



警报和警报 StorageGRID

NetApp
November 04, 2025

目录

警报和警报	1
管理警报和警报：概述	1
警报系统	1
传统警报系统	1
比较警报和警报	1
管理警报	4
管理警报：概述	4
查看警报规则	5
创建自定义警报规则	7
编辑警报规则	9
禁用警报规则	12
删除自定义警报规则	12
管理警报通知	13
警报参考	23
设备警报	23
审核和系统日志警报	25
存储分段警报	25
Cassandra警报	25
云存储池警报	26
跨网格复制警报	26
DHCP警报	26
调试和跟踪警报	27
电子邮件和AutoSupport 警报	27
纠删编码(EC)警报	27
证书到期警报	27
网格网络警报	28
网格联盟警报	28
高使用量或高延迟警报	28
身份联合警报	28
信息生命周期管理(ILM)警报	28
密钥管理服务器(KMS)警报	28
本地时钟偏移警报	29
内存不足或空间不足警报	29
节点或节点网络警报	30
对象警报	31
平台服务警报	31
存储卷警报	32
StorageGRID 服务警报	32
租户警报	32

常用的 Prometheus 指标	32
什么是Prometheus指标?	32
Prometheus指标在哪里使用?	33
列出最常见的指标	33
获取所有指标的列表	38
管理警报 (旧系统)	38
管理警报 (旧系统)	38
查看旧警报	57
警报参考 (旧系统)	58

警报和警报

管理警报和警报：概述

StorageGRID 警报系统旨在通知您需要关注的操作问题。旧警报系统已弃用。

警报系统

警报系统是用于监控 StorageGRID 系统中可能发生的任何问题的主要工具。警报系统提供了一个易于使用的界面，用于检测，评估和解决问题。

当警报规则条件评估为 true 时，系统将在特定严重性级别触发警报。触发警报后，将执行以下操作：

- 在网格管理器的信息板上会显示警报严重性图标、当前警报的计数将递增。
- 警报显示在 * 节点 * 摘要页面和 * 节点 * > * 节点 _ * > * 概述 * 选项卡上。
- 假定您已配置 SMTP 服务器并为收件人提供了电子邮件地址，则会发送电子邮件通知。
- 假定您已配置 StorageGRID SNMP 代理，则会发送简单网络管理协议（SNMP）通知。

传统警报系统

与警报一样，当属性达到定义的阈值时，也会在特定严重性级别触发警报。但是，与警报不同的是，对于可以安全忽略的事件，系统会触发许多警报，这可能会导致电子邮件或 SNMP 通知过多。



警报系统已弃用，将在未来版本中删除。如果您仍在使用传统警报，则应尽快完全过渡到警报系统。

触发警报后，将执行以下操作：

- 警报将显示在 * 支持 * > * 警报（原有） * > * 当前警报 * 页面上。
- 假定您已配置 SMTP 服务器并配置了一个或多个邮件列表，则会发送电子邮件通知。
- 假设您已配置 StorageGRID SNMP 代理，则可能会发送 SNMP 通知。（不会针对所有警报或警报严重程度发送SNMP通知。）

比较警报和警报

警报系统和传统警报系统之间有几个相似之处、但警报系统具有显著优势、并且更易于使用。

请参见下表，了解如何执行类似操作。

	警报	警报（旧系统）
如何查看哪些警报处于活动状态？	<ul style="list-style-type: none"> 选择信息板上的*当前警报*链接。 在*节点*>*概述*页面上选择警报。 选择*警报*>*当前*。 <p>"查看当前警报"</p>	<p>选择*支持*>*警报（原有）*>*当前警报*。</p> <p>"管理警报（旧系统）"</p>
触发警报或警报的原因是什么？	<p>如果警报规则中的 Prometheus 表达式在特定触发条件和持续时间下评估为 true ，则会触发警报。</p> <p>"查看警报规则"</p>	<p>当 StorageGRID 属性达到阈值时，将触发警报。</p> <p>"管理警报（旧系统）"</p>
如果触发警报或警报，如何解决根本问题？	<p>电子邮件通知中包含警报的建议操作，您可以从网格管理器的警报页面中获取这些操作。</p> <p>StorageGRID 文档会根据需要提供追加信息。</p> <p>"警报参考"</p>	<p>您可以通过选择属性名称来了解警报，也可以在 StorageGRID 文档中搜索警报代码。</p> <p>"警报参考（旧系统）"</p>
在哪里可以看到已解决的警报或警报列表？	<p>选择*警报*>*已解决*。</p> <p>"查看当前警报和已解决警报"</p>	<p>选择*支持*>*警报（原有）*>*历史警报*。</p> <p>"管理警报（旧系统）"</p>
在何处管理设置？	<p>选择*警报*>*规则*。</p> <p>"管理警报"</p>	<p>选择*支持*。然后，使用菜单*警报（原有）*部分中的选项。</p> <p>"管理警报（旧系统）"</p>
我需要哪些用户组权限？	<ul style="list-style-type: none"> 可以登录到网格管理器的任何人都可以查看当前警报和已解决警报。 您必须具有管理警报权限才能管理静音、警报通知和警报规则。 <p>"管理 StorageGRID"</p>	<ul style="list-style-type: none"> 可以登录到网格管理器的任何人都可以查看旧警报。 您必须具有确认警报权限才能确认警报。 您必须同时具有网格拓扑页面配置和其他网格配置权限、才能管理全局警报和电子邮件通知。 <p>"管理 StorageGRID"</p>

	警报	警报 (旧系统)
如何管理电子邮件通知?	<p>选择 * 警报 * > * 电子邮件设置 *。</p> <ul style="list-style-type: none"> 注意：* 由于警报和警报是独立的系统，因此用于警报和 AutoSupport 通知的电子邮件设置不用于警报通知。但是，您可以对所有通知使用同一邮件服务器。 <p>"为警报设置电子邮件通知"</p>	<p>选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。</p> <p>"管理警报 (旧系统) "</p>
如何管理 SNMP 通知?	<p>选择 * 配置 * > * 监控 * > * SNMP 代理 *。</p> <p>"使用 SNMP 监控"</p>	不支持
如何控制谁接收通知?	<ol style="list-style-type: none"> 选择 * 警报 * > * 电子邮件设置 *。 在 * 收件人 * 部分中，为每个电子邮件列表或发生警报时应接收电子邮件的人员输入一个电子邮件地址。 <p>"为警报设置电子邮件通知"</p>	<ol style="list-style-type: none"> 选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。 创建邮件列表。 选择 * 通知 *。 选择邮件列表。 <p>"管理警报 (旧系统) "</p>
哪些管理节点会发送通知?	<p>一个管理节点(首选发送方)。</p> <p>"什么是管理节点? "</p>	<p>一个管理节点(首选发送方)。</p> <p>"什么是管理节点? "</p>
如何禁止某些通知?	<ol style="list-style-type: none"> 选择 * 警报 * > * 静音 *。 选择要静音的警报规则。 指定静音的持续时间。 选择要静音的警报的严重性。 选择可对整个网格，单个站点或单个节点应用静音。 <ul style="list-style-type: none"> 注 *：如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 <p>"静音警报通知"</p>	<ol style="list-style-type: none"> 选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。 选择 * 通知 *。 选择一个邮件列表，然后选择 * 禁止 *。 <p>"管理警报 (旧系统) "</p>

	警报	警报 (旧系统)
如何禁止所有通知?	<p>选择 * 警报 * > * 静音 *。然后选择 * 所有规则 *。</p> <ul style="list-style-type: none"> 注 *：如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 <p>"静默警报通知"</p>	不支持
如何自定义条件和触发器?	<ol style="list-style-type: none"> 选择 * 警报 * > * 规则 *。 选择要编辑的默认规则，或者选择 * 创建自定义规则 *。 <p>"编辑警报规则"</p> <p>"创建自定义警报规则"</p>	<ol style="list-style-type: none"> 选择 * 支持 * > * 警报 (原有) * > * 全局警报 *。 创建全局自定义警报以覆盖默认警报或监控没有默认警报的属性。 <p>"管理警报 (旧系统) "</p>
如何禁用单个警报?	<ol style="list-style-type: none"> 选择 * 警报 * > * 规则 *。 选择规则，然后选择 * 编辑规则 *。 清除 *Enabled*(已启用)复选框。 <p>"禁用警报规则"</p>	<ol style="list-style-type: none"> 选择 * 支持 * > * 警报 (原有) * > * 全局警报 *。 选择规则，然后选择编辑图标。 清除 *Enabled*(已启用)复选框。 <p>"管理警报 (旧系统) "</p>

管理警报

管理警报：概述

警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

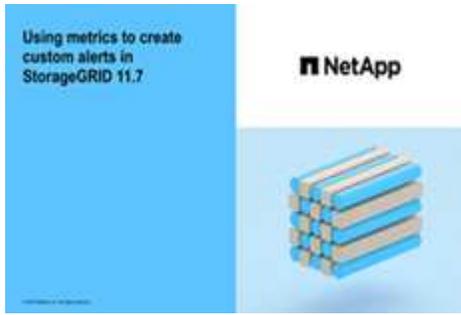
您可以创建自定义警报、编辑或禁用警报以及管理警报通知。

了解更多信息：

- 观看视频： ["视频： StorageGRID 11.7的警报概述"](#)



- 观看视频: ["视频: 在StorageGRID 11.7中使用指标创建自定义警报"](#)



- 请参见 ["警报参考"](#)。

查看警报规则

警报规则用于定义触发的条件 **"特定警报"**。StorageGRID 包含一组默认警报规则，您可以按原定义使用或修改这些规则，也可以创建自定义警报规则。

您可以查看所有默认和自定义警报规则的列表，以了解将触发每个警报的条件以及是否已禁用任何警报。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或root访问权限。
- 您也可以观看以下视频: ["视频: StorageGRID 11.7的警报概述"](#)



步骤

1. 选择 *** 警报 *** > *** 规则 ***。

此时将显示 "Alert Rules" 页面。

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

Name	Conditions	Type	Status
<input type="radio"/> Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
<input type="radio"/> Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. 查看警报规则表中的信息：

列标题	Description
Name	警报规则的唯一名称和问题描述。首先列出自定义警报规则，然后列出默认警报规则。警报规则名称是电子邮件通知的主题。
条件	<p>用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。</p> <ul style="list-style-type: none"> * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述。如果未解决问题描述，可能会导致服务中断和数据丢失。 * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决无法自行清除的次要警报，以确保它们不会导致更严重的问题。

列标题	Description
Type	<p>警报规则的类型：</p> <ul style="list-style-type: none"> • * 默认 *：随系统提供的警报规则。您可以禁用默认警报规则或编辑默认警报规则的条件和持续时间。您无法删除默认警报规则。 • * 默认值 *：包含已编辑条件或持续时间的默认警报规则。根据需要，您可以轻松地将修改后的条件还原回原始默认值。 • * 自定义 *：创建的警报规则。您可以禁用，编辑和删除自定义警报规则。
Status	<p>当前是否已启用此警报规则。系统不会评估已禁用警报规则的条件、因此不会触发警报。</p>

创建自定义警报规则

您可以创建自定义警报规则来定义自己触发警报的条件。

开始之前

- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)
- 您具有管理警报或root访问权限
- 您熟悉 ["常用的 Prometheus 指标"](#)
- 您了解 ["Prometheus 查询的语法"](#)
- 您也可以观看以下视频：["视频：在StorageGRID 11.7中使用指标创建自定义警报"](#)



关于此任务

StorageGRID 不会验证自定义警报。如果您决定创建自定义警报规则，请遵循以下一般准则：

- 查看默认警报规则的条件，并将其用作自定义警报规则的示例。
- 如果为警报规则定义了多个条件，请对所有条件使用相同的表达式。然后，更改每个条件的阈值。
- 仔细检查每个条件是否存在拼写错误和逻辑错误。
- 请仅使用网格管理 API 中列出的指标。
- 在网格管理API测试表达式时、请注意、"成功"响应可能是空响应正文(未触发警报)。要查看警报是否实际触发，您可以临时将阈值设置为您希望当前为 true 的值。

例如、用于测试表达式 `node_memory_MemTotal_bytes < 24000000000`、请先执行 `node_memory_MemTotal_bytes >= 0` 并确保获得预期结果(所有节点均返回一个值)。然后，将运算符和阈值改回预期值并重新执行。无结果表明此表达式当前没有警报。

- 除非您已验证自定义警报是按预期触发的、否则不要假定该警报正常工作。

步骤

1. 选择 * 警报 * > * 规则 *。

此时将显示 "Alert Rules" 页面。

2. 选择 * 创建自定义规则 *。

此时将显示创建自定义规则对话框。

Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions (optional)

Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

3. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。

4. 输入以下信息：

字段	Description
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
Description	所发生问题的问题描述。问题描述是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1,024 个字符之间。

5. 在条件部分中，为一个或多个警报严重性级别输入一个 Prometheus 表达式。

基本表达式通常采用以下形式：

```
[metric] [operator] [value]
```

表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

如果节点的已安装 RAM 量小于 24,000,000,000 字节（24 GB），则此表达式会触发警报。

```
node_memory_MemTotal_bytes < 24000000000
```

要查看可用指标并测试 Prometheus 表达式，请选择帮助图标  并单击网络管理 API 中的指标部分链接。

6. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的的时间量，然后选择一个时间单位。

要在条件变为 true 时立即触发警报，请输入 *。增加此值可防止临时条件触发警报。

默认值为 5 分钟。

7. 选择 * 保存 *。

此时，对话框将关闭，新的自定义警报规则将显示在 "Alert Rules" 表中。

编辑警报规则

您可以编辑警报规则以更改触发条件，对于自定义警报规则，您还可以更新规则名称，问题描述 和建议的操作。

开始之前

- 您将使用登录到网络管理器 [支持的 Web 浏览器](#)。
- 您具有管理警报或root访问权限。

关于此任务

编辑默认警报规则时，您可以更改次要警报，主要警报和严重警报的条件以及持续时间。编辑自定义警报规则时，您还可以编辑规则的名称，问题描述 和建议的操作。



决定编辑警报规则时请务必小心。如果更改了触发值，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

1. 选择 * 警报 * > * 规则 * 。

此时将显示 "Alert Rules" 页面。

2. 选择要编辑的警报规则对应的单选按钮。
3. 选择 * 编辑规则 * 。

此时将显示编辑规则对话框。此示例显示了一个默认警报规则：“唯一名称”、“问题描述 ”和“建议操作”字段已禁用，无法编辑。

Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional) VMware installation- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)
"/>

Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

4. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。



如果您对当前警报禁用警报规则，则必须等待几分钟，使警报不再显示为活动警报。



通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

5. 对于自定义警报规则，请根据需要更新以下信息。



您无法编辑默认警报规则的此信息。

字段	Description
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
Description	所发生问题的问题描述。问题描述是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1,024 个字符之间。

