分析性能事件

Active IQ Unified Manager

NetApp
November 13, 2026

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

目录

分析性能事件 . . . 1
- 分析 Active IQ Unified Manager 中的性能事件 . . . 1
- 在 Active IQ Unified Manager 中显示性能事件信息 . . . 1
- 分析用户定义的性能阈值事件 . . . 1
  - 分析 Active IQ Unified Manager 中用户定义的性能阈值产生的事件 . . . 2
  - 在 Active IQ Unified Manager 中响应用户定义的性能阈值事件 . . . 2
- 分析系统定义的性能阈值事件 . . . 2
  - 分析 Active IQ Unified Manager 中系统定义的性能阈值事件 . . . 2
  - 响应 Active IQ Unified Manager 中系统定义的性能阈值事件 . . . 3
  - 响应 Active IQ Unified Manager 中的 QoS 策略组性能事件 . . . 3
  - 了解 Active IQ Unified Manager 中具有已定义块大小的自适应 QoS 事件 . . . 4
  - 响应 Active IQ Unified Manager 中的节点资源过度利用事件 . . . 5
  - 响应 Active IQ Unified Manager 中的集群不平衡性能事件 . . . 6
- 分析动态性能阈值事件 . . . 7
  - 分析 Active IQ Unified Manager 中动态性能阈值的事件 . . . 7
  - 在 Active IQ Unified Manager 中识别动态性能事件中的受害工作负载 . . . 7
  - 在 Active IQ Unified Manager 中识别动态性能事件中的欺凌工作负载 . . . 8
  - 在 Active IQ Unified Manager 中识别动态性能事件中的鲨鱼工作负载 . . . 8
  - MetroCluster 配置的性能事件分析 . . . 8
  - 响应 Active IQ Unified Manager 中的动态 QoS 限速事件 . . . 11
  - 响应 Active IQ Unified Manager 中由磁盘故障引起的性能事件 . . . 12
  - 响应 Active IQ Unified Manager 中因 HA 接管引起的性能事件 . . . 13

分析性能事件

分析 **Active IQ Unified Manager** 中的性能事件

您可以分析性能事件以确定它们何时被检测到，它们是活动的（新的还是已确认的）还是过时的，涉及的工作负载和集群组件，以及用于自行解决事件的选项。

在 **Active IQ Unified Manager** 中显示性能事件信息

您可以使用事件管理清单页面查看由 Unified Manager 监控的集群上的所有性能事件列表。通过查看此信息，您可以确定最关键的事件，然后深入查看详细信息以确定事件的原因。

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。

事件列表按检测时间排序，最近的事件列在前面。您可以单击列标题，根据该列对事件进行排序。例如，您可以按“状态”列进行排序，以按严重程度查看事件。如果您正在查找特定事件或特定类型的事件，则可以使用筛选器和搜索机制来优化列表中显示的事件列表。

所有来源的事件都显示在此页面上：

- 用户定义的性能阈值策略
- 系统定义的性能阈值策略
- 动态性能阈值

“事件类型”列列出了事件的来源。您可以选择一个事件，在“事件详细信息”页面中查看有关该事件的详细信息。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 在“视图”菜单中，选择 活动性能事件。

   该页面显示过去 7 天内生成的所有“新建”和“已确认”性能事件。

3. 找到要分析的事件，然后单击该事件名称。

   此时将显示此事件的详细信息页面。

> 您也可以通过单击 Performance Explorer 页面中的事件名称链接或警报电子邮件中的链接来显示事件的详细信息页面。

分析用户定义的性能阈值事件

分析 **Active IQ Unified Manager** 中用户定义的性能阈值产生的事件

从用户定义的阈值生成的事件指示特定存储对象（例如聚合或卷）的性能计数器已超过您在策略中定义的阈值。这表示集群对象遇到性能问题。

您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

在 **Active IQ Unified Manager** 中响应用户定义的性能阈值事件

您可以使用 Unified Manager 调查由性能计数器超出用户定义的警告或严重阈值引起的性能事件。您还可以使用 Unified Manager 检查集群组件的运行状况，以查看在组件上检测到的近期运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的或过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Latency value of 456 ms/op has triggered a WARNING event based on threshold setting of 400 ms/op” 表示该对象发生了延迟警告事件。

