈值 * > * 聚合 *。
2. 为容量，增长和 Snapshot 副本配置适当的阈值。
3. 单击 * 保存 *。

配置全局卷运行状况阈值

您可以为所有卷配置全局运行状况阈值，以跟踪任何违反阈值的情况。系统会针对违反运行状况阈值的情况生成相应的事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控卷的阈值最佳实践设置来配置全局值。

开始之前

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

大多数阈值选项都具有默认值，以便更好地进行监控。但是，您可以根据环境要求更改这些值。

请注意，在卷上启用自动增长时，根据自动增长设置的最大卷大小（而不是原始卷大小），容量阈值被视为已违反。



默认值 1000 个 Snapshot 副本仅适用于 ONTAP 版本为 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本为 9.8 及更高版本的 FlexGroup 卷。对于使用旧版 ONTAP 软件安装的集群，最大数量为每个卷 250 个 Snapshot 副本。对于这些较旧版本，Unified Manager 会将此数字 1000（以及介于 1000 和 250 之间的任意数字）解释为 250；这意味着当 Snapshot 副本数量达到 250 时，您将继续接收事件。如果要为这些较旧版本将此阈值设置为小于 250，则必须在此处，运行状况：所有卷视图或卷 / 运行状况详细信息页面中将此阈值设置为 250 或更低。

步骤

1. 在左侧导航窗格中，单击 * 事件阈值 * > * 卷 *。
2. 为容量，Snapshot 副本，qtree 配额，卷增长和索引节点配置适当的阈值。
3. 单击 * 保存 *。

配置全局 qtree 运行状况阈值

您可以为所有 qtree 配置全局运行状况阈值，以跟踪任何违反阈值的情况。系统会针对违反运行状况阈值的情况生成相应的事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控 qtree 的阈值最佳实践设置来配置全局值。

开始之前

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

阈值选项具有默认值，以便更好地进行监控，但是，您可以根据环境要求更改这些值。

只有在 qtree 上设置了 qtree 配额或默认配额后，才会为该 qtree 生成事件。如果用户配额或组配额中定义的空间超过阈值，则不会生成事件。

步骤

1. 在左侧导航窗格中，单击 * 事件阈值 * > * qtree* 。
2. 配置适当的容量阈值。
3. 单击 * 保存 * 。

为非受管保护关系配置滞后阈值设置

您可以编辑非受管保护关系的全局默认滞后警告和错误运行状况阈值设置，以便根据您的需要按一定间隔生成事件。

开始之前

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

滞后时间不能超过定义的传输计划间隔。例如，如果传输计划为每小时，则滞后时间不得超过一小时。滞后阈值指定滞后时间不得超过的百分比。以一小时为例，如果滞后阈值定义为 150%，则当滞后时间超过 1.5 小时时，您将收到一个事件。

此任务中所述的设置将全局应用于所有非受管保护关系。无法指定这些设置并将其仅应用于一个非受管保护关系。

步骤

1. 在左侧导航窗格中，单击 * 事件阈值 * > * 关系 * 。
2. 根据需要增加或减少全局默认警告或错误滞后时间百分比。
3. 要禁止从任何滞后阈值量触发警告或错误事件，请取消选中 * 已启用 * 旁边的框。
4. 单击 * 保存 * 。

编辑单个聚合运行状况阈值设置

您可以编辑一个或多个聚合的聚合容量，增长和 Snapshot 副本的运行状况阈值设置。超过阈值时，系统会生成警报并向您发送通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

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

根据对阈值的更改，将在下一个监控周期生成或废弃事件。

如果对位于聚合上的卷启用自动增长，则根据自动增长设置的最大卷大小，而不是原始卷大小，聚合容量阈值将视为已违反。

步骤

1. 在左侧导航窗格中，单击 * 存储 * > * 聚合 *。
2. 在 * 运行状况：所有聚合 * 视图中，选择一个或多个聚合，然后单击 * 编辑阈值 *。
3. 在 * 编辑聚合阈值 * 对话框中，通过选中相应的复选框并修改设置来编辑以下其中一项的阈值设置：容量，增长或 Snapshot 副本。
4. 单击 * 保存 *。

编辑单个卷运行状况阈值设置

您可以编辑一个或多个卷的卷容量，增长，配额和空间预留的运行状况阈值设置。超过阈值时，系统会生成警报并向您发送通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

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

根据对阈值的更改，将在下一个监控周期生成或废弃事件。

请注意，在卷上启用自动增长时，根据自动增长设置的最大卷大小（而不是原始卷大小），容量阈值被视为已违反。



默认值 1000 个 Snapshot 副本仅适用于 ONTAP 版本为 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本为 9.8 及更高版本的 FlexGroup 卷。对于使用旧版 ONTAP 软件安装的集群，最大数量为每个卷 250 个 Snapshot 副本。对于这些较旧版本，Unified Manager 会将此数字 1000（以及介于 1000 和 250 之间的任意数字）解释为 250；这意味着当 Snapshot 副本数量达到 250 时，您将继续接收事件。如果要为这些较旧版本将此阈值设置为小于 250，则必须在此处，运行状况：所有卷视图或卷 / 运行状况详细信息页面中将此阈值设置为 250 或更低。

步骤

1. 在左侧导航窗格中，单击 * 存储 * > * 卷 *。
2. 在 * 运行状况：所有卷 * 视图中，选择一个或多个卷，然后单击 * 编辑阈值 *。
3. 在 * 编辑卷阈值 * 对话框中，通过选中相应的复选框并修改设置来编辑以下其中一项的阈值设置：容量，Snapshot 副本，qtree 配额，增长或索引节点。
4. 单击 * 保存 *。

编辑单个 qtree 运行状况阈值设置

您可以编辑一个或多个 qtree 的 qtree 容量的运行状况阈值设置。超过阈值时，系统会生成警报并向您发送通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

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

根据对阈值的更改，将在下一个监控周期生成或废弃事件。

步骤

1. 在左侧导航窗格中，单击 * 存储 * > * qtree* 。
2. 在 * 容量：所有 qtree* 视图中，选择一个或多个 qtree ，然后单击 * 编辑阈值 * 。
3. 在 * 编辑 qtree 阈值 * 对话框中，更改选定 qtree 或 qtree 的容量阈值，然后单击 * 保存 * 。



您还可以从 Storage VM/ 运行状况详细信息页面上的 qtree 选项卡设置各个 qtree 阈值。

管理集群安全目标

Unified Manager 提供了一个信息板，用于根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议确定 ONTAP 集群， Storage Virtual Machine （ SVM ）和卷的安全程度。

此安全信息板的目标是，显示 ONTAP 集群与 NetApp 建议的准则不一致的任何区域，以便您可以修复这些潜在问题。大多数情况下，您将使用 ONTAP 系统管理器或 ONTAP 命令行界面修复这些问题。您的组织可能不会遵循所有建议，因此在某些情况下，您不需要进行任何更改。

请参见 "《适用于 ONTAP 9 的 NetApp 安全加固指南》" （ TR-4569 ），了解详细的建议和解决方案。

除了报告安全状态之外， Unified Manager 还会为存在安全违规的任何集群或 SVM 生成安全事件。您可以在事件管理清单页面中跟踪这些问题，并为这些事件配置警报，以便在发生新的安全事件时通知存储管理员。

评估的安全标准是什么

通常，我们会根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议评估 ONTAP 集群， Storage Virtual Machine （ SVM ）和卷的安全标准。

部分安全检查包括：

- 集群是否正在使用安全身份验证方法，例如 SAML
- 对等集群的通信是否已加密
- Storage VM 是否已启用审核日志
- 卷已启用软件加密还是硬件加密

请参见有关合规性类别的主题和 "《适用于 ONTAP 9 的 NetApp 安全加固指南》" 了解详细信息。



从 Active IQ 平台报告的升级事件也视为安全事件。这些事件确定了需要升级 ONTAP 软件，节点固件或操作系统软件才能解决的问题（针对安全建议）。这些事件不会显示在“安全性”面板中，但可从“事件管理”清单页面访问。

集群合规性类别

下表介绍了 Unified Manager 评估的集群安全合规性参数，NetApp 建议以及该参数是否影响对集群是否合规性的整体判断。

集群上存在不合规的 SVM 将影响集群的合规性值。因此，在某些情况下，您可能需要先修复 SVM 的安全问题，然后才能将集群安全性视为合规。

请注意，并非所有安装都显示以下列出的所有参数。例如，如果您没有对等集群，或者您在集群上禁用了 AutoSupport，则您将不会在 UI 页面中看到集群对等或 AutoSupport HTTPS 传输项。

参数	Description	建议	影响集群合规性
全局 FIPS	指示是否已启用全局 FIPS（联邦信息处理标准）140-2 合规模式。启用 FIPS 后，TLSv1 和 SSLv3 将被禁用，并且仅允许使用 TLSv1.1 和 TLSv1.2。	enabled	是的。
Telnet	指示是启用还是禁用了对系统的 Telnet 访问。NetApp 建议使用安全 Shell（SSH）进行安全远程访问。	已禁用	是的。
SSH 设置不安全	指示 SSH 是否使用不安全的密码、例如以开头的密码 *cbc。	否	是的。
登录横幅	指示是否为访问系统的用户启用了登录横幅。	enabled	是的。
集群对等	指示对等集群之间的通信是加密的还是未加密的。必须在源集群和目标集群上配置加密，才能将此参数视为合规。	Encrypted	是的。

参数	Description	建议	影响集群合规性
网络时间协议	指示集群是否已配置一个或多个 NTP 服务器。为了获得冗余和最佳服务，NetApp 建议至少将三个 NTP 服务器与集群相关联。	Configured	是的。
OCSP	指示 ONTAP 中是否存在未配置 OCSP（联机证书状态协议）的应用程序，因此通信不会加密。此时将列出不合规的应用程序。	enabled	否
远程审核日志记录	指示日志转发（ Syslog ）是加密还是未加密。	Encrypted	是的。
AutoSupport HTTPS 传输	指示是否使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。	enabled	是的。
默认管理员用户	指示是启用还是禁用默认管理员用户（内置）。NetApp 建议锁定（禁用）任何不需要的内置帐户。	已禁用	是的。
SAML 用户	指示是否已配置 SAML。通过 SAML，您可以将多因素身份验证（ Multi-Factor Authentication，MFA）配置为单点登录的登录方法。	无建议	否
Active Directory 用户	指示是否已配置 Active Directory。Active Directory 和 LDAP 是访问集群的用户的的首选身份验证机制。	无建议	否
LDAP 用户	指示是否已配置 LDAP。对于通过本地用户管理集群的用户来说，Active Directory 和 LDAP 是首选身份验证机制。	无建议	否

参数	Description	建议	影响集群合规性
证书用户	指示是否已将证书用户配置为登录到集群。	无建议	否
本地用户	指示是否已将本地用户配置为登录到集群。	无建议	否

SVM 合规性类别

下表介绍了 Unified Manager 评估的 Storage Virtual Machine (SVM) 安全合规性标准，NetApp 建议以及参数是否影响对 SVM 是否合规的整体判断。

参数	Description	建议	影响 SVM 合规性
审核日志	指示是否已启用审核日志记录。	enabled	是的。
SSH 设置不安全	指示SSH是否使用不安全的密码、例如以开头的密码 cbc*。	否	是的。
登录横幅	指示是否为访问系统上 SVM 的用户启用了登录横幅。	enabled	是的。
LDAP 加密	指示是否已启用 LDAP 加密。	enabled	否
NTLM 身份验证	指示是否已启用 NTLM 身份验证。	enabled	否
LDAP 有效负载签名	指示是否已启用 LDAP 有效负载签名。	enabled	否
CHAP 设置	指示是否已启用 CHAP 。	enabled	否
Kerberos V5	指示是启用还是禁用 Kerberos V5 身份验证。	enabled	否

卷合规性类别

下表介绍了 Unified Manager 评估的卷加密参数，这些参数用于确定卷上的数据是否受到充分保护，不会被未经授权的用户访问。

请注意，卷加密参数不会影响集群或 Storage VM 是否合规。

参数	Description
软件加密	显示使用 NetApp 卷加密（ NetApp Volume Encryption ， NVE ）或 NetApp 聚合加密（ NetApp Aggregate Encryption ， NAE ）软件加密解决方案保护的卷数。
硬件已加密	显示使用 NetApp 存储加密（ NetApp Storage Encryption ， NSE ）硬件加密进行保护的卷数。
软件和硬件已加密	显示受软件和硬件加密保护的卷数。
未加密	显示未加密的卷数。

不合规的含义

如果不满足根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议评估的任何安全标准，则会将集群和 Storage Virtual Machine （ SVM ）视为不合规。此外，如果任何 SVM 被标记为不合规，则集群将被视为不合规。

安全卡中的状态图标对于其合规性具有以下含义：

-  - 此参数已按照建议进行配置。
-  - 未按建议配置参数。
-  —未在集群上启用此功能，或者未按建议配置此参数，但此参数不会影响对象的合规性。

请注意，卷加密状态不会影响集群或 SVM 是否合规。

查看集群安全状态概况

Unified Manager 信息板上的 " 安全性 " 面板根据当前视图显示所有集群或单个集群的高级别安全状态。

步骤

1. 在左侧导航窗格中，单击 * 信息板 * 。
2. 根据您要查看所有受监控集群或单个集群的安全状态，选择 * 所有集群 * 或从下拉菜单中选择一个集群。
3. 查看 * 安全性 * 面板以查看整体状态。

此面板将显示：

- 列出过去 24 小时内收到的安全事件
- 从每个事件到 " 事件 " 详细信息页面的链接
- 一个链接，用于在事件管理清单页面中查看所有活动安全事件
- 集群安全状态（合规或不合规的集群数量）

- SVM 安全状态（合规或不合规的 SVM 数量）
- 卷加密状态（已加密或未加密的卷数）

4. 单击面板顶部的右箭头可在 * 安全性 * 页面中查看安全详细信息。

查看集群和 SVM 的详细安全状态

" 安全性 " 页面显示所有集群的高级别安全状态以及各个集群的详细安全状态。详细的集群状态包括集群合规性，SVM 合规性和卷加密合规性。

步骤

1. 在左侧导航窗格中，单击 * 信息板 *。
2. 根据您要查看所有受监控集群或单个集群的安全状态，选择 * 所有集群 * 或从下拉菜单中选择一个集群。
3. 单击 * 安全性 * 面板中的右箭头。

" 安全性 " 页面将显示以下信息：

- 集群安全状态（合规或不合规的集群数量）
 - SVM 安全状态（合规或不合规的 SVM 数量）
 - 卷加密状态（已加密或未加密的卷数）
 - 每个集群上使用的集群身份验证方法
4. 请参见 " [《适用于 ONTAP 9 的 NetApp 安全加固指南》](#) " 有关如何使所有集群，SVM 和卷符合 NetApp 安全建议的说明。

查看可能需要更新软件或固件的安全事件

某些安全事件的影响区域为 "Upgrade` "。这些事件是从 Active IQ 平台报告的，它们确定了需要升级 ONTAP 软件，节点固件或操作系统软件才能解决的问题（有关安全建议）。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

您可能希望对其中某些问题立即执行更正操作，而其他问题则可以等待您的下一次计划维护。您可以查看所有这些事件，并将其分配给可以解决这些问题的用户。此外，如果您不希望收到有关某些安全升级事件的通知，此列表可帮助您确定这些事件，以便您可以禁用它们。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。

默认情况下，所有活动（新增和已确认）事件都会显示在事件管理清单页面上。

2. 从 " 视图 " 菜单中，选择 * 升级事件 *。

此页面将显示所有活动的升级安全事件。

查看如何在所有集群上管理用户身份验证

"安全性" 页面显示用于对每个集群上的用户进行身份验证的身份验证类型，以及使用每种类型访问集群的用户数量。这样，您就可以验证是否按照贵组织的定义安全地执行用户身份验证。

步骤

1. 在左侧导航窗格中，单击 * 信息板 *。
2. 从信息板上部的下拉菜单中选择 * 所有集群 *。
3. 单击 * 安全性 * 面板中的右箭头，此时将显示 * 安全性 * 页面。
4. 查看 * 集群身份验证 * 卡，查看使用每种身份验证类型访问系统的用户数。
5. 查看 * 集群安全性 * 卡，查看用于对每个集群上的用户进行身份验证的身份验证机制。

结果

如果某些用户使用不安全的方法或 NetApp 不建议的方法访问系统，您可以禁用此方法。

查看所有卷的加密状态

您可以查看所有卷的列表及其当前加密状态，以便确定卷上的数据是否受到充分保护，不会被未经授权的用户访问。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

可应用于卷的加密类型包括：

- 软件—使用 NetApp 卷加密（NVE）或 NetApp 聚合加密（NAE）软件加密解决方案进行保护的卷。
- 硬件—使用 NetApp 存储加密（NetApp Storage Encryption，NSE）硬件加密进行保护的卷。
- 软件和硬件—受软件和硬件加密保护的卷。
- 无—未加密的卷。

步骤

1. 在左侧导航窗格中，单击 * 存储 * > * 卷 *。
2. 在 * 查看 * 菜单中、选择 * 运行状况 * > * 卷加密 *
3. 在 * 运行状况：卷加密 * 视图中、对 * 加密类型 * 字段进行排序、或者使用筛选器显示具有特定加密类型或未加密的卷(加密类型 "None")。

查看所有活动安全事件

您可以查看所有活动的安全事件，然后将每个事件分配给一个可以解决问题描述的用户。此外，如果您不想接收某些安全事件，此列表可帮助您确定要禁用的事件。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。

默认情况下，"新建"和"已确认"事件将显示在"事件管理"清单页面上。

2. 从"视图"菜单中，选择 * 活动安全事件 *。

此页面将显示过去 7 天生成的所有新增和已确认安全事件。

为安全事件添加警报

您可以为单个安全事件配置警报，就像 Unified Manager 收到的任何其他事件一样。此外，如果您希望对所有安全事件进行同样的处理并将电子邮件发送给同一个人，则可以创建一个警报，以便在触发任何安全事件时向您发出通知。

开始之前

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

以下示例显示了如何为 "Telnet Protocol Enabled" 安全事件创建警报。如果为远程管理访问集群配置了 Telnet 访问，则此操作将发送警报。您可以使用相同的方法为所有安全事件创建警报。

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 *，然后选择要启用此警报的集群。
5. 单击 * 事件 * 并执行以下操作：
 - a. 在事件严重性列表中，选择 * 警告 *。
 - b. 在匹配事件列表中，选择 * 已启用 Telnet 协议 *。
6. 单击 * 操作 *，然后在 * 提醒这些用户 * 字段中选择要接收警报电子邮件的用户的名称。
7. 在此页面上配置任何其他选项，以确定通知频率，发出 SNMP 陷阱和执行脚本。

8. 单击 * 保存 *。

禁用特定安全事件

默认情况下，所有事件均处于启用状态。您可以禁用特定事件，以防止为环境中不重要的事件生成通知。如果要恢复接收已禁用事件的通知，可以启用这些事件。

开始之前

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

禁用事件时，系统中先前生成的事件将标记为已废弃，并且不会触发为这些事件配置的警报。启用已禁用的事件后，将从下一个监控周期开始生成这些事件的通知。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 事件设置 *。
2. 在 * 事件设置 * 页面中，通过选择以下选项之一禁用或启用事件：

如果您要 ...	然后执行此操作 ...
禁用事件	<ol style="list-style-type: none">1. 单击 * 禁用 *。2. 在禁用事件对话框中，选择 * 警告 * 严重性。此类别适用于所有安全事件。3. 在匹配事件列中，选择要禁用的安全事件，然后单击右箭头将这些事件移动到禁用事件列。4. 单击 * 保存并关闭 *。5. 验证已禁用的事件是否显示在 Event Setup 页面的列表视图中。
启用事件	<ol style="list-style-type: none">1. 从已禁用事件列表中，选中要重新启用的一个或多个事件对应的复选框。2. 单击 * 启用 *。

安全事件

安全事件根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义参数，为您提供有关 ONTAP 集群，Storage Virtual Machine (SVM) 和卷的安全状态的信息。这些事件会向您通知潜在问题，以便您评估其严重性并在必要时修复问题描述。

安全事件按源类型分组，并包括事件和陷阱名称，影响级别和严重性。这些事件显示在集群和 Storage VM 事件类别中。

管理备份和还原操作

您可以创建 Active IQ Unified Manager 的备份，并使用还原功能在系统发生故障或数据丢失时将备份还原到同一（本地）系统或新（远程）系统。

根据安装 Unified Manager 的操作系统以及要管理的集群和节点的数量，有三种备份和还原方法：

操作系统	部署规模	建议的备份方法
VMware vSphere	任意	Unified Manager 虚拟设备的 VMware 快照
Red Hat Enterprise Linux 或 CentOS Linux	小型	Unified Manager MySQL 数据库转储
	大型	Unified Manager 数据库的 NetApp Snapshot
Microsoft Windows	小型	Unified Manager MySQL 数据库转储
	大型	采用 iSCSI 协议的 Unified Manager 数据库的 NetApp Snapshot

以下各节将介绍这些不同的方法。

在虚拟设备上备份和还原 Unified Manager

安装在虚拟设备上的 Unified Manager 的备份和还原模式是捕获和还原完整虚拟应用程序的映像。

通过以下任务，您可以完成虚拟设备的备份：

1. 关闭虚拟机并为 Unified Manager 虚拟设备创建 VMware 快照。
2. 在数据存储库上创建 NetApp Snapshot 副本以捕获 VMware 快照。

如果数据存储库未托管在运行 ONTAP 软件的系统上，请按照存储供应商准则为 VMware 快照创建备份。

3. 将 NetApp Snapshot 副本或等效快照复制到备用存储。
4. 删除 VMware 快照。

您应使用这些任务实施备份计划，以确保 Unified Manager 虚拟设备在出现问题时受到保护。

要还原虚拟机，您可以使用创建的 VMware 快照将虚拟机还原到备份时间点状态。

使用 MySQL 数据库转储进行备份和还原

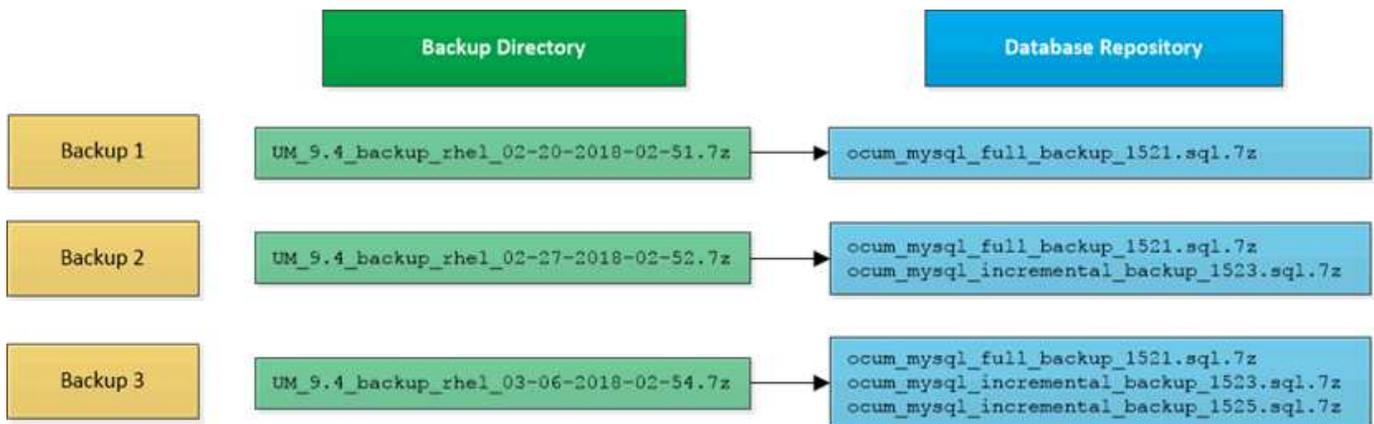
MySQL 数据库转储备份是 Active IQ Unified Manager 数据库和配置文件的副本，可在发生系统故障或数据丢失时使用。您可以计划将备份写入本地目标或远程目标。强烈建议您定义 Active IQ Unified Manager 主机系统外部的远程位置。



如果 Unified Manager 安装在 Linux 和 Windows 服务器上，则 MySQL 数据库转储是默认的备份机制。对于 Red Hat Enterprise Linux，CentOS Linux 系统或 Windows，如果 Active IQ Unified Manager 正在管理大量集群和节点，或者您的 MySQL 备份需要数小时才能完成，则可以使用 NetApp Snapshot 备份方法。

数据库转储备份由备份目录中的一个文件和数据库存储库目录中的一个或多个文件组成。备份目录中的文件非常小，因为它仅包含指向重新创建备份所需的数据库存储库目录中的文件的指针。

首次生成数据库备份时，将在备份目录中创建一个文件，并在数据库存储库目录中创建一个完整备份文件。下次生成备份时，将在备份目录中创建一个文件，并在数据库存储库目录中创建一个增量备份文件，其中包含与完整备份文件的差异。此过程将在您创建其他备份时继续进行，直到达到最大保留设置，如下图所示。



请勿重命名或删除这两个目录中的任何备份文件，否则任何后续还原操作将失败。

如果您将备份文件写入本地系统，则应启动一个将备份文件复制到远程位置的过程，以便在系统问题描述需要完全还原时可以使用这些文件。

在开始备份操作之前，Active IQ Unified Manager 会执行完整性检查，以验证所有必需的备份文件和备份目录是否存在且可写。它还会检查系统上是否有足够的空间来创建备份文件。

配置数据库转储备份的目标和计划

您可以配置 Unified Manager 数据库转储备份设置，以设置数据库备份路径，保留数量和备份计划。您可以启用每日或每周计划备份。默认情况下，计划的备份处于禁用状态，但您应设置备份计划。

开始之前

- 您必须具有操作员，应用程序管理员或存储管理员角色。
- 在定义为备份路径的位置中，必须至少有 150 GB 的可用空间。

建议使用 Unified Manager 主机系统外部的远程位置。

- 如果 Unified Manager 安装在 Linux 系统上并使用 MySQL 备份，请确保在备份目录上设置了以下权限和所有权。

权限：0750 ， 所有权： jboss : 维护

- 如果 Unified Manager 安装在 Windows 系统上并使用 MySQL 备份，请确保只有管理员才能访问备份目录。

关于此任务

与后续备份相比，首次执行备份所需的时间要多，因为第一次备份是完整备份。完整备份可能超过 1 GB ， 并且可能需要三到四个小时。后续备份是增量备份，所需时间更短。



- 如果您发现增量备份文件的数量过大，无法容纳为备份分配的空间，则可以定期创建新的完整备份，以替换旧的完整备份及其所有子增量文件。另外，如果 Unified Manager 安装在 Linux 系统上，则您可能需要开始使用 NetApp Snapshot 备份方法。
- 在添加新集群的最初 15 天内进行的备份可能不够准确，无法获取历史性能数据。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 数据库备份 * 。
2. 在 * 数据库备份 * 页面中，单击 * 备份设置 * 。
3. 为备份路径，保留数量和计划配置适当的值。

保留数量的默认值为 10 ； 您可以使用 0 创建无限备份。

4. 选择 * 计划每日 * 或 * 计划每周 * 按钮，然后指定计划详细信息。
5. 单击 * 应用 * 。

结果

数据库转储备份文件会根据计划创建。您可以在数据库备份页面中查看可用的备份文件。

什么是数据库还原

MySQL 数据库还原是指将现有 Unified Manager 备份文件还原到相同或不同 Unified Manager 服务器的过程。您可以从 Unified Manager 维护控制台执行还原操作。

如果在同一（本地）系统上执行还原操作，并且备份文件全部存储在本地，则可以使用默认位置运行还原选项。如果要在其他 Unified Manager 系统（远程系统）上执行还原操作，则必须先将备份文件从二级存储复制到本地磁盘，然后再运行还原选项。

