事件窗口和对话框说明

Active IQ Unified Manager

NetApp
November 13, 2026

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

目录

事件窗口和对话框说明 1
了解 Active IQ Unified Manager 中的通知页面 1
电子邮件 1
SMTP 服务器 1
SNMP 2
了解 Active IQ Unified Manager 中的事件管理清单页面 3
筛选组件 3
命令按钮 3
事件列表 4
事件详细信息页面 6
了解 Active IQ Unified Manager 中的事件详细信息页面 6
了解 Active IQ Unified Manager 中的事件信息部分 7
了解 Active IQ Unified Manager 中的建议操作 10
了解 Active IQ Unified Manager 中的系统诊断 10
了解 Active IQ Unified Manager 中的事件设置页面 11
命令按钮 11
列表视图 11
禁用 Active IQ Unified Manager 中的"事件"对话框 11
事件属性区域 12
命令按钮 12

事件窗口和对话框说明

了解 Active IQ Unified Manager 中的通知页面

您可以将 Unified Manager 服务器配置为在生成事件或将事件分配给用户时发送通知。您还可以配置通知机制。例如，通知可以作为电子邮件或 SNMP 陷阱发送。

您必须具有应用程序管理员或存储管理员角色。

电子邮件

此区域用于配置以下用于告警通知的电子邮件设置：

- 发件人地址

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

SMTP 服务器

此区域用于配置以下 SMTP 服务器设置：

- 主机名或 **IP** 地址

  指定 SMTP 主机服务器的主机名，该主机名用于向指定的收件人发送警报通知。

- 用户名

  指定 SMTP 用户名。只有在 SMTP 服务器中启用 SMTPAUTH 时，才需要 SMTP 用户名。

- 密码

  指定 SMTP 密码。只有在 SMTP 服务器中启用 SMTPAUTH 时，才需要 SMTP 用户名。

- 端口

  指定 SMTP 主机服务器用于发送警报通知的端口。

  默认值为 25。

- 使用 **START/TLS**

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

- 使用 **SSL**

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

SNMP

此区域用于配置以下 SNMP 陷阱设置：

- 版本

  根据所需的安全类型指定要使用的 SNMP 版本。选项包括版本 1、版本 3、版本 3（含身份验证）和版本 3（含身份验证和加密）。默认值为版本 1。

- **Trap** 目标主机

  指定接收管理服务器发送的 SNMP 陷阱的主机名或 IP 地址（IPv4 或 IPv6）。要指定多个陷阱目的地，请使用逗号分隔每个主机。

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

- 出站陷阱端口

  指定 SNMP 服务器接收管理服务器发送的陷阱所通过的端口。

  默认值为 162。

- 社区

  用于访问主机的社区字符串。

- 引擎 **ID**

  指定 SNMP 代理的唯一标识符，并由管理服务器自动生成。引擎 ID 可用于 SNMP 版本 3、SNMP 版本 3（含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 用户名

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

- 身份验证协议

  指定用于对用户进行身份验证的协议。协议选项包括 MD5 和 SHA。MD5 是默认值。身份验证协议可用于 SNMP 版本 3 （含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 身份验证密码

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

- 隐私协议

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

- 隐私密码

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

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

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

事件管理清单页面使您能够查看当前事件及其属性的列表。您可以执行确认、解决和分配事件等任务。您还可以为特定事件添加警报。

此页面上的信息每 5 分钟自动刷新一次，以确保显示最新的新事件。

筛选组件

使您能够自定义事件列表中显示的信息。可以使用以下组件优化显示的事件列表：

- 查看菜单可从预定义的筛选器选择列表中进行选择。

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

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

命令按钮

这些命令按钮可用来执行下列任务：

- 分配给

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

  - 自己

    将事件分配给当前登录的用户。

  - 其他用户

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

- 确认

  确认选定事件。

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

  

