了解性能事件和警报

Active IQ Unified Manager

NetApp
November 13, 2026

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

目录

了解性能事件和警报 . . . 1
- 了解 Active IQ Unified Manager 中的性能事件和警报 . . . 1
- 确定 Active IQ Unified Manager 中性能事件的来源 . . . 1
- 在 Active IQ Unified Manager 中按严重性对性能事件进行优先级排序 . . . 1
- 监控 Active IQ Unified Manager 检测到的配置更改 . . . 2
- 了解 Active IQ Unified Manager 中系统定义的性能阈值策略 . . . 3
  - 集群阈值策略 . . . 3
  - 节点阈值策略 . . . 3
  - 聚合阈值策略 . . . 4
  - 工作负载延迟阈值策略 . . . 4
  - QoS 阈值策略 . . . 4
- 分析 Active IQ Unified Manager 中的性能事件和通知 . . . 5
  - 事件分析 . . . 5
  - 事件状态 . . . 6
  - 事件通知 . . . 6
  - 事件交互 . . . 6
- 了解 Active IQ Unified Manager 如何确定事件的性能影响 . . . 7
- 了解 Active IQ Unified Manager 中的集群组件和争用情况 . . . 7
- 在 Active IQ Unified Manager 中识别性能事件中的工作负载角色 . . . 9

了解性能事件和警报

了解 Active IQ Unified Manager 中的性能事件和警报

性能事件是与集群上的工作负载性能相关的事件。它们可帮助您识别响应时间较慢的工作负载。结合同时发生的运行状况事件，您可以确定可能导致或促成响应时间缓慢的问题。

当 Unified Manager 检测到同一集群组件出现多次相同事件条件时，它会将所有事件视为单个事件，而不是单独的事件。

您可以配置警报，以便在发生某些严重性类型的性能事件时自动发送电子邮件通知。

确定 Active IQ Unified Manager 中性能事件的来源

性能事件是与集群上的工作负载性能相关的问题。它们可帮助您识别响应时间较慢的存储对象，也称为高延迟。结合同时发生的其他运行状况事件，您可以确定可能导致或促成响应时间缓慢的问题。

Unified Manager 从下列来源接收性能事件：

- 用户定义的性能阈值策略事件

  基于您设置的自定义阈值的性能问题。您可以为存储对象（例如聚合和卷）配置性能阈值策略，以便在超过性能计数器的阈值时生成事件。

  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 的安装中，以涵盖常见的性能问题。

  默认情况下会启用这些阈值策略，您可能会在添加集群后不久看到事件。

- 动态性能阈值事件

  由于 IT 基础架构中的故障或错误，或由于工作负载过度使用集群资源而导致的性能问题。这些事件的原因可能是一个简单的问题，可以在一段时间内自行纠正，也可以通过修复或配置更改来解决。动态阈值事件表示，由于其他工作负载对共享集群组件的使用率较高，ONTAP 系统上的工作负载速度较慢。

  默认情况下会启用这些阈值，从新集群收集数据三天后，您可能会看到事件。

在 Active IQ Unified Manager 中按严重性对性能事件进行优先级排序

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

- 严重

  发生了一个性能事件，如果不立即采取纠正措施，可能会导致服务中断。

  严重事件仅从用户定义的阈值发送。

- 警告

  集群对象的性能计数器超出正常范围，应进行监控以确保其未达到严重级别。此严重级别的事件不会导致服务中断，可能不需要立即采取纠正措施。

  警告事件从用户定义、系统定义或动态阈值发送。

- 信息

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

  当检测到配置更改时，信息事件将直接从 ONTAP 发送。

有关详细信息，请参见以下链接：

- "收到事件时会发生什么情况"
- "警报电子邮件中包含哪些信息"
- "添加警报"
- "为性能事件添加警报"

监控 Active IQ Unified Manager 检测到的配置更改

Unified Manager 监控您的集群的配置更改，以帮助您确定更改是否可能导致或促成性能事件。性能资源管理器页面显示更改事件图标（），以指示检测到更改的日期和时间。

您可以在“性能资源管理器”页面和“工作负载分析”页面中查看性能图表，以查看更改事件是否影响所选集群对象的性能。如果在性能事件发生的同时或前后检测到更改，则该更改可能是导致问题的原因，从而触发了事件警报。

