管理事件和警报

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-918/events/concept_what_active_iq_platform_events_are.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

管理事件和警报 1
管理事件 1
了解 Active IQ Unified Manager 中的 Active IQ 平台事件 1
Event Management System 事件是什么 1
了解 Active IQ Unified Manager 如何处理收到的事件 5
在 Active IQ Unified Manager 中查看事件详细信息 6
在 Active IQ Unified Manager 中查看未分配的事件 7
确认并解决 Active IQ Unified Manager 中的事件 7
在 Active IQ Unified Manager 中将事件分配给特定用户 8
在 Active IQ Unified Manager 中禁用不需要的事件 8
使用 Active IQ Unified Manager 中的自动修复功能修复问题 9
在 Active IQ Unified Manager 中启用和禁用 Active IQ 事件报告 10
在 Active IQ Unified Manager 中上传新的 Active IQ 规则文件 11
Active IQ Unified Manager 如何生成 Active IQ 平台事件 11
在 Active IQ Unified Manager 中解决 Active IQ 平台事件 12
在 Active IQ Unified Manager 中配置事件保留设置 13
什么是 Unified Manager 维护窗口 13
在 Active IQ Unified Manager 中管理主机系统资源事件 15
详细了解事件 16
事件和严重性类型列表 20
事件窗口和对话框说明 63
管理提醒 75
了解 Active IQ Unified Manager 中的警报 75
Active IQ Unified Manager 警报电子邮件中包含的信息 75
添加警报 76
在 Active IQ Unified Manager 中添加性能事件警报 78
在 Active IQ Unified Manager 中测试警报 79
在 Active IQ Unified Manager 中禁用已解决和已过时事件的警报 79
在 Active IQ Unified Manager 中排除灾难恢复目标卷以避免生成警报 80
在 Active IQ Unified Manager 中查看警报 80
在 Active IQ Unified Manager 中编辑警报 81
删除 Active IQ Unified Manager 中的警报 81
警报窗口和对话框的说明 81
管理脚本 87
在 Active IQ Unified Manager 中管理脚本 87
脚本如何与 Active IQ Unified Manager 中的警报配合使用 87
在 Active IQ Unified Manager 中添加脚本 88
删除 Active IQ Unified Manager 中的脚本 89
在 Active IQ Unified Manager 中执行测试脚本 89

了解受支持的 Active IQ Unified Manager CLI 命令 90
脚本窗口和对话框的说明 94

管理事件和警报

管理事件

了解 **Active IQ Unified Manager** 中的 **Active IQ** 平台事件

Unified Manager 可显示 Active IQ 平台发现的事件。这些事件是通过针对由 Unified Manager 监视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，并且仅在有新规则时才下载新文件。在没有外部网络访问权限的站点中，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 事件不会与现有的 Unified Manager 事件重叠，它们可识别与系统配置、布线、最佳实践和可用性问题相关的突发事件或风险。

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 Active IQ 规则文件"。

NetApp Active IQ 是一种基于云的服务，可提供预测分析和主动支持，以优化整个 NetApp 混合云的存储系统运行。有关详细信息，请参见 "NetApp Active IQ"。

Event Management System 事件是什么

了解 **Active IQ Unified Manager** 中的事件管理系统事件

Event Management System (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。集中式监控和管理简化了基于这些 EMS 事件的关键 EMS 事件和警报通知的配置。

将集群添加到 Unified Manager 时，会将 Unified Manager 地址作为通知目标添加到集群。EMS 事件在集群中发生后立即报告。

在 Unified Manager 中接收 EMS 事件有两种方法：

- 一定数量的重要 EMS 事件会自动报告。
- 您可以订阅接收单个 EMS 事件。

Unified Manager 生成的 EMS 事件会根据生成事件的方法进行不同的报告：

功能	自动 **EMS** 消息	订阅的 **EMS** 消息
可用的 EMS 事件	EMS 事件的子集	所有 EMS 事件
触发时的 EMS 消息名称	Unified Manager 事件名称（从 EMS 事件名称转换而来）	非特定，格式为“Error EMS received”。详细消息提供实际 EMS 事件的点符号格式

功能	自动 **EMS** 消息	订阅的 **EMS** 消息
收到的消息	一旦发现此集群	在将每个所需的 EMS 事件添加到 Unified Manager 之后，以及在接下来的 15 分钟轮询周期之后
事件生命周期	与其他 Unified Manager 事件相同：新建、已确认、已解决和已废弃状态	在事件创建 15 分钟后，集群刷新后，EMS 事件将被废弃
在 Unified Manager 停机期间捕获事件	是，当系统启动时，它与每个集群通信以获取缺失的事件	否
事件详情	建议的纠正措施直接从 ONTAP 导入，以提供一致的解决方案	事件详细信息页面中无可用的纠正措施

一些新的自动 EMS 事件是指示先前事件已解决的信息事件。例如，“FlexGroup Constituents Space Status All OK”信息事件指示“FlexGroup Constituents Have Space Issues”错误事件已解决。信息事件不能使用与其他事件严重性类型相同的事件生命周期来管理，但是，如果同一卷收到另一个“`Space Issues`”错误事件，则该事件将自动废弃。

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

以下 ONTAP EMS 事件将自动添加到 Unified Manager。这些事件将在 Unified Manager 正在监视的任何群集上触发时生成。

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

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
用于聚合重新定位的云层访问被拒绝	arl.netra.ca.check.failed	聚合	错误
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	错误
FabricPool 镜像复制重新同步已完成	wafl.ca.resync.complete	集群	错误
FabricPool 空间接近全满	fabricpool.nearly.full	集群	错误
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 宽限期已结束	nvmf.graceperiod.expired	集群	警告
LUN 已销毁	lun.destroy	LUN	信息
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	节点	错误
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	节点	错误

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	节点	错误
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	节点	错误
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	节点	信息
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	节点	错误
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	节点	错误
无法解析云层主机	objstore.host.unresolvable	节点	错误
云层集群间网络接口已关闭	objstore.interclusterlifDown	节点	错误
请求与云层签名不匹配	osc.signatureMismatch	节点	错误
一个 NFSv4 池已用尽	Nblade.nfsV4PoolExhaust	节点	关键
QoS 监控内存已达到上限	qos.monitor.memory.maxed	节点	错误
QoS 监控内存已缩减	qos.monitor.memory.abated	节点	信息
NVMeNS 已销毁	NVMeNS.destroy	命名空间	信息
NVMeNS 联机	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.of.space	命名空间	警告
同步复制未同步	sms.status.out.of.sync	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	错误
多个 CIFS 连接	Nblade.cifsManyAuths	SVM	错误
超出 CIFS 连接数上限	Nblade.cifsMaxOpenSameFile	SVM	错误
超出每用户 CIFS 连接数上限	Nblade.cifsMaxSessPerUsrConn	SVM	错误
CIFS NetBIOS 名称冲突	Nblade.cifsNbNameConflict	SVM	错误
尝试连接不存在的 CIFS 共享	Nblade.cifsNoPrivShare	SVM	关键
CIFS 卷影复制操作失败	cifs.shadowcopy.failure	SVM	错误
AV 服务器发现病毒	Nblade.vscanVirusDetected	SVM	错误

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
没有可用于病毒扫描的 AV 服务器连接	Nblade.vscanNoScannerConn	SVM	关键
未注册 AV 服务器	Nblade.vscanNoRegdScanner	SVM	错误
AV 服务器连接无响应	Nblade.vscanConnInactive	SVM	信息
AV 服务器太忙，无法接受新的扫描请求	Nblade.vscanConnBackPressure	SVM	错误
用户未经授权尝试访问 AV 服务器	Nblade.vscanBadUserPrivAccess	SVM	错误
FlexGroup 成分卷存在空间问题	flexgroup.constituents.have.space.issues	卷	错误
FlexGroup 成分卷空间状态一切正常	flexgroup.constituents.space.status.all.ok	卷	信息
FlexGroup 成分卷存在索引节点问题	flexgroup.constituents.have.inodes.issues	卷	错误
FlexGroup 成分卷索引节点状态一切正常	flexgroup.constituents.inodes.status.all.ok	卷	信息
卷逻辑空间接近全满	monitor.vol.nearFull.inc.sav	卷	警告
卷逻辑空间全满	monitor.vol.full.inc.sav	卷	错误
卷逻辑空间正常	monitor.vol.one.ok.inc.sav	卷	信息
WAFL 卷 AutoSize 失败	wafl.vol.autoSize.fail	卷	错误
WAFL 卷自动调整大小已完成	wafl.vol.autoSize.done	卷	信息
WAFL READDIR 文件操作超时	wafl.readdir.expired	卷	错误

在 **Active IQ Unified Manager** 中订阅 **ONTAP EMS** 事件

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。EMS 事件的一个子集会自动报告给 Unified Manager，但只有在您订阅了这些事件时，才会报告其他 EMS 事件。

开始之前

不要订阅已自动添加到 Unified Manager 的 EMS 事件，因为在接收同一问题的两个事件时，这可能会导致混淆。

您可以订阅任意数量的 EMS 事件。系统将验证您订阅的所有事件，并且仅将已验证的事件应用于您在 Unified Manager 中监控的集群。*ONTAP 9 EMS* 事件目录 提供指定版本的 ONTAP 9 软件的所有 EMS 消息的详细信息。从 ONTAP 9 产品文档页面中找到相应版本的 *EMS* 事件目录，以获取适用事件的列表。

"ONTAP 9 产品库"

您既可以为订阅的 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。

如果未收到已订阅的 ONTAP EMS 事件，则集群的 DNS 配置可能存在问题，导致集群无法访问 Unified Manager 服务器。要解决此问题，集群管理员必须更正集群的 DNS 配置，然后重新启动 Unified Manager。这样做会将挂起的 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. 在事件设置页面中，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。

   要从 ONTAP 集群 shell 查看您可以订阅的 EMS 事件的名称，您可以使用 `event route show` 命令（在 ONTAP 9 之前）或 `event catalog show` 命令（ONTAP 9 或更高版本）。

   "如何在 Active IQ Unified Manager 中配置并接收来自 ONTAP EMS 事件订阅的警报"

4. 单击 **Add**。

   EMS 事件已添加至已订阅 EMS 事件列表，但“适用于群集”列显示您添加的 EMS 事件的状态为“Unknown”。

5. 单击*保存并关闭*以在集群中注册 EMS 事件订阅。
6. 再次点击 订阅 **EMS** 事件。

   状态 “是” 出现在您添加的 EMS 事件的“适用于集群”列中。

   如果状态不是 “Yes”，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，然后再次添加该事件。

当 ONTAP EMS 事件发生时，该事件将显示在“事件”页面上。您可以在“事件详细信息”页面中选择该事件，以查看有关 EMS 事件的详细信息。您还可以管理事件的处置或为该事件创建警报。

了解 **Active IQ Unified Manager** 如何处理收到的事件

当 Unified Manager 收到事件时，它将显示在“仪表板”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”选项卡以及特定对象的清单页面（例如，“卷/运行状况”清单页面）中。

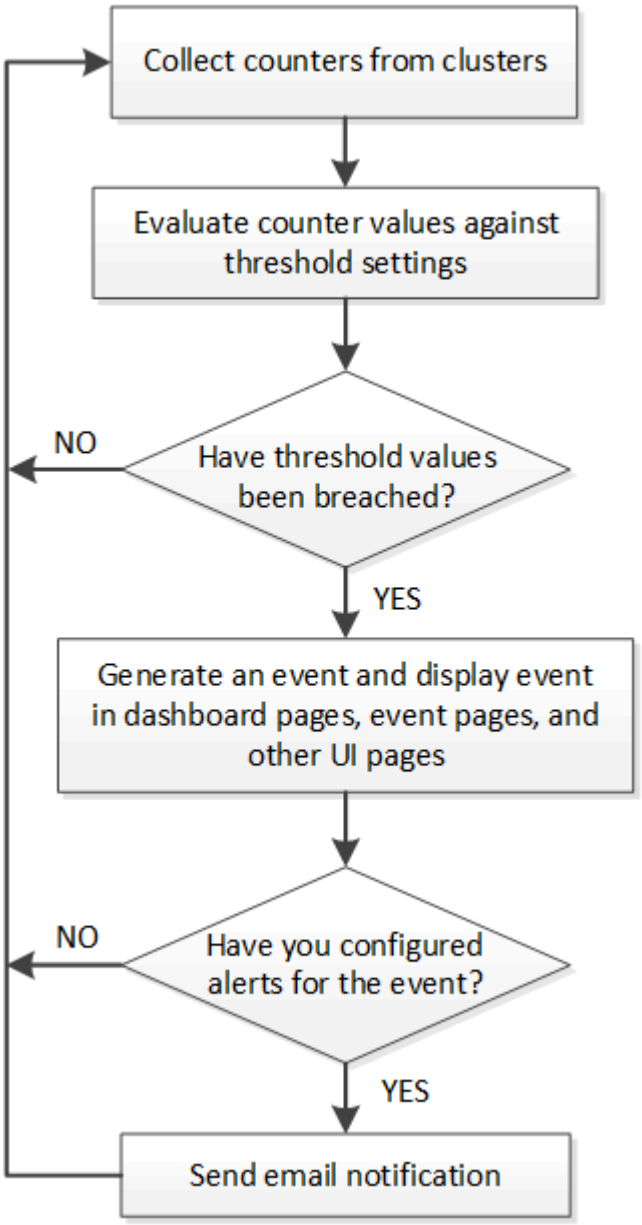
当 Unified Manager 检测到同一集群组件连续多次出现相同的事件条件时，它会将所有这些情况视为单个事件，而不是单独的事件。事件的持续时间会递增，以指示该事件仍处于活动状态。

根据您在“警报设置”页面中配置设置的方式，您可以将这些事件通知其他用户。警报会导致启动以下操作：

- 可以向所有 Unified Manager 管理员用户发送有关该事件的电子邮件。
- 该事件可以发送给其他电子邮件收件人。
- SNMP 陷阱可以发送到陷阱接收器。

