使用 SNMP 监控

StorageGRID 11.8

NetApp
March 19, 2024

目录

使用 SNMP 监控

使用SNMP监控：概述

如果要使用简单网络管理协议（ Simple Network Management Protocol ， SNMP ）监控 StorageGRID ，则必须配置 StorageGRID 附带的 SNMP 代理。

- "配置 SNMP 代理"
- "更新 SNMP 代理"

功能

每个StorageGRID 节点都运行一个SNMP代理或守护进程、用于提供MIB。StorageGRID MIB 包含警报和警报的表和通知定义。MIB 还包含系统问题描述 信息，例如每个节点的平台和型号。每个 StorageGRID 节点还支持一组 MIB-II 对象。

> 请参见 "访问MIB文件" 要在网格节点上下载MIB文件的选项。

最初，所有节点上都会禁用 SNMP 。配置 SNMP 代理时，所有 StorageGRID 节点都会收到相同的配置。

StorageGRID SNMP 代理支持所有三个版本的 SNMP 协议。它为查询提供只读 MIB 访问权限，并可向管理系统发送两种类型的事件驱动型通知：

陷阱
: 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
: 通知与陷阱类似，但需要管理系统确认。如果SNMP代理未在一定时间内收到确认、则会重新发送通知、直到收到确认或已达到最大重试值为止。

  SNMPv2c 和 SNMPv3 支持 INFORM 。

在以下情况下会发送陷阱和通知通知通知：

- 默认或自定义警报将在任何严重性级别触发。要禁止警报的SNMP通知、您必须执行此操作 "配置静音" 警报。警报通知由发送 "首选发件人管理节点"。

  每个警报都会根据警报的严重性级别映射到以下三种陷阱类型之一： activeMinorAlert ， activeMajorAlert 和 activeCriticalAlert 。有关可触发这些陷阱的警报列表、请参见 "警报参考"。

- 肯定的 "警报(传统系统)" 在指定严重性级别或更高级别触发。

  > 不会针对每个警报或每个警报严重性发送SNMP通知。

SNMP 版本支持

下表简要总结了每个 SNMP 版本支持的功能。

	SNMPv1	SNMPv2c	SNMPv3
查询	只读 MIB 查询	只读 MIB 查询	只读 MIB 查询
查询身份验证	社区字符串	社区字符串	基于用户的安全模型（ USM ）用户
通知	仅陷阱	陷阱和通知	陷阱和通知
通知身份验证	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的 USM 用户

限制

- StorageGRID 支持只读 MIB 访问。不支持读写访问。
- 网格中的所有节点都接收相同的配置。
- SNMPv3： StorageGRID 不支持传输支持模式（ TSM ）。
- SNMPv3： 支持的唯一身份验证协议是 SHA （ HMAC-SHA-96 ）。
- SNMPv3： 支持的唯一隐私协议是 AES 。

配置 SNMP 代理

您可以将StorageGRID SNMP代理配置为使用第三方SNMP管理系统进行只读MIB访问和通知。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

关于此任务

StorageGRID SNMP代理支持SNMPv1、SNMPv2c和SNMPv3。您可以为代理配置一个或多个版本。 对于SNMPv3、仅支持用户安全模型(User Security Model、USM)身份验证。

网格中的所有节点都使用相同的SNMP配置。

指定基本配置

首先、启用StorageGRID SMNP代理并提供基本信息。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

此时将显示SNMP代理页面。

2. 要在所有网格节点上启用SNMP代理，请选中*Enable SNMP*复选框。
3. 在Basic configuration部分中输入以下信息。

字段	Description
系统联系人	可选。StorageGRID系统的主要联系人、在SNMP消息中以sysContact的形式返回。 系统联系人通常是一个电子邮件地址。此值用于适用场景StorageGRID系统中的所有节点。*系统联系人*最多可以包含255个字符。
系统位置	可选。StorageGRID系统的位置、在SNMP消息中以sysLocation的形式返回。 系统位置可以是任何有助于确定StorageGRID系统所在位置的信息。例如，您可以使用设施的街道地址。此值用于适用场景StorageGRID系统中的所有节点。*系统位置*最多可以是255个字符。
启用SNMP代理通知	• 如果选中此选项、StorageGRID SNMP代理将发送陷阱和通知通知。 • 如果未选中、则SNMP代理支持只读MIB访问、但不会发送任何SNMP通知。
启用身份验证陷阱	如果选中此选项、则StorageGRID SNMP代理会在收到未经正确身份验证的协议消息时发送身份验证陷阱。