  您无法确认信息事件。

- 标记为已解决

  使您能够将事件状态更改为已解决。

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

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

- 报告

  使您能够将当前事件视图的详细信息导出为逗号分隔值 (.csv) 文件或 PDF 文档。

- 显示/隐藏列选择器

  使您能够选择在页面上显示的列，并选择它们的显示顺序。

事件列表

显示按触发时间排序的所有事件的详细信息。

默认情况下，将显示所有活动事件视图，以显示前七天具有事件或风险影响级别的新事件和已确认事件。

- 触发时间

  生成事件的时间。

- 严重程度

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

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 影响级别

  事件影响级别：突发事件、风险、事件或升级。

- 影响区域

  事件影响区域：可用性、容量、性能、保护、配置或安全性。

- 名称

  事件名称。您可以选择名称以显示该事件的“事件详细信息”页面。

- 源

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

当发生共享 QoS 策略违规时，此字段中仅显示占用最多 IOPS 或 MB/s 的工作负载对象。使用此策略的其他工作负载将显示在事件详细信息页面中。

- 源类型

  与事件关联的对象类型（例如，Storage VM、卷或 Qtree）。

- 分配给

  事件分配到的用户名称。

- 事件起源

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

- 注释名称

  分配给存储对象的批注的名称。

- 备注

  为事件添加的注释数。

- 待处理天数

  事件最初生成后的天数。

- 分配时间

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

- 确认人

  确认此事件的用户的名称。如果事件未确认，此字段为空。

- 确认时间

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

- 解决者

  解决事件的用户的名称。如果事件未解决，则此字段为空。

- 解决时间

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

- 废弃时间

  事件状态变为已过时的时间。

事件详细信息页面

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

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

- 事件名称

  事件的名称和上次发现事件的时间。

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

- 事件描述

  对事件的简要描述。

  在某些情况下，事件触发的原因会在事件描述中提供。

- 争用组件

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

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

事件信息、系统诊断和建议操作部分在其他主题中进行了说明。

命令按钮

这些命令按钮可用来执行下列任务：

- 备注图标

  使您可以添加或更新有关事件的备注，并查看其他用户留下的所有备注。

操作菜单

- 分配给我

  将此事件分配给您。

- 分配给其他人

  打开“分配所有者”对话框，用于将事件分配或重新分配给其他用户。

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

  您也可以将所有权字段留空，以取消分配事件。

- 确认

确认所选事件，这样您就不会继续收到重复警报通知。

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

- 标记为已解决

  使您能够将事件状态更改为“已解决”。

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

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

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

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

不适用于该事件类型的字段将被隐藏。您可以查看以下事件详细信息：

- 事件触发时间

  生成事件的时间。

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 废弃原因

  导致事件被废弃的操作，例如，问题已修复。

- 事件持续时间

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

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

- 上次查看时间

  上次将事件显示为活动的日期和时间。

  对于性能事件，此值可能比事件触发时间更新，因为只要事件处于活动状态，此字段就会在每次新的性能数据收集之后更新。对于其他类型的事件，当处于“新建”或“已确认”状态时，此内容不会更新，因此该字段将被隐藏。