3. 将光标悬停在策略名称上，以显示有关触发此事件的阈值策略的详细信息。

   这包括策略名称、正在评估的性能计数器、必须突破才能被视为严重或警告事件的计数器值，以及计数器必须超过该值的持续时间。

4. 记下*事件触发时间*，以便调查是否有其他事件在同一时间发生，从而可能对此事件产生影响。
5. 按照以下选项之一进一步调查事件，以确定是否需要执行任何操作来解决性能问题：

选项	可能的调查操作
单击源对象名称以显示该对象的“资源管理器”页面。	通过此页面，您可以查看对象详细信息，并将此对象与其他类似的存储对象进行比较，以查看其他存储对象是否大约在同一时间存在性能问题。例如，查看同一聚合中的其他卷是否也存在性能问题。
单击集群名称以显示“集群摘要”页面。	通过此页面，您可以查看此对象所在集群的详细信息，以了解大约在同一时间是否发生了其他性能问题。

分析系统定义的性能阈值事件

分析 **Active IQ Unified Manager** 中系统定义的性能阈值事件

系统定义的性能阈值生成的事件指示特定存储对象的性能计数器或性能计数器集已超过系统定义策略的阈值。这表示存储对象（例如聚合或节点）遇到性能问题。

您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系统上未启用系统定义的阈值策略。

响应 **Active IQ Unified Manager** 中系统定义的性能阈值事件

您可以使用 Unified Manager 调查性能计数器超出系统定义的警告阈值引起的性能事件。您还可以使用 Unified Manager 检查集群组件的运行状况，以查看在组件上检测到的最近事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的或过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Node utilization value of 90 % has triggered a WARNING event based on threshold setting of 85 %” 表示集群对象发生了节点利用率警告事件。

3. 记下*事件触发时间*，以便调查是否有其他事件在同一时间发生，从而可能对此事件产生影响。
4. 在*系统诊断*下，查看系统定义策略对集群对象执行的分析类型的简要说明。

   对于某些事件，诊断旁边会显示绿色或红色图标，以指示在该特定诊断中是否发现了问题。对于其他类型的系统定义事件，计数器图表显示对象的性能。

5. 在*建议操作*下，单击*帮助我执行此操作*链接以查看您可以执行的建议操作，尝试自行解决性能事件。

响应 **Active IQ Unified Manager** 中的 **QoS** 策略组性能事件

当工作负载吞吐量（IOPS、IOPS/TB或MBps）超过定义的ONTAP QoS策略设置且工作负载延迟受到影响时，Unified Manager会生成QoS策略警告事件。这些系统定义的事件提供了在许多工作负载受延迟影响之前纠正潜在性能问题的机会。

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。
- 必须存在新的、已确认的或已过时的性能事件。

当工作负载吞吐量在前一小时的每个性能收集期间超过定义的 QoS 策略设置时，Unified Manager 会生成 QoS 策略违规的警告事件。在每个收集期间，工作负载吞吐量可能仅在短时间内超过 QoS 阈值，但 Unified Manager 仅在图表上显示收集期间的“`average`”吞吐量。因此，即使工作负载的吞吐量可能未超过图表中显示的策略阈值，您也可能会收到 QoS 事件。

您可以使用 System Manager 或 ONTAP 命令来管理策略组，包括以下任务：

- 为工作负载创建新策略组

- 在策略组中添加或删除工作负载
- 在策略组之间移动工作负载
- 更改策略组的吞吐量限制
- 将工作负载移动到其他聚合或节点

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “vol1_NFS1 上的 IOPS 值为 1,352 IOPS 已触发 WARNING 事件以确定工作负载的潜在性能问题” 表示卷 vol1_NFS1 上发生了 QoS 最大 IOPS 事件。

3. 查看*事件信息*部分，了解有关事件发生时间以及事件处于活动状态多长时间的更多详细信息。

   此外，对于共享 QoS 策略吞吐量的卷或 LUN，您可以看到消耗最多 IOPS 或 MBps 的前三个工作负载的名称。

4. 在 系统诊断 部分下，查看两个图表：一个用于总平均 IOPS 或 MBps（取决于事件），另一个用于延迟。通过这种排列方式，您可以看到当工作负载接近 QoS 最大限制时，哪些集群组件对延迟的影响最大。

