管理事件和警报

Active IQ Unified Manager

NetApp
January 15, 2026

目录

管理事件和警报

管理活动

事件可帮助您确定受监控集群中的问题。

什么是 **Active IQ** 平台事件

Unified Manager 可以显示 Active IQ 平台发现的事件。这些事件是通过对 Unified Manager 所监控的所有存储系统生成的 AutoSupport 消息运行一组规则来创建的。

有关详细信息，请参见 "如何生成 Active IQ 平台事件"。

Unified Manager 会自动检查新规则文件，只有在存在较新规则时才会下载新文件。在无法访问外部网络的站点中，您需要从 * 存储管理 * > * 事件设置 * > * 上传规则 * 手动上传规则。

这些 Active IQ 事件不会与现有 Unified Manager 事件重叠，它们可确定与系统配置，布线，最佳实践和可用性问题相关的意外事件或风险。

有关启用平台事件的详细信息，请参见 "启用 Active IQ 门户事件"。有关上传规则文件的详细信息，请参见 "上传新的 Active IQ 规则文件"。

NetApp Active IQ 是一项基于云的服务，可提供预测性分析和主动式支持，以优化 NetApp 混合云中的存储系统操作。请参见 "NetApp Active IQ" 有关详细信息 …

什么是事件管理系统事件

事件管理系统（ EMS ）从 ONTAP 内核的不同部分收集事件数据，并提供事件转发机制。这些 ONTAP 事件可以在 Unified Manager 中报告为 EMS 事件。集中式监控和管理可简化根据这些 EMS 事件配置关键 EMS 事件和警报通知的过程。

将集群添加到 Unified Manager 时， Unified Manager 地址将作为通知目标添加到集群中。一旦集群中发生 EMS 事件，就会报告该事件。

在 Unified Manager 中接收 EMS 事件的方法有两种：

- 系统会自动报告一定数量的重要 EMS 事件。
- 您可以订阅以接收单个 EMS 事件。

根据 Unified Manager 生成 EMS 事件的方法，报告此事件的方式会有所不同：

功能	自动 **EMS** 消息	已订阅 **EMS** 消息
可用 EMS 事件	EMS 事件的子集	所有 EMS 事件

功能	自动 **EMS** 消息	已订阅 **EMS** 消息
触发的 EMS 消息名称	Unified Manager 事件名称（从 EMS 事件名称转换而来）	格式为 " 收到错误 EMS " 的非特定格式。详细消息提供了实际 EMS 事件的点表示法
收到的消息	发现集群后立即执行	将每个必需的 EMS 事件添加到 Unified Manager 之后，以及下一个 15 分钟轮询周期之后
事件生命周期	与其他 Unified Manager 事件相同：" 新增 "，" 已确认 "，" 已解决 " 和 " 已废弃 " 状态	自事件创建之日起 15 分钟后刷新集群后， EMS 事件将变为废弃
捕获 Unified Manager 停机期间的事件	可以，系统启动后，它会与每个集群通信以获取缺少的事件	否
事件详细信息	建议的更正操作直接从 ONTAP 导入，以提供一致的解决方案	" 事件详细信息 " 页面中未提供更正操作

某些新的自动 EMS 事件属于信息性事件，表示先前的事件已解决。例如，" FlexGroup 成分卷空间状态一切正常 " 信息事件表示 " FlexGroup 成分卷存在空间问题 " 错误事件已解决。无法使用与其他事件严重性类型相同的事件生命周期来管理信息性事件，但是，如果同一卷收到另一个 " `Space issues` " 错误事件，则此事件将自动废弃。

自动添加到 **Unified Manager** 的 **EMS** 事件

以下 ONTAP EMS 事件将自动添加到 Unified Manager 中。如果在 Unified Manager 监控的任何集群上触发这些事件，则会生成这些事件。

在监控运行 ONTAP 9.5 或更高版本软件的集群时，可以使用以下 EMS 事件：

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
聚合重新定位时，云层访问被拒绝	arl.netra.ca.check.failed	聚合	error
在存储故障转移期间，用于聚合重新定位的云层访问被拒绝	gb.netra.ca.check.failed	聚合	error
FabricPool 镜像复制重新同步已完成	wafl.ca.resync.complete	集群	error
FabricPool 空间接近全满	fabricpool.nNearly.full	集群	error

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
NVMe-oF 宽限期已开始	nvmf.graceperiod.start	集群	警告
NVMe-oF 宽限期处于活动状态	nvmf.graceperiod.active	集群	警告
NVMe-oF 宽限期已过期	nvmf.graceperiod.expired	集群	警告
LUN 已销毁	lun.destroy	LUN	信息
Cloud AWS MetaDataConnFail	cloud 。aws.metadataConnFail	Node	error
Cloud AWS IAMCredsExpired	cloud 。aws.iamCredsExpire	Node	error
Cloud AWS IAMCredsInvalid	cloud 。aws.iamCredsInvalid	Node	error
Cloud AWS IAMCredsNotFound	cloud 。aws.iamCredsNotFound	Node	error
Cloud AWS IAMCredsNotInitialized	cloud 。aws.iamNotInitialized	Node	信息
Cloud AWS IAMRoleInvalid	cloud 。aws.iamRoleInvalid	Node	error
Cloud AWS IAMRoleNotFound	cloud 。aws.iamRoleNotFound	Node	error
无法解析云层主机	objstore.host.unresolvable	Node	error
云层集群间网络接口已关闭	objstore.interclusterlifDown	Node	error
请求不匹配云层签名	OSC.signatureMismatch	Node	error
其中一个 NFSv4 池已用尽	nblade.nfsV4PoolExhaust	Node	严重
QoS 监控内存已达到上限	qos.monitor.memory.maxed	Node	error

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
QoS 监控器内存已减少	qos.monitor.memory.abated	Node	信息
NVMeNS 销毁	NVMeNS.destroy	命名空间	信息
NVMeNS Online	NVmeNS.offline	命名空间	信息
NVMeNS 脱机	NVmeNS.online	命名空间	信息
NVMeNS 空间不足	nvmens.out 。 space	命名空间	警告
同步复制不同步	sms.status.out	SnapMirror 关系	警告
同步复制已还原	sms.status.in.sync	SnapMirror 关系	信息
同步复制自动重新同步失败	sms.resync.Attempt.failed	SnapMirror 关系	error
多个 CIFS 连接	nblade.cifsManyAss	SVM	error
已超过最大 CIFS 连接数	nblade.cifsMaxOpenSameFile	SVM	error
已超过每个用户的最大 CIFS 连接数	nblade.cifsMaxSessPerUsrConn	SVM	error
CIFS NetBIOS 名称冲突	nblade.cifsNbNameConflict	SVM	error
尝试连接不存在的 CIFS 共享	nblade.cifsNoPrivShare	SVM	严重
CIFS 卷影复制操作失败	CIFS.ShadowCopy.Failure	SVM	error
AV 服务器发现病毒	已检测 Nblade.vscanVirusDetened.	SVM	error
没有用于病毒扫描的 AV 服务器连接	nblade.vscanNoScannerConn	SVM	严重

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重性
未注册 AV 服务器	nblade.vscanNoRegd扫描程序	SVM	error
AV 服务器连接无响应	nblade.vscanConnInactive.	SVM	信息
AV 服务器太忙，无法接受新扫描请求	nblade.vscanConnBackPressure	SVM	error
未经授权的用户尝试访问 AV 服务器	nblade.vscanBadUserPrivAccess	SVM	error
FlexGroup 成分卷存在空间问题	flexgroup.constitutions.have .space.issues	Volume	error
FlexGroup 成分卷空间状态一切正常	flexgroup.constitutions.space.status.all.ok	Volume	信息
FlexGroup 成分卷存在索引节点问题	flexgroup.constituents.have.inodes.issues	Volume	error
FlexGroup 成分卷索引节点状态一切正常	flexgroup.constituents.inodes.status.all.ok	Volume	信息
卷逻辑空间接近全满	monitor.vol.nearFull.inc.sav	Volume	警告
卷逻辑空间已满	monitor.vol.full.inc.sav	Volume	error
卷逻辑空间正常	monitor.vol.one.ok.inc.sav	Volume	信息
WAFL 卷自动调整大小失败	wafl.vol.autoSize.fail	Volume	error
WAFL 卷自动调整大小已完成	wafl.vol.autoSize.done	Volume	信息
WAFL READDIR 文件操作超时	wafl.readdir.expired.	Volume	error

订阅 **ONTAP EMS** 活动

您可以订阅接收由安装了 ONTAP 软件的系统生成的事件管理系统（ EMS ）事件。系统会

自动向 Unified Manager 报告一部分 EMS 事件，但只有在订阅这些事件后，才会报告其他 EMS 事件。

开始之前

请勿订阅已自动添加到 Unified Manager 的 EMS 事件，因为这可能会在收到同一问题描述的两个事件时造成发生原因混淆。

您可以订阅任意数量的 EMS 事件。您订阅的所有事件都会经过验证，并且只有经过验证的事件才会应用于您在 Unified Manager 中监控的集群。_EMS ONTAP 9 事件目录 _ 提供指定版本 ONTAP 9 软件的所有 EMS 消息的详细信息。有关适用事件的列表，请从 ONTAP 9 产品文档页面找到 _EMS 事件目录 _ 的相应版本。

"ONTAP 9 产品库"

您可以为订阅的 ONTAP EMS 事件配置警报，也可以为这些事件创建要执行的自定义脚本。

> 如果您未收到订阅的 ONTAP EMS 事件，则可能存在具有集群 DNS 配置的问题描述，从而阻止集群访问 Unified Manager 服务器。要解决此问题描述，集群管理员必须更正集群的 DNS 配置，然后重新启动 Unified Manager 。这样做会将待定 EMS 事件刷新到 Unified Manager 服务器。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 事件设置 * 。
2. 在 Event Setup 页面中，单击 * 订阅 EMS 事件 * 按钮。
3. 在订阅 EMS 事件对话框中，输入要订阅的 ONTAP EMS 事件的名称。

   要查看可订阅的 EMS 事件的名称，可以从 ONTAP 集群 Shell 使用 `event route show` 命令（ ONTAP 9 之前的版本）或 `event catalog show` 命令（ ONTAP 9 或更高版本）。

   "如何在 Active IQ Unified Manager 中配置和接收 ONTAP EMS 事件订阅的警报"

4. 单击 * 添加 * 。

   EMS 事件将添加到 " 已订阅 EMS 事件 " 列表中，但 " 适用于集群 " 列会将您添加的 EMS 事件的状态显示为 "`未知` " 。

5. 单击 * 保存并关闭 * 向集群注册 EMS 事件订阅。
6. 再次单击 * 订阅 EMS 事件 * 。

   对于您添加的 EMS 事件，状态 "`是` " 将显示在 " 适用于集群 " 列中。

   如果状态不是 "`是` " ，请检查 ONTAP EMS 事件名称的拼写。如果输入的名称不正确，则必须删除不正确的事件，然后重新添加此事件。

发生 ONTAP EMS 事件时，事件将显示在事件页面上。您可以选择事件以在事件详细信息页面中查看有关 EMS 事件的详细信息。您还可以管理事件的处理方式或为事件创建警报。

收到事件时会发生什么情况

Unified Manager 收到事件后，该事件将显示在 " 信息板 " 页面， " 事件管理 " 清单页面， " 集群 / 性能 " 页面的 " 摘要 " 和 " 资源管理器 " 选项卡以及对象特定的清单页面（例如 "

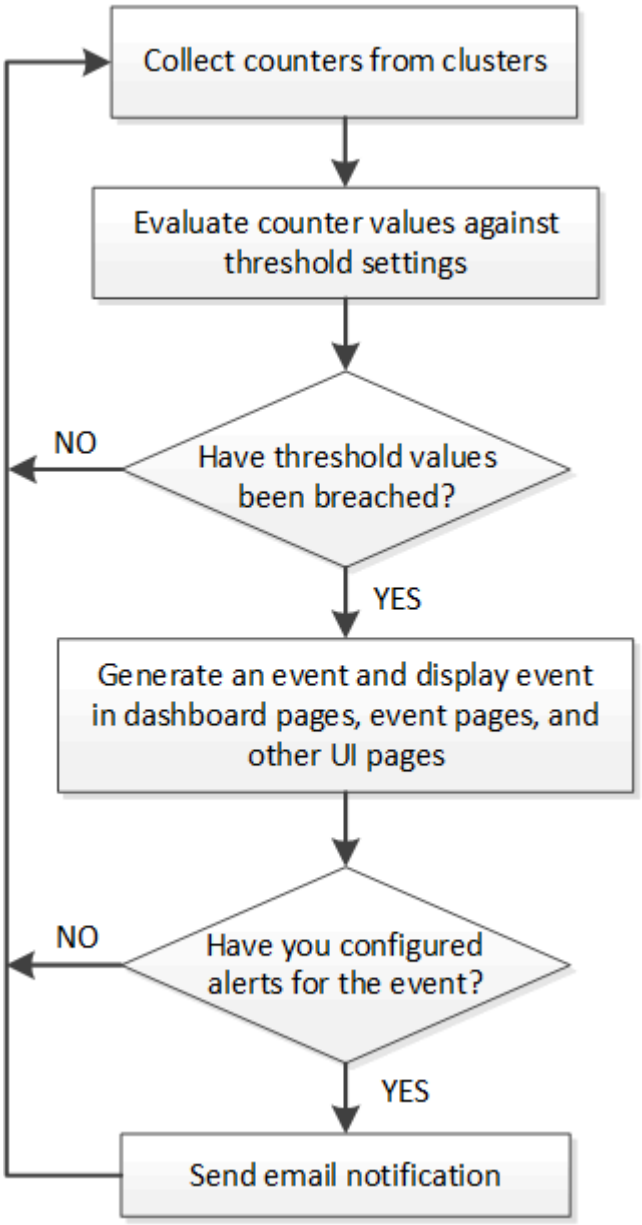
卷 / 运行状况 " 清单页面）中。

如果 Unified Manager 检测到同一集群组件多次连续出现相同的事件条件，则会将所有发生的事件视为单个事件，而不是单独的事件。事件持续时间将递增，表示事件仍处于活动状态。

根据您在 "Alert Setup" 页面中配置设置的方式，您可以向其他用户通知这些事件。此警报将启动以下操作：

- 可以向所有 Unified Manager 管理员用户发送有关此事件的电子邮件。
- 可以将此事件发送给其他电子邮件收件人。
- SNMP 陷阱可以发送到陷阱接收方。
- 可以执行自定义脚本以执行操作。

下图显示了此工作流。



查看活动和活动详情

您可以查看有关 Unified Manager 触发的事件的详细信息以采取更正操作。例如，如果存在运行状况事件 " 卷脱机 " ，则可以单击该事件以查看详细信息并执行更正操作。

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。

事件详细信息包括事件源，事件的发生原因以及与事件相关的任何注释等信息。

步骤

1. 在左侧导航窗格中，单击 * 事件管理 * 。

   默认情况下，所有活动事件视图会显示过去 7 天内生成的影响级别为 " 意外事件 " 或 " 风险 " 的 " 新增 " 和 " 已确认 " （活动）事件。

2. 如果要查看特定类别的事件，例如容量事件或性能事件，请单击 * 查看 * 并从事件类型菜单中选择。
3. 单击要查看其详细信息的事件名称。

   事件详细信息将显示在事件详细信息页面中。

查看未分配的事件

您可以查看未分配的事件，然后将每个事件分配给可以解决这些事件的用户。

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 * 筛选器 * 窗格的 * 已分配给 * 区域中选择 * 未分配 * 筛选器选项。

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。

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	a. 单击事件名称。 b. 在事件详细信息页面中，确定事件的发生原因。 c. 单击 * 确认 * 。 d. 采取适当的更正操作。 e. 单击 * 标记为已解决 * 。
确认多个事件并将其标记为已解决	a. 从相应的事件详细信息页面确定事件的发生原因。 b. 选择事件。 c. 单击 * 确认 * 。 d. 采取适当的更正操作。 e. 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。

