



监控事件

StorageGRID 11.5

NetApp
April 11, 2024

目录

监控事件	1
从节点页面查看事件	1
从网格拓扑页面查看事件	1
查看以前的事件	1
正在重置事件计数	2
创建自定义系统日志事件	4
将自定义事件计数重置为零	5

监控事件

您可以监控网格节点检测到的事件，包括您为跟踪记录到系统日志服务器的事件而创建的自定义事件。网络管理器中显示的最后一个事件消息提供了有关最新事件的详细信息。

事件消息也会在中列出 `/var/local/log/bycast-err.log` 日志文件。

网络问题，断电或升级等问题可能会重复触发 SMTT"（事件总数）" 警报。本节介绍了有关调查事件的信息，以便您更好地了解发生这些警报的原因。如果由于已知问题描述 而发生事件，则可以安全地重置事件计数器。

从节点页面查看事件

节点页面列出了每个网格节点的系统事件。

1. 选择*节点*。
2. 选择*GRID NODE*>*事件*。
3. 在页面顶部、确定是否为*上次事件*显示事件、该事件描述了网格节点检测到的最后一个事件。

此事件将从网格节点逐字中继、并包含严重性级别为错误或严重的任何日志消息。

4. 查看此表、查看任何事件或错误的计数是否为零。
5. 解决问题后、单击*重置事件计数*以将计数恢复为零。

从网络拓扑页面查看事件

"网络拓扑"页面还列出了每个网格节点的系统事件。

1. 选择*支持*>*工具*>*网络拓扑*。
2. 选择 * 站点 _ * > * 网格节点 _ * > * SSM * > * 事件 * > * 概述 * > * 主 * 。

相关信息

["正在重置事件计数"](#)

["日志文件参考"](#)

查看以前的事件

您可以生成先前事件消息的列表、以帮助隔离过去发生的问题。

1. 选择*支持*>*工具*>*网络拓扑*。
2. 选择 * 站点 _ * > * 网格节点 _ * > * SSM * > * 事件 * > * 报告 * 。
3. 选择 * 文本 * 。

"图表"视图中不显示*最后一个事件*属性。

4. 将 * 属性 * 更改为 * 最后一个事件 * 。
5. 也可以选择 * 快速查询 * 的时间段。
6. 单击 * 更新 * 。

Reports (Text): SSM (170-41) - Events

Attribute: Last Event Results Per Page: 20 Start Date: 2009/04/15 15:19:53
 Quick Query: Last 5 Minutes Update Raw Data: End Date: 2009/04/15 15:24:53

Text Results for Last Event
 2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

相关信息

["使用图表和报告"](#)

正在重置事件计数

解决系统事件后、您可以将事件计数重置为零。

您需要的内容

- 您必须使用支持的浏览器登录到网络管理器。
- 您必须具有网络拓扑页面配置权限。


























步骤

1. 选择*节点*>*网络节点_*>*事件*。
2. 确保已解决计数大于0的任何事件。
3. 单击*重置事件计数*。

Events

Last Event

No Events

Description	Count	
Abnormal Software Events	0	
Account Service Events	0	
Cassandra Heap Out Of Memory Errors	0	
Cassandra unhandled exceptions	0	
Chunk Service Events	0	
Custom Events	0	
Data-Mover Service Events	0	
File System Errors	0	
Forced Termination Events	0	
Hotfix Installation Failure Events	0	
I/O Errors	0	
IDE Errors	0	
Identity Service Events	0	
Kernel Errors	0	
Kernel Memory Allocation Failure	0	
Keystone Service Events	0	
Network Receive Errors	0	
Network Transmit Errors	0	
Node Errors	0	
Out Of Memory Errors	0	
Replicated State Machine Service Events	0	
SCSI Errors	0	
Stat Service Events	0	
Storage Hardware Events	0	
System Time Events	0	

[Reset event counts !\[\]\(e2376d476d06eb31946dc01a69a4403a_img.jpg\)](#)