   对于共享 QoS 策略事件，吞吐量图表中会显示前三个工作负载。如果共享 QoS 策略的工作负载超过三个，则其他工作负载将汇总至"`Other workloads`"类别。此外，延迟图表会显示 QoS 策略中所有工作负载的平均延迟。

   请注意，对于自适应 QoS 策略事件，IOPS 和 MBps 图表显示 ONTAP 已根据卷大小从分配的 IOPS/TB 阈值策略转换的 IOPS 或 MBps 值。

5. 在*建议操作*部分下，查看建议并确定应执行哪些操作以避免工作负载的延迟增加。

   如果需要，请单击 帮助 按钮以查看有关您可以执行的建议操作的更多详细信息，以尝试解决性能事件。

了解 **Active IQ Unified Manager** 中具有已定义块大小的自适应 **QoS** 事件

自适应 QoS 策略组会根据卷大小自动缩放吞吐量上限或下限，并随着卷大小的变化保持 IOPS 与 TB 的比例。从 ONTAP 9.5 开始，您可以在 QoS 策略中指定块大小，以同时有效地应用 MB/s 阈值。

在自适应 QoS 策略中分配 IOPS 阈值仅对每个工作负载中发生的操作数量设置限制。根据在生成工作负载的客户端上设置的块大小，某些 IOPS 包含更多数据，因此会给处理操作的节点带来更大的负担。

使用以下公式生成工作负载的 MB/s 值：

```
MB/s = (IOPS * Block Size) / 1000
```

如果工作负载平均为 3,000 IOPS，并且客户端上的块大小设置为 32 KB，则此工作负载的有效 MB/s 为 96。如果相同的工作负载平均为 3,000 IOPS，并且客户端上的块大小设置为 48 KB，则此工作负载的有效 MB/s 为 144。可以看到，当块大小较大时，节点处理的数据量增加了 50%。

让我们看一下以下具有定义块大小的自适应 QoS 策略，以及如何根据客户端上设置的块大小触发事件。

创建策略并将峰值吞吐量设置为 2,500 IOPS/TB，块大小为 32KB。这有效地将已用容量为 1 TB 的卷的 MB/s 阈值设置为 80 MB/s（（2500 IOPS * 32KB）/ 1000）。请注意，当吞吐量值比定义的阈值低 10% 时，Unified Manager 会生成警告事件。事件在以下情况下生成：

已用容量	当吞吐量超过此数量时生成事件.....	
	IOPS	MB/秒
1 TB	2,250 IOPS	72 MB/s
2 TB	4,500 IOPS	144 MB/s
5 TB	11,250 IOPS	360 MB/s

如果卷使用 2TB 的可用空间，并且 IOPS 为 4,000，并且客户端上的 QoS 块大小设置为 32KB，则 MB/ps 吞吐量为 128 MB/s（（4,000 IOPS * 32 KB）/ 1000）。在此方案中不会生成任何事件，因为 4,000 IOPS 和 128 MB/s 均低于使用 2 TB 空间的卷的阈值。

如果卷正在使用可用空间中的 2TB，IOPS 为 4,000，且客户端上的 QoS 块大小设置为 64KB，则 MB/s 吞吐量为 256 MB/s （（4,000 IOPS * 64 KB）/ 1000）。在这种情况下，4,000 IOPS 不会生成事件，但 256 MB/s 的 MB/s 值超过了 144 MB/s 的阈值，因此会生成事件。

因此，当基于包含块大小的自适应 QoS 策略的 MB/s 违规触发事件时，“事件详细信息”页面的“系统诊断”部分中将显示 MB/s 图表。如果基于自适应 QoS 策略的 IOPS 违规触发事件，则在“系统诊断”部分显示 IOPS 图表。如果 IOPS 和 MB/s 都发生违规，您将收到两个事件。