- 可以执行自定义脚本来执行操作。

此工作流程如下图所示。



在 **Active IQ Unified Manager** 中查看事件详细信息

您可以查看由 Unified Manager 触发以采取纠正措施的事件的详细信息。例如，如果存在运行状况事件 Volume Offline，则可以单击该事件以查看详细信息并执行纠正措施。

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的来源、事件的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”视图将显示过去 7 天内生成的具有事件或风险影响级别的新事件和已确认（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 **View** ，然后从事件类型菜单中进行选择。
3. 单击要查看其详细信息的事件名称。

   事件详细信息显示在事件详细信息页面中。

在 **Active IQ Unified Manager** 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它们的用户。

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. 在*过滤器*窗格中，在*分配给*区域中选择*未分配*过滤器选项。

确认并解决 **Active IQ Unified Manager** 中的事件

在开始处理触发事件的问题之前，您应先确认该事件，以避免持续收到重复的警报通知。针对特定事件采取纠正措施后，您应将该事件标记为已解决。

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这些事件：

目的	操作
确认单个事件并将其标记为已解决	a. 单击事件名称。 b. 从事件详细信息页面确定事件的原因。 c. 单击*确认*。 d. 采取适当的纠正措施。 e. 单击*标记为已解决*。

目的	操作
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原因。 b. 选择事件。 c. 单击*确认*。 d. 采取适当的纠正措施。 e. 单击*标记为已解决*。

在事件被标记为已解决后，该事件将被移动到已解决的事件列表中。

3. 可选：在*备注和更新*区域中，添加有关您如何处理事件的备注，然后单击*发布*。

在 **Active IQ Unified Manager** 中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，您可以将已分配的事件重新分配给其他用户。例如，当存储对象上频繁出现问题时，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

- 必须正确配置用户名和电子邮件 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*库存页面中，选择要分配的一个或多个事件。
3. 通过选择以下选项之一来分配事件：

如果要将此事件分配给.....	操作
您自己	单击 分配给 > 我。
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*。 电子邮件通知将发送给用户。 如果不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。

在 **Active IQ Unified Manager** 中禁用不需要的事件

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。您可以在要恢复接收通知时启用已禁用的事件。

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，系统中以前生成的事件将被标记为已废弃，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，将从下一监控周期开始生成这些事件的通知。

如果禁用某个对象的事件（例如， `vol offline` 事件），然后再启用该事件，则 Unified Manager 不会为在事件处于禁用状态时离线的对象生成新事件。Unified Manager 仅在重新启用事件后对象状态发生变化时才会生成新事件。

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来禁用或启用事件：

目的	操作
禁用事件	a. 单击 **Disable**。 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“事件设置”页面的列表视图中。
启用事件	a. 选中要启用的一个或多个事件的复选框。 b. 单击 启用。

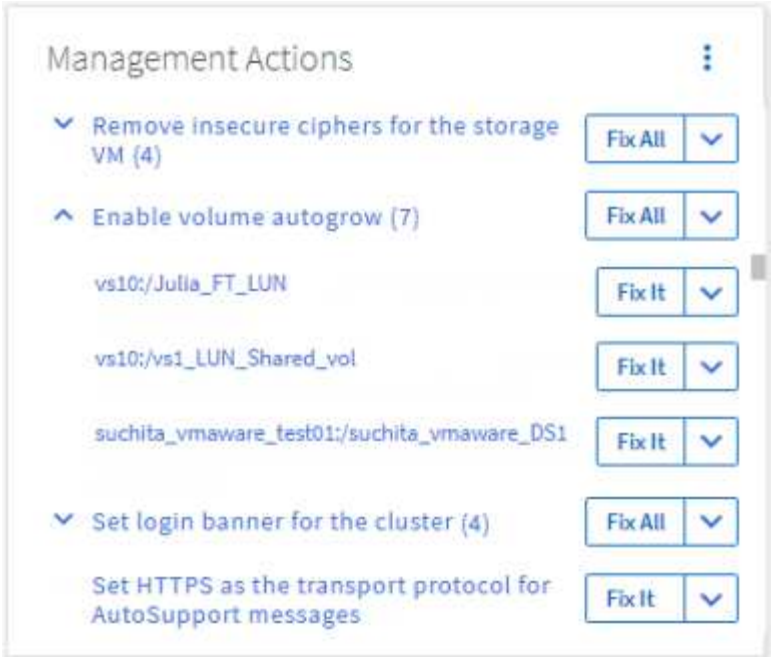
使用 **Active IQ Unified Manager** 中的自动修复功能修复问题

Unified Manager 可以使用 **Fix It** 按钮彻底诊断某些事件并提供单一解决方案。如果可用，这些解决方案将显示在仪表板、事件详细信息页面和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 CLI 实施最佳解决方案。当 Unified Manager 确定存在解决此问题的单一解决方案，并且可以使用 ONTAP CLI 命令解决此问题时，可以使用 **Fix It** 操作。

步骤

1. 要查看可通过*仪表板*修复的事件，请点击*仪表板*。



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

有关可通过自动修正修复的问题的信息，请参见 "Unified Manager 可以解决哪些问题"。

在 **Active IQ Unified Manager** 中启用和禁用 **Active IQ** 事件报告

默认情况下，Active IQ 平台事件将生成并显示在 Unified Manager 用户界面中。如果您发现这些事件过于“嘈杂”，或者您不希望在 Unified Manager 中查看这些事件，则可以禁止生成这些事件。如果您想恢复接收这些通知，可以稍后再启用它们。

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 会根据集群的时区在午夜后不久开始接收 Active IQ 平台事件。开始时间基于 Unified Manager 从每个集群接收 AutoSupport 消息的时间。

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：

目的	操作
禁用 Active IQ 平台事件	在 **Active IQ** 门户事件 面板中，向左移动滑块按钮。
启用 Active IQ 平台事件	在*Active IQ 门户事件*面板中，向右移动滑块按钮。

在 **Active IQ Unified Manager** 中上传新的 **Active IQ** 规则文件

Unified Manager 会自动检查新的 Active IQ 事件（规则）文件，并在有更新规则时下载新文件。但是，在没有外部网络访问权限的站点中，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。

当您在没有网络连接的站点中将 Unified Manager 安装或升级到特定版本时，捆绑的 Active IQ 规则将自动可用于上传。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，以确保生成更新的事件，并且您的存储系统继续保持最佳性能。

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. 在具有网络访问权限的计算机上，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，默认情况下，NetApp 知识库文章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* 文件并上传，以查看所有规则的知识库文章。

2. 将规则文件传输到您可以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上。
3. 在左侧导航窗格中，单击*存储管理* > 事件设置。
4. 在 **Event Setup** 页面中，单击 **Upload Rules** 按钮。
5. 在*上传规则*对话框中，导航到并选择您下载的规则 `.zip`文件，然后单击*上传*。

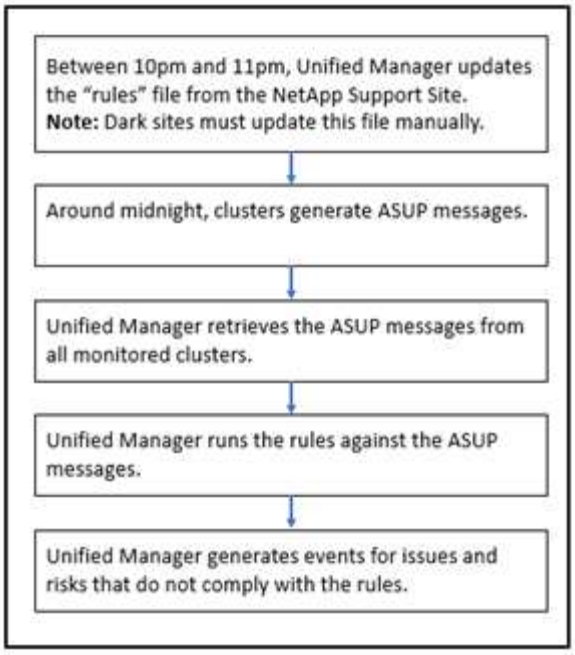
   此过程可能需要几分钟时间。

规则文件将在 Unified Manager 服务器上解压缩。在您的托管集群于午夜后生成 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突发事件。

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"。

Active IQ Unified Manager 如何生成 **Active IQ** 平台事件

Active IQ 平台事件和风险将转换为 Unified Manager 事件，如下图所示。

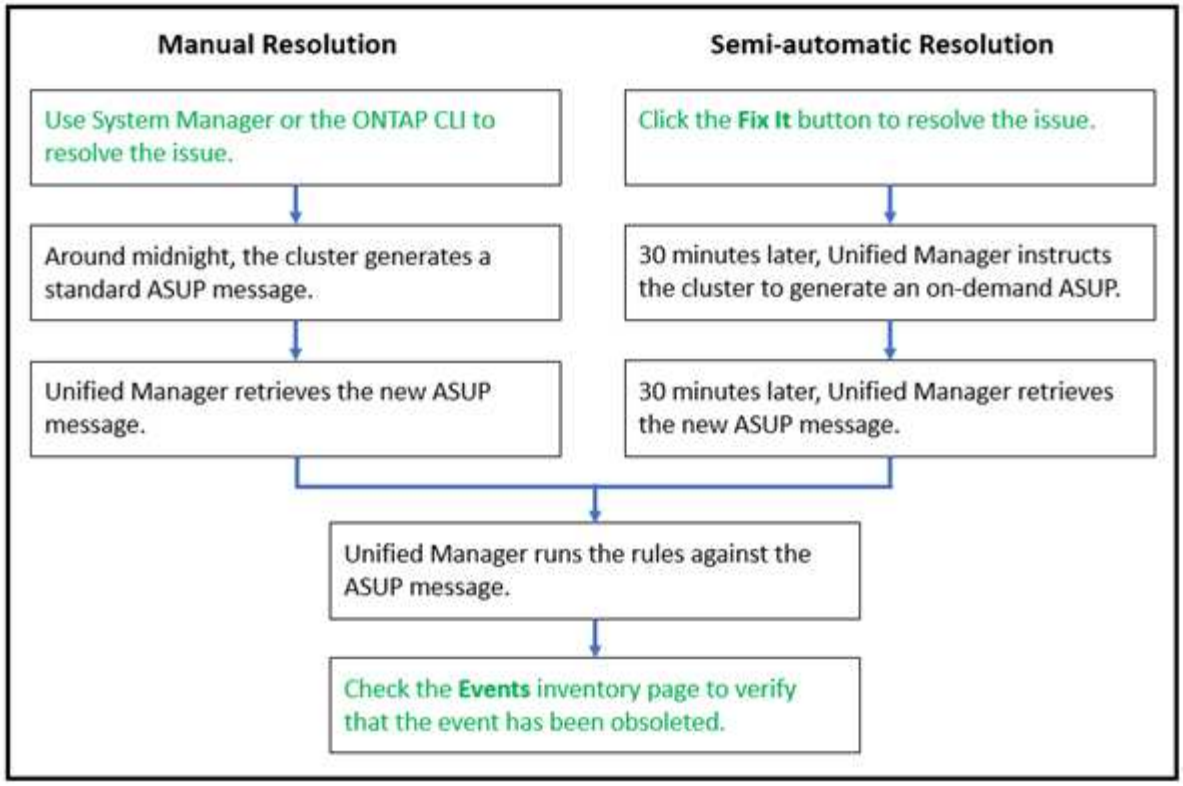


如您所见，Active IQ 平台上编译的规则文件保持最新，每天生成群集 AutoSupport 消息，Unified Manager 每天更新事件列表。

在 **Active IQ Unified Manager** 中解决 **Active IQ** 平台事件

Active IQ 平台事件和风险与其他 Unified Manager 事件类似，因为它们可以分配给其他用户进行解决，并且它们具有相同的可用状态。但是，当您使用 **Fix It** 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案。

下图显示了在解决从 Active IQ 平台生成的事件时，您必须采取的操作（绿色）以及 Unified Manager 采取的操作（黑色）。



执行手动解决时，您必须登录到 System Manager 或 ONTAP 命令行界面来修复此问题。只有在集群于午夜生成新的 AutoSupport 消息后，您才能验证此问题。

使用 **Fix It** 按钮执行半自动修复时，您可以在数小时内验证修复是否成功。

在 **Active IQ Unified Manager** 中配置事件保留设置

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。

将事件保留超过 6 个月可能会影响服务器性能，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，并将其移动到应保留事件的月数，然后单击*保存*。

什么是 **Unified Manager** 维护窗口

了解 **Active IQ Unified Manager** 维护窗口

您可以定义 Unified Manager 维护窗口，以便在已安排群集维护且不希望收到大量不需要的通知时，在特定时间范围内抑制事件和警报。

维护窗口启动时，“Object Maintenance Window Started”事件将发布到 Event Management 清单页面。此事件在维护窗口结束时会自动失效。

在维护窗口期间，仍会生成与该集群上所有对象相关的事件，但它们不会出现在任何 UI 页面中，并且不会为这些事件发送警报或其他类型的通知。但是，您可以通过选择“事件管理”清单页面上的“查看”选项之一，来查看在维护窗口期间为所有存储对象生成的事件。

您可以安排将来启动的维护窗口，可以更改计划维护窗口的开始和结束时间，也可以取消计划维护窗口。

安排维护时段以禁用 **Active IQ Unified Manager** 中的集群事件通知

如果您有计划的群集停机时间，例如升级群集或移动其中一个节点，则可以通过安排 Unified Manager 维护窗口来抑制通常在该时间范围内生成的事件和警报。

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，但它们不会显示在事件页面中，并且不会为这些事件发送警报或其他类型的通知。

您为维护时段输入的时间基于 Unified Manager 服务器的时间。

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向右移动。

   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*。

   “Scheduled” 消息出现在滑块按钮旁边。

到达开始时间时，集群进入维护模式，并生成“对象维护窗口已启动”事件。

更改或取消 **Active IQ Unified Manager** 中已计划的维护窗口

如果已将 Unified Manager 维护窗口配置为在将来发生，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，并且希望再次开始接收来自集群的事件和警报，则取消当前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：