创建自定义系统日志事件

通过自定义事件，您可以跟踪记录到系统日志服务器的所有内核，守护进程，错误和严重级别的用户事件。自定义事件可用于监控系统日志消息的发生情况（进而监控网络安全事件和硬件故障）。



关于此任务

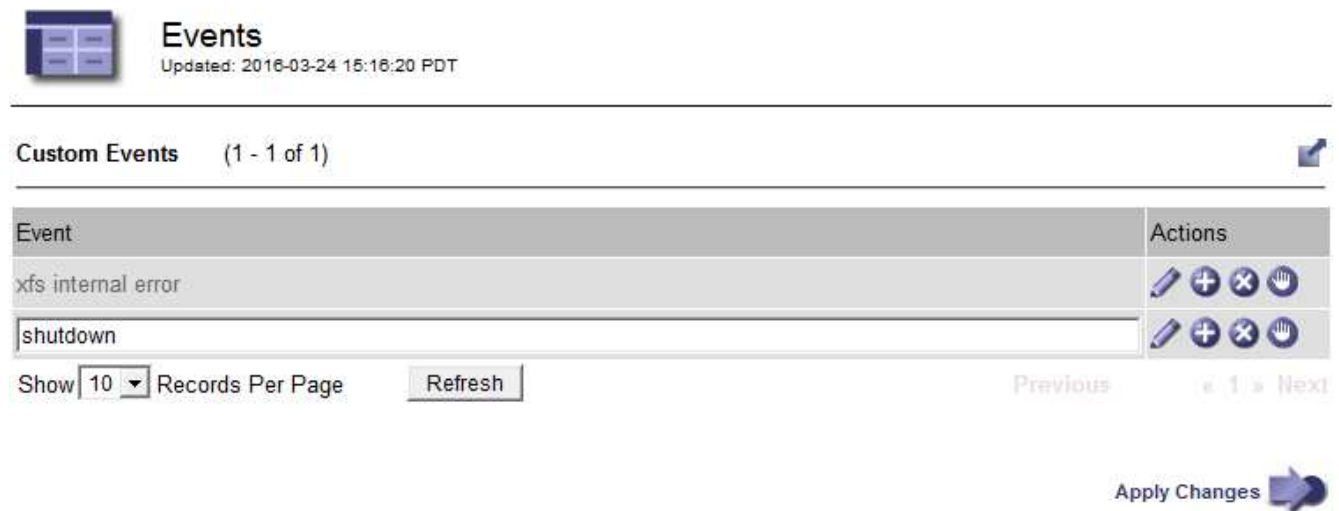
请考虑创建自定义事件以监控重复出现的问题。以下注意事项适用于自定义事件。









- 创建自定义事件后，系统会监控其每次发生情况。您可以在*节点*>*网格节点_*>*事件*页面上查看所有自定义事件的累积计数值。
- 基于中的关键字创建自定义事件 `/var/log/messages` 或 `/var/log/syslog` 文件、这些文件中的日志必须为：
 - 由内核生成
 - 由守护进程或用户程序在错误或严重级别生成

*注：*中并非所有条目 `/var/log/messages` 或 `/var/log/syslog` 除非文件满足上述要求、否则将匹配这些文件。

步骤

1. 选择*配置*>*监控*>*事件*。
2. 单击 * 编辑 *。  （或 * 插入 *  如果这不是第一个事件）。
3. 输入自定义事件字符串，例如 shutdown