6. 在条件部分中，输入或更新一个或多个警报严重性级别的 Prometheus 表达式。



如果要已将编辑默认警报规则的条件还原为其原始值，请选择已修改条件右侧的三个点。

Conditions

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes < 24000000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes <= 14000000000"/>



如果您更新了当前警报的条件，则在解决上一条件之前，可能无法实施您所做的更改。下次满足规则的其中一个条件时，警报将反映更新后的值。

基本表达式通常采用以下形式：

```
[metric] [operator] [value]
```

表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

如果节点的已安装 RAM 量小于 24,000,000,000 字节（24 GB），则此表达式会触发警报。

```
node_memory_MemTotal_bytes < 24000000000
```

7. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的的时间量，然后选择时间单位。

要在条件变为 true 时立即触发警报，请输入 *。增加此值可防止临时条件触发警报。

默认值为 5 分钟。

8. 选择 * 保存 *。

如果您编辑了默认警报规则，则 "Type" 列中将显示 "* 默认值"。如果禁用了默认或自定义警报规则，* 状态 * 列中将显示 * 已禁用 *。

禁用警报规则

您可以更改默认或自定义警报规则的启用 / 禁用状态。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或root访问权限。

关于此任务

禁用警报规则后、不会对其表达式进行评估、也不会触发警报。



通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

1. 选择 * 警报 * > * 规则 *。

此时将显示 "Alert Rules" 页面。

2. 选择要禁用或启用的警报规则对应的单选按钮。

3. 选择 * 编辑规则 *。

此时将显示编辑规则对话框。

4. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。



如果您对当前警报禁用警报规则，则必须等待几分钟，以使警报不再显示为活动警报。

5. 选择 * 保存 *。

- 已禁用 * 显示在 * 状态 * 列中。

删除自定义警报规则

如果您不想再使用自定义警报规则，可以将其删除。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或root访问权限。

步骤

1. 选择 * 警报 * > * 规则 *。

此时将显示 "Alert Rules" 页面。

2. 选择要删除的自定义警报规则对应的单选按钮。

您无法删除默认警报规则。

3. 选择 * 删除自定义规则 *。

此时将显示确认对话框。

4. 选择 * 确定 * 以删除警报规则。

任何处于活动状态的警报实例将在 10 分钟内得到解决。

管理警报通知

为警报设置 **SNMP** 通知

如果您希望 StorageGRID 在发生警报时发送 SNMP 通知，则必须启用 StorageGRID SNMP 代理并配置一个或多个陷阱目标。

您可以使用网络管理器中的 * 配置 * > * 监控 * > * SNMP 代理 * 选项或网络管理 API 的 SNMP 端点来启用和配置 StorageGRID SNMP 代理。SNMP 代理支持所有三个版本的 SNMP 协议。

要了解如何配置 SNMP 代理，请参见 ["使用 SNMP 监控"](#)。

配置 StorageGRID SNMP 代理后，可以发送两种类型的事件驱动型通知：

- 陷阱是由SNMP代理发送的通知、不需要管理系统进行确认。陷阱用于通知管理系统 StorageGRID 中发生了某种情况，例如触发警报。所有三个版本的 SNMP 均支持陷阱。
- 通知与陷阱类似，但需要管理系统确认。如果 SNMP 代理未在特定时间内收到确认，则会重新发送通知，直到收到确认或达到最大重试值为止。SNMPv2c 和 SNMPv3 支持 INFORM。

在任何严重性级别触发默认或自定义警报时，系统都会发送陷阱和通知通知。要禁止警报的 SNMP 通知，您必须为此警报配置静默。请参见 ["静默警报通知"](#)。

如果您的StorageGRID 部署包含多个管理节点、则主管理节点是警报通知、AutoSupport 消息、SNMP陷阱和通知以及原有警报通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参见 ["什么是管理节点?"](#)。

为警报设置电子邮件通知

如果您希望在出现警报时发送电子邮件通知，则必须提供有关 SMTP 服务器的信息。您还必须输入警报通知收件人的电子邮件地址。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或root访问权限。

关于此任务

由于警报和警报是独立的系统，因此用于警报通知的电子邮件设置不会用于警报通知和 AutoSupport 消息。但是，您可以对所有通知使用同一个电子邮件服务器。

如果您的StorageGRID 部署包含多个管理节点、则主管理节点是警报通知、AutoSupport 消息、SNMP陷阱和通知以及原有警报通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参见 ["什么是管理节点？"](#)。

步骤

1. 选择 * 警报 * > * 电子邮件设置 *。

此时将显示电子邮件设置页面。

Email Setup

You can configure the email server for alert notifications, define filters to limit the number of notifications, and enter email addresses for alert recipients.

Use these settings to define the email server used for alert notifications. These settings are not used for alarm notifications and AutoSupport. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID.](#)

Enable Email Notifications

Save

2. 选中*启用电子邮件通知*复选框以指示您希望在警报达到配置的阈值时发送通知电子邮件。

此时将显示电子邮件（SMTP）服务器，传输层安全（TLS），电子邮件地址和筛选器部分。

3. 在电子邮件（SMTP）服务器部分中，输入 StorageGRID 访问 SMTP 服务器所需的信息。

如果 SMTP 服务器需要身份验证，则必须同时提供用户名和密码。

字段	输入 ...
邮件服务器	SMTP 服务器的完全限定域名（FQDN）或 IP 地址。
Port	用于访问 SMTP 服务器的端口。必须介于 1 到 65535 之间。
用户名（可选）	如果 SMTP 服务器需要身份验证，请输入要进行身份验证的用户名。

字段	输入 ...
密码 (可选)	如果 SMTP 服务器需要身份验证, 请输入用于进行身份验证的密码。

Email (SMTP) Server

Mail Server 	<input type="text" value="10.224.1.250"/>
Port 	<input type="text" value="25"/>
Username (optional) 	<input type="text" value="smtpuser"/>
Password (optional) 	<input type="password" value="*****"/>

4. 在电子邮件地址部分中, 输入发件人和每个收件人的电子邮件地址。
 - a. 对于 * 发件人电子邮件地址 *, 请指定一个有效的电子邮件地址, 用作警报通知的发件人地址。
例如: storagegrid-alerts@example.com
 - b. 在收件人部分中, 为每个电子邮件列表或发生警报时应接收电子邮件的人员输入电子邮件地址。
选择加号图标 **+** 以添加收件人。

Email Addresses

Sender Email Address 	<input type="text" value="storagegrid-alerts@example.com"/>	
Recipient 1 	<input type="text" value="recipient1@example.com"/>	
Recipient 2 	<input type="text" value="recipient2@example.com"/>	 

5. 如果要与 SMTP 服务器进行通信, 需要使用传输层安全 (TLS), 请在传输层安全 (TLS) 部分中选择 * 需要 TLS*。
 - a. 在 * CA 证书 * 字段中, 提供用于验证 SMTP 服务器标识的 CA 证书。
您可以将内容复制并粘贴到此字段中, 或者选择 * 浏览 * 并选择文件。

您必须提供一个文件, 其中包含来自每个中间颁发证书颁发机构 (CA) 的证书。此文件应包含 PEM 编码的每个 CA 证书文件, 并按证书链顺序串联。
 - b. 如果SMTP电子邮件服务器要求电子邮件发件人提供客户端证书以进行身份验证, 请选中*发送客户端证书*复选框。
 - c. 在 * 客户端证书 * 字段中, 提供 PEM 编码的客户端证书以发送到 SMTP 服务器。

您可以将内容复制并粘贴到此字段中, 或者选择 * 浏览 * 并选择文件。

d. 在 * 专用密钥 * 字段中, 输入未加密 PEM 编码的客户端证书的专用密钥。

您可以将内容复制并粘贴到此字段中, 或者选择 * 浏览 * 并选择文件。



如果需要编辑电子邮件设置, 请选择铅笔图标以更新此字段。

Transport Layer Security (TLS)