有关调整 QoS 设置的更多信息，请参见 "性能管理概述"。

响应 **Active IQ Unified Manager** 中的节点资源过度利用事件

当单个节点运行超出其运行效率的界限，从而可能影响工作负载延迟时，Unified Manager 会生成节点资源过度使用的警告事件。这些系统定义的事件提供了在许多工作负载受到延迟影响之前纠正潜在性能问题的机会。

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。
- 必须有新的或过时的性能事件。

Unified Manager 通过查找使用超过 100% 性能容量超过 30 分钟的节点，为节点资源过度使用策略违规生成警告事件。

您可以使用 System Manager 或 ONTAP 命令来更正此类型的性能问题，包括以下任务：

- 创建 QoS 策略并将其应用于任何过度使用系统资源的卷或 LUN
- 降低已应用工作负载的策略组的 QoS 最大吞吐量限制
- 将工作负载移动到其他聚合或节点
- 通过向节点添加磁盘或升级为 CPU 更快且 RAM 更大的节点来提高容量

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Perf.simplicity-02 上的 Capacity Used 值为 139%，已触发 WARNING 事件以确定 Data Processing 单元中的潜在性能问题。” 表示节点 simplicity-02 上的性能容量被过度使用并影响节点性能。

3. 在*系统诊断*部分下，查看三个图表：一个用于节点上使用的性能容量，一个用于顶级工作负载使用的平均存储 IOPS，一个用于顶级工作负载上的延迟。以这种方式排列时，您可以查看哪些工作负载是节点上延迟的原因。

   您可以通过将光标移到 IOPS 图表上来查看哪些工作负载应用了 QoS 策略，哪些未应用 QoS 策略。

4. 在*建议操作*部分下，查看建议并确定应执行哪些操作以避免工作负载的延迟增加。

   如果需要，请单击 帮助 按钮以查看有关您可以执行的建议操作的更多详细信息，以尝试解决性能事件。

响应 **Active IQ Unified Manager** 中的集群不平衡性能事件

当群集中的一个节点以比其他节点高得多的负载运行时，Unified Manager 将生成群集不平衡警告事件，因此可能会影响工作负载延迟。这些系统定义的事件提供了在许多工作负载受到延迟影响之前纠正潜在性能问题的机会。

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。

Unified Manager 通过比较集群中所有节点的性能容量使用值，以查看任何节点之间是否存在 30% 的负载差异，从而为集群不平衡阈值策略违规生成警告事件。

这些步骤可帮助您确定以下资源，以便将高性能工作负载移动到利用率较低的节点：

- 同一集群上利用率较低的节点
- 新节点上利用率最低的聚合
- 当前节点上性能最高的卷

步骤

1. 显示*事件*详细信息页面以查看有关事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息“已用性能容量计数器表示集群 `Dallas-1-8` 中节点之间存在 `62%` 的负载差异，并已根据系统阈值 `30%` 触发警告事件”表示其中一个节点上的性能容量被过度使用并影响节点性能。

3. 查看 **Suggested Actions** 中的文本，以将高性能卷从性能容量使用值较高的节点移至性能容量使用值最低的节点。
4. 识别具有最高和最低性能容量使用值的节点：
   a. 在*事件信息*部分，单击源集群的名称。
   b. 在*集群/性能摘要*页面中，单击*托管对象*区域中的*节点*。
   c. 在*节点*清单页面中，按*已用性能容量*列对节点进行排序。

d. 确定性能容量使用值最高和最低的节点，并记录这些节点的名称。

5. 确定在具有最高性能容量使用值的节点上使用最多 IOPS 的卷：
   a. 单击具有最高性能容量使用值的节点。
   b. 在*节点/性能资源管理器*页面中，从*查看和比较*菜单中选择*此节点上的聚合*。
   c. 单击具有最高性能容量使用值的聚合。
   d. 在*聚合/性能资源管理器*页面中，从*查看和比较*菜单中选择*此聚合上的卷*。
   e. 按 **IOPS** 列对卷进行排序，并记下使用最多 IOPS 的卷的名称，以及该卷所在聚合的名称。
6. 识别性能容量使用值最低的节点上利用率最低的聚合：
   a. 单击*存储* > *聚合*以显示*聚合*清单页面。
   b. 选择*性能：所有聚合*视图。
   c. 单击 过滤器 按钮并添加一个过滤器，其中 “Node” 等于您在步骤 4 中记下的已用性能容量值最低的节点的名称。
   d. 写下性能容量使用值最低的聚合的名称。
7. 将卷从过载节点移动到您确定在新节点上利用率较低的聚合。