- 严重程度

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

- 影响级别

  事件影响级别：突发事件、风险、事件或升级。

- 影响区域

  事件影响区域：可用性、容量、性能、保护、配置或安全性。

- 源

  发生事件的对象的名称。

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

  您可以单击源名称链接来显示该对象的运行状况或性能详细信息页面。

- 源注释

  显示与事件关联的对象的批注名称和值。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源组

  显示受影响对象所属的所有组的名称。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源类型

  与事件关联的对象类型（例如 SVM、Volume 或 Qtree）。

- 在集群上

  发生事件的集群的名称。

  您可以单击集群名称链接来显示该集群的运行状况或性能详细信息页面。

- 受影响对象计数

  受此事件影响的对象数。

  您可以单击对象链接来显示包含当前受此事件影响的对象的清单页面。

  此字段仅针对性能事件显示。

- 受影响的卷

  受此事件影响的卷数。

此字段仅针对节点或聚合上的性能事件显示。

- 触发策略

  发出事件的阈值策略的名称。

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

  此字段仅针对性能事件显示。

- 规则 **ID**

  对于 Active IQ 平台事件，这是触发生成此事件的规则编号。

- 确认人

  确认该事件的人员的姓名和确认该事件的时间。

- 解决者

  解决事件的人员姓名和事件解决的时间。

- 分配给

  被指派处理该事件的人员的姓名。

- 警报设置

  此时将显示有关警报的以下信息：

  - 如果没有与选定事件关联的警报，则会显示*添加警报*链接。

    您可以通过单击链接打开“添加警报”对话框。

  - 如果有一个警报与所选事件关联，则会显示警报名称。

    您可以通过单击链接打开“编辑警报”对话框。

  - 如果有多个警报与所选事件相关联，则会显示警报数量。

    您可以通过单击链接打开“警报设置”页面，以查看有关这些警报的更多详细信息。

  已禁用的警报不会显示。

- 上次发送的通知

  发送最新警报通知的日期和时间。

- 发送方式

  用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- 上次脚本运行

  生成警报时所执行脚本的名称。

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

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

此区域仅针对某些类型的事件显示。

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

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

如果要更详细地分析对象和事件，请单击*分析工作负载*按钮以显示工作负载分析页面。

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

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

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

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

此区域仅针对某些事件显示。

某些性能事件会提供与已触发的特定事件相关的图表。通常，这包括前十天的 IOPS 或 MBps 图表以及延迟图表。以这种方式排列后，您可以看到在事件处于活动状态时，哪些存储组件对延迟的影响最大，或受延迟影响最大。

对于动态性能事件，将显示以下图表：

- 工作负载延迟 - 显示处于争用状态的组件中最严重的受害者、欺凌者或鲨鱼工作负载的延迟历史记录。
- 工作负载活动 - 显示有关处于争用状态的集群组件的工作负载使用情况的详细信息。
- 资源活动 - 显示争用中的集群组件的历史性能统计信息。

当某些集群组件处于争用状态时，将显示其他图表。

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

了解 Active IQ Unified Manager 中的事件设置页面

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

仅当您具有应用程序管理员或存储管理员角色时，才能访问此页面。

命令按钮

命令按钮可用于为所选事件执行以下任务：

- 禁用

  启动“禁用事件”对话框，您可以使用它来禁用事件。

- 启用

  启用之前选择禁用的选定事件。

- 上传规则

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

- 订阅 **EMS** 事件

  启动 Subscribe to EMS Events（订阅 EMS 事件）对话框，使您能够订阅从正在监视的集群接收特定事件管理系统 (EMS) 事件。EMS 收集有关集群上发生的事件的信息。当收到已订阅 EMS 事件的通知时，将生成具有适当严重程度的 Unified Manager 事件。

列表视图

列表视图以表格格式显示有关已禁用事件的信息。您可以使用列筛选器自定义显示的数据。

- 事件

  显示已禁用事件的名称。

- 严重程度

  显示事件的严重程度。严重程度可以是严重、错误、警告或信息。

- 源类型

  显示为其生成事件的源类型。

禁用 Active IQ Unified Manager 中的"事件"对话框

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

组事件禁用事件类型的事件。

您必须具有应用程序管理员或存储管理员角色。

事件属性区域

事件属性区域指定以下事件属性：

- 事件严重程度

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

- 事件名称包含

  使您能够筛选名称包含指定字符的事件。

- 匹配事件

  显示与事件严重性类型和您指定的文本字符串匹配的事件列表。

- 禁用事件

  显示选定要禁用的事件列表。

  还会显示事件的严重性以及事件名称。

命令按钮

通过命令按钮，可以为选定事件执行以下任务：

- 保存并关闭

  禁用此事件类型并关闭此对话框。

- 取消

  放弃更改并关闭对话框。

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。