Require TLS

CA Certificate

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Send Client Certificate

Client Certificate

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Private Key

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890  
-----BEGIN PRIVATE KEY-----
```

Browse

6. 在筛选器部分中, 选择应导致电子邮件通知的警报严重性级别, 除非特定警报的规则已被静音。

severity	Description
次要, 重大, 严重	满足警报规则的次要, 主要或严重条件时, 系统会发送电子邮件通知。
主要, 关键	当满足警报规则的主要或关键条件时, 系统会发送电子邮件通知。不会针对次要警报发送通知。

severity	Description
仅严重	只有在满足警报规则的严重条件时，才会发送电子邮件通知。不会针对次要或重大警报发送通知。

Filters

Severity ⓘ Minor, major, critical Major, critical Critical only

Send Test Email

Save

7. 准备好测试电子邮件设置后，请执行以下步骤：

a. 选择 * 发送测试电子邮件 *。

此时将显示一条确认消息，指示已发送测试电子邮件。

b. 检查所有电子邮件收件人的收件箱，确认已收到测试电子邮件。



如果在几分钟内未收到电子邮件，或者触发了 * 电子邮件通知失败 * 警报，请检查您的设置并重试。

c. 登录到任何其他管理节点并发送测试电子邮件以验证所有站点的连接。



在测试警报通知时，您必须登录到每个管理节点以验证连接。这与测试AutoSupport 消息和传统警报通知不同、在测试中、所有管理节点都会发送测试电子邮件。

8. 选择 * 保存 *。

发送测试电子邮件不会保存您的设置。您必须选择 * 保存 *。

此时将保存电子邮件设置。

警报电子邮件通知中包含的信息

配置 SMTP 电子邮件服务器后，在触发警报时，系统会向指定的收件人发送电子邮件通知，除非警报规则被静默禁止。请参见 "[静默警报通知](#)"。

电子邮件通知包括以下信息：

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

5

Sent from: DC1-ADM1-225

Callout	Description
1.	警报名称，后跟此警报的活动实例数。
2.	警报的问题描述。
3.	为警报建议的任何操作。
4.	有关警报的每个活动实例的详细信息，包括受影响的节点和站点，警报严重性，触发警报规则的 UTC 时间以及受影响作业和服务的名称。
5.	发送通知的管理节点的主机名。

如何对警报进行分组

为了防止在触发警报时发送过多的电子邮件通知，StorageGRID 会尝试在同一通知中对多个警报进行分组。

有关 StorageGRID 如何在电子邮件通知中对多个警报进行分组的示例，请参见下表。

行为	示例
每个警报通知仅适用于同名警报。如果同时触发两个名称不同的警报，则会发送两封电子邮件通知。	<ul style="list-style-type: none"> • 警报 A 会同时在两个节点上触发。仅发送一个通知。 • 节点 1 上触发警报 A，节点 2 上同时触发警报 B。系统会发送两个通知—每个警报一个。
对于特定节点上的特定警报，如果达到阈值的严重性超过一个，则仅针对最严重警报发送通知。	<ul style="list-style-type: none"> • 此时将触发警报 A，并达到次要，主要和严重警报阈值。系统会为严重警报发送一条通知。
首次触发警报时，StorageGRID 会等待 2 分钟，然后再发送通知。如果在此期间触发了其他同名警报，则 StorageGRID 会在初始通知中对所有警报进行分组。	<ol style="list-style-type: none"> 1. 节点 1 上的警报 A 在 08：00 触发。不会发送任何通知。 2. 节点 2 上的警报 A 在 08：01 触发。不会发送任何通知。 3. 8：02 发送通知以报告两个警报实例。
如果触发另一个同名警报，StorageGRID 将等待 10 分钟，然后再发送新通知。新通知会报告所有活动警报（当前未静音的警报），即使先前已报告这些警报也是如此。	<ol style="list-style-type: none"> 1. 节点 1 上的警报 A 在 08：00 触发。通知在 08：02 发送。 2. 节点 2 上的警报 A 在 08：05 触发。第二个通知将在 8：15（10 分钟后）发送。此时将报告这两个节点。
如果当前存在多个同名警报且其中一个警报已解决，则在已解决警报的节点上重新出现此警报时，不会发送新通知。	<ol style="list-style-type: none"> 1. 已针对节点 1 触发警报 A。此时将发送通知。 2. 已针对节点 2 触发警报 A。此时将发送第二个通知。 3. 已解决节点 2 的警报 A，但此警报对于节点 1 仍处于活动状态。 4. 此时将再次触发节点 2 的警报 A。不会发送任何新通知，因为此警报对于节点 1 仍处于活动状态。
StorageGRID 会继续每 7 天发送一次电子邮件通知，直到所有警报实例均已解决或警报规则已静音为止。	<ol style="list-style-type: none"> 1. 3 月 8 日为节点 1 触发警报 A。此时将发送通知。 2. 警报 A 未解决或静音。其他通知将于 3 月 15 日，3 月 22 日，3 月 29 日等时间发送。

对警报电子邮件通知进行故障排除

如果触发了 * 电子邮件通知失败 * 警报，或者您无法收到测试警报电子邮件通知，请按照以下步骤解决问题描述。

开始之前

- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或 root 访问权限。

步骤

1. 验证设置。
 - a. 选择 * 警报 * > * 电子邮件设置 *。
 - b. 验证电子邮件（SMTP）服务器设置是否正确。
 - c. 验证您是否为收件人指定了有效的电子邮件地址。
2. 检查垃圾邮件筛选器，确保电子邮件未发送到垃圾文件夹。
3. 请您的电子邮件管理员确认来自发件人地址的电子邮件未被阻止。
4. 收集管理节点的日志文件，然后联系技术支持。

技术支持可以使用日志中的信息帮助确定出现问题的原因。例如，prometheus.log 文件在连接到您指定的服务器时可能会显示错误。

请参见 ["收集日志文件和系统数据"](#)。

静默警报通知

或者，您也可以配置静音以临时禁止警报通知。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您具有管理警报或root访问权限。

关于此任务

您可以对整个网络，单个站点或单个节点以及一个或多个严重性静默警报规则。每次静默都将禁止针对单个警报规则或所有警报规则发出所有通知。

如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。



在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。



由于警报和警报是独立的系统、因此不能使用此功能来禁止警报通知。

步骤

1. 选择 * 警报 * > * 静音 *。

此时将显示 Silences 页面。

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create Edit Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
<i>No results found.</i>				

2. 选择 * 创建 *。

此时将显示创建静默对话框。

Create Silence

Alert Rule

Description (optional)

Duration

Severity Minor only Minor, major Minor, major, critical

Nodes StorageGRID Deployment

- Data Center 1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3

3. 选择或输入以下信息：

字段	Description
警报规则	要静默的警报规则的名称。您可以选择任何默认或自定义警报规则，即使警报规则已禁用也是如此。 • 注： * 如果要使用此对话框中指定的标准将所有警报规则静默，请选择 * 所有规则 *。
Description	也可以选择静默问题描述。例如，请描述此静默的目的。

字段	Description
Duration	<p>希望此静默保持有效的时间，以分钟，小时或天为单位。静默时间为 5 分钟到 1,825 天（5 年）。</p> <ul style="list-style-type: none"> 注意：* 不应将警报规则静默较长时间。如果某个警报规则已静音，则在阻止完成关键操作之前，您可能无法检测到潜在问题。但是，如果警报是由特定的有意配置触发的，则可能需要使用长时间静默，例如，"* 服务设备链路已关闭 " 警报和 "* 存储设备链路已关闭 " 警报可能会出现这种情况。
severity	<p>应将哪个警报严重性或严重性静音。如果在选定严重性之一触发警报，则不会发送任何通知。</p>
节点	<p>您希望此静默应用于哪个或哪些节点。您可以禁止整个网格，单个站点或单个节点上的警报规则或所有规则。如果选择整个网格，则会将适用场景 静默所有站点和所有节点。如果选择站点，则此静默状态仅适用于该站点上的节点。</p> <p>*注意：*每次静默不能选择多个节点或多个站点。如果要同时在多个节点或多个站点上禁止相同的警报规则，则必须创建其他静音。</p>

4. 选择 * 保存 *。

5. 如果要在静默过期之前修改或结束静默，可以对其进行编辑或删除。

选项	Description
编辑静默	<ol style="list-style-type: none"> 选择 * 警报 * > * 静音 *。 从表中，选择要编辑的静默设置对应的单选按钮。 选择 * 编辑 *。 更改问题描述，剩余时间，选定严重性或受影响的节点。 选择 * 保存 *。
取消静默	<ol style="list-style-type: none"> 选择 * 警报 * > * 静音 *。 从表中，选择要删除的静默设置对应的单选按钮。 选择 * 删除 *。 选择 * 确定 * 确认要删除此静默状态。 <p>。注意*：现在，在触发此警报时，系统将发送通知（除非被另一个静默禁止）。如果当前触发此警报，则发送电子邮件或 SNMP 通知以及更新警报页面可能需要几分钟的时间。</p>

相关信息

- ["配置 SNMP 代理"](#)

警报参考

此参考列出了网格管理器中显示的默认警报。建议的操作会显示在您收到的警报消息中。

您可以根据需要创建自定义警报规则，以适合您的系统管理方法。

某些默认警报使用 ["Prometheus 指标"](#)。

设备警报

警报名称	Description
设备电池已过期	设备存储控制器中的电池已过期。
设备电池出现故障	设备存储控制器中的电池出现故障。
设备电池的已学习容量不足	设备存储控制器中的电池已获取容量不足。
设备电池即将过期	设备存储控制器中的电池即将过期。
已取出设备电池	设备存储控制器中的电池缺失。
设备电池过热	设备存储控制器中的电池过热。
设备 BMC 通信错误	与基板管理控制器（BMC）的通信已丢失。
设备缓存备份设备失败	永久性缓存备份设备出现故障。
设备缓存备份设备容量不足	缓存备份设备容量不足。
设备缓存备份设备已写保护	缓存备份设备受写保护。
设备缓存内存大小不匹配	设备中的两个控制器具有不同的缓存大小。
设备计算控制器机箱温度过高	StorageGRID 设备中计算控制器的温度已超过额定阈值。
设备计算控制器 CPU 温度过高	StorageGRID 设备中计算控制器的 CPU 温度已超过额定阈值。
设备计算控制器需要引起注意	在 StorageGRID 设备的计算控制器中检测到硬件故障。
设备计算控制器电源 A 出现问题	计算控制器中的电源A出现问题。
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。

警报名称	Description
设备计算硬件监控服务已停止	监控存储硬件状态的服务已停止。
检测到设备DAS驱动器故障	检测到设备中的直连存储(DAS)驱动器存在问题。
设备DAS驱动器正在重建	正在重建直连存储(DAS)驱动器。如果最近更换或移除/重新插入、则这是预期的。
检测到设备风扇故障	检测到产品中的风扇装置有问题。
检测到设备光纤通道故障	检测到设备存储控制器与计算控制器之间存在光纤通道链路问题
设备光纤通道 HBA 端口故障	光纤通道 HBA 端口出现故障或出现故障。
设备闪存缓存驱动器非最佳	用于 SSD 缓存的驱动器并非最佳驱动器。
已卸下设备互连 / 电池箱	互连 / 电池箱缺失。
缺少设备 LACP 端口	StorageGRID 设备上的端口不参与 LACP 绑定。
检测到设备NIC故障	检测到设备中的网络接口卡(NIC)有问题。
设备整体电源性能下降	StorageGRID 设备的电源已偏离建议的工作电压。
设备SSD严重警告	设备SSD报告严重警告。
设备存储控制器 A 出现故障	StorageGRID 设备中的存储控制器 A 出现故障。
设备存储控制器 B 故障	StorageGRID 设备中的存储控制器 B 出现故障。
设备存储控制器驱动器故障	StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器。
设备存储控制器硬件问题描述	SANtricity 软件报告 StorageGRID 设备中的某个组件 " 需要关注 " 。
设备存储控制器电源 A 出现故障	StorageGRID 设备中的电源 A 与建议的工作电压不同。
设备存储控制器电源 B 故障	StorageGRID 设备中的电源 B 与建议的工作电压不同。
设备存储硬件监控服务已停止	监控存储硬件状态的服务已停止。
设备存储架降级	存储设备存储架中某个组件的状态为已降级。

警报名称	Description
已超过设备温度	已超过设备存储控制器的额定或最大温度。
已卸下设备温度传感器	已卸下温度传感器。
磁盘 I/O 速度非常慢	磁盘 I/O 非常慢可能会影响网络性能。
检测到存储设备风扇故障	检测到设备存储控制器中的风扇单元出现问题。
存储设备存储连接已降级	计算控制器和存储控制器之间的一个或多个连接出现问题。
无法访问存储设备	无法访问存储设备。

审核和系统日志警报

警报名称	Description
正在将审核日志添加到内存队列中	节点无法将日志发送到本地系统日志服务器、并且内存队列已满。
外部系统日志服务器转发错误	节点无法将日志转发到外部系统日志服务器。
审核队列较大	审核消息的磁盘队列已满。如果不解决此问题、S3或Swift操作可能会失败。
正在将日志添加到磁盘队列中	节点无法将日志转发到外部系统日志服务器、并且磁盘队列已满。

存储分段警报

警报名称	Description
FabricPool 存储分段具有不受支持的存储分段一致性设置	FabricPool 存储分段使用可用的一致性级别、此级别不受支持。

Cassandra警报

警报名称	Description
Cassandra auto-compactor 错误	Cassandra 自动 compactor 出现错误。
Cassandra 自动数据压缩器指标已过期	描述 Cassandra 自动数据压缩器的指标已过时。
Cassandra 通信错误	运行 Cassandra 服务的节点无法彼此通信。

警报名称	Description
Cassandra compActions 已过载	Cassandra 数据缩减过程过载。
Cassandra 特写错误	内部StorageGRID 进程向Cassandra发送了一个过大的写入请求。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过时。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度缓慢。
Cassandra 修复服务不可用	Cassandra 修复服务不可用。
Cassandra 表损坏	Cassandra 检测到表损坏。如果 Cassandra 检测到表损坏，则它会自动重新启动。
已禁用改进的读取可用性	如果禁用了改进的读取可用性、则在存储节点不可用时、获取和机头请求可能会失败。

云存储池警报

警报名称	Description
云存储池连接错误	云存储池的运行状况检查检测到一个或多个新错误。

跨网格复制警报

警报名称	Description
跨网格复制永久失败	发生跨网格复制错误、需要用户干预才能解决。
跨网格复制资源不可用	由于资源不可用、跨网格复制请求处于待处理状态。

DHCP警报

警报名称	Description
DHCP 租约已过期	网络接口上的 DHCP 租约已过期。
DHCP 租约即将到期	网络接口上的 DHCP 租约即将到期。
DHCP 服务器不可用	DHCP 服务器不可用。

调试和跟踪警报

警报名称	Description
调试性能影响	启用调试模式后、系统性能可能会受到负面影响。
已启用跟踪配置	启用跟踪配置后、系统性能可能会受到负面影响。

电子邮件和AutoSupport 警报

警报名称	Description
无法发送AutoSupport 消息	无法发送最新的AutoSupport 消息。
电子邮件通知失败	无法发送警报电子邮件通知。

纠删编码(EC)警报

警报名称	Description
EC 重新平衡失败	EC重新平衡操作步骤 失败或已停止。
EC 修复失败	EC数据的修复作业失败或已停止。
EC 修复已停止	EC数据的修复作业已停止。

证书到期警报

警报名称	Description
客户端证书到期	一个或多个客户端证书即将过期。
S3和Swift的全局服务器证书到期	S3和Swift的全局服务器证书即将过期。
负载均衡器端点证书到期	一个或多个负载均衡器端点证书即将过期。
管理接口的服务器证书到期	用于管理接口的服务器证书即将过期。
外部系统日志 CA 证书到期	用于签署外部系统日志服务器证书的证书颁发机构（CA）证书即将过期。
外部系统日志客户端证书到期	外部系统日志服务器的客户端证书即将过期。
外部系统日志服务器证书到期	外部系统日志服务器提供的服务器证书即将过期。

网格网络警报

警报名称	Description
网格网络 MTU 不匹配	网格网络接口(eth0)的MTU设置在网格中的各个节点之间差别很大。

网格联盟警报

警报名称	Description
网格联合证书到期	一个或多个网格联合证书即将过期。
网格联合连接失败	本地网格与远程网格之间的网格联合连接不起作用。

高使用量或高延迟警报

警报名称	Description
Java 堆使用率较高	正在使用的 Java 堆空间百分比很高。