输入社区字符串

如果使用SNMPv1或SNMPv2c、请完成社区字符串部分。

当管理系统查询 StorageGRID MIB 时，它会发送一个社区字符串。如果社区字符串与此处指定的值之一匹配，则 SNMP 代理会向管理系统发送响应。

步骤

1. 对于*只读社区*，可选择输入社区字符串，以允许对IPv4和IPv6代理地址进行只读MIB访问。

   为确保StorageGRID系统的安全性、请勿使用"public"作为社区字符串。如果将此字段留空、SNMP代理将使用StorageGRID系统的网格ID作为社区字符串。

   每个社区字符串最多可以包含32个字符、并且不能包含空格字符。

2. 选择*添加其他社区字符串*以添加其他字符串。

   最多允许五个字符串。

创建陷阱目标

使用其他配置部分中的陷阱目标选项卡为StorageGRID陷阱或通知定义一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

步骤

1. 对于*默认陷阱社区*字段、可选择输入要用于SNMPv1或SNMPv2陷阱目标的默认社区字符串。

   定义特定陷阱目标时、您可以根据需要提供不同的("自定义")社区字符串。

   *默认陷阱社区*最多可包含32个字符、不能包含空格字符。

2. 要添加陷阱目标，请选择*Cree*。
3. 选择要用于此陷阱目标的SNMP版本。
4. 完成所选版本的创建陷阱目标表单。

SNMPv1

如果选择SNMPv1作为版本、请填写这些字段。

字段	Description
Type	必须为SNMPv1陷阱。
主机	用于接收陷阱的IPv4或IPv6地址或完全限定域名(FQDN)。
Port	使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含32个字符、并且不能包含空格。

SNMPv2c

如果选择SNMPv2c作为版本、请填写这些字段。

字段	Description
Type	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。
Port	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含32个字符、并且不能包含空格。

SNMPv3

如果选择SNMPv3作为版本、请填写这些字段。

字段	Description
Type	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。

字段	Description
Port	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
USM用户	要用于身份验证的USM用户。 • 如果选择了 * 陷阱 * ，则仅显示不具有权威引擎 ID 的 USM 用户。 • 如果选择 * 通知 * ，则仅显示具有权威引擎 ID 的 USM 用户。 • 如果未显示任何用户： i. 创建并保存陷阱目标。 ii. 转至 创建USM用户 并创建用户。 iii. 返回到陷阱目标选项卡，从表中选择保存的目标，然后选择*Edit*。 iv. 选择用户。

5. 选择 * 创建 * 。

   此时将创建陷阱目标并将其添加到表中。

创建代理地址

(可选)使用“其他配置”部分中的“业务代表地址”选项卡指定一个或多个“侦听地址”。 这些地址是SNMP代理可以接收查询的StorageGRID地址。

如果不配置代理地址、则所有StorageGRID 网络上的默认侦听地址均为UDP端口161。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	Description
互联网协议	此地址将使用IPv4还是IPv6。 默认情况下， SNMP 使用 IPv4 。
传输协议	此地址将使用UDP还是TCP。 默认情况下， SNMP 使用 UDP 。

字段	Description
StorageGRID网络	代理将侦听哪个StorageGRID网络。 • 网格、管理和客户端网络：SNMP代理将侦听所有三个网络上的查询。 • 网格网络 • 管理网络 • 客户端网络 注意：如果使用客户端网络处理不安全的数据，并为客户端网络创建代理地址，请注意SNMP流量也不安全。
Port	(可选) SNMP代理应侦听的端口号。 SNMP 代理的默认 UDP 端口为 161 ，但您可以输入任何未使用的端口号。 注意：保存SNMP代理时，StorageGRID会自动打开内部防火墙上的代理地址端口。您必须确保任何外部防火墙允许访问这些端口。

