



管理事件

Active IQ Unified Manager

NetApp
March 26, 2025

目录

| | |
|--------------------------------|----|
| 管理事件 | 1 |
| 什么是运行状况事件 | 1 |
| 什么是性能事件 | 1 |
| 性能事件的来源 | 1 |
| 系统定义的性能阈值策略的类型 | 2 |
| 什么是 Active IQ 平台事件 | 4 |
| 什么是事件管理系统事件 | 4 |
| 自动添加到 Unified Manager 的 EMS 事件 | 5 |
| 收到事件时会发生什么情况 | 9 |
| 配置事件通知设置 | 10 |
| 开始之前 | 10 |
| 步骤 | 11 |
| 查看事件和事件详细信息 | 11 |
| 开始之前 | 11 |
| 关于此任务 | 11 |
| 步骤 | 11 |
| 查看未分配的事件 | 12 |
| 开始之前 | 12 |
| 步骤 | 12 |
| 确认并解决事件 | 12 |
| 开始之前 | 12 |
| 关于此任务 | 12 |
| 步骤 | 12 |
| 将事件分配给特定用户 | 13 |
| 开始之前 | 13 |
| 步骤 | 13 |
| 禁用不需要的事件 | 14 |
| 开始之前 | 14 |
| 关于此任务 | 14 |
| 步骤 | 14 |
| 使用 Unified Manager 自动修复解决问题 | 15 |
| 关于此任务 | 15 |
| 步骤 | 15 |
| 启用和禁用 Active IQ 事件报告 | 16 |
| 开始之前 | 16 |
| 关于此任务 | 16 |
| 步骤 | 16 |
| 上传新的 Active IQ 规则文件 | 16 |
| 开始之前 | 16 |

| | |
|--------------------------|----|
| 关于此任务 | 16 |
| 步骤 | 17 |
| 结果 | 17 |
| 如何生成 Active IQ 平台事件 | 17 |
| 解决 Active IQ 平台事件 | 17 |
| 订阅 ONTAP EMS 事件 | 18 |
| 开始之前 | 18 |
| 关于此任务 | 18 |
| 步骤 | 19 |
| 完成后 | 19 |
| 配置事件保留设置 | 19 |
| 开始之前 | 19 |
| 关于此任务 | 19 |
| 步骤 | 20 |
| 什么是 Unified Manager 维护窗口 | 20 |
| 计划维护窗口以禁用集群事件通知 | 20 |
| 更改或取消计划的维护窗口 | 21 |
| 查看维护窗口期间发生的事件 | 21 |
| 管理主机系统资源事件 | 22 |
| 关于此任务 | 22 |
| 步骤 | 22 |
| 了解有关事件的更多信息 | 22 |
| 事件状态定义 | 23 |
| 事件严重性类型的问题描述 | 23 |
| 事件影响级别的问题描述 | 24 |
| 事件影响区域的问题描述 | 24 |
| 如何计算对象状态 | 25 |
| 动态性能事件图表详细信息 | 25 |
| Unified Manager 检测到配置更改 | 26 |
| 事件和严重性类型的列表 | 27 |
| 聚合事件 | 27 |
| 集群事件 | 31 |
| 磁盘事件 | 35 |
| 机箱事件 | 36 |
| 风扇事件 | 37 |
| 闪存卡事件 | 37 |
| 索引节点事件 | 38 |
| 逻辑接口(LIF)事件 | 38 |
| LUN 事件 | 39 |
| 管理工作站事件 | 43 |
| MetroCluster 网桥事件 | 44 |

| | |
|--------------------|----|
| MetroCluster 连接事件 | 45 |
| MetroCluster 交换机事件 | 47 |
| NVMe 命名空间事件 | 48 |
| 节点事件 | 49 |
| NVRAM 电池事件 | 53 |
| 端口事件 | 54 |
| 电源事件 | 55 |
| 保护事件 | 55 |
| qtree 事件 | 56 |
| 服务处理器事件 | 56 |
| SnapMirror 关系事件 | 57 |
| SnapMirror和存储关系事件 | 58 |
| Snapshot 事件 | 59 |
| SnapVault 关系事件 | 59 |
| 存储故障转移设置事件 | 60 |
| 存储服务事件 | 61 |
| 存储架事件 | 62 |
| SVM事件 | 62 |
| SVM存储类事件 | 66 |
| 用户和组配额事件 | 67 |
| 卷事件 | 68 |
| 卷移动状态事件 | 74 |
| 事件窗口和对话框的问题描述 | 75 |
| 通知页面 | 75 |
| 事件管理清单页面 | 77 |
| 事件详细信息页面 | 80 |
| 事件设置页面 | 85 |
| 禁用事件对话框 | 86 |

管理事件

事件可帮助您确定受监控集群中的问题。

什么是运行状况事件

运行状况事件是指在发生预定义情况或对象超过运行状况阈值时自动生成的通知。通过这些事件、您可以采取措施、防止出现可能导致性能低下和系统不可用的问题。事件包括影响区域、严重性和影响级别。

运行状况事件按可用性、容量、配置或保护等影响区域类型进行分类。此外、还会为事件分配严重性类型和影响级别、以帮助确定是否需要立即采取操作。

您可以将警报配置为在发生特定事件或特定严重性的事件时自动发送通知。

系统会自动记录废弃、已解决和信息性事件、并将其保留默认值180天。

对于严重性级别为“错误”或“严重”的事件、请务必立即采取更正操作。

什么是性能事件

性能事件是指与集群上的工作负载性能相关的事件。它们可以帮助您确定响应时间较长的工作负载。与同时发生的运行状况事件一起，您可以确定可能导致或导致响应时间较慢的问题。

