管理警报和警报

StorageGRID

NetApp
October 03, 2025

目录

管理警报和警报 . . . 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 . . . 6
  - 创建自定义警报规则 . . . 8
  - 编辑警报规则 . . . 11
  - 禁用警报规则 . . . 14
  - 删除自定义警报规则 . . . 14
  - 管理警报通知 . . . 15
- 管理警报（旧系统） . . . 25
  - 警报类（旧系统） . . . 25
  - 警报触发逻辑（旧系统） . . . 25
  - 确认当前警报（旧系统） . . . 28
  - 查看默认警报（旧系统） . . . 29
  - 查看历史警报和警报频率（传统系统） . . . 30
  - 创建全局自定义警报（旧系统） . . . 31
  - 禁用警报（旧系统） . . . 33
  - 配置警报通知（旧系统） . . . 37

管理警报和警报

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：

- 网格管理器的信息板上会显示一个警报严重性图标，当前警报计数将递增。
- 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。（并非针对所有警报或警报严重性发送 SNMP 通知。）

比较警报和警报

警报系统与传统警报系统之间存在许多相似之处，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？	• 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 * 。 查看当前警报	选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。 管理警报（旧系统）
触发警报或警报的原因是什么？	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。 查看警报规则	当 StorageGRID 属性达到阈值时，将触发警报。 管理警报（旧系统）
如果触发警报或警报，如何解决根本问题？	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。 StorageGRID 文档会根据需要提供追加信息 。 警报参考	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。 警报参考（旧系统）
在哪里可以看到已解决的警报或警报列表？	选择 * 警报 * > * 已解决 * 。 查看已解决的警报	选择 * 支持 * > * 警报（原有） * > * 历史警报 * 。 管理警报（旧系统）
在何处管理设置？	选择 * 警报 * > * 规则 * 。 管理警报	选择 * 支持 * 。然后，使用菜单 * 警报（原有） * 部分中的选项。 管理警报（旧系统）
我需要哪些用户组权限？	• 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。 管理 StorageGRID	• 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。 • 要管理全局警报和电子邮件通知，您必须同时具有网格拓扑页面配置和其他网格配置权限。 管理 StorageGRID

	警报	警报（旧系统）
如何管理电子邮件通知？	选择 * 警报 * > * 电子邮件设置 * 。 • 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。 为警报设置电子邮件通知	选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 管理警报（旧系统）
如何管理 SNMP 通知？	选择 * 配置 * > * 监控 * > * SNMP 代理 * 。 使用 SNMP 监控	选择 * 配置 * > * 监控 * > * SNMP 代理 * 。 使用 SNMP 监控 • 注 * ： 不会针对每个警报或警报严重性发送 SNMP 通知。 生成 SNMP 通知的警报（旧系统）
如何控制谁接收通知？	1. 选择 * 警报 * > * 电子邮件设置 * 。 2. 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。 为警报设置电子邮件通知	1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 2. 创建邮件列表。 3. 选择 * 通知 * 。 4. 选择邮件列表。 管理警报（旧系统）
哪些管理节点会发送通知？	一个管理节点（ "`preferred sender"` ）。 管理 StorageGRID	一个管理节点（ "`preferred sender"` ）。 管理 StorageGRID

	警报	警报（旧系统）
如何禁止某些通知？	1. 选择 * 警报 * > * 静音 * 。 2. 选择要静默的警报规则。 3. 指定静默的持续时间。 4. 选择要静默的警报的严重性。 5. 选择可对整个网格，单个站点或单个节点应用静默。 ◦ 注 * ： 如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 静默警报通知	1. 选择 * 支持 * > * 警报（旧版） * > * 旧版电子邮件设置 * 。 2. 选择 * 通知 * 。 3. 选择一个邮件列表，然后选择 * 禁止 * 。 管理警报（旧系统）
如何禁止所有通知？	选择 * 警报 * > * 静音 * 。然后选择 * 所有规则 * 。 • 注 * ： 如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。 静默警报通知	1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。 2. 选中 * 通知禁止全部 * 复选框。 ◦ 注 * ： 在系统范围内禁止电子邮件通知还会禁止事件触发的 AutoSupport 电子邮件。 管理警报（旧系统）
如何自定义条件和触发器？	1. 选择 * 警报 * > * 规则 * 。 2. 选择要编辑的默认规则，或者选择 * 创建自定义规则 * 。 编辑警报规则 创建自定义警报规则	1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。 2. 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。 管理警报（旧系统）
如何禁用单个警报？	1. 选择 * 警报 * > * 规则 * 。 2. 选择规则，然后选择 * 编辑规则 * 。 3. 取消选中 * 已启用 * 复选框。 禁用警报规则	1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。 2. 选择规则，然后选择编辑图标。 3. 取消选中 * 已启用 * 复选框。 管理警报（旧系统）

管理警报

管理警报：概述

通过警报，您可以监控 StorageGRID 系统中的各种事件和状况。您可以通过创建自定义警

报，编辑或禁用默认警报，设置警报电子邮件通知以及使警报通知静音来管理警报。

关于 **StorageGRID** 警报

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。

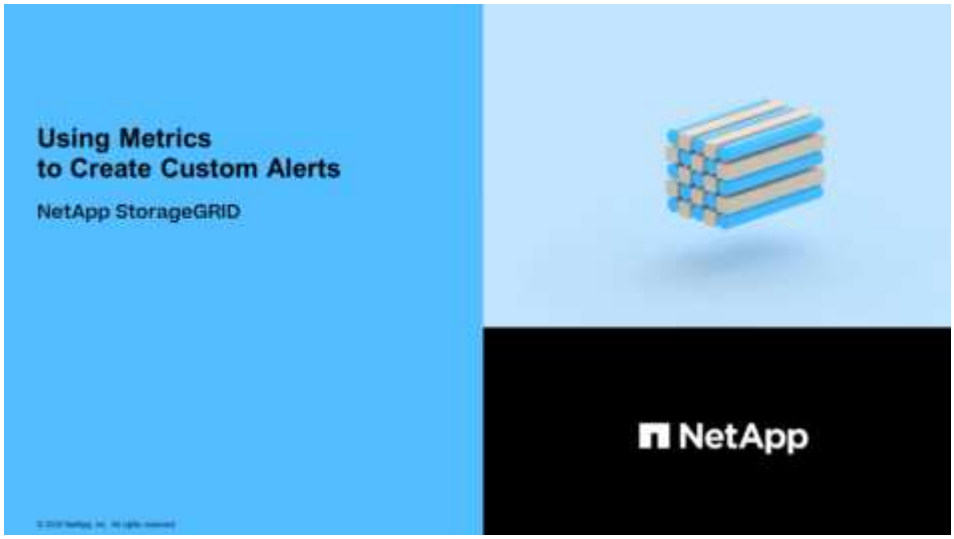
- 警报系统侧重于系统中可操作的问题。对于需要您立即关注的事件，系统会触发警报，而对于可以安全忽略的事件，则不会触发警报。
- " 当前警报 " 页面提供了一个便于用户查看当前问题的界面。您可以按各个警报和警报组对列表进行排序。例如，您可能希望按节点 / 站点对所有警报进行排序，以查看哪些警报正在影响特定节点。或者，您可能希望按触发时间对组中的警报进行排序，以查找特定警报的最新实例。
- " 已解决警报 " 页面提供的信息与 " 当前警报 " 页面上的信息类似，但您可以搜索和查看已解决警报的历史记录，包括警报触发时间和解决时间。
- 同一类型的多个警报会分组到一个电子邮件中，以减少通知数量。此外，同一类型的多个警报将在警报页面上显示为一个组。您可以展开和折叠警报组以显示或隐藏各个警报。例如，如果多个节点报告 "* 无法与节点 * 通信 " 警报大致同时出现，则只会发送一封电子邮件，并且警报会在警报页面上显示为一个组。
- 警报使用直观的名称和说明来帮助您快速了解问题。警报通知包括有关受影响节点和站点的详细信息，警报严重性，触发警报规则的时间以及与警报相关的指标的当前值。
- 警报电子邮件通知以及 " 当前警报 " 和 " 已解决警报 " 页面上的警报列表提供了解决警报的建议操作。这些建议操作通常包括直接链接到 StorageGRID 文档中心，以便于查找和访问更详细的故障排除过程。
- 如果需要在一个或多个严重性级别临时禁止警报通知，您可以轻松地在指定持续时间内对整个网格，单个站点或单个节点静默特定警报规则。您还可以将所有警报规则静默，例如，在软件升级等计划内维护操作步骤期间。
- 您可以根据需要编辑默认警报规则。您可以完全禁用警报规则，也可以更改其触发条件和持续时间。
- 您可以创建自定义警报规则，以确定与您的情况相关的特定条件，并提供您自己的建议操作。要定义自定义警报的条件，请使用网格管理 API 的 " 指标 " 部分提供的 Prometheus 指标创建表达式。

了解更多信息。

要了解更多信息，请查看以下视频：

- "视频：警报概述"

- "视频：使用指标创建自定义警报"