目的	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“Scheduled”。 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持续时间	a. 单击滑块按钮旁边的文本“活动”。 b. 更改结束日期和时间，然后单击*应用*。
取消计划的维护时间段	选择滑块按钮并将其向左移动。
取消活动的维护时段	选择滑块按钮并将其向左移动。

查看在 **Active IQ Unified Manager** 维护窗口期间生成的事件

如果需要，您可以查看在 Unified Manager 维护窗口期间为所有存储对象生成的事件。一旦维护窗口结束且所有系统资源恢复运行，大多数事件将显示为“已过时”状态。

开始之前

在任何事件可用之前，必须至少完成一个维护窗口。

默认情况下，在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（新建和已确认）事件都将显示在事件管理清单页面上。

2. 从“查看”窗格中，选择选项*维护期间生成的所有事件*。

   显示过去 7 天内从所有维护时段会话和所有群集触发的事件列表。

3. 如果单个集群有多个维护窗口，则可以单击*触发时间*日历图标，并选择您有兴趣查看的维护窗口事件的时间段。

在 **Active IQ Unified Manager** 中管理主机系统资源事件

Unified Manager 包括一项服务，用于监控安装了 Unified Manager 的主机系统上的资源问题。主机系统上缺少可用磁盘空间或内存不足等问题可能会触发管理站事件，这些事件在 UI 的顶端显示为横幅消息。

管理站事件指示安装 Unified Manager 的主机系统出现问题。管理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而导致统计分析未完成或延迟完成。

与所有其他 Unified Manager 事件消息不同，这些特定的管理站警告和关键事件显示在横幅消息中。

步骤

1. 要查看管理站事件信息，请执行以下操作：

目的	操作
查看事件详情	单击此事件横幅可显示“事件详细信息”页面，其中包含此问题的建议解决方案。
查看所有管理站事件	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“过滤器”窗格中，单击“源类型”列表中“管理工作站”的框。

详细了解事件

Active IQ Unified Manager 中的事件状态

事件的状态可帮助您确定是否需要采取适当的纠正措施。事件可以是“新建”、“已确认”、“已解决”或“已过时”。请注意，“新建”和“已确认”事件均被视为活动事件。

事件状态如下：

- 新增

  新事件的状态。

- 已确认

  已确认事件时的状态。

- 已解决

  事件被标记为已解决时的状态。

- 已废弃

  事件自动更正或事件原因不再有效时的状态。

  您无法确认或解决废弃的事件。

事件不同状态的示例

以下示例说明了手动和自动事件状态更改。

当触发 Cluster Not Reachable 事件时，事件状态为 New。当您确认该事件时，事件状态将变为 Acknowledged。在采取适当的纠正措施后，您必须将该事件标记为已解决。然后，事件状态将变为 Resolved。

如果由于停电而生成了 Cluster Not Reachable 事件，则在恢复供电后，群集将在没有任何管理员干预的情况下开始运行。因此，Cluster Not Reachable 事件不再有效，并且事件状态将在下一监控周期更改为 Obsolete。

当事件处于“已过时”或“已解决”状态时，Unified Manager 会发送警报。警报的电子邮件主题行和电子邮件内容提供了有关事件状态的信息。SNMP 陷阱还包含有关事件状态的信息。

了解 **Active IQ Unified Manager** 中的事件严重性类型

每个事件都与严重程度类型相关联，以帮助您对需要立即采取纠正措施的事件进行优先级排序。

- 严重

  发生了一个问题，如果不立即采取纠正措施，可能会导致服务中断。

  性能关键事件仅从用户定义的阈值发送。

- 错误

  事件源仍在运行；但是，需要采取纠正措施以避免服务中断。

- 警告

  事件源发生了您应注意的事件，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未达到严重级别。此严重程度的事件不会导致服务中断，可能不需要立即采取纠正措施。

  性能警告事件从用户定义、系统定义或动态阈值发送。

- 信息

  当发现新对象或执行用户操作时，会发生此事件。例如，当删除任何存储对象或发生任何配置更改时，将生成严重性类型为“信息”的事件。

  当检测到配置更改时，信息事件将直接从 ONTAP 发送。

了解 **Active IQ Unified Manager** 中的事件影响级别

每个事件都与影响级别（突发事件、风险、事件或升级）相关联，以帮助您优先处理需要立即采取纠正措施的事件。

- 事件

  事件是一组可能导致集群停止向客户端提供数据并耗尽数据存储空间的事件。影响级别为"事件"的事件最为严重。应立即采取纠正措施，以避免服务中断。

- 风险

  风险是一组事件，这些事件可能会导致集群停止向客户端提供数据，并耗尽用于存储数据的空间。影响级别为“风险”的事件可能会导致服务中断。可能需要采取纠正措施。

- 事件

  事件是存储对象及其属性的状态或状态更改。影响级别为“事件”的事件仅供参考，无需采取纠正措施。

- 升级

  升级事件是 Active IQ 平台报告的特定类型的事件。这些事件指出的问题，其解决方案需要您升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）。您可能需要立即对其中一些问题采取纠正措施，而其他

问题则可以等到下一次计划内维护时再处理。

了解 **Active IQ Unified Manager** 中的事件影响区域

事件分为六个影响领域（可用性、容量、配置、性能、保护和安全性），使您能够专注于自己负责的事件类型。

- 可用性

  如果存储对象脱机、协议服务关闭、发生存储故障转移问题或发生硬件问题，可用性事件会通知您。

- 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，或者您的环境的增长率是否异常。

- 配置

  配置事件会通知您存储对象的发现、删除、添加、移除或重命名。配置事件的影响级别为事件，严重性类型为信息。

- 性能

  性能事件会通知您群集上的资源、配置或活动条件，这些条件可能会对受监视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

  保护事件会通知您涉及 SnapMirror 关系的事件或风险、目标容量问题、SnapVault 关系问题或保护作业问题。托管辅助卷和保护关系的任何 ONTAP 对象（特别是聚合、卷和 SVM）都归类在保护影响区域中。

- 安全

  安全事件根据 "适用于 ONTAP 9 的 NetApp 安全强化指南"中定义的参数，通知您 ONTAP 集群、存储虚拟机（SVM）和卷的安全程度。

  此外，此区域还包括 Active IQ 平台报告的升级事件。

Active IQ Unified Manager 如何计算对象状态

对象状态由当前处于“新建”或“已确认”状态的最严重事件确定。例如，如果对象状态为 Error，则对象的某个事件的严重性类型为 Error。采取纠正措施后，事件状态将变为“已解决”。

了解 **Active IQ Unified Manager** 中的动态性能事件

对于动态性能事件，“事件详细信息”页面的“系统诊断”部分列出了存在争用的集群组件延迟或使用率最高的顶级工作负载。

性能统计数据基于检测到性能事件的时间，直至上次分析事件的时间。图表还显示处于争用状态的集群组件的历史性能统计信息。

例如，您可以识别组件利用率高的工作负载，以确定将哪些工作负载转移到利用率较低的组件。移动工作负载将减少当前组件的工作量，可能使组件脱离争用状态。本节顶部是检测到事件并进行上次分析的时间和日期范围。对于活动事件（新事件或已确认事件），上次分析的时间将被更新。

将光标悬停在图表上时，延迟和活动图表会显示顶级工作负载的名称。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 *sharks* 、 *bullies* 或 *victims* ）对工作负载进行排序，并显示有关其延迟及其在争用集群组件中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的延迟或使用范围。有关信息，请参阅 "由 Unified Manager 监控的工作负载类型"。

当您按延迟的峰值偏差排序时，系统定义的工作负载不会显示在表中，因为延迟仅适用于用户定义的工作负载。具有极低延迟值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 "分析动态性能阈值生成的事件"。

有关 Unified Manager 如何对工作负载进行排序和确定排序顺序的信息，请参见 "Unified Manager 如何确定事件对性能的影响"。

图表中的数据显示了上次分析事件之前的 24 小时性能统计数据。每个工作负载的实际值和预期值基于工作负载参与事件的时间。例如，工作负载可能会在检测到事件后参与事件，因此其性能统计信息可能与事件检测时的值不匹配。默认情况下，工作负载按延迟的峰值（最高）偏差进行排序。

由于 Unified Manager 最多保留 30 天的 5 分钟历史性能和事件数据，因此如果此事件是 30 多天前的，则不会显示任何性能数据。

- **Workload Sort** 列
  - 延迟图表

    显示上次分析过程中事件对工作负载延迟的影响。

  - **Component Usage** 列

    显示有关发生争用的集群组件的工作负载使用情况的详细信息。在图表中，实际使用情况显示为一条蓝线。红色条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外的活动，因此不会显示此列。

  - 组件使用

    以百分比显示网络处理、数据处理和聚合组件的利用率历史记录，或以百分比显示 QoS 策略组组件的活动历史记录。不显示网络或互连组件的图表。您可以指向统计数据以查看特定时间点的使用统计数据。

  - 总写入 **MB/s** 历史记录

    仅对于 MetroCluster Resources 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，以兆字节每秒（MBps）为单位。

  - 事件历史记录

    显示红色阴影线条以指示争用组件的历史事件。对于过时的事件，图表显示在检测到所选事件之前和解决该事件之后发生的事件。

Active IQ Unified Manager 检测到的配置更改

Unified Manager 监控您的集群的配置更改，以帮助您确定更改是否可能导致或促成性能事件。性能资源管理器页面显示更改事件图标（●），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所选集群对象的性能。如果在性能事件发生的同时或前后检测到更改，则该更改可能是导致问题的原因，从而触发了事件警报。

Unified Manager 可以检测到以下变更事件，这些事件被归类为信息事件：

- 卷在聚合之间移动。

  Unified Manager 可以检测移动是正在进行、已完成还是已失败。如果 Unified Manager 在卷移动期间停止运行，则在恢复运行时，它会检测到卷移动并为其显示一个更改事件。

- 包含一个或多个受监控工作负载的 QoS 策略组的吞吐量（MB/s 或 IOPS）限制发生更改。

  更改策略组限制可能会导致延迟（响应时间）出现间歇性峰值，这也可能触发策略组的事件。延迟会逐渐恢复正常，由峰值引起的任何事件都会过时。

- HA 对中的节点接管或交还其伙伴节点的存储。

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

- 已成功完成 ONTAP 升级或还原操作。

  将显示先前版本和新版本。

事件和严重性类型列表

了解 **Active IQ Unified Manager** 中的聚合事件

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

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合离线（ocumEvtAggregateStateOffline）	意外事件	聚合	关键
聚合失败（ocumEvtAggregateStateFailed）	意外事件	聚合	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
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
云层无法访问（ocumEventCloudTierUnreachable）	风险	聚合	错误
用于聚合重新定位的云层访问被拒绝*（arlNetraCaCheckFailed）	风险	聚合	错误
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	错误
MetroCluster 聚合遗留（ocumEvtMetroClusterAggregateLeftBehind）	风险	聚合	错误
MetroCluster 聚合镜像已降级（ocumEvtMetroClusterAggregateMirrorDegraded）	风险	聚合	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合空间接近全满（ocumEvtAggregateNearlyFull）	风险	聚合	警告
聚合空间全满（ocumEvtAggregateFull）	风险	聚合	错误
聚合达到全满前的天数（ocumEvtAggregateDaysUntilFullSoon）	风险	聚合	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合过度配置（ocumEvtAggregateOvercommitted）	风险	聚合	错误
聚合接近过量提交（ocumEvtAggregateAlmostOvercommitted）	风险	聚合	警告
聚合 Snapshot 预留满（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	严重性
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
聚合已删除（不适用）	事件	节点	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反聚合 IOPS 严重阈值（ocumAggregateIopsIncident）	意外事件	聚合	关键
已违反聚合 IOPS 警告阈值（ocumAggregateIopsWarning）	风险	聚合	警告
已违反聚合 MB/s 严重阈值（ocumAggregateMbpsIncident）	意外事件	聚合	关键
已违反聚合 MB/s 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	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反聚合延迟警告阈值（ocumAggregateLatencyWarning）	风险	聚合	警告
已违反已用聚合性能容量严重阈值（ocumAggregatePerfCapacityUsedIncident）	意外事件	聚合	关键
已违反聚合已用性能容量警告阈值（ocumAggregatePerfCapacityUsedWarning）	风险	聚合	警告
已违反聚合利用率严重阈值（ocumAggregateUtilizationIncident）	意外事件	聚合	关键
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

了解 **Active IQ Unified Manager** 中的集群事件

集群事件提供了有关集群状态的信息，可用于监控集群中的潜在问题。事件按影响区域进行分组，且包括事件名称、陷阱名称、影响级别、源类型和严重性。

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
集群缺少备用磁盘（ocumEvtDisksNoSpares）	风险	集群	警告
集群无法访问（ocumEvtClusterUnreachable）	风险	集群	错误
集群监控失败（ocumEvtClusterMonitoringFailed）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反集群 FabricPool 许可证容量限制（ocumEvtExternalCapacityTierSpaceFull）	风险	集群	警告
NVMe-oF 宽限期已开始 *（nvmfGracePeriodStart）	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（objectMaintenanceWindowStarted）	事件	集群	关键
对象维护窗口已结束（objectMaintenanceWindowEnded）	事件	集群	信息
MetroCluster 备用磁盘遗留（ocumEvtSpareDiskLeftBehind）	风险	集群	错误
MetroCluster 自动计划外切换已禁用（ocumEvtMccAutomaticUnplannedSwitchOverDisabled）	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	严重性
已超过集群容量不平衡阈值（ocumConformanceNodeImbalanceWarning）	风险	集群	警告
集群云层规划（clusterCloudTierPlanningWarning）	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