如果 Unified Manager 检测到同一集群组件多次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。

性能事件的来源

性能事件是指与集群上的工作负载性能相关的问题。它们可以帮助您识别响应时间较长的存储对象，也称为高延迟。与同时发生的其他运行状况事件一起，您可以确定可能导致或导致响应时间较慢的问题。

Unified Manager 从以下源接收性能事件：

- * 用户定义的性能阈值策略事件 *

根据您设置的自定义阈值确定的性能问题。您可以为存储对象（例如聚合和卷）配置性能阈值策略，以便在违反性能计数器的阈值时生成事件。

您必须定义性能阈值策略并将其分配给存储对象以接收这些事件。

- * 系统定义的性能阈值策略事件 *

基于系统定义的阈值的性能问题。这些阈值策略包含在 Unified Manager 安装中，用于解决常见的性能问题。

默认情况下，这些阈值策略处于启用状态，您可能会在添加集群后不久看到相关事件。

- * 动态性能阈值事件 *

因 IT 基础架构故障或错误或工作负载过度利用集群资源而导致的性能问题。这些事件的发生原因可能是一个简单的问题描述，可以在一段时间内自行更正，也可以通过修复或更改配置来解决。动态阈值事件表示由于其他工作负载大量使用共享集群组件，ONTAP 系统上的工作负载速度较慢。

默认情况下，这些阈值处于启用状态，从新集群收集数据三天后，您可能会看到事件。

系统定义的性能阈值策略的类型

Unified Manager 提供了一些标准阈值策略，用于监控集群性能并自动生成事件。默认情况下，这些策略处于启用状态，如果违反监控的性能阈值，它们将生成警告或信息事件。



Cloud Volumes ONTAP，ONTAP Edge 或 ONTAP Select 系统上未启用系统定义的性能阈值策略。

如果您从任何系统定义的性能阈值策略收到不必要的事件，则可以从事件设置页面禁用各个策略的事件。

集群阈值策略

默认情况下，系统定义的集群性能阈值策略会分配给 Unified Manager 监控的每个集群：

- 集群不平衡阈值

确定一个节点的运行负载远高于集群中其他节点，从而可能影响工作负载延迟的情况。

为此，它会比较集群中所有节点的已用性能容量值，以确定任何节点之间是否存在 30% 的负载差异。这是一个警告事件。

节点阈值策略

默认情况下，系统定义的节点性能阈值策略会分配给 Unified Manager 所监控集群中的每个节点：

- 节点资源已过度利用

确定单个节点运行超过其运行效率上限从而可能影响工作负载延迟的情况。

为此，它会查找使用 100% 以上性能容量且持续 12 小时以上的节点。这是一个警告事件。

- * 节点 HA 对已过度利用 *

确定 HA 对中的节点在超出 HA 对操作效率限制的情况。

为此，它会查看 HA 对中两个节点的已用性能容量值。如果这两个节点的总已用性能容量超过 200% 且持续 12 小时以上，则控制器故障转移将影响工作负载延迟。这是一个信息性事件。

- * 节点磁盘碎片化 *

确定聚合中的一个或多个磁盘碎片化，从而降低关键系统服务的速度并可能影响节点上的工作负载延迟的情

况。

为此，它会查看节点上所有聚合的特定读写操作比率。在 SyncMirror 重新同步期间或在磁盘擦除操作期间发现错误时，也可能会触发此策略。这是一个警告事件。



"节点磁盘碎片" 策略仅分析纯 HDD 聚合；不分析 Flash Pool，SSD 和 FabricPool 聚合。

聚合阈值策略

默认情况下，系统定义的聚合性能阈值策略会分配给 Unified Manager 所监控集群中的每个聚合：

• * 聚合磁盘过度利用 *

确定聚合运行超过其运行效率限制从而可能影响工作负载延迟的情况。它通过查找聚合中磁盘利用率超过 95% 且持续 30 分钟以上的聚合来确定这些情况。然后，此多条件策略将执行以下分析，以帮助确定问题描述的发生原因：

- 聚合中的磁盘当前是否正在进行后台维护活动？

磁盘可能正在进行的一些后台维护活动包括磁盘重建，磁盘擦除，SyncMirror 重新同步和重新解析。

- 磁盘架光纤通道互连是否存在通信瓶颈？
- 聚合中的可用空间是否太少？只有当三个从属策略中的一个（或多个）也被视为违反时，才会为此策略发出警告事件。如果只有聚合中的磁盘利用率超过 95%，则不会触发性能事件。



"聚合磁盘过度利用" 策略可分析纯 HDD 聚合和 Flash Pool（混合）聚合；不会分析 SSD 和 FabricPool 聚合。

工作负载延迟阈值策略

系统定义的工作负载延迟阈值策略将分配给已配置性能服务级别策略且定义了 "expected latency" 值的任何工作负载：

• 已违反性能服务级别 * 定义的 * 工作负载卷 /LUN 延迟阈值

确定已超过 "预期延迟" 限制且影响工作负载性能的卷（文件共享）和 LUN。这是一个警告事件。

为此，它会查找前一小时 30% 时间内超过预期延迟值的工作负载。

QoS 阈值策略

系统定义的 QoS 性能阈值策略将分配给已配置 ONTAP QoS 最大吞吐量策略（IOPS，IOPS/TB 或 MB/秒）的任何工作负载。当工作负载吞吐量值比配置的 QoS 值低 15% 时，Unified Manager 将触发事件：