Event	Actions
xfs internal error	   
shutdown	   

4. 单击 * 应用更改 *。
5. 选择*节点*。然后、选择*网格节点_*>*事件*。
6. 在事件表中找到自定义事件条目，并监控 * 计数 * 的值。

如果计数增加，则会在该网格节点上触发您正在监控的自定义事件。

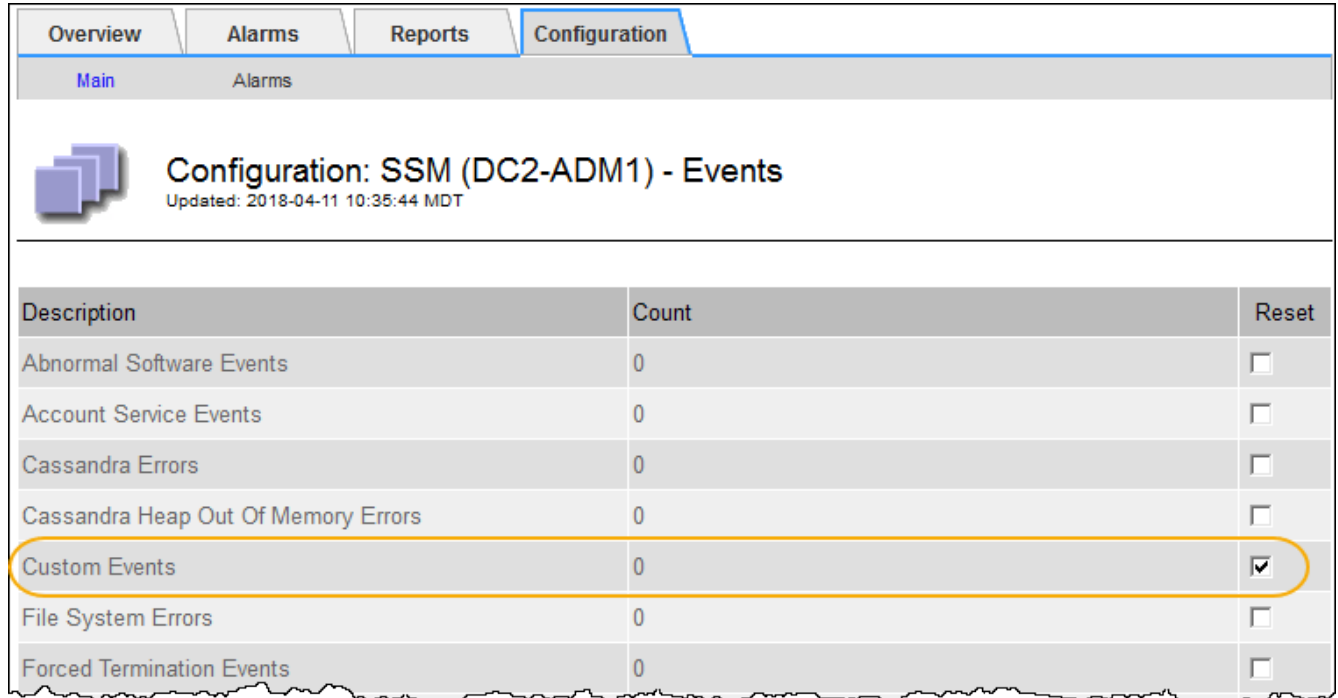
将自定义事件计数重置为零

如果只想重置自定义事件的计数器，则必须使用支持菜单中的网格拓扑页面。

关于此任务

重置计数器会导致下一个事件触发警报。相反，确认警报时，只有在达到下一阈值级别时才会重新触发该警报。

1. 选择*支持*>*工具*>*网格拓扑*。
2. 选择 **GRID NODE** > * SSM* > * 事件 * > * 配置 * > * 主 * 。
3. 选中自定义事件的 * 重置 * 复选框。



Description	Count	Reset
Abnormal Software Events	0	<input type="checkbox"/>
Account Service Events	0	<input type="checkbox"/>
Cassandra Errors	0	<input type="checkbox"/>
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>
Custom Events	0	<input checked="" type="checkbox"/>
File System Errors	0	<input type="checkbox"/>
Forced Termination Events	0	<input type="checkbox"/>

4. 单击 * 应用更改 * 。

版权信息

版权所有 © 2024 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。