在还原过程中，您将从 Unified Manager 中注销。还原过程完成后，您可以登录到系统。

如果要将备份映像还原到新服务器，则在还原操作完成后，您需要生成新的 HTTPS 安全证书并重新启动 Unified Manager 服务器。在将备份映像还原到新服务器时，如果需要，您还需要重新配置 SAML 身份验证设置。



在 Unified Manager 升级到较新版本的软件后，不能使用旧的备份文件来还原映像。为了节省空间，升级 Unified Manager 时会自动删除除最新文件之外的所有旧备份文件。

在 Linux 系统上还原 MySQL 数据库备份

如果发生数据丢失或数据损坏，您可以将 Unified Manager 还原到先前的稳定状态，同时最大程度地减少数据丢失。您可以使用 Unified Manager 维护控制台将 Unified Manager 数据库还原到本地或远程 Red Hat Enterprise Linux 或 CentOS 系统。

开始之前

- 您必须具有安装 Unified Manager 的 Linux 主机的 root 用户凭据。
- 您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须已将 Unified Manager 备份文件和数据库存储库目录的内容复制到要执行还原操作的系统。

建议将备份文件复制到默认目录 `/data/ocum-backup`。必须将数据库存储库文件复制到 `/database-dumps-repo` 下的子目录 `/ocum-backup` 目录。

- 备份文件必须为 `.7z` 类型。

关于此任务

还原功能是针对平台和版本的。您只能在同一版本的 Unified Manager 上还原 Unified Manager 备份。您可以将 Linux 备份文件或虚拟设备备份文件还原到 Red Hat Enterprise Linux 或 CentOS 系统。



如果备份文件夹名称包含空格，则必须使用双引号将绝对路径或相对路径包括在内。

步骤

1. 如果要还原到新服务器，则在安装 Unified Manager 后，请勿启动用户界面，也不要再在安装完成后配置任何集群，用户或身份验证设置。备份文件会在还原过程中填充此信息。
2. 使用安全 Shell 连接到 Unified Manager 系统的 IP 地址或完全限定域名。
3. 使用维护用户（`umadmin`）名称和密码登录到系统。
4. 输入命令 `...maintenance_console` 然后按 Enter 键。
5. 在维护控制台 * 主菜单 * 中，输入 * 备份还原 * 选项的编号。
6. 输入 * 还原 MySQL Backup * 的编号。
7. 出现提示时，输入备份文件的绝对路径。

```
Bundle to restore from: /data/ocum-  
backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
```

还原操作完成后，您可以登录到 Unified Manager。

完成后

还原备份后，如果 OnCommand Workflow Automation 服务器不起作用，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 在 Unified Manager 服务器上，如果在步骤 1 中采集失败，请重置数据库密码。

在 Windows 上还原 MySQL 数据库备份

如果发生数据丢失或数据损坏，您可以使用还原功能将 Unified Manager 还原到先前的稳定状态，同时最大程度地减少丢失。您可以使用 Unified Manager 维护控制台将 Unified Manager MySQL 数据库还原到本地 Windows 系统或远程 Windows 系统。

开始之前

- 您必须具有 Windows 管理员权限。
- 您必须已将 Unified Manager 备份文件和数据库存储库目录的内容复制到要执行还原操作的系统。

建议将备份文件复制到默认目录 `\ProgramData\NetApp\OnCommandAppData\ocum\backup`。必须将数据库存储库文件复制到 `\database_dumps_repo` 下的子目录 `\backup` 目录。

- 备份文件必须为 `.7z` 类型。

关于此任务

还原功能是针对平台和版本的。您只能在同一版本的 Unified Manager 上还原 Unified Manager MySQL 备份，并且 Windows 备份只能在 Windows 平台上还原。



如果文件夹名称包含空格，则必须使用双引号将备份文件的绝对路径或相对路径包括在内。

步骤

1. 如果要还原到新服务器，则在安装 Unified Manager 后，请勿启动用户界面，也不要安装完成后配置任何集群，用户或身份验证设置。备份文件会在还原过程中填充此信息。
2. 使用管理员凭据登录到 Unified Manager 系统。
3. 以 Windows 管理员身份启动 PowerShell 或命令提示符。
4. 输入命令 `... maintenance_console` 然后按 Enter 键。
5. 在维护控制台 * 主菜单 * 中，输入 * 备份还原 * 选项的编号。
6. 输入 * 还原 MySQL Backup * 的编号。
7. 出现提示时，输入备份文件的绝对路径。

```
Bundle to restore from:  
\\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_backup_windows_02-20-2020-02-51.7z
```

还原操作完成后，您可以登录到 Unified Manager 。

完成后

还原备份后，如果 OnCommand Workflow Automation 服务器不起作用，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 在 Unified Manager 服务器上，如果在步骤 1 中采集失败，请重置数据库密码。

使用 NetApp Snapshot 进行备份和还原

NetApp Snapshot 备份会为 Unified Manager 数据库和配置文件创建一个时间点映像，您可以使用此映像发生在系统故障或数据丢失时进行还原。您计划定期将 Snapshot 备份写入其中一个 ONTAP 集群上的卷，以便始终具有最新副本。



此功能不适用于虚拟设备上安装的 Active IQ Unified Manager 。

在 Linux 上配置备份

如果 Active IQ Unified Manager 安装在 Linux 计算机上，则可以决定使用 NetApp Snapshot 配置备份和还原。

Snapshot 备份所需时间非常短，通常只需几分钟，Unified Manager 数据库锁定时间非常短，因此不会对安装造成任何中断。此映像占用的存储空间极少，并且性能开销极低，因为它仅记录自上次创建 Snapshot 副本以来对文件所做的更改。由于 Snapshot 是在 ONTAP 集群上创建的，因此您可以根据需要利用 SnapMirror 等其他 NetApp 功能来创建二级保护。

在开始备份操作之前，Unified Manager 会执行完整性检查以验证目标系统是否可用。



- 您只能在同一版本的 Active IQ Unified Manager 上还原 Snapshot 备份。
- 例如，如果您在 Unified Manager 9.9 上创建备份，则只能在 Unified Manager 9.9 系统上还原备份。
- 如果对 Snapshot 配置进行了任何更改，则可能会将此快照发生原因为无效。

配置 Snapshot 备份位置

您可以使用 ONTAP 系统管理器或 ONTAP 命令行界面配置将 Snapshot 备份存储在其中一个 ONTAP 集群上的卷。

开始之前

集群，Storage VM 和卷必须满足以下要求：

- 集群要求：
 - 必须安装 ONTAP 9.3 或更高版本

- 它应在地理位置上靠近 Unified Manager 服务器
- 它可以由 Unified Manager 监控，但不是必需的
- Storage VM 要求：
 - 必须将名称开关和名称映射设置为使用 "files"
 - 为与客户端用户相对应而创建的本地用户
 - 确保已选择所有读 / 写访问权限
 - 确保在导出策略中将超级用户访问设置为 "any"
 - 适用于 Linux 的 NetApp Snapshot 的 NFS
 - 必须在客户端和 Storage VM 上指定的 NFS 服务器和 NFSv4 ID 域上启用 NFSv4
 - 此卷应至少是 Unified Manager 大小的两倍 /opt/netapp/data 目录

使用命令 `du -sh /opt/netapp/data/` 以检查当前大小。

- 卷要求：
 - 此卷应至少是 Unified Manager /opt/netapp/data 目录大小的两倍
 - 安全模式必须设置为 UNIX
 - 必须禁用本地快照策略
 - 应启用卷自动调整大小
 - 应将性能服务级别设置为 IOPS 高且延迟低的策略，例如 "Extreme"

关于此任务

有关创建 NFS 卷的详细步骤，请参见 ["如何在 ONTAP 9 中配置 NFSv4"](#) 和 ["《ONTAP 9 NFS 配置快速指南》"](#)。

指定 Snapshot 备份的目标位置

您可以在已在其中一个 ONTAP 集群中配置的卷上配置 Active IQ Unified Manager Snapshot 备份的目标位置。您可以从 Active IQ Unified Manager 维护控制台定义位置。

开始之前

- 您必须具有安装 Active IQ Unified Manager 的 Linux 主机的 root 用户凭据。
- 您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须具有集群管理 IP 地址，Storage VM 的名称，卷的名称以及存储系统用户名和密码。
- 您必须已将卷挂载到 Active IQ Unified Manager 主机，并且必须具有挂载路径。

步骤

1. 使用安全 Shell 连接到 Active IQ Unified Manager 系统的 IP 地址或 FQDN。
2. 使用维护用户（umadmin）名称和密码登录到系统。

3. 输入命令 `... maintenance_console` 然后按Enter键。
4. 在维护控制台 * 主菜单 * 中，输入 * 备份还原 * 选项的编号。
5. 输入 * 配置 NetApp Snapshot 备份 * 的编号。
6. 输入数字以配置 NFS 。
7. 查看需要提供的信息，然后为 * 输入备份配置详细信息 * 输入数字。
8. 要确定要写入 Snapshot 的卷，请输入集群管理界面的 IP 地址， Storage VM 的名称，卷的名称， LUN 名称，存储系统用户名和密码以及挂载路径。
9. 验证此信息并输入 `y`。

系统将执行以下任务：

- 建立与集群的连接
 - 停止所有服务
 - 在卷中创建一个新目录并复制 Active IQ Unified Manager 数据库配置文件
 - 从 Active IQ Unified Manager 中删除文件并创建指向新数据库目录的符号链接
 - 重新启动所有服务
10. 如果尚未创建 Snapshot 备份计划，请退出维护控制台并启动 Active IQ Unified Manager 界面以创建此计划。

在 Windows 上配置备份

Active IQ Unified Manager 支持使用 iSCSI 协议通过 LUN 在 Windows 操作系统上使用 NetApp Snapshot 进行备份和还原。

可以在所有 UM 服务运行时进行基于 Snapshot 的备份。由于备份会在整个数据库上设置全局读取锁定，从而阻止任何并发写入，因此会在 Snapshot 中捕获数据库的一致状态。要使 Windows 操作系统上安装的 Unified Manager 系统使用 NetApp Snapshot 执行备份和还原，您应首先使用维护控制台将 Unified Manager 备份配置为 Snapshot 。

在为 Active IQ Unified Manager 备份配置 Snapshot 安装之前，您需要执行以下配置任务。

- 配置 ONTAP 集群
- 配置 Windows 主机

配置 Windows 的备份位置

即使在 Windows 上安装了 Active IQ Unified Manager ，您也应配置要存储 Snapshot 备份的卷。

开始之前

集群， Storage VM 和卷必须满足以下要求：

- 集群要求：

- 必须安装 ONTAP 9.3 或更高版本
- 它应在地理位置上靠近 Unified Manager 服务器
- 它由 Unified Manager 监控
- Storage VM 要求：
 - ONTAP 集群上的 iSCSI 连接
 - 必须为配置的计算机启用 iSCSI 协议
 - 您应该有一个专用卷和 LUN 用于备份配置。选定卷只能包含一个 LUN，而不能包含任何其他 LUN。
 - LUN 的大小应至少是 9.9 Active IQ Unified Manager 中预期处理的数据大小的两倍。

这样也会对卷设置相同的大小要求。

 - 确保已选择所有读 / 写访问权限
 - 确保在导出策略中将超级用户访问设置为 "any"
- 卷和 LUN 要求：
 - 此卷应至少是 Unified Manager MySQL 数据目录大小的两倍。
 - 安全模式必须设置为 Windows
 - 必须禁用本地快照策略
 - 应启用卷自动调整大小
 - 应将性能服务级别设置为 IOPS 高且延迟低的策略，例如 "Extreme"

正在配置 ONTAP 集群

在为 Windows 配置 Active IQ Unified Manager for Snapshot 备份和还原之前，您应该对 ONTAP 和 Windows 主机执行少量预配置。

您可以使用命令提示符或 System Manager 用户界面配置 ONTAP 集群。配置 ONTAP 集群涉及到将数据 LIF 配置为可用作 iSCSI LIF 分配给 Storage VM。下一步是使用 System Manager 用户界面配置启用了 iSCSI 的 Storage VM。您需要为此 Storage VM 配置一个静态网络路由，以控制 LIF 如何将网络用于出站流量。



您应该有一个专用卷和一个 LUN 用于备份配置。选定卷应仅包含一个 LUN。LUN 的大小应至少是 Active IQ Unified Manager 预期处理的数据大小的两倍。

您需要执行以下配置：

1. 配置启用了 iSCSI 的 Storage VM 或使用具有相同配置的现有 Storage VM。
2. 为已配置的 Storage VM 配置网络路由。
3. 配置一个容量适当的卷以及一个 LUN，确保该卷仅专用于此 LUN。
4. 在 Storage VM 中配置启动程序组。
5. 配置端口集。
6. 将 igroup 与端口集集成。
7. 将 LUN 映射到 igroup。

配置 Windows 主机

您需要配置安装了 Active IQ Unified Manager 的 Windows 主机，以便为 NetApp Snapshot 备份做好准备。要在 Windows 主机上启动 Microsoft iSCSI 启动程序，请在搜索栏中键入 "iSCSI"，然后单击 * iSCSI 启动程序 *。

开始之前

您应清理主机上先前的任何配置。

关于此任务

如果您尝试在全新安装的 Windows 上启动 iSCSI 启动程序，系统将提示您进行确认，确认后，将显示 iSCSI 属性对话框。如果是现有的 Windows 安装，则会显示 iSCSI 属性对话框，其中的目标为非活动或正在尝试连接。因此，您需要确保删除 Windows 主机上先前的所有配置。

步骤

1. 清理主机上先前的所有配置。
2. 发现目标门户。
3. 连接到目标门户。
4. 使用多路径连接到目标门户。
5. 发现这两个 LIF。
6. 发现在 Windows 计算机中配置为设备的 LUN。
7. 在 Windows 中将发现的 LUN 配置为新的卷驱动器。

指定 Windows Snapshot 备份的目标位置

您应在已在其中一个 ONTAP 集群中配置的卷上配置 Active IQ Unified Manager Snapshot 备份的目标位置，并使用维护控制台定义该位置。

开始之前

- 您必须具有安装 Active IQ Unified Manager 的 Windows 主机的管理员权限。
- 您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须具有集群管理 IP 地址，Storage VM 的名称，卷的名称，LUN 名称以及存储系统用户名和密码。
- 您必须已将卷作为网络驱动器挂载到 Active IQ Unified Manager 主机，并且必须具有挂载驱动器。

步骤

1. 使用 Power Shell 连接到 Active IQ Unified Manager 系统的 IP 地址或完全限定域名。
2. 使用维护用户（umadmin）名称和密码登录到系统。
3. 输入命令 ... maintenance_console 然后按Enter键。
4. 在维护控制台 * 主菜单 * 中，输入 * 备份还原 * 选项的编号。

5. 输入 * 配置 NetApp Snapshot 备份 * 的编号。
6. 输入数字以配置 iSCSI。
7. 查看需要提供的信息，然后为 * 输入备份配置详细信息 * 输入数字。
8. 要确定要写入 Snapshot 的卷，请输入集群管理界面的 IP 地址， Storage VM 的名称，卷的名称， LUN 名称，存储系统用户名和密码以及挂载驱动器。
9. 验证此信息并输入 *y*。

系统将执行以下任务：

- 已验证 Storage VM
 - 已验证卷
 - 已验证挂载驱动器和状态
 - LUN 存在和状态
 - 网络驱动器存在
 - 验证已挂载卷上是否存在建议空间（mysql 数据目录的两倍以上）
 - 与卷中的专用 LUN 对应的 LUN 路径
 - igroup 名称
 - 挂载网络驱动器的卷的 GUID
 - 用于与 ONTAP 通信的 iSCSI 启动程序
10. 如果尚未创建 Snapshot 备份计划，请退出维护控制台并启动 Active IQ Unified Manager 界面以创建此计划。

从维护控制台配置 **NetApp Snapshot** 备份

您应从维护控制台将 Active IQ Unified Manager 备份配置为 NetApp Snapshot 备份。

开始之前

您应了解系统的以下详细信息：

- 集群 IP 地址
- Storage VM 名称
- Volume name
- LUN name
- 挂载路径
- 存储系统凭据

步骤

1. 访问 Unified Manager 的维护控制台。
2. 输入 ... 4 选择*备份还原*。

3. 输入 ... 2 选择*使用NetApp Snapshot*进行备份和还原。



如果要更改备份配置、请输入 3 用于更新NetApp Snapshot备份配置。您只能更新密码。

4. 在菜单中、输入 1 选择*配置NetApp Snapshot备份*。

5. 输入 ... 1 以提供所需信息。

6. 提供维护控制台的用户名和密码，然后确认 LUN 已挂载到主机上。

然后，此过程将验证数据目录， LUN 路径， Storage VM ， 卷， 空间可用性， 您提供的驱动器等均正确无误。在后台继续执行的操作包括：

- 服务已停止
- 数据库目录将移至已挂载的存储
- 删除数据库目录并建立符号链接
- 在 Active IQ Unified Manager 界面中完成配置后，服务将重新启动，备份类型将修改为 NetApp Snapshot ，并在用户界面中显示为数据库备份（基于 Snapshot ）。

示例

在开始备份操作之前，您必须检查 Snapshot 配置是否有任何更改，因为它可能会将快照发生原因设置为无效。假设您在 G 驱动器和 Snapshot 已创建中配置了备份。您稍后会根据新配置将备份重新配置到 E 驱动器，并将数据保存到 E 驱动器。如果尝试还原在 G 驱动器中创建的 Snapshot ，则会失败，并显示错误，指出 G 驱动器不存在。

为 Linux 和 Windows 定义备份计划

您可以使用 Unified Manager UI 配置创建 Unified Manager Snapshot 备份的计划。

开始之前

- 您必须具有操作员，应用程序管理员或存储管理员角色。
- 您必须已从维护控制台配置 NetApp Snapshot 备份设置，以确定要创建快照的目标。

关于此任务

Snapshot 备份只需几分钟即可创建完毕， Unified Manager 数据库仅锁定几秒钟。



在添加新集群的最初 15 天内进行的备份可能不够准确，无法获取历史性能数据。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 数据库备份 * 。
2. 在 * 数据库备份 * 页面中，单击 * 备份设置 * 。
3. 在 * 保留数量 * 字段中输入要保留的最大 Snapshot 副本数。

保留数量的默认值为 10 。最大 Snapshot 副本数取决于集群上的 ONTAP 软件版本。您可以将此字段留空以实施最大值，而不管 ONTAP 版本如何。

4. 选择 * 计划每日 * 或 * 计划每周 * 按钮，然后指定计划详细信息。

5. 单击 * 应用 *。

结果

Snapshot 备份文件会根据计划创建。您可以在数据库备份页面中查看可用的备份文件。

完成后

由于此卷和快照的重要性，您可能需要为此卷创建一个或两个警报，以便在以下任一情况下收到通知：

- 卷空间已满 90%。使用事件 * 卷空间已满 * 设置警报。

您可以使用 ONTAP 系统管理器或 ONTAP 命令行界面向卷添加容量，以使 Unified Manager 数据库不会用尽空间。

- 快照数量接近上限。使用事件 * Snapshot 副本太多 * 设置警报。

您可以使用 ONTAP 系统管理器或 ONTAP 命令行界面删除较早的快照，以便始终有空间进行新的快照备份。

您可以在警报设置页面中配置警报。

还原 Linux 和 Windows 的 Snapshot 备份

如果发生数据丢失或数据损坏，您可以将 Unified Manager 还原到先前的稳定状态，同时最大程度地减少数据丢失。您可以使用 Unified Manager 维护控制台将 Unified Manager Snapshot 数据库还原到本地或远程操作系统。

开始之前

- 您必须具有 Linux 主机的 root 用户凭据以及安装了 Unified Manager 的 Windows 主机的管理权限。
- 您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

关于此任务

还原功能是针对平台和版本的。您只能在同一版本的 Unified Manager 上还原 Unified Manager 备份。

步骤

1. 连接到 Unified Manager 系统的 IP 地址或完全限定域名。

* Linux *	安全外壳
• Windows *	Power Shell

1. 使用维护用户（umadmin）名称和密码登录到系统。

2. 输入命令 ... maintenance_console 然后按Enter键。

3. 在维护控制台 * 主菜单 * 中，输入 * 备份还原 * 选项的编号。
4. 输入 * 使用 NetApp Snapshot* 进行备份和还原的编号。

如果要还原到新服务器，则在安装 Unified Manager 后，请勿启动用户界面，也不要安装完成后配置任何集群，用户或身份验证设置。输入 * 配置 NetApp Snapshot 备份 * 的编号，然后按照原始系统上配置的方式配置 Snapshot 备份设置。

5. 输入 * 使用 NetApp Snapshot* 还原的数字。
6. 选择要还原的 Snapshot 备份文件，然后按 * 输入 * 。
7. 还原过程完成后，登录到 Unified Manager 用户界面。

完成后

还原备份后，如果 Workflow Automation 服务器不起作用，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 在 Unified Manager 服务器上，如果在步骤 1 中采集失败，请重置数据库密码。

修改备份类型

如果要更改 Active IQ Unified Manager 系统的备份类型，则可以使用维护控制台选项。通过取消配置 NetApp Snapshot 备份选项，您可以回退到基于 MySQL 的备份。

开始之前

您必须拥有有权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

步骤

1. 访问维护控制台
2. 选择 ... 4 从*主菜单*执行备份还原。
3. 选择 ... 2 从*备份和还原菜单*。
4. 选择 ... 4 用于*取消配置NetApp Snapshot备份*。

此时将显示所执行的操作，这些操作包括停止服务，中断符号链接，将数据从存储移动到目录，然后重新启动服务。

取消配置 NetApp Snapshot 备份后，备份机制将更改为基于 MySQL 的默认备份机制。此更改将显示在常规设置的数据库备份部分中。

Unified Manager 的按需备份

您可以根据需要使用 Active IQ Unified Manager 用户界面生成按需备份。通过按需备份，您可以使用现有备份方法瞬时创建备份。按需备份不区分基于 MySQL 的备份或基于 NetApp Snapshot 的备份。

您可以使用数据库备份页面上的 * 立即备份 * 按钮执行按需备份。按需备份不取决于您为 Active IQ Unified

Manager 配置的计划。

将 Unified Manager 虚拟设备迁移到 Linux 系统

如果要更改运行 Unified Manager 的主机操作系统，您可以将 Unified Manager MySQL 数据库转储备份从虚拟设备还原到 Red Hat Enterprise Linux 或 CentOS Linux 系统。

开始之前

- 在虚拟设备上：
 - 您必须具有操作员，应用程序管理员或存储管理员角色。
 - 您必须知道要执行还原操作的 Unified Manager 维护用户的名称。
- 在 Linux 系统上：
 - 您必须已按照安装指南中的说明在 RHEL 或 CentOS 服务器上安装 Unified Manager 。
 - 此服务器上的 Unified Manager 版本必须与使用备份文件的虚拟设备上的版本相同。
 - 安装后，请勿启动 UI 或在 Linux 系统上配置任何集群，用户或身份验证设置。备份文件会在还原过程中填充此信息。
 - 您必须具有 Linux 主机的 root 用户凭据。

关于此任务

以下步骤介绍如何在虚拟设备上创建备份文件，将备份文件复制到 Red Hat Enterprise Linux 或 CentOS 系统，然后将数据库备份还原到新系统。

步骤

1. 在虚拟设备上，单击 * 管理 * > * 数据库备份 * 。
2. 在 * 数据库备份 * 页面中，单击 * 备份设置 * 。
3. 将备份路径更改为 /jail/support。
4. 在计划部分中，选择 * 计划每日 * ，并输入当前时间过几分钟的时间，以便很快创建备份。
5. 单击 * 应用 * 。
6. 等待几小时，以便生成备份。

完整备份可能超过 1 GB ，并且可能需要三到四个小时才能完成。

7. 以root用户身份登录到安装了Unified Manager的Linux主机、然后从复制备份文件 /support 在虚拟设备上使用SCP.root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/*

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

确保已复制 .7z 备份文件和所有 .7z 中的存储库文件 /database-dumps-repo 子目录。

8. 在命令提示符处、还原备份：um backup restore -f
/<backup_file_path>/<backup_file_name>

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. 还原操作完成后，登录到 Unified Manager Web UI。

完成后

您应执行以下任务：

- 生成新的 HTTPS 安全证书并重新启动 Unified Manager 服务器。
- 将备份路径更改为Linux系统的默认设置 (/data/ocum-backup)、或者您选择的新路径、因为没有 /jail/support Linux系统上的路径。
- 如果正在使用 WFA ，请重新配置 Workflow Automation 连接的两端。
- 如果使用的是 SAML ，请重新配置 SAML 身份验证设置。

确认 Linux 系统上的所有内容均按预期运行后，您可以关闭并删除 Unified Manager 虚拟设备。

管理脚本

您可以使用脚本在 Unified Manager 中自动修改或更新多个存储对象。此脚本与警报关联。当事件触发警报时，将执行脚本。您可以上传自定义脚本，并在生成警报时测试其执行情况。

默认情况下，可以将脚本上传到 Unified Manager 并运行这些脚本。如果贵组织出于安全原因不希望允许使用此功能，则可以从 * 存储管理 * > * 功能设置 * 禁用此功能。

脚本如何处理警报

您可以将警报与脚本关联，以便在 Unified Manager 中针对事件发出警报时执行脚本。您可以使用这些脚本解决存储对象的问题，或者确定正在生成事件的存储对象。

在 Unified Manager 中为事件生成警报时，系统会向指定的收件人发送警报电子邮件。如果已将警报与脚本关联，则会执行此脚本。您可以从警报电子邮件获取传递给脚本的参数的详细信息。



如果您已创建自定义脚本并将其与特定事件类型的警报关联，则会根据您针对该事件类型的自定义脚本执行操作，并且默认情况下，"Management Actions" 页面或 Unified Manager 信息板上不提供 * 修复 IT* 操作。

该脚本使用以下参数执行：

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType

- -eventState
- -eventArgs

您可以在脚本中使用参数，并收集相关事件信息或修改存储对象。

从脚本获取参数的示例

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

生成警报时，将执行此脚本并显示以下输出：

```
-eventID : 290
-eventSourceID : 4138
```

正在添加脚本

您可以在 Unified Manager 中添加脚本，并将这些脚本与警报关联。生成警报时，系统会自动执行这些脚本，您可以通过这些脚本获取有关生成事件的存储对象的信息。

开始之前

- 您必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 脚本支持的文件格式为 Perl、Shell、PowerShell、Python 和 .bat 文件。

安装 Unified Manager 的平台	支持的语言
VMware	Perl 和 Shell 脚本
Linux	Perl , Python 和 Shell 脚本
Windows	PowerShell , Perl , Python 和 .bat 脚本

- 对于 Perl 脚本，必须在 Unified Manager 服务器上安装 Perl。对于 VMware 安装，默认情况下会安装 Perl 5，并且脚本仅支持 Perl 5 支持的功能。如果 Perl 是在 Unified Manager 之后安装的，则必须重新启动 Unified Manager 服务器。
- 对于 PowerShell 脚本，必须在 Windows 服务器上设置相应的 PowerShell 执行策略，以便可以执行这些脚本。



如果脚本创建日志文件以跟踪警报脚本进度，则必须确保日志文件不会在 Unified Manager 安装文件夹中的任何位置创建。

- 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

您可以上传自定义脚本并收集有关警报的事件详细信息。



如果您在用户界面中看不到此功能，则是因为管理员已禁用此功能。如果需要，可以从 * 存储管理 * > * 功能设置 * 启用此功能。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 脚本 *。
2. 在 * 脚本 * 页面中，单击 * 添加 *。
3. 在 * 添加脚本 * 对话框中，单击 * 浏览 * 以选择脚本文件。
4. 输入所选脚本的问题描述。
5. 单击 * 添加 *。

正在删除脚本

当不再需要脚本或脚本无效时，您可以从 Unified Manager 中删除该脚本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 脚本不得与警报关联。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 脚本 *。
2. 在 * 脚本 * 页面中，选择要删除的脚本，然后单击 * 删除 *。
3. 在 * 警告 * 对话框中，单击 * 是 * 确认删除。