• * QoS 最大 IOPS 或 MB/秒阈值 *

确定已超过其 QoS 最大 IOPS 或 MB/秒吞吐量限制且影响工作负载延迟的卷和 LUN。这是一个警告事件。

将单个工作负载分配给策略组后，它会查找在前一小时的每个收集期间内超过分配的 QoS 策略组中定义的最大吞吐量阈值的工作负载。

如果多个工作负载共享一个 QoS 策略，则可以通过在策略中添加所有工作负载的 IOPS 或 MB/ 秒并根据阈值检查该总数来实现此目的。

- 具有块大小阈值的 * QoS 峰值 IOPS/TB 或 IOPS/TB *

确定已超过自适应 QoS 峰值 IOPS/TB 吞吐量限制（或具有块大小限制的 IOPS/TB）且正在影响工作负载延迟的卷。这是一个警告事件。

为此，它会根据每个卷的大小将自适应 QoS 策略中定义的峰值 IOPS/TB 阈值转换为 QoS 最大 IOPS 值，然后查找在上一小时的每个性能收集期间超过 QoS 最大 IOPS 的卷。



只有当集群安装了 ONTAP 9.3 及更高版本的软件时，此策略才会应用于卷。

在自适应 QoS 策略中定义 "block size" 元素后，此阈值将根据每个卷的大小转换为 QoS 最大 MB/ 秒值。然后，它会查找在上一小时的每个性能收集期间超过 QoS 最大 MB/ 秒的卷。



只有当集群安装了 ONTAP 9.5 及更高版本的软件时，此策略才会应用于卷。

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。

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。

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 |
| 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"Error EMS received"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"信息性事件表示"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 | waf.ca.resync.complete | 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 |
|-------------------------------------|----------------------------------|--------|---------------------|
| FabricPool 空间接近全满 | fabricpool.nNearly.full | 集群 | error |
| 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 LIF 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 |

| Unified Manager 事件名称 | EMS 事件名称 | 受影响的资源 | Unified Manager 严重性 |
|----------------------|-----------------------------------|---------------|---------------------|
| QoS 监控内存已达到上限 | qos.monitor.memory.maxed | Node | error |
| 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.cifsMaxSessPerUserConn | 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.vscanVirusDetected. | SVM | error |

| Unified Manager 事件名称 | EMS 事件名称 | 受影响的资源 | Unified Manager 严重性 |
|-------------------------|---|--------|---------------------|
| 没有用于病毒扫描的 AV 服务器连接 | nblade.vscanNoScannerConn | SVM | 严重 |
| 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 | wافل.vol.autoSize.fail | Volume | error |
| WAFL 卷自动调整大小已完成 | wافل.vol.autoSize.done | Volume | 信息 |
| WAFL READDIR 文件操作超时 | wافل.readdir.expired. | Volume | error |

收到事件时会发生什么情况

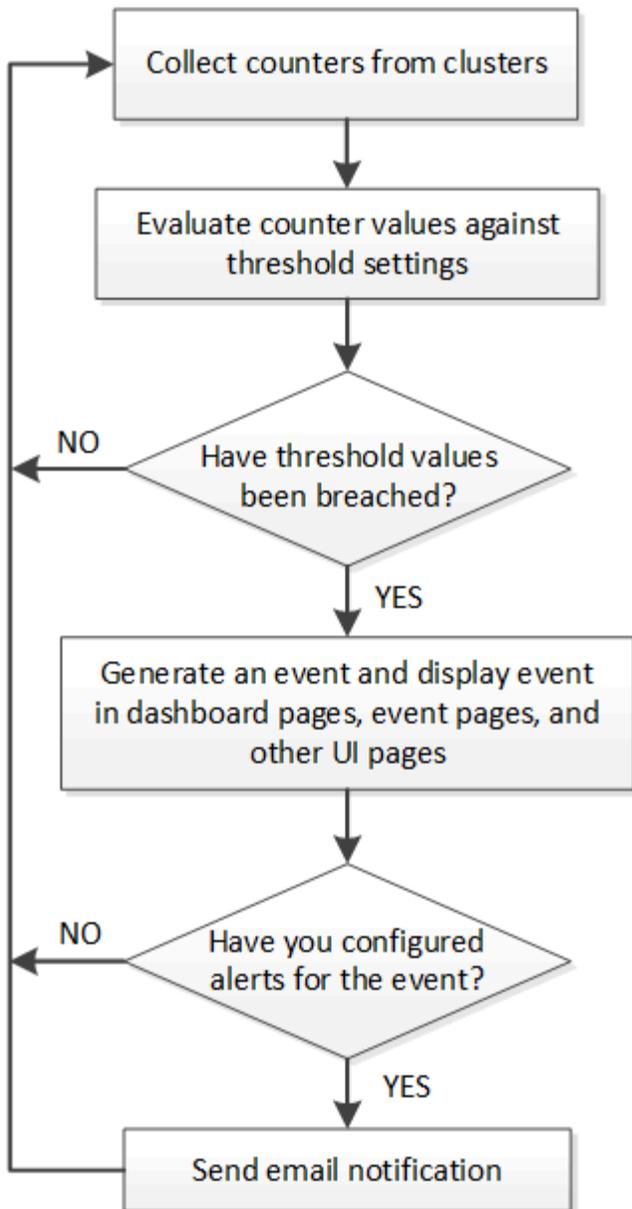
Unified Manager 收到事件后，该事件将显示在 " 信息板 " 页面， " 事件管理 " 清单页面， " 集群 / 性能 " 页面的 " 摘要 " 和 " 资源管理器 " 选项卡以及对象特定的清单页面（例如 " 卷 / 运行状况 " 清单页面）中。