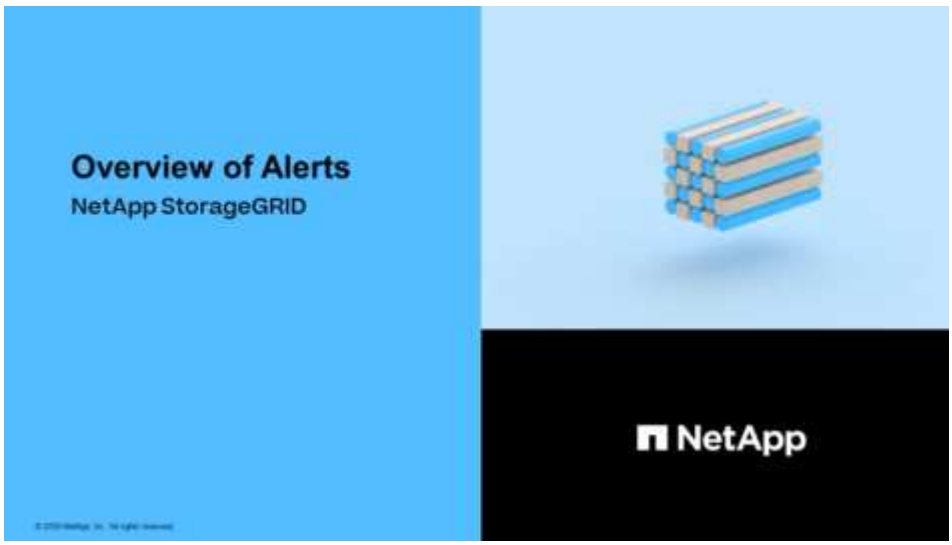
查看警报规则

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。

您需要的内容

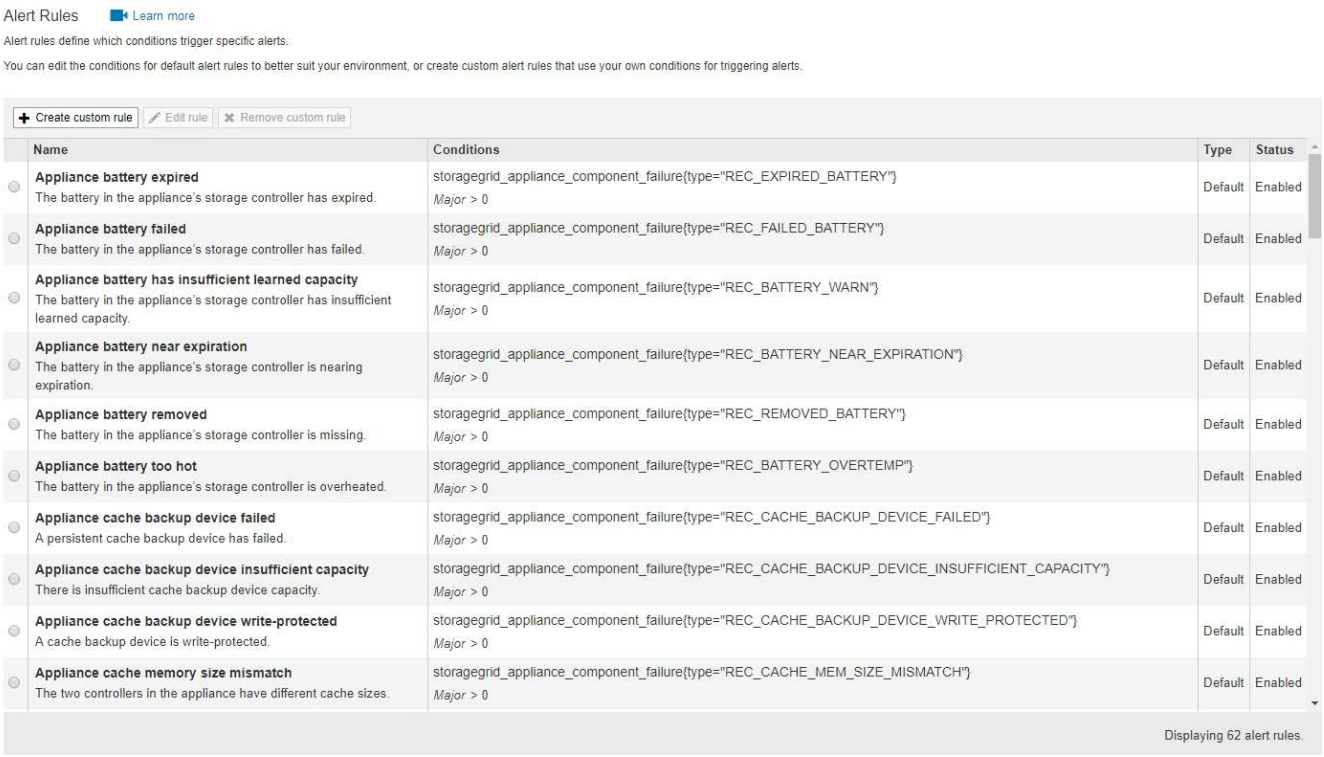
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。
- 您也可以观看以下视频： "视频：警报概述"



步骤

1. 选择 * 警报 * > * 规则 * 。

此时将显示 "Alert Rules" 页面。



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	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。 • * 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。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。

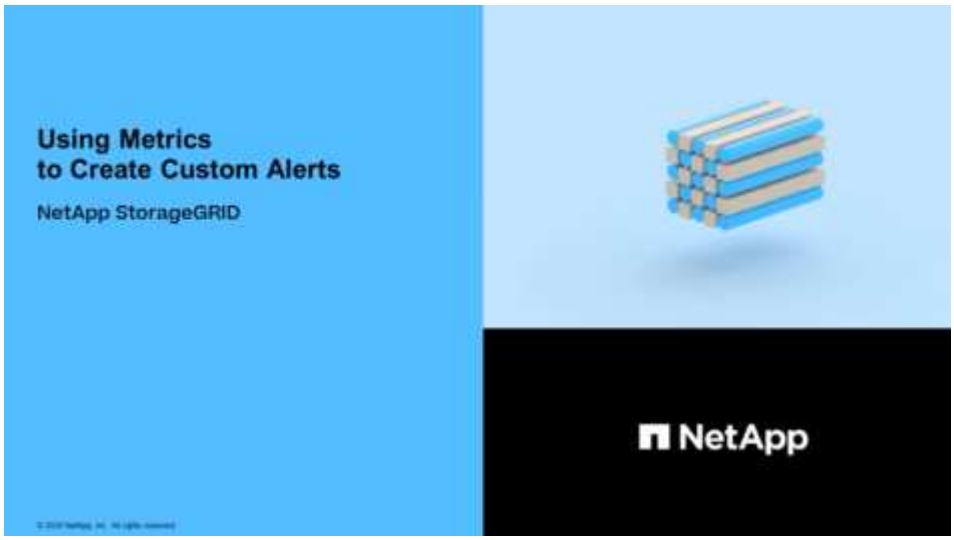
列标题	Description
Type	警报规则的类型： • * 默认 * ： 随系统提供的警报规则。您可以禁用默认警报规则或编辑默认警报规则的条件和持续时间。您不能删除默认警报规则。 • * 默认值 * ： 包含已编辑条件或持续时间的默认警报规则。根据需要，您可以轻松地将修改后的条件还原回原始默认值。 • * 自定义 * ： 创建的警报规则。您可以禁用，编辑和删除自定义警报规则。
Status	当前是否已启用此警报规则。不会评估已禁用警报规则的条件，因此不会触发任何警报。

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。

您需要的内容

- 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 " 根访问 " 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：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。
- 在使用网格管理 API 测试表达式时，请注意 " `s`成功 " 响应可能只是空响应正文（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，要测试表达式 `node_memory_MemTotal_bytes < 240000000` ，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。

- 除非您验证警报是在预期时间触发的，否则请勿假定自定义警报正在运行。

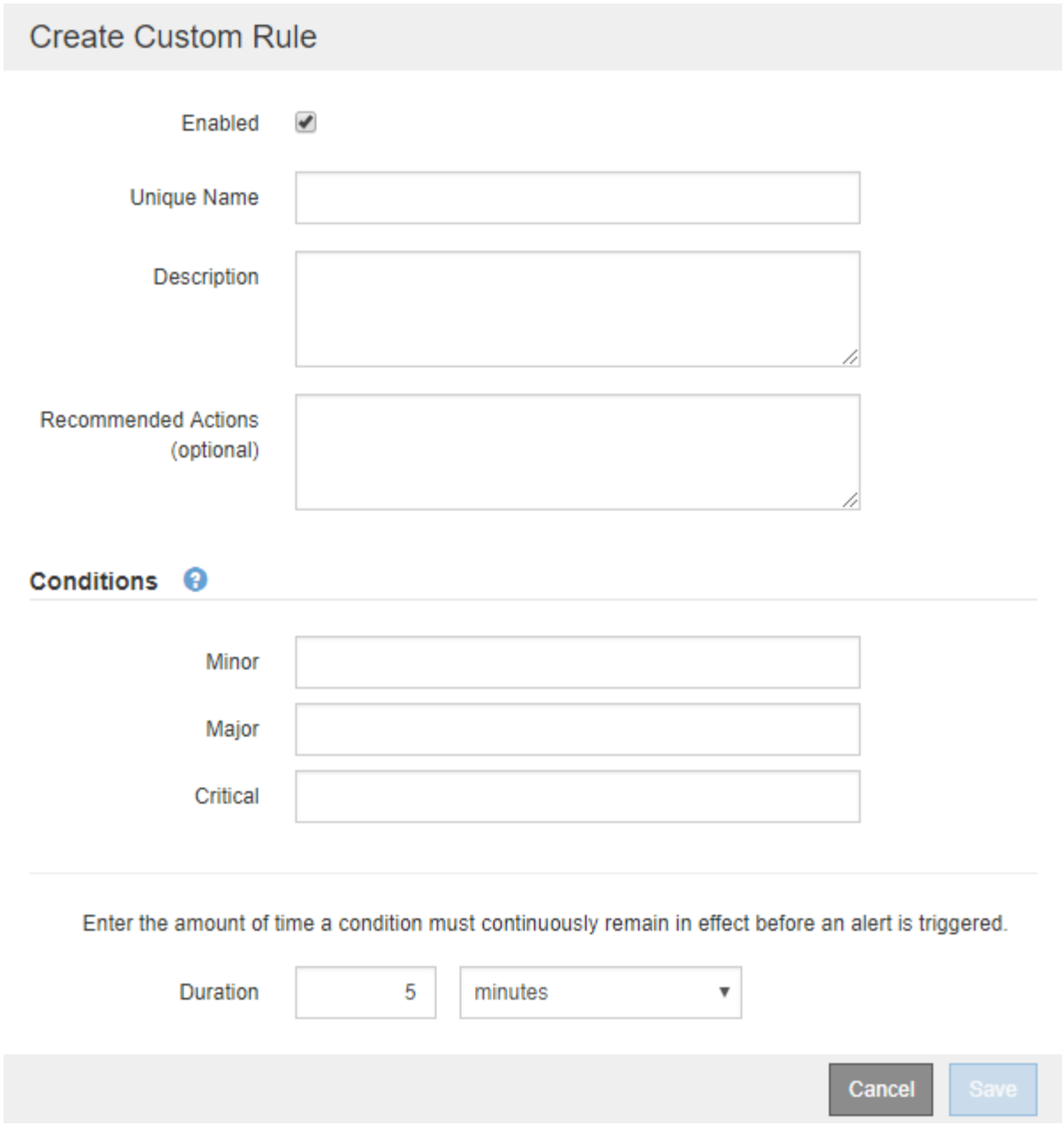
步骤

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。



3. 选中或取消选中 * 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，则不会评估其表达式，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。