测试脚本执行

在为存储对象生成警报时，您可以验证脚本是否已正确执行。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已将支持的文件格式的脚本上传到 Unified Manager 。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 脚本 *。
2. 在 * 脚本 * 页面中，添加测试脚本。
3. 在左侧导航窗格中，单击 * 存储管理 * > * 警报设置 *。

4. 在 * 警报设置 * 页面中，执行以下操作之一：

至 ...	执行此操作 ...
添加警报	<ol style="list-style-type: none">1. 单击 * 添加 * 。2. 在操作部分中，将警报与测试脚本关联。
编辑警报	<ol style="list-style-type: none">1. 选择警报，然后单击 * 编辑 * 。2. 在操作部分中，将警报与测试脚本关联。

1. 单击 * 保存 * 。
2. 在 * 警报设置 * 页面中，选择您添加或修改的警报，然后单击 * 测试 * 。

使用 " -test` " 参数执行脚本，并向创建警报时指定的电子邮件地址发送通知警报。

管理和监控组

您可以在 Unified Manager 中创建组来管理存储对象。

了解组

您可以在 Unified Manager 中创建组来管理存储对象。了解有关组的概念以及如何通过组规则向组添加存储对象，将有助于您管理环境中的存储对象。

什么是组

组是异构存储对象（集群，SVM 或卷）的动态集合。您可以在 Unified Manager 中创建组，以便轻松管理一组存储对象。组中的成员可能会发生更改，具体取决于 Unified Manager 在某一时间点监控的存储对象。

- 每个组都有一个唯一的名称。
- 您必须为每个组至少配置一个组规则。
- 您可以将一个组与多个组规则关联。
- 每个组可以包含多种类型的存储对象，例如集群，SVM 或卷。
- 存储对象会根据创建组规则的时间或 Unified Manager 完成监控周期而动态添加到组中。
- 您可以同时对组中的所有存储对象应用操作，例如为卷设置阈值。

组规则如何用于组

组规则是您定义的一个标准，用于将存储对象（卷，集群或 SVM）包含在特定组中。您可以使用条件组或条件为组定义组规则。

- 您必须将组规则与组关联。

- 您必须为组规则关联一个对象类型；一个组规则只关联一个对象类型。
- 在每个监控周期之后，或者在创建，编辑或删除规则时，系统会从组中添加或删除存储对象。
- 一个组规则可以具有一个或多个条件组，每个条件组可以具有一个或多个条件。
- 根据您创建的组规则，存储对象可以属于多个组。

条件

您可以创建多个条件组，每个条件组可以具有一个或多个条件。您可以将组规则中定义的所有条件组应用于组，以指定组中包含的存储对象。

条件组中的条件使用逻辑 AND 执行。必须满足条件组中的所有条件。创建或修改组规则时，系统会创建一个条件，此条件仅应用，选择和分组满足条件组中所有条件的存储对象。如果要缩小要包含在一个组中的存储对象的范围，可以在一个条件组中使用多个条件。

您可以使用以下操作数和运算符并指定所需值来创建存储对象的条件。

存储对象类型	适用的操作数
Volume	<ul style="list-style-type: none"> • 对象名称 • 所属集群名称 • 所属 SVM 名称 • 标注
SVM	<ul style="list-style-type: none"> • 对象名称 • 所属集群名称 • 标注
集群	<ul style="list-style-type: none"> • 对象名称 • 标注

如果选择标注作为任何存储对象的操作数，则可以使用 "is" 运算符。对于所有其他操作数，您可以选择 "is" 或 "contains" 作为运算符。

- 操作数

Unified Manager 中的操作数列表会根据选定对象类型而发生变化。此列表包括您在 Unified Manager 中定义的对象名称，所属集群名称，所属 SVM 名称和标注。

- 运算符

操作符列表会根据为条件选择的操作数而发生变化。Unified Manager 中支持的运算符为 "is" 和 "contains"。

如果选择 "is" 运算符，则会评估条件，以确定操作数值与为选定操作数提供的值是否完全匹配。

如果选择 "contains" 运算符，则系统会评估此条件以满足以下条件之一：

- 该操作数值与为选定操作数提供的值完全匹配
- 操作数值包含为选定操作数提供的值
 - 价值

值字段会根据选定操作数发生变化。

包含条件的组规则示例

考虑具有以下两个条件的卷的条件组：

- 名称包含 "vol"
- SVM 名称为 data_svm

此条件组会选择名称中包含 "vol" 且托管在名称为 "data_svm" 的 SVM 上的所有卷。

条件组

条件组使用逻辑或执行，然后应用于存储对象。存储对象必须满足要包括在组中的一个条件组。所有条件组的存储对象将合并在一起。您可以使用条件组来扩大要包含在组中的存储对象的范围。

包含条件组的组规则示例

请考虑为一个卷设置两个条件组，每个条件组包含以下两个条件：

- 条件组 1
 - 名称包含 "vol"
 - SVM 名称为 data_svm 条件组 1 会选择名称中包含 "vol" 且托管在名称为 data_svm 的 SVM 上的所有卷。
- 条件组 2
 - 名称包含 "vol"
 - data-priority 的标注值为 "critical" 条件组 2 会选择名称中包含 "vol" 且使用数据优先级标注值标注为 "critical" 的所有卷。

如果将包含这两个条件组的组规则应用于存储对象，则会将以下存储对象添加到选定组：

- 名称中包含 "vol" 且托管在名称为 "data_svm" 的 SVM 上的所有卷。
- 名称中包含 "vol" 且标注了数据优先级标注值 "Critical" 的所有卷。

组操作如何对存储对象执行

组操作是对组中的所有存储对象执行的操作。例如，您可以将卷阈值组操作配置为同时更改组中所有卷的卷阈值。

组支持唯一的组操作类型。您的组只能包含一个卷运行状况阈值组操作类型。但是，您可以为同一组配置不同类型的组操作（如果可用）。组操作的排名决定了将该操作应用于存储对象的顺序。存储对象的详细信息页面提供了有关对存储对象应用哪些组操作的信息。

唯一组操作示例

假设卷 A 属于组 G1 和 G2，并且已为这些组配置以下卷运行状况阈值组操作：

- Change_capacity_threshold 排名为1的组操作、用于配置卷的容量
- Change_snapshot_copies 排名为2的组操作、用于配置卷的Snapshot副本

。 Change_capacity_threshold 组操作始终优先于 Change_snapshot_copies 组操作、并应用于卷A。当 Unified Manager 完成一个监控周期后、将根据重新评估卷A的运行状况阈值相关事件 Change_capacity_threshold 组操作。您不能为 G1 或 G2 组配置其他卷阈值类型的组操作。

添加组

您可以创建组来组合集群，卷和 Storage Virtual Machine（SVM），以便于管理。

开始之前

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

您可以定义组规则，以便在组中添加或删除成员以及修改组的组操作。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组 * 选项卡中，单击 * 添加 *。
3. 在 * 添加组 * 对话框中，输入组的名称和问题描述。
4. 单击 * 添加 *。

编辑组

您可以编辑在 Unified Manager 中创建的组的名称和问题描述。

开始之前

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

编辑组以更新名称时，必须指定唯一名称；不能使用现有组名称。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组 * 选项卡中，选择要编辑的组，然后单击 * 编辑 *。
3. 在 * 编辑组 * 对话框中，更改组的名称，问题描述或两者。

4. 单击 * 保存 *。

删除组

当不再需要某个组时，您可以从 Unified Manager 中删除该组。

开始之前

- 任何存储对象（集群，SVM 或卷）都不能与与要删除的组关联的任何组规则相关联。
- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组 * 选项卡中，选择要删除的组，然后单击 * 删除 *。
3. 在 * 警告 * 对话框中，单击 * 是 * 确认删除。

删除组不会删除与组关联的组操作。但是，删除组后，这些组操作将取消映射。

正在添加组规则

您可以为组创建组规则，以便将卷，集群或 Storage Virtual Machine（SVM）等存储对象动态添加到组。要创建组规则，必须至少配置一个条件组并至少配置一个条件。

开始之前

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

创建组规则后，系统会立即添加当前受监控的存储对象。只有在监控周期完成后，才会添加新对象。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组规则 * 选项卡中，单击 * 添加 *。
3. 在 * 添加组规则 * 对话框中，指定组规则的名称。
4. 在 * 目标对象类型 * 字段中，选择要分组的存储对象类型。
5. 在 * 组 * 字段中，选择要为其创建组规则的所需组。
6. 在 * 条件 * 部分中，执行以下步骤以创建条件，条件组或同时创建这两者：

要创建	执行此操作 ...
条件	<ol style="list-style-type: none"> 1. 从操作数列表选择一个操作数。 2. 选择 * 包含 * 或 * 是 * 作为运算符。 3. 输入一个值，或者从可用列表选择一个值。
条件组	<ol style="list-style-type: none"> 1. 单击 * 添加条件组 * 2. 从操作数列表选择一个操作数。 3. 选择 * 包含 * 或 * 是 * 作为运算符。 4. 输入一个值，或者从可用列表选择一个值。 5. 如果需要，单击 * 添加条件 * 以创建更多条件，然后对每个条件重复步骤 a 到 d。

1. 单击 * 添加 *。

创建组规则的示例

在添加组规则对话框中执行以下步骤以创建组规则，包括配置条件和添加条件组：

1. 指定组规则的名称。
2. 选择对象类型作为 Storage Virtual Machine （ SVM ）。
3. 从组列表选择一个组。
4. 在条件部分中，选择 * 对象名称 * 作为操作数。
5. 选择 * 包含 * 作为操作符。
6. 将值输入为 svm_data。
7. 单击 * 添加条件组 *。
8. 选择 * 对象名称 * 作为操作数。
9. 选择 * 包含 * 作为操作符。
10. 将值输入为 vol。
11. 单击 * 添加条件 *。
12. 重复步骤 8 到 10，方法是在步骤 8 中选择 * data-priority * 作为操作数，在步骤 9 中选择 * is-* 作为操作符，在步骤 10 中选择 * critical* 作为值。
13. 单击 * 添加 * 为组规则创建条件。

编辑组规则

您可以编辑组规则以修改条件组以及条件组中的条件，以便向特定组添加或删除存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组规则 * 选项卡中，选择要编辑的组规则，然后单击 * 编辑 *。
3. 在 * 编辑组规则 * 对话框中，根据需要更改组规则名称，关联的组名称，条件组和条件。



您不能更改组规则的目标对象类型。

4. 单击 * 保存 *。

正在删除组规则

当不再需要组规则时，您可以从 Active IQ Unified Manager 中删除组规则。

开始之前

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

删除组规则后，关联的存储对象将从组中删除。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组规则 * 选项卡中，选择要删除的组规则，然后单击 * 删除 *。
3. 在 * 警告 * 对话框中，单击 * 是 * 确认删除。

正在添加组操作

您可以配置要应用于组中存储对象的组操作。通过为组配置操作，您可以节省时间，因为不必将这些操作单独添加到每个对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组操作 * 选项卡中，单击 * 添加 *。
3. 在 * 添加组操作 * 对话框中，输入操作的名称和问题描述。

4. 从 * 组 * 菜单中，选择要为其配置操作的组。
5. 从 * 操作类型 * 菜单中，选择一种操作类型。

此时，对话框将展开，您可以使用所需参数配置选定的操作类型。

6. 为所需参数输入适当的值以配置组操作。
7. 单击 * 添加 *。

编辑组操作

您可以编辑在 Unified Manager 中配置的组操作参数，例如组操作名称，问题描述，关联的组名称以及操作类型的参数。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组操作 * 选项卡中，选择要编辑的组操作，然后单击 * 编辑 *。
3. 在 * 编辑组操作 * 对话框中，根据需要更改组操作名称，问题描述，关联的组名称以及操作类型的参数。
4. 单击 * 保存 *。

为组配置卷运行状况阈值

您可以为容量， Snapshot 副本， qtree 配额， 增长和索引节点配置组级卷运行状况阈值。

开始之前

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

组操作的卷运行状况阈值类型仅适用于组中的卷。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组操作 * 选项卡中，单击 * 添加 *。
3. 输入组操作的名称和问题描述。
4. 从 * 组 * 下拉框中，选择要为其配置组操作的组。
5. 选择 * 操作类型 * 作为卷运行状况阈值。
6. 选择要为其设置阈值的类别。

7. 为运行状况阈值输入所需的值。

8. 单击 * 添加 *。

正在删除组操作

当不再需要组操作时，您可以从 Unified Manager 中删除组操作。

开始之前

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

删除卷运行状况阈值的组操作时，全局阈值将应用于该组中的存储对象。在存储对象上设置的任何对象级别运行状况阈值均不受影响。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组操作 * 选项卡中，选择要删除的组操作，然后单击 * 删除 *。
3. 在 * 警告 * 对话框中，单击 * 是 * 确认删除。

重新排列组操作

您可以更改要应用于组中存储对象的组操作的顺序。组操作会根据存储对象的排名按顺序应用于这些对象。最低排名将分配给您上次配置的组操作。您可以根据需要更改组操作的排名。

开始之前

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

您可以选择一行或多行，然后执行多个拖放操作来更改组操作的排名。但是，您必须保存所做的更改，才能在组操作网格中反映重新划分优先级的情况。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 组 *。
2. 在 * 组操作 * 选项卡中，单击 * 重新排序 *。
3. 在 * 重新排列组操作 * 对话框中，拖放行以根据需要重新排列组操作的顺序。
4. 单击 * 保存 *。

使用标注确定存储对象事件的优先级

您可以创建标注规则并将其应用于存储对象，以便根据应用的标注类型及其优先级来标识和筛选这些对象。

了解有关标注的更多信息

了解有关标注的概念有助于您管理与环境中存储对象相关的事件。

什么是标注

标注是分配给另一个文本字符串（值）的文本字符串（名称）。每个标注名称 - 值对都可以使用标注规则与存储对象动态关联。将存储对象与预定义的标注关联后，您可以筛选和查看与其相关的事件。您可以将标注应用于集群，卷和 Storage Virtual Machine（SVM）。

每个标注名称可以有多个值；每个名称 - 值对都可以通过规则与存储对象关联。

例如，您可以创建一个名为 `data-center` 的标注，其值为 `"Boston"` 和 `"Canada"`。然后，您可以将标注 `"data-center"` 与值 `"Boston"` 应用于卷 `v1`。如果为卷 `v1` 上标注有 `data-center` 的任何事件生成警报，则生成的电子邮件将指示卷的位置 `"Boston"`，这样您就可以确定问题描述的优先级并解决此问题。

标注规则在 **Unified Manager** 中的工作原理

标注规则是您定义的用于标注存储对象（卷，集群或 Storage Virtual Machine（SVM））的标准。您可以使用条件组或条件来定义标注规则。

- 您必须将标注规则与标注关联。
- 您必须为标注规则关联一个对象类型；一个标注规则只能关联一个对象类型。
- Unified Manager 会在每个监控周期之后，或者在创建，编辑，删除或重新排列规则时从存储对象添加或删除标注。
- 一个标注规则可以具有一个或多个条件组，每个条件组可以具有一个或多个条件。
- 存储对象可以具有多个标注。特定标注的标注规则也可以在规则条件中使用不同的标注来向已标注的对象添加另一个标注。

条件

您可以创建多个条件组，每个条件组可以具有一个或多个条件。您可以在标注的标注规则中应用定义的所有条件组，以便为存储对象添加标注。

条件组中的条件使用逻辑 AND 执行。必须满足条件组中的所有条件。创建或修改标注规则时，系统会创建一个条件，此条件仅应用，选择和标注满足条件组中所有条件的存储对象。如果要缩小要标注的存储对象的范围，可以在一个条件组中使用多个条件。

您可以使用以下操作数和运算符并指定所需值来创建存储对象的条件。

存储对象类型	适用的操作数
Volume	<ul style="list-style-type: none"> • 对象名称 • 所属集群名称 • 所属 SVM 名称 • 标注
SVM	<ul style="list-style-type: none"> • 对象名称 • 所属集群名称 • 标注
集群	<ul style="list-style-type: none"> • 对象名称 • 标注

如果选择标注作为任何存储对象的操作数，则可以使用 "is" 运算符。对于所有其他操作数，您可以选择 "is" 或 "contains" 作为运算符。如果选择 "is" 运算符，则会评估此条件，以确定该操作数值与为选定操作数提供的值是否完全匹配。如果选择 "contains" 运算符，则系统会评估此条件以满足以下条件之一：

- 该操作数值与选定操作数的值完全匹配。
- 操作数值包含为选定操作数提供的值。

包含条件的标注规则示例

对于具有以下两个条件的卷，请考虑使用一个条件组的标注规则：

- 名称包含 "vol"
- SVM 名称为 data_svm

此标注规则会将名称中包含 "vol" 且托管在名称为 data_svm 的 SVM 上的所有卷添加到选定标注和标注类型中。

条件组

条件组使用逻辑或执行，然后应用于存储对象。存储对象必须满足要标注的条件组之一的要求。满足所有条件组条件的存储对象将添加标注。您可以使用条件组来扩大要标注的存储对象的范围。

包含条件组的标注规则示例

假设一个卷具有两个条件组的标注规则；每个组包含以下两个条件：

- 条件组 1
 - 名称包含 "vol"
 - SVM 名称是 data_svm。此条件组会为名称中包含 "vol" 且托管在名称为 "data_svm" 的 SVM 上的所有卷添加标注。
- 条件组 2.

- 名称包含 "`vol` "
- data-priority 的标注值为 "`critical` " 此条件组会为名称中包含 "`vol` " 且使用数据优先级标注值 "`Critical` " 标注的所有卷添加标注。

如果将包含这两个条件组的标注规则应用于存储对象，则会为以下存储对象添加标注：

- 名称中包含 "`vol` " 且托管在名称为 " data_svm " 的 SVM 上的所有卷。
- 名称中包含 "`vol` " 且使用数据优先级标注值 "`Critical` " 进行标注的所有卷。

预定义标注值的问题描述

- 数据优先级 * 是预定义的标注，其值为任务关键型，高和低。通过这些值，您可以根据存储对象所含数据的优先级为其添加标注。您不能编辑或删除预定义的标注值。

- * 数据优先级：任务关键型 *

此标注适用于包含任务关键型数据的存储对象。例如，包含生产应用程序的对象可以视为任务关键型对象。

- * 数据优先级：高 *

此标注适用于包含高优先级数据的存储对象。例如，托管业务应用程序的对象可以视为高优先级对象。

- * 数据优先级：低 *

此标注适用于包含低优先级数据的存储对象。例如，二级存储上的对象，例如备份和镜像目标，可能具有较低的优先级。

动态添加标注

创建自定义标注时，Unified Manager 会使用规则将集群，Storage Virtual Machine (SVM) 和卷与标注动态关联起来。这些规则会自动将标注分配给存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注 * 页面中，单击 * 添加标注 *。
3. 在 * 添加标注 * 对话框中，键入标注的名称和问题描述。
4. 可选：在 * 标注值 * 部分中，单击 * 添加 * 向标注添加值。
5. 单击 * 保存 *。

将值添加到标注

您可以向标注添加值，然后将存储对象与特定标注名称 - 值对关联起来。将值添加到标注

有助于更有效地管理存储对象。

开始之前

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

您不能向预定义标注添加值。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注 * 页面中，选择要添加值的标注，然后在 * 值 * 部分中单击 * 添加 *。
3. 在 * 添加标注值 * 对话框中，为标注指定一个值。

您指定的值对于选定标注必须是唯一的。

4. 单击 * 添加 *。

删除标注

您可以删除不再需要的自定义标注及其值。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 标注值不得用于其他标注或组规则。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注 * 选项卡中，选择要删除的标注。

此时将显示选定标注的详细信息。

3. 单击 * 操作 * > * 删除 * 以删除选定标注及其值。
4. 在警告对话框中，单击 * 是 * 确认删除。

查看标注列表和详细信息

您可以查看与集群，卷和 Storage Virtual Machine (SVM) 动态关联的标注列表。您还可以查看详细信息，例如问题描述，创建者，创建日期，值，规则，以及与标注关联的对象。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注 * 选项卡中，单击标注名称以查看关联的详细信息。

从标注中删除值

如果与自定义标注关联的值不再对标注进行适用场景，则可以删除该值。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 标注值不得与任何标注规则或组规则关联。

关于此任务

您不能从预定义标注中删除值。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注 * 选项卡的标注列表中，选择要从中删除值的标注。
3. 在 * 标注 * 选项卡的 * 值 * 区域中，选择要删除的值，然后单击 * 删除 *。
4. 在 * 警告 * 对话框中，单击 * 是 *。

此值将被删除，并且不再显示在选定标注的值列表中。

正在创建标注规则

您可以创建 Unified Manager 用于动态标注存储对象（例如卷，集群或 Storage Virtual Machine（SVM））的标注规则。

开始之前

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

创建标注规则后，系统会立即为当前受监控的存储对象添加标注。只有在监控周期完成后，才会为新对象添加标注。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注规则 * 选项卡中，单击 * 添加 *。
3. 在 * 添加标注规则 * 对话框中，指定标注规则的名称。

4. 在 * 目标对象类型 * 字段中，选择要标注的存储对象类型。
5. 在 * 应用标注 * 字段中，选择要使用的标注和标注值。
6. 在*条件*部分中、执行相应的操作以创建条件、条件组或同时创建这两者：

要创建 ...	执行此操作 ...
条件	<ol style="list-style-type: none"> 1. 从操作数列表选择一个操作数。 2. 选择 * 包含 * 或 * 是 * 作为运算符。 3. 输入一个值，或者从可用列表选择一个值。
条件组	<ol style="list-style-type: none"> 1. 单击 * 添加条件组 * 。 2. 从操作数列表选择一个操作数。 3. 选择 * 包含 * 或 * 是 * 作为运算符。 4. 输入一个值，或者从可用列表选择一个值。 5. 如果需要，单击 * 添加条件 * 以创建更多条件，然后对每个条件重复步骤 a 到 d 。

1. 单击 * 添加 * 。

创建标注规则的示例

在添加标注规则对话框中执行以下步骤以创建标注规则，包括配置条件和添加条件组：

1. 指定标注规则的名称。
2. 选择目标对象类型作为 Storage Virtual Machine （ SVM ） 。
3. 从标注列表选择一个标注，然后指定一个值。
4. 在条件部分中，选择 * 对象名称 * 作为操作数。
5. 选择 * 包含 * 作为操作符。
6. 将值输入为 `svm_data`。
7. 单击 * 添加条件组 * 。
8. 选择 * 对象名称 * 作为操作数。
9. 选择 * 包含 * 作为操作符。
10. 将值输入为 `vol`。
11. 单击 * 添加条件 * 。
12. 重复步骤 8 到 10 ， 方法是在步骤 8 中选择 * data-priority * 作为操作数，在步骤 9 中选择 * is-* 作为操作符，在步骤 10 中选择 * 任务关键型 * 作为值。
13. 单击 * 添加 * 。

手动向单个存储对象添加标注

您可以手动为选定卷，集群和 SVM 添加标注，而无需使用标注规则。您可以为一个或多个存储对象添加标注，并为标注指定所需的名称 - 值对组合。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 导航到要标注的存储对象：

要添加标注的对象	执行此操作 ...
集群	<ol style="list-style-type: none">1. 单击 * 存储 * > * 集群 * 。2. 选择一个或多个集群。
Volumes	<ol style="list-style-type: none">1. 单击 * 存储 * > * 卷 * 。2. 选择一个或多个卷。
svms	<ol style="list-style-type: none">1. 单击 * 存储 * > * SVMs * 。2. 选择一个或多个 SVM 。

1. 单击 * 标注 * 并选择一个名称 - 值对。
2. 单击 * 应用 * 。

编辑标注规则

您可以编辑标注规则来修改条件组中的条件组和条件，以便在存储对象中添加标注或删除标注。

开始之前

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

编辑关联的标注规则时，标注将与存储对象解除关联。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 * 。
2. 在 * 标注规则 * 选项卡中，选择要编辑的标注规则，然后单击 * 操作 * > * 编辑 * 。
3. 在 * 编辑标注规则 * 对话框中，根据需要更改规则名称，标注名称和值，条件组和条件。

您不能更改标注规则的目标对象类型。

4. 单击 * 保存 *。

配置标注规则的条件

您可以配置一个或多个条件以创建 Unified Manager 应用于存储对象的标注规则。满足标注规则的存储对象将使用规则中指定的值进行标注。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注规则 * 选项卡中，单击 * 添加 *。
3. 在 * 添加标注规则 * 对话框中，输入规则的名称。
4. 从目标对象类型列表中选择对象类型，然后从列表中选择标注名称和值。
5. 在对话框的 * 条件 * 部分中，从列表选择一个操作数和一个运算符，然后输入条件值，或者单击 * 添加条件 * 以创建新条件。
6. 单击 * 保存并添加 *。

配置标注规则条件的示例

请考虑对象类型 SVM 的条件，其中对象名称包含 `svm_data`。

在添加标注规则对话框中执行以下步骤以配置条件：

1. 输入标注规则的名称。
2. 选择目标对象类型 SVM。
3. 从标注列表选择一个标注和一个值。
4. 在 * 条件 * 字段中，选择 * 对象名称 * 作为操作数。
5. 选择 * 包含 * 作为操作符。
6. 将值输入为 `svm_data`。
7. 单击 * 添加 *。

正在删除标注规则

当不再需要标注规则时，您可以从 Active IQ Unified Manager 中删除这些规则。

开始之前

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

删除标注规则时，该标注将解除关联并从存储对象中删除。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注规则 * 选项卡中，选择要删除的标注规则，然后单击 * 删除 *。
3. 在 * 警告 * 对话框中，单击 * 是 * 确认删除。

重新排列标注规则

您可以更改 Unified Manager 将标注规则应用于存储对象的顺序。标注规则会根据存储对象的排名按顺序应用于这些对象。配置标注规则时，排名最低。但是，您可以根据需要更改标注规则的排名。

开始之前

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

您可以选择一行或多行，并执行多个拖放操作来更改标注规则的排名。但是，您必须保存所做的更改，重新排列优先级才能显示在标注规则选项卡中。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 标注 *。
2. 在 * 标注规则 * 选项卡中，单击 * 重新排序 *。
3. 在 * 重新排列标注规则 * 对话框中，拖放单行或多行以重新排列标注规则的顺序。
4. 单击 * 保存 *。

您必须保存所做的更改，才能显示重新排序。

管理 SAML 身份验证设置

配置远程身份验证设置后，您可以启用安全断言标记语言（ Security Assertion Markup Language ， SAML ）身份验证，以便远程用户先通过安全身份提供程序（ IdP ）进行身份验证，然后才能访问 Unified Manager Web UI 。

请注意，启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI 。此配置不会影响访问维护控制台的用户。

身份提供程序要求

在将 Unified Manager 配置为使用身份提供程序（ Identity Provider ， IdP ）对所有远程

用户执行 SAML 身份验证时，您需要了解一些必需的配置设置，以便成功连接到 Unified Manager 。

您必须在 IdP 服务器中输入 Unified Manager URI 和元数据。您可以从 Unified Manager SAML 身份验证页面复制此信息。在安全断言标记语言（SAML）标准中，Unified Manager 被视为服务提供商（Service Provider，SP）。

支持的加密标准

- 高级加密标准（AES）：AES-128 和 AES-256
- 安全哈希算法（Secure Hash Algorithm，SHA）：SHA-1 和 SHA-256

经过验证的身份提供程序

- Shibboleth
- Active Directory 联合身份验证服务（ADFS）

ADFS 配置要求

- 您必须按以下顺序定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。

声明规则	价值
sam 帐户名称	名称 ID
sam 帐户名称	urn : OID : 0.9.2342.19200300.100.1.1
令牌组—非限定名称	urn : OID : 1.3.6.1.4.1.5923.1.5.1.1