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。



配置事件通知设置

您可以将 Unified Manager 配置为在生成事件或将事件分配给用户时发送警报通知。您可以配置用于发送警报的 SMTP 服务器，也可以设置各种通知机制，例如，警报通知可以通过电子邮件或 SNMP 陷阱发送。

开始之前

您必须具有以下信息：

- 发送警报通知的电子邮件地址

电子邮件地址将显示在已发送警报通知的 "from" 字段中。如果由于任何原因无法传送此电子邮件，则此电子邮件地址也会用作无法传送的邮件的收件人。

- 用于访问服务器的 SMTP 服务器主机名以及用户名和密码
- 要接收 SNMP 陷阱的陷阱目标主机的主机名或 IP 地址，以及 SNMP 版本，出站陷阱端口，社区和其他所需的 SNMP 配置值

要指定多个陷阱目标，请使用逗号分隔每个主机。在这种情况下，列表中所有主机的所有其他 SNMP 设置（例如版本和出站陷阱端口）都必须相同。

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * 通知 *。
2. 在 * 通知 * 页面中、配置相应的设置并单击 * 保存 *。



****If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.**

**** If the host name of the SMTP server cannot be resolved, you can specify the IP address (IPv4 or IPv6) of the SMTP server instead of the host name.**

查看事件和事件详细信息

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。

关于此任务

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。

关于此任务

您可以同时确认和解决多个事件。



您无法确认信息事件。

步骤

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

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

- 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 | <p>a. 单击 * 分配给 * > * 其他用户 *。</p> <p>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。</p> <p>c. 单击 * 分配 *。</p> <p>系统会向用户发送电子邮件通知。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  如果未输入用户名或从下拉列表中选择用户，然后单击 * 分配 *，则事件将保持未分配状态。 </div> |

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。

关于此任务

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

禁用对象的事件时(例如、vol offline 事件)、然后在启用此事件后、Unified Manager不会为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 | <ol style="list-style-type: none"> 单击 * 禁用 *。 在禁用事件对话框中，选择事件严重性。 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。 单击 * 保存并关闭 *。 验证已禁用的事件是否显示在 Event Setup 页面的列表视图中。 |
| 启用事件 | <ol style="list-style-type: none"> 选中要启用的一个或多个事件对应的复选框。 单击 * 启用 *。 |

使用 Unified Manager 自动修复解决问题

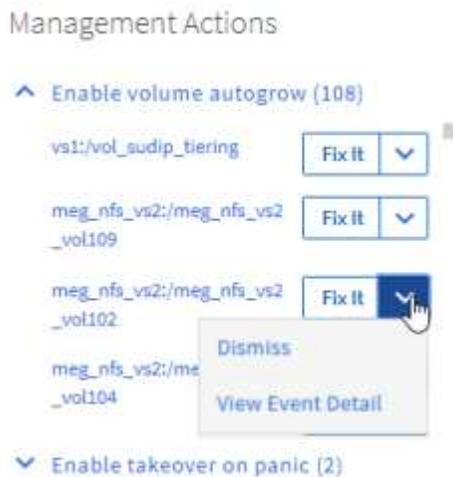
Unified Manager 可以对某些事件进行全面诊断并提供单一解决方案。如果可用，这些解决方案将显示在信息板，事件详细信息页面以及左侧导航菜单上的工作负载分析选项中。

关于此任务

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。

步骤

- 要查看可通过 * 信息板 * 修复的事件，请单击 * 信息板 *。



- 要解决 Unified Manager 可以修复的任何问题，请单击 * 修复它 * 按钮。

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。如果您发现这些事件太“很吵”、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。

关于此任务

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 会自动检查新的 Active IQ 规则文件，并在存在较新规则时下载新文件。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。

开始之前

- 必须启用 Active IQ 事件报告。
- 您必须从 NetApp 支持站点下载规则文件。

关于此任务

建议您大约每月下载一次新的规则文件，以确保存储系统受到保护并以最佳方式运行。规则文件位于：
http://mysupport.netapp.com/NOW/public/unified_manager/bin/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
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、导航到并选择规则 .zip 下载的文件、然后单击*上传*。

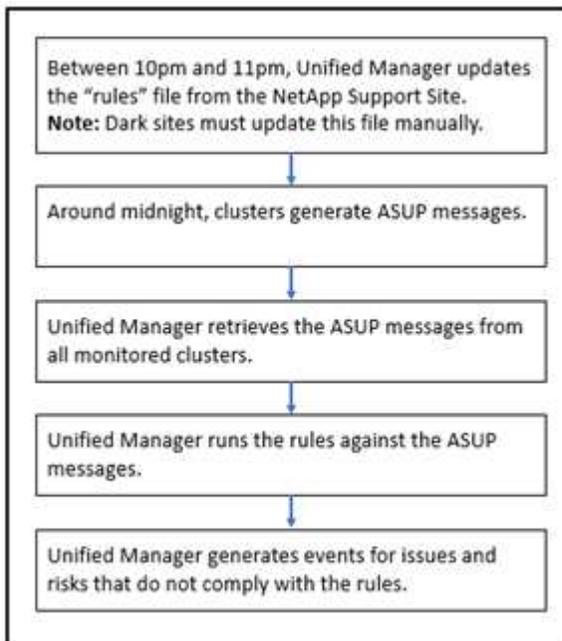
此过程可能需要几分钟时间。

结果

规则文件将在 Unified Manager 服务器上解压缩。在受管集群午夜后生成 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。