3. 选择 * 创建 * 。

   此时将创建代理地址并将其添加到表中。

创建USM用户

如果使用SNMPv3、请使用其他配置部分中的USM用户选项卡定义有权查询MIB或接收陷阱和通知的USM用户。

SNMPv3 _INFORM _目标必须具有具有引擎ID的用户。SNMPv3 _陷阱_目标不能包含具有引擎ID的用户。

如果您仅使用SNMPv1或SNMPv2c、则这些步骤不适用。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	Description
Username	此USM用户的唯一名称。 用户名最多可以包含32个字符、且不能包含空格字符。创建用户后、无法更改此用户名。

字段	Description
只读MIB访问	如果选中、则此用户应对MIB具有只读访问权限。
权威引擎ID	如果要在通知目标中使用此用户、则为该用户的权威引擎ID。 输入10到64个十六进制字符(5到32字节)、不含空格。要在陷阱目标中选择用于通知的USM用户需要此值。要在陷阱目标中为陷阱选择的USM用户不允许使用此值。 注意：如果您选择了*只读MIB访问*，则不会显示此字段，因为具有只读MIB访问权限的USM用户不能具有引擎ID。
安全级别	USM用户的安全级别： • * authPriv* ： 此用户与身份验证和隐私（加密）通信。您必须指定身份验证协议和密码以及隐私协议和密码。 • * authNoPriv* ： 此用户使用身份验证进行通信，并且没有隐私（无加密）。您必须指定身份验证协议和密码。
身份验证协议	始终设置为SHA、这是唯一支持的协议(HMAC-SHA-96)。
Password	此用户将用于身份验证的密码。
隐私协议	仅当您选择了*authPriv*并始终设置为AES时显示，AES是唯一支持的隐私协议。
Password	仅在选择了*authSv*时显示。此用户用于保护隐私的密码。

3. 选择 * 创建 * 。

   此时将创建 USM 用户并将其添加到表中。

4. 完成SNMP代理配置后，选择*Save*。

   新的 SNMP 代理配置将变为活动状态。

更新 SNMP 代理

您可以禁用SNMP通知、更新社区字符串、或者添加或删除代理地址、USM用户和陷阱目标。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

关于此任务

请参见 "配置 SNMP 代理" 有关SNMP代理页面上每个字段的详细信息。您必须选择页面底部的*保存*以提交您在每个选项卡上所做的任何更改。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示SNMP代理页面。

2. 要在所有网格节点上禁用SNMP代理，请清除*Enable SNMP*复选框，然后选择*Save*。

   如果重新启用SNMP代理、则会保留先前的任何SNMP配置设置。

3. (可选)更新Basic configuration部分中的信息：

   a. 根据需要更新*系统联系人*和*系统位置*。

   b. (可选)选中或清除*启用SNMP代理通知*复选框以控制StorageGRID SNMP代理是否发送陷阱和通知通知。

      清除此复选框后、SNMP代理支持只读MIB访问、但不会发送SNMP通知。

   c. (可选)选中或清除*启用身份验证陷阱*复选框，以控制StorageGRID SNMP代理在收到未经正确身份验证的协议消息时是否发送身份验证陷阱。

4. 如果使用SNMPv1或SNMPv2c，则可以选择在“团体字符串”部分中更新或添加*只读社区*。

5. 要更新陷阱目标、请选择其他配置部分中的陷阱目标选项卡。

   使用此选项卡可以定义StorageGRID陷阱或通知通知的一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

   有关输入内容的详细信息、请参见 "创建陷阱目标"。

   - (可选)更新或删除默认陷阱社区。

     如果删除默认陷阱团体、则必须先确保任何现有陷阱目标使用自定义社区字符串。

   - 要添加陷阱目标，请选择*Cree*。
   - 要编辑陷阱目标，请选择单选按钮，然后选择*Edit*。
   - 要删除陷阱目标，请选择单选按钮，然后选择*Remove*。
   - 要提交更改，请选择页面底部的*保存*。