   您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，请检查您是否从此集群接收到相同的集群不平衡事件。

分析动态性能阈值事件

分析 **Active IQ Unified Manager** 中动态性能阈值的事件

由动态阈值生成的事件表明，与预期响应时间范围相比，工作负载的实际响应时间（延迟）过高或过低。您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

在 Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系统上未启用动态性能阈值。

在 **Active IQ Unified Manager** 中识别动态性能事件中的受害工作负载

在 Unified Manager 中，您可以识别哪些卷工作负载的响应时间（延迟）偏差最大，这是由争用中的存储组件引起的。识别这些工作负载有助于您了解为什么访问它们的客户端应用程序的执行速度比平时慢。

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。
- 必须有新的、已确认的或过时的动态性能事件。

“事件详细信息”页面显示用户定义和系统定义工作负载的列表，按组件上活动或使用情况的最大偏差或受事件影响最大进行排名。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Victim Workloads**。
3. 将光标悬停在图表上，以查看影响组件的主要用户定义工作负载以及受害者工作负载的名称。

在 **Active IQ Unified Manager** 中识别动态性能事件中的欺凌工作负载

在 Unified Manager 中，您可以识别哪些工作负载对处于争用状态的集群组件的使用量偏差最大。识别这些工作负载有助于您了解集群中某些卷的响应时间（延迟）较慢的原因。

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。
- 必须有新的、已确认的或过时的动态性能事件。

“事件详细信息”页面显示用户定义和系统定义的工作负载列表，这些工作负载按组件的最高使用率或受事件影响最大的程度进行排序。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示事件详细信息页面以查看有关事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Bully Workloads**。
3. 将光标悬停在图表上以查看影响组件的排名靠前的用户定义恶霸工作负载。

在 **Active IQ Unified Manager** 中识别动态性能事件中的鲨鱼工作负载

在 Unified Manager 中，您可以识别哪些工作负载在争用中的存储组件的使用率偏差最大。识别这些工作负载可帮助您确定是否应将这些工作负载迁移到利用率较低的集群。

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。
- 有新的、已确认的或过时的性能动态事件。

“事件详细信息”页面显示用户定义和系统定义的工作负载列表，这些工作负载按组件的最高使用率或受事件影响最大的程度进行排序。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Shark Workloads**。
3. 将光标悬停在图表上，以查看影响组件的顶级用户定义的工作负载以及 shark 工作负载的名称。

MetroCluster 配置的性能事件分析

使用 **Active IQ Unified Manager** 分析 **MetroCluster** 性能事件

您可以使用 Unified Manager 分析 MetroCluster 配置的性能事件。您可以识别此事件所涉

及的工作负载，并查看解决此问题的建议措施。

MetroCluster 性能事件可能是由于 *bully* workloads 过度使用群集之间的交换机间链路（ISL），或是由于链路运行状况问题。Unified Manager 独立监控 MetroCluster 配置中的每个群集，而不考虑伙伴群集上的性能事件。

MetroCluster 配置中两个集群的性能事件也会显示在 Unified Manager 仪表板页面上。您还可以查看 Unified Manager 的运行状况页面，以检查每个集群的运行状况并查看其关系。

在 **Active IQ Unified Manager** 中的集群上分析 **MetroCluster** 性能事件

您可以使用 Unified Manager 在检测到性能事件的 MetroCluster 配置中分析集群。您可以确定集群名称、事件检测时间以及所涉及的 *bully* 和 *victim* 工作负载。

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。
- MetroCluster 配置必须有新的、已确认的或过时的性能事件。
- MetroCluster 配置中的两个集群必须由同一个 Unified Manager 实例监控。