- 您必须将身份验证方法设置为 "Forms Authentication"，否则用户可能会在注销 Unified Manager 时收到错误。请按照以下步骤操作：
 - a. 打开 ADFS 管理控制台。
 - b. 单击左侧树视图中的身份验证策略文件夹。
 - c. 在右侧的 "Actions" 下，单击 Edit Global Primary Authentication Policy。
 - d. 将 "Intranet Authentication Method"（内部网身份验证方法）设置为 "Forms Authentication"，而不是默认值 "Windows Authentication"。
- 在某些情况下，如果 Unified Manager 安全证书是 CA 签名的，则通过 IdP 登录将被拒绝。要解决此问题描述，可以使用两种解决方法：
 - 按照链接中的说明在 ADFS 服务器上禁用对链接的 CA 证书关联依赖方进行的撤消检查：

"禁用每个依赖方信任的撤消检查"

- 将 CA 服务器驻留在 ADFS 服务器中，以便对 Unified Manager 服务器证书请求进行签名。

其他配置要求

- Unified Manager 时钟偏差设置为 5 分钟，因此 IdP 服务器和 Unified Manager 服务器之间的时间差不能超过 5 分钟，否则身份验证将失败。

启用 SAML 身份验证

您可以启用安全断言标记语言（SAML）身份验证，以便远程用户在访问 Unified Manager Web UI 之前先通过安全身份提供程序（IdP）进行身份验证。

开始之前

- 您必须已配置远程身份验证并验证它是否成功。
- 您必须已至少创建一个具有应用程序管理员角色的远程用户或远程组。
- Unified Manager 必须支持身份提供程序（IdP），并且必须对其进行配置。
- 您必须具有 IdP URL 和元数据。
- 您必须有权访问 IdP 服务器。

关于此任务

从 Unified Manager 启用 SAML 身份验证后，只有在为 IdP 配置了 Unified Manager 服务器主机信息之后，用户才能访问图形用户界面。因此，在开始配置过程之前，您必须准备好完成连接的两个部分。可以在配置 Unified Manager 之前或之后配置 IdP。

启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI。此配置不会影响访问维护控制台，Unified Manager 命令或 ZAPI 的用户。



在此页面上完成 SAML 配置后，Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 *。

2. 选中 * 启用 SAML 身份验证 * 复选框。

此时将显示配置 IdP 连接所需的字段。

3. 输入将 Unified Manager 服务器连接到 IdP 服务器所需的 IdP URI 和 IdP 元数据。

如果可以直接从 Unified Manager 服务器访问 IdP 服务器，则可以在输入 IdP URI 后单击 * 提取 IdP 元数据 * 按钮以自动填充 IdP 元数据字段。

4. 复制 Unified Manager 主机元数据 URI，或者将主机元数据保存到 XML 文本文件中。

此时，您可以使用此信息配置 IdP 服务器。

5. 单击 * 保存 *。

此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager。

6. 单击 * 确认并注销 * ， Unified Manager 将重新启动。

结果

授权远程用户下次尝试访问 Unified Manager 图形界面时，他们将在 IdP 登录页面而不是 Unified Manager 登录页面中输入凭据。

完成后

如果尚未完成，请访问 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。



使用 ADFS 作为身份提供程序时，Unified Manager 图形用户界面不会遵守 ADFS 超时要求，它将继续工作，直到达到 Unified Manager 会话超时为止。您可以通过单击 * 常规 * > * 功能设置 * > * 非活动超时 * 来更改 GUI 会话超时。

更改用于 SAML 身份验证的身份提供程序

您可以更改 Unified Manager 用于对远程用户进行身份验证的身份提供程序（IdP）。

开始之前

- 您必须具有 IdP URL 和元数据。
- 您必须有权访问 IdP 。

关于此任务

可以在配置 Unified Manager 之前或之后配置新的 IdP 。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 * 。
2. 输入将 Unified Manager 服务器连接到 IdP 所需的新 IdP URI 和 IdP 元数据。

如果 IdP 可直接从 Unified Manager 服务器访问，则在输入 IdP URL 后，您可以单击 * 提取 IdP 元数据 * 按钮以自动填充 IdP 元数据字段。

3. 复制 Unified Manager 元数据 URI ，或将元数据保存到 XML 文本文件。
4. 单击 * 保存配置 * 。

此时将显示一个消息框，确认您要更改配置。

5. 单击 * 确定 * 。

完成后

访问新 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

授权远程用户下次尝试访问 Unified Manager 图形界面时，他们将在新的 IdP 登录页面中输入凭据，而不是在旧的 IdP 登录页面中输入凭据。

更改 Unified Manager 安全证书后更新 SAML 身份验证设置

对 Unified Manager 服务器上安装的 HTTPS 安全证书进行任何更改都需要更新 SAML 身份验证配置设置。如果您重命名主机系统，为主机系统分配新的 IP 地址或手动更改系统的安全证书，则此证书将更新。

关于此任务

更改安全证书并重新启动 Unified Manager 服务器后，SAML 身份验证将无法正常运行，用户将无法访问 Unified Manager 图形界面。您必须同时更新 IdP 服务器和 Unified Manager 服务器上的 SAML 身份验证设置，才能重新启用对用户界面的访问。

步骤

1. 登录到维护控制台。
2. 在 * 主菜单 * 中，输入 * 禁用 SAML 身份验证 * 选项的编号。

此时将显示一条消息，确认您要禁用 SAML 身份验证并重新启动 Unified Manager 。

3. 使用更新后的 FQDN 或 IP 地址启动 Unified Manager 用户界面，接受更新后的服务器证书并使用维护用户凭据登录。
4. 在 * 设置 / 身份验证 * 页面中，选择 * SAML 身份验证 * 选项卡并配置 IdP 连接。
5. 复制 Unified Manager 主机元数据 URI ，或者将主机元数据保存到 XML 文本文件中。
6. 单击 * 保存 * 。

此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager 。

7. 单击 * 确认并注销 * ， Unified Manager 将重新启动。
8. 访问 IdP 服务器并输入 Unified Manager 服务器 URI 和元数据以完成配置。

身份提供程序	配置步骤
ADFS	<ol style="list-style-type: none">1. 在 ADFS 管理 GUI 中删除现有的依赖方信任条目。2. 使用添加新的依赖方信任条目 <code>saml_sp_metadata.xml</code> 从更新后的 Unified Manager 服务器。3. 定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。4. 重新启动 ADFS Windows 服务。
Shibboleth	<ol style="list-style-type: none">1. 将 Unified Manager 服务器的新 FQDN 更新到 <code>attribute-filter.xml</code> 和 <code>relying-party.xml</code> 文件。2. 重新启动 Apache Tomcat Web 服务器并等待端口 8005 联机。

1. 登录到 Unified Manager 并验证 SAML 身份验证是否可通过 IdP 按预期工作。

禁用 SAML 身份验证

如果要在远程用户登录到 Unified Manager Web UI 之前停止通过安全身份提供程序（IdP）进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证后，配置的目录服务提供程序（例如 Active Directory 或 LDAP）将执行登录身份验证。

关于此任务

禁用 SAML 身份验证后，除了配置的远程用户之外，本地用户和维护用户还可以访问图形用户界面。

如果您无法访问图形用户界面，也可以使用 Unified Manager 维护控制台禁用 SAML 身份验证。



禁用 SAML 身份验证后，Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 *。
2. 取消选中 * 启用 SAML 身份验证 * 复选框。
3. 单击 * 保存 *。

此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager。

4. 单击 * 确认并注销 *，Unified Manager 将重新启动。

结果

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入凭据。

完成后

访问 IdP 并删除 Unified Manager 服务器 URI 和元数据。

从维护控制台禁用 SAML 身份验证

如果无法访问 Unified Manager 图形用户界面，则可能需要从维护控制台禁用 SAML 身份验证。如果配置不当或 IdP 不可访问，则可能会发生这种情况。

开始之前

您必须以维护用户身份访问维护控制台。

关于此任务

禁用 SAML 身份验证后，配置的目录服务提供程序（例如 Active Directory 或 LDAP）将执行登录身份验证。除了配置的远程用户之外，本地用户和维护用户还可以访问图形用户界面。

您还可以从 UI 的设置 / 身份验证页面禁用 SAML 身份验证。



禁用 SAML 身份验证后，Unified Manager 将自动重新启动。

步骤

1. 登录到维护控制台。
2. 在 * 主菜单 * 中，输入 * 禁用 SAML 身份验证 * 选项的编号。

此时将显示一条消息，确认您要禁用 SAML 身份验证并重新启动 Unified Manager 。

3. 键入 * 。 y* ，然后按 Enter 键， Unified Manager 将重新启动。

结果

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入凭据。

完成后

如果需要，请访问 IdP 并删除 Unified Manager 服务器 URL 和元数据。

通过 Web UI 和维护控制台发送支持包

如果您所拥有的问题描述需要比 AutoSupport 消息提供的诊断和故障排除更详细的信息，则应发送支持包。您可以使用 Unified Manager Web UI 和维护控制台向技术支持发送支持包。

关于此任务

Unified Manager 一次最多可存储两个完整支持包和三个轻型支持包。

将 **AutoSupport** 消息和支持包发送给技术支持

通过 AutoSupport 页面，您可以向技术支持团队发送预定义的按需 AutoSupport 消息，以确保环境正常运行，并帮助您维护环境的完整性。默认情况下，AutoSupport 处于启用状态，不应将其禁用，这样您才能获得 NetAppActive IQ 的优势。

您可以根据需要在消息中发送有关 Unified Manager 服务器的诊断系统信息和详细数据，计划定期发送消息，甚至生成支持包并将其发送给技术支持团队。



具有存储管理员角色的用户可以生成按需 AutoSupport 消息和支持包并将其发送给技术支持。但是、只有管理员或维护用户才能启用或禁用定期 AutoSupport 以及配置 HTTP 设置、如中所述 [设置 HTTP 代理服务器](#)。在需要使用 HTTP 代理服务器的环境中，存储管理员应先完成配置，然后才能将按需 AutoSupport 消息和支持包发送给技术支持。

发送按需 **AutoSupport** 消息

您可以生成按需消息并将其发送给技术支持，指定的电子邮件收件人或两者。

1. 导航到 * 常规 * > * AutoSupport * ，然后执行以下一项或两项操作：
2. 如果要将 AutoSupport 消息发送给技术支持，请选中 * 发送给技术支持 * 复选框。
3. 如果要将 AutoSupport 消息发送到特定电子邮件收件人，请选中 * 发送到电子邮件收件人 * 复选框，然后输入收件人的电子邮件地址。
4. 单击 * 保存 * 。
5. 单击 * 生成并发送 AutoSupport * 。

启用定期 **AutoSupport**

您可以定期向技术支持发送特定的预定义消息，以进行问题描述诊断和解决。默认情况下，此功能处于启用状态。如果禁用，则管理员或维护用户可以启用这些设置。

1. 导航到 * 常规 * > * AutoSupport * 。
2. 在定期 AutoSupport 部分中，选中 * 启用定期向 Active IQ 发送 AutoSupport 数据 * 复选框。
3. 如果需要、请按照中所述定义HTTP代理服务器的名称、端口和身份验证信息 [设置 HTTP 代理服务器](#)。
4. 单击 * 保存 * 。

上传按需支持包

您可以根据故障排除要求生成支持包并将其发送给技术支持。Unified Manager 仅存储最近生成的两个支持包。旧的支持包将从系统中删除。

由于某些类型的支持数据可能会占用大量集群资源或需要很长时间才能完成，因此，在选择完整的支持包时，您可以包括或排除特定的数据类型以减小支持包大小。您还可以选择创建一个轻型支持包，该包只包含 30 天的日志和配置数据库记录，它不包括性能数据，采集录制文件和服务器堆转储。

1. 导航到 * 常规 * > * AutoSupport * 。
2. 在按需支持包部分中，单击 * 生成并发送支持包 * 。
3. 要向技术支持发送轻型支持包，请在生成和发送支持包弹出窗口中选中 "*" 生成轻型支持包 "*" 复选框。
4. 或者，要发送完整的支持包，请选中 * 生成完整的支持包 * 复选框。选择要在支持包中包含或排除的特定数据类型。



即使不选择任何数据类型，仍会使用其他 Unified Manager 数据生成支持包。

5. 选中 * 将捆绑包发送给技术支持 * 复选框以生成捆绑包并将其发送给技术支持。如果不选中此复选框，则会在 Unified Manager 服务器本地生成并存储此捆绑包。生成的支持包可供日后在中使用 /support VMware 系统上的目录、在中 /opt/netapp/data/support/ 在Linux系统和在 ProgramData\NetApp\OnCommandAppData\ocum\support 在Windows系统上。
6. 单击 * 发送 * 。

设置 HTTP 代理服务器

如果您的环境不提供从 Unified Manager 服务器直接访问的权限，您可以指定一个代理来提供 Internet 访问，以便向支持部门发送 AutoSupport 内容。此部分仅适用于管理员和维护用户。

• * 使用 HTTP 代理 *

选中此框可标识用作 HTTP 代理的服务器。

输入代理服务器的主机名或 IP 地址，以及用于连接到该服务器的端口号。

• * 使用身份验证 *

如果需要提供身份验证信息来访问用作 HTTP 代理的服务器，请选中此框。

输入向 HTTP 代理进行身份验证所需的用户名和密码。



不支持仅提供基本身份验证的 HTTP 代理。

访问维护控制台

如果 Unified Manager 用户界面未运行，或者您需要执行用户界面中不可用的功能，则可以访问维护控制台来管理 Unified Manager 系统。

开始之前

您必须已安装并配置 Unified Manager 。

关于此任务

处于非活动状态 15 分钟后，维护控制台会将您注销。



安装在 VMware 上后，如果您已通过 VMware 控制台以维护用户身份登录，则无法使用安全 Shell 同时登录。

步骤

1. 按照以下步骤访问维护控制台：

在此操作系统上 ...	请按照以下步骤操作 ...
VMware	<ol style="list-style-type: none">1. 使用安全 Shell 连接到 Unified Manager 虚拟设备的 IP 地址或完全限定域名。2. 使用您的维护用户名和密码登录到维护控制台。

在此操作系统上 ...	请按照以下步骤操作 ...
Linux	<ol style="list-style-type: none"> 1. 使用安全 Shell 连接到 Unified Manager 系统的 IP 地址或完全限定域名。 2. 使用维护用户（umadmin）名称和密码登录到系统。 3. 输入命令 ... maintenance_console 然后按Enter键。
Windows	<ol style="list-style-type: none"> 1. 使用管理员凭据登录到 Unified Manager 系统。 2. 以 Windows 管理员身份启动 PowerShell 。 3. 输入命令 ... maintenance_console 然后按Enter键。

此时将显示 Unified Manager 维护控制台菜单。

生成并上传支持包

您可以生成包含诊断信息的支持包，以便将其发送给技术支持以获取故障排除帮助。从 Unified Manager 9.8 开始，如果 Unified Manager 服务器已连接到 Internet，您还可以从维护控制台将支持包上传到 NetApp 。

开始之前

您必须以维护用户身份访问维护控制台。

关于此任务

由于某些类型的支持数据可能会占用大量集群资源或需要很长时间才能完成，因此，在选择完整支持包时，您可以指定要包含或排除的数据类型以减小支持包大小。您还可以选择创建一个轻型支持包，该包只包含 30 天的日志和配置数据库记录，它不包括性能数据，采集录制文件和服务器堆转储。

Unified Manager 仅存储最近生成的两个支持包。旧的支持包将从系统中删除。

步骤

1. 在维护控制台 * 主菜单 * 中，选择 * 支持 / 诊断 * 。
2. 根据您希望在支持包中具有的信息详细级别，选择 * 生成轻型支持包 * 或 * 生成支持包 * 。
3. 如果选择完整的支持包，请选择或取消选择要在支持包中包含或排除的以下数据类型：
 - * 数据库转储 *

MySQL Server 数据库的转储。

- * 堆转储 *

主要 Unified Manager 服务器进程状态的快照。默认情况下，此选项处于禁用状态，只有在客户支持请

求时才应选择此选项。

◦ * 采集记录 *

记录 Unified Manager 与受监控集群之间的所有通信。



如果取消选择所有数据类型，则仍会使用其他 Unified Manager 数据生成支持包。

4. Type g、然后按Enter生成支持包。

由于生成支持包是一项内存密集型操作，因此系统会提示您确认此时确实要生成支持包。

5. Type y、然后按Enter生成支持包。

如果此时不想生成支持包、请键入 n、然后按Enter键。

6. 如果完整支持包中包含数据库转储文件，则系统会提示您指定希望包含性能统计信息的时间段。包括性能统计信息可能需要大量时间和空间，因此您也可以在不包含性能统计信息的情况下转储数据库：

a. 以 YYMMDD 格式输入开始日期。

例如、输入 20210101 适用于2021年1月1日。输入 ... n 如果不希望包括性能统计信息。

b. 输入要包括的统计信息天数，从上午 12 点开始指定的开始日期。

您可以输入 1 到 10 之间的数字。

如果要包括性能统计信息，则系统将显示收集性能统计信息的时间段。

7. 创建支持包后，系统会提示您是否要将其上传到 NetApp 。 Type y、然后按Enter键。

系统将提示您输入支持案例编号。

8. 如果您已有案例编号，请输入此编号并按 Enter 键。否则，只需按 Enter 即可。

支持包将上传到 NetApp 。

完成后

如果 Unified Manager 服务器未连接到 Internet ，或者由于任何其他原因无法上传支持包，则可以手动检索并发送。您可以使用 SFTP 客户端或 UNIX 或 Linux 命令行界面命令检索它。在 Windows 安装中，您可以使用远程桌面（RDP）检索支持包。

生成的支持包位于中 /support VMware系统上的目录、在中 /opt/netapp/data/support/ 在Linux系统和
中 ProgramData\NetApp\OnCommandAppData\ocum\support 在Windows系统上。

使用 Windows 客户端检索支持包

如果您是 Windows 用户，则可以下载并安装一个工具，以便从 Unified Manager 服务器检索支持包。您可以将支持包发送给技术支持，以便对问题描述进行更详细的诊断。例如，

可以使用 FileZilla 或 WinSCP 工具。

开始之前

您必须是维护用户才能执行此任务。

您必须使用支持 SCP 或 SFTP 的工具。

步骤

1. 下载并安装用于检索支持包的工具。
2. 打开工具。
3. 通过 SFTP 连接到 Unified Manager 管理服务器。

该工具将显示的内容 /support 目录、您可以查看所有现有支持包。

4. 选择要复制的支持包的目标目录。
5. 选择要复制的支持包，然后使用工具将文件从 Unified Manager 服务器复制到本地系统。
 - 相关信息 *

"Filezilla - <https://filezilla-project.org/>"

"WinSCP - <http://winscp.net>"

使用 UNIX 或 Linux 客户端检索支持包

如果您是 UNIX 或 Linux 用户，则可以使用 Linux 客户端服务器上的命令行界面（CLI）从 vApp 检索支持包。您可以使用 SCP 或 SFTP 检索支持包。

开始之前

您必须是维护用户才能执行此任务。

您必须已使用维护控制台生成支持包并具有可用的支持包名称。

步骤

1. 使用 Linux 客户端服务器通过 Telnet 或控制台访问 CLI。
2. 访问 /support 目录。
3. 使用以下命令检索支持包并将其复制到本地目录：

如果您使用的是 ...	然后使用以下命令 ...
SCP	<pre>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></pre>

如果您使用的是 ...	然后使用以下命令 ...
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

使用维护控制台生成支持包时，系统会为您提供支持包的名称。

1. 输入维护用户密码。

示例

以下示例使用 SCP 检索支持包：

```
$ scp admin@10.10.12.69:/support/support_bundle_20160216_145359.7z
.
Password: <maintenance_user_password>
support_bundle_20160216_145359.7z 100% 119MB 11.9MB/s 00:10
```