3. * 可选 * ： 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 * 。

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 * 。

要将事件分配给 ...	然后执行此操作 ...
其他用户	a. 单击 * 分配给 * > * 其他用户 * 。 b. 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。 c. 单击 * 分配 * 。 系统会向用户发送电子邮件通知。 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。

禁用不需要的事件

默认情况下，所有事件均处于启用状态。您可以全局禁用事件，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，您可以启用这些事件。

开始之前

您必须具有应用程序管理员或存储管理员角色。

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。

如果您禁用某个对象的事件（例如， `vol offline` event ），然后再启用该事件，则 Unified Manager 不会为该事件处于禁用状态时脱机的对象生成新事件。只有在重新启用事件后对象状态发生更改时， Unified Manager 才会生成新事件。

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	a. 单击 * 禁用 * 。 b. 在禁用事件对话框中，选择事件严重性。 c. 在匹配事件列中，根据事件严重性选择要禁用的事件，然后单击右箭头将这些事件移动到禁用事件列。 d. 单击 * 保存并关闭 * 。 e. 验证已禁用的事件是否显示在 Event Setup 页面的列表视图中。

如果您要 ...	然后执行此操作 ...
启用事件	a. 选中要启用的一个或多个事件对应的复选框。 b. 单击 * 启用 * 。

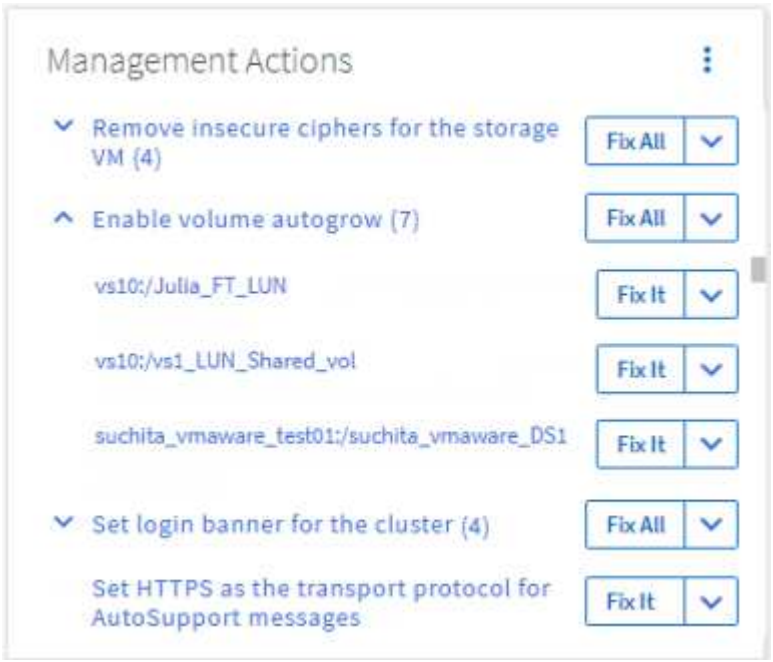
使用 **Unified Manager** 自动修复功能解决问题

Unified Manager 可以对某些事件进行全面诊断，并使用 * 修复它 * 按钮提供单一解决方案。如果可用，这些解决方案将显示在信息板，事件详细信息页面以及左侧导航菜单上的工作负载分析选项中。

大多数事件都有各种可能的解决方案，这些解决方案显示在事件详细信息页面中，因此您可以使用 ONTAP System Manager 或 ONTAP 命令行界面实施最佳解决方案。如果 Unified Manager 已确定修复问题描述需要一个解决方案，并且可以使用 ONTAP 命令行界面命令解决此问题，则可以执行 * 修复它 * 操作。

步骤

1. 要查看可通过 * 信息板 * 修复的事件，请单击 * 信息板 * 。



2. 要解决 Unified Manager 可以修复的任何问题，请单击 * 修复它 * 按钮。要修复多个对象上的问题描述，请单击 * 全部修复 * 按钮。

有关可通过自动修复修复修复的问题的信息，请参见 "Unified Manager 可以修复哪些问题"。

启用和禁用 **Active IQ** 事件报告

默认情况下， Active IQ 平台事件会生成并显示在 Unified Manager 用户界面中。如果发现这些事件太 " 干扰 " ，或者您不想在 Unified Manager 中查看这些事件，则可以禁止生成这些事件。如果您稍后要恢复接收这些通知，可以启用它们。

开始之前

您必须具有应用程序管理员角色。

禁用此功能后， Unified Manager 将立即停止接收 Active IQ 平台事件。

启用此功能后， Unified Manager 将根据集群的时区在午夜后不久开始接收 Active IQ 平台事件。开始时间取决于 Unified Manager 何时从每个集群接收 AutoSupport 消息。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 功能设置 * 。
2. 在 * 功能设置 * 页面中，通过选择以下选项之一禁用或启用 Active IQ 平台事件：

如果您要 ...	然后执行此操作 ...
禁用 Active IQ 平台事件	在 * Active IQ 门户事件 * 面板中，将滑块按钮移至左侧。
启用 Active IQ 平台事件	在 * Active IQ 门户事件 * 面板中，将滑块按钮移至右侧。

上传新的 **Active IQ** 规则文件

Unified Manager会自动检查是否存在新的Active IQ 事件(规则)文件、如果存在较新的规则、则会下载新文件。但是，在无法访问外部网络的站点中，您需要手动上传规则文件。

Active IQ 规则也称为Config Advisor (CA)安全规则。

如果在没有网络连接的站点中安装Unified Manager或将Unified Manager升级到特定版本、则捆绑的Active IQ 规则将自动可上传。但是、建议您大约每月从NetApp支持站点下载一次新的规则文件、以确保生成更新后的事件、并且存储系统仍能以最佳状态运行。

开始之前

- 必须启用Active IQ 门户事件报告。默认情况下，此功能处于启用状态。有关信息，请参见 "启用 Active IQ 门户事件"。
- 您必须从 NetApp 支持站点下载规则文件。

  规则文件位于： https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

步骤

1. 在可访问网络的计算机上，导航到 NetApp 支持站点并下载当前规则 ` .zip` 文件。

   捆绑的规则软件包包括规则存储库、数据源和NetApp知识库文章。

在Windows系统上、在没有网络连接的站点中、NetApp知识库文章默认不会与安装程序捆绑在一起。您可以从支持站点下载_secure rules.zip文件并将其上传、以查看所有规则的知识库文章。

2. 将规则文件传输到可带入安全区域的某些介质，然后将其复制到安全区域的系统。
3. 在左侧导航窗格中，单击 * 存储管理 * > * 事件设置 * 。
4. 在 * 事件设置 * 页面中，单击 * 上传规则 * 按钮。
5. 在 * 上传规则 * 对话框中，导航到您下载的规则 ` .zip` 文件并选择该文件，然后单击 * 上传 * 。

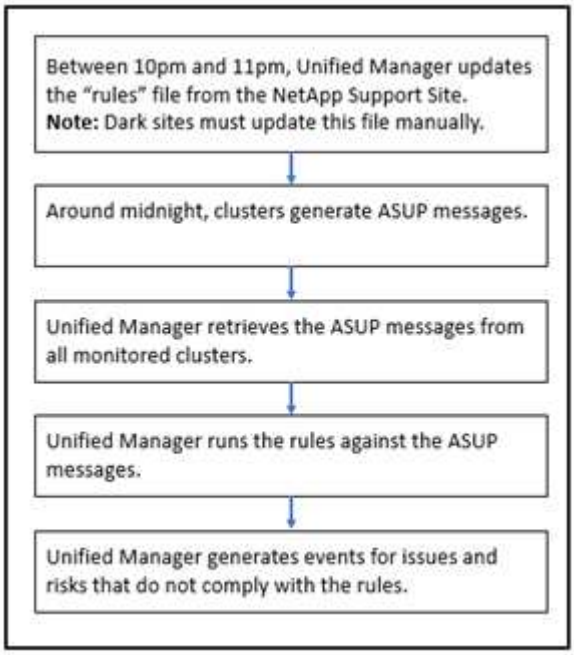
   此过程可能需要几分钟时间。

规则文件将在 Unified Manager 服务器上解压缩。在受管集群在午夜后生成AutoSupport 文件后、Unified Manager将根据规则文件检查集群、并根据需要生成新的风险和意外事件。

有关详细信息、请参见此知识库(KB)文章： "如何在Active IQ Unified Manager 中手动更新AIQCASecure规则"。

如何生成 **Active IQ** 平台事件

Active IQ 平台意外事件和风险会转换为 Unified Manager 事件，如下图所示。

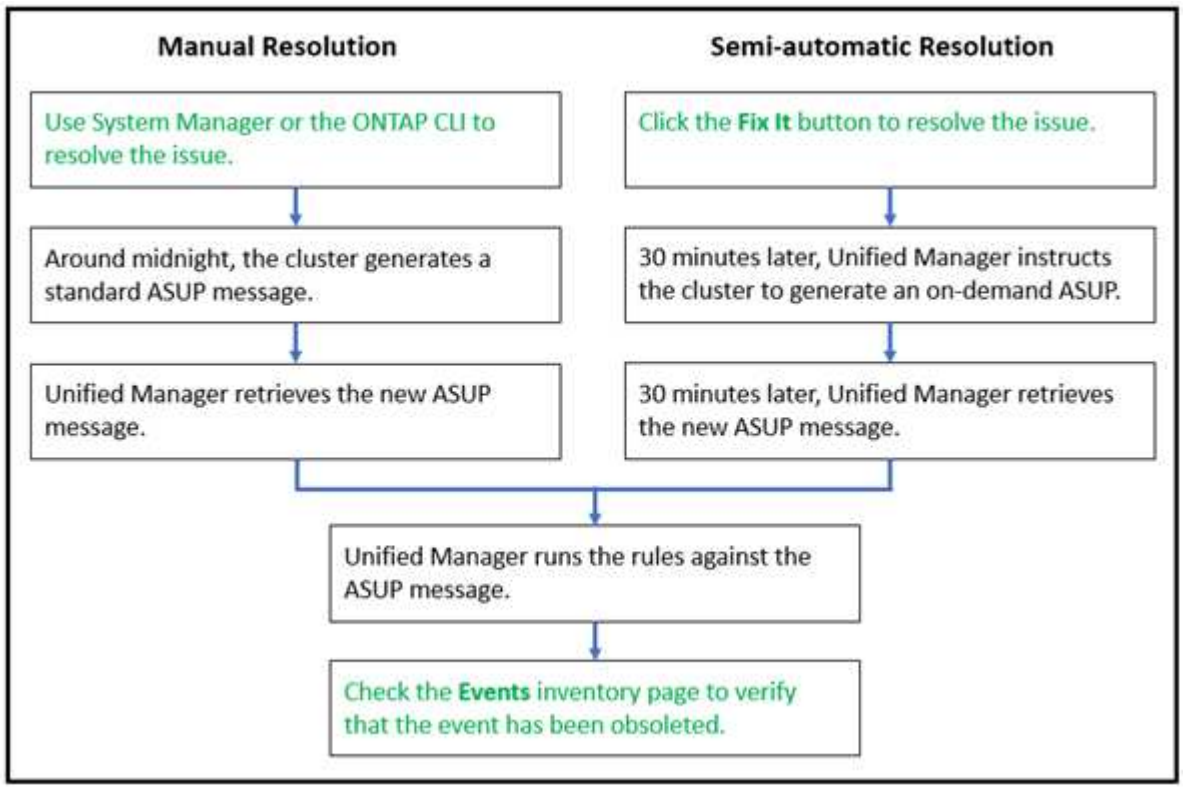


如您所见，在 Active IQ 平台上编译的规则文件将保持最新，并且每天都会生成集群 AutoSupport 消息，并且 Unified Manager 会每天更新事件列表。

解决 **Active IQ** 平台事件

Active IQ 平台意外事件和风险与其他 Unified Manager 事件类似，因为它们可以分配给其他用户进行解决，并且具有相同的可用状态。但是，使用 * 修复它 * 按钮解决这些类型的事件时，您可以在数小时内验证解决方法。

下图显示了在解决从 Active IQ 平台生成的事件时必须执行的操作（绿色）以及 Unified Manager 执行的操作（黑色）。



在执行手动解决方案时，您必须登录到 System Manager 或 ONTAP 命令行界面以修复问题描述。只有在集群在午夜生成新的 AutoSupport 消息后，您才能验证问题描述。

使用 * 修复它 * 按钮执行半自动解决方案时，您可以在数小时内验证修复是否成功。

配置事件保留设置

您可以指定事件在自动删除之前在 Unified Manager 服务器中保留的月数。

开始之前

您必须具有应用程序管理员角色。

将事件保留 6 个月以上可能会影响服务器性能，因此不建议这样做。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 数据保留 * 。
2. 在 * 数据保留 * 页面中，选择事件保留区域中的滑块并将其移动到事件应保留的月数，然后单击 * 保存 * 。

什么是 **Unified Manager** 维护窗口

您可以定义 Unified Manager 维护窗口，以便在已计划集群维护且您不希望收到大量不需要的通知时禁止特定时间范围内的事件和警报。

维护窗口启动后， " 对象维护窗口已启动 " 事件将发布到 " 事件管理 " 清单页面。维护窗口结束时，此事件将自

动废弃。

在维护窗口期间，仍会生成与该集群上的所有对象相关的事件，但这些事件不会显示在任何用户界面页面中，并且不会针对这些事件发送任何警报或其他类型的通知。但是，您可以通过在事件管理清单页面上选择一个视图选项来查看维护窗口期间为所有存储对象生成的事件。

您可以计划将来启动维护窗口，更改计划维护窗口的开始和结束时间以及取消计划维护窗口。

安排维护时段以禁用集群事件通知

如果您为集群计划了停机时间，例如，要升级集群或移动其中一个节点，则可以通过计划 Unified Manager 维护窗口来禁止在该时间段内通常生成的事件和警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

在维护窗口期间，仍会生成与该集群上的所有对象相关的事件，但这些事件不会显示在事件页面中，并且不会针对这些事件发送任何警报或其他类型的通知。

为维护窗口输入的时间取决于 Unified Manager 服务器上的时间。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 集群设置 * 。
2. 在集群的 * 维护模式 * 列中，选择滑块按钮并将其移至右侧。

   此时将显示日历窗口。

3. 选择维护窗口的开始和结束日期和时间，然后单击 * 应用 * 。

   滑块按钮旁边会显示消息 "schedule" 。

达到开始时间后，集群将进入维护模式，并生成 " 对象维护窗口已启动 " 事件。

更改或取消计划的维护时段

如果您已将 Unified Manager 维护窗口配置为将来发生，则可以更改开始和结束时间或取消维护窗口。

开始之前

您必须具有应用程序管理员或存储管理员角色。

如果您在计划的维护窗口结束时间之前完成了集群维护，并且希望重新开始从集群接收事件和警报，则取消当前正在运行的维护窗口非常有用。

步骤

1. 在左侧导航窗格中，单击 * 存储管理 * > * 集群设置 * 。
2. 在集群的 * 维护模式 * 列中：

如果您要 ...	执行此步骤 ...
更改计划维护窗口的时间范围	a. 单击滑块按钮旁边的文本 "schedule" 。 b. 更改开始和 / 或结束日期和时间，然后单击 * 应用 * 。
延长活动维护窗口的长度	a. 单击滑块按钮旁边的文本 "Active" 。 b. 更改结束日期和时间，然后单击 * 应用 * 。
取消计划的维护窗口	选择滑块按钮并将其移至左侧。
取消活动维护窗口	选择滑块按钮并将其移至左侧。

查看维护时段内发生的事件

如有必要，您可以查看 Unified Manager 维护窗口期间为所有存储对象生成的事件。维护窗口完成且所有系统资源均已备份和运行后，大多数事件将显示为 " 已废弃 " 状态。

开始之前

必须至少完成一个维护窗口，才能显示任何事件。

默认情况下，维护窗口期间发生的事件不会显示在事件管理清单页面上。

步骤

1. 在左侧导航窗格中，单击 * 事件 * 。

   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. 从视图窗格中，选择 * 维护期间生成的所有事件 * 选项。