6. 要更新业务代表地址，请选择其他配置部分中的业务代表地址选项卡。

   使用此选项卡指定一个或多个"侦听地址"。 这些地址是SNMP代理可以接收查询的StorageGRID地址。

   有关输入内容的详细信息、请参见 "创建代理地址"。

   - 要增加业务代表地址，请选择*Cree*。
   - 要编辑业务代表地址，请选择单选按钮，然后选择*Edit*。

- 要删除业务代表地址，请选择单选按钮，然后选择*Remove*。
- 要提交更改，请选择页面底部的*保存*。

7. 要更新USM用户、请选择其他配置部分中的USM用户选项卡。

   使用此选项卡可定义有权查询 MIB 或接收陷阱并通知的 USM 用户。

   有关输入内容的详细信息、请参见 "创建USM用户"。

   - 要添加USM用户，请选择*Cree*。
   - 要编辑USM用户，请选择单选按钮，然后选择*Edit*。

     无法更改现有USM用户的用户名。如果需要更改用户名，必须删除此用户并创建新用户名。

     > 如果添加或删除用户的权威引擎ID、并且当前已为目标选择该用户、则必须编辑或删除目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要删除USM用户，请选择单选按钮，然后选择*Remove*。

     > 如果您删除的用户当前已被选定为陷阱目标、则必须编辑或删除该目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要提交更改，请选择页面底部的*保存*。

8. 更新SNMP代理配置后，选择*Save*。

访问MIB文件

MIB文件包含有关网格中节点的受管资源和服务属性的定义和信息。您可以访问用于定义StorageGRID 对象和通知的MIB文件。这些文件可用于监控网格。

请参见 "使用 SNMP 监控" 有关SNMP和MIB文件的详细信息。

访问MIB文件

按照以下步骤访问MIB文件。

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。
2. 在SNMP代理页面上、选择要下载的文件：
   - **NetApp-STORAGEGRID-MIB.TXT**：定义可在所有管理节点上访问的警报表和通知(陷阱)。
   - **ES-NetApp-06-MIB.MIB**：为基于E系列的设备定义对象和通知。
   - **mib_1_10.zip**：使用BMC接口为设备定义对象和通知。

您还可以在任何StorageGRID节点上访问以下位置的MIB文件：
`/usr/share/snmp/mibs`

3. 要从MIB文件中提取StorageGRID OID、请执行以下操作：

   a. 获取StorageGRID MIB根目录的OID：

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

结果 `.1.3.6.1.4.1.789.28669` (`28669` 始终是StorageGRID 的OID)

   a. 整个树中StorageGRID OID的gep (使用 `paste` 连接线)：

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

。 `snmptranslate` 命令提供了许多可用于浏览MIB的选项。此命令可在任何StorageGRID 节点上使用。

MIB文件内容

所有对象都位于StorageGRID OID下。

对象名称	对象ID (OID)	Description
iso.org.dod.internet。+ 私有企业。+ NetApp.storagegrid		NetApp StorageGRID实体的MIB模块。

MIB对象

对象名称	对象ID (OID)	Description
活动的计数	1.3.6.1.4.1。+ 789.28669.1.3	activeAlert表中活动警报的数量。
活动的活动的表	1.3.6.1.4.1。+ 789.28669.1.4	StorageGRID 中活动警报的表。
活动的标识号	1.3.6.1.4.1。+ 789.28669.1.4.1.1	警报的ID。仅在当前一组活动警报中是唯一的。
活动报告名称	1.3.6.1.4.1。+ 789.28669.1.4.1.2	警报的名称。

对象名称	对象ID (OID)	Description
已执行的活动的活动的实例	1.3.6.1.4.1。+ 789.28669.6.4.1.3	生成警报的实体的名称、通常为节点名称。
活动告警严重性	1.3.6.1.4.1。+ 789.28669.1.4.1.4	警报的严重性。
活动的起始时间	1.3.6.1.4.1。+ 789.28669.1.4.1.5	触发警报的日期和时间。

通知类型(陷阱)

所有通知都包含以下变量作为变量绑定：

- 活动的标识号
- 活动报告名称
- 已执行的活动的活动的实例
- 活动告警严重性
- 活动的起始时间

通知类型	对象ID (OID)	Description
活动MinorAlert	1.3.6.1.4.1。+ 789.28669.0.6	严重性较低的警报
活动主要警报	1.3.6.1.4.1。+ 789.28669.0.7	严重性为"重大"的警报
活动状态警报	1.3.6.1.4.1。+ 789.28669.0.8	严重性为严重的警报