元数据查询延迟较长	Cassandra 元数据查询的平均时间过长。

身份联合警报

警报名称	Description
身份联合同步失败	无法从身份源同步联合组和用户。
租户的身份联合同步失败	无法从租户配置的身份源同步联合组和用户。

信息生命周期管理(ILM)警报

警报名称	Description
无法实现 ILM 放置	无法为某些对象实现ILM规则中的放置指令。
ILM 扫描周期过长	扫描、评估ILM并将其应用于对象所需的时间过长。
ILM 扫描速率低	ILM 扫描速率设置为每秒不到 100 个对象。

密钥管理服务器(KMS)警报

警报名称	Description
Kms CA 证书到期	用于对密钥管理服务器（KMS）证书进行签名的证书颁发机构（CA）证书即将过期。
Kms 客户端证书到期	密钥管理服务器的客户端证书即将过期
无法加载 Kms 配置	密钥管理服务器的配置存在，但无法加载。
Kms 连接错误	设备节点无法连接到其站点的密钥管理服务器。
未找到 Kms 加密密钥名称	配置的密钥管理服务器没有与提供的名称匹配的加密密钥。
Kms 加密密钥轮换失败	所有设备卷均已成功解密、但一个或多个卷无法转换为最新密钥。
未配置公里	此站点不存在密钥管理服务器。
Kms 密钥无法对设备卷进行解密	无法使用当前 KMS 密钥对启用了节点加密的设备上的一个或多个卷进行解密。
Kms 服务器证书到期	密钥管理服务器（KMS）使用的服务器证书即将过期。

本地时钟偏移警报

警报名称	Description
本地时钟大时间偏移	本地时钟和网络时间协议(NTP)时间之间的偏移过大。

内存不足或空间不足警报

警报名称	Description
审核日志磁盘容量低	可用于审核日志的空间不足。如果不解决此问题、S3或Swift操作可能会失败。
可用节点内存不足	节点上的可用 RAM 量较低。
存储池可用空间不足	存储节点中可用于存储对象数据的空间不足。
节点内存不足	节点上安装的内存量不足。
元数据存储不足	可用于存储对象元数据的空间不足。
低指标磁盘容量	可用于指标数据库的空间不足。

警报名称	Description
对象数据存储不足	可用于存储对象数据的空间不足。
低只读水印覆盖	存储卷软只读水印覆盖小于存储节点的最小优化水印。
根磁盘容量低	根磁盘上的可用空间不足。
系统数据容量低	/var/local挂载点上可用于StorageGRID 系统数据的空间不足。
tmp 目录可用空间不足	/tmp 目录中的可用空间不足。

节点或节点网络警报

警报名称	Description
防火墙配置失败	无法应用防火墙配置。
节点网络连接错误	在节点之间传输数据时出错。
节点网络接收帧错误	节点收到的网络帧中有很高比例出现错误。
节点与 NTP 服务器不同步	此节点与网络时间协议(NTP)服务器不同步。
节点未使用 NTP 服务器锁定	节点未锁定到网络时间协议（NTP）服务器。
非设备节点网络已关闭	一个或多个网络设备已关闭或断开连接。
管理网络上的服务设备链接已关闭	管理网络(eth1)的设备接口已关闭或断开连接。
管理网络端口 1 上的服务设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。
客户端网络上的服务设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。
网络端口1上的服务设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的服务设备链路已关闭	设备上的网络端口2已关闭或断开连接。
网络端口3上的服务设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的服务设备链路关闭	设备上的网络端口4已关闭或断开连接。

警报名称	Description
管理网络上的存储设备链路关闭	管理网络(eth1)的设备接口已关闭或断开连接。
管理网络端口 1 上的存储设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。
客户端网络上的存储设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。
网络端口1上的存储设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的存储设备链路关闭	设备上的网络端口2已关闭或断开连接。
网络端口3上的存储设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的存储设备链路关闭	设备上的网络端口4已关闭或断开连接。
存储节点未处于所需的存储状态	由于内部错误或与卷相关的问题描述、存储节点上的LDR服务无法过渡到所需状态
无法与节点通信	一个或多个服务无响应或无法访问此节点。
节点意外重新启动	节点在过去 24 小时内意外重新启动。

对象警报

警报名称	Description
对象存在检查失败	对象存在检查作业失败。
对象存在检查已停止	对象存在检查作业已停止。
对象丢失	一个或多个对象已从网格中丢失。
S3放置对象大小太大	客户端尝试的Put Object操作超出S3大小限制。
检测到未标识的损坏对象	在复制的对象存储中找到无法标识为复制对象的文件。

平台服务警报

警报名称	Description
平台服务不可用	具有 RSM 服务的存储节点在站点上运行或可用的数量太少。

存储卷警报

警报名称	Description
存储卷需要引起注意	存储卷已脱机、需要引起注意。
需要还原存储卷	存储卷已恢复、需要还原。
存储卷脱机	某个存储卷已脱机5分钟以上、可能是因为这个节点在卷格式化步骤期间重新启动。
卷还原无法启动复制的数据修复	无法自动启动已修复卷的复制数据修复。

StorageGRID 服务警报

警报名称	Description
使用备份配置的NGinx服务	Nginx服务的配置无效。现在正在使用先前的配置。
使用备份配置的Ngins-GW服务	Ngins-GW服务的配置无效。现在正在使用先前的配置。
使用备份配置的SSH服务	SSH服务的配置无效。现在正在使用先前的配置。

租户警报

警报名称	Description
租户配额使用量高	正在使用的配额空间百分比较高。默认情况下、此规则处于禁用状态、因为它可能发生原因 会发送过多通知。

常用的 Prometheus 指标

请参阅此常用Prometheus指标列表、以更好地了解默认警报规则中的条件或构建自定义警报规则的条件。

您也可以 [获取所有指标的完整列表](#)。

有关Prometheus查询语法的详细信息、请参见 "[正在查询Prometheus](#)"。

什么是Prometheus指标？

Prometheus指标是时间序列测量值。管理节点上的Prometheus服务会从所有节点上的服务收集这些指标。指标会存储在每个管理节点上，直到为 Prometheus 数据预留的空间已满为止。当 `/var/local/mysql_ibdata/` 卷达到容量时、系统会先删除最早的指标。

Prometheus指标在哪里使用？

Prometheus收集的指标在网格管理器的多个位置使用：

- * 节点页面 *：节点页面上提供的选项卡上的图形和图表使用 Grafana 可视化工具显示 Prometheus 收集的时间序列指标。Grafana 以图形和图表格式显示时间序列数据，而 Prometheus 用作后端数据源。



- * 警报 *：如果使用 Prometheus 指标的警报规则条件评估为 true，则会在特定严重性级别触发警报。
- * 网格管理 API*：您可以在自定义警报规则中使用 Prometheus 指标，也可以使用外部自动化工具来监控 StorageGRID 系统。有关完整的 Prometheus 指标列表，请访问网格管理 API。(从网格管理器的顶部，选择帮助图标，然后选择*API documents*>*metrics*。)尽管有超过1000个指标可用、但监控最关键的StorageGRID 操作所需的指标数量相对较少。



名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

- 支持*>*工具*>*诊断*页面和*支持*>*工具*>*指标*页面：这些页面主要供技术支持使用，提供了多个使用 Prometheus 指标值的工具和图表。



指标页面中的某些功能和菜单项有意不起作用，可能会发生更改。

列出最常见的指标

以下列表包含最常用的 Prometheus 指标。



名称中包含 *_privly_* 的指标仅供内部使用、可能会在不同 StorageGRID 版本之间进行更改、恕不另行通知。

alertmanager_notifications_failed_total

失败警报通知的总数。

node_filesystem_avail_bytes

可供非root用户使用的文件系统空间量(以字节为单位)。

node_memory_MemAvailable_bytes

内存信息字段 MemAvailable_bytes。

node_network_Carrier

托架值为 /sys/class/net/iface。

node_network_receive ; errs_total

网络设备统计信息 receive_errs。

node_network_transmit_errs_total

网络设备统计信息 transmit_errs。

storaggrid_administratively 关闭

由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。

storagegrid_appliance_compute_controller_hardware_status

设备中计算控制器硬件的状态。

storagegrid_appliance_failed_disks

对于设备中的存储控制器、不是最佳驱动器的数量。

storagegrid_appliance_storage_controller_hardware_status

设备中存储控制器硬件的整体状态。

storagegrid_content_bages_and_containers

此存储节点已知的 S3 存储分段和 Swift 容器总数。

storaggrid_content_objects

此存储节点已知的 S3 和 Swift 数据对象总数。计数仅适用于通过 S3 或 Swift 与系统连接的客户端应用程序创建的数据对象。

storaggrid_content_objects_lost

此服务在 StorageGRID 系统中检测到缺失的对象总数。应采取措施确定丢失的发生原因 以及是否可以恢复。

["对丢失和丢失的对象数据进行故障排除"](#)

storagegrid_http_sessions_incoming_attempted

尝试访问存储节点的 HTTP 会话总数。

storagegrid_http_sessions_incoming_currently 已建立

存储节点上当前处于活动状态（已打开）的 HTTP 会话数。

storagegrid_http_sessions_incoming_failed

由于 HTTP 请求格式错误或在处理操作时失败而无法成功完成的 HTTP 会话总数。

storagegrid_http_sessions_incoming_successful

已成功完成的 HTTP 会话总数。

storaggrid_ilm_awaiting 背景对象

此节点上等待通过扫描进行 ILM 评估的对象总数。

storaggrid_ilm_awaiting 客户端评估对象每秒对象数

根据此节点上的 ILM 策略评估对象的当前速率。

storaggrid_ilm_awaiting 客户端对象

此节点上等待通过客户端操作进行 ILM 评估的对象总数（例如，载入）。

storaggrid_ilm_awaing_total_objects

等待 ILM 评估的对象总数。

storagegrid_ilm_scanned_objects_per_second

此节点拥有的对象在 ILM 中进行扫描和排队的速率。

storaggrid_ilm_scann_period_estimated_minutes

在此节点上完成完整 ILM 扫描的估计时间。

- 注：* 完全扫描并不能保证 ILM 已应用于此节点拥有的所有对象。

storagegrid_load_Balancer_endpoint_ct_expiry_time

负载均衡器端点证书自 Epoch 以来的到期时间（以秒为单位）。

storaggrid_metadata_queries_average ; latency ; 毫秒

通过此服务对元数据存储运行查询所需的平均时间。

storaggrid_network_received_bytes

自安装以来接收的总数据量。

storaggrid_network_transmated_bytes

自安装以来发送的总数据量。

storagegrid_node_cpu_utilization 百分比

此服务当前正在使用的可用 CPU 时间的百分比。指示服务的繁忙程度。可用 CPU 时间量取决于服务器的 CPU 数量。

storaggrid_ntp_chosed_time_source_offset_mms

选定时间源提供的系统时间偏移。如果到达某个时间源的延迟与该时间源到达 NTP 客户端所需的时间不相等，则会引入偏移。

storaggrid_ntp_locked

此节点未锁定到网络时间协议(NTP)服务器。

storaggrid_s3_data_transfers_bytes_ingested

自上次重置属性以来从 S3 客户端载入到此存储节点的总数据量。

已检索 storagegrid_s3_data_transfers_bytes_reRetrieved

自上次重置属性以来 S3 客户端从此存储节点检索的总数据量。

storaggrid_s3_operations_failed

S3 操作失败的总数（HTTP 状态代码 4xx 和 5xx），不包括因 S3 授权失败而导致的操作。

storaggrid_s3_operations_successful

成功执行 S3 操作的总数（HTTP 状态代码 2xx）。

storaggrid_s3_operations_unauthorized

授权失败导致的 S3 操作失败的总数。

storageRid_servercertificate_management_interface_cert_expiry_days

管理接口证书到期前的天数。

storageRid_servercertificate_storage_api_Endpoints" 证书到期日 "

对象存储 API 证书到期前的天数。

storaggrid_service_cpu_seconds

自安装以来此服务使用 CPU 的累积时间。

storagegrid_service_memory_usage_bytes

此服务当前正在使用的内存量（RAM）。此值与 Linux 顶部实用程序显示的值相同，即 Res。

storaggrid_service_network_received_bytes

自安装以来此服务收到的总数据量。

storaggrid_service_network_transmated_bytes

此服务发送的总数据量。

storagegrid_service_Restart

重新启动服务的总次数。

storaggrid_service_runtime_seconds

自安装以来服务一直运行的总时间量。

storaggrid_service_uptime_seconds

服务自上次重新启动以来的总运行时间。

storaggrid_storage_state_current

存储服务的当前状态。属性值为：

- 10 = 脱机
- 15 = 维护
- 20 = 只读
- 30 = 联机

storagegrid_storage_status

存储服务的当前状态。属性值为：

- 0 = 无错误

- 10 = 正在过渡
- 20 = 可用空间不足
- 30 = 卷不可用
- 40 = 错误

storagegrid存储利用率数据字节

存储节点上复制和擦除编码的对象数据的估计总大小。

storaggrid_storage_utilization metadata_allowed_bytes

每个存储节点的卷 0 上允许用于对象元数据的总空间。此值始终小于为节点上的元数据预留的实际空间，因为必要的数据库操作（如数据缩减和修复）以及未来的硬件和软件升级都需要预留部分空间。对象元数据允许的空间控制整体对象容量。

storaggrid_storage_utilization metadata_bytes

存储卷 0 上的对象元数据量，以字节为单位。

storaggrid_storage_utilization 总空间字节

分配给所有对象存储的存储空间总量。

storagegRid_storage_utilization_usable_space_bytes

剩余的对象存储空间总量。计算方法是将存储节点上所有对象存储的可用空间量相加。

storagegrid_swif_data_transfers_bytes_ingested

自上次重置属性以来从 Swift 客户端载入到此存储节点的总数据量。

已检索 storagegrid_swif_data_transfers_bytes_reRetrieved

自上次重置属性以来 Swift 客户端从此存储节点检索的总数据量。

storagegrid_swif_operations_failed

Swift 操作失败的总数（HTTP 状态代码 4xx 和 5xx），不包括因 Swift 授权失败而导致的操作。

storagegrid_swif_operations_successful

成功的 Swift 操作总数（HTTP 状态代码 2xx）。

storaggrid_swif_operations_unauthorized

授权失败导致的 Swift 操作失败的总数（HTTP 状态代码 401，403，405）。

storagegrid_tenant_usage_data_bytes

租户的所有对象的逻辑大小。

storagegrid_tenant_usage_object_count

租户的对象数。

storagegRid_tenant_usage_quota_bytes

可用于租户对象的最大逻辑空间量。如果未提供配额指标，则可用空间量不受限制。

获取所有指标的列表

[[obtain all-metrics]]要获取完整的指标列表、请使用网格管理API。

1. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
2. 找到 * 指标 * 操作。
3. 执行 GET /grid/metric-names 操作。
4. 下载结果。

管理警报（旧系统）

管理警报（旧系统）

StorageGRID 警报系统是一种传统系统，用于识别正常运行期间有时会出现的故障点。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