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。

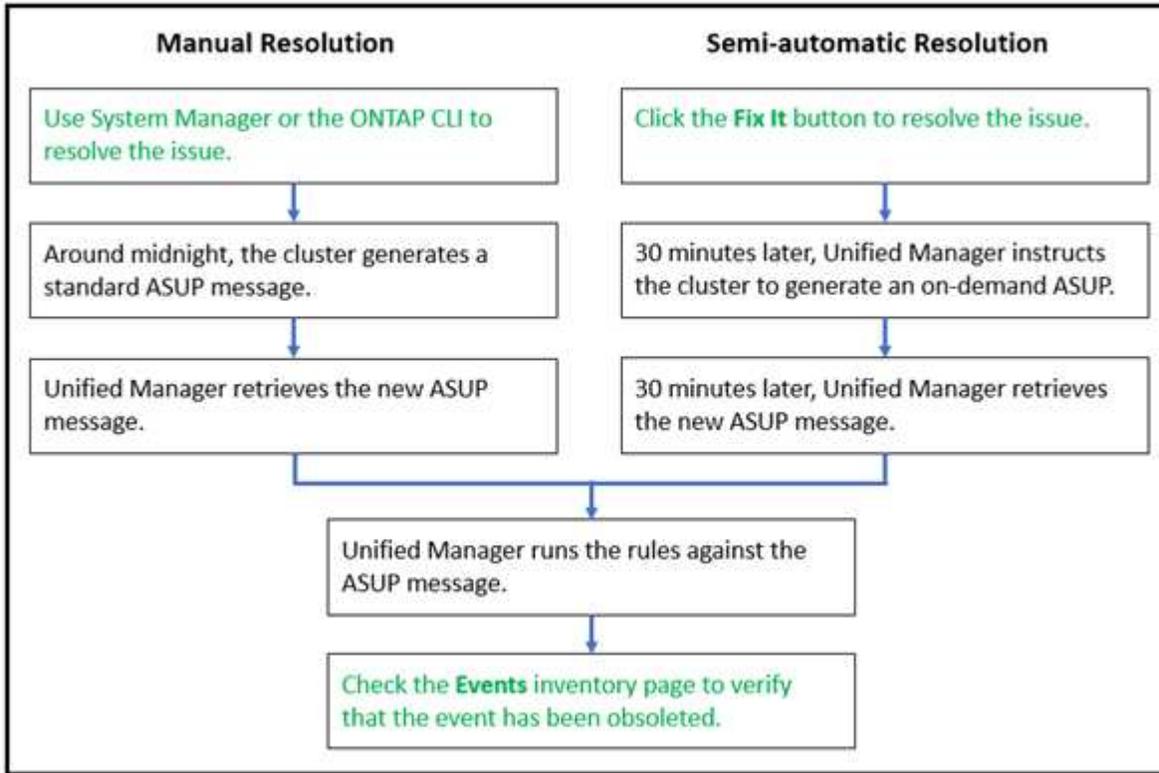


如您所见，在 Active IQ 平台上编译的规则文件将保持最新，并且每天都会生成集群 AutoSupport 消息，并且 Unified Manager 会每天更新事件列表。

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。

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。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。

关于此任务

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*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)。有关识别各个EMS事件的详细说明、请参见知识库问题解答 1072320。

"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。

完成后

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。

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。

关于此任务

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，"Object Maintenance window started"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。

计划维护窗口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。

关于此任务

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`Scheduled`。

结果

达到开始时间后、集群将进入维护模式、并生成"Object Maintenance window started"事件。

更改或取消计划的维护窗口

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。

关于此任务

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 | <ol style="list-style-type: none">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长度 | <ol style="list-style-type: none">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。 |

查看维护窗口期间发生的事件

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。

关于此任务

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。

关于此任务

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 | <ol style="list-style-type: none">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。 |

了解有关事件的更多信息

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" 。

动态性能事件图表详细信息

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。此部分的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），上次分析的时间将继续更新。

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。请参见 [Unified Manager监控的工作负载](#)。



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 ["什么是事件"](#)。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"](#)。



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 |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|--|------|-----|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|-----|----------|
| 聚合空间已满 (ocumEvtAggregateFull) | 风险 | 聚合 | error |
| 聚合达到全满前的天数 (ocumEvtAggregateDaysUntilFullSoon) | 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 (ocumEvtAggregateSnapshotReserveFull) | 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 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 (ocumEvtMccAutomaticUnplannedSwitchOverDisabled) | 风险 | 集群 | 警告 |

影响区域：容量

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|-----|----------|
| 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 * (wafCaResyncComplete) | 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|----------------|------|-----|----------|
| 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 |
| 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 |

| Unified Manager 事件严重性级别 | ONTAP EMS 事件严重性级别 |
|-------------------------|--------------------------------|
| 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 |
| 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 |
| 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 |

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（ ocumEvtClusterFlashDisk FewerSpareBlockError） | 风险 | 集群 | error |
| 闪存磁盘 - 无备用块（ ocumEvtClusterFlashDisk NoSpareBlockCritical） | 意外事件 | 集群 | 严重 |
| 某些未分配磁盘（ ocumEvtClusterUnasiged DiskSome） | 风险 | 集群 | 警告 |
| 某些故障磁盘（ ocumEvtDisksSomeFailed） | 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的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： <ul style="list-style-type: none"> • 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 |