字段	Description
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：

   `，指标，运算符，值，`

   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 < 240000000
   ```

   要查看可用指标并测试 Prometheus 表达式，请选择帮助图标 并单击网格管理 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。

您需要的内容

- 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 " 根访问 " 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。

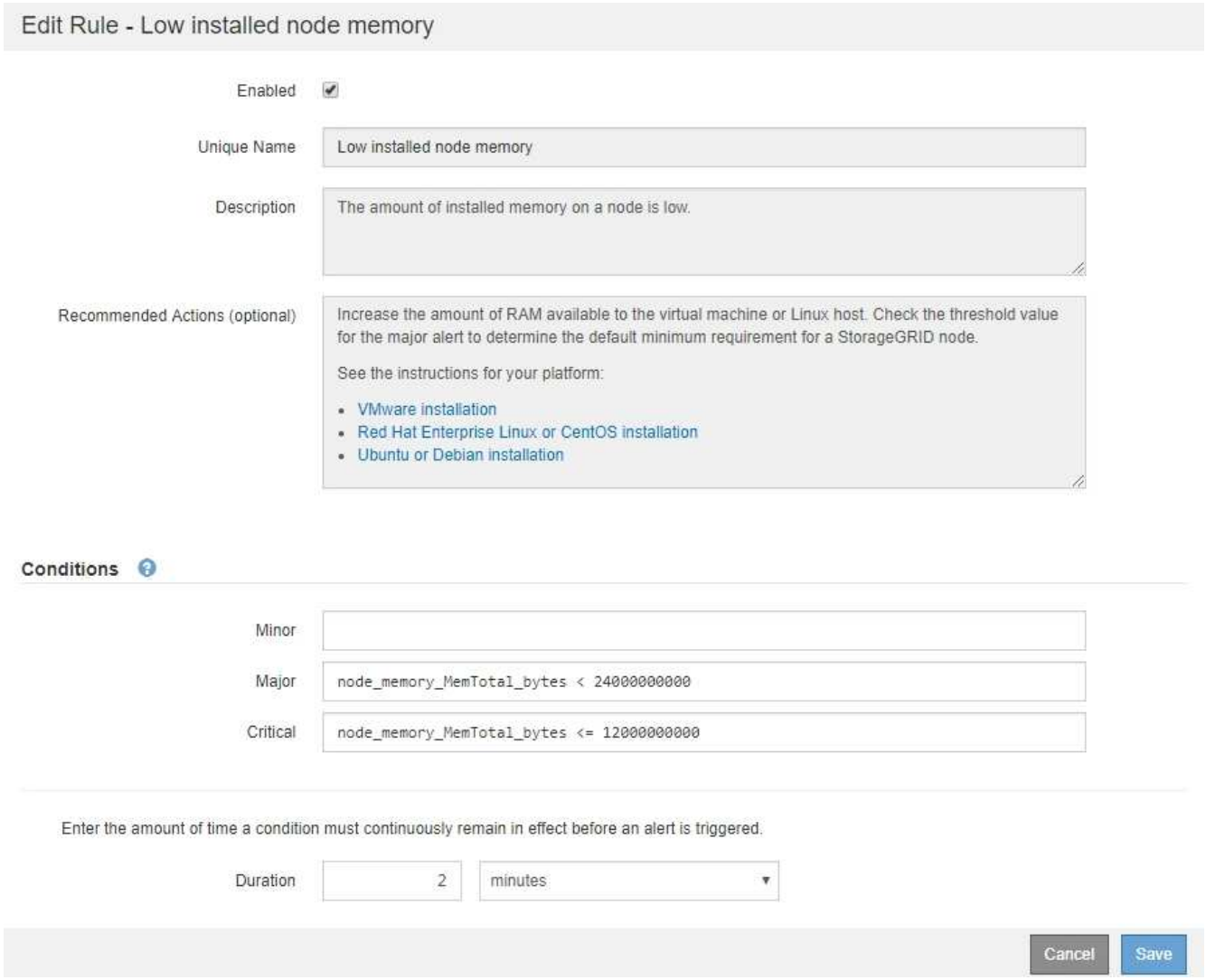
步骤

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— Unique Name ，问题描述 和 Recommended Actions 字段已禁用，无法编辑。



4. 选中或取消选中 * 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，则不会评估其表达式，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。

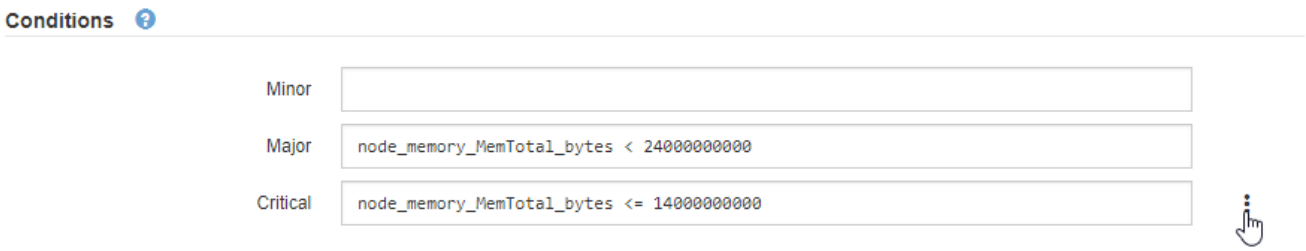
5. 对于自定义警报规则，请根据需要更新以下信息。

您不能为默认警报规则编辑此信息。

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。

如果要将已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。



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：

`，指标，运算符，值，`

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 < 240000000
```

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。

您需要的内容

- 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 " 根访问 " 权限。

关于此任务

禁用警报规则后，不会评估其表达式，也不会触发任何警报。

> 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. 选中或取消选中 * 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，则不会评估其表达式，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。

您需要的内容

- 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 " 根访问 " 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。

您不能删除默认警报规则。

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。

您可以使用网格管理器中的 * 配置 * > * 监控 * > * SNMP 代理 * 选项或网格管理 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：

- 陷阱是指 SNMP 代理发送的通知，不需要管理系统确认。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。

警报通知由配置为首选发送方的任何管理节点发送。默认情况下，会选择主管理节点。请参见 有关管理 StorageGRID 的说明。

> 在指定严重性级别或更高级别触发某些警报（传统系统）时，也会发送陷阱和通知通知通知；但是，不会针对每个警报或每个警报严重性发送 SNMP 通知。请参见 生成 SNMP 通知的警报（旧系统）。

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。

您需要的内容

- 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 " 根访问 " 权限。

关于此任务

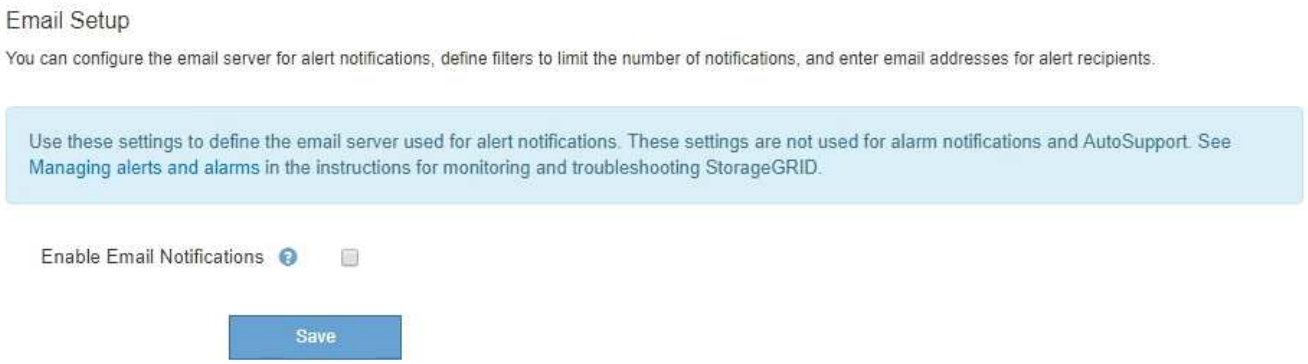
由于警报和警报是独立的系统，因此用于警报通知的电子邮件设置不会用于警报通知和 AutoSupport 消息。但是，您可以对所有通知使用同一个电子邮件服务器。

如果您的 StorageGRID 部署包含多个管理节点，则可以选择哪个管理节点应是警报通知的首选发送方。警报通知和 AutoSupport 消息也会使用相同的 "`首选发件人` " 。默认情况下，会选择主管理节点。有关详细信息，请参见 有关管理 StorageGRID 的说明。

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。



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。
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。

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。

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用于身份验证的客户端证书，请选中 * 发送客户端证书 * 复选框。