事件名称（陷阱名称）	影响级别	源类型	严重性
FabricPool 空间接近全满 *（fabricpoolNearlyFull）	风险	集群	错误

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已添加节点（不适用）	事件	集群	信息
节点已删除（不适用）	事件	集群	信息
群集已删除（不适用）	事件	集群	信息
集群添加失败（不适用）	事件	集群	错误
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	关键
收到严重 EMS（不适用）	事件	集群	关键
收到 EMS 警报（不适用）	事件	集群	错误
收到 EMS 错误（不适用）	事件	集群	警告
收到 EMS 警告（不适用）	事件	集群	警告
收到调试 EMS（不适用）	事件	集群	警告
收到 EMS 通知（不适用）	事件	集群	警告
收到信息性 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
关键	紧急 关键
错误	警报
警告	错误 警告 调试 通知 信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已超出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	关键
已违反集群 IOPS 警告阈值（ocumClusterIopsWarning）	风险	集群	警告
已违反集群 MB/s 严重阈值（ocumClusterMbpsIncident）	意外事件	集群	关键
已违反集群 MB/s 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	严重性
AutoSupport HTTPS传输已禁用（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
已禁用 FIPS 模式（ocumClusterFipsDisabled）	风险	集群	警告
已禁用登录横幅（ocumClusterLoginBannerDisabled）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
登录横幅已更改（ocumClusterLoginBannerChanged）	风险	集群	警告
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正在使用不安全密码（ocumClusterSSHInsecure）	风险	集群	警告
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（ocumClusterMD5PasswordHashUsed）	风险	集群	警告
群集使用自签名证书（ocumClusterSelfSignedCertificate）	风险	集群	警告
集群远程 Shell 已启用（ocumClusterRshDisabled）	风险	集群	警告
群集证书即将过期（ocumEvtClusterCertificateAboutToExpire）	风险	集群	警告
群集证书已过期（ocumEvtClusterCertificateExpired）	风险	集群	错误

了解 **Active IQ Unified Manager** 中的磁盘事件

磁盘事件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，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
闪存磁盘 - 几乎用尽备用数据块（ocumEvtClusterFlashDiskFewerSpareBlockError）	风险	集群	错误
闪存磁盘 - 无备用数据块（ocumEvtClusterFlashDiskNoSpareBlockCritical）	意外事件	集群	关键
一些未分配的磁盘（ocumEvtClusterUnassignedDisksSome）	风险	集群	警告
部分故障磁盘（ocumEvtDisksSomeFailed）	意外事件	集群	关键

了解 **Active IQ Unified Manager** 中的机柜事件

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，以便您监控潜在问题。事件按影响区域分组，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	严重性
磁盘架风扇出现故障（ocumEvtShelfFanFailed）	意外事件	存储架	关键
磁盘架电源出现故障（ocumEvtShelfPowerSupplyFailed）	意外事件	存储架	关键
未配置磁盘架多路径（ocumDiskShelfConnectivityNotInMultiPath） 此事件不适用于： • 处于 MetroCluster 配置中的集群 • 以下平台：FAS2554、FAS2552、FAS2520 和 FAS2240	风险	节点	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	严重性
已发现磁盘架（不适用）	事件	节点	信息
已移除磁盘架（不适用）	事件	节点	信息

了解 **Active IQ Unified Manager** 中的风扇事件

风扇事件为您提供有关数据中心内节点上风扇状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
一个或多个风扇出现故障（ocumEvtFansOneOrMoreFailed）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的闪存卡事件

闪存卡事件为您提供有关安装在数据中心节点上的闪存卡状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
闪存卡离线（ocumEvtFlashCardOffline）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的 **inode** 事件

当 inode 已满或接近已满时，inode 事件会提供相关信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型以及严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
索引节点接近全满（ocumEvtInodesAlmostFull）	风险	卷	警告
Inodes Full（ocumEvtInodesFull）	风险	卷	错误

Active IQ Unified Manager 中的网络接口事件

网络接口事件提供有关网络接口（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，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
网络接口状态已关闭（ocumEvtLifStatusDown）	风险	接口	错误
FC/FCoE 网络接口状态已关闭（ocumEvtFCLifStatusDown）	风险	接口	错误
无法进行网络接口故障转移（ocumEvtLifFailoverNotPossible）	风险	接口	警告
网络接口不位于主端口（ocumEvtLifNotAtHomePort）	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	严重性
网络接口路由未配置（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	严重性
已违反网络接口 MB/s 严重阈值（ocumNetworkLifMbpsIncident）	意外事件	接口	关键
已违反网络接口 MB/s 警告阈值（ocumNetworkLifMbpsWarning）	风险	接口	警告
已违反 FC 网络接口 MB/s 严重阈值（ocumFcpLifMbpsIncident）	意外事件	接口	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 FC 网络接口 MB/s 警告阈值（ocumFcpLifMbpsWarning）	风险	接口	警告
已违反 NVMf FC 网络接口 MB/s 严重阈值（ocumNvmfFcLifMbpsIncident）	意外事件	接口	关键
已违反 NVMf FC 网络接口 MB/s 警告阈值（ocumNvmfFcLifMbpsWarning）	风险	接口	警告

了解 **Active IQ Unified Manager** 中的 **LUN** 事件

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

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN 离线（ocumEvtLunOffline）	意外事件	LUN	关键
LUN 已销毁 *（lunDestroy）	事件	LUN	信息
igroup 中映射了不受支持的操作系统的 LUN（igroupUnsupportedOsType）	意外事件	LUN	警告
访问 LUN 的单一活动路径（ocumEvtLunSingleActivePath）	风险	LUN	警告
没有可访问 LUN 的活动路径（ocumEvtLunNotReachable）	意外事件	LUN	关键
没有可访问 LUN 的优化路径（ocumEvtLunOptimizedPathInactive）	风险	LUN	警告
没有可从 HA 配对节点（ocumEvtLunHaPathInactive）访问 LUN 的路径	风险	LUN	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
无路径可从 HA 对中的一个节点访问 LUN（ocumEvtLunNodePathStatusDown）	风险	LUN	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN Snapshot 副本的空间不足（ocumEvtLunSnapshotNotPossible）	风险	卷	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
igroup 中映射了不受支持的操作系统的 LUN（igroupUnsupportedOsType）	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	严重性
已违反 LUN IOPS 严重阈值（ocumLunIopsIncident）	意外事件	LUN	关键
已违反 LUN IOPS 警告阈值（ocumLunIopsWarning）	风险	LUN	警告
已违反 LUN MB/s 严重阈值（ocumLunMbpsIncident）	意外事件	LUN	关键
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）关键阈值（ocumLunLatencyIncident）	意外事件	LUN	关键
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	严重性
已违反 LUN 延迟和 IOPS 严重阈值（ocumLunLatencyIopsIncident）	意外事件	LUN	关键
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/s 严重阈值（ocumLunLatencyMbpsIncident）	意外事件	LUN	关键
已违反 LUN 延迟和 MB/s 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	关键
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	关键
LUN 延迟和聚合利用率警告阈值已违反（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	关键
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

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN 延迟和已用节点性能容量 - 已违反接管严重阈值（ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident）	意外事件	LUN	关键
LUN 延迟和已用节点性能容量 - 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	关键
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/s 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

了解 **Active IQ Unified Manager** 中的管理站事件

管理站事件可为您提供有关安装了 Unified Manager 的服务器状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
管理服务器磁盘空间接近全满（ocumEvtUnifiedManagerDiskSpaceNearlyFull）	风险	管理站	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
管理服务器磁盘空间已满（ocumEvtUnifiedManagerDiskSpaceFull）	意外事件	管理站	关键
管理服务器内存不足（ocumEvtUnifiedManagerMemoryLow）	风险	管理站	警告
管理服务器内存几乎用尽（ocumEvtUnifiedManagerMemoryAlmostOut）	意外事件	管理站	关键
MySQL 日志文件大小已增加；需要重新启动（ocumEvtMysqlLogFileSizeWarning）	意外事件	管理站	警告
审核日志总大小分配即将满	风险	管理站	警告
Syslog 服务器证书即将过期	风险	管理站	警告
Syslog 服务器证书已过期	风险	管理站	错误
审核日志文件已篡改	风险	管理站	警告
审核日志文件已删除	风险	管理站	警告
Syslog 服务器连接错误	风险	管理站	错误
Syslog 服务器配置已更改	事件	管理站	警告

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
性能数据分析受影响（ocumEvtUnifiedManagerDataMissingAnalyze）	风险	管理站	警告
性能数据收集受影响（ocumEvtUnifiedManagerDataMissingCollection）	意外事件	管理站	关键

最后两个性能事件仅适用于 Unified Manager 7.2。如果这些事件中的任何一个处于“新建”状态，然后您升级到较新版本的 Unified Manager 软件，则不会自动清除这些事件。您需要手动将事件移至“已解决”状态。

了解 **Active IQ Unified Manager** 中的 **MetroCluster Bridge** 事件

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

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
网桥不可达（ocumEvtBridgeUnreachable）	意外事件	MetroCluster 桥接	关键
桥温异常（ocumEvtBridgeTemperatureAbnormal）	意外事件	MetroCluster 桥接	关键

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 连接事件

连接事件为您提供有关群集组件之间以及基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置中群集之间连接的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

两种配置中常见的事件

这些连接事件在基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置中都很常见。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
MetroCluster 伙伴之间的所有链路均已关闭（ocumEvtMetroClusterAllLinksBetweenPartnersDown）	意外事件	MetroCluster 关系	关键
MetroCluster 无法通过对等网络访问配对集群（ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork）	意外事件	MetroCluster 关系	关键
MetroCluster 灾难恢复功能受影响（ocumEvtMetroClusterDRStatusImpacted）	风险	MetroCluster 关系	关键
MetroCluster 配置已切换（ocumEvtMetroClusterDRStatusImpacted）	风险	MetroCluster 关系	警告

MetroCluster 基于 **FC** 的配置

这些事件与基于 FC 的 MetroCluster 配置有关。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
所有交换机间链路已关闭（ocumEvtMetroClusterAllISLBetweenSwitchesDown）	意外事件	MetroCluster 交换机间连接	关键
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	关键
MetroCluster 配置已部分切换（ocumEvtMetroClusterDRStatusPartiallyImpacted）	风险	MetroCluster 关系	错误
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	关键
节点到 FC 交换机的一个或多个 FC 启动器链路已关闭（ocumEvtMccNodeSwitchFcLinksOneOrMoreDown）	风险	MetroCluster 节点交换机连接	警告
节点到 FC 交换机所有 FC 启动程序链路断开（ocumEvtMccNodeSwitchFcLinksDown）	意外事件	MetroCluster 节点交换机连接	关键
交换机到 FC-SAS 网桥的 FC 链路已关闭（ocumEvtMccSwitchBridgeFcLinksDown）	意外事件	MetroCluster 交换机网桥连接	关键
Inter Node All FC VI InterConnect 链路全部断开(ocumEvtMccInterNodeLinksDown)	意外事件	节点间连接	关键
节点间的一个或多个 FC VI InterConnect 链路已关闭（ocumEvtMccInterNodeLinksOneOrMoreDown）	风险	节点间连接	警告
节点到网桥的链路已关闭（ocumEvtMccNodeBridgeLinksDown）	意外事件	节点网桥连接	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
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	关键
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

这些事件涉及基于 IP 的 MetroCluster 配置。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
MetroCluster IP 站点间连接状态为已关闭（mccIntersiteconnectivityStatusDown）	风险	MetroCluster 关系	关键
MetroCluster-IP 节点到交换机连接离线（mccIpPortStatusOffline）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 交换机事件

针对基于 FC 的 MetroCluster 配置的 MetroCluster 交换机事件可为您提供有关 MetroCluster 交换机状态的信息，以便您监控潜在问题。事件按影响区域分组，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	严重性
交换机温度异常（ocumEvtSwitchTemperatureAbnormal）	意外事件	MetroCluster 交换机	关键
交换机无法访问（ocumEvtSwitchUnreachable）	意外事件	MetroCluster 交换机	关键
交换机风扇出现故障（ocumEvtSwitchFansOneOrMoreFailed）	意外事件	MetroCluster 交换机	关键

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

了解 **Active IQ Unified Manager** 中的 **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，以便您可以监视潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

星号（*）用于标识已转换为 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	严重性
NVMeNS 离线 *（nvmeNamespaceStatusOffline）	事件	命名空间	信息
NVMeNS 在线 *(nvmeNamespaceStatusOnline)	事件	命名空间	信息
NVMeNS 空间不足 *（nvmeNamespaceSpaceOutOfSpace）	风险	命名空间	警告
NVMeNS 销毁 *（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	严重性
NVMe 命名空间 IOPS 严重阈值已突破（ocumNvmeNamespaceIopsIncident）	意外事件	命名空间	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 NVMe 命名空间 IOPS 警告阈值（ocumNvmeNamespaceIopsWarning）	风险	命名空间	警告
NVMe 命名空间 MB/s 严重阈值已超出（ocumNvmeNamespaceMbpsIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间 MB/s 警告阈值（ocumNvmeNamespaceMbpsWarning）	风险	命名空间	警告
NVMe 命名空间延迟 ms/op 严重阈值已违反（ocumNvmeNamespaceLatencyIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间延迟 ms/op 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	关键
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/s 严重阈值（ocumNvmeNamespaceLatencyMbpsIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间延迟和 MB/s 警告阈值（ocumNvmeNamespaceLatencyMbpsWarning）	风险	命名空间	警告

了解 **Active IQ Unified Manager** 中的节点事件

节点事件提供了有关节点状态的信息，可用于监控潜在的问题。事件按影响区域进行分组，并可提供事件和陷阱名称、影响级别、源类型和严重性。

星号（*）用于标识已转换为 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	严重性
节点根卷空间即将满（ocumEvtClusterNodeRootVolumeSpaceNearlyFull）	风险	节点	警告
Cloud AWS MetaDataConnFail *（ocumCloudAwsMetadataConnFail）	风险	节点	错误
云 AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	风险	节点	错误
云 AWS IAMCredsInvalid *（ocumCloudAwsIamCredsInvalid）	风险	节点	错误
云 AWS IAMCredsNotFound *（ocumCloudAwsIamCredsNotFound）	风险	节点	错误
云 AWS IAMCredsNotInitialized *（ocumCloudAwsIamCredsNotInitialized）	事件	节点	信息
云 AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	风险	节点	错误
云 AWS IAMRoleNotFound *（ocumCloudAwsIamRoleNotFound）	风险	节点	错误
云层主机无法解析 *（ocumObjstoreHostUnresolvable）	风险	节点	错误
云层集群间网络接口已关闭 *（ocumObjstoreInterClusterLifDown）	风险	节点	错误
其中一个 NFSv4 池已耗尽 *（nbladeNfsv4PoolEXhaust）	意外事件	节点	关键
请求与云分层签名不匹配 *(oscSignatureMismatch)	风险	节点	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
QoS Monitor 内存已达上限 *（ocumQosMonitorMemoryMaxed）	风险	节点	错误
QoS 监控内存已缩减 *（ocumQosMonitorMemoryAbated）	事件	节点	信息