警报类（旧系统）

旧警报可以属于两个相互排斥的警报类之一。

- 每个StorageGRID 系统都提供了默认警报、无法修改。但是，您可以禁用默认警报或通过定义全局自定义警报来覆盖这些警报。
- 全局自定义警报可监控 StorageGRID 系统中给定类型的所有服务的状态。您可以创建全局自定义警报以覆盖默认警报。您还可以创建新的全局自定义警报。这对于监控 StorageGRID 系统的任何自定义条件非常有用。

警报触发逻辑（旧系统）

当 StorageGRID 属性达到阈值时，系统将触发传统警报，该阈值将根据警报类（默认或全局自定义）和警报严重性级别的组合计算为 true 。

图标。	颜色	警报严重性	含义
	黄色	通知	节点已连接到网格，但存在不影响正常操作的异常情况。
	浅橙色	次要	节点已连接到网格，但存在异常情况，可能会影响未来的运行。您应进行调查以防止上报。
	深橙色	major	节点已连接到网格，但存在当前影响操作的异常情况。这需要立即引起注意，以防止升级。
	红色	严重	节点已连接到网格，但存在已停止正常操作的异常情况。您应立即解决此问题描述。

可以为每个数字属性设置警报严重性和相应的阈值。每个管理节点上的 NMS 服务会根据已配置的阈值持续监控当前属性值。触发警报后，系统会向所有指定人员发送通知。

请注意，严重性级别为 " 正常 " 不会触发警报。

将根据为属性定义的已启用警报列表评估属性值。系统将按以下顺序检查警报列表，以查找第一个警报类，该警报类已为属性定义并启用警报：

1. 全局自定义警报，其警报严重性从严重到通知不等。
2. 警报严重性从严重到通知的默认警报。

在较高的警报类中找到已启用的属性警报后，NMS 服务仅会在该类中进行评估。NMS 服务不会根据其他低优先级类进行评估。也就是说，如果某个属性启用了全局自定义警报，则 NMS 服务仅根据全局自定义警报评估属性值。不评估默认警报。因此，为某个属性启用的默认警报可以满足触发警报所需的条件，但由于为同一属性启用了全局自定义警报（不符合指定的标准），因此不会触发此警报。不会触发任何警报，也不会发送任何通知。

警报触发示例

您可以使用此示例了解如何触发全局自定义警报和默认警报。

对于以下示例，属性定义并启用了全局自定义警报和默认警报，如下表所示。

	全局自定义警报阈值（已启用）	默认警报阈值（已启用）
通知	≥ 1500	≥ 1000
次要	$\geq 15,000$	≥ 1000
major	$\geq 150,000$	$\geq 250,000$

如果在该属性的值为 1000 时对其进行评估，则不会触发任何警报，也不会发送任何通知。

全局自定义警报优先于默认警报。值 1000 不会达到全局自定义警报的任何严重性级别的阈值。因此，警报级别将评估为正常。

在上述情形之后，如果禁用了全局自定义警报，则不会发生任何更改。在触发新的警报级别之前，必须重新评估属性值。

在禁用全局自定义警报的情况下，重新评估属性值时，系统会根据默认警报的阈值评估属性值。警报级别将触发通知级别警报，并向指定人员发送电子邮件通知。

严重性相同的警报

如果同一属性的两个全局自定义警报的严重性相同，则会使用 "top down" 优先级对警报进行评估。

例如，如果 UMEM 降至 50 MB，则会触发第一个警报（= 50000），但不会触发其下一个警报（ ≤ 100000000 ）。



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		

如果顺序相反，则在 UMEM 降至 100 MB 时，将触发第一个警报（<=100000000），但不会触发其下一个警报（= 50000000）。



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

通知

通知用于报告警报发生情况或服务状态发生变化。可以通过电子邮件或 SNMP 发送警报通知。

为了避免在达到警报阈值时发送多个警报和通知，系统会根据属性的当前警报严重性检查警报严重性。如果没有更改，则不会采取进一步操作。这意味着，随着 NMS 服务继续监控系统，它只会在首次发现某个属性的警报条件时发出警报并发送通知。如果达到并检测到属性的新值阈值，则警报严重性会发生变化，并会发送新通知。当条件恢复到正常水平时，警报将被清除。

警报状态通知中显示的触发值将四舍五入为小数点后三位。因此，属性值 1.9999 将触发阈值小于 (<) 2.0 的警报，但警报通知会将触发值显示为 2.0。

新服务

随着通过添加新网格节点或站点来添加新服务，这些服务将继承默认警报和全局自定义警报。

警报和表

表中显示的警报属性可以在系统级别禁用。不能为表中的单个行禁用警报。

例如，下表显示了两个严重条目可用（VMFI）警报。（选择 * 支持 * > * 工具 * > * 网格拓扑 *。然后，选择 * 存储节点_* > * SSM* > * 资源*。）

您可以禁用VMFI警报、以便不触发严重级别VMFI警报(表中当前的两个严重警报均显示为绿色)；但是、您不能在表行中禁用单个警报、以便一个VMFI警报显示为严重级别警报、而另一个警报保持绿色。

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

确认当前警报（旧系统）

当系统属性达到警报阈值时，系统会触发原有警报。或者，如果要减少或清除旧警报列表，您也可以确认这些警报。

开始之前

- 您必须使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有确认警报权限。

关于此任务

由于传统警报系统仍受支持，因此每当发生新警报时，"当前警报"页面上的原有警报列表都会增加。通常、您可以忽略警报(因为警报可提供更好的系统视图)、也可以确认警报。



或者，在完全过渡到警报系统后，您可以禁用每个旧警报，以防止其被触发并添加到旧警报计数中。

确认警报后，它将不再列在网格管理器的"当前警报"页面上，除非警报在下一个严重性级别触发，或者已解决并再次发生。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 *。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

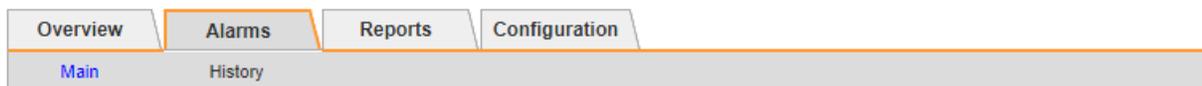
Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page Previous < 1 > Next

2. 在表中选择服务名称。

此时将显示选定服务的警报选项卡（*支持* > *工具* > *网络拓扑* > *网络节点_* > *服务_* > *警报*）。



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
 Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes 

3. 选中报警的*Accheckbox*(确认*)复选框，然后单击*Apply changes*(应用更改*)。

报警不再显示在信息板或当前报警页面上。



确认警报后，确认不会复制到其他管理节点。因此、如果您从其他管理节点查看信息板、则可能仍会看到活动警报。

4. 根据需要查看已确认的警报。

- 选择 *支持* > *警报 (原有)* > *当前警报*。
- 选择 *显示已确认警报*。

此时将显示任何已确认的警报。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 17:38:58 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable	2020-05-27 17:38:14 MDT

Show Records Per Page Previous « 1 » Next

查看默认警报（旧系统）

您可以查看所有默认旧警报的列表。

开始之前

- 您必须使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 *。
2. 对于 Filter by ，选择 * 属性代码 * 或 * 属性名称 *。
3. 对于等于、输入一个星号： *
4. 单击箭头  或按 * 输入 *。

此时将列出所有默认警报。



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by Attribute Code equals *

221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
<input checked="" type="checkbox"/>		XCVF (% Completion)	Notice	Foreground Verification Completed	=	100	
<input checked="" type="checkbox"/>	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
<input checked="" type="checkbox"/>	ADC	ADCE (ADC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
<input checked="" type="checkbox"/>	ADC	ALOS (Outbound Attribute Sessions)	Notice	Over 200	>=	200	

查看历史警报和警报频率（传统系统）

对问题描述 进行故障排除时，您可以查看过去触发传统警报的频率。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 按照以下步骤获取一段时间内触发的所有警报的列表。
 - a. 选择 * 支持 * > * 警报（原有） * > * 历史警报 *。
 - b. 执行以下操作之一：
 - 单击一个时间段。
 - 输入自定义范围，然后单击 * 自定义查询 *。

2. 按照以下步骤了解针对特定属性触发警报的频率。
 - a. 选择 * 支持 * > * 工具 * > * 网格拓扑 *。
 - b. 选择 **GRID NODE** > * 服务或组件 _ * > * 警报 * > * 历史记录 *。
 - c. 从列表中选择属性。
 - d. 执行以下操作之一：
 - 单击一个时间段。
 - 输入自定义范围，然后单击 * 自定义查询 *。
- 警报按时间倒序列出。
- e. 要返回到警报历史记录请求表单，请单击 * 历史记录 *。

创建全局自定义警报（旧系统）

您可能已对旧系统使用全局自定义警报来满足特定监控要求。全局自定义警报的警报级别可能会覆盖默认警报，也可能会监控没有默认警报的属性。

开始之前

- 您必须使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

全局自定义警报会覆盖默认警报。除非绝对必要，否则不应更改默认警报值。通过更改默认警报，您将面临隐藏可能触发警报的问题的风险。



更改报警设置时要小心。例如，如果您增加警报的阈值，则可能无法检测到潜在问题。在更改警报设置之前，请与技术支持讨论您建议的更改。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 *。
2. 向全局自定义警报表添加新行：
 - 要添加新警报，请单击 * 编辑 * （如果这是第一个条目）或 * 插入 * .



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000		

Default Alarms

Filter by Attribute Code equals AR*

9 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	
<input checked="" type="checkbox"/>	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Notice	Standby	<=	19	

Apply Changes

- 要修改默认警报，请搜索默认警报。
 - i. 在 Filter by 下，选择 * 属性代码 * 或 * 属性名称 *。
 - ii. 键入搜索字符串。

指定四个字符或使用通配符（例如， a???? 或 AB*）。星号（*）表示多个字符，问号（?）表示单个字符。
 - iii. 单击箭头 ，或按 * 输入 *。
 - iv. 在结果列表中，单击 * 复制 * 要修改的警报旁边。

默认警报将复制到全局自定义警报表。

3. 对全局自定义警报设置进行任何必要的更改：

标题	Description
enabled	选中或清除该复选框以启用或禁用警报。

标题	Description
属性	从适用于选定服务或组件的所有属性列表中选择要监控的属性的名称和代码。要显示有关属性的信息，请单击 * 信息 *  属性名称旁边。
severity	指示警报级别的图标和文本。
message	警报的原因（连接丢失，存储空间低于 10% 等）。
运算符	<p>用于根据值阈值测试当前属性值的运算符：</p> <ul style="list-style-type: none"> • = 等于 • > 大于 • 小于 • >= 大于或等于 • <= 小于或等于 • ≠ 不等于
价值	用于使用运算符根据属性的实际值测试的警报阈值。此条目可以是单个数字，使用冒号（1：3）指定的数字范围，也可以是以逗号分隔的数字和范围列表。
其他收件人	<p>触发警报时要通知的电子邮件地址的补充列表。这是对 * 警报 * > * 电子邮件设置 * 页面上配置的邮件列表的补充。列表以逗号分隔。</p> <p>*注意：*邮件列表需要设置SMTP服务器才能运行。在添加邮件列表之前，请确认已配置 SMTP。自定义警报通知可以覆盖全局自定义或默认警报的通知。</p>
操作	<p>控制按钮用于：  编辑行</p> <p>+  插入一行</p> <p>+  删除行</p> <p>+  向上或向下拖动行</p> <p>+  复制行</p>

4. 单击 * 应用更改 *。

禁用警报（旧系统）

默认情况下、原有警报系统中的警报处于启用状态、但您可以禁用不需要的警报。您还可以在完全过渡到新警报系统后禁用原有警报。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

禁用默认警报（传统系统）

您可以为整个系统禁用一个原有的默认警报。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。

关于此任务

如果为当前已触发警报的属性禁用警报，则不会清除当前警报。下次属性超过警报阈值时，警报将被禁用，您也可以清除触发的警报。



在完全转换到新警报系统之前、请勿禁用任何原有警报。否则，在无法完成关键操作之前，您可能无法检测到底层问题。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 *。
2. 搜索要禁用的默认警报。

- a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 *。
- b. 键入搜索字符串。

指定四个字符或使用通配符（例如，a????? 或 AB*）。星号（*）表示多个字符，问号（?）表示单个字符。

- c. 单击箭头 , 或按 * 输入 *。



选择 * 已禁用默认值 * 将显示当前已禁用的所有默认警报的列表。

3. 在搜索结果表中，单击编辑图标  要禁用的警报。



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

Default Alarms

Filter by equals

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Critical	Under 10000000	<=	10000000	
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Major	Under 50000000	<=	50000000	
<input type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 100000000	<=	100000000	

Apply Changes

选定报警的*Enabled"(已启用)复选框将被激活。

- 清除*Enabled"(已启用)复选框。
- 单击 * 应用更改 *。

默认警报已禁用。

禁用全局自定义警报 (旧系统)

您可以为整个系统禁用旧版全局自定义警报。

开始之前

- 您必须使用登录到网络管理器 "支持的 Web 浏览器"。
- 您必须具有特定的访问权限。

关于此任务

如果为当前已触发警报的属性禁用警报，则不会清除当前警报。下次属性超过警报阈值时，警报将被禁用，您也可以清除触发的警报。

步骤

1. 选择 * 支持 * > * 警报 (原有) * > * 全局警报 *。
2. 在全局自定义警报表中，单击 * 编辑 * 要禁用的警报旁边。
3. 清除*Enabled"(已启用)复选框。



Global Custom Alarms (1 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>	All	RDTE (Tivoli Storage Manager State)	Major	Offline	=	10		

Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

4. 单击 * 应用更改 *。

已禁用全局自定义警报。

清除触发的警报（旧系统）

如果触发了旧警报，您可以清除它，而不是确认它。

开始之前

- 您必须具有 Passwords.txt 文件

如果为当前已触发警报的属性禁用警报，则不会清除此警报。下次更改属性时，此警报将被禁用。您可以确认警报，或者，如果您希望立即清除警报，而不是等待属性值发生更改（从而导致警报状态发生更改），则可以清除触发的警报。如果您希望立即针对某个属性清除警报，而该属性的值不会经常更改（例如，状态属性），则此功能可能会很有用。

1. 禁用警报。
2. 登录到主管理节点：
 - a. 输入以下命令：`ssh admin@primary_Admin_Node_IP`
 - b. 输入中列出的密码 Passwords.txt 文件
 - c. 输入以下命令切换到root：`su -`
 - d. 输入中列出的密码 Passwords.txt 文件

以root用户身份登录后、提示符将从变为 \$ to #。

3. 重新启动NMS服务：`service nms restart`
4. 从管理节点中注销：`exit`

警报已清除。

配置警报通知（旧系统）

StorageGRID 系统可以自动发送电子邮件和 "SNMP 通知" 触发警报或服务状态发生变化时。

默认情况下，不会发送警报电子邮件通知。对于电子邮件通知，您必须配置电子邮件服务器并指定电子邮件收件人。对于 SNMP 通知，您必须配置 SNMP 代理。