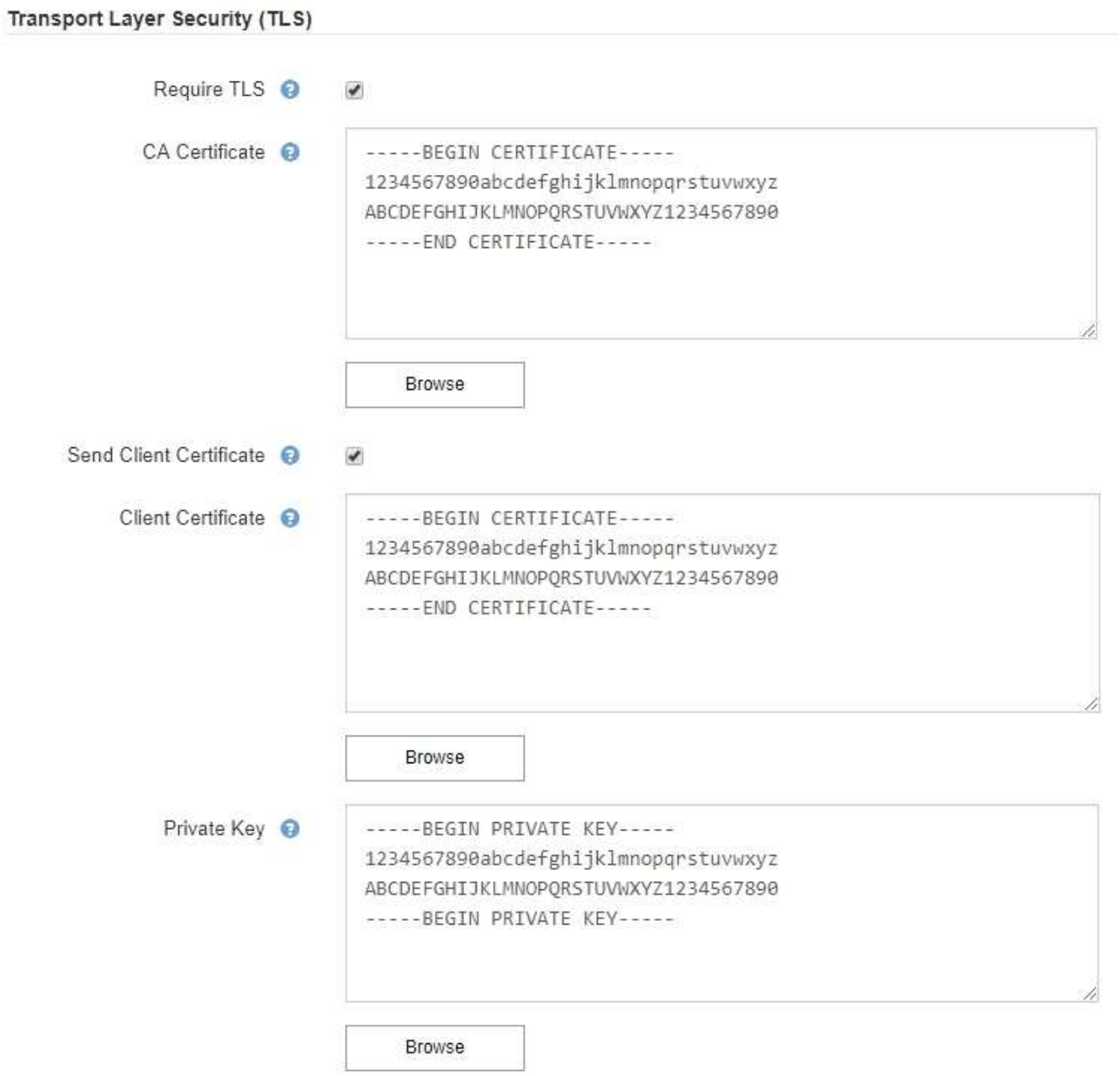
   c. 在 * 客户端证书 * 字段中，提供 PEM 编码的客户端证书以发送到 SMTP 服务器。

      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。



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。
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。对于次要或主要警报，不会发送通知。

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。这与测试警报通知和 AutoSupport 消息不同，所有管理节点都会发送测试电子邮件。

8. 选择 * 保存 * 。

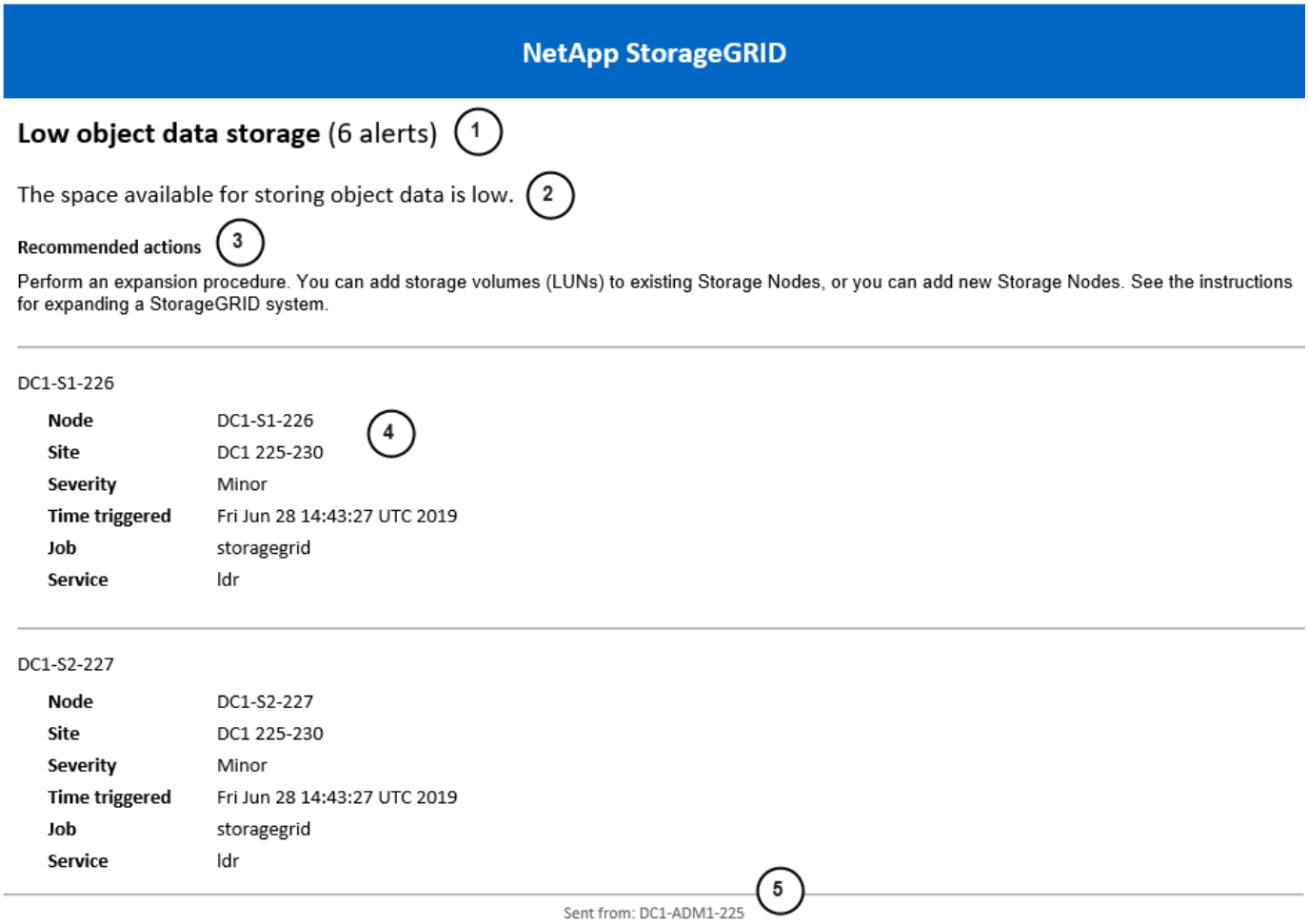
   发送测试电子邮件不会保存您的设置。您必须选择 * 保存 * 。

   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：



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。	• 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。	• 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。	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。	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。	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。	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。

您需要的内容

- 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 " 根访问 " 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不会阻止来自发件人地址的电子邮件。
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。

您需要的内容

- 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 " 根访问 " 权限。

关于此任务

您可以对整个网格，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。

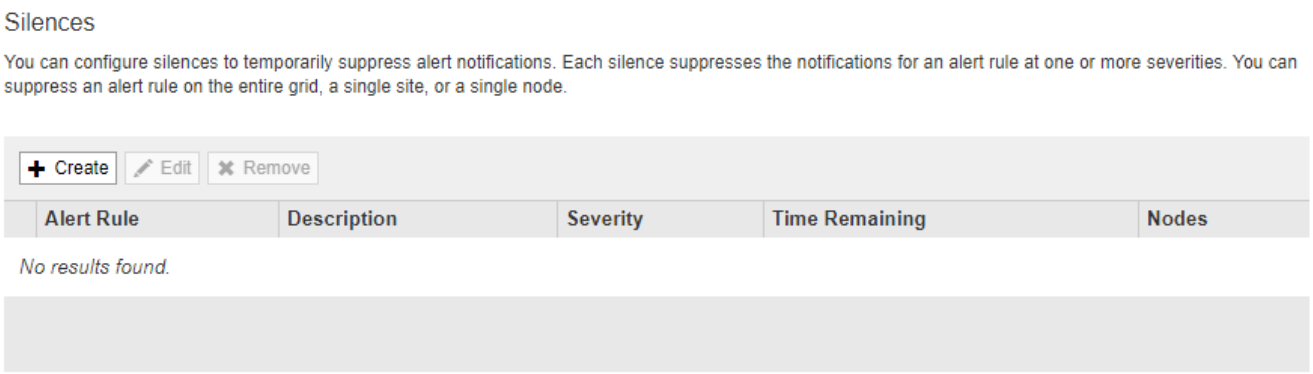
> 在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