逻辑接口(LIF)事件

LIF事件可提供有关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 |
|---|------|-----|----------|
| LIF状态为已关闭(ocumEvtLifeStatusDown) | 风险 | 接口 | error |
| 无法执行LIF故障转移(ocumEvtLifeFailoverNotPossible) | 风险 | 接口 | 警告 |
| LIF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LIF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FCP接口MB/秒严重阈值(ocumFcpLifeMbpsIncident) | 意外事件 | 接口 | 严重 |
| 已违反FCP接口MB/秒警告阈值(ocumFcpLifeMbpsWarning) | 风险 | 接口 | 警告 |
| 已违反NVMf FCP接口MB/秒严重阈值(ocumNvmfclifMbpsIncident) | 意外事件 | 接口 | 严重 |
| 已违反NVMf FCP接口MB/秒警告阈值(ocumNvmfclifMbpsWarning) | 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* | 事件 | LUN | 信息 |
| 已在igroup中使用不受支持的操作系统映射LUN | 意外事件 | LUN | 警告 |
| 访问 LUN 的单个活动路径 (ocumEvtLunSingleActive Path) | 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 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 |
| 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 | severity |
|---|------|-----|----------|
| 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 | 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 |
|--|------|-------|----------|
| Unified Manager服务器磁盘空间接近全满(ocumEvtUnifiedManagerDiskSpaceNearlyFull) | 风险 | 管理工作站 | 警告 |
| Unified Manager服务器磁盘空间已满(ocumEvtUnifiedManagerDiskSpaceFull) | 意外事件 | 管理工作站 | 严重 |
| Unified Manager服务器内存不足(ocumEvtUnifiedManagerMemoryLow) | 风险 | 管理工作站 | 警告 |
| Unified Manager服务器内存几乎用尽(ocumEvtUnifiedManagerMemoryAlmostOut) | 意外事件 | 管理工作站 | 严重 |

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 (ocumEvtUnifiedManagerDataMissingCollection) | 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 网桥事件为您提供有关网桥状态的信息，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 |
|---|------|-----------------|----------|
| 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 MetroCluster 配置中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。

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 (ocumEvtMetroClusterAllSwitchesDown) | 意外事件 | MetroCluster 交换机间连接 | 严重 |
| 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 |
| 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 |
| MetroCluster 配置已切换(ocumEvtMetroClusterDRStatusImpacted) | 风险 | MetroCluster 关系 | 警告 |
| MetroCluster 配置已部分切换 (ocumEvtMetroClusterDRStatusPartiallyImpacted) | 风险 | MetroCluster 关系 | error |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|-----------------------|----------|
| 受影响的 MetroCluster 灾难恢复功能 (ocumEvtMetroClusterDR StatusImpacted) | 风险 | MetroCluster 关系 | 严重 |
| 无法通过对等网络访问 MetroCluster 合作伙伴 (ocumEvtMetroClusterPart nersNotReachebleOverPe eringNetwork) | 意外事件 | MetroCluster 关系 | 严重 |
| 节点到 FC 交换机的所有 FC-VI 互连链路已关闭 (ocumEvtMccNodeSwitchF cviLinksDown) | 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 (ocumEvtMccNodeSwitchF cLinksOneOrMoreDown) | 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 (ocumEvtMccNodeSwitchF cLinksDown) | 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 (ocumEvtMccSwitchBridge FcLinksDown) | 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 (ocumEvtMccInterNodeLin ksDown) | 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 (ocumEvtMccInterNodeLin ksOneOrMoreDown) | 风险 | 节点间连接 | 警告 |
| 节点到网桥的链路关闭 (ocumEvtMccNodeBridgeL inksDown) | 意外事件 | 节点网桥连接 | 严重 |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|--|------|--------|----------|
| 节点到存储堆栈的所有 SAS 链路已关闭（ocumEvtMccNodeStackLinksDown） | 意外事件 | 节点堆栈连接 | 严重 |
| 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 |

MetroCluster 交换机事件

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 |
| 交换机电源出现故障（ocumEvtSwitchPowerSuppliesOneOrMoreFailed） | 意外事件 | MetroCluster 交换机 | 严重 |
| 交换机温度传感器出现故障（ocumEvtSwitchTemperatureSensorFailed） | 意外事件 | MetroCluster 交换机 | 严重 |
|  此事件仅适用于 Cisco 交换机。 | | | |

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 *（ nvmeNamespaceStatusOf fline） | 事件 | 命名空间 | 信息 |
| NVMeNS Online *（ nvmeNamespaceStatusO nline） | 事件 | 命名空间 | 信息 |
| NVMeNS 空间不足 *（ nvmeNamespaceSpaceO utOfSpace） | 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（ ocumNvmeNamespacelo psIncident） | 意外事件 | 命名空间 | 严重 |
| 已违反 NVMe 命名空间 IOPS 警告阈值（ ocumNvmeNamespacelo psWarning） | 风险 | 命名空间 | 警告 |
| 已违反 NVMe 命名空间 MB/ 秒严重阈值（ ocumNvmeNamespaceM bpsIncident） | 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 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（ocumNvmeNamespaceLatencyMbpsIncident） | 意外事件 | 命名空间 | 严重 |
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|------|----------|
| 云层集群间 LIF 已关闭 * (ocumObjstoreInterCluster LifeDown) | 风险 | Node | error |
| 其中一个NFSv4池已耗尽* | 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 * (ocumQosMonitorMemory Maxed) | 风险 | Node | error |
| QoS 监控内存已减少 * (ocumQosMonitorMemory Abated) | 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 (ocumNodelopsIncident) | 意外事件 | Node | 严重 |
| 已违反节点 IOPS 警告阈值 (ocumNodelopsWarning) | 风险 | Node | 警告 |
| 已违反节点 MB/ 秒严重阈值 (ocumNodeMbpsIncident) | 意外事件 | Node | 严重 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|------|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|------|----------|
| 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 |
| 已违反节点过度利用阈值(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 |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|--|------|------|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|------|----------|
| 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 |
| 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。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。

| 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 |
| 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 |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|---|------|---------------|----------|
| 镜像复制重新同步失败（ ocumEvtSnapmirrorRelationshipResyncFailed） | 风险 | SnapMirror 关系 | error |
| 同步复制不同步* | 风险 | SnapMirror 关系 | 警告 |
| 同步复制已还原* | 事件 | SnapMirror 关系 | 信息 |
| 同步复制自动重新同步失败* | 风险 | SnapMirror 关系 | error |