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

- 卷在聚合之间移动。

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

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

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

- HA 对中的节点接管或交还其伙伴节点的存储。

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

- 已成功完成 ONTAP 升级或还原操作。

  将显示先前版本和新版本。

了解 Active IQ Unified Manager 中系统定义的性能阈值策略

Unified Manager 提供一些标准阈值策略，可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，当超出受监控的性能阈值时，它们会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。

如果从任何系统定义的性能阈值策略接收到不必要的事件，则可以从“事件设置”页面禁用单个策略的事件。

集群阈值策略

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

- 集群负载不平衡

  识别一个节点在比集群中的其他节点高得多的负载下运行的情况，从而可能影响工作负载延迟。

  它通过比较集群中所有节点的性能容量使用值来实现此目的，以查看是否有任何节点超过 30% 阈值的时间超过 24 小时。这是一个警告事件。

- 集群容量不平衡

  标识一个聚合的使用容量远高于集群中其他聚合的情况，因此可能会影响操作所需的空间。

  它通过比较集群中所有聚合的已用容量值来实现此目的，以查看任何聚合之间是否存在 70% 的差异。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由 Unified Manager 监控的集群中的每个节点：

- 已违反已用性能容量阈值

  识别单个节点运行超出其运行效率界限的情况，从而可能影响工作负载延迟。

  它通过查找使用超过 100% 的性能容量且持续超过 12 小时的节点来实现此目的。这是一个警告事件。

- 节点 **HA** 对已过度利用

  确定 HA 对中的节点运行效率高于 HA 对运行效率范围的情况。

  它通过查看 HA 对中两个节点的性能容量使用值来实现此目的。如果两个节点使用的总性能容量超过 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。这是一个信息事件。

- 节点磁盘碎片

  识别聚合中的一个或多个磁盘碎片化，减慢关键系统服务并可能影响节点上工作负载延迟的情况。

  它通过查看节点上所有聚合的某些读取和写入操作比率来实现。在 SyncMirror 重新同步期间或在磁盘清理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\`" 策略分析仅限 HDD 的聚合；不分析 Flash Pool、SSD 和 FabricPool 聚合。

聚合阈值策略

系统定义的聚合性能阈值策略默认分配给由 Unified Manager 监控的集群中的每个聚合：

- 聚合磁盘使用过度

  识别聚合运行超出其运行效率限制的情况，从而可能影响工作负载延迟。它通过查找聚合中的磁盘利用率超过 95% 且持续时间超过 30 分钟的聚合来识别这些情况。然后，此多条件策略将执行以下分析以帮助确定问题的原因：

  - 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、磁盘清理、SyncMirror 重新同步和重新计算奇偶校验。

  - 磁盘架光纤通道互连中是否存在通信瓶颈?
  - 聚合中的可用空间是否太少？仅当三个从属策略中的一个（或多个）也被视为违规时，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。

“聚合磁盘过度使用”策略分析仅 HDD 聚合和 Flash Pool（混合）聚合；不分析 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具有已配置性能服务级别策略的任何工作负载，该策略具有定义的“expected latency” 值：

- 已违反性能服务级别定义的工作负载卷**/LUN** 延迟阈值

  标识已超出“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。

  它通过查找在过去一小时内有 30% 的时间超过预期延迟值的工作负载来实现此目的。

QoS 阈值策略

系统定义的 QoS 性能阈值策略将分配给配置了 ONTAP QoS 最大吞吐量策略（IOPS、IOPS/TB 或 MB/s）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 会触发事件：

- **QoS 最大 IOPS 或 MB/s 阈值**

  标识已超出其 QoS 最大 IOPS 或 MB/s 吞吐量限制并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时，它通过查找在前一小时的每个收集期间超过分配的 QoS 策略组中定义的最大吞吐量阈值的工作负载来实现此目的。

  当多个工作负载共享单个 QoS 策略时，它通过将该策略中所有工作负载的 IOPS 或 MB/s 相加，并将该总数与阈值进行比较来实现这一点。

- **QoS 峰值 IOPS/TB 或带有块大小阈值的 IOPS/TB**

  标识已超过其自适应 QoS 峰值 IOPS/TB 吞吐量限制（或带块大小限制的 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，然后查找在前一小时的每个性能收集期间超过 QoS 最大 IOPS 的卷。

  仅当集群安装了 ONTAP 9.3 及更高版本软件时，此策略才应用于卷。

  当自适应 QoS 策略中定义了"`block size`"元素时，系统会根据每个卷的大小将阈值转换为 QoS 最大 MB/s 值。然后，系统会查找在前一小时内每个性能收集周期中超过 QoS 最大 MB/s 的卷。