   此时将显示所有维护窗口会话和所有集群在过去 7 天内触发的事件列表。

3. 如果一个集群有多个维护窗口，您可以单击 * 触发时间 * 日历图标并选择要查看的维护窗口事件的时间段。

管理主机系统资源事件

Unified Manager 包含一项服务，用于监控安装了 Unified Manager 的主机系统上的资源问题。主机系统上的可用磁盘空间不足或内存不足等问题可能会触发管理工作站事件，这些事件在用户界面顶部显示为横幅消息。

管理工作站事件表示问题描述与安装 Unified Manager 的主机系统一起运行。管理工作站问题的示例包括：主机系统上的磁盘空间不足； Unified Manager 缺少常规数据收集周期；以及由于启动了下一次收集轮询，统计信息分析未完成或延迟完成。

与所有其他 Unified Manager 事件消息不同，这些特定管理工作站警告和严重事件会显示在横幅消息中。

步骤

1. 要查看管理工作站事件信息，请执行以下操作：

如果您要 ...	执行此操作 ...
查看事件的详细信息	单击事件横幅以显示事件详细信息页面，其中包含为问题描述建议的解决方案。
查看所有管理工作站事件	a. 在左侧导航窗格中，单击 * 事件管理 * 。 b. 在事件管理清单页面的筛选器窗格中，单击源类型列表中的 Management Station 对应的框。

了解更多活动信息

了解事件的概念有助于您高效管理集群和集群对象并正确定义警报。

事件状态定义

事件状态有助于确定是否需要采取适当的更正操作。事件可以是 " 新增 " ， " 已确认 " ， " 已解决 " 或 " 已废弃 " 。请注意，新事件和已确认事件均视为活动事件。

事件状态如下：

- * 新增 *

  新事件的状态。

- * 已确认 *

  确认事件后的状态。

- * 已解决 *

  事件标记为已解决时的状态。

- * 已废弃 *

  事件在自动更正或事件的发生原因不再有效时的状态。

  您无法确认或解决已废弃的事件。

事件的不同状态示例

以下示例说明了手动和自动事件状态更改。

如果触发事件 Cluster not reachable ，则事件状态为 New 。确认事件后，事件状态将更改为 " 已确认 " 。采取适当的更正操作后，必须将此事件标记为已解决。然后，事件状态将更改为 "Resolved" 。

如果因断电而生成集群不可访问事件，则在恢复供电后，集群将在没有管理员干预的情况下开始运行。因此，集

群不可访问事件不再有效，事件状态将在下一个监控周期更改为 " 已废弃 " 。

当事件处于 " 已废弃 " 或 " 已解决 " 状态时， Unified Manager 将发送警报。警报的电子邮件主题行和电子邮件内容提供有关事件状态的信息。SNMP 陷阱还包括有关事件状态的信息。

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)和卷的安全程度 "《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。

如何计算对象状态

对象状态由当前处于 " 新增 " 或 " 已确认 " 状态的最严重事件确定。例如，如果对象状态为 " 错误 " ，则该对象的一个事件的严重性类型为 " 错误 " 。采取更正操作后，事件状态将变为 "Resolved" 。

对于动态性能事件，事件详细信息页面的系统诊断部分列出了处于争用状态的集群组件延迟或使用率最高的前几个工作负载。

性能统计信息基于检测到性能事件的时间，直到上次分析事件为止。这些图表还会显示处于争用状态的集群组件的历史性能统计信息。

例如，您可以确定组件利用率较高的工作负载，以确定要移至利用率较低的组件的工作负载。移动工作负载将减少当前组件的工作量，从而可能使该组件摆脱争用状态。此部分顶部是检测到事件并最后分析事件的时间和日期范围。对于活动事件(新事件或已确认事件)、将更新上次分析的时间。

将光标悬停在延迟和活动图表上方时，这些图表将显示排名靠前的工作负载的名称。单击图表右侧的工作负载类型菜单，您可以根据工作负载在事件中的角色（包括 鲨 鱼 _ ， *_bulles* 或 *victims* ）对这些工作负载进行排序，并显示有关其延迟及其在争用集群组件上的使用情况的详细信息。您可以将实际值与预期值进行比较，以查看工作负载何时超出其预期延迟或使用量范围。有关信息，请参见 "Unified Manager 监控的工作负载类型"。

> 按延迟峰值偏差排序时，表中不会显示系统定义的工作负载，因为延迟仅适用于用户定义的工作负载。延迟值非常低的工作负载不会显示在表中。

有关动态性能阈值的详细信息、请参见 "分析动态性能阈值中的事件"。

有关Unified Manager如何对工作负载进行排名并确定排序顺序的信息、请参见 "Unified Manager 如何确定事件的性能影响"。

图形中的数据显示上次分析事件之前 24 小时的性能统计信息。每个工作负载的实际值和预期值均基于工作负载参与事件的时间。例如，检测到事件后，工作负载可能会参与事件，因此其性能统计信息可能与检测事件时的值不匹配。默认情况下，工作负载按延迟峰值（最高）偏差排序。

> 由于 Unified Manager 最多可保留 30 天的 5 分钟历史性能和事件数据，因此，如果事件超过 30 天，则不会显示任何性能数据。

- * 工作负载排序列 *
  - * 延迟图表 *

    显示上次分析期间事件对工作负载延迟的影响。

  - * 组件使用情况列 *

    显示有关处于争用状态的集群组件的工作负载使用情况的详细信息。在图中，实际使用量为蓝线。红色条会突出显示从检测时间到上次分析时间的事件持续时间。有关详细信息，请参见 "工作负载性能测量值"。

    > 对于网络组件，由于网络性能统计信息来自集群之外的活动，因此不会显示此列。

  - * 组件使用情况 *

    显示网络处理，数据处理和聚合组件的利用率历史记录（以百分比表示），或者显示 QoS 策略组组件的活动历史记录（以百分比表示）。不会显示网络或互连组件的图表。您可以指向统计信息以查看特定时间点的使用情况统计信息。

- * 总写入 MB/ 秒历史记录 *

  仅对于 MetroCluster 资源组件，显示在 MetroCluster 配置中镜像到配对集群的所有卷工作负载的总写入吞吐量（以 MB/ 秒（ MBps ）为单位）。

- * 事件历史记录 *

  显示红色阴影线以指示处于争用状态的组件的历史事件。对于已废弃的事件，此图表将显示检测到选定事件之前以及解决该事件之后发生的事件。

Unified Manager 检测到配置更改

Unified Manager 可监控集群中的配置更改，以帮助您确定某个更改是否可能导致或影响性能事件。" 性能资源管理器 " 页面将显示一个更改事件图标（●）以指示检测到更改的日期和时间。

您可以在性能资源管理器页面和工作负载分析页面中查看性能图表，以查看更改事件是否影响选定集群对象的性能。如果在性能事件或与性能事件大致相同的时间检测到更改，则此更改可能会影响问题描述，从而导致触发事件警报。

Unified Manager 可以检测以下变更事件，这些事件归类为信息性事件：

- 卷在聚合之间移动。

  Unified Manager 可以检测移动正在进行，已完成或失败的时间。如果 Unified Manager 在卷移动期间关闭，则在备份时会检测到卷移动并显示其更改事件。

- 包含一个或多个受监控工作负载的 QoS 策略组的吞吐量（ MB/ 秒或 IOPS ）限制会发生变化。

  更改策略组限制可能会导致延迟（响应时间）出现发生原因间歇性峰值，进而可能会触发策略组的事件。延迟逐渐恢复正常，峰值引起的任何事件都将过时。

- HA 对中的节点接管或交还其配对节点的存储。

  Unified Manager 可以检测接管，部分接管或交还操作何时完成。如果接管是由发生崩溃的节点引起的，则 Unified Manager 不会检测到此事件。

- ONTAP 升级或还原操作已成功完成。

  此时将显示先前版本和新版本。

事件和严重性类型的列表

您可以使用事件列表更熟悉事件类别，事件名称以及在 Unified Manager 中可能看到的每个事件的严重性类型。事件按对象类别按字母顺序列出。

聚合事件

聚合事件为您提供聚合状态信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	**severity**
聚合脱机（ ocumEvtAggregateStateOffline ）	意外事件	聚合	严重
聚合失败（ ocumEvtAggregateStateFailed ）	意外事件	聚合	严重
聚合受限（ ocumEvtAggregateStateRestricted ）	风险	聚合	警告
聚合重建（ ocumEvtAggregateRaidStateReconstructing ）	风险	聚合	警告
聚合已降级（ ocumEvtAggregateRaidStateDegraded ）	风险	聚合	警告
云层可部分访问（ ocumEventCloudTierPartiallyReachable ）	风险	聚合	警告
无法访问云层（ ocumEventCloudTierUnreachable ）	风险	聚合	error
聚合重新定位的云层访问被拒绝 * （ arlNetraCaCheckFailed ）	风险	聚合	error
在存储故障转移期间，用于聚合重新定位的云层访问被拒绝 * （ gbNetraCaCheckFailed ）	风险	聚合	error
遗留的 MetroCluster 聚合（ ocumEvtMetroClusterAggregateLeftBehind ）	风险	聚合	error

事件名称（陷阱名称）	影响级别	源类型	**severity**
MetroCluster 聚合镜像已降级（ ocumEvtMetroClusterAggregateMirrorDegraded ）	风险	聚合	error

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
聚合空间接近全满（ ocumEvtAggregateNearlyFull ）	风险	聚合	警告
聚合空间已满（ ocumEvtAggregateFull ）	风险	聚合	error
聚合达到全满前的天数（ ocumEvtAggregateDaysUntireFullSoon ）	风险	聚合	error
聚合过量提交（ ocumEvtAggregateOvercommitted ）	风险	聚合	error
聚合接近过量提交（ ocumEvtAggregateAlmostOvercommitted ）	风险	聚合	警告
聚合 Snapshot 预留已满（ ocumEvtAggregateSnapReserveFull ）	风险	聚合	警告
聚合增长率异常（ ocumEvtAggregateGrowthRateAbnormal ）	风险	聚合	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已发现聚合（不适用）	事件	聚合	信息
聚合已重命名（不适用）	事件	聚合	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
已删除聚合（不适用）	事件	Node	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反聚合 IOPS 严重阈值（ ocumAggregateIopsIncident ）	意外事件	聚合	严重
已违反聚合 IOPS 警告阈值（ ocumAggregateIopsWarning ）	风险	聚合	警告
已违反聚合 MB/ 秒严重阈值（ ocumAggregateMbpsIncident ）	意外事件	聚合	严重
已违反聚合 MB/ 秒警告阈值（ ocumAggregateMbpsWarning ）	风险	聚合	警告
已违反聚合延迟严重阈值（ ocumAggregateLatencyIncident ）	意外事件	聚合	严重
已违反聚合延迟警告阈值（ ocumAggregateLatencyWarning ）	风险	聚合	警告
已违反聚合已用性能容量严重阈值（ ocumAggregatePerfCapacityUsedIncident ）	意外事件	聚合	严重
已违反聚合已用性能容量警告阈值（ ocumAggregatePerfCapacityUsedWarning ）	风险	聚合	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反聚合利用率严重阈值（ ocumAggregateUtilizationIncident ）	意外事件	聚合	严重
已违反聚合利用率警告阈值（ ocumAggregateUtilizationWarning ）	风险	聚合	警告
已违反聚合磁盘过度利用阈值（ ocumAggregateDisksOverUtilizedWarning ）	风险	聚合	警告
已违反聚合动态阈值（ ocumAggregateDynamicEventWarning ）	风险	聚合	警告

集群事件

集群事件提供了有关集群状态的信息，可用于监控集群是否存在潜在问题。事件按影响区域分组，并包括事件名称，陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	**severity**
集群缺少备用磁盘（ ocumEvtDisksNoSpares ）	风险	集群	警告
集群不可访问（ ocumEvtClusterUnreachable ）	风险	集群	error
集群监控失败（ ocumEvtClusterMonitoringFailed ）	风险	集群	警告
已违反集群 FabricPool 许可证容量限制（ ocumEvtExternalCapacityTierSpaceFull ）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
NVMe-oF 宽限期已开始 *（ nvmfGraePeriodStart ）	风险	集群	警告
NVMe-oF 宽限期处于活动状态 *（ nvmfGracePeriodActive ）	风险	集群	警告
NVMe-oF 宽限期已过期 *（ nvmfGracePeriodExpired ）	风险	集群	警告
对象维护窗口已启动（ objectMaintenanceWindow 已启动）	事件	集群	严重
对象维护窗口已结束（ objectMaintenanceWindow 已启用）	事件	集群	信息
MetroCluster 遗留的备用磁盘（ ocumEvtSpaceDiskLeftBehind ）	风险	集群	error
已禁用 MetroCluster 自动计划外切换（ ocumEvtMccAutomaticUnplanedSwitchOverDisabled ）	风险	集群	警告
集群用户密码已更改 *（ cluster.passwd.changed ）	事件	集群	信息

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反集群容量不平衡阈值（ ocumConformanceNodeImportanceWarning ）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
集群云层规划（ clusterCloudTierPlanning Warning ）	风险	集群	警告
FabricPool 镜像复制重新同步已完成 * （ waflCaResyncComplete ）	事件	集群	警告
FabricPool 空间接近全满 * （ fabricpoolNearlyFull ）	风险	集群	error

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已添加节点（不适用）	事件	集群	信息
已删除节点（不适用）	事件	集群	信息
已删除集群（不适用）	事件	集群	信息
集群添加失败（不适用）	事件	集群	error
集群名称已更改（不适用 ）	事件	集群	信息
收到紧急 EMS （不适用 ）	事件	集群	严重
收到严重 EMS （不适用 ）	事件	集群	严重
收到警报 EMS （不适用 ）	事件	集群	error
收到错误 EMS （不适用 ）	事件	集群	警告
收到警告 EMS （不适用 ）	事件	集群	警告
收到调试 EMS （不适用 ）	事件	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
收到通知 EMS （不适用）	事件	集群	警告
收到信息 EMS （不适用）	事件	集群	警告

ONTAP EMS 事件分为三个 Unified Manager 事件严重性级别。

Unified Manager 事件严重性级别	ONTAP EMS 事件严重性级别
严重	紧急 严重
error	警报
警告	error 警告 调试 通知 信息性

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反集群负载不平衡阈值（）	风险	集群	警告
已违反集群 IOPS 严重阈值（ ocumClusterIopsIncident ）	意外事件	集群	严重
已违反集群 IOPS 警告阈值（ ocumClusterIopsWarning ）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反集群 MB/ 秒严重阈值（ ocumClusterMbpsIncident ）	意外事件	集群	严重
已违反集群 MB/ 秒警告阈值（ ocumClusterMbpsWarning ）	风险	集群	警告
已违反集群动态阈值（ ocumClusterDynamicEventWarning ）	风险	集群	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	**severity**
已禁用 AutoSupport HTTPS 传输（ ocumClusterASUPHttpsConfiguredDisabled ）	风险	集群	警告
日志转发未加密（ ocumClusterAuditLogUnencrypted ）	风险	集群	警告
已启用默认本地管理员用户（ ocumClusterDefaultAdminEnabled ）	风险	集群	警告
FIPS 模式已禁用（ ocumClusterFipsDisabled ）	风险	集群	警告
已禁用登录横幅（已禁用 ocumClusterLoginBannerDisabled ）	风险	集群	警告
已更改登录横幅（ ocumClusterLoginBannerChanged ）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
日志转发目标已更改（ ocumLogForwardDestinationsChanged ）	风险	集群	警告
NTP 服务器名称已更改（ ocumNtpServerNamesChanged ）	风险	集群	警告
NTP 服务器计数低（ securityConfigNTPServerCountLowRisk ）	风险	集群	警告
集群对等通信未加密（ ocumClusterPeerEncryptionDisabled ）	风险	集群	警告
SSH 正在使用不安全的密码（ ocumClusterSSHInsecure ）	风险	集群	警告
已启用 Telnet 协议（已启用 ocumClusterTelnetEnabled ）	风险	集群	警告
某些 ONTAP 用户帐户的密码使用不太安全的 MD5 哈希函数（ ocumClusterMD5 密码哈希函数）	风险	集群	警告
集群使用自签名证书（ ocumClusterSelfSignedCertificate ）	风险	集群	警告
已启用集群远程 Shell （ ocumClusterRshDisabled ）	风险	集群	警告
集群证书即将过期(ocumEvtClusterCertificateAboutToExpire)	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
集群证书已过期(ocumEvtClusterCertificateExpirered)	风险	集群	error