步骤

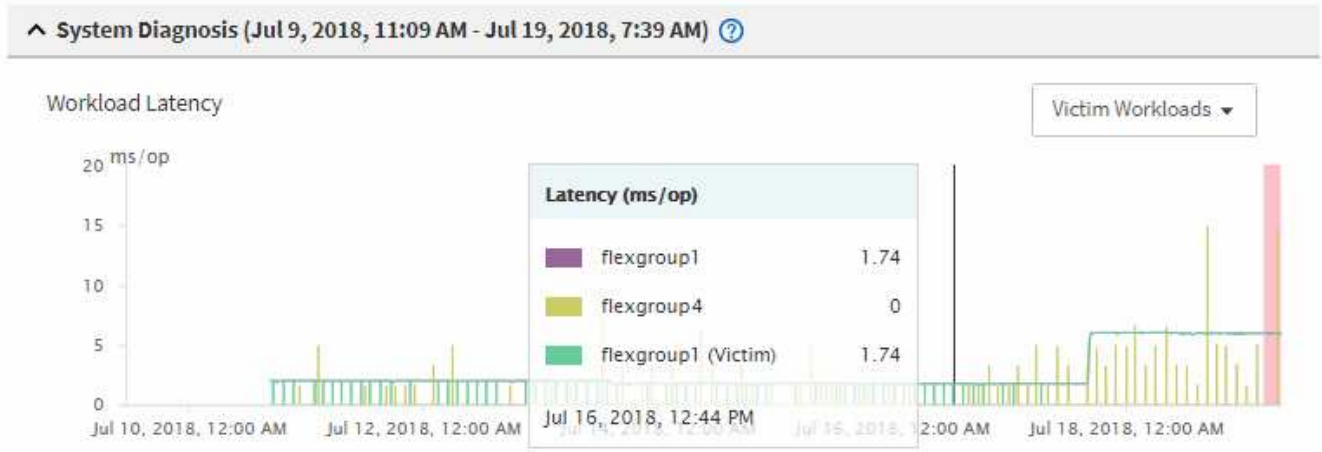
1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看事件描述，了解所涉及的工作负载名称以及所涉及的工作负载数量。

   在此示例中，“MetroCluster 资源”图标为红色，表示 MetroCluster 资源处于争用状态。将光标定位在图标上以显示图标的说明。



3. 记下集群名称和事件检测时间，您可以使用这些信息来分析配对集群上的性能事件。
4. 在图表中，查看 *victim* 工作负载，以确认其响应时间高于性能阈值。

   在此示例中，受害者工作负载显示在悬停文本中。延迟图表在较高层面上显示了所涉及的受害者工作负载的一致延迟模式。即使受害者工作负载的异常延迟触发了事件，一致的延迟模式也可能表明工作负载正在其预期范围内执行，但 I/O 峰值增加了延迟并触发了事件。



如果您最近在访问这些卷工作负载的客户端上安装了一个应用程序，并且该应用程序向它们发送了大量的 I/O，则您可能会预期它们的延迟会增加。如果工作负载的延迟返回到预期范围内，事件状态更改为已过时，并保持此状态超过 30 分钟，则您可能可以忽略该事件。如果事件正在进行中，并且仍处于新状态，则可以进一步进行调查，以确定是否有其他问题导致该事件。

5. 在工作负载吞吐量图表中，选择*恶霸工作负载*以显示恶霸工作负载。

   欺凌工作负载的存在表明，该事件可能是由本地集群上的一个或多个工作负载过度使用 MetroCluster 资源引起的。欺凌工作负载的写入吞吐量（MB/s）偏差较高。

   此图表在较高层级上显示了工作负载的写入吞吐量（MB/s）模式。您可以查看写入 MB/s 模式以识别异常吞吐量，这可能表明工作负载过度使用 MetroCluster 资源。

   如果事件中不涉及恶霸工作负载，则该事件可能是由于集群之间的链路存在运行状况问题或配对集群上的性能问题而引起的。您可以使用 Unified Manager 检查 MetroCluster 配置中两个集群的运行状况。您还可以使用 Unified Manager 检查和分析配对集群上的性能事件。