影响区域：配置

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

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反节点 IOPS 严重阈值（ocumNodeIopsIncident）	意外事件	节点	关键
已违反节点 IOPS 警告阈值（ocumNodeIopsWarning）	风险	节点	警告
节点 MB/s 严重阈值已违反（ocumNodeMbpsIncident）	意外事件	节点	关键
已违反节点 MB/s 警告阈值（ocumNodeMbpsWarning）	风险	节点	警告
已违反节点延迟毫秒/操作严重阈值（ocumNodeLatencyIncident）	意外事件	节点	关键
已违反节点延迟毫秒/操作警告阈值（ocumNodeLatencyWarning）	风险	节点	警告
违反节点已用性能容量严重阈值（ocumNodePerfCapacityUsedIncident）	意外事件	节点	关键

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

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
咨询 ID：NTAP-<*advisory ID*>（ocumx）	风险	节点	关键

了解 **Active IQ Unified Manager** 中的 **NVRAM** 电池事件

NVRAM 电池事件可为您提供有关电池状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
NVRAM 电池电量低（ocumEvtNvramBatteryLow）	风险	节点	警告
NVRAM 电池已放电（ocumEvtNvramBatteryDischarged）	风险	节点	错误
NVRAM 电池充电过度（ocumEvtNvramBatteryOverCharged）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的端口事件

端口事件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	严重性
端口状态已关闭（ocumEvtPortStatusDown）	意外事件	节点	关键

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反网络端口 MB/s 严重阈值（ocumNetworkPortMbpsIncident）	意外事件	端口	关键
已违反网络端口 MB/s 警告阈值（ocumNetworkPortMbpsWarning）	风险	端口	警告
已违反 FCP 端口 MB/s 严重阈值（ocumFcpPortMbpsIncident）	意外事件	端口	关键
已违反 FCP 端口 MB/s 警告阈值（ocumFcpPortMbpsWarning）	风险	端口	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反网络端口利用率严重阈值（ocumNetworkPortUtilizationIncident）	意外事件	端口	关键
已违反网络端口利用率警告阈值（ocumNetworkPortUtilizationWarning）	风险	端口	警告
已违反 FCP 端口利用率严重阈值（ocumFcpPortUtilizationIncident）	意外事件	端口	关键
FCP 端口利用率警告阈值已违反（ocumFcpPortUtilizationWarning）	风险	端口	警告

了解 **Active IQ Unified Manager** 中的电源事件

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

影响区域：可用性

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

了解 **Active IQ Unified Manager** 中的保护事件

保护事件会告诉您作业是否已失败或中止，以便您可以监控问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：保护

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

了解 **Active IQ Unified Manager** 中的 **Qtree** 事件

Qtree 事件为您提供有关 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，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
Qtree 空间接近全满（ocumEvtQtreeSpaceNearlyFull）	风险	qtree	警告
Qtree 空间已满（ocumEvtQtreeSpaceFull）	风险	qtree	错误
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	关键
已违反 Qtree 文件软限制（ocumEvtQtreeFilesSoftLimitBreached）	风险	qtree	警告
已达到 Qtree 空间硬限制（ocumEvtQtreeSpaceHardLimitReached）	意外事件	qtree	关键
已违反 qtree 空间软限制（ocumEvtQtreeSpaceSoftLimitBreached）	风险	qtree	警告

了解 **Active IQ Unified Manager** 中的 **Service Processor** 事件

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

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
服务处理器未配置（ocumEvtServiceProcessorNotConfigured）	风险	节点	警告
服务处理器离线（ocumEvtServiceProcessorOffline）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的 **SnapMirror** 关系事件

SnapMirror 关系事件为您提供有关异步和同步 SnapMirror 关系状态的信息，以便您可以监控潜在问题。异步 SnapMirror 关系事件是为 Storage VM 和卷生成的，而同步 SnapMirror 关系事件仅为卷关系生成。不会为属于 Storage VM 灾难恢复关系的组成卷生成任何事件。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：保护

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

SnapMirror 关系事件是为受 Storage VM 灾难恢复保护的 Storage VM 生成的，但不会为任何组成对象关系生成。

事件名称（陷阱名称）	影响级别	源类型	严重性
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	错误
镜像复制初始化失败（ocumEvtSnapmirrorRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
镜像复制更新失败（ocumEvtSnapmirrorRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
镜像复制滞后错误（ocumEvtSnapMirrorRelationshipLagError）	风险	SnapMirror 关系	错误
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	错误
同步复制未同步 *（syncSnapmirrorRelationshipOutofsync）	风险	SnapMirror 关系	警告
同步复制已还原 *（syncSnapmirrorRelationshipInSync）	事件	SnapMirror 关系	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
同步复制自动重新同步失败*（syncSnapmirrorRelationshipAutoSyncRetryFailed）	风险	SnapMirror 关系	错误
在集群（snapmirrorMediatorAdded）上添加了 Ontap Mediator	事件	集群	信息
已从集群中删除 Ontap Mediator（snapmirrorMediatorRemoved）	事件	集群	信息
无法从集群访问 Ontap Mediator（snapmirrorMediatorUnreachable）	风险	调解器	警告
无法从集群访问 Ontap Mediator（snapmirrorMediatorMisconfigured）	风险	调解器	错误
Ontap Mediator 连接已重新建立，并且已重新同步，准备好进行 SnapMirror 活动同步（snapmirrorMediatorInQuorum）	事件	调解器	信息

了解 **Active IQ Unified Manager** 中的异步镜像和 **Vault** 关系事件

异步镜像和 Vault 关系事件为您提供有关异步 SnapMirror 和 Vault 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 Vault 关系事件。但是，只有 Vault 关系不支持 Storage VM 灾难恢复。事件按影响区域分组，包括事件和 trap 名称、影响级别、源类型和严重程度。

影响区域：保护

还会为受 Storage VM 灾难恢复保护的 Storage VM 生成 SnapMirror 和 Vault 关系事件，但不会为任何组成对象关系生成。

事件名称（陷阱名称）	影响级别	源类型	严重性
异步镜像和存储不正常（ocumEvtMirrorVaultRelationshipUnhealthy）	风险	SnapMirror 关系	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
异步镜像和保管库已断开（ocumEvtMirrorVaultRelationshipStateBrokenoff）	风险	SnapMirror 关系	错误
异步镜像和存储库初始化失败（ocumEvtMirrorVaultRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
异步镜像和存储更新失败（ocumEvtMirrorVaultRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
异步镜像和存储滞后错误（ocumEvtMirrorVaultRelationshipLagError）	风险	SnapMirror 关系	错误
异步镜像和存储滞后警告（ocumEvtMirrorVaultRelationshipLagWarning）	风险	SnapMirror 关系	警告
异步镜像和存储库重新同步失败（ocumEvtMirrorVaultRelationshipResyncFailed）	风险	SnapMirror 关系	错误

"SnapMirror 更新失败"事件由 Active IQ 门户（Config Advisor）引发。

了解 **Active IQ Unified Manager** 中的 **Snapshot** 事件

快照事件提供有关快照状态的信息，使您能够监控快照以发现潜在问题。事件按影响区域分组，包括事件名称、陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
快照自动删除已禁用（不适用）	事件	卷	信息
已启用快照自动删除（不适用）	事件	卷	信息
快照自动删除配置已修改（不适用）	事件	卷	信息

了解 **Active IQ Unified Manager** 中的 **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，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	严重性
异步 Vault 不正常（ocumEvtSnapVaultRelationshipUnhealthy）	风险	SnapMirror 关系	警告
异步 Vault 已断开（ocumEvtSnapVaultRelationshipStateBrokenoff）	风险	SnapMirror 关系	错误
异步 Vault 初始化失败（ocumEvtSnapVaultRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
异步 Vault 更新失败（ocumEvtSnapVaultRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
异步 Vault 滞后错误（ocumEvtSnapVaultRelationshipLagError）	风险	SnapMirror 关系	错误
异步 Vault 滞后警告（ocumEvtSnapVaultRelationshipLagWarning）	风险	SnapMirror 关系	警告
异步 Vault 重新同步失败（ocumEvtSnapvaultRelationshipResyncFailed）	风险	SnapMirror 关系	错误

了解 **Active IQ Unified Manager** 中的存储故障转移设置事件

存储故障转移（SFO）设置事件可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，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
存储故障转移互连一个或多个链路已关闭（ocumEvtSfoInterconnectOneOrMoreLinksDown）	风险	节点	警告
存储故障转移已禁用（ocumEvtSfoSettingsDisabled）	风险	节点	错误
未配置存储故障转移（ocumEvtSfoSettingsNotConfigured）	风险	节点	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
存储故障转移状态 - 接管（ocumEvtSfoStateTakeover）	风险	节点	警告
存储故障转移状态 - 部分交还（ocumEvtSfoStatePartialGiveback）	风险	节点	错误
存储故障转移节点状态为已关闭（ocumEvtSfoNodeStatusDown）	风险	节点	错误
无法执行存储故障转移接管（ocumEvtSfoTakeoverNotPossible）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的存储服务事件

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

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
存储服务已创建（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	严重性
意外删除受管 SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	风险	存储服务	警告
意外删除存储服务成员卷（ocumEvtStorageServiceUnexpectedVolumeDeletion）	意外事件	存储服务	关键

了解 **Active IQ Unified Manager** 中的存储架事件

存储磁盘架事件会告诉您存储磁盘架是否出现异常，以便您监控潜在问题。事件按影响区域分组，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	严重性
电压范围异常（ocumEvtShelfVoltageAbnormal）	风险	存储架	警告
异常电流范围（ocumEvtShelfCurrentAbnormal）	风险	存储架	警告
温度异常（ocumEvtShelfTemperatureAbnormal）	风险	存储架	警告

了解 **Active IQ Unified Manager** 中的 **Storage VM** 事件

存储 VM（存储虚拟机，也称为 SVM）事件可为您提供有关存储 VM（SVM）状态的信息，以便您可以监视潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

星号（*）用于标识已转换为 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	严重性
Storage VM CIFS 服务已关闭（ocumEvtVserverCifsServiceStatusDown）	意外事件	SVM	关键
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	关键
CIFS NetBIOS 名称冲突 *（nbladeCifsNbNameConflict）	风险	SVM	错误
CIFS 卷影复制操作失败 *（cifsShadowCopyFailure）	风险	SVM	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
许多 CIFS 连接 *（nbladeCifsManyAuths）	风险	SVM	错误
超出 CIFS 连接数上限 *（nbladeCifsMaxOpenSameFile）	风险	SVM	错误
超出每用户 CIFS 连接数上限 *（nbladeCifsMaxSessPerUsrConn）	风险	SVM	错误
SVM FC/FCoE 服务关闭（ocumEvtVserverFcServiceStatusDown）	意外事件	SVM	关键
SVM iSCSI 服务已关闭（ocumEvtVserverIscsiServiceStatusDown）	意外事件	SVM	关键
Storage VM NFS 服务已关闭（ocumEvtVserverNfsServiceStatusDown）	意外事件	SVM	关键
SVM FC/FCoE 服务未配置（不适用）	事件	SVM	信息
SVM iSCSI 服务未配置（不适用）	事件	SVM	信息
SVM NFS 服务未配置（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	错误
没有可用于病毒扫描的 AV 服务器连接 *（nbladeVscanNoScannerConn）	意外事件	SVM	关键
未注册 AV 服务器 *（nbladeVscanNoRegdScanner）	风险	SVM	错误
AV 服务器连接无响应 *（nbladeVscanConnInactive）	事件	SVM	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
未经授权的用户尝试访问 AV 服务器 *（nbladeVscanBadUserPrivAccess）	风险	SVM	错误
AV 服务器发现病毒 *（nbladeVscanVirusDetected）	风险	SVM	错误

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已发现 SVM（不适用）	事件	SVM	信息
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	严重性
SVM IOPS 严重阈值已违反（ocumSvmIopsIncident）	意外事件	SVM	关键
已违反 SVM IOPS 警告阈值（ocumSvmIopsWarning）	风险	SVM	警告
已违反 SVM MB/s 严重阈值（ocumSvmMbpsIncident）	意外事件	SVM	关键
已违反 SVM MB/s 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	关键
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	严重性
审核日志已禁用（ocumVserverAuditLogDisabled）	风险	SVM	警告
登录横幅已禁用（ocumVserverLoginBannerDisabled）	风险	SVM	警告
SSH 正在使用不安全密码（ocumVserverSSHInsecure）	风险	SVM	警告
登录横幅已更改（ocumVserverLoginBannerChanged）	风险	SVM	警告
Storage VM 反勒索软件监控已禁用（antiRansomwareSvmStateDisabled）	风险	SVM	警告
Storage VM 反勒索软件监控已启用（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）（ocumEvtSvmArwCandidate）	事件	SVM	信息

了解 **Active IQ Unified Manager** 中的用户和组配额事件

用户和组配额事件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，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反用户或组配额磁盘空间软限制（ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached）	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	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反用户或组配额文件数软限制（ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached）	风险	用户或组配额	警告
已达到用户或组配额文件数硬限制（ocumEvtUserOrGroupQuotaFileCountHardLimitReached）	意外事件	用户或组配额	关键