  仅当集群安装了 ONTAP 9.5 及更高版本软件时，此策略才应用于卷。

分析 Active IQ Unified Manager 中的性能事件和通知

性能事件会通知您由集群组件上的争用引起的工作负载上的 I/O 性能问题。Unified Manager 将分析事件，以确定所涉及的所有工作负载、发生争用的组件以及事件是否仍然是您可能需要解决的问题。

Unified Manager 监控集群上卷的 I/O 延迟（响应时间）和 IOPS（操作）。例如，当其他工作负载过度使用集群组件时，该组件会处于争用状态，无法以最佳水平运行来满足工作负载需求。使用相同组件的其他工作负载的性能可能会受到影响，从而导致其延迟增加。如果延迟超过动态性能阈值，Unified Manager 将触发性能事件以通知您。

事件分析

Unified Manager 使用过去 15 天的性能统计信息执行以下分析，以确定事件中涉及的受害工作负载、恶霸工作负载和集群组件：

- 识别延迟超过动态性能阈值的受害者工作负载，动态性能阈值是延迟预测的上限：
  - 对于 HDD 或 Flash Pool 混合聚合（本地层）上的卷，仅当延迟大于 5 毫秒（ms）且 IOPS 大于每秒 10 次操作（ops/sec）时才会触发事件。
  - 对于全 SSD 聚合或 FabricPool 聚合（云层）上的卷，仅当延迟大于 1 ms 且 IOPS 大于 100 ops/sec 时才会触发事件。
- 标识争用中的集群组件。

如果集群互连处的受害工作负载延迟大于 1 毫秒，Unified Manager 会将其视为重大问题，并触发集群互连事件。

- 标识过度使用集群组件并导致其处于争用状态的欺凌工作负载。
- 根据集群组件利用率或活动的偏差对所涉及的工作负载进行排名，以确定哪些欺凌者对集群组件的使用率变化最大，哪些受害者受到的影响最大。

事件可能仅发生短暂的时间，并在其使用的组件不再发生争用后自行恢复。连续事件是指在五分钟间隔内对同一集群组件重复发生并保持活动状态的事件。对于连续事件，Unified Manager 在连续两个分析间隔期间检测到同一事件后会触发警报。

当事件解决后，它在 Unified Manager 中仍然可用，作为卷过去性能问题记录的一部分。每个事件都有一个唯一的 ID，用于标识事件类型以及所涉及的卷、集群和集群组件。

单个卷可以同时涉及多个事件。

事件状态

事件可能处于以下状态之一：

- 活动

  指示性能事件当前处于活动状态（新建或已确认）。导致事件的问题尚未自行更正或尚未解决。存储对象的性能计数器仍高于性能阈值。

- 已废弃

  指示该事件不再处于活动状态。导致该事件的问题已自行更正或已解决。存储对象的性能计数器不再高于性能阈值。

事件通知

事件显示在“仪表板”页面和用户界面的许多其他页面上，这些事件的警报将发送到指定的电子邮件地址。您可以在“事件详细信息”页面和“工作负载分析”页面上查看有关事件的详细分析信息并获取解决该事件的建议。

事件交互

在“事件详细信息”页面和“工作负载分析”页面上，您可以通过以下方式与事件进行交互：

- 将鼠标移到事件上会显示一条消息，显示检测到事件的日期和时间。

  如果同一时间段存在多个事件，消息将显示事件数量。

- 单击单个事件将显示一个对话框，其中显示有关该事件的更详细信息，包括所涉及的集群组件。

  竞争中的组件以红色圆圈突出显示。您可以单击 **View full analysis** 以在 Event details 页面上查看完整分析。如果同一时间段内存在多个事件，该对话框将显示最近三个事件的详细信息。您可以单击某个事件，以在 Event details 页面上查看事件分析。

了解 Active IQ Unified Manager 如何确定事件的性能影响

Unified Manager 使用工作负载的活动、利用率、写入吞吐量、集群组件使用率或 I/O 延迟（响应时间）的偏差来确定对工作负载性能的影响程度。这些信息决定了每个工作负载在事件中的角色以及它们在事件详细信息页面上的排名方式。