以下示例使用 SFTP 检索支持包：

```
$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .
Password: <maintenance_user_password>
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

向技术支持发送支持包

如果问题描述需要比 AutoSupport 消息提供的诊断和故障排除信息更详细，您可以向技术支持发送支持包。

开始之前

您必须有权访问支持包，才能将其发送给技术支持。

您必须已通过技术支持网站生成案例编号。

步骤

1. 登录到 NetApp 支持站点。
2. 上传文件。

与多个工作流相关的任务和信息

Unified Manager 中的许多工作流都使用一些可帮助您了解和完成工作流的任务和参考文本，其中包括添加和查看有关事件的注释，分配事件，确认和解决事件以及有关卷，Storage Virtual Machine（SVM），聚合的详细信息，等等。

添加和查看有关事件的注释

在处理事件时、您可以使用事件详细信息页面中的"注释和更新"区域添加有关如何处理问题描述的信息。此信息可以使分配了此事件的另一个用户能够处理此事件。您还可以根据最近的时间戳查看上次处理事件的用户添加的信息。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 事件 *。
2. 在*事件管理*清单页面中、单击要添加事件相关信息的事件。
3. 在*事件*详细信息页面的*备注和更新*区域中添加所需信息。
4. 单击*发布*。

将事件分配给特定用户

您可以将未分配的事件分配给自己或其他用户，包括远程用户。如果需要，您可以将分配的事件重新分配给其他用户。例如，当存储对象经常出现问题时，您可以将这些问题的事件分配给管理该对象的用户。

开始之前

- 必须正确配置用户的名称和电子邮件 ID。
- 您必须具有操作员，应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。
2. 在 * 事件管理 * 清单页面中，选择要分配的一个或多个事件。
3. 选择以下选项之一来分配事件：

要将事件分配给 ...	然后执行此操作 ...
您自己	单击 * 分配给 * > * 我 *。
其他用户	<ol style="list-style-type: none"> 单击 * 分配给 * > * 其他用户 *。 在分配所有者对话框中，输入用户名或从下拉列表中选择用户。 单击 * 分配 *。 <p>系统会向用户发送电子邮件通知。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  如果未输入用户名或从下拉列表中选择用户，然后单击 * 分配 *，则事件将保持未分配状态。 </div>

确认并解决事件

在开始处理生成事件的问题描述之前，您应确认某个事件，这样您就不会继续收到重复的警报通知。对特定事件采取更正操作后，应将此事件标记为已解决。

开始之前

您必须具有操作员，应用程序管理员或存储管理员角色。

关于此任务

您可以同时确认和解决多个事件。



您无法确认信息事件。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 *。
2. 从事件列表中，执行以下操作以确认事件：

如果您要 ...	执行此操作 ...
确认一个事件并将其标记为已解决	<ol style="list-style-type: none"> 1. 单击事件名称。 2. 在事件详细信息页面中，确定事件的发生原因。 3. 单击 * 确认 *。 4. 采取适当的更正操作。 5. 单击 * 标记为已解决 *。

如果您要 ...	执行此操作 ...
确认多个事件并将其标记为已解决	<ol style="list-style-type: none"> 1. 从相应的事件详细信息页面确定事件的发生原因。 2. 选择事件。 3. 单击 * 确认 *。 4. 采取适当的更正操作。 5. 单击 * 标记为已解决 *。

将事件标记为已解决后，此事件将移至已解决事件列表。

1. 在*备注和更新*区域中、添加有关如何处理此事件的注释、然后单击*发布*。

事件详细信息页面

在事件详细信息页面中，您可以查看选定事件的详细信息，例如事件严重性，影响级别，影响区域和事件源。此外，您还可以查看追加信息，了解可通过哪些修复方法来解析问题描述。

- * 事件名称 *

事件的名称以及上次查看事件的时间。

对于非性能事件，当事件处于 " 新增 " 或 " 已确认 " 状态时，上次看到的信息未知，因此会隐藏。

- * 事件问题描述 *

事件的简短问题描述。

在某些情况下，事件问题描述会提供触发事件的原因。

- * 争用组件 *

对于动态性能事件，此部分显示的图标表示集群的逻辑组件和物理组件。如果某个组件处于争用状态，则其图标会圈出并以红色突出显示。

请参见 [集群组件及其可能发生争用的原因](#) 此处显示的组件的问题描述。

" 事件信息 " ， " 系统诊断 " 和 " 建议的操作 " 部分将在其他主题中进行介绍。

命令按钮

命令按钮可用于执行以下任务：

- * 注释图标 *

用于添加或更新有关事件的注释，并查看其他用户留下的所有注释。

- 操作菜单 *

- * 分配给我 *

将事件分配给您。

- * 分配给他人 *

打开分配所有者对话框，在此可以将事件分配或重新分配给其他用户。

将事件分配给用户时，系统会将用户的名称以及事件分配时间添加到选定事件的事件列表中。

您也可以通过将所有权字段留空来取消分配事件。

- * 确认 *

确认选定事件，以使您不再收到重复的警报通知。

确认事件后，您的用户名以及确认事件的时间将添加到选定事件的事件列表（确认者）中。确认事件后，您将负责管理该事件。

- * 标记为已解决 *

用于将事件状态更改为已解决。

解决某个事件时，系统会将您的用户名和事件解决时间添加到选定事件的事件列表（解决者）中。对事件采取更正操作后，必须将事件标记为已解决。

- * 添加警报 *

显示添加警报对话框，在此可以为选定事件添加警报。

Event Information 部分显示的内容

您可以使用事件详细信息页面上的事件信息部分查看有关选定事件的详细信息，例如事件严重性，影响级别，影响区域和事件源。

不适用于事件类型的字段将被隐藏。您可以查看以下事件详细信息：

- * 事件触发时间 *

生成事件的时间。

- * 状态 *

事件状态："新增"，"已确认"，"已解决"或"已废弃"。

- * 已废弃发生原因 *

导致事件废弃的操作，例如，问题描述已修复。

- * 事件持续时间 *

对于活动（新事件和已确认事件）事件，此时间为检测到事件与上次分析事件之间的时间。对于已废弃的事

件，此时间为检测到事件与解决事件之间的时间。

对于所有性能事件，此字段都将显示，而对于其他事件类型，此字段仅在解决或废弃后显示。

- * 上次查看 *

上次将事件视为活动的日期和时间。

对于性能事件，此值可能比事件触发时间更晚，因为只要事件处于活动状态，此字段就会在每次收集新的性能数据后更新。对于其他类型的事件，如果处于 " 新增 " 或 " 已确认 " 状态，则此内容不会更新，因此此字段将被隐藏。

- * 严重性 *

事件严重性：严重 (❌)，错误 (⚠️)，警告 (⚠️) 和信息 (ℹ️)。

- * 影响级别 *

事件影响级别： " 意外事件 "， " 风险 "， " 事件 " 或 " 升级 "。

- * 影响区域 *

事件影响区域：可用性，容量，性能，保护，配置，或安全性。

- * 源 *

发生事件的对象的名称。

在查看共享 QoS 策略事件的详细信息时，此字段最多会列出占用 IOPS 或 MBps 最多的三个工作负载对象。

您可以单击源名称链接以显示该对象的运行状况或性能详细信息页面。

- * 源标注 *

显示与事件关联的对象的标注名称和值。

只有集群， SVM 和卷上的运行状况事件才会显示此字段。

- * 源组 *

显示受影响对象所属的所有组的名称。

只有集群， SVM 和卷上的运行状况事件才会显示此字段。

- * 源类型 *

与事件关联的对象类型（例如 SVM ， 卷或 qtree ）。

- * 在集群 * 上

发生事件的集群的名称。

您可以单击集群名称链接以显示该集群的运行状况或性能详细信息页面。

- * 受影响对象计数 *

受事件影响的对象数。

您可以单击对象链接以显示填充了当前受此事件影响的对象的清单页面。

只有性能事件才会显示此字段。

- * 受影响的卷 *

受此事件影响的卷数。

只有节点或聚合上的性能事件才会显示此字段。

- * 触发的策略 *

发出事件的阈值策略的名称。

您可以将光标悬停在策略名称上方以查看阈值策略的详细信息。对于自适应 QoS 策略，还会显示定义的策略，块大小和分配类型（已分配空间或已用空间）。

只有性能事件才会显示此字段。

- * 规则 ID*

对于 Active IQ 平台事件，这是为生成事件而触发的规则的编号。

- * 确认者 *

确认事件的人员姓名以及事件的确认时间。

- * 解决者 *

解决事件的人员姓名以及事件的解决时间。

- * 已分配给 *

被分配处理事件的人员的姓名。

- * 警报设置 *

此时将显示以下有关警报的信息：

- 如果没有与选定事件关联的警报，则会显示 * 添加警报 * 链接。

您可以通过单击链接打开添加警报对话框。

- 如果有一个与选定事件关联的警报，则会显示警报名称。

您可以通过单击链接打开 " 编辑警报 " 对话框。

- 如果与选定事件关联的警报不止一个，则会显示警报数量。

您可以通过单击链接打开警报设置页面，以查看有关这些警报的更多详细信息。

不会显示已禁用的警报。

- * 上次发送通知 *

发送最新警报通知的日期和时间。

- * 发送者 *

用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- * 上一个脚本运行 *

生成警报时执行的脚本的名称。

系统诊断部分显示的内容

事件详细信息页面的系统诊断部分提供的信息可帮助您诊断可能导致此事件的问题。

此区域仅针对某些事件显示。

某些性能事件提供了与已触发的特定事件相关的图表。通常包括前 10 天的 IOPS 或 MBps 图表和延迟图表。按这种方式排列时，您可以查看事件处于活动状态时哪些存储组件对延迟影响最大或受延迟影响最大。

对于动态性能事件，将显示以下图表：

- 工作负载延迟—显示处于争用状态的组件上受影响最大的工作负载，抢占资源的工作负载或强占资源的工作负载的延迟历史记录。
- 工作负载活动—显示有关争用集群组件的工作负载使用情况的详细信息。
- 资源活动—显示处于争用状态的集群组件的历史性能统计信息。

当某些集群组件处于争用状态时，会显示其他图表。

其他事件可提供系统对存储对象执行的分析类型的简短问题描述。在某些情况下，会有一行或多行；对于已分析的每个组件，一行用于分析多个性能计数器的系统定义的性能策略。在这种情况下，诊断旁边会显示一个绿色或红色图标，指示在该特定诊断中是否找到了问题描述。

建议的操作部分显示的内容

事件详细信息页面的建议操作部分提供了事件的可能原因，并提供了一些操作建议，以便您可以尝试自行解决事件。建议的操作将根据已违反的事件类型或阈值类型进行自定义。

只有某些类型的事件才会显示此区域。

在某些情况下，页面上提供了 * 帮助 * 链接，这些链接会引用追加信息来执行许多建议的操作，包括执行特定操作的说明。某些操作可能涉及使用 Unified Manager，ONTAP System Manager，OnCommand Workflow Automation，ONTAP 命令行界面命令或这些工具的组合。

您应将此处建议的操作视为解决此事件的唯一指导。您为解决此事件而采取的操作应基于您的环境背景。

如果要更详细地分析对象和事件，请单击 * 分析工作负载 * 按钮以显示 " 工作负载分析 " 页面。

Unified Manager 可以对某些事件进行全面诊断并提供单一解决方案。如果可用，则这些解决方法会显示为 * 修复它 * 按钮。单击此按钮可让 Unified Manager 修复导致事件的问题描述。

对于 Active IQ 平台事件，本节可能包含一个 NetApp 知识库文章（如果有）的链接，该文章介绍了问题描述和可能的解决方案。在无法访问外部网络的站点中，知识库文章的 PDF 将在本地打开；PDF 是您手动下载到 Unified Manager 实例的规则文件的一部分。

事件严重性类型的问题描述

每个事件都与一个严重性类型相关联，以帮助您确定需要立即采取更正操作的事件的优先级。

- * 严重 *

发生的问题可能会导致服务中断，如果不立即采取更正操作。

性能严重事件仅从用户定义的阈值发送。

- * 错误 *

事件源仍在执行；但是，需要采取更正操作以避免服务中断。

- * 警告 *

事件源发生了您应注意的情况，或者集群对象的性能计数器超出正常范围，应进行监控以确保其不会达到严重严重性。此严重性的事件不会中断发生原因服务，因此可能不需要立即采取更正操作。

性能警告事件是从用户定义的阈值，系统定义的阈值或动态阈值发送的。

- * 信息 *

发现新对象或执行用户操作时会发生此事件。例如，删除任何存储对象或进行任何配置更改时，将生成严重性类型为 " 信息 " 的事件。

信息事件在检测到配置更改时直接从 ONTAP 发送。

事件影响级别的问题描述

每个事件都与一个影响级别（意外事件，风险，事件或升级）关联，以帮助您确定需要立即采取更正操作的事件的优先级。

- * 意外事件 *

意外事件是指一组事件，可通过发生原因使集群停止向客户端提供数据并用尽数据存储空间。影响级别为 " 意外事件 " 的事件最严重。应立即采取更正操作，以避免服务中断。

- * 风险 *

风险是指一组事件，这些事件可能会通过发生原因使集群停止向客户端提供数据，并用尽用于存储数据的空间。具有影响风险级别的事件可能会导致发生原因服务中断。可能需要采取更正操作。

- * 事件 *

事件是指存储对象及其属性的状态或状态更改。影响级别为 " 事件 " 的事件属于信息性事件，不需要采取更正操作。

- * 升级 *

升级事件是指从 Active IQ 平台报告的特定类型的事件。这些事件确定了需要升级 ONTAP 软件，节点固件或操作系统软件才能解决的问题（针对安全建议）。您可能希望对其中某些问题立即执行更正操作，而其他问题则可以等待您的下一次计划维护。

事件影响区域的问题描述

事件分为六个影响区域（可用性，容量，配置，性能，保护，和安全性）以使您能够集中精力处理您负责的事件类型。

- * 可用性 *

可用性事件用于通知您存储对象是否脱机，协议服务是否关闭，是否发生具有存储故障转移的问题描述或是否发生具有硬件的问题描述。

- * 容量 *

容量事件会通知您聚合，卷，LUN 或命名空间是否接近或已达到大小阈值，或者增长速率对于您的环境而言是否不正常。

- * 配置 *

配置事件用于通知您发现，删除，添加，删除或重命名存储对象。配置事件的影响级别为 " 事件 "，严重性类型为 " 信息 "。

- * 性能 *

性能事件用于通知您集群上的资源，配置或活动状况，这些状况可能会对受监控存储对象上的数据存储输入或检索速度产生不利影响。

- * 保护 *

保护事件用于通知您涉及 SnapMirror 关系的意外事件或风险，目标容量问题，SnapVault 关系问题或保护作业问题。托管二级卷和保护关系的任何 ONTAP 对象（尤其是聚合，卷和 SVM）都会在保护影响区域进行分类。

- * 安全性 *

安全事件会根据中定义的参数通知您 ONTAP 集群，Storage Virtual Machine（SVM）和卷的安全性 "《[适用于 ONTAP 9 的 NetApp 安全加固指南](#)》"。

此外，此区域还包括从 Active IQ 平台报告的升级事件。

集群组件及其可能发生争用的原因

您可以在集群组件发生争用时确定集群性能问题。使用此组件的工作负载的性能下降，其客户端请求响应时间（延迟）增加，从而在 Unified Manager 中触发事件。

处于争用状态的组件无法以最佳性能运行。其性能已下降，而其他集群组件和工作负载（称为 *victims*）的性能可能会增加延迟。要使某个组件摆脱争用状态，您必须减少其工作负载或提高其处理更多工作的能力，以使性能恢复到正常水平。由于 Unified Manager 每五分钟收集并分析一次工作负载性能，因此只有在集群组件持续过度使用时，它才会检测到这种情况。不会检测到在五分钟内持续很短时间的瞬时过度使用峰值。

例如，某个存储聚合可能处于争用状态，因为该聚合上的一个或多个工作负载正在争用它们的 I/O 请求来满足。聚合上的其他工作负载可能会受到影响，从而导致其性能下降。要减少聚合上的活动量，您可以采取不同的步骤，例如将一个或多个工作负载移动到不太繁忙的聚合或节点，以减少当前聚合上的整体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制或将工作负载移动到其他策略组，以使这些工作负载不再受到限制。

Unified Manager 会监控以下集群组件，以便在它们处于争用状态时向您发出警报：

- * 网络 *

表示集群上外部网络协议发出的 I/O 请求的等待时间。等待时间是指集群在响应 I/O 请求之前等待 "transfer ready" 事务完成所花费的时间。如果网络组件处于争用状态，则表示协议层的等待时间较长，正在影响一个或多个工作负载的延迟。

- * 网络处理 *

表示协议层和集群之间的 I/O 处理所涉及的集群软件组件。自检测到事件以来，处理网络处理的节点可能已发生更改。如果网络处理组件处于争用状态，则表示网络处理节点上的高利用率正在影响一个或多个工作负载的延迟。

在主动 - 主动配置中使用全 SAN 阵列集群时，将显示两个节点的网络处理延迟值，以便您可以验证这些节点是否均衡共享负载。

- * QoS 限制最大值 *

表示分配给工作负载的存储服务质量（QoS）策略组的最大吞吐量（峰值）设置。如果策略组组件处于争用状态，则表示策略组中的所有工作负载都受到所设置的吞吐量限制的限制，从而影响一个或多个工作负载的延迟。

- * QoS 限制最小值 *

表示分配给其他工作负载的 QoS 吞吐量最小值（预期）设置所导致的工作负载延迟。如果为某些工作负载设置的 QoS 最小值使用大部分带宽来保证承诺的吞吐量，则其他工作负载将受到限制，并会出现更多延迟。

- * 集群互连 *

表示与集群节点物理连接的缆线和适配器。如果集群互连组件处于争用状态，则表示集群互连中 I/O 请求的等待时间较长，正在影响一个或多个工作负载的延迟。

- * 数据处理 *

表示集群中与工作负载所在的存储聚合之间的 I/O 处理所涉及的集群软件组件。自检测到事件以来，处理数据处理的节点可能已发生更改。如果数据处理组件处于争用状态，则表示数据处理节点上的高利用率正在影响

响一个或多个工作负载的延迟。

- * 卷激活 *

表示跟踪所有活动卷使用情况的过程。在活动卷超过 1000 个的大型环境中，此过程会跟踪需要同时通过节点访问资源的关键卷数量。如果并发活动卷数超过建议的最大阈值，则某些非关键卷将出现此处所述的延迟。

- * MetroCluster 资源 *

表示用于在 MetroCluster 配置中的集群之间镜像数据的 MetroCluster 资源，包括 NVRAM 和交换机间链路（ISL）。如果 MetroCluster 组件处于争用状态，则表示本地集群上的工作负载写入吞吐量较高，或者链路运行状况问题描述正在影响本地集群上一个或多个工作负载的延迟。如果集群不在 MetroCluster 配置中，则不会显示此图标。

- * 聚合或 SSD 聚合操作 *

表示运行工作负载的存储聚合。如果聚合组件处于争用状态，则表示聚合上的高利用率正在影响一个或多个工作负载的延迟。聚合由所有 HDD 组成，或者由 HDD 和 SSD 组成（Flash Pool 聚合），或者由 HDD 和云层组成（FabricPool 聚合）。"SSD 聚合"由所有 SSD（全闪存聚合）组成，或者由 SSD 和云层（FabricPool 聚合）组成。

- * 云延迟 *

表示集群中与存储用户数据的云层之间的 I/O 处理相关的软件组件。如果云延迟组件处于争用状态，则表示从云层上托管的卷进行的大量读取正在影响一个或多个工作负载的延迟。

- * 同步 SnapMirror*

表示在 SnapMirror 同步关系中将用户数据从主卷复制到二级卷所涉及的集群软件组件。如果同步 SnapMirror 组件处于争用状态，则表示 SnapMirror 同步操作的活动正在影响一个或多个工作负载的延迟。

卷 / 运行状况详细信息页面

您可以使用卷 / 运行状况详细信息页面查看有关选定卷的详细信息，例如容量，存储效率，配置，保护，标注和生成的事件。您还可以查看有关该卷的相关对象和相关警报的信息。

您必须具有应用程序管理员或存储管理员角色。

命令按钮

使用命令按钮可以对选定卷执行以下任务：

- * 切换到性能视图 *

用于导航到卷 / 性能详细信息页面。

- * 操作 *

- 添加警报

用于向选定卷添加警报。

- 编辑阈值

用于修改选定卷的阈值设置。

- 标注

用于为选定卷添加标注。

- 保护

用于为选定卷创建 SnapMirror 或 SnapVault 关系。

- 关系

用于执行以下保护关系操作：

- 编辑

启动编辑关系对话框，在此可以更改现有保护关系的现有 SnapMirror 策略，计划和最大传输速率。

- 中止

中止选定关系正在进行的传输。您也可以选择删除基线传输以外的传输的重新启动检查点。您不能删除基线传输的检查点。

- 暂停

暂时禁用选定关系的计划更新。已在进行的传输必须在关系暂停之前完成。

- 中断

中断源卷和目标卷之间的关系，并将目标更改为读写卷。

- 删除

永久删除选定源和目标之间的关系。卷不会销毁，卷上的 Snapshot 副本也不会删除。此操作无法撤销。

- 恢复

为已暂停的关系启用计划传输。在下一个计划传输间隔，如果存在重新启动检查点，则会使用该检查点。

- 重新同步

用于重新同步先前已断开的关系。

- 初始化 / 更新

用于对新保护关系执行首次基线传输，或者在关系已初始化时执行手动更新。

- 反向重新同步

用于重新建立先前已断开的保护关系，通过将源作为原始目标的副本来反转源和目标的功能。源上的内容将被目标上的内容覆盖，比通用 Snapshot 副本上的数据更新的数据将被删除。

- 还原

用于将数据从一个卷还原到另一个卷。



对于处于同步保护关系的卷，"还原"按钮和"关系"操作按钮不可用。

- * 查看卷 *

用于导航到运行状况：所有卷视图。

容量选项卡

容量选项卡可显示有关选定卷的详细信息，例如，卷的物理容量，逻辑容量，阈值设置，配额容量以及任何卷移动操作的信息：

- * 物理容量 *

详细说明卷的物理容量：

- Snapshot 溢出

显示 Snapshot 副本占用的数据空间。

- 已用

显示卷中数据使用的空间。

- 警告

表示卷中的空间接近全满。如果违反此阈值，则会生成空间接近全满事件。

- error

指示卷中的空间已满。如果违反此阈值，则会生成空间已满事件。

- 不可用

表示已生成 "精简配置卷空间存在风险" 事件，而精简配置卷中的空间由于聚合容量问题而存在风险。只有精简配置的卷才会显示不可用容量。

- 数据图

显示卷的总数据容量和已用数据容量。

如果启用了自动增长，则数据图形还会显示聚合中的可用空间。数据图形显示卷中的数据可以使用的有效存储空间，可以是以下空间之一：

- 在以下情况下卷的实际数据容量：
 - 已禁用自动增长。
 - 启用了自动增长的卷已达到最大大小。
 - 启用了自动增长的厚配置卷无法进一步增长。
- 在考虑最大卷大小后卷的数据容量（对于精简配置卷，以及在聚合有空间可使卷达到最大大小时为厚配置卷）
- 在考虑下一个可能的自动增长大小后卷的数据容量（适用于具有自动增长百分比阈值的厚配置卷）
- Snapshot 副本图形

只有在已用 Snapshot 容量或 Snapshot 预留不为零时，才会显示此图形。

如果已用 Snapshot 容量超过 Snapshot 预留，则这两个图形都会显示 Snapshot 容量超过 Snapshot 预留的容量。

• * 容量逻辑 *

显示卷的逻辑空间特征。逻辑空间表示磁盘上存储的数据的实际大小，而不会因使用 ONTAP 存储效率技术而节省空间。

◦ 逻辑空间报告

显示卷是否配置了逻辑空间报告。此值可以是 " 已启用 "，" 已禁用 " 或 " 不适用 "。对于旧版 ONTAP 上的卷或不支持逻辑空间报告的卷，将显示 " 不适用 "。

◦ 已用

显示卷中数据正在使用的逻辑空间量，以及根据总数据容量计算的已用逻辑空间百分比。

◦ 逻辑空间强制实施

显示是否为精简配置卷配置了逻辑空间强制实施。如果设置为 " 已启用 "，则卷的逻辑已用大小不能大于当前设置的物理卷大小。

• * 自动增长 *

显示卷是否在空间不足时自动增长。

• * 空间保证 *

显示卷从聚合中删除可用块时的 FlexVol 卷设置控制。然后，保证这些块可用于写入卷中的文件。空间保证可设置为以下选项之一：

◦ 无

没有为此卷配置空间保证。

◦ 文件

保证稀疏写入的文件（例如 LUN）的完整大小。

- Volume

保证卷的完整大小。

- 部分

FlexCache 卷根据其大小预留空间。如果 FlexCache 卷的大小为 100 MB 或更多，则默认情况下最小空间保证设置为 100 MB。如果 FlexCache 卷的大小小于 100 MB，则最小空间保证设置为 FlexCache 卷的大小。如果 FlexCache 卷的大小稍后增加，则最小空间保证不会递增。



如果卷的类型为 "数据缓存"，则空间保证为 "部分"。

- * 详细信息 (物理) *

显示卷的物理特征。

- * 总容量 *

显示卷中的总物理容量。

- * 数据容量 *

显示卷使用的物理空间量 (已用容量) 以及卷中仍然可用的物理空间量 (可用容量)。这些值还会显示为总物理容量的百分比。

为精简配置卷生成 "精简配置卷空间存在风险" 事件时，将显示卷已用空间量 (已用容量) 以及卷中可用但由于聚合容量问题而无法使用的空间量 (不可用容量)。

- * Snapshot 预留 *

显示 Snapshot 副本使用的空间量 (已用容量) 以及卷中可用于 Snapshot 副本的空间量 (可用容量)。这些值还会以 Snapshot 预留总量的百分比形式显示。

为精简配置卷生成 "精简配置卷空间存在风险" 事件时，Snapshot 副本使用的空间量 (已用容量) 以及卷中可用但无法用于创建 Snapshot 副本的空间量 (不可用容量) 因为显示聚合容量问题。

- * 卷阈值 *

显示以下卷容量阈值：

- 接近全满阈值

指定卷接近全满时的百分比。

- 全满阈值

指定卷已满时的百分比。

- * 其他详细信息 *

- 自动增长最大大小

显示卷可自动增长到的最大大小。默认值为创建时卷大小的 120%。只有在为卷启用了自动增长时，才

会显示此字段。

- qtree 配额已提交容量

显示配额中预留的空间。

- qtree 配额过量提交的容量

显示系统生成卷 qtree 配额过量提交事件之前可使用的空间量。

- 预留百分比

控制覆盖预留的大小。默认情况下，预留百分比设置为 100，表示预留了所需预留空间的 100%，以便完全保护对象，防止覆盖。如果预留百分比小于 100%，则该卷中所有预留空间文件的预留空间将减少为预留百分比。

- Snapshot 每日增长率

显示选定卷中 Snapshot 副本每 24 小时发生的更改（以百分比或 KB，MB，GB 等单位）。

- 快照达到全满的天数

显示在卷中为 Snapshot 副本预留的空间达到指定阈值之前预计剩余的天数。

如果卷中 Snapshot 副本的增长率为零或负，或者没有足够的数据来计算增长率，则 Snapshot 达到全满天数字段将显示不适用的值。

- Snapshot 自动删除

指定在对卷的写入因聚合中空间不足而失败时是否自动删除 Snapshot 副本以释放空间。

- Snapshot 副本

显示有关卷中 Snapshot 副本的信息。

卷中 Snapshot 副本的数量显示为一个链接。单击此链接将打开卷上的 Snapshot 副本对话框，其中显示了 Snapshot 副本的详细信息。

Snapshot 副本计数大约每小时更新一次；但是，Snapshot 副本列表将在您单击该图标时更新。这可能会导致拓扑中显示的 Snapshot 副本计数与单击此图标时列出的 Snapshot 副本数量有所不同。

- * 卷移动 *

显示当前或最后对卷执行的卷移动操作的状态以及其他详细信息，例如正在进行的卷移动操作的当前阶段，源聚合，目标聚合，开始时间，结束时间，和估计结束时间。

还显示对选定卷执行的卷移动操作的数量。您可以单击 * 卷移动历史记录 * 链接来查看有关卷移动操作的详细信息。

配置选项卡

配置选项卡可显示有关选定卷的详细信息，例如卷的导出策略，RAID 类型，容量和存储效率相关功能：

• * 概述 *

◦ 全名

显示卷的全名。

◦ 聚合

显示卷所在聚合的名称或 FlexGroup 卷所在聚合的数量。

◦ Tiering policy

显示为卷设置的分层策略；如果卷部署在启用了 FabricPool 的聚合上。此策略可以是 "无"，"仅 Snapshot"，"备份"，"自动" 或 "全部"。

◦ 存储 VM

显示包含卷的 SVM 的名称。

◦ Junction path

显示路径的状态，可以是活动路径或非活动路径。此外，还会显示 SVM 中卷挂载到的路径。您可以单击 * 历史记录 * 链接以查看最近对接合路径所做的五项更改。

◦ 导出策略

显示为卷创建的导出策略的名称。您可以单击此链接来查看有关在属于 SVM 的卷上启用的导出策略，身份验证协议和访问的详细信息。

◦ 模式

显示卷模式。卷模式可以是 FlexVol 或 FlexGroup。

◦ Type

显示选定卷的类型。卷类型可以是读写，负载共享，数据保护，数据缓存或临时卷。

◦ RAID 类型

显示选定卷的 RAID 类型。RAID 类型可以是 RAID0，RAID4，RAID-DP 或 RAID-TEC。



对于 FlexGroup 卷，可能会显示多种 RAID 类型，因为 FlexGroup 的成分卷可以位于不同类型的聚合上。

◦ Snaplock type

显示卷所在聚合的 SnapLock 类型。

◦ SnapLock 到期

显示 SnapLock 卷的到期日期。

• * 容量 *

- 精简配置

显示是否为卷配置精简配置。

- 自动增长

显示灵活卷是否在聚合内自动增长。

- Snapshot 自动删除

指定在对卷的写入因聚合中空间不足而失败时是否自动删除 Snapshot 副本以释放空间。

- 配额

指定是否为卷启用配额。

- * 效率 *

- 压缩

指定是启用还是禁用压缩。

- 重复数据删除

指定是启用还是禁用重复数据删除。

- 重复数据删除模式

指定在卷上启用的重复数据删除操作是手动操作，计划操作还是基于策略的操作。如果模式设置为已计划，则会显示操作计划；如果模式设置为策略，则会显示策略名称。

- 重复数据删除类型

指定在卷上运行的重复数据删除操作的类型。如果卷处于 SnapVault 关系中，则显示的类型为 SnapVault。对于任何其他卷，此类型将显示为常规。

- 存储效率策略

指定通过 Unified Manager 为此卷分配的存储效率策略的名称。此策略可以控制数据压缩和重复数据删除设置。

- * 保护 *

- Snapshot 副本

指定是启用还是禁用自动 Snapshot 副本。