磁盘事件

磁盘事件可为您提供有关磁盘状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
闪存磁盘 - 备用块几乎已使用（ ocumEvtClusterFlashDiskFewerSpareBlockError ）	风险	集群	error
闪存磁盘 - 无备用块（ ocumEvtClusterFlashDiskNoSpareBlockCritical ）	意外事件	集群	严重
某些未分配磁盘（ ocumEvtClusterUnasigedDisksome ）	风险	集群	警告
某些故障磁盘（ ocumEvtDisksScomeFailed ）	意外事件	集群	严重

机箱事件

机箱事件可为您提供有关数据中心中磁盘架机箱状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
磁盘架风扇出现故障（ ocumEvtShelfFanFailed ）	意外事件	存储架	严重
磁盘架电源出现故障（ ocumEvtShelfPowerSupplyFailed ）	意外事件	存储架	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
未配置磁盘架多路径（ ocumDiskShelfConnectivityNotInMultiPath ） 此事件不适用于： • MetroCluster 配置中的集群 • 以下平台： FAS2554 ， FAS2552 ， FAS2520 和 FAS2240	风险	Node	警告
磁盘架路径故障（ ocumDiskShelfConnectivityPathFailure ）	风险	存储架	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已发现磁盘架（不适用）	事件	Node	信息
已删除磁盘架（不适用）	事件	Node	信息

风扇事件

风扇事件为您提供数据中心节点上的风扇状态信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
一个或多个故障风扇（ ocumEvtFansOneOrMoreFailed ）	意外事件	Node	严重

闪存卡事件

闪存卡事件可为您提供有关数据中心节点上安装的闪存卡的状态的信息，以便您可以监控潜在的问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
闪存卡脱机（ ocumEvtFlashCardOffline ）	意外事件	Node	严重

索引节点事件

索引节点事件在索引节点已满或接近已满时提供信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
索引节点接近全满（ ocumEvtIdnodesAlmostFull ）	风险	Volume	警告
索引节点已满（ ocumEvtIdnodesFull ）	风险	Volume	error

网络接口（ **LIF** ）事件

网络接口事件可提供有关网络接口（ LIF ）状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
网络接口状态为已关闭（ ocumEvtLifeStatusDown ）	风险	接口	error
FC/FCoE 网络接口状态为已关闭（ ocumEvtFCLifStatusDown ）	风险	接口	error
无法进行网络接口故障转移（ ocumEvtLifeFailoverNotPossible ）	风险	接口	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
网络接口不在主端口（ ocumEvtLifeNotAtHomePort ）	风险	接口	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
未配置网络接口路由（不适用）	事件	接口	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反网络接口 MB/ 秒严重阈值（ ocumNetworkLifeMbpsIncident ）	意外事件	接口	严重
已违反网络接口 MB/ 秒警告阈值（ ocumNetworkLifeMbpsWarning ）	风险	接口	警告
已违反 FC 网络接口 MB/ 秒严重阈值（ ocumFcpLifeMbpsIncident ）	意外事件	接口	严重
已违反 FC 网络接口 MB/ 秒警告阈值（ ocumFcpLifeMbpsWarning ）	风险	接口	警告
已违反 NVMf FC 网络接口 MB/ 秒严重阈值（ ocumNvmffclifMbpsIncident ）	意外事件	接口	严重
已违反 NVMf FC 网络接口 MB/ 秒警告阈值（ ocumNvmffclifMbpsWarning ）	风险	接口	警告

LUN 事件

LUN 事件可为您提供有关 LUN 状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	**severity**
LUN 脱机（ ocumEvtLunOffline ）	意外事件	LUN	严重
LUN 已销毁 * （ lunDestroy ）	事件	LUN	信息
igroup 中映射的 LUN 不受支持的操作系统（ igroup 不支持的 OsType ）	意外事件	LUN	警告
访问 LUN 的单个活动路径（ ocumEvtLunSingleActivePath ）	风险	LUN	警告
没有用于访问 LUN 的活动路径（ ocumEvtLunNotReachable ）	意外事件	LUN	严重
没有可用于访问 LUN 的优化路径（ ocumEvtLunOptimizedPathInactive ）	风险	LUN	警告
没有从 HA 配对节点访问 LUN 的路径（ ocumEvtLunHAPathInactive ）	风险	LUN	警告
没有从 HA 对中的一个节点访问 LUN 的路径（ ocumEvtLunNodePathStatusDown ）	风险	LUN	error

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
LUN Snapshot 副本空间不足（ ocumEvtLunSnapshotNotPossible ）	风险	Volume	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
igroup 中映射的 LUN 不受支持的操作系统（ igroup 不支持的 OsType ）	风险	LUN	警告

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 LUN IOPS 严重阈值（ ocumLunIopsIncident ）	意外事件	LUN	严重
已违反 LUN IOPS 警告阈值（ ocumLunIopsWarning ）	风险	LUN	警告
已违反 LUN MB/ 秒严重阈值（ ocumLunMbpsIncident ）	意外事件	LUN	严重
已违反 LUN MB/ 秒警告阈值（ ocumLunMbpsWarning ）	风险	LUN	警告
已违反 LUN 延迟毫秒 / 操作严重阈值（ ocumLunLatencyIncident ）	意外事件	LUN	严重
已违反 LUN 延迟毫秒 / 操作警告阈值（ ocumLunLatencyWarning ）	风险	LUN	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 LUN 延迟和 IOPS 严重阈值（ ocumLunLatencyIopsIncident ）	意外事件	LUN	严重
已违反 LUN 延迟和 IOPS 警告阈值（ ocumLunLatencyIopsWarning ）	风险	LUN	警告
已违反 LUN 延迟和 MB/秒严重阈值（ ocumLunLatencyMbpsIncident ）	意外事件	LUN	严重
已违反 LUN 延迟和 MB/秒警告阈值（ ocumLunLatencyMbpsWarning ）	风险	LUN	警告
已违反 LUN 延迟和聚合已用性能容量严重阈值（ ocumLunLatencyAggregatePerfCapacityUsedIncident ）	意外事件	LUN	严重
已违反 LUN 延迟和聚合已用性能容量警告阈值（ ocumLunLatencyAggregatePerfCapacityUsedWarning ）	风险	LUN	警告
已违反 LUN 延迟和聚合利用率严重阈值（ ocumLunLatencyAggregateUtilizationIncident ）	意外事件	LUN	严重
已违反 LUN 延迟和聚合利用率警告阈值（ ocumLunLatencyAggregateUtilizationWarning ）	风险	LUN	警告
已违反 LUN 延迟和节点已用性能容量严重阈值（ ocumLunLatencyNodePerfCapacityUsedIncident ）	意外事件	LUN	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 LUN 延迟和节点已用性能容量警告阈值（ ocumLunLatencyNodePerfCapacityUsedWarning ）	风险	LUN	警告
LUN 延迟和节点已用性能容量 - 已违反接管严重阈值（ ocumLunLatencyAggregatePerfCapacityUsedTakeOverIncident ）	意外事件	LUN	严重
LUN 延迟和节点已用性能容量 - 已违反接管警告阈值（ ocumLunLatencyAggregatePerfCapacityUsedTakeOverWarning ）	风险	LUN	警告
已违反 LUN 延迟和节点利用率严重阈值（ ocumLunLatencyNodeUtilizationIncident ）	意外事件	LUN	严重
已违反 LUN 延迟和节点利用率警告阈值（ ocumLunLatencyNodeUtilizationWarning ）	风险	LUN	警告
已违反 QoS LUN 最大 IOPS 警告阈值（ ocumQosLunMaxIopsWarning ）	风险	LUN	警告
已违反 QoS LUN 最大 MB/ 秒警告阈值（ ocumQosLunMaxMbpsWarning ）	风险	LUN	警告
已违反性能服务级别策略定义的工作负载 LUN 延迟阈值（ ocumConformanceLatencyWarning ）	风险	LUN	警告

管理工作站事件

管理工作站事件为您提供安装 Unified Manager 的服务器的状态信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
管理服务器磁盘空间接近全满（ ocumEvtUnifiedManagerDiskSpaceNearlyFull ）	风险	管理工作站	警告
管理服务器磁盘空间已满（ ocumEvtUnifiedManagerDiskSpaceFull ）	意外事件	管理工作站	严重
管理服务器内存不足（ ocumEvtUnifiedManagerMemoryLow ）	风险	管理工作站	警告
管理服务器内存几乎用尽（ ocumEvtUnifiedManagerMemoryAlmostOut ）	意外事件	管理工作站	严重
MySQL 日志文件大小增加；需要重新启动（ ocumEvtMysqlLogFileSizeWarning ）	意外事件	管理工作站	警告
审核日志总大小分配即将达到全满	风险	管理工作站	警告
系统日志服务器证书即将过期	风险	管理工作站	警告
系统日志服务器证书已过期	风险	管理工作站	error
审核日志文件已被篡改	风险	管理工作站	警告
已删除审核日志文件	风险	管理工作站	警告
系统日志服务器连接错误	风险	管理工作站	error

事件名称（陷阱名称）	影响级别	源类型	**severity**
已更改系统日志服务器配置	事件	管理工作站	警告

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
性能数据分析受影响（ ocumEvtUnifiedManagerDataMissingAnalyze ）	风险	管理工作站	警告
性能数据收集受影响（ ocumEvtUnifiedManagerDataMisingCollection ）	意外事件	管理工作站	严重

最后两个性能事件仅适用于 Unified Manager 7.2 。如果其中任一事件处于 " 新建 " 状态，然后升级到较新版本的 Unified Manager 软件，则这些事件不会自动清除。您需要手动将事件移至已解决状态。

MetroCluster 网桥事件

MetroCluster 网桥事件可为您提供有关网桥状态的信息、以便您可以监控基于FC的MetroCluster 配置中的潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
无法访问网桥（ ocumEvtBridgeUnreachable ）	意外事件	MetroCluster 网桥	严重
网桥温度异常（ ocumEvtBridgeTemperatureAbnormal ）	意外事件	MetroCluster 网桥	严重

MetroCluster 连接事件

连接事件可为您提供有关集群组件之间以及基于FC和MetroCluster 基于IP的MetroCluster 配置中的集群之间的连接的信息、以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

这两种配置中通用的事件

这些连接事件对于基于FC的MetroCluster 和基于IP的MetroCluster 配置都很常见。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
MetroCluster 配对节点之间的所有链路已关闭（ocumEvtMetroClusterAllLinksBetweenPartnersDown ）	意外事件	MetroCluster 关系	严重
无法通过对等网络访问 MetroCluster 合作伙伴（ocumEvtMetroClusterPartnersNotReachebleOverPeeringNetwork ）	意外事件	MetroCluster 关系	严重
受影响的 MetroCluster 灾难恢复功能（ocumEvtMetroClusterDRStatusImpacted ）	风险	MetroCluster 关系	严重
MetroCluster 配置已切换（ocumEvtMetroClusterDRStatusImpacted ）	风险	MetroCluster 关系	警告

基于**FC**的**MetroCluster** 配置

这些事件与基于FC的MetroCluster 配置相关。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
所有交换机间链路已关闭（ocumEvtMetroClusterAllISLBetweenSwitchesDown ）	意外事件	MetroCluster 交换机间连接	严重
FC-SAS 网桥到存储堆栈的链路已关闭（ocumEvtBridgeSasPortDown ）	意外事件	MetroCluster 网桥堆栈连接	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
MetroCluster 配置已部分切换（ ocumEvtMetroClusterDRStatusPartiallyImpacted ）	风险	MetroCluster 关系	error
节点到 FC 交换机的所有 FC-VI 互连链路已关闭（ ocumEvtMccNodeSwitchFcviLinksDown ）	意外事件	MetroCluster 节点交换机连接	严重
节点到 FC 交换机一个或多个 FC-Initiator 链路已关闭（ ocumEvtMccNodeSwitchFcLinksOneOrMoreDown ）	风险	MetroCluster 节点交换机连接	警告
节点到 FC 交换机的所有 FC-Initiator 链路已关闭（ ocumEvtMccNodeSwitchFcLinksDown ）	意外事件	MetroCluster 节点交换机连接	严重
切换到 FC-SAS 网桥 FC 链路关闭（ ocumEvtMccSwitchBridgeFcLinksDown ）	意外事件	MetroCluster 交换机网桥连接	严重
节点间所有 FC VI 互连链路已关闭（ ocumEvtMccInterNodeLinksDown ）	意外事件	节点间连接	严重
节点间一个或多个 FC VI 互连链路已关闭（ ocumEvtMccInterNodeLinksOneOrMoreDown ）	风险	节点间连接	警告
节点到网桥的链路关闭（ ocumEvtMccNodeBridgeLinksDown ）	意外事件	节点网桥连接	严重
节点到存储堆栈的所有 SAS 链路已关闭（ ocumEvtMccNodeStackLinksDown ）	意外事件	节点堆栈连接	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
节点到存储堆栈的一个或多个 SAS 链路已关闭（ ocumEvtMccNodeStackLinksOneOrMoreDown ）	风险	节点堆栈连接	警告

基于**IP**的**MetroCluster** 配置

这些事件与基于IP的MetroCluster 配置相关。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
MetroCluster IP站点间连接状态为已关闭(mccIntersiteeconnectivityStatusDown)	风险	MetroCluster 关系	严重
MetroCluser-IP节点到交换机的连接脱机(mccIpPortStatusOffline)	风险	Node	error

MetroCluster 交换机事件

对于基于FC的MetroCluster 配置、MetroCluster 交换机事件可为您提供有关MetroCluster 交换机状态的信息、以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
交换机温度异常（ ocumEvtSwitchTemperatureAbnormal ）	意外事件	MetroCluster 交换机	严重
交换机不可访问（ ocumEvtSwitchUnreachable ）	意外事件	MetroCluster 交换机	严重
交换机风扇出现故障（ ocumEvtSwitchFansOneOrMoreFailed ）	意外事件	MetroCluster 交换机	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
交换机电源出现故障（ ocumEvtSwitchPowerSupplies OneOrMoreFailed ）	意外事件	MetroCluster 交换机	严重
交换机温度传感器出现故障（ ocumEvtSwitchTemperatureSenorFailed ） 此事件仅适用于 Cisco 交换机。	意外事件	MetroCluster 交换机	严重

NVMe 命名空间事件

NVMe 命名空间事件可为您提供有关命名空间状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
NVMeNS 脱机 * （ nvmeNamespaceStatusOffline ）	事件	命名空间	信息
NVMeNS Online * （ nvmeNamespaceStatusOnline ）	事件	命名空间	信息
NVMeNS 空间不足 * （ nvmeNamespaceSpaceOutOfSpace ）	风险	命名空间	警告
NVmeNS destroy * （ nvmeNamespaceDestroy ）	事件	命名空间	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 NVMe 命名空间 IOPS 严重阈值（ ocumNvmeNamespaceIopsIncident ）	意外事件	命名空间	严重
已违反 NVMe 命名空间 IOPS 警告阈值（ ocumNvmeNamespaceIopsWarning ）	风险	命名空间	警告
已违反 NVMe 命名空间 MB/ 秒严重阈值（ ocumNvmeNamespaceMbpsIncident ）	意外事件	命名空间	严重
已违反 NVMe 命名空间 MB/ 秒警告阈值（ ocumNvmeNamespaceMbpsWarning ）	风险	命名空间	警告
已违反 NVMe 命名空间延迟毫秒 / 操作严重阈值（ ocumNvmeNamespaceLatencyIncident ）	意外事件	命名空间	严重
已违反 NVMe 命名空间延迟毫秒 / 操作警告阈值（ ocumNvmeNamespaceLatencyWarning ）	风险	命名空间	警告
已违反 NVMe 命名空间延迟和 IOPS 严重阈值（ ocumNvmeNamespaceLatencyIopsIncident ）	意外事件	命名空间	严重
已违反 NVMe 命名空间延迟和 IOPS 警告阈值（ ocumNvmeNamespaceLatencyIopsWarning ）	风险	命名空间	警告
已违反 NVMe 命名空间延迟和 MB/ 秒严重阈值（ ocumNvmeNamespaceLateencyMbpsIncident ）	意外事件	命名空间	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 NVMe 命名空间延迟和 MB/ 秒警告阈值（ ocumNvmeNamespaceLatencyMbpsWarning ）	风险	命名空间	警告