SnapMirror和存储关系事件

SnapMirror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。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 |
| 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（ ocumEvtMirrorVaultRelationshipLagshipError） | 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 |

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 |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|---|------|---------------|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|------|----------|
| 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 (ocumEvtShelfCurrentAbnormal) | 风险 | 存储架 | 警告 |
| 温度异常 (ocumEvtShelfTemperatureAbnormal) | 风险 | 存储架 | 警告 |

SVM事件

SVM事件为您提供有关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。

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 |
|---|------|-----|----------|
| SVM 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* | 意外事件 | SVM | 严重 |
| CIFS NetBIOS名称冲突* | 风险 | SVM | error |
| CIFS卷影复制操作失败* | 风险 | SVM | error |
| 多个CIFS连接* | 风险 | SVM | error |
| 已超过最大CIFS连接数* | 风险 | SVM | error |
| 已超过每个用户的最大CIFS连接数* | 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 |
| SVM NFS 服务已关闭（ ocumEvtVserverNfsServiceStatusDown） | 意外事件 | SVM | 严重 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----------|----------|
| SVM 已停止 (ocumEvtVserverDown) | 风险 | SVM | 警告 |
| AV服务器太忙、无法接受新扫描请求* | 风险 | SVM | error |
| 没有用于病毒扫描的AV服务器连接* | 意外事件 | SVM | 严重 |
| 未注册AV服务器* | 风险 | SVM | error |
| 无响应AV服务器连接* | 事件 | SVM | 信息 |
| 未经授权的用户尝试访问AV服务器* | 风险 | SVM | error |
| AV服务器发现病毒* | 风险 | SVM | error |
| 带有无限卷的SVM存储不可用(ocumEvtVserverStorageNotAvailable) | 意外事件 | 带有无限卷的SVM | 严重 |
| 带有无限卷的SVM存储部分可用(ocumEvtVserverStoragePartiallyAvailable) | 风险 | 带有无限卷的SVM | error |
| 带有无限卷的SVM命名空间镜像成分卷存在可用性问题(ocumEvtVserverNsMirrorAvailabilityHavingIssues) | 风险 | 带有无限卷的SVM | 警告 |

影响区域：容量

以下容量事件仅适用于带有无限卷的SVM。

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|-----------------------------------|------|-----|----------|
| 带有无限卷的SVM空间已满(ocumEvtVserverFull) | 风险 | SVM | error |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 带有无限卷的SVM空间接近全满(ocumEvtVserverNearlyFull) | 风险 | SVM | 警告 |
| 已超过带有无限卷的SVM Snapshot使用量限制(ocumEvtVserverSnapshotUsageExceeded) | 风险 | SVM | 警告 |
| 带有无限卷的SVM命名空间空间已满(ocumEvtVserverNameSpaceFull) | 风险 | SVM | error |
| 带有无限卷的SVM命名空间接近全满(ocumEvtVserverNameSpaceNearlyFull) | 风险 | SVM | 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 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 | 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| 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 (ocumVserverLoginBanner Disabled) | 风险 | SVM | 警告 |
| SSH正在使用不安全的密 码(ocumVserverSSHInsec ure) | 风险 | SVM | 警告 |

SVM存储类事件

SVM存储类事件可为您提供有关存储类状态的信息、以便您可以监控潜在问题。SVM存储类仅存在于带有无限卷的SVM中。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。

以下SVM存储类事件仅适用于带有无限卷的SVM。

影响区域：可用性

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|-----|----------|
| SVM存储类不可用(ocumEvtVserverStorageClassNot Available) | 意外事件 | 存储类 | 严重 |
| SVM存储类部分可用(ocumEvtVserverStorageClassPartiallyAvailable) | 风险 | 存储类 | error |

影响区域：容量

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|-----|----------|
| SVM存储类空间接近全满(ocumEvtVserverStorageClassNearlyFull) | 风险 | 存储类 | 警告 |
| SVM存储类空间已满(ocumEvtVserverStorageClassFull) | 风险 | 存储类 | error |
| 已超过SVM存储类Snapshot使用量限制(ocumEvtVserverStorageClassSnapshotUsageExceeded) | 风险 | 存储类 | 警告 |

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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|---|------|--------|----------|
| 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 |
| 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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|--------|----------|
| 卷接合路径处于非活动状态 (ocumEvtVolumeJunctionPathInactive) | 风险 | Volume | 警告 |
| 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* (flexGroupConstituentsHaveSpacelssues) | 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 * (flexGroupConstituents SpaceStatusAllOK) | 事件 | Volume | 信息 |
| FlexGroup 成分卷存在索引节点问题 * (flexGroupConstituents HaveInodesIssues) | 风险 | Volume | error |
| FlexGroup 成分卷索引节点状态一切正常 * (flexGroupConstituents InodesStatusAllOK) | 事件 | Volume | 信息 |
| WAFL 卷自动调整大小失败* | 风险 | Volume | error |
| WAFL 卷自动调整大小已完成* | 事件 | Volume | 信息 |