Unified Manager 将工作负载的最后分析值与值的预期范围（延迟预测）进行比较。上次分析的值与预期值范围之间的差异标识了性能受事件影响最大的工作负载。

例如，假设集群包含两个工作负载：工作负载 A 和工作负载 B。工作负载 A 的延迟预测为每次操作 5-10 毫秒（ms/op），其实际延迟通常约为 7 ms/op。工作负载 B 的延迟预测为 10-20 ms/op，其实际延迟通常约为 15 ms/op。这两个工作负载都在其延迟预测范围内。由于集群上的竞争，两个工作负载的延迟都增加到 40 ms/op，跨越了动态性能阈值（即延迟预测的上限），并触发了事件。工作负载 A 的延迟偏差（从预期值到高于性能阈值的值）约为 33 ms/op，工作负载 B 的偏差约为 25 ms/op。两个工作负载的延迟均飙升至 40 ms/op，但工作负载 A 对性能的影响更大，因为它的延迟偏差更高，达到了 33 ms/op。

在“事件详细信息”页面的“系统诊断”部分，您可以按集群组件的活动、利用率或吞吐量偏差对工作负载进行排序。您还可以按延迟对工作负载进行排序。当您选择排序选项时，Unified Manager 会分析自检测到事件以来活动、利用率、吞吐量或延迟与预期值的偏差，以确定工作负载的排序顺序。对于延迟，红点（🔴）表示受害工作负载超出了性能阈值，以及随后对延迟产生的影响。每个红点表示更高水平的延迟偏差，这有助于您识别延迟受事件影响最大的受害工作负载。

了解 Active IQ Unified Manager 中的集群组件和争用情况

当集群组件发生争用时，您可以识别集群性能问题。使用该组件的工作负载性能会下降，其对客户端请求的响应时间（延迟）会增加，这会在 Unified Manager 中触发事件。

处于争用状态的组件无法在最佳水平下运行。其性能会有所下降，并且其他集群组件和工作负载（称为 *victims* ）的性能可能会出现延迟增加的情况。要使组件摆脱争用状态，必须减少其工作负载或提高其处理更多工作的能力，以便性能能够恢复到正常水平。由于 Unified Manager 每隔五分钟收集并分析一次工作负载性能，因此它仅在集群组件被持续过度使用时才会检测到。在五分钟间隔内仅持续很短时间的暂时性过度使用峰值不会被检测到。

例如，存储聚合可能存在争用，因为其上的一个或多个工作负载正在争用以满足其 I/O 请求。聚合上的其他工作负载可能会受到影响，导致其性能下降。为了减少聚合上的活动量，您可以采取不同的步骤，例如将一个或多个工作负载移动到不太繁忙的聚合或节点，以减少当前聚合的整体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制，或将工作负载移动到其他策略组，以便不再限制工作负载。

Unified Manager 可监控以下集群组件，以便在它们发生争用时向您发出警报：

- 网络

  表示集群上外部网络协议对 I/O 请求的等待时间。等待时间是指集群在对 I/O 请求做出响应前等待 “transfer ready” 事务完成的时间。如果网络组件存在争用，则意味着协议层的等待时间过长会影响一个或多个工作负载的延迟。

- 网络处理

  表示集群中涉及协议层和集群之间 I/O 处理的软件组件。自检测到事件以来，负责网络处理的节点可能已发生更改。如果网络处理组件处于争用状态，则意味着网络处理节点的高利用率正在影响一个或多个工作负载的延迟。

在双活配置中使用全 SAN 阵列集群时，将显示两个节点的网络处理延迟值，以便您验证节点是否平均分担负载。

- 服务质量（**QoS**）上限

  表示分配给工作负载的存储服务质量（QoS）策略组的吞吐量最大值（峰值）设置。如果策略组组件存在争用，则表示策略组中的所有工作负载都受到设置的吞吐量限制的限制，这会影响其中一个或多个工作负载的延迟。

- **QoS** 限制下限

  表示分配给其他工作负载的 QoS 吞吐量最小（预期）设置导致的工作负载延迟。如果在某些工作负载上设置的 QoS 最小值使用了大部分带宽来保证承诺的吞吐量，则其他工作负载将受到限制并出现更高的延迟。

- 集群互连

  表示与已加入集群的节点物理连接的缆线和适配器。如果集群互连组件处于争用状态，则意味着在集群互连处等待 I/O 请求的时间较长，这会影响一个或多个工作负载的延迟。

- **Data Processing**

  表示集群中涉及集群和包含工作负载的存储聚合之间的 I/O 处理的软件组件。负责 Data Processing 的节点可能会在检测到事件后发生更改。如果 Data Processing 组件存在争用，则意味着 Data Processing 节点的高利用率会影响一个或多个工作负载的延迟。