了解 **Active IQ Unified Manager** 中的卷事件

卷事件提供有关卷状态的信息，使您能够监控潜在问题。事件按影响区域分组，包括事件名称、陷阱名称、影响级别、源类型和严重程度。

星号（*）用于标识已转换为 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	严重性
卷受限（ocumEvtVolumeRestricted）	风险	卷	警告
卷脱机（ocumEvtVolumeOffline）	意外事件	卷	关键
卷部分可用（ocumEvtVolumePartiallyAvailable）	风险	卷	错误
卷已卸载（不适用）	事件	卷	信息
卷已挂载（不适用）	事件	卷	信息
卷已重新挂载（不适用）	事件	卷	信息
卷接合路径非活动（ocumEvtVolumeJunctionPathInactive）	风险	卷	警告
已启用卷自动调整大小（不适用）	事件	卷	信息
卷自动调整大小-禁用（不适用）	事件	卷	信息
卷自动调整大小最大容量已修改（不适用）	事件	卷	信息
卷自动调整大小增量大小已修改（不适用）	事件	卷	信息

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
精简配置卷空间存在风险（ocumThinProvisionVolumeSpaceAtRisk）	风险	卷	警告
卷效率操作错误（ocumEvtVolumeEfficiencyOperationError）	风险	卷	错误
卷空间已满（ocumEvtVolumeFull）	风险	卷	错误
卷空间接近全满（ocumEvtVolumeNearlyFull）	风险	卷	警告
卷逻辑空间已满 *（volumeLogicalSpaceFull）	风险	卷	错误
卷逻辑空间接近全满 *（volumeLogicalSpaceNearlyFull）	风险	卷	警告
卷逻辑空间正常 *(volumeLogicalSpaceAllOK)	事件	卷	信息
卷 Snapshot 预留空间已满（ocumEvtSnapshotFull）	风险	卷	警告
Snapshot 副本太多（ocumEvtSnapshotTooMany）	风险	卷	错误
卷 Qtree 配额已过量提交（ocumEvtVolumeQtreeQuotaOvercommitted）	风险	卷	错误
卷 Qtree 配额接近过量提交（ocumEvtVolumeQtreeQuotaAlmostOvercommitted）	风险	卷	警告
卷增长率异常（ocumEvtVolumeGrowthRateAbnormal）	风险	卷	警告
卷达到全满前的天数（ocumEvtVolumeDaysUntilFullSoon）	风险	卷	错误
卷空间保证已禁用（不适用）	事件	卷	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
卷空间保证已启用（不适用）	事件	卷	信息
卷空间保证已修改（不适用）	事件	卷	信息
卷 Snapshot 预留达到全满前的天数（ocumEvtVolumeSnapshotReserveDaysUntilFullSoon）	风险	卷	错误
FlexGroup 成分存在空间问题 *（flexGroupConstituentsHaveSpaceIssues）	风险	卷	错误
FlexGroup 成分卷空间状态一切正常 *(flexGroupConstituentsSpaceStatusAllOK)	事件	卷	信息
FlexGroup 成分卷存在索引节点问题*（flexGroupConstituentsHaveInodesIssues）	风险	卷	错误
FlexGroup 成分卷 Inode 状态全部正常 *(flexGroupConstituentsInodesStatusAllOK)	事件	卷	信息
WAFL 卷 AutoSize 失败 *（waflVolAutoSizeFail）	风险	卷	错误
WAFL 卷 AutoSize 已完成*（waflVolAutoSizeDone）	事件	卷	信息
FlexGroup 卷利用率超过 80%*	意外事件	卷	错误
FlexGroup 卷利用率超过 90%*	意外事件	卷	关键
卷存储效率异常（ocumVolumeAbnormalStorageEfficiencyWarning）	风险	卷	警告
卷 Snapshot 预留未充分利用（volumeSnaphotReserveUnderutilizedWarning）	事件	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
卷 Snapshot 预留未充分利用（volumeSnaphotReserveUnderutilizedCleared）	事件	卷	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
卷已重命名（不适用）	事件	卷	信息
发现的卷（不适用）	事件	卷	信息
卷已删除（不适用）	事件	卷	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 QoS 卷最大 IOPS 警告阈值（ocumQosVolumeMaxIopsWarning）	风险	卷	警告
已违反 QoS 卷最大 MB/s 警告阈值（ocumQosVolumeMaxMbpsWarning）	风险	卷	警告
已违反 QoS 卷最大 IOPS/TB 警告阈值（ocumQosVolumeMaxIopsPerTbWarning）	风险	卷	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	卷	警告
已违反卷 IOPS 严重阈值（ocumVolumeIopsIncident）	意外事件	卷	关键
已违反卷 IOPS 警告阈值（ocumVolumeIopsWarning）	风险	卷	警告
已违反卷 MB/s 严重阈值（ocumVolumeMbpsIncident）	意外事件	卷	关键
卷 MB/s 警告阈值已突破（ocumVolumeMbpsWarning ）	风险	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反卷延迟严重阈值（ocumVolumeLatencyIncident）	意外事件	卷	关键
已违反卷延迟警告阈值（ocumVolumeLatencyWarning）	风险	卷	警告
已违反卷缓存未命中率严重阈值（ocumVolumeCacheMissRatioIncident）	意外事件	卷	关键
已违反卷缓存未命中率警告阈值（ocumVolumeCacheMissRatioWarning）	风险	卷	警告
已违反卷延迟和 IOPS 严重阈值（ocumVolumeLatencyIopsIncident）	意外事件	卷	关键
已违反卷延迟和 IOPS 警告阈值（ocumVolumeLatencyIopsWarning）	风险	卷	警告
已违反卷延迟和 MB/s 严重阈值（ocumVolumeLatencyMbpsIncident）	意外事件	卷	关键
已违反卷延迟和 MB/s 警告阈值（ocumVolumeLatencyMbpsWarning）	风险	卷	警告
已违反卷延迟和聚合已用性能容量严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedIncident）	意外事件	卷	关键
已违反卷延迟和聚合已用性能容量警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedWarning）	风险	卷	警告
已违反卷延迟和聚合利用率严重阈值（ocumVolumeLatencyAggregateUtilizationIncident）	意外事件	卷	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反卷延迟和聚合利用率警告阈值（ocumVolumeLatencyAggregateUtilizationWarning）	风险	卷	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	卷	关键
已违反卷延迟和节点已用性能容量警告阈值（ocumVolumeLatencyNodePerfCapacityUsedWarning）	风险	卷	警告
卷延迟和已用节点性能容量 - 已违反接管严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident）	意外事件	卷	关键
卷延迟和已用节点性能容量 - 已违反接管警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning）	风险	卷	警告
已违反卷延迟和节点利用率严重阈值（ocumVolumeLatencyNodeUtilizationIncident）	意外事件	卷	关键
已违反卷延迟和节点利用率警告阈值（ocumVolumeLatencyNodeUtilizationWarning）	风险	卷	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
卷反勒索软件监控已启用（活动模式）（antiRansomwareVolumeStateEnabled）	事件	卷	信息
卷反勒索软件监控已禁用（antiRansomwareVolumeStateDisabled）	风险	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
卷反勒索软件监控已启用（学习模式）（antiRansomwareVolumeStateDryrun）	事件	卷	信息
卷反勒索软件监控已暂停（学习模式）（antiRansomwareVolumeStateDryrunPaused）	风险	卷	警告
卷反勒索软件监控已暂停（活动模式）（antiRansomwareVolumeStateEnablePaused）	风险	卷	警告
卷防勒索软件监控正在禁用（antiRansomwareVolumeStateDisableInProgress）	风险	卷	警告
已发现勒索软件活动（callHomeRansomwareActivitySeen）	意外事件	卷	关键
适用于反勒索软件监控的卷（学习模式）（ocumEvtVolumeArwCandidate）	事件	卷	信息
适用于反勒索软件监控的卷（活动模式）（ocumVolumeSuitedForActiveAntiRansomwareDetection）	风险	卷	警告
卷显示频繁的反勒索软件警报（antiRansomwareFeatureNoisyVolume）	风险	卷	警告

影响领域：数据保护

事件名称（陷阱名称）	影响级别	源类型	严重性
卷的本地快照保护不足（volumeLacksLocalProtectionWarning）	风险	卷	警告
卷的本地快照保护不足（volumeLacksLocalProtectionCleared）	风险	卷	警告

了解 **Active IQ Unified Manager** 中的卷移动状态事件

卷移动状态事件可告知您卷移动的状态，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
卷移动状态：正在进行中（不适用）	事件	卷	信息
卷移动状态 - 失败（ocumEvtVolumeMoveFailed）	风险	卷	错误
卷移动状态：已完成（不适用）	事件	卷	信息
卷移动 - 转换延迟（ocumEvtVolumeMoveCutoverDeferred）	风险	卷	警告

事件窗口和对话框说明

了解 **Active IQ Unified Manager** 中的通知页面

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，通知可以作为电子邮件或 SNMP 陷阱发送。

您必须具有应用程序管理员或存储管理员角色。

电子邮件

此区域用于配置以下用于告警通知的电子邮件设置：

- 发件人地址

  指定发送警报通知的电子邮件地址。此值在共享时也用作报告的发件人地址。如果发件人地址预先填写了地址“ActiveIQUnifiedManager@localhost.com”，则应将其更改为真实有效的电子邮件地址，以确保成功发送所有电子邮件通知。

SMTP 服务器

此区域用于配置以下 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，该主机名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 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 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**

  选中此框可通过使用 TLS/SSL 协议（也称为 start_tls 和 StartTLS）在 SMTP 服务器与管理服务器之间提供安全通信。

- 使用 **SSL**

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

SNMP

此区域用于配置以下 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、版本 3（含身份验证）和版本 3（含身份验证和加密）。默认值为版本 1。

- **Trap** 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）。要指定多个陷阱目的地，请使用逗号分隔每个主机。

  所有其他 SNMP 设置（例如“版本”和“出站端口”）对于此列表中的所有主机必须相同。

- 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、SNMP 版本 3（含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 用户名

指定 SNMP 用户名。用户名可用于 SNMP 版本 3、SNMP 版本 3（含身份验证）和 SNMP 版本 3（含身份验证和加密）。

- 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。MD5 是默认值。身份验证协议可用于 SNMP 版本 3 （含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 身份验证密码

  指定对用户进行身份验证时使用的密码。SNMP 版本 3（含身份验证）和 SNMP 版本 3（含身份验证和加密）提供身份验证密码。

- 隐私协议

  指定用于加密 SNMP 消息的隐私协议。协议选项包括 AES 128 和 DES。默认值为 AES 128。隐私协议适用于具有身份验证和加密功能的 SNMP 版本 3。

- 隐私密码

  指定使用隐私协议时的密码。隐私密码可用于具有身份验证和加密的 SNMP 版本 3。

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

了解 **Active IQ Unified Manager** 中的事件管理清单页面

事件管理清单页面使您能够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

使您能够自定义事件列表中显示的信息。可以使用以下组件优化显示的事件列表：

- 查看菜单可从预定义的筛选器选择列表中进行选择。

  这包括所有活动（新建和确认）事件、活动性能事件、分配给我（登录用户）的事件以及所有维护期间生成的所有事件等项目。

- 搜索窗格，用于通过输入完整或部分术语来细化事件列表。
- 用于启动“筛选器”窗格的“筛选器”按钮，以便您可以从每个可用的字段和字段属性中进行选择以优化事件列表。

命令按钮

这些命令按钮可用来执行下列任务：

- 分配给

  使您能够选择要将事件分配给的用户。将事件分配给用户时，用户名和分配事件的时间将添加到所选事件的事件列表中。

- 自己

  将事件分配给当前登录的用户。

- 其他用户

  显示“分配所有者”对话框，通过该对话框可以将事件分配或重新分配给其他用户。您也可以将所有权字段留空以取消分配事件。

- 确认

  确认选定事件。

  当您确认事件时，您的用户名和确认事件的时间将添加到选定事件的事件列表中。当您确认某个事件时，您有责任管理该事件。

  您无法确认信息事件。

- 标记为已解决

  使您能够将事件状态更改为已解决。

  解决事件时，您的用户名和解决该事件的时间将添加到所选事件的事件列表中。对事件采取纠正措施后，必须将该事件标记为已解决。

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

- 报告

  使您能够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

  使您能够选择在页面上显示的列，并选择它们的显示顺序。

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，以显示前七天具有事件或风险影响级别的新事件和已确认事件。

- 触发时间

  生成事件的时间。

- 严重程度

  事件严重性：Critical （严重） （）、Error （错误） （）、Warning （警告） （）和 Information （信息） （）。

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 影响级别

  事件影响级别：突发事件、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。您可以选择名称以显示该事件的“事件详细信息”页面。

- 源

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

  当发生共享 QoS 策略违规时，此字段中仅显示占用最多 IOPS 或 MB/s 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）。