节点事件

节点事件可为您提供有关节点状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
节点根卷空间接近全满（ ocumEvtClusterNodeRootVolumeSpaceNearlyFull ）	风险	Node	警告
Cloud AWS MetaDataConnFail * （ ocumCloudAwsMetadataConnFail ）	风险	Node	error
Cloud AWS IAMCredsExpired * （ ocumCloudAwsIamCredsExpired ）	风险	Node	error
Cloud AWS IAMCredsInvalid * （ ocumCloudAwsIamCredsInvalid ）	风险	Node	error
Cloud AWS IAMCredsNotFound * （ ocumCloudAwsIamCredsNotFound ）	风险	Node	error
Cloud AWS IAMCredsNotInitialized * （ ocumCloudAwsIamCredsNotInitialized ）	事件	Node	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
Cloud AWS IAMRoleInvalid *（ ocumCloudAwsIamRoleInvalid ）	风险	Node	error
Cloud AWS IAMRoleNotFound *（ ocumCloudAwsIamRoleNotFound ）	风险	Node	error
无法解析云层主机 *（ ocumObjstoreHostUnresolvable ）	风险	Node	error
云层集群间网络接口已关闭*(ocumObjstoreInterClusterLifDown)	风险	Node	error
一个 NFSv4 池已耗尽 *（ nbladeNfsv4PoolEXhaust ）	意外事件	Node	严重
请求不匹配云层签名 *（ 签名不匹配）	风险	Node	error

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
QoS 监控内存已达到上限 *（ ocumQosMonitorMemoryMaxed ）	风险	Node	error
QoS 监控内存已减少 *（ ocumQosMonitorMemoryAbated ）	事件	Node	信息

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
节点已重命名（不适用）	事件	Node	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反节点 IOPS 严重阈值（ ocumNodeIopsIncident ）	意外事件	Node	严重
已违反节点 IOPS 警告阈值（ ocumNodeIopsWarning ）	风险	Node	警告
已违反节点 MB/ 秒严重阈值（ ocumNodeMbpsIncident ）	意外事件	Node	严重
已违反节点 MB/ 秒警告阈值（ ocumNodeMbpsWarning ）	风险	Node	警告
已违反节点延迟毫秒 / 操作严重阈值（ ocumNodeLatencyIncident ）	意外事件	Node	严重
已违反节点延迟毫秒 / 操作警告阈值（ ocumNodeLatencyWarning ）	风险	Node	警告
已违反节点已用性能容量严重阈值（ ocumNodePerfCapacityUsedIncident ）	意外事件	Node	严重
已违反节点已用性能容量警告阈值（ ocumNodePerfCapacityUsedWarning ）	风险	Node	警告
已用节点性能容量 - 已违反接管严重阈值（ ocumNodePerfCapacityUsedTakeoverIncident ）	意外事件	Node	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已用节点性能容量 - 已违反接管警告阈值（ ocumNodePerfCapacityUsedTakeoverWarning ）	风险	Node	警告
已违反节点利用率严重阈值（ ocumNodeUtilizationIncident ）	意外事件	Node	严重
已违反节点利用率警告阈值（ ocumNodeUtilizationWarning ）	风险	Node	警告
已违反节点 HA 对过度利用阈值（ ocumNodeHAPairOverUtilizedInformation ）	事件	Node	信息
已违反节点磁盘碎片化阈值（ ocumNodeDiskFragmentationWarning ）	风险	Node	警告
已违反已用性能容量阈值（ ocumNodeOverUtilizedWarning ）	风险	Node	警告
已违反节点动态阈值（ ocumNodeDynamicEventWarning ）	风险	Node	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	**severity**
建议 ID： ntap-<_advisory ID__> （ ocumx ）	风险	Node	严重

NVRAM 电池事件

NVRAM 电池事件可为您提供电池状态信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
NVRAM 电池电量低（ ocumEvtNvram"BatteryLow" ）	风险	Node	警告
NVRAM 电池已放电（ ocumEvtNvramBatteryDis 荷 电）	风险	Node	error
NVRAM 电池充电过度（ ocumEvtNvram"BatteryOverCharged ）	意外事件	Node	严重

端口事件

端口事件可为您提供有关集群端口的状态，以便您可以监控端口上的更改或问题，例如端口是否已关闭。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
端口状态为已关闭（ ocumEvtPortStatusDown ）	意外事件	Node	严重

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反网络端口 MB/ 秒严重阈值（ ocumNetworkPortMbpsIncident ）	意外事件	Port	严重
已违反网络端口 MB/ 秒警告阈值（ ocumNetworkPortMbpsWarning ）	风险	Port	警告
已违反 FCP 端口 MB/ 秒严重阈值（ ocumFcpPortMbpsIncident ）	意外事件	Port	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 FCP 端口 MB/ 秒警告阈值（ ocumFcpPortMbpsWarning ）	风险	Port	警告
已违反网络端口利用率严重阈值（ ocumNetworkPortUtilizationIncident ）	意外事件	Port	严重
已违反网络端口利用率警告阈值（ ocumNetworkPortUtilizationWarning ）	风险	Port	警告
已违反 FCP 端口利用率严重阈值（ ocumFcpPortUtilizationIncident ）	意外事件	Port	严重
已违反 FCP 端口利用率警告阈值（ ocumFcpPortUtilizationWarning ）	风险	Port	警告

电源事件

电源事件可为您提供有关硬件状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
一个或多个电源出现故障（ ocumEvtPowerSupplyOneOrMoreFailed ）	意外事件	Node	严重

保护事件

保护事件会告诉您作业是失败还是已中止，以便您可以监控问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	**severity**
保护作业失败（ocumEvtProtectionJobTaskFailed ）	意外事件	卷或存储服务	严重
保护作业已中止（ocumEvtProtectionJobAborted ）	风险	卷或存储服务	警告

qtree 事件

qtree 事件可为您提供有关 qtree 容量以及文件和磁盘限制的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
qtree 空间接近全满（ocumEvtQtreeSpaceNearlyFull ）	风险	qtree	警告
qtree 空间已满（ocumEvtQtreeSpaceFull ）	风险	qtree	error
qtree 空间正常（ocumEvtQtreeSpaceThresholdOk ）	事件	qtree	信息
已达到 qtree 文件硬限制（ocumEvtQtreeFilesHardLimitReached ）	意外事件	qtree	严重
已违反 qtree 文件软限制（已达到ocumEvtQtreeFilesSoftLimitBreached ）	风险	qtree	警告
已达到 qtree 空间硬限制（ocumEvtQtreeSpaceHardLimitReached ）	意外事件	qtree	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 qtree 空间软限制（已达到 ocumEvtQtreeSpaceSoftLimit ）	风险	qtree	警告

服务处理器事件

服务处理器事件为您提供处理器状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
未配置服务处理器（ ocumEvtServiceProcessorNotConfigured ）	风险	Node	警告
服务处理器脱机（ ocumEvtServiceProcessorOffline ）	风险	Node	error

SnapMirror 关系事件

SnapMirror 关系事件可为您提供有关异步和同步 SnapMirror 关系的状态信息，以便您可以监控潜在问题。系统会为 Storage VM 和卷生成异步 SnapMirror 关系事件，但仅为卷关系生成同步 SnapMirror 关系事件。不会为属于 Storage VM 灾难恢复关系的成分卷生成任何事件。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：保护

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

对于受 Storage VM 灾难恢复保护的 Storage VM ，系统会生成 SnapMirror 关系事件，但对于任何成分卷对象关系，不会生成这些事件。

事件名称（陷阱名称）	影响级别	源类型	**severity**
镜像复制运行不正常（ ocumEvtSnapmirrorRelationshipUnhealthy ）	风险	SnapMirror 关系	警告
镜像复制已断开（ ocumEvtSnapmirrorRelationshipStateBrokenoff ）	风险	SnapMirror 关系	error

事件名称（陷阱名称）	影响级别	源类型	**severity**
镜像复制初始化失败（ocumEvtSnapmirrorRelationshipInitializeFailed ）	风险	SnapMirror 关系	error
镜像复制更新失败（ocumEvtSnapmirrorRelationshipUpdateFailed ）	风险	SnapMirror 关系	error
镜像复制滞后错误（ocumEvtSnapMirrorRelationshipLagError ）	风险	SnapMirror 关系	error
镜像复制滞后警告（ocumEvtSnapMirrorRelationshipLagWarning ）	风险	SnapMirror 关系	警告
镜像复制重新同步失败（ocumEvtSnapmirrorRelationshipResyncFailed ）	风险	SnapMirror 关系	error
同步复制不同步 *（syncSnapmirrorRelationshipOutofsync ）	风险	SnapMirror 关系	警告
同步复制已还原 *（syncSnapmirrorRelationshipInSync ）	事件	SnapMirror 关系	信息
同步复制自动重新同步失败 *（syncSnapmirrorRelationshipAutoSyncRetryFailed ）	风险	SnapMirror 关系	error
已在集群上添加ONTAP 调解器(snapmirrorMediatorAdded)	事件	集群	信息
已从集群中删除ONTAP 调解器(已删除snapmirrorMediator)	事件	集群	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
无法从集群访问ONTAP 调解器(snapmirrorMediatorUnreachable)	风险	调解器	警告
无法从集群访问ONTAP 调解器(snapmirrorMediatorMisconfigured)	风险	调解器	error
已重新建立ONTAP调解器连接、并且已重新同步并已准备好进行SnapMirror活动同步(snapmirector介质 仲裁)	事件	调解器	信息

异步镜像和存储关系事件

异步镜像和存储关系事件可为您提供有关异步 SnapMirror 和存储关系状态的信息，以便您可以监控潜在问题。卷和 Storage VM 保护关系均支持异步镜像和存储关系事件。但是，Storage VM 灾难恢复仅支持存储关系。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：保护

对于受 Storage VM 灾难恢复保护的 Storage VM ，也会生成 SnapMirror 和存储关系事件，但对于任何成分卷对象关系，不会生成这些事件。

事件名称（陷阱名称）	影响级别	源类型	**severity**
异步镜像和存储运行不正常（ocumEvtMirrorVaultRelationshipUnhealthy ）	风险	SnapMirror 关系	警告
异步镜像和存储已断开（ocumEvtMirrorVaultRelationshipStateBrokenoff ）	风险	SnapMirror 关系	error
异步镜像和存储初始化失败（ocumEvtMirrorVaultRelationshipInitializeFailed ）	风险	SnapMirror 关系	error

事件名称（陷阱名称）	影响级别	源类型	**severity**
异步镜像和存储更新失败（ ocumEvtMirrorVaultRelationshipUpdateFailed ）	风险	SnapMirror 关系	error
异步镜像和存储滞后错误（ ocumEvtMirrorVaultRelationLagshipError ）	风险	SnapMirror 关系	error
异步镜像和存储滞后警告（ ocumEvtMirrorVaultRelationLagshipWarning ）	风险	SnapMirror 关系	警告
异步镜像和存储重新同步失败（ ocumEvtMirrorVaultRelationshipResyncFailed ）	风险	SnapMirror 关系	error

Active IQ 门户（ Config Advisor ）引发 "SnapMirror update failure" 事件。

Snapshot 事件

Snapshot 事件提供了有关快照状态的信息，可用于监控快照是否存在潜在问题。事件按影响区域分组，并包括事件名称，陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
已禁用 Snapshot 自动删除（不适用）	事件	Volume	信息
已启用 Snapshot 自动删除（不适用）	事件	Volume	信息
Snapshot 自动删除配置已修改（不适用）	事件	Volume	信息

SnapVault 关系事件

SnapVault 关系事件可为您提供有关 SnapVault 关系状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	**severity**
异步存储运行不正常（ ocumEvtSnapVaultRelationshipUnhealthy ）	风险	SnapMirror 关系	警告
异步存储已断开（ ocumEvtSnapVaultRelationshipStateBrokenoff ）	风险	SnapMirror 关系	error
异步存储初始化失败（ ocumEvtSnapVaultRelationshipInitializeFailed ）	风险	SnapMirror 关系	error
异步存储更新失败（ ocumEvtSnapVaultRelationshipUpdateFailed ）	风险	SnapMirror 关系	error
异步存储滞后错误（ ocumEvtSnapVaultRelationshipLagError ）	风险	SnapMirror 关系	error
异步存储滞后警告（ ocumEvtSnapVaultRelationshipLagWarning ）	风险	SnapMirror 关系	警告
异步存储重新同步失败（ ocumEvtSnapvaultRelationshipResyncFailed ）	风险	SnapMirror 关系	error

存储故障转移设置事件

存储故障转移（ Storage Failover ， SFO ）设置事件为您提供有关存储故障转移是否已禁用或未配置的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
存储故障转移互连一个或多个链路已关闭（ ocumEvtSfoInterconnectOneOrMoreLinksDown ）	风险	Node	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已禁用存储故障转移（ ocumEvtSfoSettings 已禁用）	风险	Node	error
未配置存储故障转移（ ocumEvtSfoSettings NotConfigured ）	风险	Node	error
存储故障转移状态 - 接管（ ocumEvtSfoStateTakeover ）	风险	Node	警告
存储故障转移状态 - 部分交还（ ocumEvtSfoStatePartialGiveback ）	风险	Node	error
存储故障转移节点状态为已关闭（ ocumEvtSfoNodeStatusDown ）	风险	Node	error
无法执行存储故障转移接管（ ocumEvtSfoTakeoverNotPossible ）	风险	Node	error

存储服务事件

存储服务事件为您提供有关存储服务的创建和订阅的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已创建存储服务（不适用）	事件	存储服务	信息
已订阅存储服务（不适用）	事件	存储服务	信息
存储服务已取消订阅（不适用）	事件	存储服务	信息

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	**severity**
意外删除受管 SnapMirror RelationshipocumEvtStorageServiceUnsultedRelationshipDeletion	风险	存储服务	警告
意外删除存储服务成员卷（ ocumEvtStorageServiceUnexpectedVolumeDelay ）	意外事件	存储服务	严重

存储架事件

存储架事件会告诉您存储架是否异常，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
电压范围异常（ ocumEvtShelfVolumeAbnormal ）	风险	存储架	警告
异常电流范围（ ocumEvtShellfCurrentAbnormal ）	风险	存储架	警告
温度异常（ ocumEvtShellfTemperatureAbnormal ）	风险	存储架	警告