保护选项卡

"保护"选项卡可显示有关选定卷的保护详细信息，例如滞后信息，关系类型和关系拓扑。

- * 摘要 *

显示选定卷的保护关系（ SnapMirror ， SnapVault 或 Storage VM DR ）属性。对于任何其他关系类型，仅显示 " 关系类型 " 属性。如果选择主卷，则仅显示受管和本地 Snapshot 副本策略。为 SnapMirror 和 SnapVault 关系显示的属性包括：

- 源卷

如果选定卷是目标卷，则显示选定卷的源名称。

- 滞后状态

显示保护关系的更新或传输滞后状态。状态可以是 " 错误 " ， " 警告 " 或 " 严重 " 。

滞后状态不适用于同步关系。

- 滞后持续时间

显示镜像上的数据滞后于源的时间。

- 上次成功更新

显示最近成功更新保护的日期和时间。

上次成功更新不适用于同步关系。

- 存储服务成员

显示 " 是 " 或 " 否 " 以指示卷是否属于存储服务并由存储服务管理。

- 版本灵活复制

显示是，是和备份选项或无。是表示即使源卷和目标卷运行的 ONTAP 软件版本不同，也可以进行 SnapMirror 复制。" 是，使用备份 " 选项表示实施 SnapMirror 保护，并能够在目标上保留多个版本的备份副本。无表示未启用版本灵活复制。

- 关系功能

指示可用于保护关系的 ONTAP 功能。

- 保护服务

如果关系由保护合作伙伴应用程序管理，则显示保护服务的名称。

- 关系类型

显示任何关系类型，包括异步镜像，异步存储，异步镜像存储， StrictSync ， 和 Sync 。

- 关系状态

显示 SnapMirror 或 SnapVault 关系的状态。此状态可以是 Uninitialized ， SnapMirrored 或 Broken-off 。如果选择了源卷，则关系状态不适用，也不会显示。

- 传输状态

显示保护关系的传输状态。传输状态可以是以下状态之一：

- 正在中止

SnapMirror 传输已启用；但是，正在执行传输中止操作，此操作可能包括删除检查点。

- 正在检查

目标卷正在进行诊断检查，并且没有正在进行的传输。

- 正在完成

SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输后阶段。

- 空闲

已启用传输，并且未进行任何传输。

- 同步

同步关系中的两个卷中的数据会同步。

- 不同步

目标卷中的数据不会与源卷同步。

- 正在准备

SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输前阶段。

- 已排队

SnapMirror 传输已启用。没有正在进行的传输。

- 已暂停

SnapMirror 传输已禁用。没有正在进行的传输。

- 正在暂停

正在进行 SnapMirror 传输。已禁用其他传输。

- 正在传输

SnapMirror 传输已启用，正在进行传输。

- 正在过渡

从源卷到目标卷的异步数据传输已完成，并且已开始过渡到同步操作。

- 正在等待

SnapMirror 传输已启动，但某些关联任务正在等待排队。

- 最大传输速率

显示关系的最大传输速率。最大传输速率可以是以 KB/ 秒 (Kbps) , MB/ 秒 (MBps) , GB/ 秒 (Gbps) 或 TB/ 秒 (Tbps) 为单位的数值。如果显示 " 无限制 " , 则关系之间的基线传输不受限制。

- SnapMirror 策略

显示卷的保护策略。DPDefault 表示默认的异步镜像保护策略, XDPDefault 表示默认的异步存储策略, DPSyncDefault 表示默认的异步镜像存储策略。StrictSync 表示默认的同步严格保护策略, Sync 表示默认的同步策略。您可以单击策略名称以查看与该策略关联的详细信息, 包括以下信息:

- 传输优先级
- 忽略访问时间设置
- 尝试次数限制
- 注释
- SnapMirror 标签
- 保留设置
- 实际 Snapshot 副本
- 保留 Snapshot 副本
- 保留警告阈值
- 在级联 SnapVault 关系中, 源卷为数据保护 (DP) 卷且无保留设置的 Snapshot 副本, 仅适用规则 `sm_created`。

- 更新计划

显示分配给关系的 SnapMirror 计划。将光标置于信息图标上方可显示计划详细信息。

- 本地 Snapshot 策略

显示卷的 Snapshot 副本策略。此策略为默认, 无或为自定义策略指定的任何名称。

- 受保护

显示选定卷使用的保护类型。此字段还提供了一个链接、可将您重新定向到包含其 Storage VM 灾难恢复关系的页面。此链接仅适用于成分卷关系。

- * 视图 *

显示选定卷的保护拓扑。此拓扑包括与选定卷相关的所有卷的图形表示。选定卷以深灰色边框表示, 拓扑中卷之间的直线表示保护关系类型。拓扑中关系的方向从左到右显示, 每个关系的源位于左侧, 目标位于右侧。

双粗线用于指定异步镜像关系, 单粗线用于指定异步存储关系, 双单线用于指定异步镜像存储关系, 粗线和非粗线用于指定同步关系。下表显示了同步关系是 StrictSync 关系还是 Sync 关系。

右键单击某个卷将显示一个菜单, 您可以从中选择保护该卷或将数据还原到该卷。右键单击某个关系将显示一个菜单, 您可以从中选择编辑, 中止, 暂停, 中断, 删除, 或恢复关系。

在以下情况下, 菜单不会显示:

- 如果 RBAC 设置不允许执行此操作，例如您只有操作员权限
- 卷处于同步保护关系时
- 如果卷 ID 未知，例如，当您具有集群间关系且尚未发现目标集群时，单击拓扑中的另一个卷可选择并显示该卷的信息。问号 (?) 卷左上角的表示卷缺失或尚未发现。它还可能指示缺少容量信息。将光标置于问号上方可显示追加信息，其中包括补救措施建议。

如果拓扑符合多个常见拓扑模板之一，则会显示有关卷容量，滞后，Snapshot 副本和上次成功数据传输的信息。如果拓扑不符合其中一个模板，则有关卷滞后和上次成功数据传输的信息将显示在拓扑下的关系表中。在这种情况下，表中突出显示的行表示选定卷，而在拓扑视图中，带有蓝点的粗线表示选定卷与其源卷之间的关系。

拓扑视图包括以下信息：

- Capacity

显示卷使用的总容量。将光标置于拓扑中的某个卷上方可在当前阈值设置对话框中显示该卷的当前警告和严重阈值设置。您可以通过单击当前阈值设置对话框中的 * 编辑阈值 * 链接来编辑阈值设置。清除 * 容量 * 复选框将隐藏拓扑中所有卷的所有容量信息。

- 滞后

显示传入保护关系的滞后持续时间和滞后状态。清除 * 滞后 * 复选框将隐藏拓扑中所有卷的所有滞后信息。当 * 滞后 * 复选框灰显时，选定卷的滞后信息将显示在拓扑下面的关系表中，以及所有相关卷的滞后信息。

- Snapshot

显示卷的可用 Snapshot 副本数。清除 * 快照 * 复选框将隐藏拓扑中所有卷的所有 Snapshot 副本信息。单击 Snapshot 副本图标 () 显示卷的 Snapshot 副本列表。图标旁边显示的 Snapshot 副本计数大约每小时更新一次；但是，单击该图标时会更新 Snapshot 副本列表。这可能会导致拓扑中显示的 Snapshot 副本计数与单击此图标时列出的 Snapshot 副本数量有所不同。

- 上次成功传输

显示上次成功传输数据的数量，持续时间，时间和日期。如果 * 上次成功传输 * 复选框灰显，则选定卷的上次成功传输信息将显示在拓扑下面的关系表中，以及所有相关卷的上次成功传输信息。

- * 历史记录 *

以图形方式显示选定卷的传入 SnapMirror 和 SnapVault 保护关系的历史记录。有三个历史记录图形可用：传入关系滞后持续时间、传入关系传输持续时间和传入关系已传输大小。只有在选择目标卷时，才会显示历史记录信息。如果选择主卷、则图形为空、并显示消息 No data found 将显示

您可以从历史记录窗格顶部的下拉列表中选择一种图形类型。您还可以选择 1 周，1 个月或 1 年来查看特定时间段的详细信息。历史记录图可以帮助您确定趋势：例如，如果在一天或一周的同一时间传输大量数据，或者始终违反滞后警告或滞后错误阈值，您可以采取相应的措施。此外，您还可以单击 * 导出 * 按钮为正在查看的图表创建 CSV 格式的报告。

保护历史记录图显示以下信息：

- * 关系滞后持续时间 *

在垂直 (y) 轴上显示秒，分钟或小时，在水平 (x) 轴上显示天，月或年，具体取决于选定的持续时间

段。y 轴上的上限值表示在 x 轴上显示的持续时间内达到的最大滞后持续时间。图形上的橙色水平线表示滞后错误阈值，黄色水平线表示滞后警告阈值。将光标置于这些线上方可显示阈值设置。蓝色水平线表示滞后持续时间。您可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。

- * 关系传输持续时间 *

在垂直 (y) 轴上显示秒，分钟或小时，在水平 (x) 轴上显示天，月或年，具体取决于选定的持续时间段。y 轴上的上限值表示在 x 轴所示的持续时间内达到的最大传输持续时间。您可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。



此图表不适用于处于同步保护关系中的卷。

- * 关系已传输大小 *

根据传输大小在纵轴 (y) 上显示字节，千字节，兆字节等，并根据选定时间段在横轴 (x) 上显示天数，月数或年数。y 轴上的上限值表示在 x 轴所示的持续时间内达到的最大传输大小。您可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。



此图表不适用于处于同步保护关系中的卷。

历史记录区域

历史记录区域显示的图形提供了有关选定卷的容量和空间预留的信息。此外，您还可以单击 * 导出 * 按钮为正在查看的图表创建 CSV 格式的报告。

图形可能为空、并且显示消息 No data found 当卷的数据或状态在一段时间内保持不变时显示。

您可以从历史记录窗格顶部的下拉列表中选择一种图形类型。您还可以选择 1 周，1 个月或 1 年来查看特定时间段的详细信息。历史记录图可以帮助您确定趋势，例如，如果卷使用量持续违反接近全满阈值，您可以采取相应的措施。

历史记录图显示以下信息：

- * 已用卷容量 *

在纵轴 (y) 上以折线图的形式显示卷中的已用容量以及根据使用情况历史记录使用卷容量的趋势 (以字节，千字节，兆字节等单位)。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已用卷容量 " 图例时，" 已用卷容量 " 图形线将处于隐藏状态。

- * 已用卷容量与总计 *

以折线图的形式显示根据使用情况历史记录使用卷容量的趋势，以及已用容量，总容量以及通过重复数据删除和数据压缩节省的空间的详细信息 (以字节，千字节，兆字节为单位)。在垂直 (y) 轴上，依此类推。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已用趋势容量 " 图例时，" 已用趋势容量 " 图形线将处于隐藏状态。

- * 已用卷容量 (%) *

在纵轴 (y) 上以折线图的形式显示卷中的已用容量以及根据使用情况历史记录使用卷容量的趋势 (以百分比表示)。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置

于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已用卷容量 " 图例时，" 已用卷容量 " 图形线将处于隐藏状态。

- * 已用 Snapshot 容量 (%) *

在纵轴 (y) 上以折线图的形式显示 Snapshot 预留和 Snapshot 警告阈值，并以面积图的形式显示 Snapshot 副本使用的容量 (以百分比表示)。Snapshot 溢出用不同的颜色表示。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 Snapshot 预留图例时，Snapshot 预留图形线将被隐藏。

事件列表

事件列表显示有关新事件和已确认事件的详细信息：

- * 严重性 *

显示事件的严重性。

- * 事件 *

显示事件名称。

- * 触发时间 *

显示自事件生成以来经过的时间。如果经过的时间超过一周，则会显示生成事件的时间戳。

相关标注窗格

" 相关标注 " 窗格可用于查看与选定卷关联的标注详细信息。详细信息包括标注名称和应用于卷的标注值。您也可以从 " 相关标注 " 窗格中删除手动标注。

相关设备窗格

" 相关设备 " 窗格可用于查看和导航到与卷相关的 SVM ， 聚合， qtree ， LUN 和 Snapshot 副本：

- * Storage Virtual Machine*

显示包含选定卷的 SVM 的容量和运行状况。

- * 聚合 *

显示包含选定卷的聚合的容量和运行状况。对于 FlexGroup 卷，将列出构成 FlexGroup 的聚合数。

- * 聚合中的卷 *

显示属于选定卷的父聚合的所有卷的数量和容量。此外，还会根据最高严重性级别显示卷的运行状况。例如，如果聚合包含十个卷，其中五个卷显示 " 警告 " 状态，其余五个卷显示 " 严重 " 状态，则显示的状态为 " 严重 "。对于 FlexGroup 卷，不会显示此组件。

- * qtree*

显示选定卷包含的 qtree 数量以及选定卷包含的具有配额的 qtree 容量。此时将显示具有配额的 qtree 的容量与卷数据容量相关。此外，还会根据最高严重性级别显示 qtree 的运行状况。例如，如果卷有十个 qtree，五个 qtree 的状态为 "警告"，其余五个 qtree 的状态为 "严重"，则显示的状态为 "严重"。

- * NFS 共享 *

显示与卷关联的 NFS 共享的数量和状态。

- * SMB 共享 *

显示 SMB/CIFS 共享的数量和状态。

- * LUN *

显示选定卷中所有 LUN 的数量和总大小。此外，还会根据最高严重性级别显示 LUN 的运行状况。

- * 用户和组配额 *

显示与卷及其 qtree 关联的用户和用户组配额的数量和状态。

- * FlexClone 卷 *

显示选定卷的所有克隆卷的数量和容量。只有当选定卷包含任何克隆卷时，才会显示此数量和容量。

- * 父卷 *

显示选定 FlexClone 卷的父卷的名称和容量。只有当选定卷为 FlexClone 卷时，才会显示父卷。

相关组窗格

通过 "相关组" 窗格，您可以查看与选定卷关联的组列表。

相关警报窗格

"相关警报" 窗格可用于查看为选定卷创建的警报列表。您也可以通过单击添加警报链接来添加警报，或者通过单击警报名称来编辑现有警报。

Storage VM/ 运行状况详细信息页面

您可以使用 Storage VM/ 运行状况详细信息页面查看有关选定 Storage VM 的详细信息，例如其运行状况，容量，配置，数据策略，逻辑接口（LIF），LUN，qtree，用户，用户组配额和保护详细信息。您还可以查看有关 Storage VM 的相关对象和相关警报的信息。



您只能监控数据 Storage VM。

命令按钮

使用命令按钮可以对选定 Storage VM 执行以下任务：

- * 切换到性能视图 *

用于导航到 Storage VM/ 性能详细信息页面。

- * 操作 *

- 添加警报

用于向选定 Storage VM 添加警报。

- 标注

用于为选定 Storage VM 添加标注。

- * 查看 Storage VM*

用于导航到运行状况：所有 Storage VM 视图。

运行状况选项卡

运行状况选项卡可显示有关卷，聚合，NAS LIF，SAN LIF，LUN 等各种对象的数据可用性，数据容量和保护问题的详细信息。协议，服务，NFS 共享和 CIFS 共享。

您可以单击某个对象的图形来查看经过筛选的对象列表。例如，您可以单击显示警告的卷容量图形以查看容量问题严重性为警告的卷列表。

- * 可用性问题 *

以图形方式显示对象总数，包括存在可用性问题的对象和没有任何可用性相关问题的对象。图形中的颜色表示问题的不同严重性级别。图形下方的信息提供了有关可能会影响或已影响 Storage VM 中数据可用性的可用性问题的详细信息。例如，将显示有关已关闭的 NAS LIF 和 SAN LIF 以及已脱机的卷的信息。

您还可以查看有关当前正在运行的相关协议和服务以及 NFS 和 CIFS 共享的数量和状态的信息。

- * 容量问题 *

以图形方式显示对象总数，包括存在容量问题的对象和没有任何容量相关问题的对象。图形中的颜色表示问题的不同严重性级别。图形下方的信息提供了有关可能会影响或已影响 Storage VM 中数据容量的容量问题的详细信息。例如，将显示可能违反设置阈值的聚合的相关信息。

- * 保护问题 *

以字段对话框的形式显示与 Storage VM 保护相关的运行状况，其中包括存在保护问题的关系以及不存在任何保护相关问题的关系。您还可以查看选定 Storage VM 的 Storage VM DR 关系的状态。此时将显示 Storage VM DR 关系事件，单击这些事件将转到事件详细信息页面。存在未受保护的卷时，单击此链接将转到运行状况：所有卷视图，在此可以查看 Storage VM 上未受保护的卷的筛选列表。图形中的颜色表示问题的不同严重性级别。单击某个图形将转到 " 关系：所有关系 " 视图，在此可以查看经过筛选的保护关系详细信息列表。图形下方的信息提供了有关可能会影响或已影响 Storage VM 中数据保护的 protection 问题的详细信息。例如，显示有关 Snapshot 副本预留接近全满的卷或有关 SnapMirror 关系滞后问题的信息。

容量选项卡

容量选项卡显示有关选定 SVM 的数据容量的详细信息。

对于包含 FlexVol 卷或 FlexGroup 卷的 Storage VM，将显示以下信息：

- * 容量 *

容量区域显示有关从所有卷分配的已用容量和可用容量的详细信息：

- Total capacity

显示 Storage VM 的总容量。

- 已用

显示属于 Storage VM 的卷中的数据所使用的空间。

- 保证可用

显示可供 Storage VM 中的卷使用的数据使用的保证可用空间。

- 无保证

显示为 Storage VM 中精简配置卷分配的数据的剩余可用空间。

- * 存在容量问题的卷 *

存在容量问题的卷列表以表格形式显示有关存在容量问题的卷的详细信息：

- Status

指示卷具有指示严重性的容量相关问题描述。

您可以将指针移动到状态上方，以查看有关为卷生成的容量相关事件的详细信息。

如果卷的状态是由单个事件确定的，则可以查看事件名称，事件触发时间和日期，事件分配给其的管理员的名称以及事件的发生原因等信息。您可以使用 * 查看详细信息 * 按钮查看有关事件的详细信息。

如果卷的状态是由严重性相同的多个事件确定的，则会显示前三个事件，其中包含事件名称，事件触发时间和日期以及将事件分配到的管理员的名称等信息。您可以通过单击事件名称来查看有关每个事件的更多详细信息。您也可以单击 * 查看所有事件 * 链接以查看生成的事件列表。



一个卷可以具有多个严重性相同或不同的事件。但是，仅显示最高严重性。例如，如果卷具有严重性为 " 错误 " 和 " 警告 " 的两个事件，则仅显示 " 错误 " 严重性。

- Volume

显示卷的名称。

- 已用数据容量

以图形方式显示有关卷容量使用情况的信息（以百分比表示）。

- 达到全满前的天数

显示在卷容量达到全满前的预计剩余天数。

- 精简配置

显示是否为选定卷设置了空间保证。有效值为 "是" 和 "否"

- 聚合

对于 FlexVol 卷，显示包含该卷的聚合的名称。对于 FlexGroup 卷，显示 FlexGroup 中使用的聚合数。

配置选项卡

"配置" 选项卡可显示有关选定 Storage VM 的配置详细信息，例如集群，根卷，所含卷的类型（FlexVol 卷），策略以及在 Storage VM 上创建的保护：

- * 概述 *

- 集群

显示 Storage VM 所属集群的名称。

- 允许的卷类型

显示可在 Storage VM 中创建的卷的类型。类型可以是 FlexVol 或 FlexVol/FlexGroup。

- 根卷

显示 Storage VM 根卷的名称。

- 允许的协议

显示可在 Storage VM 上配置的协议类型。此外，还指示协议是否已启动 (●)，down (●) 或未配置 (●)。

- * 数据网络接口 *

- NAS

显示与 Storage VM 关联的 NAS 接口的数量。此外，还指示接口是否已启动 (●) 或 down (●)。

- SAN

显示与 Storage VM 关联的 SAN 接口的数量。此外，还指示接口是否已启动 (●) 或 down (●)。

- FC-NVMe

显示与 Storage VM 关联的 FC-NVMe 接口的数量。此外，还指示接口是否已启动 (●) 或 down (●)。

- * 管理网络接口 *

- 可用性

显示与 Storage VM 关联的管理接口的数量。此外，还指示管理接口是否已启动 (●) 或 down (●)。

- * 策略 *

- 快照

显示在 Storage VM 上创建的 Snapshot 策略的名称。

- 导出策略

如果创建了一个策略，则显示导出策略的名称；如果创建了多个策略，则显示导出策略的数量。

- * 保护 *

- Storage VM 灾难恢复

显示选定 Storage VM 是受保护的，目标的还是未受保护的，以及受保护 Storage VM 的目标的名称。如果选定 Storage VM 是目标，则会显示源 Storage VM 的详细信息。如果发生扇出，此字段将显示受此 Storage VM 保护的目標 Storage VM 的总数。计数链接将转到在源 Storage VM 上筛选的 Storage VM 关系网。

- 受保护卷

显示选定 Storage VM 上总卷数中的受保护卷数。如果正在查看目标 Storage VM，则此数字链接适用于选定 Storage VM 的目标卷。

- 未受保护的卷

显示选定 Storage VM 上未受保护的卷的数量。

- * 服务 *

- Type

显示在 Storage VM 上配置的服务类型。类型可以是域名系统 (DNS) 或网络信息服务 (NIS)。

- State

显示服务的状态，该状态可以是 up (●)，down (●) 或未配置 (●)。

- 域名

显示 DNS 服务的 DNS 服务器的完全限定域名 (FQDN) 或 NIS 服务的 NIS 服务器。启用 NIS 服务器后，将显示 NIS 服务器的活动 FQDN。禁用 NIS 服务器后，将显示所有 FQDN 的列表。

- IP 地址

显示 DNS 或 NIS 服务器的 IP 地址。启用 NIS 服务器后，将显示 NIS 服务器的活动 IP 地址。禁用 NIS 服务器后，将显示所有 IP 地址的列表。

网络接口选项卡

网络接口选项卡显示有关在选定 Storage VM 上创建的数据网络接口 (LIF) 的详细信息：

- * 网络接口 *

显示在选定 Storage VM 上创建的接口的名称。

- * 运行状态 *

显示接口的运行状态，该状态可以是 up (↑)，down (↓) 或未知 (?)。接口的运行状态由其物理端口的状态决定。

- * 管理状态 *

显示接口的管理状态，该状态可以是 up (↑)，down (↓) 或未知 (?)。接口的管理状态由存储管理员控制，以便对配置进行更改或进行维护。管理状态可以与运行状态不同。但是，如果接口的管理状态为 down，则默认情况下运行状态为 down。

- * IP 地址 /WWPN

显示以太网接口的 IP 地址和 FC LIF 的全球通用端口名称 (WWPN)。

- * 协议 *

显示为接口指定的数据协议列表，例如 CIFS，NFS，iSCSI，FC/FCoE，FC-NVMe 和 FlexCache。

- * 角色 *

显示接口角色。角色可以是 "数据" 或 "管理"。

- * 主端口 *

显示接口最初关联的物理端口。

- * 当前端口 *

显示接口当前关联的物理端口。如果该接口已迁移，则当前端口可能与主端口不同。

- * 端口集 *

显示接口映射到的端口集。

- * 故障转移策略 *

显示为接口配置的故障转移策略。对于 NFS，CIFS 和 FlexCache 接口，默认故障转移策略为 "下一个可用"。故障转移策略不适用于 FC 和 iSCSI 接口。

- * 路由组 *

显示路由组的名称。您可以单击路由组名称来查看有关路由和目标网关的详细信息。

ONTAP 8.3 或更高版本不支持路由组，因此会为这些集群显示一个空列。

- * 故障转移组 *

显示故障转移组的名称。

qtree 选项卡

qtree 选项卡可显示有关 qtree 及其配额的信息。如果要编辑一个或多个 qtree 的 qtree 容量的运行状况阈值设置，可以单击 * 编辑阈值 * 按钮。

使用*导出*按钮创建逗号分隔值 (.csv)文件、其中包含所有受监控qtree的详细信息。导出到 CSV 文件时，您可以选择为当前 Storage VM，当前集群中的所有 Storage VM 或数据中心中所有集群的所有 Storage VM 创建 qtree 报告。导出的 CSV 文件中会显示一些额外的 qtree 字段。

- * 状态 *

显示 qtree 的当前状态。此状态可以为严重 (❌)，错误 (❗)，警告 (⚠️) 或正常 (✅)。

您可以将指针移动到状态图标上方，以查看有关为 qtree 生成的事件的详细信息。

如果 qtree 的状态是由单个事件确定的，则可以查看事件名称，事件触发时间和日期，事件分配给其的管理人员的名称以及事件的发生原因等信息。您可以使用 * 查看详细信息 * 查看有关事件的详细信息。

如果 qtree 的状态是由严重性相同的多个事件确定的，则会显示前三个事件，其中包含事件名称，事件触发时间和日期以及事件分配到的管理人员的名称等信息。您可以通过单击事件名称来查看有关每个事件的更多详细信息。您也可以使用 * 查看所有事件 * 来查看生成的事件列表。



一个 qtree 可以具有多个严重性相同或不同的事件。但是，仅显示最高严重性。例如，如果 qtree 具有严重性为 " 错误 " 和 " 警告 " 的两个事件，则仅显示 " 错误 " 严重性。

- * qtree*

显示 qtree 的名称。

- 集群

显示包含 qtree 的集群的名称。仅显示在导出的 CSV 文件中。

- * Storage Virtual Machine*

显示包含 qtree 的 Storage Virtual Machine (SVM) 名称。仅显示在导出的 CSV 文件中。

- * 卷 *

显示包含 qtree 的卷的名称。

您可以将指针移动到卷名称上方以查看有关该卷的详细信息。

- * 配额集 *

指示是否已在 qtree 上启用配额。

- * 配额类型 *

指定配额是针对用户，用户组还是 qtree。仅显示在导出的 CSV 文件中。

- * 用户或组 *

显示用户或用户组的名称。每个用户和用户组将包含多行。如果配额类型为 qtree 或未设置配额，则此列为空。仅显示在导出的 CSV 文件中。

- * 磁盘已用 %*

显示已用磁盘空间的百分比。如果设置了磁盘硬限制，则此值基于磁盘硬限制。如果设置的配额没有磁盘硬限制，则该值基于卷数据空间。如果未设置配额或 qtree 所属卷上的配额已关闭，则网格页面中会显示 "不适用"，并且 CSV 导出数据中的字段为空。

- * 磁盘硬限制 *

显示为 qtree 分配的最大磁盘空间量。如果达到此限制且不允许进一步写入磁盘，则 Unified Manager 将生成严重事件。在以下情况下，此值将显示为 "无限制"：设置了配额而无磁盘硬限制，未设置配额，或者 qtree 所属卷上的配额未启用。

- * 磁盘软限制 *

显示在生成警告事件之前为 qtree 分配的磁盘空间量。在以下情况下，此值将显示为 "无限制"：设置了配额而无磁盘软限制，未设置配额，或者 qtree 所属卷上的配额未启用。默认情况下，此列处于隐藏状态。

- * 磁盘阈值 *

显示在磁盘空间上设置的阈值。在以下条件下，此值将显示为 "无限制"：设置了配额而无磁盘阈值限制，未设置配额，或者 qtree 所属卷上的配额未启用。默认情况下，此列处于隐藏状态。

- * 已用文件 %*

显示 qtree 中已用文件的百分比。如果设置了文件硬限制，则此值基于文件硬限制。如果设置了配额且没有文件硬限制，则不会显示任何值。如果未设置配额或 qtree 所属卷上的配额已关闭，则网格页面中会显示 "不适用"，并且 CSV 导出数据中的字段为空。

- * 文件硬限制 *

显示 qtree 上允许的文件数的硬限制。在以下情况下，此值将显示为 "无限制"：设置了配额而无文件硬限制，未设置配额，或者 qtree 所属卷上的配额未启用。

- * 文件软限制 *

显示 qtree 上允许的文件数的软限制。在以下条件下，此值将显示为 "无限制"：设置了配额而无文件软限制，未设置配额，或者 qtree 所属卷上的配额未启用。默认情况下，此列处于隐藏状态。

用户和组配额选项卡

显示有关选定 Storage VM 的用户和用户组配额的详细信息。您可以查看配额状态，用户或用户组名称，磁盘和文件上设置的软限制和硬限制，已用磁盘空间量和文件数量以及磁盘阈值等信息。您还可以更改与用户或用户组关联的电子邮件地址。

- * 编辑电子邮件地址命令按钮 *

打开编辑电子邮件地址对话框，其中显示选定用户或用户组的当前电子邮件地址。您可以修改电子邮件地址。如果 "编辑电子邮件地址" 字段为空、则使用默认规则为选定用户或用户组生成电子邮件地址。

如果多个用户具有相同的配额，则这些用户的名称将显示为逗号分隔值。此外，不会使用默认规则生成电子

邮件地址，因此，您必须提供所需的电子邮件地址才能发送通知。

- * 配置电子邮件规则命令按钮 *

用于创建或修改规则，以便为 Storage VM 上配置的用户或用户组配额生成电子邮件地址。如果存在违反配额的情况，系统会向指定的电子邮件地址发送通知。

- * 状态 *

显示配额的当前状态。此状态可以为严重 (❌)，警告 (⚠️) 或正常 (✅)。

您可以将指针移动到状态图标上方，以查看有关为配额生成的事件的详细信息。

如果配额的状态是由单个事件确定的，则可以查看事件名称，事件触发时间和日期，事件分配到的管理员姓名以及事件的发生原因等信息。您可以使用 * 查看详细信息 * 查看有关事件的详细信息。

如果配额状态由严重性相同的多个事件确定，则会显示前三个事件，其中包含事件名称，事件触发时间和日期以及事件分配给的管理员的名称等信息。您可以通过单击事件名称来查看有关每个事件的更多详细信息。您也可以使用 * 查看所有事件 * 来查看生成的事件列表。



一个配额可以具有多个严重性相同或不同的事件。但是，仅显示最高严重性。例如，如果配额具有严重性为 " 错误 " 和 " 警告 " 的两个事件，则仅显示 " 错误 " 严重性。

- * 用户或组 *

显示用户或用户组的名称。如果多个用户具有相同的配额，则这些用户的名称将显示为逗号分隔值。

如果 ONTAP 由于 SecD 错误而未提供有效的用户名，则此值将显示为 " 未知 "。

- * 类型 *

指定配额是针对用户还是用户组。

- * 卷或 qtree *

显示指定用户或用户组配额的卷或 qtree 的名称。

您可以将指针移动到卷或 qtree 的名称上方，以查看有关卷或 qtree 的更多信息。

- * 磁盘已用 % *

显示已用磁盘空间的百分比。如果设置的配额没有磁盘硬限制，则此值将显示为 " 不适用 "。

