分析动态性能阈值事件

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_events_from_dynamic_performance_thresholds.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

分析动态性能阈值事件 . . . 1
- 分析 Active IQ Unified Manager 中动态性能阈值的事件 . . . 1
- 在 Active IQ Unified Manager 中识别动态性能事件中的受害工作负载 . . . 1
- 在 Active IQ Unified Manager 中识别动态性能事件中的欺凌工作负载 . . . 1
- 在 Active IQ Unified Manager 中识别动态性能事件中的鲨鱼工作负载 . . . 2
- MetroCluster 配置的性能事件分析 . . . 2
  - 使用 Active IQ Unified Manager 分析 MetroCluster 性能事件 . . . 2
  - 在 Active IQ Unified Manager 中的集群上分析 MetroCluster 性能事件 . . . 2
  - 在 Active IQ Unified Manager 中的远程集群上分析 MetroCluster 性能事件 . . . 4
- 响应 Active IQ Unified Manager 中的动态 QoS 限速事件 . . . 4
- 响应 Active IQ Unified Manager 中由磁盘故障引起的性能事件 . . . 5
- 响应 Active IQ Unified Manager 中因 HA 接管引起的性能事件 . . . 6

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

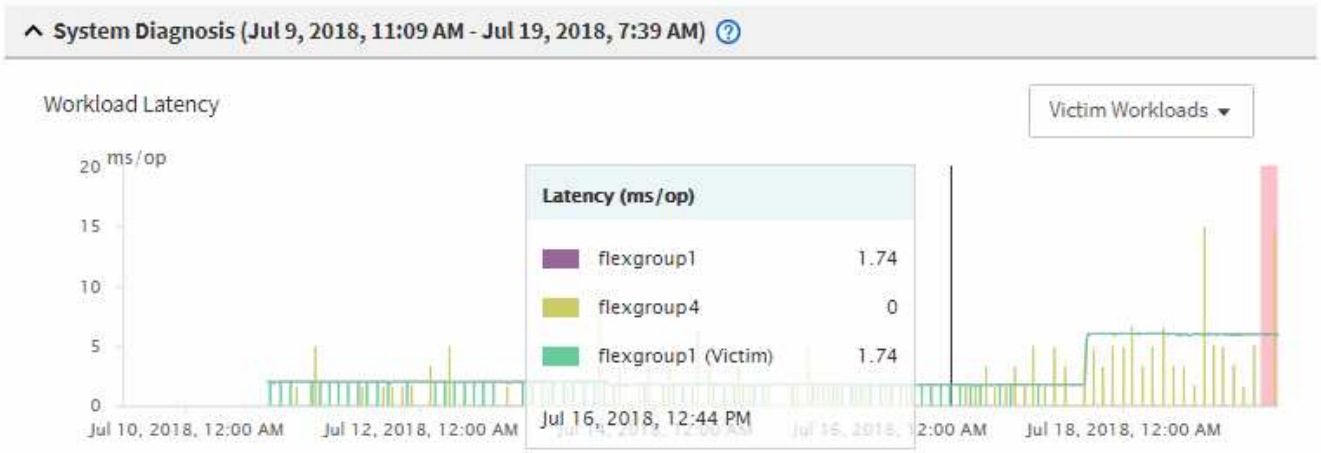
1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看事件描述，了解所涉及的工作负载名称以及所涉及的工作负载数量。

   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。