Storage VM 事件

Storage VM （ Storage Virtual Machine ，也称为 SVM ）事件可为您提供有关 Storage VM （ SVM ）状态的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
Storage VM CIFS服务已关闭(ocumEvtVserverCifsServiceStatusDown)	意外事件	SVM	严重
SVM CIFS 服务未配置（不适用）	事件	SVM	信息
尝试连接不存在的 CIFS 共享 *（nbladeCifsNoPrivShare）	意外事件	SVM	严重
CIFS NetBIOS 名称冲突 *（nbladeCifsNbNameConflict）	风险	SVM	error
CIFS 卷影复制操作失败 *（cifsShadow CopyFailure）	风险	SVM	error
多个 CIFS 连接 *（nbladeCifsManyAus）	风险	SVM	error
已超过最大 CIFS 连接数 *（nbladeCifsMaxOpenSameFile）	风险	SVM	error
已超过每个用户的 CIFS 连接数上限 *（nbladeCifsMaxSessPerUsrConn）	风险	SVM	error
SVM FC/FCoE 服务已关闭（ocumEvtVserverFcServiceStatusDown）	意外事件	SVM	严重
SVM iSCSI 服务已关闭（ocumEvtVserverIscsiServiceStatusDown）	意外事件	SVM	严重
Storage VM NFS服务已关闭(ocumEvtVserverNfsServiceStatusDown)	意外事件	SVM	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
SVM FC/FCoE 服务未配置（不适用）	事件	SVM	信息
未配置 SVM iSCSI 服务（不适用）	事件	SVM	信息
未配置 SVM NFS 服务（不适用）	事件	SVM	信息
Storage VM已停止(ocumEvtVserverDown)	风险	SVM	警告
AV 服务器太忙，无法接受新的扫描请求 *（nbladeVscanConnBackPressure）	风险	SVM	error
没有用于病毒扫描的 AV 服务器连接 *（nbladeVscanNoScannerConn ）	意外事件	SVM	严重
未注册 AV 服务器 *（nbladeVscanNoRegd扫描程序）	风险	SVM	error
无响应 AV 服务器连接 *（nbladeVscanConnInactive）	事件	SVM	信息
未经授权的用户尝试访问 AV 服务器 *（nbladeVscanBadUserPrivAccess ）	风险	SVM	error
AV 服务器发现病毒 *（nbladeVscanVirusDetected-）	风险	SVM	error

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已发现 SVM （不适用）	事件	SVM	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
SVM 已删除（不适用）	事件	集群	信息
SVM 已重命名（不适用）	事件	SVM	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 SVM IOPS 严重阈值（ ocumSvmIopsIncident ）	意外事件	SVM	严重
已违反 SVM IOPS 警告阈值（ ocumSvmIopsWarning ）	风险	SVM	警告
已违反 SVM MB/ 秒严重阈值（ ocumSvmMbpsIncident ）	意外事件	SVM	严重
已违反 SVM MB/ 秒警告阈值（ ocumSvmMbpsWarning ）	风险	SVM	警告
已违反 SVM 延迟严重阈值（ ocumSvmLatencyIncident ）	意外事件	SVM	严重
已违反 SVM 延迟警告阈值（ ocumSvmLatencyWarning ）	风险	SVM	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	**severity**
已禁用审核日志（ ocumVserverAudit 日志已禁用）	风险	SVM	警告
已禁用登录横幅（ ocumVserverLoginBannerDisabled ）	风险	SVM	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
SSH 正在使用不安全的密码（ ocumVserverSSHInsecure ）	风险	SVM	警告
已更改登录横幅（ ocumVserverLoginBannerChanged ）	风险	SVM	警告
已禁用 Storage VM 反勒索软件监控（已禁用反勒索软件服务）	风险	SVM	警告
已启用 Storage VM 反勒索软件监控（学习模式）（ antiRansomwareSvmStateDryrun ）	事件	SVM	信息
适用于反勒索软件监控的 Storage VM （学习模式）（ ocumEvtSvmArwCandidt ）	事件	SVM	信息

用户和组配额事件

用户和组配额事件可为您提供有关用户和用户组配额容量以及文件和磁盘限制的信息，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反用户或组配额磁盘空间软限制（已达到 ocumEvtUserOrGroupQuotaDiskSpaceSoftLimit ）	风险	用户或组配额	警告
已达到用户或组配额磁盘空间硬限制（ ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached ）	意外事件	用户或组配额	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反用户或组配额文件数软限制（已达到 ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached. ）	风险	用户或组配额	警告
已达到用户或组配额文件计数硬限制（ ocumEvtUserOrGroupQuotaFileCountHardLimit 已缓存）	意外事件	用户或组配额	严重

卷事件

卷事件提供了有关卷状态的信息，可用于监控潜在问题。事件按影响区域分组，并包括事件名称，陷阱名称，影响级别，源类型和严重性。

星号（ * ）表示已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	**severity**
卷受限（ ocumEvtVolumeRestricted ）	风险	Volume	警告
卷脱机（ ocumEvtVolumeOffline ）	意外事件	Volume	严重
卷部分可用（ ocumEvtVolumePartiallyAvailable ）	风险	Volume	error
已卸载卷（不适用）	事件	Volume	信息
卷已挂载（不适用）	事件	Volume	信息
卷已重新挂载（不适用）	事件	Volume	信息
卷接合路径处于非活动状态（ ocumEvtVolumeJunctionPathInactive ）	风险	Volume	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已启用卷自动调整大小（不适用）	事件	Volume	信息
卷自动调整大小 - 已禁用（不适用）	事件	Volume	信息
已修改卷自动调整大小最大容量（不适用）	事件	Volume	信息
已修改卷自动调整大小增量大小（不适用）	事件	Volume	信息

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
精简配置卷空间存在风险（ ocumThinProvisionVolumeSpaceAtRisk ）	风险	Volume	警告
卷效率操作错误(ocumEvtVolumeEfficiencyOperationError)	风险	Volume	error
卷空间已满（ ocumEvtVolumeFull ）	风险	Volume	error
卷空间接近全满（ ocumEvtVolumeNearlyFull ）	风险	Volume	警告
卷逻辑空间已满 *（ volumeLogicalSpaceFull ）	风险	Volume	error
卷逻辑空间接近全满 *（ volumeLogicalSpaceNearlyFull ）	风险	Volume	警告
卷逻辑空间正常 *（ volumeLogicalSpaceAllOK ）	事件	Volume	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
卷 Snapshot 预留空间已满（ ocumEvtSnapshotFull ）	风险	Volume	警告
Snapshot 副本太多（ ocumEvtSnapshotTooMany ）	风险	Volume	error
卷 qtree 配额已过量提交（ ocumEvtVolumeQtreeQuotaOvercommitted ）	风险	Volume	error
卷 qtree 配额接近过量提交（ ocumEvtVolumeQtreeQuotaAlmostOvercommitted ）	风险	Volume	警告
卷增长率异常（ ocumEvtVolumeGrowthRateAbnormal ）	风险	Volume	警告
卷达到全满前的天数（ ocumEvtVolumeDaysUntilFullSoon ）	风险	Volume	error
已禁用卷空间保证（不适用）	事件	Volume	信息
已启用卷空间保证（不适用）	事件	Volume	信息
已修改卷空间保证（不适用）	事件	Volume	信息
卷 Snapshot 预留达到全满前的天数（ ocumEvtVolumeSnapshotReserveDaysUntileFullSoon ）	风险	Volume	error
FlexGroup 成分卷存在空间问题 * （ flexGroupConconstituentsHaveSpaceIssues ）	风险	Volume	error

事件名称（陷阱名称）	影响级别	源类型	**severity**
FlexGroup 成分卷空间状态一切正常 *（ flexGroupConconstituentsSpaceStatusAllOK ）	事件	Volume	信息
FlexGroup 成分卷存在索引节点问题 *（ flexGroupConconstituentsHaveInodesIssues ）	风险	Volume	error
FlexGroup 成分卷索引节点状态一切正常 *（ flexGroupConconstituentsInodesStatusAllOK ）	事件	Volume	信息
WAFL 卷自动调整大小失败 *（ waflVolAutoSizeFail ）	风险	Volume	error
WAFL 卷自动调整大小已完成 *（ waflVolAutoSizeDone ）	事件	Volume	信息
FlexGroup 卷的利用率超过 80%*	意外事件	Volume	error
FlexGroup 卷的利用率超过 90% *	意外事件	Volume	严重
卷存储效率异常（ ocumVolumeAbnomStorageEfficiencyWarning ）	风险	Volume	警告
卷Snapshot预留未充分利用(volumeSnaphotReserveUnutilizedWarning)	事件	Volume	警告
卷Snapshot预留未充分利用(volumeSnaphotReserveUnutilizedCleared)	事件	Volume	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	**severity**
已重命名卷（不适用）	事件	Volume	信息
已发现卷（不适用）	事件	Volume	信息
已删除卷（不适用）	事件	Volume	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反 QoS 卷最大 IOPS 警告阈值（ ocumQosVolumeMaxIopsWarning ）	风险	Volume	警告
已违反 QoS 卷最大 MB/秒警告阈值（ ocumQosVolumeMaxMbpsWarning ）	风险	Volume	警告
已违反 QoS 卷最大 IOPS/TB 警告阈值（ ocumQosVolumeMaxIopsPerTbWarning ）	风险	Volume	警告
已违反性能服务级别策略定义的工作负载卷延迟阈值（ ocumConformanceLatencyWarning ）	风险	Volume	警告
已违反卷 IOPS 严重阈值（ ocumVolumeIopsIncident ）	意外事件	Volume	严重
已违反卷 IOPS 警告阈值（ ocumVolumeIopsWarning ）	风险	Volume	警告
已违反卷 MB/ 秒严重阈值（ ocumVolumeMbpsIncident ）	意外事件	Volume	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反卷 MB/ 秒警告阈值（ ocumVolumeMbpsWarning ）	风险	Volume	警告
已违反卷延迟严重阈值(ocumVolumeLatencyIncident)	意外事件	Volume	严重
已违反卷延迟警告阈值(ocumVolumeLatencyWarning)	风险	Volume	警告
已违反卷缓存未命中率严重阈值（ ocumVolumeCachedMisRatioIncident ）	意外事件	Volume	严重
已违反卷缓存未命中率警告阈值（ ocumVolumeCachedMisSRatioWarning ）	风险	Volume	警告
已违反卷延迟和 IOPS 严重阈值（ ocumVolumeLatencyIopsIncident ）	意外事件	Volume	严重
已违反卷延迟和 IOPS 警告阈值（ ocumVolumeLatencyIopsWarning ）	风险	Volume	警告
已违反卷延迟和 MB/ 秒严重阈值（ ocumVolumeLateLatencyMbpsIncident ）	意外事件	Volume	严重
已违反卷延迟和 MB/ 秒警告阈值（ ocumVolumeLatencyMbpsWarning ）	风险	Volume	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反卷延迟和聚合已用性能容量严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedIncident ）	意外事件	Volume	严重
已违反卷延迟和聚合已用性能容量警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedWarning ）	风险	Volume	警告
已违反卷延迟和聚合利用率严重阈值（ocumVolumeLatencyAggregateUtilizationIncident ）	意外事件	Volume	严重
已违反卷延迟和聚合利用率警告阈值（ocumVolumeLatencyAggregateUtilizationWarning ）	风险	Volume	警告
已违反卷延迟和节点已用性能容量严重阈值（ocumVolumeLatencyNodePerfCapacityUsedIncident ）	意外事件	Volume	严重
已违反卷延迟和节点已用性能容量警告阈值（ocumVolumeLatencyNodePerfCapacityUsedWarning ）	风险	Volume	警告
卷延迟和节点已用性能容量 - 已违反接管严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeOverIncident ）	意外事件	Volume	严重
卷延迟和节点已用性能容量 - 已违反接管警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeOverWarning ）	风险	Volume	警告

事件名称（陷阱名称）	影响级别	源类型	**severity**
已违反卷延迟和节点利用率严重阈值（ ocumVolumeLatencyNodeUtilizationIncident ）	意外事件	Volume	严重
已违反卷延迟和节点利用率警告阈值（ ocumVolumeLatencyNodeUtilizationWarning ）	风险	Volume	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	**severity**
已启用卷反勒索软件监控（活动模式）（已启用反勒索软件卷状态）	事件	Volume	信息
已禁用卷反勒索软件监控（已禁用反勒索软件卷）	风险	Volume	警告
已启用卷反勒索软件监控（学习模式）（ antiRansomwareVolumeStateDryrun ）	事件	Volume	信息
卷反勒索软件监控已暂停（学习模式）（ antiRansomwareVolumeStatedryrunPaused ）	风险	Volume	警告
卷反勒索软件监控已暂停（活动模式）（ antiRansomwareVolumeStateEnablePaused ）	风险	Volume	警告
卷反勒索软件监控正在禁用（ antiRansomwareVolumeStateDisableInProtect ）	风险	Volume	警告
发现的勒索软件活动（ callHomeRansomwareActivitySeen ）	意外事件	Volume	严重

事件名称（陷阱名称）	影响级别	源类型	**severity**
适用于反勒索软件监控的卷（学习模式）（ocumEvtVolumeArwCandidate/ ）	事件	Volume	信息
适用于反勒索软件监控的卷（主动模式）（ocumVolumeSuitedForActiveAn反 勒索软件检测）	风险	Volume	警告
卷出现高噪声反勒索软件警报（anantiRansomwareFeatureNoisyVolume ）	风险	Volume	警告

影响区域：数据保护

事件名称（陷阱名称）	影响级别	源类型	**severity**
卷的本地Snapshot保护不足(volumeLacksLocalProtectionWarning)	风险	Volume	警告
卷的本地Snapshot保护不足(volumeLacksLocalProtectionCleared)	风险	Volume	警告

卷移动状态事件

卷移动状态事件会告诉您卷移动的状态，以便您可以监控潜在问题。事件按影响区域分组，并包括事件和陷阱名称，影响级别，源类型和严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	**severity**
卷移动状态：正在进行（不适用）	事件	Volume	信息
卷移动状态 - 失败（ocumEvtVolumeMoveFailed ）	风险	Volume	error
卷移动状态：已完成（不适用）	事件	Volume	信息

事件名称（陷阱名称）	影响级别	源类型	**severity**
卷移动 - 转换延迟（ ocumEvtVolumeMoveCutoverDeferred ）	风险	Volume	警告

事件窗口和对话框的问题描述

事件会就您的环境中的任何问题向您发出通知。您可以使用事件管理清单页面和事件详细信息页面监控所有事件。您可以使用通知设置选项对话框配置通知。您可以使用事件设置页面禁用或启用事件。

通知页面

您可以将 Unified Manager 服务器配置为在生成事件或将事件分配给用户时发送通知。您还可以配置通知机制。例如，可以通过电子邮件或 SNMP 陷阱发送通知。

您必须具有应用程序管理员或存储管理员角色。

email

通过此区域，您可以为警报通知配置以下电子邮件设置：

- * 发件人地址 *

  指定发送警报通知的电子邮件地址。共享报告时，此值也用作报告的发件人地址。如果 " 发件人地址 " 已预先填充地址 ActiveIQUnifiedManager@localhost.com ，则应将其更改为实际有效的电子邮件地址，以确保所有电子邮件通知均已成功传送。

SMTP 服务器

使用此区域可以配置以下 SMTP 服务器设置：

- * 主机名或 IP 地址 *

  指定 SMTP 主机服务器的主机名，该主机服务器用于向指定的收件人发送警报通知。

- * 用户名 *

  指定 SMTP 用户名。只有在 SMTP 服务器中启用了 SMTPAUTH 时，才需要 SMTP 用户名。

- * 密码 *

  指定 SMTP 密码。只有在 SMTP 服务器中启用了 SMTPAUTH 时，才需要 SMTP 用户名。

- * 端口 *

  指定 SMTP 主机服务器用于发送警报通知的端口。

  默认值为 25. 。

- * 使用 start/tls*

  选中此复选框可使用 TLS/SSL 协议（也称为 start_tls 和 StartTLS ）在 SMTP 服务器和管理服务器之间提供安全通信。

- * 使用 SSL*

  选中此复选框可使用 SSL 协议在 SMTP 服务器和管理服务器之间提供安全通信。

SNMP

使用此区域可以配置以下 SNMP 陷阱设置：

- * 版本 *

  根据所需的安全类型指定要使用的 SNMP 版本。选项包括版本 1 ，版本 3 ，具有身份验证的版本 3 以及具有身份验证和加密的版本 3 。默认值为版本 1 。

- * 陷阱目标主机 *

  指定接收管理服务器发送的 SNMP 陷阱的主机名或 IP 地址（ IPv4 或 IPv6 ）。要指定多个陷阱目标，请使用逗号分隔每个主机。

  列表中所有主机的所有其他 SNMP 设置都必须相同，例如 " 版本 " 和 " 出站端口 " 。

- * 出站陷阱端口 *

  指定 SNMP 服务器接收管理服务器发送的陷阱所通过的端口。

  默认值为 162. 。

- * 社区 *

  用于访问主机的社区字符串。

- * 引擎 ID*

  指定 SNMP 代理的唯一标识符，并由管理服务器自动生成。引擎 ID 可用于 SNMP 版本 3 ，具有身份验证的 SNMP 版本 3 和具有身份验证和加密的 SNMP 版本 3 。