- 分配给

  事件分配到的用户名称。

- 事件起源

  事件是源自“Active IQ Portal”还是直接源自“Active IQ Unified Manager”。

- 注释名称

  分配给存储对象的批注的名称。

- 备注

  为事件添加的注释数。

- 待处理天数

  事件最初生成后的天数。

- 分配时间

  事件分配给用户后经过的时间。如果经过的时间超过一周，则会显示事件分配给用户的时间戳。

- 确认人

确认此事件的用户的名称。如果事件未确认，此字段为空。

- 确认时间

  事件确认后经过的时间。如果经过的时间超过一周，则会显示事件确认的时间戳。

- 解决者

  解决事件的用户的名称。如果事件未解决，则此字段为空。

- 解决时间

  事件解决后经过的时间。如果经过的时间超过一周，则会显示事件解决的时间戳。

- 废弃时间

  事件状态变为已过时的时间。

事件详细信息页面

了解 **Active IQ Unified Manager** 中的事件详细信息页面

从“事件详细信息”页面，您可以查看所选事件的详细信息，例如事件严重程度、影响级别、影响区域和事件源。您还可以查看有关可能的修复措施的其他信息，以解决此问题。

- 事件名称

  事件的名称和上次发现事件的时间。

  对于非性能事件，当事件处于“新建”或“已确认”状态时，最后看到的信息未知，因此被隐藏。

- 事件描述

  对事件的简要描述。

  在某些情况下，事件触发的原因会在事件描述中提供。

- 争用组件

  对于动态性能事件，此部分显示表示集群的逻辑和物理组件的图标。如果组件处于争用状态，其图标将带圆圈并突出显示为红色。

  有关此处显示的组件的说明，请参阅 *Cluster components and why they can be in contention*。

事件信息、系统诊断和建议操作部分在其他主题中进行了说明。

命令按钮

这些命令按钮可用来执行下列任务：

- 备注图标

使您可以添加或更新有关事件的备注，并查看其他用户留下的所有备注。

操作菜单

- 分配给我

  将此事件分配给您。

- 分配给其他人

  打开“分配所有者”对话框，用于将事件分配或重新分配给其他用户。

  将事件分配给用户时，用户的名称和事件分配的时间将添加到选定事件的事件列表中。

  您也可以将所有权字段留空，以取消分配事件。

- 确认

  确认所选事件，这样您就不会继续收到重复警报通知。

  当您确认事件时，您的用户名和确认事件的时间将添加到选定事件的事件列表（确认人）中。当您确认某个事件时，您负责管理该事件。

- 标记为已解决

  使您能够将事件状态更改为“已解决”。

  当您解决事件时，您的用户名和解决该事件的时间将添加到所选事件的事件列表（解决者）中。对事件采取纠正措施后，必须将该事件标记为已解决。

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

了解 **Active IQ Unified Manager** 中的事件信息部分

您可以使用事件详细信息页面上的"事件信息"部分，查看有关所选事件的详细信息，例如事件严重性、影响级别、影响区域和事件源。

不适用于该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。

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 废弃原因

  导致事件被废弃的操作，例如，问题已修复。

- 事件持续时间

  对于活动（新建和已确认）事件，这是检测到事件与上次分析事件之间的时间。对于过时的事件，这是检测到事件和解决事件之间的时间。

  此字段针对所有性能事件显示，对于其他事件类型，仅在它们已解决或已过时后才显示。

- 上次查看时间

  上次将事件显示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新，因为只要事件处于活动状态，此字段就会在每次新的性能数据收集之后更新。对于其他类型的事件，当处于“新建”或“已确认”状态时，此内容不会更新，因此该字段将被隐藏。

- 严重程度

  事件严重性：Critical （严重） （）、Error （错误） （）、Warning （警告） （）和 Information （信息） （）。

- 影响级别

  事件影响级别：突发事件、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。

  查看共享 QoS 策略事件的详细信息时，此字段中最多会列出三个消耗 IOPS 或 MBps 最多的工作负载对象。

  您可以单击源名称链接来显示该对象的运行状况或性能详细信息页面。

- 源注释

  显示与事件关联的对象的批注名称和值。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源组

  显示受影响对象所属的所有组的名称。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源类型

  与事件关联的对象类型（例如 SVM、Volume 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来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

  受此事件影响的对象数。

  您可以单击对象链接来显示包含当前受此事件影响的对象的清单页面。

  此字段仅针对性能事件显示。

- 受影响的卷

  受此事件影响的卷数。

  此字段仅针对节点或聚合上的性能事件显示。

- 触发策略

  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，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（分配空间或已用空间）。

  此字段仅针对性能事件显示。

- 规则 **ID**

  对于 Active IQ 平台事件，这是触发生成此事件的规则编号。

- 确认人

  确认该事件的人员的姓名和确认该事件的时间。

- 解决者

  解决事件的人员姓名和事件解决的时间。

- 分配给

  被指派处理该事件的人员的姓名。

- 警报设置

  此时将显示有关警报的以下信息：

  - 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。

- 如果有一个警报与所选事件关联，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。

- 如果有多个警报与所选事件相关联，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。

已禁用的警报不会显示。

- 上次发送的通知

  发送最新警报通知的日期和时间。

- 发送方式

  用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- 上次脚本运行

  生成警报时所执行脚本的名称。

了解 **Active IQ Unified Manager** 中的建议操作

“事件详细信息”页面的“建议操作”部分提供了此事件的可能原因，并建议了一些操作，以便您可以尝试自行解决此事件。建议的操作是根据已违反的事件类型或阈值类型进行自定义的。

此区域仅针对某些类型的事件显示。

在某些情况下，页面上提供的*帮助*链接会引用许多建议操作的其他信息，包括执行特定操作的说明。其中一些操作可能涉及使用 Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLI 命令或这些工具的组合。

此处建议的操作仅供解决事件时参考。您应根据具体环境情况来确定用于解决此事件的操作。

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 可以彻底诊断某些事件并提供单一解决方案。如果可用，这些解决方案将通过 修复 按钮显示。单击此按钮可让 Unified Manager 修复导致此事件的问题。

对于 Active IQ 平台事件，此部分可能包含指向 NetApp 知识库文章的链接（如果可用），该文章描述了问题和可能的解决方案。在没有外部网络访问权限的站点中，知识库文章的 PDF 将在本地打开；该 PDF 是手动下载到 Unified Manager 实例的规则文件的一部分。

了解 **Active IQ Unified Manager** 中的系统诊断

“事件详细信息”页面的“系统诊断”部分提供了可以帮助您诊断可能导致该事件的问题的信息。

此区域仅针对某些事件显示。

某些性能事件会提供与已触发的特定事件相关的图表。通常，这包括前十天的 IOPS 或 MBps 图表以及延迟图表。以这种方式排列后，您可以看到在事件处于活动状态时，哪些存储组件对延迟的影响最大，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中最严重的受害者、欺凌者或鲨鱼工作负载的延迟历史记录。
- 工作负载活动 - 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。
- 资源活动 - 显示争用中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，将显示其他图表。

其他事件提供了系统对存储对象执行的分析类型的简要描述。在某些情况下，会有一行或多行；对于分析多个性能计数器的系统定义性能策略，每个已分析的组件对应一行。在这种情况下，诊断旁边将显示一个绿色或红色图标，以指示在该特定诊断中是否发现了问题。

了解 **Active IQ Unified Manager** 中的事件设置页面

"Event Setup"页面显示已禁用的事件列表，并提供关联对象类型和事件严重性等信息。您也可以执行全局禁用或启用事件等任务。

仅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

命令按钮可用于为所选事件执行以下任务：

- 禁用

  启动“禁用事件”对话框，您可以使用它来禁用事件。

- 启用

  启用之前选择禁用的选定事件。

- 上传规则

  启动“上传规则”对话框，使没有外部网络访问权限的站点能够手动将 Active IQ 规则文件上传到 Unified Manager。这些规则根据群集 AutoSupport 消息运行，以生成 Active IQ 平台定义的系统配置、布线、最佳实践和可用性的事件。

- 订阅 **EMS** 事件

  启动 Subscribe to EMS Events（订阅 EMS 事件）对话框，使您能够订阅从正在监视的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。当收到已订阅 EMS 事件的通知时，将生成具有适当严重程度的 Unified Manager 事件。

列表视图

列表视图以表格格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

  显示已禁用事件的名称。

- 严重程度

  显示事件的严重程度。严重程度可以是严重、错误、警告或信息。

- 源类型

  显示为其生成事件的源类型。

禁用 **Active IQ Unified Manager** 中的**"**事件**"**对话框

“禁用事件”对话框显示可以禁用事件的事件类型列表。您可以根据特定严重程度或针对一组事件禁用事件类型的事件。

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：

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”、“警告”或“信息”。

- 事件名称包含

  使您能够筛选名称包含指定字符的事件。

- 匹配事件

  显示与事件严重性类型和您指定的文本字符串匹配的事件列表。

- 禁用事件

  显示选定要禁用的事件列表。

  还会显示事件的严重性以及事件名称。

命令按钮

通过命令按钮，可以为选定事件执行以下任务：

- 保存并关闭

  禁用此事件类型并关闭此对话框。

- 取消

  放弃更改并关闭对话框。

管理提醒

了解 **Active IQ Unified Manager** 中的警报

虽然事件不断发生，但 Unified Manager 仅在事件满足指定的过滤条件时才会生成警报。您可以选择应为其生成警报的事件，例如，当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。

Active IQ Unified Manager 警报电子邮件中包含的信息

Unified Manager 警报电子邮件提供事件的类型、事件的严重性、被违反并导致事件的策略或阈值的名称以及事件的描述。电子邮件消息还为每个事件提供了一个超链接，使您能够在 UI 中查看该事件的详细信息页面。

警报电子邮件将发送给已订阅接收警报的所有用户。

如果性能计数器或容量值在收集期间发生较大变化，则可能会导致同一阈值策略同时触发严重事件和警告事件。在这种情况下，您可能会收到一封关于警告事件的电子邮件和一封关于严重事件的电子邮件。这是因为 Unified Manager 允许您单独订阅以接收警告和严重阈值违规的警报。

警报电子邮件示例如下所示：

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

在 **Active IQ Unified Manager** 中添加警报

您可以配置警报，以便在生成特定事件时通知您。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。您可以指定要收到通知的频率，并将脚本关联到警报。

开始之前

- 您必须配置通知设置（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。
- 您必须知道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，则必须使用“脚本”页面将脚本添加到 Unified Manager。
- 您必须具有应用程序管理员或存储管理员角色。

除了从“警报设置”页面创建警报之外，您还可以在收到事件后直接从“事件详细信息”页面创建警报，如此处所述。

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*，并输入警报的名称和描述。
4. 单击*资源*，然后选择要包含在此警报中或从此警报中排除的资源。

   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。根据指定的文本字符串，可用资源列表仅显示与筛选规则匹配的资源。指定的文本字符串区分大小写。

   如果资源同时符合已指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除资源相关的事件生成警报。

5. 单击*事件*，并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，请在进行选择时按 Ctrl 键。

6. 单击 操作，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器，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”字段将显示为空白，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，如果从“用户”页面修改了所选用户的电子邮件地址，则不会为所选用户更新已修改的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 **Save**。

添加警报的示例

此示例演示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，不包括名称包含“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”、“Test”脚本，并且必须每 15 分钟通知一次用户

请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*，然后在包含选项卡中，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. 从可用资源区域中选择 **<<All Volumes whose name contains 'abc'>>**，并将其移动到选定资源区域。
   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 **All Critical Events**，然后将其移动到"已选择事件"区域。
5. 单击*操作*，然后在提醒这些用户字段中输入*`sample@domain.com`*。
6. 选择*每 15 分钟提醒一次*，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重复向收件人发送通知。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 **Test** 脚本。
8. 单击 **Save**。

在 **Active IQ Unified Manager** 中添加警报的准则

您可以根据资源（如群集、节点、聚合或卷）以及特定严重性类型的事件添加警报。作为最佳做法，您可以在添加对象所属的群集后，为任何关键对象添加警报。

您可以使用以下指南和注意事项来创建警报，以有效地管理您的系统：

- 警报说明

  您应提供警报的描述，以帮助您有效跟踪警报。

- 资源

  您应该决定哪个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视聚合，则必须从资源列表中选择所需的聚合。

  如果您选择一个资源类别，例如 **<<All User or Group Quotas>>**，则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，如果您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。您不会收到有关节点、聚合等严重事件的警报。

- 事件严重性

您应该决定指定严重程度类型（严重、错误、警告）的事件是否应触发警报，如果是，则决定哪种严重程度类型。

- 选定事件

  如果根据生成的事件类型添加警报，则应决定哪些事件需要警报。

  如果您选择事件严重程度，但未选择任何单个事件（如果将“所选事件”列留空），则您将收到该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相关联，以便在生成警报时执行。

- 通知频率

  您可以将警报配置为在指定时间内重复向收件人发送通知。您应该确定警报的事件通知处于活动状态的时间。如果要在事件被确认之前重复事件通知，则应确定重复通知的频率。

- 执行脚本

  您可以将脚本与警报相关联。生成警报时会执行脚本。

在 **Active IQ Unified Manager** 中添加性能事件警报

您可以为单个性能事件配置警报，就像 Unified Manager 接收的任何其他事件一样。此外，如果您希望以相同方式处理所有性能事件，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通知您。

开始之前

您必须具有应用程序管理员或存储管理员角色。

下面的示例演示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和所有警告事件中选择事件。

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*，并输入警报的名称和描述。
4. 请勿在*资源*页面上选择任何资源。

   由于未选择任何资源，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. 在事件严重程度列表中，选择*严重*。
   b. 在事件名称包含字段中，输入*`latency`*，然后单击箭头以选择所有匹配的事件。
   c. 在事件名称包含字段中，输入 **`iops`**，然后单击箭头以选择所有匹配的事件。

d. 在事件名称包含字段中，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*字段中选择将接收警报电子邮件的用户的名称。
7. 配置此页面上用于发出 SNMP 陷阱和执行脚本的任何其他选项。
8. 单击 **Save**。

在 **Active IQ Unified Manager** 中测试警报

您可以测试警报以验证其配置是否正确。触发事件时，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来验证通知是否已发送以及脚本是否已执行。

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*。

   测试警报电子邮件将发送到您在创建警报时指定的电子邮件地址。

在 **Active IQ Unified Manager** 中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，当这些事件通过所有可用状态（新建、已解决和已过时）转换时，将发送警报消息。如果不希望在事件进入"已解决"和"已过时"状态时接收事件警报，则可以配置全局设置以抑制这些警报。

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，事件进入“已解决”和“已废弃”状态时不会发送警报。

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，使用项目*已解决和已废弃事件的警报*旁边的滑块控件执行以下操作之一：

目的	操作
在事件已解决或已过时时停止发送警报	将滑块控件向左移动
在事件已解决或已过时时开始发送警报	将滑块控件向右移动

在 **Active IQ Unified Manager** 中排除灾难恢复目标卷以避免生成警报

配置卷警报时，您可以在“警报”对话框中指定一个字符串来标识一个卷或一组卷。但是，如果您已为 SVM 配置了灾难恢复，则源卷和目标卷具有相同的名称，因此您将收到两个卷的警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

可以通过排除具有目标 SVM 名称的卷来禁用灾难恢复目标卷的警报。这是可行的，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>”。