警报通知类型（旧系统）

触发传统警报时，StorageGRID 系统会发送两种类型的警报通知：严重性级别和服务状态。

严重性级别通知

在选定严重性级别触发旧警报时，系统会发送警报电子邮件通知：

- 通知
- 次要
- major
- 严重

邮件列表将接收与选定严重性的警报相关的所有通知。当警报离开警报级别时，也会发送通知—解决或输入其他警报严重性级别。

服务状态通知

服务（例如 LDR 服务或 NMS 服务）进入选定服务状态以及离开选定服务状态时，系统会发送服务状态通知。服务状态通知在服务进入或离开以下服务状态之一时发送：

- 未知
- 已管理员关闭

邮件列表将接收与选定状态下的更改相关的所有通知。

为警报配置电子邮件服务器设置（旧系统）

如果您希望 StorageGRID 在触发旧警报时发送电子邮件通知，则必须指定 SMTP 邮件服务器设置。StorageGRID 系统仅发送电子邮件、无法接收电子邮件。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。

关于此任务

使用这些设置可以定义用于传统警报电子邮件通知和 AutoSupport 电子邮件消息的 SMTP 服务器。这些设置不用于警报通知。



如果使用 SMTP 作为 AutoSupport 消息的协议，则可能已配置 SMTP 邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤。请参见 ["有关管理 StorageGRID 的说明"](#)。

SMTP 是唯一支持发送电子邮件的协议。

步骤

1. 选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。
2. 从电子邮件菜单中, 选择 * 服务器 *。

此时将显示电子邮件服务器页面。此页面还用于为 AutoSupport 消息配置电子邮件服务器。

Use these settings to define the email server used for alarm notifications and for AutoSupport messages. These settings are not used for alert notifications. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).



Email Server

Updated: 2016-03-17 11:11:59 PDT

E-mail Server (SMTP) Information

Mail Server	<input type="text"/>
Port	<input type="text"/>
Authentication	<input type="button" value="Off"/>
Authentication Credentials	Username: <input type="text" value="root"/> Password: <input type="password" value="....."/>
From Address	<input type="text"/>
Test E-mail	To: <input type="text"/> <input type="checkbox"/> Send Test E-mail

Apply Changes

3. 添加以下 SMTP 邮件服务器设置:

项目	Description
邮件服务器	SMTP 邮件服务器的 IP 地址。如果先前已在管理节点上配置了 DNS 设置, 则可以输入主机名而不是 IP 地址。
Port	用于访问 SMTP 邮件服务器的端口号。
身份验证	允许对 SMTP 邮件服务器进行身份验证。默认情况下, 身份验证处于关闭状态。
身份验证凭据	SMTP 邮件服务器的用户名和密码。如果身份验证设置为 on, 则必须提供用于访问 SMTP 邮件服务器的用户名和密码。

4. 在 * 发件人地址 * 下, 输入 SMTP 服务器将识别为发送电子邮件地址的有效电子邮件地址。这是用于发送电子邮件的官方电子邮件地址。

5. (可选) 发送测试电子邮件以确认 SMTP 邮件服务器设置正确无误。
 - a. 在 * 测试电子邮件 * > * 至 * 框中, 添加一个或多个可访问的地址。

您可以输入一个电子邮件地址或一个逗号分隔的电子邮件地址列表。由于 NMS 服务在发送测试电子邮件时不会确认成功或失败, 因此您必须能够检查测试收件人的收件箱。

- b. 选择 * 发送测试电子邮件 *。

6. 单击 * 应用更改 *。

此时将保存 SMTP 邮件服务器设置。如果您为测试电子邮件输入了信息, 则会发送该电子邮件。测试电子邮件会立即发送到邮件服务器、而不会通过通知队列发送。在具有多个管理节点的系统中, 每个管理节点都会发送一封电子邮件。收到测试电子邮件将确认 SMTP 邮件服务器设置正确, 并且 NMS 服务已成功连接到邮件服务器。NMS 服务和邮件服务器之间的连接问题会在次要严重性级别触发旧的分钟 (NMS 通知状态) 警报。

创建警报电子邮件模板 (旧系统)

通过电子邮件模板, 您可以自定义旧警报电子邮件通知的页眉, 页脚和主题行。您可以使用电子邮件模板向不同的邮件列表发送包含相同正文的唯一通知。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。

关于此任务

使用这些设置可以定义用于旧警报通知的电子邮件模板。这些设置不用于警报通知。

不同的邮件列表可能需要不同的联系信息。模板不包括电子邮件的正文。

步骤

1. 选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。
2. 从电子邮件菜单中, 选择 * 模板 *。
3. 单击 * 编辑 *。  (或 * 插入 *  如果这不是第一个模板)。



Template (0 - 0 of 0)

Template Name	Subject Prefix	Header	Footer	Actions
Template One	Notifications	All Email Lists	From SGWS	

Show Records Per Page

4. 在新行中添加以下内容：

项目	Description
模板名称	用于标识模板的唯一名称。模板名称不能重复。
主题前缀	可选。将显示在电子邮件主题行开头的前缀。前缀可用于轻松配置电子邮件筛选器和组织通知。
标题	可选。显示在电子邮件正文开头的标题文本。可以使用标题文本在电子邮件内容的前面添加公司名称和地址等信息。
页脚	可选。显示在电子邮件正文末尾的页脚文本。可以使用页脚文本关闭包含提醒信息的电子邮件，例如联系人电话号码或网站链接。

5. 单击 * 应用更改 * 。

此时将为通知添加一个新模板。

为警报通知创建邮件列表（旧系统）

通过邮件列表，您可以在触发旧警报或服务状态发生变化时通知收件人。您必须至少创建一个邮件列表，然后才能发送任何警报电子邮件通知。要向单个收件人发送通知，请使用一个电子邮件地址创建一个邮件列表。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

关于此任务

使用这些设置可以定义用于旧警报电子邮件通知的邮件列表。这些设置不用于警报通知。

步骤

1. 选择 * 支持 * > * 警报 (旧版) * > * 旧版电子邮件设置 *。
2. 从电子邮件菜单中, 选择 * 列表 *。
3. 单击 * 编辑 *。  (或 * 插入 *  如果这不是第一个邮件列表)。



Email Lists

Updated: 2016-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  

Show Records Per Page

Apply Changes 

4. 在新行中, 添加以下内容:

项目	Description
组名称	用于标识邮件列表的唯一名称。不能复制邮件列表名称。 <ul style="list-style-type: none">• 注意: * 如果更改了邮件列表的名称, 则此更改不会传播到使用邮件列表名称的其他位置。您必须手动更新所有已配置的通知, 才能使用新的邮件列表名称。
收件人	单个电子邮件地址, 先前配置的邮件列表或将通知发送到的电子邮件地址和邮件列表的逗号分隔列表。 <ul style="list-style-type: none">• 注意: * 如果电子邮件地址属于多个邮件列表, 则在发生通知触发事件时仅发送一封电子邮件通知。
模板	或者, 也可以选择一个电子邮件模板, 以便向发送给此邮件列表的所有收件人的通知添加唯一的页眉, 页脚和主题行。

5. 单击 * 应用更改 *。

此时将创建一个新的邮件列表。

配置警报电子邮件通知 (旧系统)

要接收传统报警系统的电子邮件通知、收件人必须是邮件列表的成员、并且必须将该列表添加到通知页面中。通知配置为仅在触发具有指定严重性级别的警报或服务状态发生更改时才向收件人发送电子邮件。因此, 收件人只会收到需要接收的通知。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。
- 您必须已配置电子邮件列表。

关于此任务

使用这些设置为旧警报配置通知。这些设置不用于警报通知。

如果某个电子邮件地址（或列表）属于多个邮件列表，则在发生通知触发事件时仅会发送一封电子邮件通知。例如，可以将组织中的一组管理员配置为接收所有警报的通知，而不管严重性如何。另一个组可能只需要针对严重性为 "严重" 的警报发出通知。您可以同时属于这两个列表。如果触发严重警报，您只会收到一条通知。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 *。
2. 从电子邮件菜单中，选择 * 通知 *。
3. 单击 * 编辑 *。 （或 * 插入 *  如果这不是第一个通知）。
4. 在电子邮件列表下，选择邮件列表。
5. 选择一个或多个警报严重性级别和服务状态。
6. 单击 * 应用更改 *。

触发或更改具有选定警报严重性级别或服务状态的警报时，系统会向邮件列表发送通知。

禁止发送邮件列表的警报通知（旧系统）

如果您不再希望邮件列表接收有关警报的通知，则可以禁止此邮件列表的警报通知。例如，在过渡到使用警报电子邮件通知后，您可能希望禁止有关旧警报的通知。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您必须具有特定的访问权限。

使用这些设置可禁止向原有警报系统发送电子邮件通知。这些设置不适用于警报电子邮件通知。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 *。
2. 从电子邮件菜单中，选择 * 通知 *。
3. 单击 * 编辑 *。  要禁止其通知的邮件列表旁边。
4. 在禁止下，选中要禁止的邮件列表旁边的复选框，或选择列顶部的 * 禁止 * 以禁止所有邮件列表。
5. 单击 * 应用更改 *。

选定邮件列表将禁止使用旧警报通知。

查看旧警报

当系统属性达到警报阈值时，将触发警报（传统系统）。您可以从当前警报页面查看当前活动的警报。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

开始之前

- 您必须使用登录到网络管理器 ["支持的 Web 浏览器"](#)。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 *。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show Records Per Page Previous < 1 > Next

警报图标指示每个警报的严重性，如下所示：

图标。	颜色	警报严重性	含义
	黄色	通知	节点已连接到网格，但存在不影响正常操作的异常情况。
	浅橙色	次要	节点已连接到网格，但存在异常情况，可能会影响未来的运行。您应进行调查以防止上报。
	深橙色	major	节点已连接到网格，但存在当前影响操作的异常情况。这需要立即引起注意，以防止升级。
	红色	严重	节点已连接到网格，但存在已停止正常操作的异常情况。您应立即解决此问题描述。

2. 要了解触发警报的属性，请右键单击表中的属性名称。
3. 要查看有关警报的其他详细信息，请单击表中的服务名称。

此时将显示选定服务的警报选项卡（* 支持 * > * 工具 * > * 网络拓扑 * > * 网络节点 _ * > * 服务 _ * > * 警报 *）。



Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes

4. 如果要清除当前警报计数，您可以选择执行以下操作：

- 确认警报。已确认的警报将不再包含在原有警报计数中，除非它在下一严重性级别触发，或者已解决并再次发生。
- 为整个系统禁用特定的默认警报或全局自定义警报，以防止再次触发该警报。

相关信息

["警报参考（旧系统）"](#)

["确认当前警报（旧系统）"](#)

["禁用警报（旧系统）"](#)

警报参考（旧系统）

下表列出了所有原有的默认警报。如果触发了警报，您可以在此表中查找警报代码以查找建议的操作。



虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

代码	Name	服务	建议的操作
ABRL	可用属性中继	BADC , BAMS , BARC , BCLB , BCMN , BLDR , BNMS , BSSM , BDDS	尽快恢复与运行属性中继服务的连接（一种模数转换器服务）的连接。如果没有连接的属性中继、则网络节点无法向NMS服务报告属性值。因此，NMS 服务无法再监控服务的状态，也无法更新服务的属性。 如果问题仍然存在，请联系技术支持。
ACMS	可用元数据服务	BARR , BLDR , BCMN	如果 LDR 或 ARC-Service 与 DDS 服务断开连接，则会触发警报。如果发生这种情况、则无法处理入数据或检索事务。如果 DDS 服务不可用只是一个短暂的瞬时问题描述，则事务可能会延迟。 检查并还原与 DDS 服务的连接，以清除此警报并使此服务恢复完整功能。

代码	Name	服务	建议的操作
行为	云分层服务状态	圆弧	<p>仅适用于目标类型为 Cloud Tiering 的归档节点 - 简单存储服务 (S3)。</p> <p>如果归档节点的 "Acts " 属性设置为 "Read-Only Enabled" 或 "Read-Write Disabled" ，则必须将此属性设置为 "Read-Write Enabled" 。</p> <p>如果因身份验证失败而触发重大警报，请验证与目标存储分段关联的凭据，并根据需要更新值。</p> <p>如果因任何其他原因触发重大警报，请联系技术支持。</p>
ADCA	模数转换器状态	模数转换器	<p>如果触发警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _ * > * 网格节点 _ * > * ADC * > * 概述 * > * 主要 * 和 * ADC * > * 警报 * > * 主要 * 来确定警报的发生原因。</p> <p>如果问题仍然存在，请联系技术支持。</p>
ADCE	模数转换器状态	模数转换器	<p>如果 "ADC-State" 的值为 "Standby" ，请继续监控此服务，如果问题仍然存在，请联系技术支持。</p> <p>如果 "ADC" 状态的值为脱机，请重新启动此服务。如果问题仍然存在，请联系技术支持。</p>
AITE	检索状态	BARC-B	<p>仅适用于目标类型为 Tivoli Storage Manager (TSM) 的归档节点。</p> <p>如果检索状态值正在等待目标，请检查 TSM 中间件服务器并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。</p> <p>如果 " 归档检索状态 " 的值为 " 脱机 " ，请尝试将此状态更新为 " 联机 " 。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _ * > * 网格节点 _ * > * ARC * > * 检索 * > * 配置 * > * 主要 * ，选择 * 归档检索状态 * > * 联机 * ，然后单击 * 应用更改 * 。</p> <p>如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
AITU-A	检索状态	BARC-B	<p>如果检索状态的值为目标错误，请检查目标外部归档存储系统是否存在错误。</p> <p>如果归档检索状态的值为会话丢失，请检查目标外部归档存储系统以确保其联机并正常运行。检查与目标的网络连接。</p> <p>如果 " 归档检索状态 " 的值为未知错误，请联系技术支持。</p>
Alis	进站属性会话	模数转换器	<p>如果属性中继上的进站属性会话数增长得太大，则可能表示 StorageGRID 系统已变得不平衡。在正常情况下，属性会话应均匀分布在各个模块转换服务之间。不平衡可能导致性能问题。</p> <p>如果问题仍然存在，请联系技术支持。</p>
ALOS	出站属性会话	模数转换器	<p>此 ADE 服务具有大量属性会话，并且正在过载。如果触发此警报，请联系技术支持。</p>
Alur	无法访问的属性存储库	模数转换器	<p>检查与 NMS 服务的网络连接，以确保此服务可以与属性存储库联系。</p> <p>如果触发此警报且网络连接良好，请联系技术支持。</p>
AMQS	已排队的审核消息	BADC , BAMS , BARC , BCLB , BCMN , BLDR , BNMS , BDDS	<p>如果无法立即将审核消息转发到审核中继或存储库、则这些消息将存储在磁盘队列中。如果磁盘队列已满，则可能发生中断。</p> <p>为了及时做出响应以防止中断，当磁盘队列中的消息数量达到以下阈值时，系统将触发 AMQS 警报：</p> <ul style="list-style-type: none"> • 注意：超过 100 , 000 条消息 • 次要：至少 500 , 000 条消息 • 主要：至少 2 , 000 , 000 条消息 • 严重：至少 5 , 000 , 000 条消息 <p>如果触发了 AMQS 警报，请检查系统上的负载—如果存在大量事务，则该警报应随着时间的推移自行解决。在这种情况下，您可以忽略警报。</p> <p>如果警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 "配置审核消息和日志目标"。</p>

代码	Name	服务	建议的操作
AOTE	存储状态	BARC-B	<p>仅适用于目标类型为 Tivoli Storage Manager (TSM) 的归档节点。</p> <p>如果 "Store State" 的值为 "Waiting for Target"，请检查外部归档存储系统并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。</p> <p>如果 "存储状态" 的值为 "脱机"，请检查 "存储状态" 的值。在将存储状态移回联机之前更正所有问题。</p>