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 (ocumQosVolumeMaxIops Warning) | 风险 | Volume | 警告 |
| 已违反 QoS 卷最大 MB/秒警告阈值 (ocumQosVolumeMaxMbpsWarning) | 风险 | Volume | 警告 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|--------|----------|
| 已违反 QoS 卷最大 IOPS/TB 警告阈值 (ocumQosVolumeMaxIops PerTbWarning) | 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 | 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 |
| 已违反卷 MB/ 秒警告阈值 (ocumVolumeMbpsWarning) | 风险 | Volume | 警告 |
| 已违反卷延迟毫秒 / 操作严重阈值 (ocumVolumeLatencyIncident) | 意外事件 | Volume | 严重 |
| 已违反卷延迟毫秒 / 操作警告阈值 (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 |

| 事件名称 (陷阱名称) | 影响级别 | 源类型 | severity |
|--|------|--------|----------|
| 已违反卷缓存未命中率警告阈值 (ocumVolumeCachedMisS RatioWarning) | 风险 | Volume | 警告 |
| 已违反卷延迟和 IOPS 严重阈值 (ocumVolumeLatencylopsl ncident) | 意外事件 | Volume | 严重 |
| 已违反卷延迟和 IOPS 警告阈值 (ocumVolumeLatencylops Warning) | 风险 | Volume | 警告 |
| 已违反卷延迟和 MB/ 秒严重阈值 (ocumVolumeLateLatency MbpsIncident) | 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 |
| 已违反卷延迟和聚合已用性能容量严重阈值 (ocumVolumeLatencyAggregatePerfCapacityUsedIn cident) | 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 (ocumVolumeLatencyAggregatePerfCapacityUsedW arning) | 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 |

| 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 |
| 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 |

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 |
| 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"Version"和"Outbound Port"。

- * 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。

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。

- 导出

用于将所有事件的详细信息导出为逗号分隔值 (.csv) 文件。

- * 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 (ℹ️)。

- * 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 SVM, 卷或 qtree)。

- * 已分配给 *

将事件分配到的用户的名称。

- * 事件源 *

事件是源自 "Active IQ 门户" 还是直接源自 "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。

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

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

命令按钮

命令按钮可用于执行以下任务：

- * 注释图标 *

用于添加或更新有关事件的注释，并查看其他用户留下的所有注释。

- * 操作菜单 *

- * 分配给我 *

将事件分配给您。

- * 分配给他人 *

打开分配所有者对话框，在此可以将事件分配或重新分配给其他用户。

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

您也可以通过将所有权字段留空来取消分配事件。

- * 确认 *

确认选定事件，以使您不再收到重复的警报通知。

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

- * 标记为已解决 *

用于将事件状态更改为已解决。

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

- * 添加警报 *

显示添加警报对话框，在此可以为选定事件添加警报。

Event Information 部分显示的内容

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

不适用于事件类型的字段将被隐藏。您可以查看以下事件详细信息：

- * 事件触发时间 *

生成事件的时间。

- * 状态 *

事件状态："新增"，"已确认"，"已解决"或"已废弃"。

- * 已废弃发生原因 *

导致事件废弃的操作，例如，问题描述已修复。

- * 事件持续时间 *

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

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

- * 上次查看 *

上次将事件视为活动的日期和时间。

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

- * 严重性 *

事件严重性：严重 (❌)，错误 (❗)，警告 (⚠️) 和信息 (ℹ️)。

- * 影响级别 *

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

- * 影响区域 *

事件影响区域：可用性，容量，性能，保护，配置，或安全性。

- * 源 *

发生事件的对象的名称。

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

您可以单击源名称链接以显示该对象的运行状况或性能详细信息页面。

- * 源标注 *

显示与事件关联的对象的标注名称和值。

只有集群，SVM 和卷上的运行状况事件才会显示此字段。

- * 源组 *

显示受影响对象所属的所有组的名称。

只有集群，SVM 和卷上的运行状况事件才会显示此字段。

- * 源类型 *

与事件关联的对象类型（例如 SVM，卷或 qtree）。

- * 在集群 * 上

发生事件的集群的名称。

您可以单击集群名称链接以显示该集群的运行状况或性能详细信息页面。

- * 受影响对象计数 *

受事件影响的对象数。

您可以单击对象链接以显示填充了当前受此事件影响的对象的清单页面。

只有性能事件才会显示此字段。

- * 受影响的卷 *

受此事件影响的卷数。

只有节点或聚合上的性能事件才会显示此字段。

- * 触发的策略 *

发出事件的阈值策略的名称。

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

只有性能事件才会显示此字段。

- * 规则 ID *

对于 Active IQ 平台事件，这是为生成事件而触发的规则的编号。

- * 确认者 *

确认事件的人员姓名以及事件的确认时间。

- * 解决者 *

解决事件的人员姓名以及事件的解决时间。

- * 已分配给 *

被分配处理事件的人员的姓名。

- * 警报设置 *

此时将显示以下有关警报的信息：

- 如果没有与选定事件关联的警报，则会显示 * 添加警报 * 链接。

您可以通过单击链接打开添加警报对话框。

- 如果有一个与选定事件关联的警报，则会显示警报名称。

您可以通过单击链接打开 " 编辑警报 " 对话框。

- 如果与选定事件关联的警报不止一个，则会显示警报数量。

您可以通过单击链接打开警报设置页面，以查看有关这些警报的更多详细信息。

不会显示已禁用的警报。

- * 上次发送通知 *

发送最新警报通知的日期和时间。

- * 发送者 *

用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- * 上一个脚本运行 *

生成警报时执行的脚本的名称。

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。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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