> 由于警报和警报是独立的系统，因此不能使用此功能禁止警报通知。

步骤

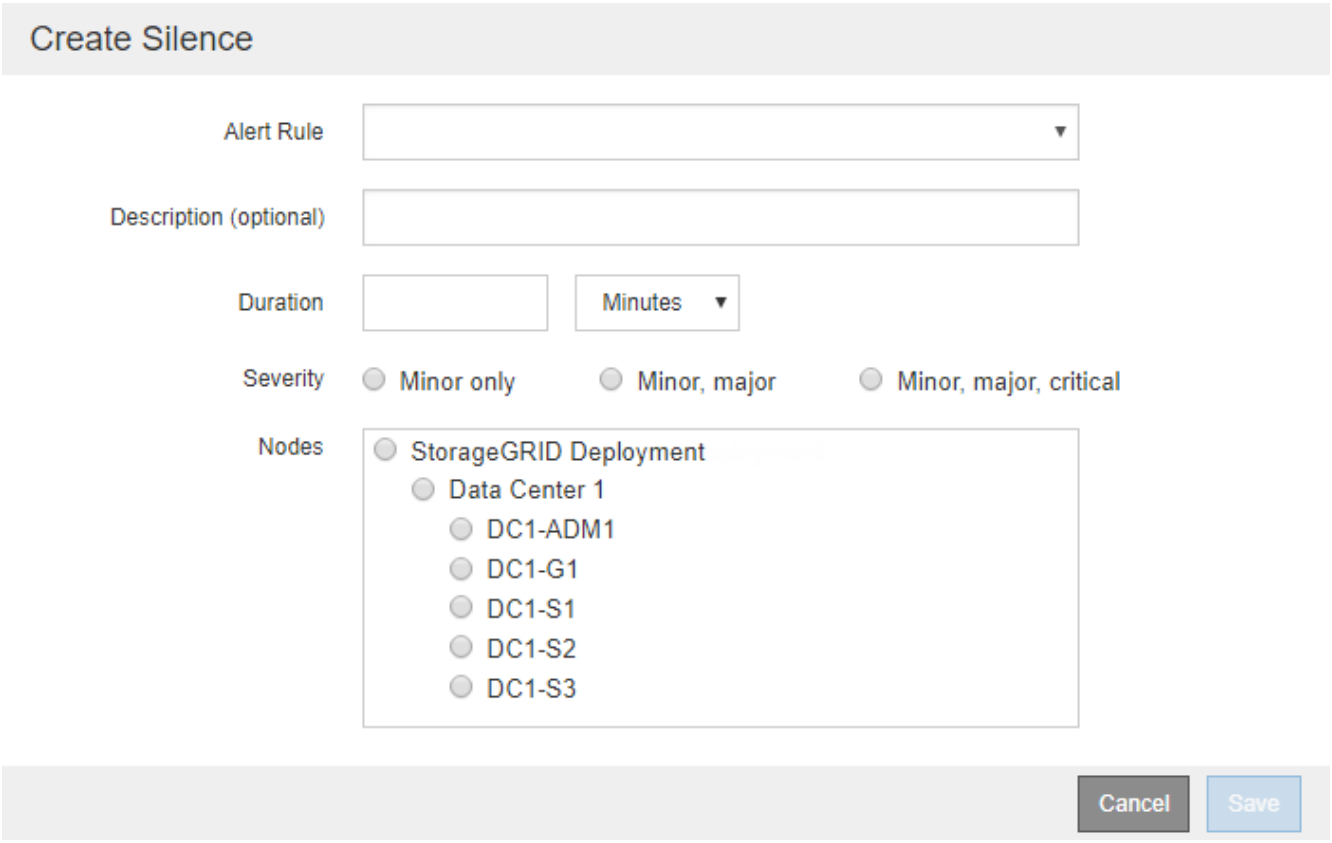
1. 选择 * 警报 * > * 静音 * 。

   此时将显示 Silences 页面。



2. 选择 * 创建 * 。

   此时将显示创建静默对话框。



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	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）。 • 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	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。
节点	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。 • 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。

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	a. 选择 * 警报 * > * 静音 * 。 b. 从表中，选择要编辑的静默设置对应的单选按钮。 c. 选择 * 编辑 * 。 d. 更改问题描述 ，剩余时间，选定严重性或受影响的节点。 e. 选择 * 保存 * 。
取消静默	a. 选择 * 警报 * > * 静音 * 。 b. 从表中，选择要删除的静默设置对应的单选按钮。 c. 选择 * 删除 * 。 d. 选择 * 确定 * 确认要删除此静默状态。 ◦ 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。

相关信息

- 配置 SNMP 代理

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	>= 15 ， 000	>= 1000
major	>=150 ， 000	>= 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 ）。

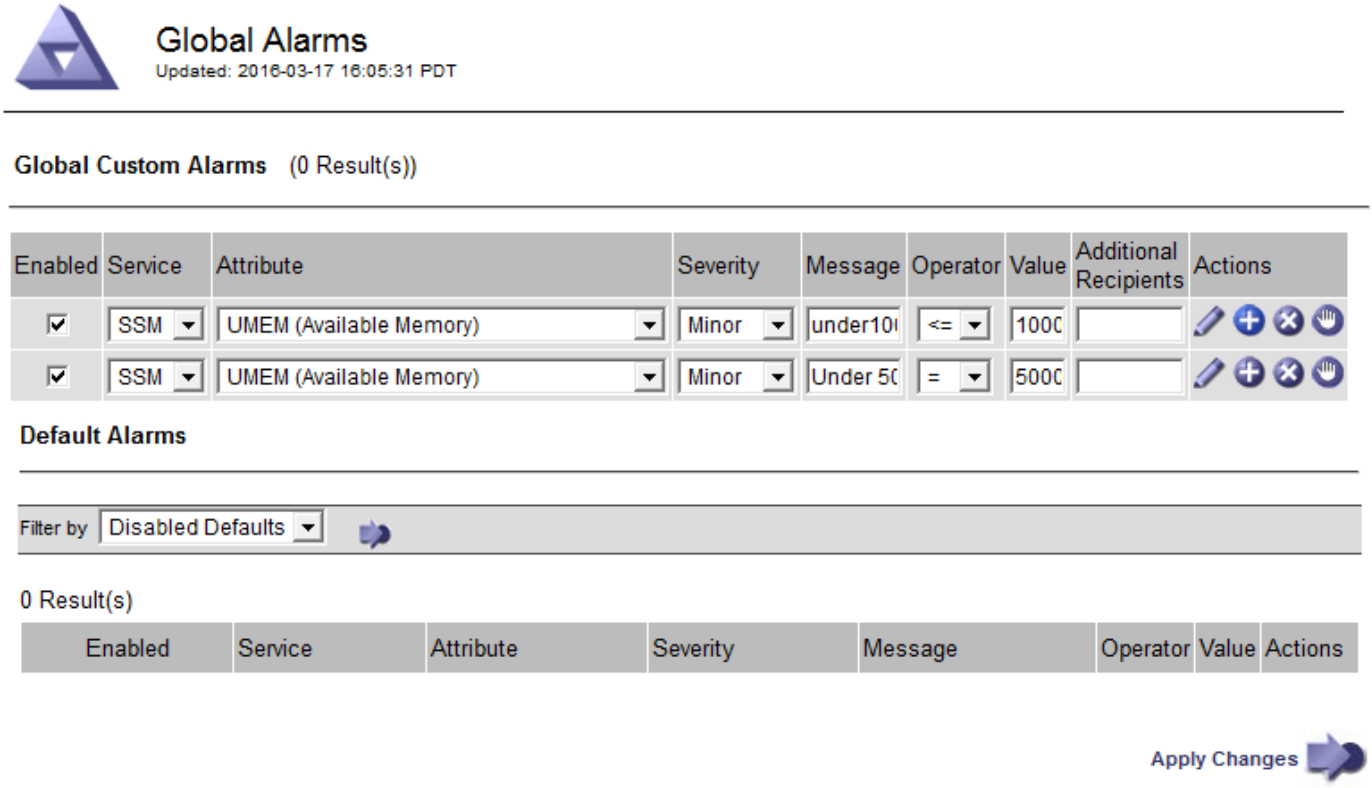
Global Alarms

Updated: 2016-03-17 16:05:31 PDT

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	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 ）。



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。不能为表中的各个行禁用警报。

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的 VMFI 警报（当前严重警报均会在表中显示为绿色）； 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。

您需要的内容

- 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。您通常可以忽略警报（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。

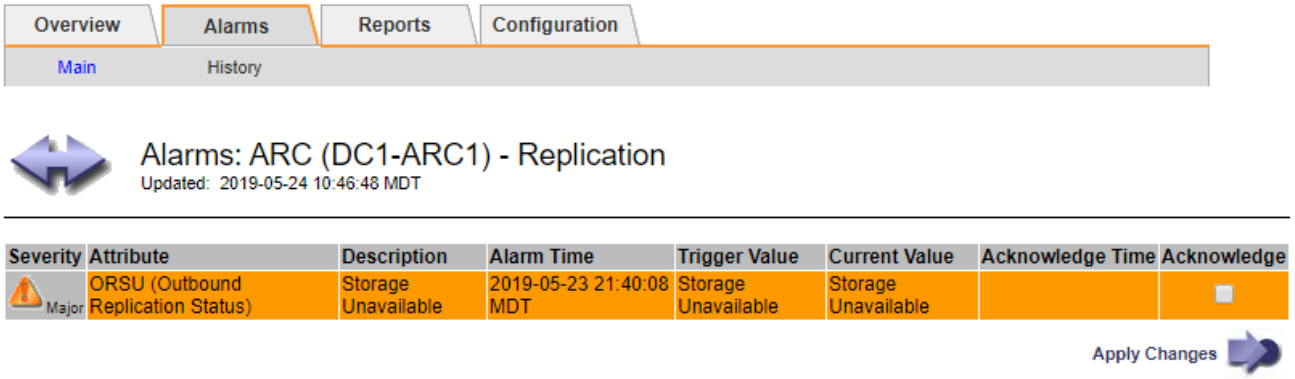
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。