AOTU	存储状态	BARC-B	<p>如果 "Store Status" (存储状态) 的值为 "Session lost" (会话丢失)，请检查外部归档存储系统是否已连接并联机。</p> <p>如果 "Target Error" 的值为，请检查外部归档存储系统是否存在错误。</p> <p>如果 "Store Status" 的值为 "Unknown" 错误，请联系技术支持。</p>
APM	存储多路径连接	SSM	<p>如果多路径状态警报显示为 Degraded (选择 * 支持 * > * 工具 * > * 网络拓扑 *，然后选择 * 站点 _ * > * 网络节点 _ * > * SSM * > * 事件 *)，请执行以下操作：</p> <ol style="list-style-type: none"> 1. 插入或更换不显示任何指示灯的缆线。 2. 等待一到五分钟。 <p>插入另一根电缆至少五分钟后再拔下另一根电缆。过早拔出可能会使根卷发生原因 变为只读，这要求重新启动硬件。</p> <ol style="list-style-type: none"> 3. 返回到 * SSM * > * 资源 * 页面，并验证存储硬件部分中的 Degraded 多路径状态是否已更改为 "nominal" 。
Arce	弧状态	圆弧	<p>在所有旋转组件 (复制, 存储, 检索, 目标) 启动之前, 此旋转式应用程序服务的状态均为 "备用"。然后过渡到联机。</p> <p>如果 "ARC-State" 值未从 "备用" 过渡到 "联机", 请检查这些组件的状态。</p> <p>如果 "ARC-State" 的值为 "Offlin", 请重新启动此服务。如果问题仍然存在, 请联系技术支持。</p>

代码	Name	服务	建议的操作
AROQ	已排队的对象	圆弧	<p>如果可移动存储设备由于目标外部归档存储系统出现问题而运行缓慢，或者遇到多个读取错误，则可能会触发此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。</p> <p>在某些情况下，此错误可能是由于数据请求率较高而导致的。监控在系统活动减少时排队的对象数量。</p>
ARRF	请求失败	圆弧	<p>如果从目标外部归档存储系统检索失败，则归档节点会重试检索，因为此失败可能是由于瞬时问题描述造成的。但是，如果对象数据已损坏或已标记为永久不可用，则检索不会失败。相反，归档节点会持续重试检索，而请求失败的值会继续增加。</p> <p>此警报可能指示保存所请求数据的存储介质已损坏。检查外部归档存储系统以进一步诊断此问题。</p> <p>如果确定对象数据不再位于归档中，则必须从 StorageGRID 系统中删除该对象。有关详细信息，请联系技术支持。</p> <p>触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点_* > * 网络节点_* > * ARC* > * 检索 * > * 配置 * > * 主*，选择 * 重置请求失败计数 * 并单击 * 应用更改 *。</p>
ARRV	验证失败	圆弧	<p>要诊断并更正此问题，请联系技术支持。</p> <p>触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点_* > * 网络节点_* > * ARC* > * 检索 * > * 配置 * > * 主*，选择 * 重置验证失败计数 * 并单击 * 应用更改 *。</p>
ARVF	存储故障	圆弧	<p>如果目标外部归档存储系统出错，可能会出现此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。</p> <p>触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点_* > * 网络节点_* > * ARC* > * 检索 * > * 配置 * > * 主*，选择 * 重置存储故障计数 *，然后单击 * 应用更改 *。</p>
ASXP	审核共享	AMS	<p>如果审核共享的值为未知，则会触发警报。此警报可能指示管理节点的安装或配置出现问题。</p> <p>如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
AUMA	AMS 状态	AMS	<p>如果 AMS Status 的值为 DB Connectivity Error ， 请重新启动网格节点。</p> <p>如果问题仍然存在，请联系技术支持。</p>
AUME	AMS 状态	AMS	<p>如果 AMS State 的值为 "Standby" ， 请继续监控 StorageGRID 系统。如果问题仍然存在，请联系技术支持。</p> <p>如果 AMS State 的值为 Offline ， 请重新启动服务。如果问题仍然存在，请联系技术支持。</p>
AUXS	审核导出状态	AMS	<p>如果触发警报，请更正根本问题，然后重新启动 AMS 服务。</p> <p>如果问题仍然存在，请联系技术支持。</p>
badd	存储控制器故障 驱动器计数	SSM	<p>如果 StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器，则会触发此警报。根据需要更换驱动器。</p>
BASF	可用对象标识符	CMN	<p>配置 StorageGRID 系统后，系统会为 CMN 服务分配固定数量的对象标识符。当 StorageGRID 系统开始用尽其对象标识符时，会触发此警报。</p> <p>要分配更多标识符，请联系技术支持。</p>
重声	标识符块分配状态	CMN	<p>默认情况下、如果由于无法达到ADC仲裁而无法分配对象标识符、则会触发警报。</p> <p>要在 CMN 服务上分配标识符块，需要使模拟学习中心服务达到联机和连接的仲裁（50% + 1）。如果仲裁不可用、则在重新建立ADC仲裁之前、CMN服务无法分配新的标识符块。如果丢失了模块转换仲裁，通常不会对 StorageGRID 系统产生任何即时影响（客户端仍可载入和检索内容），因为大约一个月的标识符会缓存在网格中的其他位置；但是，如果此情况持续存在，则 StorageGRID 系统将无法载入新内容。</p> <p>如果触发警报，请调查丢失 ADC 仲裁的原因（例如，可能是网络或存储节点故障）并采取更正措施。</p> <p>如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
BRDT	计算控制器机箱温度	SSM	<p>如果 StorageGRID 设备中计算控制器的温度超过额定阈值，则会触发警报。</p> <p>检查硬件组件和环境问题是否过热。如有必要，请更换组件。</p>
BTOF	Offset	BADC , BLDR , BNMS , BAMS , BCLB , BCMN , BARC-A	<p>如果服务时间（秒）与操作系统时间相差很大，则会触发警报。在正常情况下，服务应自行重新同步。如果服务时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。</p> <p>如果问题仍然存在，请联系技术支持。</p>
BTSE	时钟状态	BADC , BLDR , BNMS , BAMS , BCLB , BCMN , BARC-A	<p>如果服务的时间与操作系统跟踪的时间不同步，则会触发警报。在正常情况下，服务应自行重新同步。如果时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。</p> <p>如果问题仍然存在，请联系技术支持。</p>
CAHP	Java 堆使用量百分比	DDS	<p>如果 Java 无法以允许有足够堆空间使系统正常运行的速率执行垃圾收集，则会触发警报。警报可能指示用户工作负载超出整个系统可用于 DDS 元数据存储的资源。检查信息板中的ILM活动，或选择*support*>*Tools*>*网格拓扑*，然后选择*ssite*>*grid NODE*>*DDS*>*资源*>*概述*>*主*。</p> <p>如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
CASA	数据存储状态	DDS	<p>如果 Cassandra 元数据存储不可用，则会发出警报。</p> <p>检查 Cassandra 的状态：</p> <ol style="list-style-type: none"> 1. 在存储节点上、以admin和身份登录 su 使用 Passwords.txt 文件中列出的密码以 root 用户身份访问。 2. 输入 ... service cassandra status 3. 如果 Cassandra 未运行、请重新启动它： service cassandra restart <p>此警报还可能指示存储节点的元数据存储（Cassandra 数据库）需要重建。</p> <p>请参见中有关对服务进行故障排除的信息：状态 - Cassandra（SVST）警报 "对元数据问题进行故障排除"。</p> <p>如果问题仍然存在，请联系技术支持。</p>
案例	数据存储状态	DDS	<p>安装或扩展期间会触发此警报，以指示新的数据存储正在加入网格。</p>
CCNA	计算硬件	SSM	<p>如果需要注意 StorageGRID 设备中计算控制器硬件的状态，则会触发此警报。</p>

代码	Name	服务	建议的操作
CDLP	元数据已用空间 (百分比)	DDS	<p>当元数据有效空间（ Metadata Effective Space ， CEMS ）达到 70% 全满（次要警报）， 90% 全满（主要警报）和 100% 全满（严重警报）时，将触发此警报。</p> <p>如果此警报达到90%阈值、网格管理器中的信息板上将显示一条警告。要尽快添加新的存储节点，您必须执行扩展操作步骤。请参见 "扩展网格"。</p> <p>如果此警报达到 100% 阈值，则必须停止载入对象并立即添加存储节点。Cassandra 需要一定的空间来执行诸如压实和修复等基本操作。如果对对象元数据使用的空间超过允许的 100% ，则这些操作将受到影响。可能会出现不希望的结果。</p> <ul style="list-style-type: none"> 注*：如果无法添加存储节点，请联系技术支持。 <p>添加新存储节点后，系统会自动在所有存储节点之间重新平衡对象元数据，并清除警报。</p> <p>另请参见中有关对 " 低元数据存储 " 警报进行故障排除的信息 "对元数据问题进行故障排除"。</p> <p>如果问题仍然存在，请联系技术支持。</p>
CMNA	CMN 状态	CMN	<p>如果 CMN Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _ * > * 网格节点 _ * > * CMN * > * 概述 * > * 主 * 和 * CMN * > * 警报 * > * 主 * 以确定错误的发生原因 并对问题进行故障排除。</p> <p>切换 CMNS 后，在主管理节点硬件刷新期间会触发警报，并且 CMN 状态值为无联机 CMN（旧的 CMN 状态值为 " 备用 " ，新的 " 联机 " ）。</p> <p>如果问题仍然存在，请联系技术支持。</p>
CPRC	剩余容量	NMS	<p>如果剩余容量（可打开到 NMS 数据库的可用连接数）降至配置的警报严重性以下，则会触发警报。</p> <p>如果触发了警报，请联系技术支持。</p>
CPSA	计算控制器电源 A	SSM	<p>如果 StorageGRID 设备的计算控制器中存在电源为 A 的问题描述，则会触发警报。</p> <p>如有必要，请更换组件。</p>

代码	Name	服务	建议的操作
cPSB	计算控制器电源 B	SSM	<p>如果 StorageGRID 设备的计算控制器中存在电源为 B 的问题描述，则会触发警报。</p> <p>如有必要，请更换组件。</p>
CPUT	计算控制器 CPU 温度	SSM	<p>如果 StorageGRID 设备中计算控制器中的 CPU 温度超过额定阈值，则会触发警报。</p> <p>如果存储节点是 StorageGRID 设备，则 StorageGRID 系统指示需要关注控制器。</p> <p>检查硬件组件和环境问题是否存在过热情况。如有必要，请更换组件。</p>
DNST	DNS 状态	SSM	<p>安装完成后，将在 SSM 服务中触发 DNST 警报。配置 DNS 并将新服务器信息访问到所有网格节点后，警报将被取消。</p>
ECCD	检测到损坏的片段	LDR	<p>当后台验证过程检测到损坏的纠删编码片段时，将触发警报。如果检测到损坏的片段，则会尝试重建该片段。重置检测到的损坏片段，并将丢失的属性复制到零，然后对其进行监控，以查看计数是否再次增加。如果计数确实增加、则存储节点的底层存储可能存在问题。除非丢失或损坏的碎片数量违反纠删代码的容错能力，否则不会认为缺少纠删编码对象数据的副本；因此，可能存在损坏的碎片，并且仍能检索对象。</p> <p>如果问题仍然存在，请联系技术支持。</p>
ECST	验证状态	LDR	<p>此警报指示此存储节点上经过纠删编码的对象数据的后台验证过程的当前状态。</p> <p>如果后台验证过程出现错误，则会触发重大警报。</p>
FWPN	打开文件描述符	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	<p>在活动高峰期，FWPN 可能会变大。如果在活动缓慢期间不会减少，请联系技术支持。</p>
HSTE	HTTP 状态	BLDR	<p>请参见建议的 HSTU 操作。</p>

代码	Name	服务	建议的操作
HSTU	HTTP 状态	BLDR	<p>HSTE和HSTU与所有LDR流量的HTTP相关、包括S3、Swift和其他内部StorageGRID 流量。警报表示已发生以下情况之一：</p> <ul style="list-style-type: none"> • HTTP已手动脱机。 • 已禁用自动启动 HTTP 属性。 • LDR 服务正在关闭。 <p>默认情况下，自动启动 HTTP 属性处于启用状态。如果更改此设置， HTTP 可能会在重新启动后保持脱机状态。</p> <p>如有必要，请等待 LDR 服务重新启动。</p> <p>选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 存储节点 _ * > * LDR * > * 配置 * 。如果HTTP已脱机、请将其置于联机状态。验证是否已启用自动启动 HTTP 属性。</p> <p>如果HTTP保持脱机状态、请联系技术支持。</p>
HTA	自动启动 HTTP	LDR	<p>指定是否在启动时自动启动 HTTP 服务。这是用户指定的配置选项。</p>
IRSU	入站复制状态	BLDR , BARR	<p>警报指示已禁用入站复制。确认配置设置：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _ * > * 网格节点 _ * > * LDR * > * 复制 * > * 配置 * > * 主 * 。</p>
延迟	平均延迟	NMS	<p>检查连接问题。</p> <p>检查系统活动以确认系统活动有所增加。系统活动增加将导致属性数据活动增加。这种增加的活动将导致属性数据处理延迟。这可以是正常的系统活动，也可以是次要活动。</p> <p>检查是否存在多个警报。触发的警报数量过多可能表明平均延迟时间增加。</p> <p>如果问题仍然存在，请联系技术支持。</p>
LDRE	LDR 状态	LDR	<p>如果 LDR 状态值为 " 备用 " ，请继续监控此情况，如果问题仍然存在，请联系技术支持。</p> <p>如果 LDR 状态值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
已丢失	对象丢失	DDS , LDR	<p>当 StorageGRID 系统无法从系统中的任何位置检索所请求对象的副本时触发。在触发 " 丢失 (丢失的对象) " 警报之前, 系统会尝试从系统中的其他位置检索并更换缺失的对象。</p> <p>对象丢失表示数据丢失。只要对象的位置数降至零, 并且 DDS 服务未特意清除内容以满足 ILM 策略, " 丢失对象 " 属性就会递增。</p> <p>立即调查丢失 (对象丢失) 警报。如果问题仍然存在, 请联系技术支持。</p> <p>"对丢失和丢失的对象数据进行故障排除"</p>
MCEP	管理接口证书到期	CMN	<p>用于访问管理接口的证书即将过期时触发。</p> <ol style="list-style-type: none"> 1. 在网络管理器中, 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上, 选择 * 管理接口证书 * 。 3. "上传新的管理接口证书。"
分钟	电子邮件通知已排队	NMS	<p>检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外, 请确认电子邮件服务器配置正确。</p> <p>"为警报配置电子邮件服务器设置 (旧系统) "</p>
分钟	电子邮件通知状态	BNMS	<p>如果 NMS 服务无法连接到邮件服务器, 则会触发一个小警报。检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外, 请确认电子邮件服务器配置正确。</p> <p>"为警报配置电子邮件服务器设置 (旧系统) "</p>
等	NMS 接口引擎状态	BNMS	<p>如果管理节点上用于收集和生成接口内容的 NMS 接口引擎与系统断开连接, 则会触发警报。检查服务器管理器以确定服务器单个应用程序是否已关闭。</p>
Nang	网络自动协商设置	SSM	<p>检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。</p> <p>设置不正确可能会严重影响系统性能。</p>
NDUP	网络双工设置	SSM	<p>检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。</p> <p>设置不正确可能会严重影响系统性能。</p>

代码	Name	服务	建议的操作
NLNK	网络链路检测	SSM	<p>检查端口和交换机上的网络缆线连接。</p> <p>检查网络路由器，交换机和适配器配置。</p> <p>重新启动服务器。</p> <p>如果问题仍然存在，请联系技术支持。</p>
NRER	接收错误	SSM	<p>以下可能是 NRER 警报的原因：</p> <ul style="list-style-type: none"> • 正向错误更正（FEC）不匹配 • 交换机端口和 NIC MTU 不匹配 • 链路错误率较高 • NIC 环缓冲区溢出 <p>请参见中有关对网络接收错误（NRER）警报进行故障排除的信息 "对网络，硬件和平台问题进行故障排除"。</p>
NRLY	可用的审核中继	BADC，BARC，BCLB，BCM N，BLDR，BNMS，BDDS	<p>如果审核中继未连接到ADC服务、则无法报告审核事件。它们将排队，在连接恢复之前不可供用户使用。</p> <p>请尽快恢复与模数转换器服务的连接。</p> <p>如果问题仍然存在，请联系技术支持。</p>