在 **Active IQ Unified Manager** 中的远程集群上分析 **MetroCluster** 性能事件

您可以使用 Unified Manager 分析 MetroCluster 配置中远程集群上的动态性能事件。该分析可帮助您确定远程集群上的事件是否导致了其伙伴集群上的事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已在 MetroCluster 配置中分析本地集群上的性能事件，并获得了事件检测时间。
- 您必须已检查参与性能事件的本地集群及其伙伴集群的运行状况，并获取了伙伴集群的名称。

步骤

1. 登录到正在监视配对集群的 Unified Manager 实例。
2. 在左侧导航窗格中，单击*事件*以显示事件列表。
3. 从*时间范围*选择器中，选择*最近一小时*，然后单击*应用范围*。
4. 在*过滤*选择器中，从左侧下拉菜单中选择*集群*，在文本字段中键入伙伴集群的名称，然后单击*应用过滤器*。

   如果在过去一小时内选定集群没有发生任何事件，则表明该集群在其配对节点上检测到事件期间没有遇到任

何性能问题。

5. 如果所选集群在过去一小时内检测到事件，请将事件检测时间与本地集群上事件的事件检测时间进行比较。

   如果这些事件涉及在数据处理组件上引发争用的恶霸工作负载，则其中一个或多个恶霸可能在本地集群上引发该事件。您可以单击事件以对其进行分析，并在事件详细信息页面上查看解决该事件的建议操作。

   如果这些事件不涉及霸道工作负载，则它们并未导致本地集群上发生性能事件。

响应 **Active IQ Unified Manager** 中的动态 **QoS** 限速事件

您可以使用 Unified Manager 调查由服务质量 (QoS) 策略组限制工作负载吞吐量 (MB/s) 引起的性能事件。限制增加了策略组中卷工作负载的响应时间（延迟）。您可以使用事件信息确定是否需要对策略组设置新的限制来停止限制。

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。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中显示受限流影响的工作负载的名称。

   描述可以为受害者和欺凌者显示相同的工作负载，因为限制会使工作负载本身成为受害者。

3. 使用文本编辑器等应用程序记录卷的名称。

   您可以搜索该卷名称，以便稍后查找。

4. 在 Workload Latency 和 Workload Utilization 图表中，选择 **Bully Workloads**。
5. 将光标悬停在图表上可查看影响策略组的顶级用户定义工作负载。

   列表顶部的工作负载偏差最大，导致限制发生。活动是每个工作负载使用的策略组限制的百分比。

6. 在*建议操作*区域中，单击顶部工作负载的*分析工作负载*按钮。
7. 在“工作负载分析”页面中，将“延迟”图表设置为查看所有集群组件，并将“吞吐量”图表设置为查看明细。

   细分图表显示在延迟图表和 IOPS 图表下方。

8. 比较 延迟 图表中的 QoS 限制，了解事件发生时影响延迟的限制量。

   QoS 策略组的最大吞吐量为每秒 1,000 个操作（op/sec），其中的工作负载总计不能超过此限制。在事件发生时，策略组中的工作负载总吞吐量超过 1,200 op/sec，这导致策略组将其活动限制为 1,000 op/sec。

9. 将*读取/写入延迟*值与*读取/写入/其他*值进行比较。

   两个图表都显示了大量具有高延迟的读取请求，但写入请求的请求数和延迟量较低。这些值可帮助您确定是否存在增加延迟的高吞吐量或操作数。在决定对吞吐量或操作设置策略组限制时，可以使用这些值。

10. 使用 ONTAP System Manager 将策略组的当前限制增加到 1,300 个操作/秒。
11. 一天后，返回 Unified Manager 并在*工作负载分析*页面中输入您在步骤 3 中记录的工作负载。
12. 选择吞吐量分解图。

    此时将显示读取/写入/其他图表。

13. 在页面顶端，将光标指向策略组限制更改的更改事件图标（）。
14. 将*读取/写入/其他*图表与*延迟*图表进行比较。

    读取和写入请求相同，但限制已停止，并且延迟已减少。

响应 **Active IQ Unified Manager** 中由磁盘故障引起的性能事件

您可以使用 Unified Manager 调查由过度使用聚合的工作负载引起的性能事件。您还可以使用 Unified Manager 检查聚合的运行状况，以查看在聚合中检测到的最近运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中描述了事件中涉及的工作负载和争用中的集群组件。