- * 磁盘硬限制 *

显示为配额分配的最大磁盘空间量。如果达到此限制且不允许进一步写入磁盘，则 Unified Manager 将生成严重事件。如果设置的配额没有磁盘硬限制，则此值将显示为 " 无限制 "。

- * 磁盘软限制 *

显示在生成警告事件之前为配额分配的磁盘空间量。如果设置的配额没有磁盘软限制，则此值将显示为 " 无限制 "。默认情况下，此列处于隐藏状态。

- * 磁盘阈值 *

显示在磁盘空间上设置的阈值。如果设置的配额没有磁盘阈值限制，则此值将显示为 "无限制"。默认情况下，此列处于隐藏状态。

- * 已用文件 %*

显示 qtree 中已用文件的百分比。如果设置的配额没有文件硬限制，则此值将显示为 "不适用"。

- * 文件硬限制 *

显示配额允许的文件数的硬限制。如果设置的配额没有文件硬限制，则此值将显示为 "无限制"。

- * 文件软限制 *

显示配额允许的文件数的软限制。如果设置的配额没有文件软限制，则此值将显示为 "无限制"。默认情况下，此列处于隐藏状态。

- * 电子邮件地址 *

显示违反配额时要向其发送通知的用户或用户组的电子邮件地址。

NFS 共享选项卡

"NFS 共享" 选项卡可显示有关 NFS 共享的信息，例如其状态，与卷（FlexGroup 卷或 FlexVol 卷）关联的路径，客户端对 NFS 共享的访问级别以及为导出的卷定义的导出策略。在以下情况下，不会显示 NFS 共享：卷未挂载，或者与卷的导出策略关联的协议不包含 NFS 共享。

- * 状态 *

显示 NFS 共享的当前状态。此状态可以为 Error (❗) 或正常 (✅)。

- * 接合路径 *

显示卷的挂载路径。如果将显式 NFS 导出策略应用于 qtree，则此列将显示可用于访问 qtree 的卷的路径。

- * 接合路径活动 *

显示用于访问已挂载卷的路径是活动路径还是非活动路径。

- * 卷或 qtree*

显示应用 NFS 导出策略的卷或 qtree 的名称。如果 NFS 导出策略应用于卷中的 qtree，则此列将同时显示卷和 qtree 的名称。

您可以单击此链接以在相应的详细信息页面中查看有关此对象的详细信息。如果对象是 qtree，则会显示 qtree 和卷的链接。

- * 卷状态 *

显示要导出的卷的状态。此状态可以是 "脱机"，"联机"，"受限" 或 "混合"。

- 脱机

不允许对卷进行读写访问。

- 联机

允许对卷进行读写访问。

- 受限

允许执行有限的操作，例如奇偶校验重建，但不允许数据访问。

- 混合

FlexGroup 卷的成分卷并非都处于相同状态。

- * 安全模式 *

显示已导出卷的访问权限。安全模式可以是 UNIX，统一，NTFS 或混合。

- UNIX（NFS 客户端）

卷中的文件和目录具有 UNIX 权限。

- 统一：

卷中的文件和目录具有统一的安全模式。

- NTFS（CIFS 客户端）

卷中的文件和目录具有 Windows NTFS 权限。

- 混合

卷中的文件和目录可以具有 UNIX 权限或 Windows NTFS 权限。

- * UNIX 权限 *

以八进制字符串格式显示为导出的卷设置的 UNIX 权限位。它类似于 UNIX 模式的权限位。

- * 导出策略 *

显示用于为导出的卷定义访问权限的规则。您可以单击此链接以查看与导出策略关联的规则的详细信息，例如身份验证协议和访问权限。

SMB 共享选项卡

显示有关选定 Storage VM 上的 SMB 共享的信息。您可以查看 SMB 共享的状态，共享名称，与 Storage VM 关联的路径，共享接合路径的状态，包含对象，包含卷的状态，共享的安全数据以及为共享定义的导出策略等信息。您还可以确定是否存在 SMB 共享的等效 NFS 路径。



文件夹中的共享不会显示在 SMB 共享选项卡中。

- * 查看用户映射命令按钮 *

启动用户映射对话框。

您可以查看 Storage VM 的用户映射详细信息。

- * 显示 ACL 命令按钮 *

启动共享的访问控制对话框。

您可以查看选定共享的用户和权限详细信息。

- * 状态 *

显示共享的当前状态。此状态可以为正常 (✓) 或错误 (!)。

- * 共享名称 *

显示 SMB 共享的名称。

- * 路径 *

显示创建共享的接合路径。

- * 接合路径活动 *

显示用于访问共享的路径是处于活动状态还是处于非活动状态。

- * 包含对象 *

显示共享所属的包含对象的名称。包含对象可以是卷或 qtree。

通过单击此链接，您可以在相应的 " 详细信息 " 页面中查看包含对象的详细信息。如果包含的对象是 qtree，则会显示 qtree 和卷的链接。

- * 卷状态 *

显示要导出的卷的状态。此状态可以是 " 脱机 "，" 联机 "，" 受限 " 或 " 混合 "。

- 脱机

不允许对卷进行读写访问。

- 联机

允许对卷进行读写访问。

- 受限

允许执行有限的操作，例如奇偶校验重建，但不允许数据访问。

- 混合

FlexGroup 卷的成分卷并非都处于相同状态。

- * 安全性 *

显示已导出卷的访问权限。安全模式可以是 UNIX ， 统一， NTFS 或混合。

- UNIX （ NFS 客户端）

卷中的文件和目录具有 UNIX 权限。

- 统一：

卷中的文件和目录具有统一的安全模式。

- NTFS （ CIFS 客户端）

卷中的文件和目录具有 Windows NTFS 权限。

- 混合

卷中的文件和目录可以具有 UNIX 权限或 Windows NTFS 权限。

- * 导出策略 *

显示适用于共享的导出策略的名称。如果未为此 Storage VM 指定导出策略，则此值将显示为未启用。

您可以单击此链接以查看与导出策略关联的规则的信息，例如访问协议和权限。如果为选定 Storage VM 禁用了导出策略，则此链接将被禁用。

- * NFS 等效项 *

指定共享是否具有 NFS 等效项。

SAN 选项卡

显示有关选定 Storage VM 的 LUN ， 启动程序组和启动程序的详细信息。默认情况下，将显示 LUN 视图。您可以在启动程序组选项卡中查看有关启动程序组的详细信息，并在启动程序选项卡中查看有关启动程序的详细信息。

- * LUNs 选项卡 *

显示有关属于选定 Storage VM 的 LUN 的详细信息。您可以查看 LUN 名称， LUN 状态（联机或脱机），包含 LUN 的文件系统的名称（卷或 qtree ），主机操作系统的类型， LUN 的总数据容量和序列号等信息。LUN 性能列提供了一个指向 LUN/ 性能详细信息页面的链接。

您还可以查看有关是否已在 LUN 上启用精简配置以及 LUN 是否已映射到启动程序组的信息。如果已将其映射到启动程序，则可以查看映射到选定 LUN 的启动程序组和启动程序。

- * 启动程序组选项卡 *

显示有关启动程序组的详细信息。您可以查看启动程序组的名称，访问状态，组中所有启动程序使用的主机操作系统类型以及支持的协议等详细信息。单击访问状态列中的链接时，您可以查看启动程序组的当前访问状态。

- * 正常 *

启动程序组连接到多个访问路径。

- * 单路径 *

启动程序组连接到一个访问路径。

- * 无路径 *

没有连接到启动程序组的访问路径。

您可以查看启动程序组是通过端口集映射到所有接口还是特定接口。单击已映射接口列中的计数链接时，将显示所有接口或显示端口集的特定接口。不会显示通过目标门户映射的接口。此时将显示映射到启动程序组的启动程序和 LUN 总数。

您还可以查看映射到选定启动程序组的 LUN 和启动程序。

- * 启动程序选项卡 *

显示启动程序的名称和类型以及映射到此启动程序的选定 Storage VM 启动程序的启动程序组总数。

您还可以查看映射到选定启动程序组的 LUN 和启动程序组。

相关标注窗格

" 相关标注 " 窗格可用于查看与选定 Storage VM 关联的标注详细信息。详细信息包括标注名称和应用于 Storage VM 的标注值。您也可以从 " 相关标注 " 窗格中删除手动标注。

相关设备窗格

" 相关设备 " 窗格可用于查看与 Storage VM 相关的集群，聚合和卷：

- 集群

显示 Storage VM 所属集群的运行状况。

- * 聚合 *

显示属于选定 Storage VM 的聚合数。此外，还会根据最高严重性级别显示聚合的运行状况。例如，如果 Storage VM 包含十个聚合，其中五个聚合显示 " 警告 " 状态，其余五个聚合显示 " 严重 " 状态，则显示的状态为 " 严重 "。

- * 已分配聚合 *

显示分配给 Storage VM 的聚合数。此外，还会根据最高严重性级别显示聚合的运行状况。

- * 卷 *

显示属于选定 Storage VM 的卷的数量和容量。此外，还会根据最高严重性级别显示卷的运行状况。如果 Storage VM 中存在 FlexGroup 卷，则此计数还包括 FlexGroup；它不包括 FlexGroup 成分卷。

相关组窗格

" 相关组 " 窗格可用于查看与选定 Storage VM 关联的组列表。

相关警报窗格

" 相关警报 " 窗格可用于查看为选定 Storage VM 创建的警报列表。您也可以单击 * 添加警报 * 链接来添加警报，或者单击警报名称来编辑现有警报。

集群 / 运行状况详细信息页面

集群 / 运行状况详细信息页面提供了有关选定集群的详细信息，例如运行状况，容量和配置详细信息。您还可以查看有关集群的网络接口（LIF），节点，磁盘，相关设备和相关警报的信息。

集群名称旁边的状态（例如（良好））表示通信状态； Unified Manager 是否可以与集群通信。它不表示集群的故障转移状态或整体状态。

命令按钮

命令按钮可用于对选定集群执行以下任务：

- * 切换到性能视图 *

用于导航到集群 / 性能详细信息页面。

- * 操作 *

- 添加警报：打开添加警报对话框，在此可以向选定集群添加警报。
- 重新发现：启动集群的手动刷新，使 Unified Manager 能够发现最近对集群所做的更改。

如果 Unified Manager 与 OnCommand Workflow Automation 配对，则重新发现操作还会从 WFA 重新获取缓存的数据（如果有）。

启动重新发现操作后，将显示指向关联作业详细信息的链接，以便跟踪作业状态。

- 标注：用于标注选定集群。

- * 查看集群 *

用于导航到运行状况：所有集群视图。

运行状况选项卡

显示有关节点，SVM 和聚合等各种集群对象的数据可用性和数据容量问题的详细信息。可用性问题与集群对象的数据提供功能有关。容量问题与集群对象的数据存储功能有关。

您可以单击某个对象的图形来查看经过筛选的对象列表。例如，您可以单击显示警告的 SVM 容量图形来查看经过筛选的 SVM 列表。此列表包含卷或 qtree 的容量问题严重性级别为 " 警告 " 的 SVM。此外，您还可以单击显示警告的 SVM 可用性图形来查看严重性级别为 " 警告 " 的可用性问题 SVM 列表。

- * 可用性问题 *

以图形方式显示对象总数，包括存在可用性问题的对象和没有任何可用性相关问题的对象。图形中的颜色表示问题的不同严重性级别。图形下方的信息提供了有关可能会影响或已经影响集群中数据可用性的可用性问题的详细信息。例如，将显示有关已关闭的磁盘架和脱机的聚合的信息。



SFO 条形图显示的数据基于节点的 HA 状态。所有其他条形图显示的数据均根据生成的事件进行计算。

- * 容量问题 *

以图形方式显示对象总数，包括存在容量问题的对象和没有任何容量相关问题的对象。图形中的颜色表示问题的不同严重性级别。图形下方的信息提供了有关可能会影响或已影响集群中数据容量的容量问题的详细信息。例如，将显示可能违反设置阈值的聚合的相关信息。

容量选项卡

显示有关选定集群容量的详细信息。

- * 容量 *

显示有关所有已分配聚合中已用容量和可用容量的数据容量图形：

- 已用逻辑空间

存储在此集群上的所有聚合上的数据的实际大小，而不会因使用 ONTAP 存储效率技术而节省空间。

- 已用

所有聚合上的数据所使用的物理容量。这包括用于奇偶校验，规模估算和预留的容量。

- 可用

显示可用于数据的容量。

- 备件

显示所有备用磁盘中可用于存储的可存储容量。

- 已配置

显示为所有底层卷配置的容量。

- * 详细信息 *

显示有关已用容量和可用容量的详细信息。

- Total capacity

显示集群的总容量。这包括为奇偶校验分配的容量。

- 已用

显示数据使用的容量。这包括用于奇偶校验，规模估算和预留的容量。

- 可用

显示可用于数据的容量。

- 已配置

显示为所有底层卷配置的容量。

- 备件

显示所有备用磁盘中可用于存储的可存储容量。

- * 云层 *

显示集群上启用了 FabricPool 的聚合的已用云层总容量以及每个已连接云层的已用容量。FabricPool 可以是已获得许可的，也可以是未获得许可的。

- * 按磁盘类型划分的物理容量细分 *

"按磁盘类型细分的物理容量" 区域显示有关集群中各种磁盘类型的磁盘容量的详细信息。通过单击磁盘类型，您可以从磁盘选项卡查看有关磁盘类型的详细信息。

- 总可用容量

显示数据磁盘的可用容量和备用容量。

- HDD

以图形方式显示集群中所有 HDD 数据磁盘的已用容量和可用容量。虚线表示 HDD 中数据磁盘的备用容量。

- 闪存

- SSD 数据

以图形方式显示集群中 SSD 数据磁盘的已用容量和可用容量。

- SSD 缓存

以图形方式显示集群中 SSD 缓存磁盘的可存储容量。

- SSD 备用

以图形方式显示集群中 SSD，数据和缓存磁盘的备用容量。

- 未分配的磁盘

显示集群中未分配的磁盘的数量。

- * 存在容量问题的聚合列表 *

以表格形式显示有关存在容量风险问题的聚合的已用容量和可用容量的详细信息。

- Status

指示聚合具有特定严重性的容量相关问题描述。

您可以将指针移动到状态上方，以查看有关为聚合生成的事件的详细信息。

如果聚合的状态是由单个事件确定的，则可以查看事件名称，事件触发时间和日期，事件分配给其的管理人员的名称以及事件的发生原因等信息。您可以单击 * 查看详细信息 * 按钮查看有关事件的详细信息。

如果聚合的状态是由严重性相同的多个事件确定的，则会显示前三个事件，其中包含事件名称，事件触发时间和日期以及将事件分配到的管理人员的名称等信息。您可以通过单击事件名称来查看有关每个事件的更多详细信息。您也可以单击 * 查看所有事件 * 链接以查看生成的事件列表。



一个聚合可以具有多个严重性相同或不同的容量相关事件。但是，仅显示最高严重性。例如，如果聚合具有两个严重性级别为 " 错误 " 和 " 严重 " 的事件，则仅显示 " 严重 " 严重性。

- 聚合

显示聚合的名称。

- 已用数据容量

以图形方式显示有关聚合容量使用情况的信息（以百分比表示）。

- 达到全满前的天数

显示聚合达到容量全满前的预计剩余天数。

配置选项卡

显示有关选定集群的详细信息、例如IP地址、序列号、联系人和位置：

- * 集群概述 *

- 管理接口

显示 Unified Manager 用于连接到集群的集群管理 LIF 。此外，还会显示接口的运行状态。

- 主机名或 IP 地址

显示 Unified Manager 用于连接到集群的集群管理 LIF 的 FQDN ，简称或 IP 地址。

- FQDN

显示集群的完全限定域名（ FQDN ）。

- OS 版本

显示集群运行的 ONTAP 版本。如果集群中的节点运行的 ONTAP 版本不同，则会显示最早的 ONTAP 版本。

- 序列号

显示集群的序列号。

- 联系方式

显示有关在集群出现问题时应联系的管理员的详细信息。

- 位置

显示集群的位置。

- 个性化

标识此集群是否为已配置全 SAN 阵列的集群。

- * 远程集群概述 *

提供有关 MetroCluster 配置中远程集群的详细信息。只有 MetroCluster 配置才会显示此信息。

- 集群

显示远程集群的名称。您可以单击集群名称以导航到集群的详细信息页面。

- 主机名或 IP 地址

显示远程集群的 FQDN，短名称或 IP 地址。

- 序列号

显示远程集群的序列号。

- 位置

显示远程集群的位置。

- * MetroCluster 概述 *

提供有关 MetroCluster 配置中本地集群的详细信息。只有 MetroCluster 配置才会显示此信息。

- Type

显示 MetroCluster 类型是双节点还是四节点。

- Configuration

显示 MetroCluster 配置，该配置可以具有以下值：

- 使用 SAS 缆线的延伸型配置
- 使用 FC-SAS 网桥的延伸型配置
- 使用 FC 交换机的网络结构配置



对于四节点 MetroCluster，仅支持使用 FC 交换机的网络结构配置。

+

- 自动计划外切换（AUSO）

显示是否为本地集群启用了自动计划外切换。默认情况下，Unified Manager 中双节点 MetroCluster 配置中的所有集群都启用 AUSO。您可以使用命令行界面更改 AUSO 设置。

- * 节点 * :

- 可用性

显示已启动的节点数 (●) 或 down (●)。

- 操作系统版本

显示节点正在运行的 ONTAP 版本以及运行特定 ONTAP 版本的节点数。例如，9.6 (2) 和 9.3 (1) 指定两个节点运行 ONTAP 9.6，一个节点运行 ONTAP 9.3。

- * Storage Virtual Machine* :

- 可用性

显示已启动的 SVM 数 (●) 或 down (●)。

- * 网络接口 * :

- 可用性

显示已启动的非数据 LIF 的数量 (●) 或 down (●)。

- 集群管理接口

显示集群管理 LIF 的数量。

- 节点管理接口

显示节点管理 LIF 的数量。

- 集群接口

显示集群 LIF 的数量。

- 集群间接口

显示集群间 LIF 的数量。

- * 协议 * :

- 数据协议

显示为集群启用的许可数据协议列表。数据协议包括 iSCSI，CIFS，NFS，NVMe 和 FC/FCoE。

- * 云层 * :

列出此集群连接到的云层的名称。此外，还会列出云层的类型（Amazon S3，Microsoft Azure Cloud，

IBM Cloud Object Storage , Google Cloud Storage , Alibaba Cloud Object Storage 或 StorageGRID) 和状态 (可用或不可用) 。

MetroCluster 连接选项卡

显示 MetroCluster 配置中集群组件的问题和连接状态。当集群的灾难恢复配对节点出现问题时，集群将显示在一个红色框中。



只有 MetroCluster 配置中的集群才会显示 MetroCluster 连接选项卡。

您可以通过单击远程集群的名称导航到远程集群的详细信息页面。您也可以单击组件的计数链接来查看组件的详细信息。例如，单击集群中节点的计数链接会在集群的详细信息页面中显示节点选项卡。单击远程集群中磁盘的计数链接会在远程集群的详细信息页面中显示磁盘选项卡。



在管理八节点 MetroCluster 配置时，单击磁盘架组件的计数链接将仅显示默认 HA 对的本地磁盘架。此外，无法显示另一个 HA 对上的本地磁盘架。

如果存在任何问题描述，您可以将指针移动到组件上方来查看集群的详细信息和连接状态，并查看有关为问题描述生成的事件的详细信息。

如果组件之间连接问题描述的状态是由单个事件确定的，则可以查看事件名称，事件触发时间和日期，事件分配给的管理员的名称以及事件的发生原因等信息。查看详细信息按钮可提供有关事件的详细信息。

如果组件之间连接问题描述的状态是由严重性相同的多个事件确定的，则会显示前三个事件，其中包含事件名称，事件触发时间和日期以及将事件分配到的管理员的名称等信息。您可以通过单击事件名称来查看有关每个事件的更多详细信息。您也可以单击 * 查看所有事件 * 链接以查看生成的事件列表。

MetroCluster 复制选项卡

显示正在复制的数据的状态。您可以使用 MetroCluster 复制选项卡通过与已建立对等关系的集群同步镜像数据来确保数据保护。当集群的灾难恢复配对节点出现问题时，集群将显示在一个红色框中。



只有 MetroCluster 配置中的集群才会显示 MetroCluster 复制选项卡。

在 MetroCluster 环境中，您可以使用此选项卡验证本地集群与远程集群的逻辑连接和对等关系。您可以查看集群组件及其逻辑连接的目标表示形式。这有助于确定在镜像元数据和数据期间可能发生的问题。

在 MetroCluster 复制选项卡中，本地集群提供选定集群的详细图形表示，MetroCluster 配对节点是指远程集群。

网络接口选项卡

显示有关在选定集群上创建的所有非数据 LIF 的详细信息。

- * 网络接口 *

显示在选定集群上创建的 LIF 的名称。

- * 运行状态 *

显示接口的运行状态，该状态可以是 up (↑)，down (↓) 或未知 (?)。网络接口的运行状态由其

物理端口的状态决定。

- * 管理状态 *

显示接口的管理状态，该状态可以是 up (↑)，down (↓) 或未知 (?)。您可以在更改配置或进行维护时控制接口的管理状态。管理状态可以与运行状态不同。但是，如果 LIF 的管理状态为 down，则运行状态默认为 down。

- * IP 地址 *

显示接口的 IP 地址。

- * 角色 *

显示接口的角色。可能的角色包括集群管理 LIF，节点管理 LIF，集群 LIF 和集群间 LIF。

- * 主端口 *

显示接口最初关联的物理端口。

- * 当前端口 *

显示接口当前关联的物理端口。迁移 LIF 后，当前端口可能与主端口不同。

- * 故障转移策略 *

显示为接口配置的故障转移策略。

- * 路由组 *

显示路由组的名称。您可以单击路由组名称来查看有关路由和目标网关的详细信息。

ONTAP 8.3 或更高版本不支持路由组，因此会为这些集群显示一个空列。

- * 故障转移组 *

显示故障转移组的名称。

节点选项卡

显示有关选定集群中节点的信息。您可以查看有关 HA 对，磁盘架和端口的详细信息：

- * HA 详细信息 *

以图形方式显示 HA 对中节点的 HA 状态和运行状况。节点的运行状况以以下颜色表示：

- * 绿色 *

节点处于工作状态。

- * 黄色 *

节点已接管配对节点，或者节点面临一些环境问题。

- * 红色 *

节点已关闭。

您可以查看有关 HA 对可用性的信息，并采取必要措施以防止出现任何风险。例如、如果可能发生接管操作、则会显示以下消息：Storage failover possible。

您可以查看与 HA 对其环境相关的事件列表，例如风扇，电源，NVRAM 电池，闪存卡，服务处理器和磁盘架连接。您还可以查看事件触发时间。

您可以查看其他与节点相关的信息、例如型号和序列号。

如果存在单节点集群，您还可以查看有关这些节点的详细信息。

- * 磁盘架 * :

显示有关 HA 对中磁盘架的信息。

您还可以查看为磁盘架和环境组件生成的事件以及事件触发时间。

- * 磁盘架 ID*

显示磁盘所在磁盘架的 ID。

- * 组件状态 *

显示磁盘架的环境详细信息，例如电源，风扇，温度传感器，电流传感器，磁盘连接，和电压传感器。环境详细信息以以下颜色显示为图标：

- * 绿色 *

环境组件正常工作。

- * 灰色 *

没有可用于环境组件的数据。

- * 红色 *

某些环境组件已关闭。

- * 状态 *

显示磁盘架的状态。可能的状态包括脱机，联机，无状态，需要初始化，缺失，和未知。

- * 型号 *

显示磁盘架的型号。

- * 本地磁盘架 *

指示磁盘架位于本地集群还是远程集群上。只有 MetroCluster 配置中的集群才会显示此列。

- * 唯一 ID*

显示磁盘架的唯一标识符。

- * 固件版本 *

显示磁盘架的固件版本。

- * 端口 *

显示有关关联 FC ， FCoE 和以太网端口的信息。您可以单击端口图标来查看有关端口和关联 LIF 的详细信息。

您还可以查看为端口生成的事件。

您可以查看以下端口详细信息：

- 端口 ID

显示端口的名称。例如，端口名称可以是 e0M ， e0a 和 e0b 。

- Role

显示端口的角色。可能的角色包括 " 集群 " ， " 数据 " ， " 集群间 " ， " 节点管理 " 和 " 未定义 " 。

- Type

显示端口所使用的物理层协议。可能的类型包括以太网，光纤通道和 FCoE 。

- WWPN

显示端口的全球通用端口名称（ WWPN ）。

- 固件修订版

显示 FC/FCoE 端口的固件版本。

- Status

显示端口的当前状态。可能的状态包括 " 已启动 " ， " 已关闭 " ， " 链路未连接 " 或 " 未知 "（）。

您可以从事件列表中查看与端口相关的事件。您还可以查看关联的 LIF 详细信息，例如 LIF 名称，运行状态， IP 地址或 WWPN ，协议，与 LIF 关联的 SVM 的名称，当前端口，故障转移策略和故障转移组。

磁盘选项卡

显示有关选定集群中磁盘的详细信息。您可以查看与磁盘相关的信息，例如已用磁盘数，备用磁盘数，损坏的磁盘数和未分配的磁盘数。您还可以查看其他详细信息，例如磁盘名称，磁盘类型和磁盘所有者节点。

- * 磁盘池摘要 *

显示按有效类型（ FCAL ， SAS ， SATA ， MSATA ， SSD ， NVMe SSD ， SSD CAP ，阵列 LUN 和 VMDISK ）以及磁盘的状态。您还可以查看其他详细信息，例如聚合数量，共享磁盘，备用磁盘，损坏的磁

盘，未分配的磁盘，和不受支持的磁盘。如果单击有效磁盘类型计数链接，则会显示选定状态和有效类型的磁盘。例如，如果单击磁盘状态为 "已断开" 和有效类型为 SAS 的计数链接，则会显示磁盘状态为 "已断开" 和有效类型为 SAS 的所有磁盘。

- * 磁盘 *

显示磁盘的名称。

- * RAID 组 *

显示 RAID 组的名称。

- * 所有者节点 *

显示磁盘所属节点的名称。如果磁盘未分配，则此列不会显示任何值。

- * 状态 *

显示磁盘的状态：聚合，共享，备用，已断开，未分配，不支持或未知。默认情况下，此列会进行排序，以按以下顺序显示状态：已断开，未分配，不支持，备用，聚合，和共享。

- * 本地磁盘 *

显示 "是" 或 "否" 以指示磁盘位于本地集群还是远程集群上。只有 MetroCluster 配置中的集群才会显示此列。

- * 位置 *

根据容器类型显示磁盘的位置：例如，复制，数据或奇偶校验。默认情况下，此列处于隐藏状态。

- * 受影响的聚合 *

显示因磁盘故障而受影响的聚合数。您可以将指针移动到计数链接上方以查看受影响的聚合，然后单击聚合名称以查看聚合的详细信息。您也可以单击聚合计数以在运行状况：所有聚合视图中查看受影响聚合的列表。

在以下情况下，此列不显示任何值：

- 如果将包含此类磁盘的集群添加到 Unified Manager 中，则此磁盘将损坏
- 没有故障磁盘时

- * 存储池 *

显示 SSD 所属存储池的名称。您可以将指针移动到存储池名称上方以查看存储池的详细信息。

- * 可存储容量 *

显示可供使用的磁盘容量。

- * 原始容量 *

显示在调整大小和配置 RAID 之前未格式化的原始磁盘的容量。默认情况下，此列处于隐藏状态。

- * 类型 *

显示磁盘类型：例如 ATA ， SATA ， FCAL 或 VMDISK 。

- * 有效类型 *

显示 ONTAP 分配的磁盘类型。

某些 ONTAP 磁盘类型在创建和添加到聚合以及备件管理方面被视为等效类型。ONTAP 会为每种磁盘类型分配一个有效的磁盘类型。

- * 已用备用块 %*

以百分比形式显示 SSD 磁盘中使用的备用块。对于 SSD 磁盘以外的磁盘，此列为空。

- * 额定已用寿命 %*

以百分比显示根据实际 SSD 使用情况和制造商对 SSD 使用寿命的预测得出的 SSD 使用寿命估计值。如果值大于 99 ，则表示估计的持久性已耗尽，但可能并不表示 SSD 出现故障。如果此值未知，则会省略磁盘。

- * 固件 *

显示磁盘的固件版本。

- * 转数 *

显示磁盘的每分钟转数（RPM）。默认情况下，此列处于隐藏状态。

- * 型号 *

显示磁盘的型号。默认情况下，此列处于隐藏状态。

- * 供应商 *

显示磁盘供应商的名称。默认情况下，此列处于隐藏状态。

- * 磁盘架 ID*

显示磁盘所在磁盘架的 ID 。

- * 托架 *

显示磁盘所在托架的 ID 。

相关标注窗格

用于查看与选定集群关联的标注详细信息。详细信息包括标注名称和应用于集群的标注值。您也可以从 " 相关标注 " 窗格中删除手动标注。

相关设备窗格

用于查看与选定集群关联的设备详细信息。

详细信息包括连接到集群的设备的属性，例如设备类型，大小，计数和运行状况。您可以单击计数链接以对该特定设备进行进一步分析。

您可以使用 MetroCluster 合作伙伴窗格获取有关远程 MetroCluster 配对节点及其关联集群组件（例如节点，聚合和 SVM）的计数以及详细信息。只有 MetroCluster 配置中的集群才会显示 MetroCluster 合作伙伴窗格。

" 相关设备 " 窗格可用于查看和导航到与集群相关的节点，SVM 和聚合：

- * MetroCluster 合作伙伴 *

显示 MetroCluster 配对节点的运行状况。使用计数链接，您可以进一步导航并获取有关集群组件的运行状况和容量的信息。

- * 节点 * :

显示属于选定集群的节点的数量，容量和运行状况。Capacity 表示总可用容量超过可用容量。

- * Storage Virtual Machine*

显示属于选定集群的 SVM 数量。

- * 聚合 *

显示属于选定集群的聚合的数量，容量和运行状况。

相关组窗格

用于查看包含选定集群的组列表。

相关警报窗格

" 相关警报 " 窗格可用于查看选定集群的警报列表。您也可以通过单击添加警报链接来添加警报，或者通过单击警报名称来编辑现有警报。

聚合 / 运行状况详细信息页面

您可以使用聚合 / 运行状况详细信息页面查看有关选定聚合的详细信息，例如容量，磁盘信息，配置详细信息和生成的事件。您还可以查看有关该聚合的相关对象和相关警报的信息。

命令按钮



监控启用了 FabricPool 的聚合时，此页面上的已提交和过量提交值仅与本地或性能层容量相关。云层中的可用空间量不会反映在过量使用的值中。同样，聚合阈值仅与本地性能层相关。

使用命令按钮可以对选定聚合执行以下任务：

- * 切换到性能视图 *

用于导航到聚合 / 性能详细信息页面。

- * 操作 *

- 添加警报

用于向选定聚合添加警报。

- 编辑阈值

用于修改选定聚合的阈值设置。

- * 查看聚合 *

用于导航到运行状况：所有聚合视图。

容量选项卡

"容量"选项卡可显示有关选定聚合的详细信息，例如其容量，阈值和每日增长率。

默认情况下，不会为根聚合生成容量事件。此外，Unified Manager 使用的阈值不适用于节点根聚合。只有技术支持代表才能修改要生成的这些事件的设置。如果设置由技术支持代表修改，则阈值将应用于节点根聚合。

- * 容量 *

显示数据容量图形和 Snapshot 副本图形，其中显示了有关聚合的容量详细信息：

- 已用逻辑空间

在不通过使用 ONTAP 存储效率技术节省空间的情况下，当前存储在聚合上的数据的实际大小。

- 已用

聚合中数据使用的物理容量。

- 已过量提交

如果聚合中的空间过量使用，则此图表将显示一个标记以及过量使用的空间量。