NSCA	NMS 状态	NMS	<p>如果 NMS Status 的值为 DB Connectivity Error，请重新启动此服务。如果问题仍然存在，请联系技术支持。</p>
NSCE	NMS 状态	NMS	<p>如果 NMS 状态的值为 "备用"，请继续监控，如果问题仍然存在，请联系技术支持。</p> <p>如果 NMS 状况的值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。</p>
NSPD	速度	SSM	<p>这可能是由于网络连接或驱动程序兼容性问题造成的。如果问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
NBR	可用表空间	NMS	<p>如果触发警报，请检查数据库使用量变化的速度。突然下降（而不是随着时间的推移逐渐变化）表示出现错误情况。如果问题仍然存在，请联系技术支持。</p> <p>通过调整警报阈值，您可以主动管理何时需要分配更多存储。</p> <p>如果可用空间达到较低阈值（请参见警报阈值），请联系技术支持以更改数据库分配。</p>
NTER	传输错误	SSM	<p>可以在不手动重置的情况下清除这些错误。如果未清除、请检查网络硬件。检查适配器硬件和驱动程序是否已正确安装并配置，以便与网络路由器和交换机配合使用。</p> <p>解决底层问题后，重置计数器。选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点 _ * > * 网络节点 _ * > * SSM * > * 资源 * > * 配置 * > * 主 *，选择 * 重置传输错误计数 *，然后单击 * 应用更改 *。</p>
NTFQ	NTP 频率偏移	SSM	<p>如果频率偏移超过配置的阈值，则本地时钟可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。</p>
NTLK	NTP 锁定	SSM	<p>如果 NTP 守护进程未锁定到外部时间源，请检查与指定外部时间源的网络连接，这些时间源的可用性及其稳定性。</p>
NTOF	NTP 时间偏移	SSM	<p>如果时间偏移超过配置的阈值，则本地时钟的振铃器可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。</p>
NTSJ	选定时间源抖动	SSM	<p>此值表示本地服务器上的 NTP 用作参考的时间源的可靠性和稳定性。</p> <p>如果触发警报，则可能表示时间源的振荡器有缺陷，或者与时间源的 WAN 链路出现问题。</p>
Ntlu	NTP 状态	SSM	<p>如果 "NTP Status" 的值未运行，请联系技术支持。</p>
OPST	整体电源状态	SSM	<p>如果 StorageGRID 设备的电源与建议的工作电压不同，则会触发警报。</p> <p>检查电源 A 或 B 的状态以确定哪个电源运行异常。</p> <p>如有必要，请更换电源。</p>

代码	Name	服务	建议的操作
OQRT	已隔离对象	LDR	<p>在 StorageGRID 系统自动还原对象后，可以从隔离目录中删除隔离的对象。</p> <ol style="list-style-type: none"> 1. 选择 * 支持 * > * 工具 * > * 网格拓扑 *。 2. 选择 * 站点 * > * 存储节点 * > * LDR * > * 验证 * > * 配置 * > * 主 *。 3. 选择 * 删除隔离的对象 *。 4. 单击 * 应用更改 *。 <p>隔离的对象将被删除，计数将重置为零。</p>
ORSU	出站复制状态	BLDR , BARR	<p>警报指示无法进行出站复制：存储处于无法检索对象的状态。如果手动禁用了出站复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 *。然后选择 * 站点 _ * > * 网格节点 _ * > * LDR * > * 复制 * > * 配置 *。</p> <p>如果 LDR 服务不可用于复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 *。然后选择 * 站点 _ * > * 网格节点 _ * > * LDR * > * 存储 *。</p>
OSLF	磁盘架状态	SSM	<p>如果存储设备存储架中某个组件的状态为已降级，则会触发警报。存储架组件包括 IOM ， 风扇， 电源和驱动器抽盒。如果触发此警报，请参见设备的维护说明。</p>
PMEM	服务内存使用量 (百分比)	BADC , BAMS , BARC , BCLB , BCMN , BLDR , BNMS , BSSM , BDDS	<p>可以具有大于 Y% RAM 的值，其中 Y 表示服务器正在使用的内存百分比。</p> <p>低于 80% 的数字是正常的。超过 90% 被视为问题。</p> <p>如果一项服务的内存使用率较高，请监控情况进行调查。</p> <p>如果问题仍然存在，请联系技术支持。</p>
PSAS	电源 A 状态	SSM	<p>如果 StorageGRID 设备中的电源 A 与建议的工作电压不同，则会触发警报。</p> <p>如有必要，请更换电源 A</p>
PSB	电源 B 状态	SSM	<p>如果 StorageGRID 设备中的电源 B 与建议的工作电压不同，则会触发警报。</p> <p>如有必要，请更换电源 B</p>

代码	Name	服务	建议的操作
RTTE	Tivoli Storage Manager 状态	BARC-B	<p>仅适用于目标类型为 Tivoli Storage Manager (TSM) 的归档节点。</p> <p>如果 Tivoli Storage Manager State 的值为脱机，请检查 Tivoli Storage Manager 状态并解决任何问题。</p> <p>使组件重新联机。选择 * 支持 * > * 工具 * > * 网络拓扑 * 。然后选择 * 站点 _ * > * 网络节点 _ * > * ARC * > * 目标 * > * 配置 * > * 主要 * ，选择 * Tivoli Storage Manager State * > * 联机 * ，然后单击 * 应用更改 * 。</p>
RDTU	Tivoli Storage Manager 状态	BARC-B	<p>仅适用于目标类型为 Tivoli Storage Manager (TSM) 的归档节点。</p> <p>如果 Tivoli Storage Manager 状态的值为配置错误，并且刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置 TSM 中间件服务器。</p> <p>如果 Tivoli Storage Manager Status 的值为 Connection Failure 或 Connection Failure ，请重试，请检查 TSM 中间件服务器上的网络配置以及 TSM 中间件服务器和 StorageGRID 系统之间的网络连接。</p> <p>如果 Tivoli Storage Manager 状态的值为身份验证失败或身份验证失败、正在重新连接、则 StorageGRID 系统可以连接到 TSM 中间件服务器、但无法对连接进行身份验证。检查 TSM 中间件服务器是否配置了正确的用户，密码和权限，然后重新启动服务。</p> <p>如果 Tivoli Storage Manager Status 的值为 session failure ，则表示已建立的会话已意外丢失。检查 TSM 中间件服务器与 StorageGRID 系统之间的网络连接。检查中间件服务器是否存在错误。</p> <p>如果 Tivoli Storage Manager Status 的值为未知错误，请联系技术支持。</p>
RIRF	入站复制—失败	BLDR , BARR	<p>入站复制—在负载较高或网络临时中断期间，可能会发生故障警报。系统活动减少后，应清除此警报。如果失败的复制计数持续增加，请查找网络问题，并验证源和目标 LDR 以及 ARR 服务是否联机且可用。</p> <p>要重置计数，请选择 * 支持 * > * 工具 * > * 网络拓扑 * ，然后选择 * 站点 _ * > * 网络节点 _ * > * LDR * > * 复制 * > * 配置 * > * 主 * 。选择 * 重置入站复制失败计数 * ，然后单击 * 应用更改 * 。</p>

代码	Name	服务	建议的操作
RIRQ	进站复制—已排队	BLDR , BARR	在高负载或临时网络中断期间,可能会发生警报。系统活动减少后,应清除此警报。如果排队复制的数量继续增加,请查找网络问题,并验证源和目标 LDR 以及 ARR 服务是否联机且可用。
RORQ	出站复制—已排队	BLDR , BARR	出站复制队列包含要复制的对象数据,以满足客户端请求的 ILM 规则和对象。 系统过载可能会导致警报。等待系统活动下降时警报是否清除。如果警报再次出现,请通过添加存储节点来添加容量。
SAVP	总可用空间(百分比)	LDR	如果可用空间达到较低阈值,则可选择扩展 StorageGRID 系统或通过归档节点将对象数据移动到归档。
SCA	Status	CMN	如果活动网格任务的状态值为错误,请查找网格任务消息。选择 * 支持 * > * 工具 * > * 网格拓扑 *。然后选择 * 站点 _ * > * 网格节点 _ * > * CMN * > * 网格任务 * > * 概述 * > * 主 *。网格任务消息会显示有关此错误的信息(例如, "check failed on node 12130011")。 调查并更正问题后,重新启动网格任务。选择 * 支持 * > * 工具 * > * 网格拓扑 *。然后选择 * 站点 _ * > * 网格节点 _ * > * CMN * > * 网格任务 * > * 配置 * > * 主 *, 然后选择 * 操作 * > * 运行 *。 如果要停止的网格任务的状态值为错误、请重试结束网格任务。 如果问题仍然存在,请联系技术支持。
SCEP	存储 API 服务端点证书过期	CMN	用于访问存储 API 端点的证书即将过期时触发。 1. 选择 * 配置 * > * 安全性 * > * 证书 *。 2. 在 * 全局 * 选项卡上,选择 * S3 和 Swift API 证书 *。 3. "上传新的 S3 和 Swift API 证书。"
SCHR	Status	CMN	如果历史网格任务的状态值已中止,请调查原因并在需要时再次运行此任务。 如果问题仍然存在,请联系技术支持。

代码	Name	服务	建议的操作
SCSA	存储控制器 A	SSM	<p>如果 StorageGRID 设备中存在存储控制器 A 的问题描述，则会触发警报。</p> <p>如有必要，请更换组件。</p>
SCSB	存储控制器 B	SSM	<p>如果 StorageGRID 设备中存在存储控制器 B 的问题描述，则会触发警报。</p> <p>如有必要，请更换组件。</p> <p>某些设备型号没有存储控制器B</p>
SHLH	运行状况	LDR	<p>如果对对象存储的 "运行状况" 值为 "错误"，请检查并更正：</p> <ul style="list-style-type: none"> 正在挂载的卷出现问题 文件系统错误
SLSA	CPU 负载平均值	SSM	<p>值越高，系统就越繁忙。</p> <p>如果 CPU 负载平均值保持在较高的值，则应调查系统中的事务数，以确定这是否是由于当时的负载过重所致。查看 CPU 负载平均值图表：选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点 _ * > * 网络节点 _ * > * SSM * > * 资源 * > * 报告 * > * 图表 *。</p> <p>如果系统上的负载不大，但问题仍然存在，请联系技术支持。</p>
SMST	日志监控状态	SSM	<p>如果日志监控状态值在一段时间内未连接，请联系技术支持。</p>
SMTT	事件总数	SSM	<p>如果总事件的值大于零，请检查是否存在已知事件（例如网络故障），这些事件可以是发生原因。除非清除了这些错误（即，计数已重置为 0），否则可以触发事件总数警报。</p> <p>解决问题描述后，重置计数器以清除警报。选择 * 节点 * > * 站点 _ * > * 网络节点 _ * > * 事件 * > * 重置事件计数 *。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>要重置事件计数、您必须具有网络拓扑页面配置权限。</p> </div> <p>如果事件总数为零，或者数量增加且问题仍然存在，请联系技术支持。</p>

代码	Name	服务	建议的操作
SNST	Status	CMN	<p>警报表示存储网格任务包时出现问题。如果 " 状态 " 值为 " 检查点错误 " 或 " 未达到仲裁 " ，请确认大多数的 StorageGRID 服务已连接到系统（ 50% 加 1 ），然后等待几分钟。</p> <p>如果问题仍然存在，请联系技术支持。</p>
SOSS	存储操作系统状态	SSM	<p>如果 SANtricity 操作系统指示 StorageGRID 设备中存在组件为 "need attention" 的问题描述、则会触发警报。</p> <p>选择 * 节点 * 。然后选择 * 设备存储节点 * > * 硬件 * 。向下滚动以查看每个组件的状态。在 SANtricity 操作系统中、检查其他设备组件以隔离问题描述。</p>
SSMA	SSM 状态	SSM	<p>如果 SSM Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网络拓扑 * ，然后选择 * 站点 _ * > * 网络节点 _ * > * SSM * > * 概述 * 和 * SSM * > * 概述 * > * 警报 * 以确定警报的发生原因。</p> <p>如果问题仍然存在，请联系技术支持。</p>
SSME	SSM 状态	SSM	<p>如果 "SSM State" 的值为 "Standby" ，请继续监控，如果问题仍然存在，请联系技术支持。</p> <p>如果 "SSM State" 的值为 "Offlin" ，请重新启动此服务。如果问题仍然存在，请联系技术支持。</p>
SST	存储状态	BLDR	<p>如果 "Storage Status" 的值为 "Ininsufficient Available Space" ，则此存储节点上没有更多可用存储，并且数据载入将重定向到其他可用存储节点。可以继续从此网格节点传送检索请求。</p> <p>应添加更多存储。它不会影响最终用户的功能，但警报会持续存在，直到添加更多存储为止。</p> <p>如果 "Storage Status" （存储状态）的值为 "Volume Unavailage" （卷不可用），则表示部分存储不可用。无法从这些卷进行存储和检索。有关详细信息，请检查卷的运行状况：选择 * 支持 * > * 工具 * > * 网络拓扑 * 。然后选择 * 站点 _ * > * 网络节点 _ * > * LDR * > * 存储 * > * 概述 * > * 主 * 。卷的运行状况列在对象存储下。</p> <p>如果 "Storage Status" 的值为 "Error" ，请联系技术支持。</p> <p>"对存储状态（SSTS）警报进行故障排除"</p>

代码	Name	服务	建议的操作
SVST	Status	SSM	<p>解决与未运行的服务相关的其他警报后，此警报将清除。跟踪源服务警报以还原操作。</p> <p>选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点_* > * 网络节点_* > * SSM* > * 服务 * > * 概述 * > * 主 *。如果某个服务的状态显示为未运行，则其状态为 administratively down。此服务的状态可能会列为未运行，原因如下：</p> <ul style="list-style-type: none"> • 此服务已手动停止 (/etc/init.d/<service\> stop)。 • 有一个包含 MySQL 数据库的问题描述，并且 Server Manager 会关闭 MI 服务。 • 已添加网络节点，但尚未启动。 • 在安装期间，网络节点尚未连接到管理节点。 <p>如果某个服务列为未运行、请重新启动此服务 (/etc/init.d/<service\> restart)。</p> <p>此警报还可能指示存储节点的元数据存储（Cassandra 数据库）需要重建。</p> <p>如果问题仍然存在，请联系技术支持。</p> <p>"对服务进行故障排除：状态 - Cassandra（SVST）警报进行故障排除"</p>
TMEM	已安装内存	SSM	<p>如果节点运行的已安装内存小于 24 GiB，则可能会导致性能问题和系统不稳定。系统上安装的内存量应至少增加到 24 GiB。</p>
TPOP	待定操作	模数转换器	<p>消息队列可以指示此 ADA 服务过载。可以连接到 StorageGRID 系统的 ADC 服务太少。在大型部署中，可能需要添加计算资源，或者系统可能需要更多的模数转换服务。</p>
UMEM	可用内存	SSM	<p>如果可用 RAM 较低，请确定这是硬件问题描述 还是软件。如果不是硬件问题描述，或者可用内存降至 50 MB 以下（默认警报阈值），请联系技术支持。</p>
VMFI	条目可用	SSM	<p>这表示需要额外存储。请联系技术支持。</p>

代码	Name	服务	建议的操作
VMFR	可用空间	SSM	<p>如果可用空间值过低（请参见警报阈值），则需要调查是否存在超出比例的日志文件，或者对象占用的磁盘空间过多（请参见警报阈值）需要减少或删除。</p> <p>如果问题仍然存在，请联系技术支持。</p>
VMST	Status	SSM	<p>如果挂载的卷的状态值为未知，则会触发警报。如果值为未知或脱机、则表示由于底层存储设备出现问题、无法挂载或访问卷。</p>
VPRI.	验证优先级	BLDR , BARR	<p>默认情况下，验证优先级的值为自适应。如果验证优先级设置为高，则会触发警报，因为存储验证可能会减慢服务的正常运行速度。</p>
VSTU	对象验证状态	BLDR	<p>选择 * 支持 * > * 工具 * > * 网络拓扑 *。然后选择 * 站点 _ * > * 网络节点 _ * > * LDR * > * 存储 * > * 概述 * > * 主 *。</p> <p>检查操作系统是否存在任何块设备或文件系统错误的迹象。</p> <p>如果对象验证状态的值为未知错误，则通常表示文件系统或硬件问题（I/O 错误）级别较低，从而使存储验证任务无法访问存储的内容。请联系技术支持。</p>
XAMS	无法访问审核存储库	BADC , BARC , BCLB , BCMN , BLDR , BNMS	<p>检查与托管管理节点的服务器的网络连接。</p> <p>如果问题仍然存在，请联系技术支持。</p>

版权信息

版权所有 © 2025 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。