- 卷激活

  表示跟踪所有活动卷使用情况的过程。在超过 1000 个卷处于活动状态的大型环境中，此过程将跟踪有多少关键卷需要同时通过节点访问资源。当并发活动卷的数量超过建议的最大阈值时，某些非关键卷将出现此处指出的延迟。

- **MetroCluster** 资源

  表示 MetroCluster 资源，包括 NVRAM 和交换机间链路（ISL），用于在 MetroCluster 配置中的集群之间镜像数据。如果 MetroCluster 组件存在争用，则意味着本地集群上工作负载的高写入吞吐量或链路运行状况问题正在影响本地集群上一个或多个工作负载的延迟。如果集群不在 MetroCluster 配置中，则不显示此图标。

- 聚合或 **SSD** 聚合操作

  表示运行工作负载的存储聚合。如果聚合组件存在争用，则意味着聚合的高利用率正在影响一个或多个工作负载的延迟。聚合由全部 HDD，或者 HDD 和 SSD 的混合（Flash Pool 聚合），或者 HDD 和云层的混合（FabricPool 聚合）组成。“SSD Aggregate” 由全部 SSD（全闪存聚合），或者 SSD 和云层的混合（FabricPool 聚合）组成。

- 云延迟

  表示集群和存储用户数据的云层之间的 I/O 处理所涉及的软件组件。如果云延迟组件发生争用，则意味着从云层上托管的卷进行的大量读取会影响一个或多个工作负载的延迟。

- 同步 **SnapMirror**

  表示集群中涉及在 SnapMirror 同步关系中将用户数据从主卷复制到辅助卷的软件组件。如果同步 SnapMirror 组件存在争用，则表示来自 SnapMirror 同步操作的活动正在影响一个或多个工作负载的延迟。

在 Active IQ Unified Manager 中识别性能事件中的工作负载角色

Unified Manager 使用角色来识别工作负载在性能事件中的参与度。角色包括受害者、欺凌者和鲨鱼。用户定义的工作负载可能同时是受害者、欺凌者和鲨鱼。

角色	问题描述
受影响	由于过度使用集群组件的其他工作负载（称为恶霸）而导致性能下降的用户定义工作负载。仅将用户定义的工作负载标识为受害者。Unified Manager 根据延迟的偏差来识别受害者工作负载，其中事件期间的实际延迟比其延迟预测（预期范围）大大增加。
抢占资源	用户定义或系统定义的工作负载，其过度使用集群组件导致其他工作负载（称为受害者）的性能降低。Unified Manager 根据集群组件的使用偏差来识别欺凌工作负载，其中在事件期间的实际使用量比其预期的使用范围大大增加。
强占资源的工作负载	与事件中涉及的所有工作负载相比，集群组件的使用率最高的用户定义工作负载。Unified Manager 根据事件期间集群组件的使用情况来识别 shark 工作负载。

集群上的工作负载可以共享许多集群组件，例如用于网络和数据处理的聚合和 CPU。当工作负载（如卷）增加其对集群组件的使用，以至于组件无法有效地满足工作负载需求时，该组件就处于争用状态。过度使用集群组件的工作负载是欺凌者。共享这些组件且其性能受到欺凌者影响的其他工作负载是受害者。来自系统定义工作负载（例如重复数据删除或 Snapshot 副本）的活动也可能升级为 “bullying”。

当 Unified Manager 检测到事件时，它会识别所涉及的所有工作负载和集群组件，包括导致事件的恶霸工作负载、发生争用的集群组件以及由于恶霸工作负载的活动增加而导致性能下降的受害者工作负载。

如果 Unified Manager 无法识别恶霸工作负载，它只会对受害者工作负载和所涉及的集群组件发出警报。

Unified Manager 可以识别作为欺凌工作负载受害者的工作负载，并确定这些相同的工作负载何时成为欺凌工作负载。工作负载可能会欺凌自身。例如，受策略组限制所限制的高性能工作负载会导致策略组中的所有工作负载（包括其自身）受到限制。在持续发生的性能事件中，作为欺凌者或受害者的工作负载可能会更改其角色，或者不再是该事件的参与者。

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。