- 警告

在设置警告阈值的位置显示一条虚线；表示聚合中的空间接近全满。如果违反此阈值，则会生成空间接近全满事件。

- error

在设置错误阈值的位置显示一条实线；表示聚合中的空间已满。如果违反此阈值，则会生成空间已满事件。

- Snapshot 副本图形

只有在已用 Snapshot 容量或 Snapshot 预留不为零时，才会显示此图形。

如果已用 Snapshot 容量超过 Snapshot 预留，则这两个图形都会显示 Snapshot 容量超过 Snapshot 预留的容量。

- * 云层 *

显示已启用 FabricPool 的聚合的云层中数据使用的空间。FabricPool 可以是已获得许可的，也可以是未获得许可的。

当云层镜像到另一个云提供程序（"m 镜像层"）时，此处将同时显示这两个云层。

- * 详细信息 *

显示有关容量的详细信息。

- Total capacity

显示聚合中的总容量。

- 数据容量

显示聚合使用的空间量（已用容量）和聚合中的可用空间量（可用容量）。

- Snapshot 预留

显示聚合的已用 Snapshot 容量和可用 Snapshot 容量。

- 已过量使用容量

显示聚合过量使用。聚合过量使用可以提供比给定聚合实际可用的存储更多的存储，前提是当前并未使用该存储中的所有存储。使用精简配置时，聚合中卷的总大小可能会超过聚合的总容量。



如果已过量使用聚合，则必须仔细监控其可用空间，并根据需要添加存储，以避免因空间不足而导致写入错误。

- 云层

显示已启用 FabricPool 的聚合的云层中数据使用的空间。FabricPool 可以是已获得许可的，也可以是未获得许可的。当云层镜像到另一个云提供程序（镜像层）时，此处将显示这两个云层

- 总缓存空间

显示添加到 Flash Pool 聚合的固态驱动器（SSD）或分配单元的总空间。如果已为聚合启用 Flash Pool，但尚未添加任何 SSD，则缓存空间将显示为 0 KB。



如果为聚合禁用了 Flash Pool，则此字段将处于隐藏状态。

- 聚合阈值

显示以下聚合容量阈值：

- 接近全满阈值

指定聚合接近全满时的百分比。

- 全满阈值

指定聚合已满时的百分比。

- 接近过量提交阈值

指定聚合接近过量使用时的百分比。

- 过量提交阈值

指定过量使用聚合时的百分比。

- 其他详细信息：每日增长率

如果最后两个样本之间的更改率持续 24 小时，则显示聚合中使用的磁盘空间。

例如，如果聚合在下午 2 点使用 10 GB 磁盘空间，在下午 6 点使用 12 GB 磁盘空间，则此聚合的每日增长率（GB）为 2 GB。

- 卷移动

显示当前正在进行的卷移动操作的数量：

- 卷出

显示要从聚合中移出的卷的数量和容量。

您可以单击此链接以查看更多详细信息，例如卷名称，卷要移动到的聚合，卷移动操作的状态以及估计结束时间。

- 卷

显示要移入聚合的卷的数量和剩余容量。

您可以单击此链接查看更多详细信息，例如卷名称，从中移动卷的聚合，卷移动操作的状态以及估计结束时间。

- 卷移动后的估计已用容量

显示卷移动操作完成后聚合中的估计已用空间量（以百分比以及 KB，MB，GB 等单位）。

- * 容量概述 - 卷 *

显示提供聚合中所含卷容量信息的图形。此时将显示卷使用的空间量（已用容量）和卷中的可用空间量（可用容量）。为精简配置卷生成 "精简配置卷空间存在风险" 事件时，将显示卷已用空间量（已用容量）以及卷中可用但由于聚合容量问题而无法使用的空间量（不可用容量）。

您可以从下拉列表中选择要查看的图形。您可以对图形中显示的数据进行排序，以显示已用大小，已配置大小，可用容量，最快的每日增长率和最慢的增长率等详细信息。您可以根据聚合中包含卷的 Storage Virtual Machine（SVM）筛选数据。您还可以查看精简配置卷的详细信息。您可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。默认情况下，此图显示聚合中筛选的前 30 个卷。

磁盘信息选项卡

显示有关选定聚合中磁盘的详细信息，包括 RAID 类型和大小以及聚合中使用的磁盘类型。此选项卡还会以图形方式显示 RAID 组以及使用的磁盘类型（例如 SAS，ATA，FCAL，SSD 或 VMDISK）。您可以通过将光标置于奇偶校验磁盘和数据磁盘上方来查看更多信息，例如磁盘的托架，磁盘架和旋转速度。

- * 数据 *

以图形方式显示有关专用数据磁盘，共享数据磁盘或这两者的详细信息。如果数据磁盘包含共享磁盘，则会显示共享磁盘的图形详细信息。如果数据磁盘包含专用磁盘和共享磁盘，则会显示专用数据磁盘和共享数据磁盘的图形详细信息。

- * RAID 详细信息 *

仅显示专用磁盘的 RAID 详细信息。

- Type

显示 RAID 类型（RAID0，RAID4，RAID-DP 或 RAID-TEC）。

- 组大小

显示 RAID 组中允许的最大磁盘数。

- 组

显示聚合中的 RAID 组数量。

- * 已用磁盘 *

- 有效类型

显示数据磁盘的类型（例如 ATA，SATA，FCAL，SSD，或 VMDISK）。

- 数据磁盘

显示分配给聚合的数据磁盘的数量和容量。如果聚合仅包含共享磁盘，则不会显示数据磁盘详细信息。

- 奇偶校验磁盘

显示分配给聚合的奇偶校验磁盘的数量和容量。如果聚合仅包含共享磁盘，则不会显示奇偶校验磁盘详细信息。

- 共享磁盘

显示分配给聚合的共享数据磁盘的数量和容量。只有当聚合包含共享磁盘时，才会显示共享磁盘详细信息。

- * 备用磁盘 *

显示可供选定聚合中的节点使用的备用数据磁盘的磁盘有效类型，数量和容量。



当聚合故障转移到配对节点时， Unified Manager 不会显示与该聚合兼容的所有备用磁盘。

- * SSD 缓存 *

提供有关专用缓存 SSD 磁盘和共享缓存 SSD 磁盘的详细信息。

此时将显示专用缓存 SSD 磁盘的以下详细信息：

- * RAID 详细信息 *

- Type

显示 RAID 类型（ RAID0 ， RAID4 ， RAID-DP 或 RAID-TEC ）。

- 组大小

显示 RAID 组中允许的最大磁盘数。

- 组

显示聚合中的 RAID 组数量。

- * 已用磁盘 *

- 有效类型

指示聚合中用于缓存的磁盘类型为 SSD 。

- 数据磁盘

显示分配给聚合以进行缓存的数据磁盘的数量和容量。

- 奇偶校验磁盘

显示分配给聚合以进行缓存的奇偶校验磁盘的数量和容量。

- * 备用磁盘 *

显示可供选定聚合中节点用于缓存的备用磁盘的磁盘有效类型，数量和容量。



当聚合故障转移到配对节点时， Unified Manager 不会显示与该聚合兼容的所有备用磁盘。

提供共享缓存的以下详细信息：

- * 存储池 *

显示存储池的名称。您可以将指针移动到存储池名称上方以查看以下详细信息：

- Status

显示存储池的状态，可以是运行状况良好或运行状况不正常。

- 总分配量

显示存储池中的总分配单元和大小。

- 分配单元大小

显示存储池中可分配给聚合的最小空间量。

- Disks

显示用于创建存储池的磁盘数。如果存储池列中的磁盘数与该存储池的磁盘信息选项卡中显示的磁盘数不匹配，则表示一个或多个磁盘已损坏，并且存储池运行状况不正常。

- 已用分配

显示聚合使用的分配单元的数量和大小。您可以单击聚合名称以查看聚合详细信息。

- 可用分配

显示可用于节点的分配单元的数量和大小。您可以单击节点名称以查看聚合详细信息。

- * 已分配缓存 *

显示聚合使用的分配单元的大小。

- * 分配单元 *

显示聚合使用的分配单元数。

- * 磁盘 *

显示存储池中包含的磁盘数。

- * 详细信息 *

- 存储池

显示存储池的数量。

- 总大小

显示存储池的总大小。

- * 云层 *

如果已配置启用了 FabricPool 的聚合，则显示云层的名称，并显示已用总空间。当云层镜像到另一个云提供程序（镜像层）时，此处将显示这两个云层的详细信息

配置选项卡

配置选项卡可显示有关选定聚合的详细信息，例如集群节点，块类型，RAID 类型，RAID 大小和 RAID 组计数：

- * 概述 *

- Node

显示包含选定聚合的节点的名称。

- 块类型

显示聚合的块格式： 32 位或 64 位。

- RAID 类型

显示 RAID 类型（ RAID0 ， RAID4 ， RAID-DP ， RAID-TEC 或混合 RAID ）。

- RAID 大小

显示 RAID 组的大小。

- RAID 组

显示聚合中的 RAID 组数量。

- Snaplock type

显示聚合的 SnapLock 类型。

- * 云层 *

如果这是启用了 FabricPool 的聚合，则会显示云层的详细信息。某些字段因存储提供程序而异。当云层镜像到另一个云提供程序（ "m 镜像层" ）时，此处将同时显示这两个云层。

- 提供程序

显示存储提供程序的名称，例如 StorageGRID ， Amazon S3 ， IBM 云对象存储， Microsoft Azure Cloud ， Google Cloud Storage 或 Alibaba Cloud 对象存储。

- Name

显示云层由 ONTAP 创建时的名称。

- 服务器

显示云层的 FQDN 。

- Port

用于与云提供商通信的端口。

- 访问密钥或帐户

显示云层的访问密钥或帐户。

- 容器名称

显示云层的分段或容器名称。

- SSL

显示是否为云层启用 SSL 加密。

历史记录区域

历史记录区域显示的图形提供了有关选定聚合容量的信息。此外，您还可以单击 * 导出 * 按钮为正在查看的图表创建 CSV 格式的报告。

您可以从历史记录窗格顶部的下拉列表中选择一种图形类型。您还可以选择 1 周，1 个月或 1 年来查看特定时间段的详细信息。历史记录图可以帮助您确定趋势：例如，如果聚合使用量持续违反接近全满阈值，您可以采取相应的措施。

历史记录图显示以下信息：

- * 已用聚合容量 (%) *

在纵轴 (y) 上以折线图的形式显示聚合中的已用容量以及基于使用情况历史记录使用聚合容量的趋势 (以百分比表示)。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已用容量 " 图例时，" 已用容量 " 图形线将处于隐藏状态。

- * 已用聚合容量与总容量 *

以折线图的形式，根据使用情况历史记录显示聚合容量的使用趋势，以及已用容量和总容量，以字节，千字节，兆字节为单位，在垂直 (y) 轴上，依此类推。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已用趋势容量 " 图例时，" 已用趋势容量 " 图形线将处于隐藏状态。

- * 已用聚合容量 (%) 与已提交容量 (%) *

在纵轴 (y) 上以折线图的形式显示基于使用情况历史记录使用聚合容量的趋势，以及已提交空间。时间段显示在水平 (x) 轴上。您可以选择一周，一个月或一年的时间段。您可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击 " 已提交空间 " 图例时，" 已提交空间 " 图形线将处于隐藏状态。

事件列表

事件列表显示有关新事件和已确认事件的详细信息：

- * 严重性 *

显示事件的严重性。

- * 事件 *

显示事件名称。

- * 触发时间 *

显示自事件生成以来经过的时间。如果经过的时间超过一周，则会显示生成事件的时间戳。

相关设备窗格

" 相关设备 " 窗格可用于查看与聚合相关的集群节点，卷和磁盘：

- 节点

显示包含聚合的节点的容量和运行状况。Capacity 表示总可用容量超过可用容量。

- 节点中的 * 聚合 *

显示包含选定聚合的集群节点中所有聚合的数量和容量。此外，还会根据最高严重性级别显示聚合的运行状况。例如，如果集群节点包含十个聚合，其中五个聚合显示 " 警告 " 状态，其余五个聚合显示 " 严重 " 状态，则显示的状态为 " 严重 "。

- * 卷 *

显示聚合中 FlexVol 卷和 FlexGroup 卷的数量和容量；此数量不包括 FlexGroup 成分卷。此外，还会根据最高严重性级别显示卷的运行状况。

- * 资源池 *

显示与聚合相关的资源池。

- * 磁盘 *

显示选定聚合中的磁盘数。

相关警报窗格

" 相关警报 " 窗格可用于查看为选定聚合创建的警报列表。您也可以通过单击添加警报链接来添加警报，或者通过单击警报名称来编辑现有警报。

添加用户

您可以使用用户页面添加本地用户或数据库用户。您还可以添加属于身份验证服务器的远程用户或组。您可以为这些用户分配角色，并且根据这些角色的权限，用户可以使用 Unified Manager 管理存储对象和数据，或者查看数据库中的数据。

开始之前

- 您必须具有应用程序管理员角色。
- 要添加远程用户或组，必须已启用远程身份验证并配置身份验证服务器。
- 如果您计划配置 SAML 身份验证，以便身份提供程序（Identity Provider，IdP）对访问图形界面的用户进行身份验证，请确保将这些用户定义为 remote 用户。

启用 SAML 身份验证后，类型为 "local" 或 "m维护" 的用户不允许访问此 UI。

关于此任务

如果从 Windows Active Directory 添加组，则所有直接成员和嵌套子组都可以通过 Unified Manager 的身份验证，除非禁用嵌套子组。如果从 OpenLDAP 或其他身份验证服务添加组，则只有该组的直接成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 用户 *。
2. 在*用户*页面上、单击*添加*。
3. 在*添加用户*对话框中、选择要添加的用户类型、然后输入所需信息。

输入所需的用户信息时，您必须指定该用户唯一的电子邮件地址。您必须避免指定由多个用户共享的电子邮件地址。

4. 单击 * 添加 *。

创建数据库用户

要支持在 Workflow Automation 和 Unified Manager 之间建立连接或访问数据库视图，您必须先要在 Unified Manager Web UI 中创建一个具有集成架构或报告架构角色的数据库用户。

开始之前

您必须具有应用程序管理员角色。

关于此任务

数据库用户可与 Workflow Automation 集成并访问特定于报告的数据库视图。数据库用户无权访问 Unified Manager Web UI 或维护控制台，无法执行 API 调用。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 用户 *。
2. 在*用户*页面中、单击*添加*。
3. 在*添加用户*对话框的*类型*下拉列表中选择*数据库用户*。
4. 键入数据库用户的名称和密码。
5. 在 * 角色 * 下拉列表中，选择相应的角色。

如果您 ...	选择此角色
将 Unified Manager 与 Workflow Automation 连接起来	集成架构
访问报告和其他数据库视图	报告架构

6. 单击 * 添加 *。

用户类型的定义

用户类型指定用户持有的帐户类型，其中包括远程用户，远程组，本地用户，数据库用户和维护用户。其中每种类型都有自己的角色，该角色由具有管理员角色的用户分配。

Unified Manager 用户类型如下：

- * 维护用户 *

在 Unified Manager 的初始配置期间创建。然后，维护用户创建其他用户并分配角色。维护用户也是唯一有权访问维护控制台的用户。如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 CentOS 系统上，维护用户将获得用户名 "umadmin."

- * 本地用户 *

访问 Unified Manager 用户界面并根据维护用户或具有应用程序管理员角色的用户提供的角色执行功能。

- * 远程组 *

使用身份验证服务器上存储的凭据访问 Unified Manager UI 的一组用户。此帐户的名称应与身份验证服务器上存储的组的名称匹配。远程组中的所有用户均可使用其个人用户凭据访问 Unified Manager UI。远程组可以根据其分配的角色执行功能。

- * 远程用户 *

使用身份验证服务器上存储的凭据访问 Unified Manager UI。远程用户根据维护用户或具有应用程序管理员角色的用户提供的角色执行功能。

- * 数据库用户 *

对 Unified Manager 数据库中的数据具有只读访问权限，无法访问 Unified Manager Web 界面或维护控制台，并且无法执行 API 调用。

Unified Manager 用户角色和功能

根据您分配的用户角色，您可以确定可以在 Unified Manager 中执行的操作。

下表显示了每个用户角色可以执行的功能：

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
查看存储系统信息	•	•	•	•	•
查看其他数据，例如历史记录和容量趋势	•	•	•	•	•

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
查看，分配和解决事件	•	•	•		
查看存储服务对象，例如 SVM 关联和资源池	•	•	•		
查看阈值策略	•	•	•		
管理存储服务对象，例如 SVM 关联和资源池		•	•		
定义警报		•	•		
管理存储管理选项		•	•		
管理存储管理策略		•	•		
管理用户			•		
管理管理选项			•		
定义阈值策略			•		
管理数据库访问			•		
管理与 WFA 的集成，并提供对数据库视图的访问权限				•	
计划并保存报告		•	•		
从管理操作执行 "修复" 操作		•	•		
提供对数据库视图的只读访问权限					•

生成 HTTPS 安全证书

首次安装 Active IQ Unified Manager 时，将安装默认 HTTPS 证书。您可以生成一个新的 HTTPS 安全证书来替换现有证书。

开始之前

您必须具有应用程序管理员角色。

关于此任务

重新生成证书的原因可能有多种，例如您希望为可分辨名称（Distinguished Name，DN）设置更好的值，或者您希望增加密钥大小或延长到期期限，或者当前证书已过期。

如果您无法访问 Unified Manager Web UI，则可以使用维护控制台使用相同的值重新生成 HTTPS 证书。在重新生成证书时，您可以定义密钥大小和密钥的有效期。如果您使用 Reset Server Certificate 选项，则会创建一个新的 HTTPS 证书，此证书的有效期为 397 天。此证书的 RSA 密钥大小为 2048 位。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 *。
2. 单击 * 重新生成 HTTPS 证书 *。

此时将显示重新生成 HTTPS 证书对话框。

3. 根据要生成证书的方式，选择以下选项之一：

如果您要 ...	执行此操作 ...
使用当前值重新生成证书	单击 * 使用当前证书属性重新生成 * 选项。

如果您要 ...	执行此操作 ...
使用不同的值生成证书	<p>单击 * 更新当前证书属性 * 选项。</p> <p>如果不输入新值，"公用名"和"备用名称"字段将使用现有证书中的值。应将"Common Name"设置为主机的 FQDN。其他字段不需要值，但您可以输入电子邮件，公司，部门，城市，省 / 自治区 / 直辖市和国家 / 地区，以便在证书中填充这些值。您也可以从可用密钥大小（密钥算法为 "RSA"）和有效期中进行选择。</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"></p> <ul style="list-style-type: none"> 允许的密钥大小值为 2048，3072 和 4096。 有效期至少为 1 天，最多为 36500 天。 <p>即使允许使用 36500 天的有效期，建议您使用的有效期不超过 397 天或 13 个月。由于如果您选择的有效期超过 397 天，并计划导出此证书的 CSR 并使其由知名 CA 签名，则此 CA 返回给您的签名证书的有效期将缩短为 397 天。</p> <ul style="list-style-type: none"> 如果要从证书的"备用名称"字段中删除本地标识信息、可以选中"排除本地标识信息"复选框。选中此复选框后，备用名称字段将仅使用您在字段中输入的内容。如果留空，则生成的证书将根本没有备用名称字段。 </div>

- 单击 * 是 * 重新生成证书。
- 重新启动 Unified Manager 服务器，以使新证书生效。

完成后

通过查看 HTTPS 证书来验证新证书信息。

支持的 Unified Manager 命令行界面命令

作为存储管理员，您可以使用命令行界面命令对存储对象执行查询，例如，对集群，聚合，卷，qtree 和 LUN。您可以使用命令行界面命令查询 Unified Manager 内部数据库和 ONTAP 数据库。您还可以在操作开始或结束时执行或触发警报时执行的脚本中使用 CLI 命令。

所有命令都必须在前面加上命令 `um cli login` 以及用于身份验证的有效用户名和密码。

CLI 命令	Description	输出
<code>um cli login -u <username> [-p <password>]</code>	登录到命令行界面。由于安全影响、您应仅在"-u"选项后面输入用户名。以这种方式使用时，系统将提示您输入密码，并且密码不会捕获到历史记录或进程表中。会话将在自登录后三个小时后过期，之后用户必须重新登录。	显示相应的消息。

CLI 命令	Description	输出
um cli logout	从命令行界面注销。	显示相应的消息。
um help	显示所有第一级子命令。	显示所有第一级子命令。
um run cmd [-t <timeout>] <cluster> <command>	在一个或多个主机上运行命令的最简单方法。主要用于编写警报脚本，以便在 ONTAP 上获取或执行操作。可选超时参数用于设置命令在客户端上完成的最长时间限制（以秒为单位）。默认值为 0（永久等待）。	与从 ONTAP 收到的相同。
um run query <sql command>	执行 SQL 查询。仅允许从数据库读取的查询。不支持任何更新，插入或删除操作。	结果以表格形式显示。如果返回空集，或者存在任何语法错误或请求错误，则会显示相应的错误消息。
um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip>	将数据源添加到受管存储系统列表中。数据源介绍了如何连接到存储系统。添加数据源时，必须指定选项 -u（用户名）和 -P（密码）。选项 -t（protocol）指定用于与集群通信的协议（http 或 https）。如果未指定协议，则会尝试使用这两种协议选项 -p（port）指定用于与集群通信的端口。如果未指定端口，则会尝试使用相应协议的默认值。此命令只能由存储管理员执行。	提示用户接受证书并显示相应的消息。
um datasource list [<datasource-id>]	显示受管存储系统的数据源。	以表格形式显示以下值：ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message。
um datasource modify [-h <hostname-or-ip>] [-u <username>] [-P <password>] [-t <protocol>] [-p <port>] <datasource-id>	修改一个或多个数据源选项。只能由存储管理员执行。	显示相应的消息。
um datasource remove <datasource-id>	从 Unified Manager 中删除数据源（集群）。	显示相应的消息。

CLI 命令	Description	输出
um option list [<option> ..]	列出了可使用配置的所有选项 set 命令：	以表格形式显示以下值： Name, Value, Default Value, and Requires Restart.
um option set <option-name>=<option-value> [<option-name>=<option-value> ...]	设置一个或多个选项。此命令只能由存储管理员执行。	显示相应的消息。
um version	显示 Unified Manager 软件版本。	Version ("9.6")
um lun list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的 LUN 。-q 适用于所有命令，用于不显示标题。ObjectType 可以是 lun ， qtree ， cluster ， volume ， quota ， 或 SVM 。例如： um lun list -cluster 1</p> <p>在此示例中， "-cluster" 是 objectType ， "1" 是 objectID 。此命令将列出 ID 为 1 的集群中的所有 LUN 。</p>	以表格形式显示以下值： ID and LUN path。
um svm list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的 Storage VM 。ObjectType 可以是 lun ， qtree ， cluster ， volume ， quota ， 或 SVM 。例如： um svm list -cluster 1</p> <p>在此示例中， "-cluster" 是 objectType ， "1" 是 objectID 。此命令将列出 ID 为 1 的集群中的所有 Storage VM 。</p>	以表格形式显示以下值： Name and Cluster ID。
um qtree list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的 qtree 。-q 适用于所有命令，用于不显示标题。ObjectType 可以是 lun ， qtree ， cluster ， volume ， quota ， 或 SVM 。例如： um qtree list -cluster 1</p> <p>在此示例中， "-cluster" 是 objectType ， "1" 是 objectID 。此命令将列出 ID 为 1 的集群中的所有 qtree 。</p>	以表格形式显示以下值： Qtree ID and Qtree Name。

CLI 命令	Description	输出
um disk list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的磁盘。ObjectType 可以是 disk, aggr, node 或 cluster。例如： um disk list -cluster 1</p> <p>在此示例中，"-cluster" 是 objectType, "1" 是 objectID。此命令将列出 ID 为 1 的集群中的所有磁盘。</p>	以表格形式显示以下值 ObjectType and object-id.
um cluster list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的集群。ObjectType 可以是 disk, aggr, node, cluster, lun, qtree, 卷, 配额或 SVM。例如： um cluster list -aggr 1</p> <p>在此示例中，"-aggr" 是 objectType, "1" 是 objectID。此命令将列出 ID 为 1 的聚合所属的集群。</p>	以表格形式显示以下值: Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.
um cluster node list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的集群节点。ObjectType 可以是 disk, aggr, node 或 cluster。例如： um cluster node list -cluster 1</p> <p>在此示例中，"-cluster" 是 objectType, "1" 是 objectID。此命令将列出 ID 为 1 的集群中的所有节点。</p>	以表格形式显示以下值 Name and Cluster ID.
um volume list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的卷。ObjectType 可以是 lun, qtree, cluster, volume, quota, SVM 或聚合。例如: um volume list -cluster 1</p> <p>在此示例中，"-cluster" 是 objectType, "1" 是 objectID。此命令将列出 ID 为 1 的集群中的所有卷。</p>	以表格形式显示以下值 Volume ID and Volume Name.

CLI 命令	Description	输出
um quota user list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的配额用户。ObjectType 可以是 qtree , cluster , volume , quota 或 SVM 。例如: um quota user list -cluster 1</p> <p>在此示例中, "-cluster" 是 objectType , "1" 是 objectID 。此命令将列出 ID 为 1 的集群中的所有配额用户。</p>	以表格形式显示以下值 ID, Name, SID and Email.
um aggr list [-q] [-ObjectType <object-id>]	<p>列出按指定对象筛选后的聚合。ObjectType 可以是 disk , aggr , node , cluster 或 volume 。例如: um aggr list -cluster 1</p> <p>在此示例中, "-cluster" 是 objectType , "1" 是 objectID 。此命令将列出 ID 为 1 的集群中的所有聚合。</p>	以表格形式显示以下值 Aggr ID, and Aggr Name.
um event ack <event-ids>	确认一个或多个事件。	显示相应的消息。
um event resolve <event-ids>	解决一个或多个事件。	显示相应的消息。
um event assign -u <username> <event-id>	将事件分配给用户。	显示相应的消息。
um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]	列出系统或用户生成的事件。根据源, 状态和 ID 筛选事件。	以表格形式显示以下值 Source, Source type, Name, Severity, State, User and Timestamp.
um backup restore -f <backup_file_path_and_name >	使用 .7z 文件还原 MySQL 数据库备份。	显示相应的消息。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。