    存在多个受集群组件争用影响而导致延迟的受害卷。该聚合正在进行 RAID 重建，以使用备用磁盘替换故障磁盘，是争用中的集群组件。在"争用中的组件"下，聚合图标以红色突出显示，聚合名称显示在括号中。

3. 在 Workload Utilization 图表中，选择 **Bully Workloads**。
4. 将光标悬停在图表上可查看影响组件的排名靠前的霸道工作负载。

    自检测到事件以来，峰值利用率最高的顶级工作负载将显示在图表的顶部。顶级工作负载之一是系统定义的工作负载 Disk Health，它指示 RAID 重建。重建是使用备用磁盘重建聚合的内部过程。Disk Health 工作负载以及聚合上的其他工作负载，可能导致了聚合上的争用及相关事件。

5. 在确认来自磁盘运行状况工作负载的活动导致事件后，等待大约 30 分钟以完成重建，并等待 Unified Manager 分析事件并检测聚合是否仍处于争用状态。
6. 刷新*事件详细信息*。

    RAID 重建完成后，检查状态是否已过时，表示该事件已解决。

7. 在 Workload Utilization 图表中，选择 **Bully Workloads** 以按峰值利用率查看聚合上的工作负载。
8. 在*建议操作*区域中，单击顶部工作负载的*分析工作负载*按钮。
9. 在*工作负载分析*页面中，设置时间范围以显示选定卷的最近 24 小时（1 天）数据。

    在事件时间轴中，红点（）表示磁盘故障事件发生的时间。

10. 在“节点和聚合利用率”图表中，隐藏节点统计信息的线，以便仅保留“聚合”线。
11. 将此图表中的数据与*延迟*图表中事件发生时的数据进行比较。

    在事件发生时，聚合利用率显示由 RAID 重构过程引起的大量读写活动，这增加了所选卷的延迟。事件发生几个小时后，读取和写入以及延迟都已减少，确认聚合不再处于争用状态。

响应 **Active IQ Unified Manager** 中因 **HA** 接管引起的性能事件

您可以使用 Unified Manager 调查由高可用性（HA）对中的群集节点上的高数据处理引起的性能事件。您还可以使用 Unified Manager 检查节点的运行状况，以查看在节点上检测到的任何最近的运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中描述了事件中涉及的工作负载和争用中的集群组件。

    有一个受害者卷的延迟受到了发生争用的集群组件的影响。接管了其伙伴节点所有工作负载的数据处理节点是发生争用的集群组件。在“争用组件”下，Data Processing 图标突出显示为红色，并且事件发生时正在进行数据处理的节点名称显示在括号中。

3. 在*描述*中，单击卷的名称。

    此时将显示卷性能资源管理器页面。在页面的顶端，在事件时间线中，更改事件图标（）指示 Unified Manager 检测到 HA 接管开始的时间。

4. 将光标指向 HA 接管的更改事件图标，有关 HA 接管的详细信息将显示在悬停文本中。

    在延迟图表中，一个事件指示所选卷由于与 HA 接管大致相同时间的高延迟而超过性能阈值。

5. 单击*缩放视图*以在新页面上显示延迟图表。
6. 在视图菜单中，选择*集群组件*以按集群组件查看总延迟。
7. 将鼠标光标指向 HA 接管开始时的更改事件图标，并将 Data Processing 的延迟与总延迟进行比较。

    在 HA 接管时，由于数据处理节点上的工作负载需求增加，数据处理量出现了激增。CPU 利用率的增加推高了延迟并触发了该事件。

8. 修复故障节点后，使用 ONTAP System Manager 执行 HA 交还，将工作负载从配对节点移动到已修复的节点。
9. HA 交还完成后，在 Unified Manager 中进行下一次配置发现（大约 15 分钟）后，在*事件管理*清单页面中查找由 HA 接管触发的事件和工作负载。

    由 HA 接管触发的事件现在处于过时状态，这表明该事件已解决。Data Processing 组件的延迟已经降低，从而降低了总延迟。所选卷现在用于 Data Processing 的节点已解决该事件。

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。