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 * > * 网格拓扑 * > * 网格节点 _* > * 服务 _* > * 警报 * ）。



3. 选中警报的 * 确认 * 复选框，然后单击 * 应用更改 * 。

   警报不再显示在信息板或当前警报页面上。

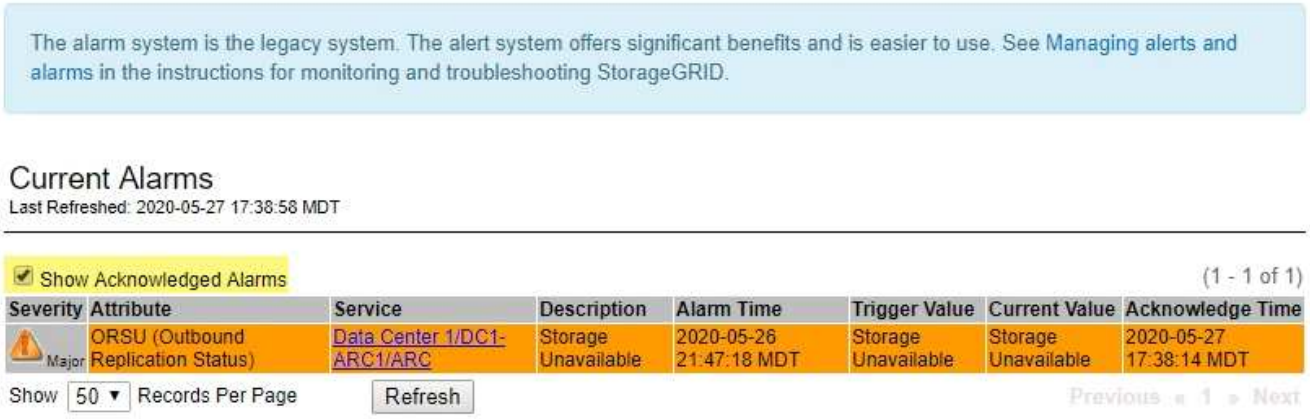
   确认警报后，确认不会复制到其他管理节点。因此，如果您从另一个管理节点查看信息板，则可能仍会看到活动警报。

4. 根据需要查看已确认的警报。

   a. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。

   b. 选择 * 显示已确认警报 * 。

      此时将显示任何已确认的警报。



查看默认警报（旧系统）

您可以查看所有默认旧警报的列表。

您需要的内容

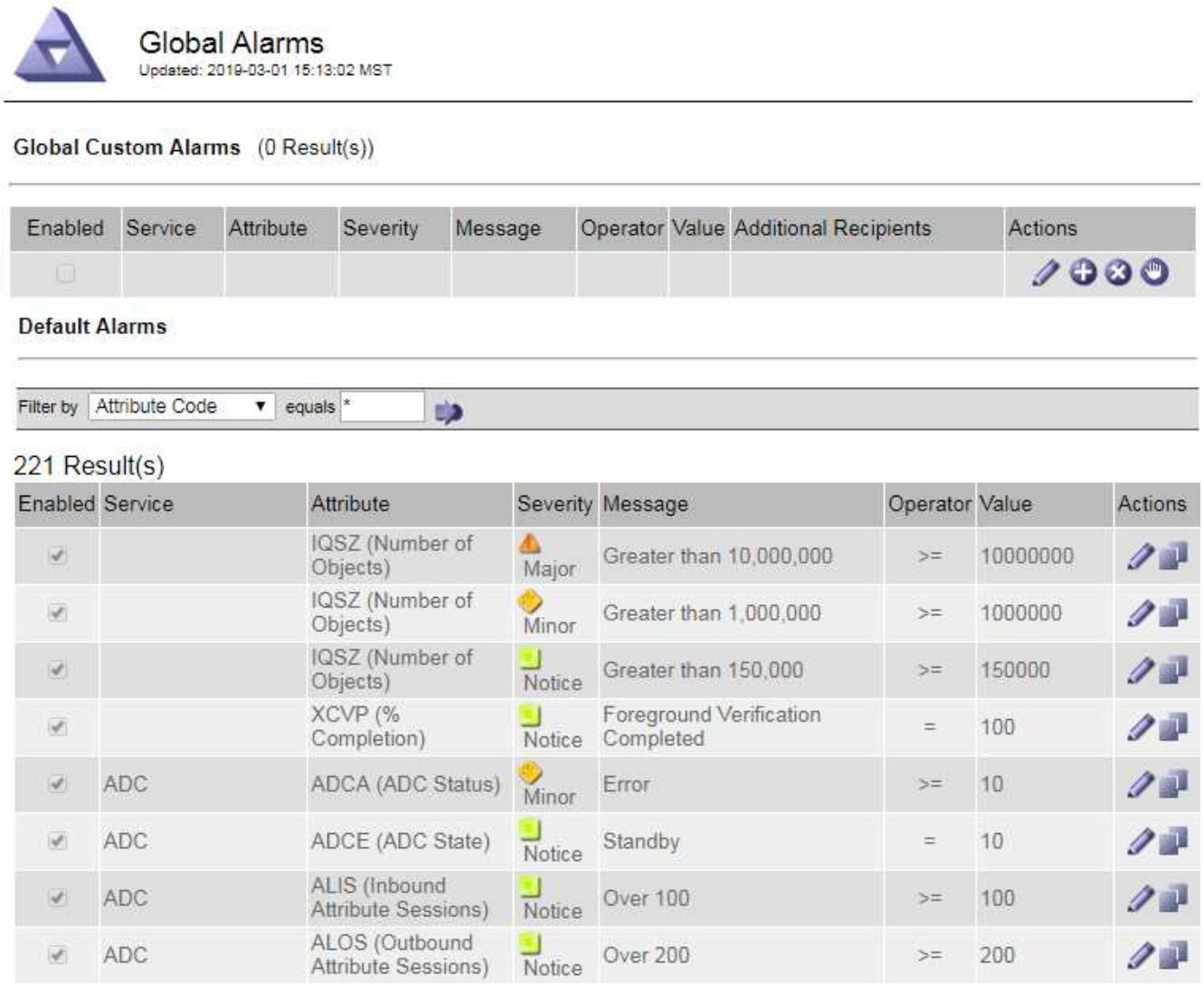
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

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，输入星号： ` *`
4. 单击箭头 或按 * 输入 * 。

   此时将列出所有默认警报。



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。

您需要的内容

- 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. 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。全局自定义警报可能具有覆盖默认警报的警报级别，或者它们可能会监控没有默认警报的属性。

您需要的内容

- 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。

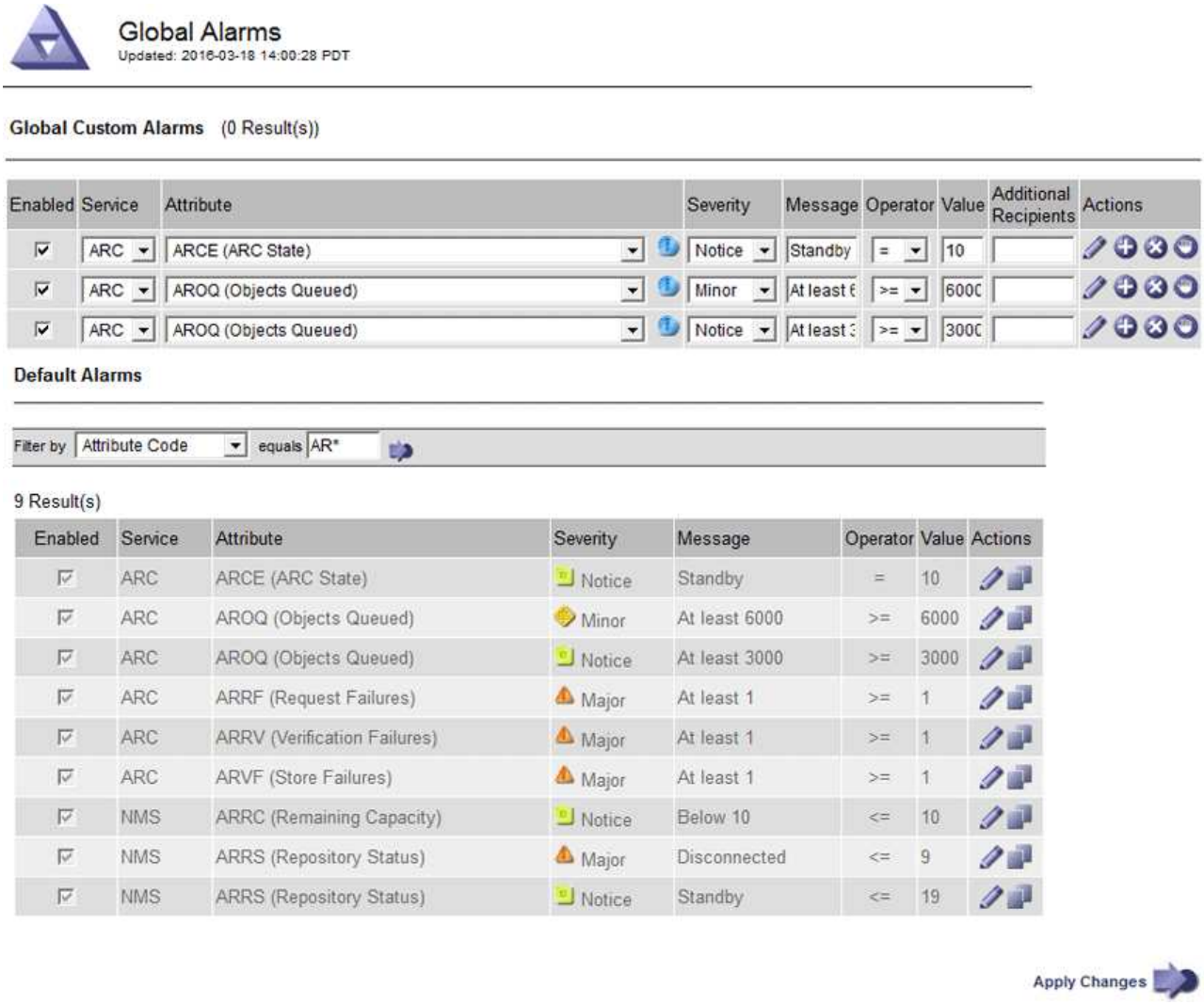
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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。