以下示例显示如何在主 SVM “vs1” 上为卷 “vol1” 创建警报，但排除在 SVM “vs1-dr” 上的同名卷上生成警报。

请在添加警报对话框中执行以下步骤：

步骤

1. 单击*名称*并输入警报的名称和描述。
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. 从*可用资源*区域选择 **<<All Volumes whose name contains 'vol1'>>**，并将其移动到*选定资源*区域。
3. 选择 **Exclude** 选项卡，选择 **Volume**，在 **Name contains** 字段中输入 **`vs1-dr`**，然后单击 **Add**。

   这排除了在 SVM "vs1-dr" 上为卷 "vol1" 生成的警报。
4. 单击*事件*并选择要应用于卷的事件。
5. 单击*操作*，然后在*提醒这些用户*字段中选择将接收警报电子邮件的用户的名称。
6. 配置此页面上用于发出 SNMP 陷阱和执行脚本的任何其他选项，然后单击 保存。

在 **Active IQ Unified Manager** 中查看警报

您可以从“警报设置”页面查看为各种事件创建的警报列表。还可以查看警报属性，例如警报描述、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。

   警报列表显示在“警报设置”页面中。

在 **Active IQ Unified Manager** 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，根据需要编辑名称、资源、事件和操作部分。

   您可以更改或删除与此警报关联的脚本。

4. 单击 **Save**。

删除 **Active IQ Unified Manager** 中的警报

您可以在不再需要时删除警报。例如，当特定资源不再受 Unified Manager 监控时，您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说明

了解 **Active IQ Unified Manager** 中的"警报设置"页面

警报设置页面显示警报列表，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

  显示用于添加新警报的“添加警报”对话框。

- 编辑

显示编辑警报对话框，用于编辑选定的警报。

- 删除

  删除选定的警报。

- 启用

  启用选定警报以发送通知。

- 禁用

  当您想要暂时停止发送通知时，禁用选定的警报。

- 测试

  测试选定警报，以在添加或编辑后验证其配置。

- 针对已解决和已废弃的事件发出的警报

  允许您在事件移动到“已解决”或“已过时”状态时启用或禁用发送警报。这可以帮助用户避免收到不必要的通知。

列表视图

列表视图以表格格式显示有关创建的警报的信息。您可以使用列筛选器自定义显示的数据。您还可以选择一个警报，以便在详细信息区域中查看有关该警报的更多信息。

- 状态

  指定警报是启用（）还是禁用（）。

- 警报

  显示警报的名称。

- 说明

  显示警报的说明。

- 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

  指定管理服务器继续发送通知的频率（分钟），直到事件被确认、解决或移至“已过时”状态。

详细信息区域

详细信息区域提供有关所选警报的更多信息。

- 警报名称

显示警报的名称。

- 警报说明

  显示警报的说明。

- 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

  显示要为其触发警报的资源组。

- 不包括

  显示不希望触发警报的资源组。

- 通知方法

  显示该警报的通知方法。

- 通知频率

  显示管理服务器继续发送警报通知的频率，直到事件被确认、解决或移至“已过时”状态。

- 脚本名称

  显示与所选警报关联的脚本的名称。生成警报时执行此脚本。

- 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。

了解 **Active IQ Unified Manager** 中的**"**添加警报**"**对话框

您可以创建警报以在生成特定事件时通知您，以便快速解决问题，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。

名称

通过此区域，您可以指定警报的名称和描述：

- 警报名称

使您可以指定警报名称。

- 警报说明

  使您能够指定警报的描述。

资源

此区域允许您选择单个资源，或根据要为其触发警报的动态规则对资源进行分组。_动态规则_是根据您指定的文本字符串筛选出的一组资源。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以显示特定资源。

如果从任何存储对象详细信息页面创建警报，则存储对象将自动包含在警报中。

- 包括

  使您能够包含要为其触发警报的资源。您可以指定文本字符串来对与该字符串匹配的资源进行分组，并选择将此组包含在警报中。例如，您可以对名称包含“abc”字符串的所有卷进行分组。

- 排除

  使您能够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。

  仅当您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，并且不会为该事件生成警报。

事件

此区域可让您选择要为其创建警报的事件。您可以根据特定严重程度为事件创建警报，也可以为一组事件创建警报。

要选择多个事件，请在进行选择时按住 Ctrl 键。

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”或“警告”。

- 事件名称包含

  使您能够选择名称包含指定字符的事件。

操作

通过此区域，您可以指定触发警报时要通知的用户。您还可以指定通知方法和通知频率。

- 提醒这些用户

  允许您指定要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”字段将显示为空白，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，如果已从“用户”页面修改所选用户的电子邮件地址，则不

会为所选用户更新已修改的电子邮件地址。

- 通知频率

  使您能够指定管理服务器在事件被确认、解决或移至过时状态之前发送通知的频率。

  您可以选择以下通知方法：

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

- 发出 **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

  使您能够将自定义脚本添加到警报。此脚本在生成警报时执行。

> 如果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，您可以从*存储管理* > *功能设置*启用此功能。

命令按钮

- 保存

  创建警报并关闭此对话框。

- 取消

  放弃更改并关闭对话框。

在 **Active IQ Unified Manager** 中编辑警报属性

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。

名称

通过此区域，您可以编辑警报的名称和描述。

- 警报名称

  使您可以编辑警报名称。

- 警报说明

  使您能够指定警报的描述。

- 警报状态

用于启用或禁用警报。

资源

此区域允许您选择单个资源，或根据要触发警报的动态规则对资源进行分组。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以显示特定资源。

- 包括

  使您能够包含要为其触发警报的资源。您可以指定文本字符串来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

  使您能够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。

  仅当您选择特定资源类型的所有资源（例如，<<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>）时，“排除”选项卡才会显示。

事件

此区域可让您选择要触发警报的事件。您可以根据特定严重程度或针对一组事件触发事件警报。

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”或“警告”。

- 事件名称包含

  使您能够选择名称包含指定字符的事件。

操作

通过此区域，您可以指定通知方法和通知频率。

- 提醒这些用户

  使您能够编辑电子邮件地址或用户名，或指定新电子邮件地址或用户名以接收通知。

- 通知频率

  使您能够编辑管理服务器发送通知的频率，直到事件被确认、解决或移至过时状态。

  您可以选择以下通知方法：

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

- 发出 **SNMP** 陷阱

  使您能够指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- 执行脚本

  使您能够将脚本与警报相关联。此脚本在生成警报时执行。

命令按钮

- 保存

  保存更改并关闭对话框。

- 取消

  放弃更改并关闭对话框。

管理脚本

在 **Active IQ Unified Manager** 中管理脚本

您可以使用脚本自动修改或更新 Unified Manager 中的多个存储对象。该脚本与警报相关联。当事件触发警报时，将执行脚本。您可以在生成警报时上传自定义脚本并测试其执行情况。

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能处于启用状态。如果您的组织出于安全原因不想允许此功能，您可以从*存储管理* > *功能设置*禁用此功能。

相关信息

"启用和禁用上传脚本的功能"

脚本如何与 **Active IQ Unified Manager** 中的警报配合使用

您可以将警报与脚本关联，以便在 Unified Manager 中引发事件警报时执行脚本。您可以使用脚本来解决存储对象的问题或识别哪些存储对象正在生成事件。

在 Unified Manager 中为事件生成警报时，将向指定收件人发送警报电子邮件。如果您将警报与脚本相关联，则会执行脚本。您可以从警报电子邮件中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相关联，则将根据该事件类型的自定义脚本采取操作，默认情况下，“管理操作”页面或 Unified Manager 仪表板上的“修复它”操作不可用。

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。

从脚本中获取参数的示例

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

生成警报时，系统将执行此脚本并显示以下输出：

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

在 **Active IQ Unified Manager** 中添加脚本

您可以在 Unified Manager 中添加脚本，并将脚本与警报相关联。这些脚本在生成警报时自动执行，使您能够获得有关为其生成事件的存储对象的信息。

开始之前

- 必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 支持的脚本文件格式有 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，脚本将仅支持 Perl 5 支持的内容。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，以便能够执行这些脚本。

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

- 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，您可以从*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*以选择您的脚本文件。
4. 输入选定脚本的说明。
5. 单击 **Add**。

相关信息

"启用和禁用上传脚本的功能"

删除 **Active IQ Unified Manager** 中的脚本

当脚本不再需要或有效时，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。
- 此脚本不得与警报相关联。

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。

在 **Active IQ Unified Manager** 中执行测试脚本

您可以验证在针对存储对象生成警报后是否正确执行了您的脚本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已将支持的文件格式的脚本上载到 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，添加您的测试脚本。
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：

目的	操作
添加警报	a. 单击 **Add**。 b. 在操作部分，将警报与测试脚本相关联。
编辑警报	a. 选择一个警报，然后单击*编辑*。 b. 在操作部分，将警报与测试脚本相关联。

5. 单击 **Save**。
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。

了解受支持的 **Active IQ Unified Manager CLI** 命令

作为存储管理员，您可以使用 CLI 命令对存储对象执行查询，例如对群集、聚合、卷、qtree 和 LUN 执行查询。您可以使用 CLI 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在触发警报时执行的脚本中使用 CLI 命令。

所有命令前面都必须加上命令 `um cli login`以及用于身份验证的有效用户名和密码。

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	问题描述	输出
`um cli login -u <username> [-p <password>]`	登录 CLI。出于安全考虑，您应该只在“-u”选项后输入用户名。以这种方式使用时，系统将提示您输入密码，并且密码不会被捕获到历史记录或进程表中。会话在登录三小时后过期，之后用户必须重新登录。	显示相应的消息。
`um cli logout`	从 CLI 注销。	显示相应的消息。
`um help`	显示所有一级子命令。	显示所有一级子命令。
`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。主要用于警报脚本，以在 ONTAP 上获取或执行操作。可选的 timeout 参数设置命令在客户端上完成的最大时间限制（以秒为单位）。默认值为 0（永久等待）。	从 ONTAP 接收到的。
`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错误请求，则会显示相应的错误消息。

CLI 命令	问题描述	输出
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	将数据源添加到托管存储系统列表。数据源描述了如何建立与存储系统的连接。添加数据源时，必须指定选项 -u（用户名）和 -P（密码）。选项 -t（协议）指定用于与集群通信的协议（http 或 https）。如果未指定协议，则将尝试两种协议。选项 -p（端口）指定用于与集群通信的端口。如果未指定端口，则将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打印相应的消息。
`um datasource list [ <datasource-id>]`	显示托管存储系统的数据源。	以表格格式显示以下值： `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。
`um option list [ <option> .. ]`	列出可使用 set 命令配置的所有选项。	以表格格式显示以下值： `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。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")`

CLI 命令	问题描述	输出
`um lun list [-q] [ -ObjectType <object-id>]`	列出筛选指定对象后的 LUN。-q 适用于所有命令，以不显示标头。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。该命令列出了 ID 为 1 的集群中的所有 LUN。	以表格格式显示以下值： `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	列出对指定对象进行筛选后的存储虚拟机。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。该命令列出集群内 ID 为 1 的所有存储 VM。	以表格格式显示以下值： `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	列出筛选指定对象后的 qtree。-q 适用于所有不显示标头的命令。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。该命令列出了 ID 为 1 的集群中的所有 qtree。	以表格格式显示以下值： `Qtree ID and Qtree Name.`

CLI 命令	问题描述	输出
`um disk list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的磁盘。ObjectType 可以是磁盘、聚合、节点或集群。 例如： **`um disk list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出了 ID 为 1 的集群中的所有磁盘。	以表格格式显示以下值 `ObjectType and object-id`。
`um cluster list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的集群。ObjectType 可以是 disk、aggr、node、cluster、lun、qtree、volume、quota 或 svm。 例如： **`um cluster list -aggr 1`** 在此示例中，“-aggr”是 objectType，“1”是 objectId。该命令列出了 ID 为 1 的聚合所属的集群。	以表格格式显示以下值： `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`。
`um cluster node list [-q] [-ObjectType <object-id>]`	在按指定对象筛选后列出集群节点。ObjectType 可以是 disk、aggr、node 或 cluster。 例如： **`um cluster node list -cluster 1`** 在此示例中，“-cluster” 为 objectType，“1” 为 objectId。该命令列出了 ID 为 1 的集群内的所有节点。	以表格格式显示以下值 `Name and Cluster ID`。
`um volume list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的卷。ObjectType 可以是 lun、qtree、cluster、volume、quota、svm 或 aggregate。 例如： **`um volume list -cluster 1`** 在此示例中，“-cluster”是 objectType，“1”是 objectId。该命令列出了 ID 为 1 的集群内的所有卷。	以表格格式显示以下值 `Volume ID and Volume Name`。

CLI 命令	问题描述	输出
`um quota user list [-q] [-ObjectType <object-id>]`	列出筛选指定对象后的配额用户。ObjectType 可以是 qtree、cluster、volume、quota 或 svm。 例如： **`um quota user list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出集群内 ID 为 1 的所有配额用户。	以表格格式显示以下值 `ID, Name, SID and Email`。
`um aggr list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的聚合。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。该命令列出了 ID 为 1 的集群内的所有聚合。	以表格格式显示以下值 `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。	以表格格式显示以下值 `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。

脚本窗口和对话框的说明

了解 **Active IQ Unified Manager** 中的脚本页面

您可以使用“脚本”页面将自定义脚本添加到 Unified Manager。您可以将这些脚本与警报相关联，以启用存储对象的自动重新配置。

您可以使用“脚本”页面在 Unified Manager 中添加或删除脚本。

命令按钮

- 添加

  显示用于添加脚本的“添加脚本”对话框。

- 删除

  删除选定脚本。

列表视图

列表视图以表格格式显示您添加到 Unified Manager 的脚本。

- 名称

  显示脚本的名称。

- 说明

  显示脚本说明。

在 **Active IQ Unified Manager** 中添加脚本对话框

“添加脚本”对话框使您可以将脚本添加到 Unified Manager。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

  使您能够为警报选择脚本。

- 说明

  使您能够指定脚本的说明。

版权信息

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

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。