- * 用户名 *

  指定 SNMP 用户名。用户名可用于 SNMP 版本 3 ， SNMP 版本 3 和 SNMP 版本 3 以及身份验证和加密。

- * 身份验证协议 *

  指定用于对用户进行身份验证的协议。协议选项包括 MD5 和 SHA 。默认值为 MD5 。身份验证协议适用于具有身份验证的 SNMP 版本 3 和具有身份验证和加密的 SNMP 版本 3 。

- * 身份验证密码 *

  指定对用户进行身份验证时使用的密码。身份验证密码可用于具有身份验证的 SNMP 版本 3 和具有身份验

证和加密的 SNMP 版本 3 。

- * 隐私协议 *

  指定用于对 SNMP 消息进行加密的隐私协议。协议选项包括 AES 128 和 DES 。默认值为 AES 128 。SNMP 版本 3 提供了隐私协议，并支持身份验证和加密。

- * 隐私密码 *

  指定使用隐私协议时的密码。隐私密码适用于具有身份验证和加密功能的 SNMP 版本 3 。

有关SNMP对象和陷阱的详细信息、您可以下载 "Active IQ Unified Manager MIB" 从NetApp 支持站点。

事件管理清单页面

通过事件管理清单页面，您可以查看当前事件及其属性的列表。您可以执行确认，解决和分配事件等任务。您还可以为特定事件添加警报。

此页面上的信息每 5 分钟自动刷新一次，以确保显示最新的新事件。

筛选组件

用于自定义事件列表中显示的信息。您可以使用以下组件细化显示的事件列表：

- 查看菜单，从预定义的筛选器选择列表中进行选择。

  其中包括所有活动（新的和已确认的）事件，活动性能事件，分配给我（已登录用户）的事件以及在所有维护窗口期间生成的所有事件等项。

- 搜索窗格，用于输入完整或部分术语来细化事件列表。
- 筛选器按钮，用于启动筛选器窗格，以便您可以从每个可用字段和字段属性中进行选择，以细化事件列表。

命令按钮

命令按钮可用于执行以下任务：

- * 分配给 *

  用于选择将事件分配给的用户。将事件分配给用户时，系统会将用户名和事件分配时间添加到选定事件的事件列表中。

  - 我

    将事件分配给当前已登录的用户。

  - 其他用户

    显示分配所有者对话框，在此可以将事件分配或重新分配给其他用户。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。

确认某个事件后，系统会将您的用户名以及事件确认时间添加到选定事件的事件列表中。确认事件后，您负责管理该事件。

您无法确认信息事件。

- * 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以及解决该事件的时间添加到选定事件的事件列表中。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。

- * 报告 *

  用于将当前事件视图的详细信息导出为逗号分隔值（ .csv ）文件或 PDF 文档。

- * 显示 / 隐藏列选择器 *

  用于选择页面上显示的列并选择其显示顺序。

事件列表

显示按触发时间排序的所有事件的详细信息。

默认情况下，将显示所有活动事件视图，以显示过去七天影响级别为 " 意外事件 " 或 " 风险 " 的 " 新增 " 和 " 已确认 " 事件。

- * 触发时间 *

  生成事件的时间。

- * 严重性 *

  事件严重性：严重（），错误（），警告（）和信息（）。

- * 状态 *

  事件状态： " 新增 " ， " 已确认 " ， " 已解决 " 或 " 已废弃 " 。

- * 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。

- * 名称 *

  事件名称。您可以选择此名称以显示该事件的 " 事件 " 详细信息页面。

- * 源 *

  发生事件的对象的名称。您可以选择此名称以显示该对象的运行状况或性能详细信息页面。

  如果发生共享 QoS 策略违规，则此字段仅会显示消耗的 IOPS 或 MB/ 秒最多的工作负载对象。使用此策略的其他工作负载将显示在事件详细信息页面中。

- * 源类型 *

  与事件关联的对象类型（例如 Storage VM ，卷或 qtree ）。

- * 已分配给 *

  将事件分配到的用户的名称。

- * 事件源 *

  事件来自 Active IQ 门户还是直接来自 Active IQ Unified Manager 。

- * 标注名称 *

  分配给存储对象的标注的名称。

- * 注释 *

  为事件添加的注释数。

- * 未完成天数 *

  自事件最初生成以来的天数。

- * 分配时间 *

  自事件分配给用户以来经过的时间。如果经过的时间超过一周，则会显示将事件分配给用户的时间戳。

- * 确认者 *

  确认事件的用户的名称。如果事件未确认，则此字段为空。

- * 确认时间 *

  自事件确认以来经过的时间。如果经过的时间超过一周，则会显示确认事件的时间戳。

- * 解决者 *

  解决此事件的用户的名称。如果事件未解决，则此字段为空。

- * 解决时间 *

自事件解决以来经过的时间。如果经过的时间超过一周，则会显示解决事件的时间戳。

- * 已废弃时间 *

  事件状态变为 " 已废弃 " 的时间。

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。

  有关此处显示的组件的问题描述，请参见 _Cluster 组件及其可能发生争用的原因。

" 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（  ）。

- * 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。

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。

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。

事件设置页面

"Event Setup" 页面将显示已禁用的事件列表，并提供相关对象类型和事件严重性等信息。您还可以执行全局禁用或启用事件等任务。

只有当您具有应用程序管理员或存储管理员角色时，才能访问此页面。

命令按钮

命令按钮可用于对选定事件执行以下任务：

- * 禁用 *

  启动 " 禁用事件 " 对话框，在此可以禁用事件。

- * 启用 *

  启用先前选择禁用的选定事件。

- * 上传规则 *

  启动 " 上传规则 " 对话框，在此可以使无法访问外部网络的站点手动将 Active IQ 规则文件上传到 Unified Manager 。这些规则针对集群 AutoSupport 消息运行，以生成 Active IQ 平台定义的系统配置，布线，最佳实践和可用性事件。

- * 订阅 EMS 事件 *

  启动订阅 EMS 事件对话框，在此可以订阅从所监控集群接收特定事件管理系统（ EMS ）事件。EMS 收集有关集群上发生的事件的信息。收到订阅 EMS 事件的通知后，系统将生成具有相应严重性的 Unified Manager 事件。

列表视图

列表视图以表格形式显示有关已禁用事件的信息。您可以使用列筛选器自定义显示的数据。

- * 事件 *

  显示已禁用的事件的名称。

- * 严重性 *

  显示事件的严重性。严重性可以是 " 严重 " ， " 错误 " ， " 警告 " 或 " 信息 " 。

- * 源类型 *

  显示生成事件的源类型。

禁用事件对话框

" 禁用事件 " 对话框将显示可禁用事件的事件类型列表。您可以根据特定严重性为事件类型禁用事件，也可以为一组事件禁用事件。

您必须具有应用程序管理员或存储管理员角色。

事件属性区域

事件属性区域指定以下事件属性：

- * 事件严重性 *

  用于根据严重性类型选择事件，可以是 " 严重 " ， " 错误 " ， " 警告 " 或 " 信息 " 。

- * 事件名称包含 *

  用于筛选名称包含指定字符的事件。

- * 匹配事件 *

  显示与您指定的事件严重性类型和文本字符串匹配的事件列表。

- * 禁用事件 *

  显示已选择禁用的事件的列表。

  此外，还会显示事件的严重性以及事件名称。

命令按钮

命令按钮可用于对选定事件执行以下任务：

- * 保存并关闭 *

  禁用事件类型并关闭对话框。

- * 取消 *

  丢弃所做的更改并关闭对话框。

管理警报

您可以将警报配置为在发生特定事件或特定严重性类型的事件时自动发送通知。您还可以将警报与触发警报时执行的脚本相关联。

什么是警报

事件持续发生时，只有当事件满足指定的筛选条件时， Unified Manager 才会生成警报。您可以选择应生成警报的事件，例如，超过空间阈值或对象脱机时。您还可以将警报与触发警报时执行的脚本相关联。

筛选条件包括对象类，名称或事件严重性。

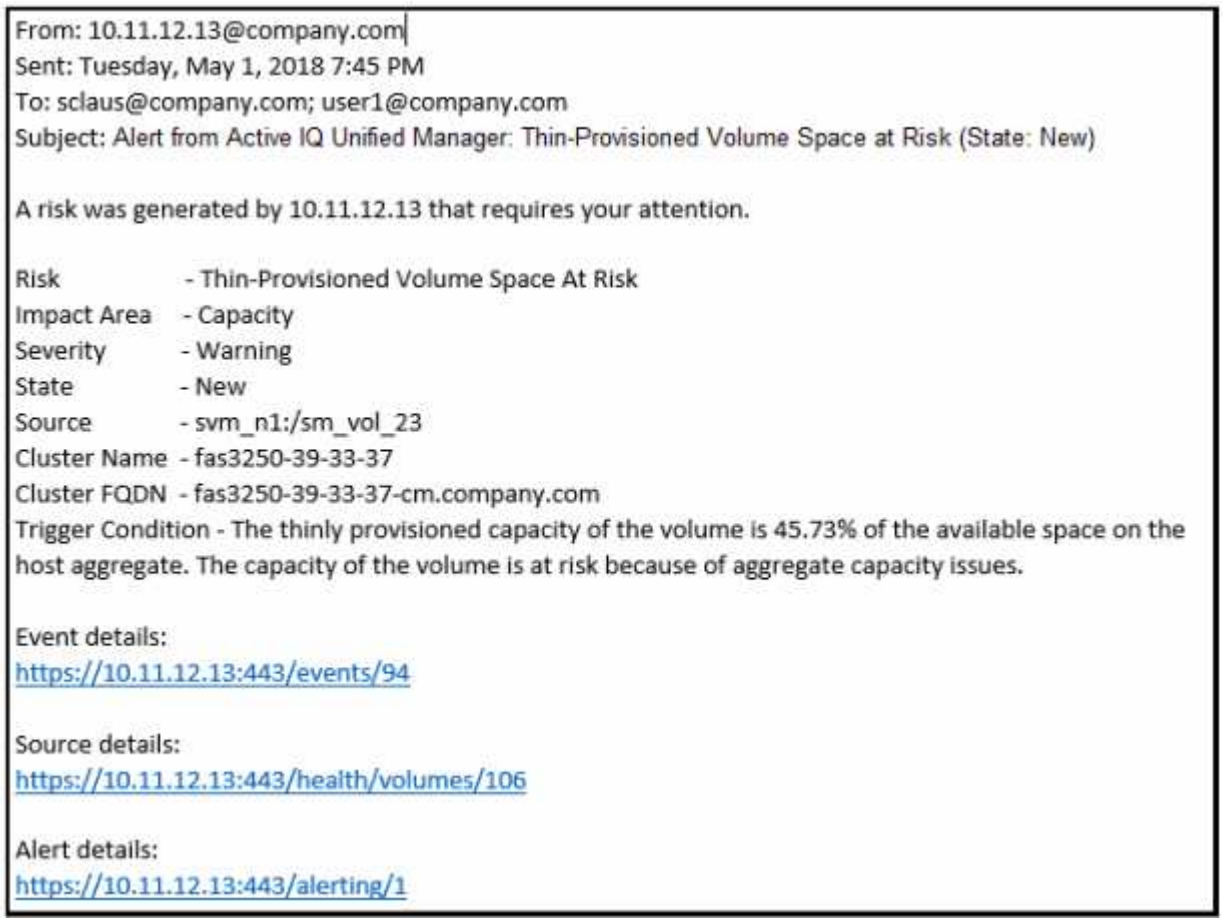
警报电子邮件中包含哪些信息

Unified Manager 警报电子邮件可提供事件类型，事件严重性，为发生原因事件而违反的策略或阈值的名称以及事件的问题描述。此电子邮件还为每个事件提供了一个超链接，可用于在用户界面中查看此事件的详细信息页面。

警报电子邮件会发送给订阅接收警报的所有用户。

如果性能计数发生原因器或容量值在收集期间发生较大变化，则对于同一阈值策略，可能会同时触发严重事件和警告事件。在这种情况下，您可能会收到一封有关警告事件的电子邮件和一封有关严重事件的电子邮件。这是因为您可以通过 Unified Manager 单独订阅来接收警告和严重阈值违规的警报。

下面显示了一个警报电子邮件示例：


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

添加警报

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

开始之前

- 您必须已配置通知设置，例如用户电子邮件地址， SMTP 服务器和 SNMP 陷阱主机，以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。
- 您必须了解要触发警报的资源和事件，以及要通知的用户的用户名或电子邮件地址。

- 如果要根据事件执行脚本，则必须已使用脚本页面将脚本添加到 Unified Manager 中。
- 您必须具有应用程序管理员或存储管理员角色。

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

步骤

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

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

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

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

   要选择多个事件，请在选择时按 Ctrl 键。

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

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

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 * 保存 * 。

添加警报的示例

此示例显示了如何创建满足以下要求的警报：

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

在添加警报对话框中执行以下步骤：

1. 单击 * 名称 * ，然后在 * 警报名称 * 字段中输入 *`HealthTest` * 。
2. 单击 * 资源 * ，然后在包括选项卡中，从下拉列表中选择 * 卷 * 。

a. 在 * 名称包含 * 字段中输入 *`abc` * ，以显示名称包含 "abc" 的卷。

b. 选择 * +[All Volumes whose name contains 'abc']从 "Available Resources" 区域中选择 +* ，然后将其移动到 "Selected Resources" 区域。

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

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

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

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

添加警报的准则

您可以根据资源添加警报，例如集群，节点，聚合或卷以及特定严重性类型的事件。作为最佳实践，您可以在添加任何关键对象所属的集群后为该对象添加警报。

您可以使用以下准则和注意事项创建警报，以便有效地管理系统：

- 警报问题描述

  您应为此警报提供一个问题描述，以帮助您有效地跟踪警报。

- Resources

  您应确定哪些物理或逻辑资源需要警报。您可以根据需要包括和排除资源。例如，如果要通过配置警报来密切监控聚合，则必须从资源列表中选择所需的聚合。

  如果选择资源类别，例如 * +[All User or Group Quotas]之后，您将收到该类别中所有对象的警报。

  > 选择集群作为资源不会自动选择该集群中的存储对象。例如，如果为所有集群的所有严重事件创建警报，则只会收到集群严重事件的警报。您不会收到节点，聚合等上的严重事件警报。

- 事件严重性

  您应确定指定严重性类型的事件（严重，错误，警告）是否应触发警报，如果是，则应触发哪种严重性类型。

- 选定事件

  如果您根据生成的事件类型添加警报，则应确定哪些事件需要警报。

  如果您选择事件严重性，但未选择任何单个事件（如果您将 " 选定事件 " 列留空），则会收到此类别中所有事件的警报。

- 操作

  您必须提供接收通知的用户的用户名和电子邮件地址。您还可以将 SNMP 陷阱指定为通知模式。您可以将脚本与警报关联，以便在生成警报时执行这些脚本。

- 通知频率

  您可以将警报配置为在指定时间内向收件人重复发送通知。您应确定警报的事件通知处于活动状态的时间。如果要在事件确认之前重复发送事件通知，则应确定重复发送通知的频率。

- 执行脚本

  您可以将脚本与警报关联。生成警报时会执行脚本。

添加性能事件警报

您可以为单个性能事件配置警报，就像 Unified Manager 收到的任何其他事件一样。此外，如果您希望对所有性能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，以便在触发任何严重或警告性能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。