如果更改警报设置，请务必小心。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 * 。



- 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	选中或取消选中此复选框可启用或禁用警报。

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	用于根据值阈值测试当前属性值的运算符： • = 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	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。 • 注： * 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。
操作	控制按钮用于： 编辑行 + 插入一行 + 删除行 + 上下拖放一行 + 复制行

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。

您需要的内容

- 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。

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。

在完全过渡到新警报系统之前，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

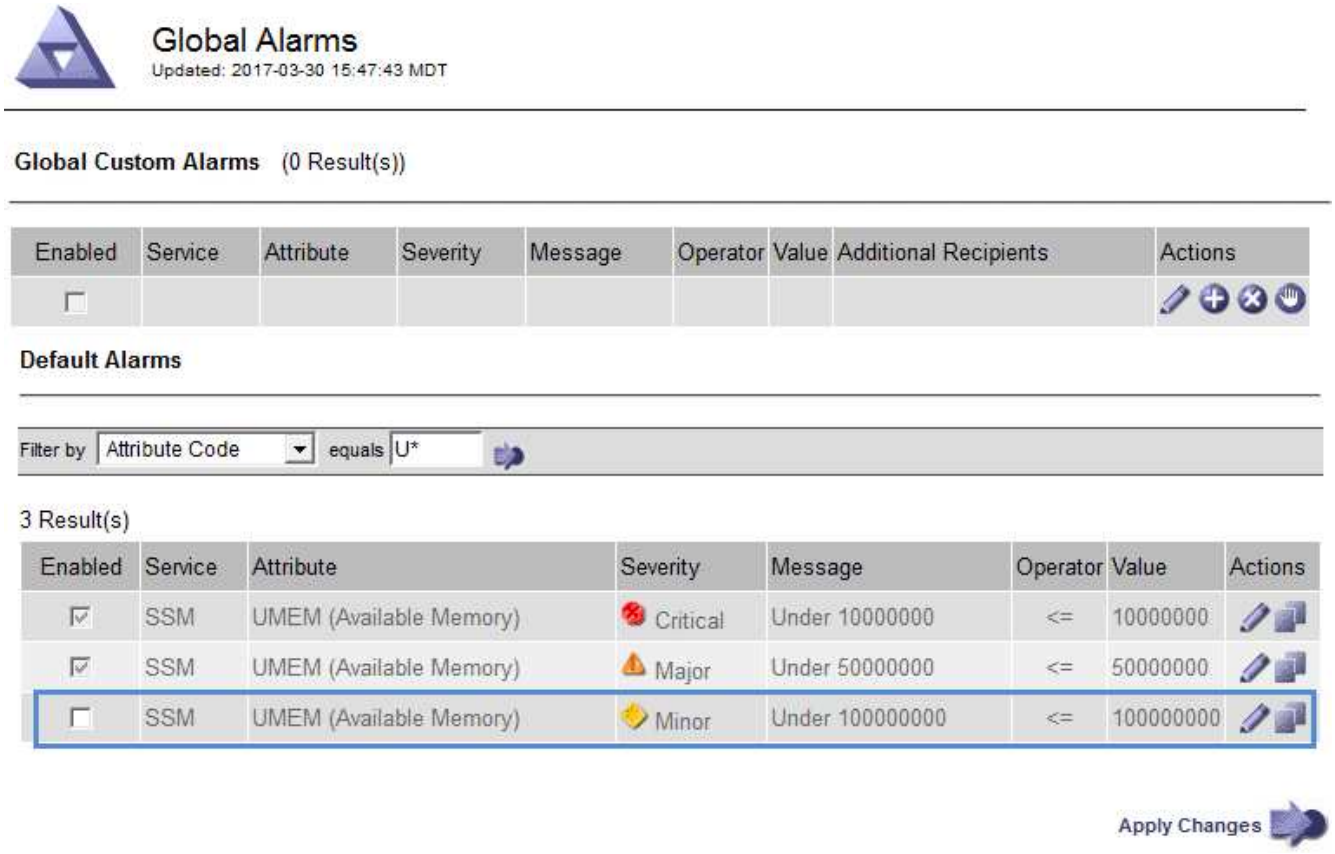
1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 搜索要禁用的默认警报。
   a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 * 。
   b. 键入搜索字符串。

      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。



选定警报的 * 已启用 * 复选框将变为活动状态。

4. 取消选中 * 已启用 * 复选框。
5. 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。

您需要的内容

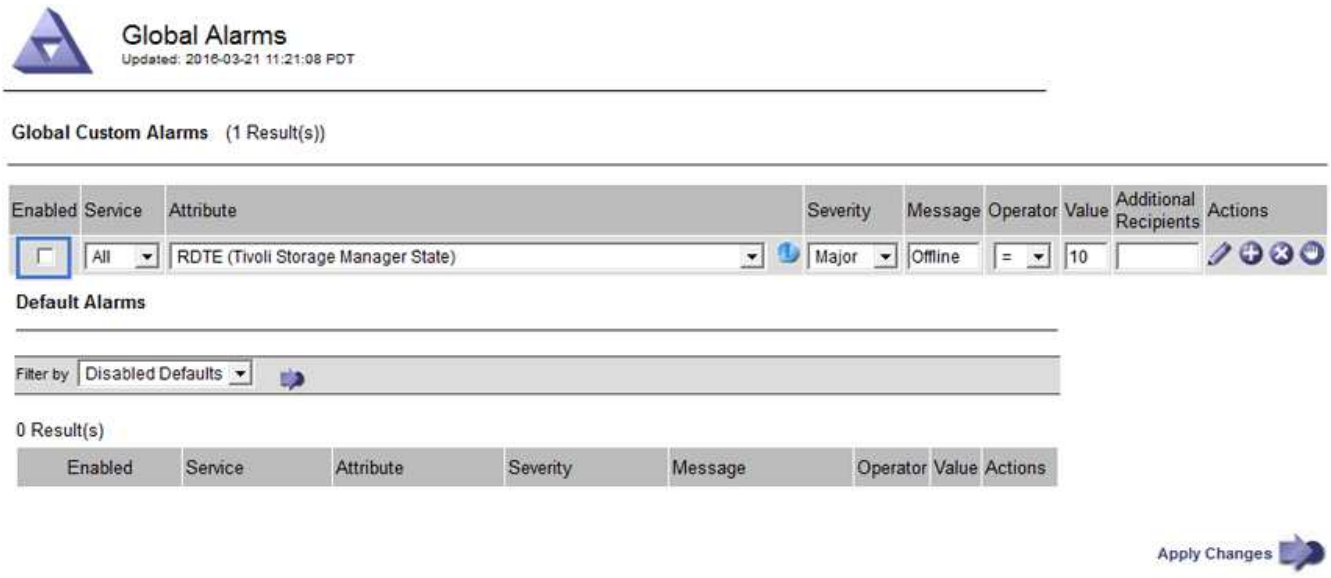
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

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. 取消选中 * 已启用 * 复选框。



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。

您需要的内容

- 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 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 重新启动 NMS 服务： `sservice 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。

您需要的内容

- 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。

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。

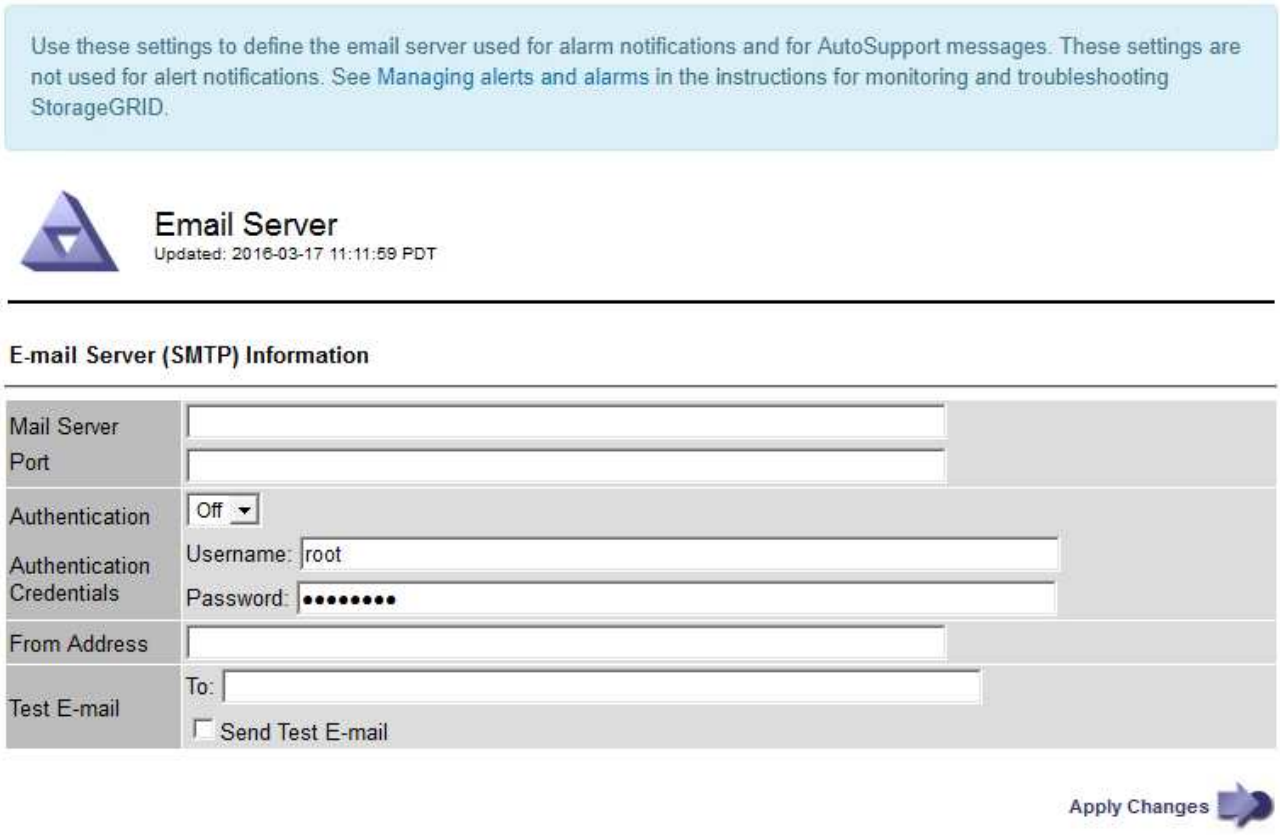
> 如果使用 SMTP 作为 AutoSupport 消息的协议，则可能已配置 SMTP 邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤 。请参见 有关管理 StorageGRID 的说明。