以下示例显示了如何为所有严重延迟， IOPS 和 MBps 事件创建事件。您可以使用相同的方法从所有性能计数器中选择事件，并为所有警告事件选择事件。

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. 请勿在 * 资源 * 页面上选择任何资源。

   由于未选择任何资源，因此警报将应用于接收这些事件的所有集群，聚合，卷等。

5. 单击 * 事件 * 并执行以下操作：
   a. 在事件严重性列表中，选择 * 严重 * 。
   b. 在 Event Name contains 字段中，输入 *`latency` * ，然后单击箭头以选择所有匹配的事件。
   c. 在 Event Name contains 字段中，输入 *`IOPS` * ，然后单击箭头以选择所有匹配的事件。
   d. 在 Event Name contains 字段中，输入 * `mbps` * ，然后单击箭头以选择所有匹配的事件。
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. 在此页面上配置用于发出 SNMP 陷阱和执行脚本的任何其他选项。
8. 单击 * 保存 * 。

测试警报

您可以测试警报，以验证是否已正确配置警报。触发事件后，系统将生成警报，并向配置的收件人发送警报电子邮件。您可以使用测试警报验证是否发送通知以及是否执行脚本。

开始之前

- 您必须已配置通知设置，例如收件人的电子邮件地址， SMTP 服务器和 SNMP 陷阱。

  Unified Manager 服务器可以使用这些设置在生成事件时向用户发送通知。

- 您必须已分配脚本并将脚本配置为在生成警报时运行。
- 您必须具有应用程序管理员角色。

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，选择要测试的警报，然后单击 * 测试 * 。

   系统会向您在创建警报时指定的电子邮件地址发送测试警报电子邮件。

启用和禁用已解决和已过时事件的警报

对于已配置为发送警报的所有事件，当这些事件过渡到所有可用状态时，系统会发送一条警报消息： " 新增 " ， " 已确认 " ， " 已解决 " 和 " 已废弃 " 。如果您不希望在事件进入 " 已解决 " 和 " 已废弃 " 状态时接收警报，则可以配置全局设置以禁止这些警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

默认情况下，当事件进入 " 已解决 " 和 " 已废弃 " 状态时，不会针对这些事件发送警报。

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，使用 * 已解决和已废弃事件的警报 * 项目旁边的滑块控件执行以下操作之一：

至 ...	执行此操作 ...
在事件已解决或已废弃时停止发送警报	将滑块控件移至左侧
在事件已解决或已废弃时开始发送警报	将滑块控件移至右侧

排除灾难恢复目标卷生成警报

配置卷警报时，您可以在警报对话框中指定一个字符串，用于标识一个卷或一组卷。但是，如果为 SVM 配置了灾难恢复，则源卷和目标卷的名称相同，因此您将收到这两个卷的警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以通过排除名称为目标 SVM 的卷来禁用灾难恢复目标卷的警报。之所以可以这样做，是因为卷事件的标识符同时包含 SVM 名称和卷名称，格式为 "<SVM_name>： /<volume_name>" 。

以下示例显示了如何在主 SVM"vs1" 上为卷 "vol1" 创建警报，但不会在 SVM"vs1-dr" 上同名的卷上生成警报。

在添加警报对话框中执行以下步骤：

步骤

1. 单击 * 名称 * ，然后输入警报的名称和问题描述。
2. 单击 * 资源 * ，然后选择 * 包括 * 选项卡。
   a. 从下拉列表中选择 * 卷 * ，然后在 * 名称包含 * 字段中输入 *`vol1` * ，以显示名称包含 "vol1" 的卷。
   b. 选择 * +[All Volumes whose name contains 'vol1']从 * 可用资源 * 区域中选择 +* ，然后将其移动到 * 选定资源 * 区域。
3. 选择 * 排除 * 选项卡，选择 * 卷 * ，在 * 名称包含 * 字段中输入 *`vs1-dr` * ，然后单击 * 添加 * 。

   这样就不会为 SVM"vs1-dr" 上的卷 "vol1" 生成警报。
4. 单击 * 事件 * 并选择要应用于卷的一个或多个事件。
5. 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。
6. 在此页面上配置用于发出 SNMP 陷阱和执行脚本的任何其他选项，然后单击 * 保存 * 。

查看警报

您可以从 "Alert Setup" 页面查看为各种事件创建的警报列表。您还可以查看警报属性，例如警报问题描述，通知方法和频率，触发警报的事件，警报的电子邮件收件人以及受影响的资源（例如集群，聚合和卷）。

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 * 存储管理 * > * 警报设置 * 。

   警报列表将显示在 "Alert Setup" 页面中。

编辑警报

您可以编辑警报属性，例如与警报关联的资源，事件，收件人，通知选项，通知频率， 和关联脚本。

开始之前

您必须具有应用程序管理员角色。

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，选择要编辑的警报，然后单击 * 编辑 * 。
3. 在 * 编辑警报 * 对话框中，编辑名称，资源，事件和操作部分， 根据需要。

   您可以更改或删除与警报关联的脚本。

4. 单击 * 保存 * 。

删除警报

您可以删除不再需要的警报。例如，如果 Unified Manager 不再监控某个特定资源，则可以删除为该资源创建的警报。

开始之前

您必须具有应用程序管理员角色。

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 * 页面上，选择要删除的警报，然后单击 * 删除 * 。
3. 单击 * 是 * 确认删除请求。

警报窗口和对话框的问题描述

您应使用添加警报对话框配置警报以接收有关事件的通知。您还可以从 "Alert Setup" 页面查看警报列表。

警报设置页面

"Alert Setup" 页面将显示警报列表，并提供有关警报名称，状态，通知方法和通知频率的信息。您还可以从此页面添加，编辑，删除，启用或禁用警报。

您必须具有应用程序管理员或存储管理员角色。

命令按钮

- * 添加 * 。

  显示添加警报对话框，在此可以添加新警报。

- * 编辑 * 。

  显示编辑警报对话框，在此可以编辑选定警报。

- * 删除 *

  删除选定警报。

- * 启用 *

  启用选定警报以发送通知。

- * 禁用 *

  如果要暂时停止发送通知，则禁用选定警报。

- * 测试 *

  添加或编辑选定警报后，将对其进行测试以验证其配置。

- * 已解决和已废弃事件的警报 *

  允许您在事件移至 " 已解决 " 或 " 已废弃 " 状态时启用或禁用警报发送。这样可以帮助用户接收不必要的通知。

列表视图

列表视图以表格形式显示有关已创建警报的信息。您可以使用列筛选器自定义显示的数据。您也可以选择警报，以便在详细信息区域中查看其详细信息。

- * 状态 *

  指定是否启用警报（  ）或已禁用（  ）。

- * 警报 *

  显示警报的名称。

- * 问题描述 *

  显示警报的问题描述。

- * 通知方法 *

  显示为警报选择的通知方法。您可以通过电子邮件或 SNMP 陷阱通知用户。

- * 通知频率 *

  指定在事件被确认，解决或移至 " 已废弃 " 状态之前管理服务器继续发送通知的频率（以分钟为单位）。

详细信息区域

详细信息区域提供了有关选定警报的详细信息。

- * 警报名称 *

  显示警报的名称。

- * 警报问题描述 *

显示警报的问题描述。

- * 事件 *

  显示要触发警报的事件。

- * 资源 *

  显示要触发警报的资源。

- * 包括 *

  显示要触发警报的资源组。

- * 不包括 *

  显示不希望触发警报的资源组。

- * 通知方法 *

  显示警报的通知方法。

- * 通知频率 *

  显示在事件被确认，解决或移至 " 已废弃 " 状态之前管理服务器继续发送警报通知的频率。

- * 脚本名称 *

  显示与选定警报关联的脚本的名称。此脚本会在生成警报时执行。

- * 电子邮件收件人 *

  显示接收警报通知的用户的电子邮件地址。

添加警报对话框

您可以创建警报，以便在生成特定事件时向您发出通知，从而快速解决问题描述问题，从而最大限度地减少对环境的影响。您可以为单个资源或一组资源以及特定严重性类型的事件创建警报。您还可以指定警报的通知方法和频率。

您必须具有应用程序管理员或存储管理员角色。

Name

使用此区域可以指定警报的名称和问题描述：

- * 警报名称 *

  用于指定警报名称。

- * 警报问题描述 *

用于指定警报的问题描述。

Resources

通过此区域，您可以根据要触发警报的动态规则选择单个资源或对资源进行分组。*dynamic rule* 是根据您指定的文本字符串筛选的一组资源。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称来显示特定资源。

如果您从任何存储对象详细信息页面创建警报，则此存储对象将自动包含在警报中。

- * 包括 *

  用于包括要触发警报的资源。您可以指定一个文本字符串，以便对与该字符串匹配的资源进行分组，并选择要包含在警报中的此组。例如，您可以对名称包含 "abc" 字符串的所有卷进行分组。

- * 排除 *

  用于排除不希望触发警报的资源。例如，您可以排除名称包含 "xyz" 字符串的所有卷。

  只有在选择特定资源类型的所有资源时，才会显示排除选项卡：例如 <<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>

  如果某个资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为此事件生成警报。

事件

通过此区域，您可以选择要为其创建警报的事件。您可以根据特定严重性为事件创建警报，也可以为一组事件创建警报。

要选择多个事件，应在选择时按住 Ctrl 键。

- * 事件严重性 *

  用于根据严重性类型选择事件，可以是 " 严重 " ， " 错误 " 或 " 警告 " 。

- * 事件名称包含 *

  用于选择名称包含指定字符的事件。

操作

通过此区域，您可以指定要在触发警报时通知的用户。您还可以指定通知方法和通知频率。

- * 向这些用户发送警报 *

  用于指定接收通知的用户的电子邮件地址或用户名。

  如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则 " 名称 " 字段将显示为空，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果您已从用户页面修改选定用户的电子邮件地址，则修改后的电子邮件地址不会针对选定用户进行更新。

- * 通知频率 *

  用于指定在事件被确认，解决或移至已废弃状态之前管理服务器发送通知的频率。

  您可以选择以下通知方法：

  - 仅通知一次
  - 按指定频率通知
  - 在指定时间范围内以指定频率通知

- * 问题描述 SNMP 陷阱 *

  选中此框可指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- * 执行脚本 *

  用于将自定义脚本添加到警报。此脚本会在生成警报时执行。

  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。

命令按钮

- * 保存 *

  创建警报并关闭对话框。

- * 取消 *

  丢弃所做的更改并关闭对话框。

编辑警报对话框

您可以编辑警报属性，例如与警报关联的资源，事件，脚本和通知选项。

Name

通过此区域，您可以编辑警报的名称和问题描述。

- * 警报名称 *

  用于编辑警报名称。

- * 警报问题描述 *

  用于指定警报的问题描述。

- * 警报状态 *

  用于启用或禁用警报。

Resources

通过此区域，您可以根据要触发警报的动态规则选择单个资源或对资源进行分组。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称来显示特定资源。

- * 包括 *

  用于包括要触发警报的资源。您可以指定一个文本字符串，以便对与该字符串匹配的资源进行分组，并选择要包含在警报中的此组。例如，您可以对名称包含 "`vol0` " 字符串的所有卷进行分组。

- * 排除 *

  用于排除不希望触发警报的资源。例如，您可以排除名称包含 "`xyz` " 字符串的所有卷。

  只有在选择特定资源类型的所有资源时，才会显示排除选项卡，例如 <<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>

事件

通过此区域，您可以选择要触发警报的事件。您可以根据特定严重性为事件触发警报，也可以针对一组事件触发警报。

- * 事件严重性 *

  用于根据严重性类型选择事件，可以是 " 严重 " ， " 错误 " 或 " 警告 " 。

- * 事件名称包含 *

  用于选择名称包含指定字符的事件。

操作

此区域用于指定通知方法和通知频率。

- * 向这些用户发送警报 *

  用于编辑电子邮件地址或用户名，或者指定新的电子邮件地址或用户名以接收通知。

- * 通知频率 *

  用于编辑管理服务器发送通知的频率，直到事件被确认，解决或移至已废弃状态为止。

  您可以选择以下通知方法：

  - 仅通知一次
  - 按指定频率通知
  - 在指定时间范围内以指定频率通知

- * 问题描述 SNMP 陷阱 *

  用于指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- * 执行脚本 *

  用于将脚本与警报关联。此脚本会在生成警报时执行。

命令按钮

- * 保存 *

  保存更改并关闭对话框。

- * 取消 *

  丢弃所做的更改并关闭对话框。

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。

- 相关信息 *

"启用和禁用脚本上传功能"

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：

- ` - 事件 ID`
- `-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`
```

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。

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 * 。

◦ 相关信息 *

"启用和禁用脚本上传功能"

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	a. 单击 * 添加 * 。 b. 在操作部分中，将警报与测试脚本关联。
编辑警报	a. 选择警报，然后单击 * 编辑 * 。 b. 在操作部分中，将警报与测试脚本关联。

5. 单击 * 保存 * 。
6. 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。

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。

所有命令都必须在命令 `um CLI login` 前面加上有效的用户名和密码以进行身份验证。

要运行_um run_命令、请确保您的帐户具有_console应用程序访问权限。

CLI 命令	Description	输出
`um CLI login -u <username> [-p <password>]`	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` 注销	从命令行界面注销。	显示相应的消息。
帮助	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。

CLI 命令	Description	输出
运行查询 `<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 ，` 和分析消息 。
`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。
`um option list [ <opment>` … 。	列出了可使用 set 命令配置的所有选项。	以表格形式显示以下值： 名称，值，默认值和需要重新启动。
`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` 版本	显示 Unified Manager 软件版本。	版本（ `"9.6"` ）

CLI 命令	Description	输出
`um lun list （ -q] ） [ -objectType <object-id>]`	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` * 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 。	以表格形式显示以下值： `ID` 和 `LUN` 路径。
`um SVM list （ -q] ） [ -objectType <object-id>]`	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` * 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 。	以表格形式显示以下值： 名称和集群 `ID` 。
`um qtree list （ -q] ） [ -objectType <object-id>]`	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` * 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 。	以表格形式显示以下值： `qtree ID` 和 `qtree` 名称。

CLI 命令	Description	输出
`um disk list （ -q] ） （ -objectType <object-id>> )`	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` * 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。	以表格形式显示以下值 `ObjectType` 和 `object-id` 。
`um cluster list （ -q] ） （ -objectType <object-id>> )`	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` * 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。	以表格形式显示以下值： 名称，全名，序列号，数据源 `ID` ，上次刷新时间， 和资源密钥 。
`um cluster node list （ -q] ） （ -objectType <object-id>> )`	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` * 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。	以表格形式显示以下值 名称和集群 `ID` 。

CLI 命令	Description	输出
`um volume list （ -q] ） （ -objectType <object-id>> )`	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` * 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。	以表格形式显示以下值 卷 `ID` 和卷名称 。
`um quota user list` （ < 配额用户列表） `"-q]` （ `-objectType < 对象 ID >` ）	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 用户列表 -cluster 1` * 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。	以表格形式显示以下值 `ID` ，名称 ， `SID` 和电子邮件 。
`um aggr list （ -q] ） （ -objectType <object-id>> )`	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` * 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。	以表格形式显示以下值 `Aggr ID` 和 `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。

CLI 命令	Description	输出
`um event assign -u <username> <event-id>`	将事件分配给用户。	显示相应的消息。
事件列表 `[ -s <source> ] [ -S <event-state-filter-list> 。] < 事件 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 `Ssource ， source type ， Name ， Severity ， State ，` 用户和时间戳 。
`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。

脚本窗口和对话框的问题描述

通过脚本页面，您可以向 Unified Manager 添加脚本。

脚本页面

通过脚本页面，您可以将自定义脚本添加到 Unified Manager 中。您可以将这些脚本与警报关联，以便自动重新配置存储对象。

通过脚本页面，您可以在 Unified Manager 中添加或删除脚本。

命令按钮

- * 添加 * 。

  显示添加脚本对话框，在此可以添加脚本。

- * 删除 *

  删除选定脚本。

列表视图

列表视图以表格形式显示您添加到 Unified Manager 的脚本。

- * 名称 *

  显示脚本的名称。

- * 问题描述 *

  显示脚本的问题描述。

通过添加脚本对话框，您可以向 Unified Manager 添加脚本。您可以使用脚本配置警报，以自动解决为存储对象生成的事件。

您必须具有应用程序管理员或存储管理员角色。

- * 选择脚本文件 *

  用于为警报选择脚本。

- * 问题描述 *

  用于为脚本指定问题描述。