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。



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。

您需要的内容

- 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。

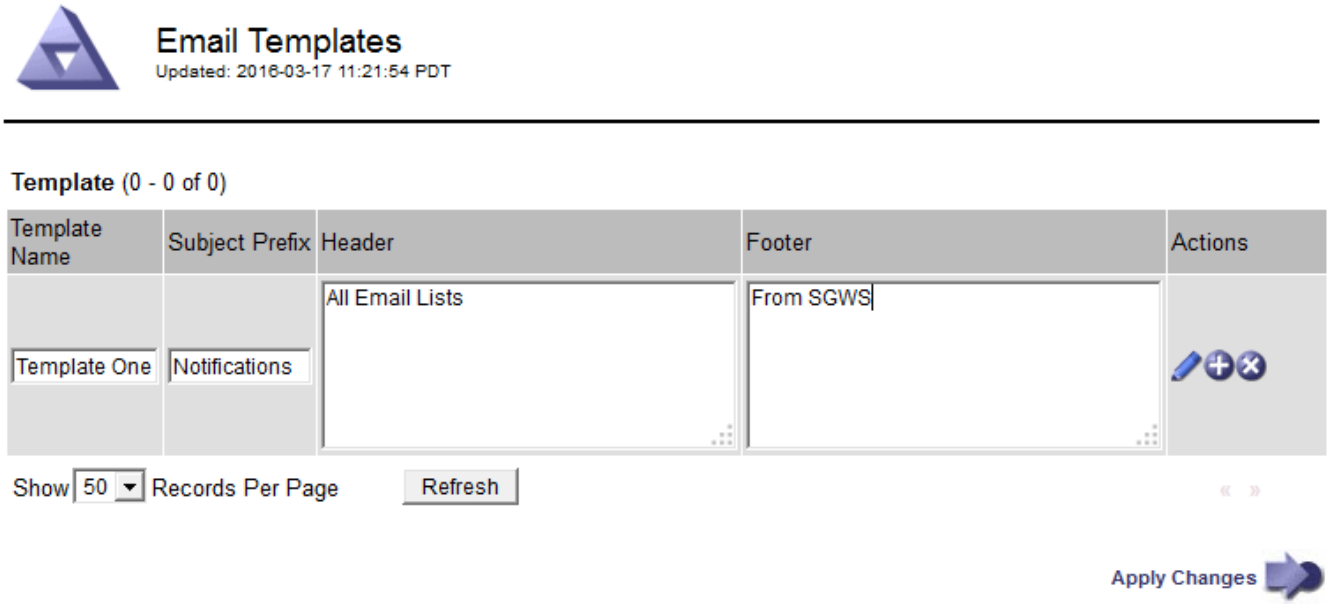
关于此任务

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。模板不包含电子邮件的正文。

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）。



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。

您需要的内容

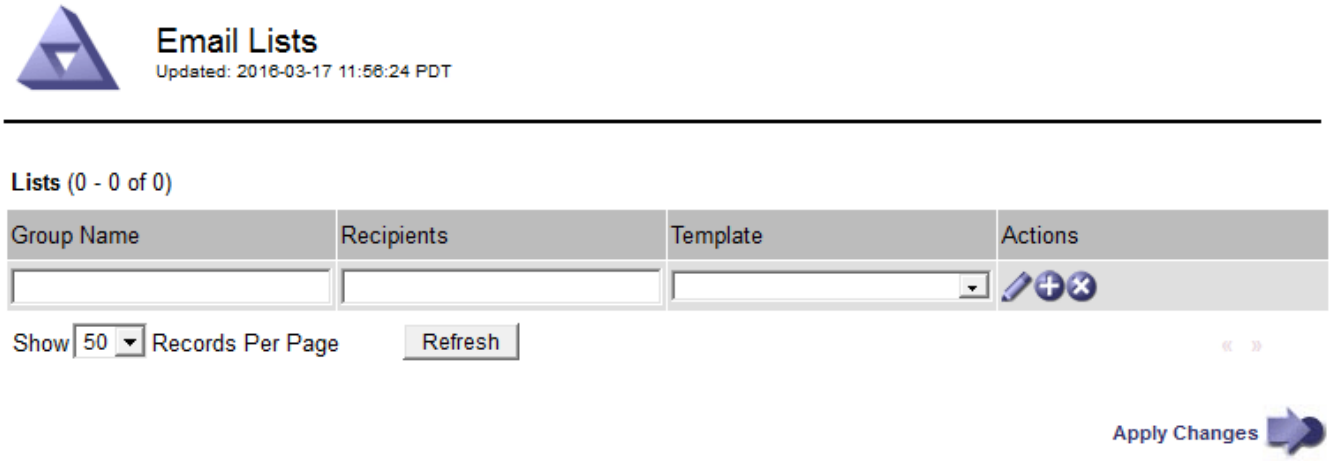
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

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）。



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。邮件列表名称不能重复。 • 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。 • 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）

要接收旧警报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。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。

您需要的内容

- 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。
- 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。

您需要的内容

- 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。

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，或者选择列顶部的 * 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。

在系统范围内禁止电子邮件通知

您可以阻止 StorageGRID 系统针对旧警报和事件触发的 AutoSupport 消息发送电子邮件通知。

您需要的内容

- 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。

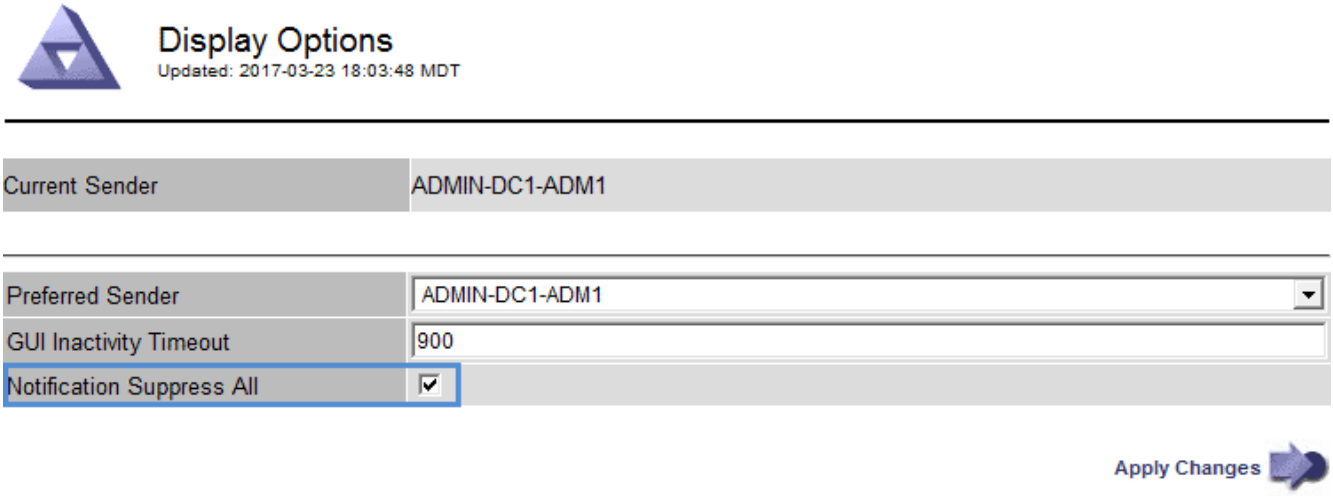
关于此任务

使用此选项可禁止对原有警报和事件触发的 AutoSupport 消息发送电子邮件通知。

此选项不会禁止警报电子邮件通知。它也不会禁止每周或用户触发的 AutoSupport 消息。

步骤

1. 选择 * 配置 * > * 系统设置 * > * 显示选项 * 。
2. 从显示选项菜单中，选择 * 选项 * 。
3. 选择 * 通知禁止全部 * 。



4. 单击 * 应用更改 * 。

通知页面（ * 配置 * > * 通知 * ）显示以下消息：

Notifications

Updated: 2016-03-17 14:06:48 PDT

All e-mail notifications are now suppressed.

Notifications (0 - 0 of 0)

	Suppress	Severity Levels				Service States		
E-mail List	☑	Notice	Minor	Major	Critical	Unknown	Administratively Down	Actions
	☐	☐	☐	☐	☐	☐	☐	

Show 50 Records Per Page Refresh

« »

Apply Changes