



使用 **SNMP** 监控 StorageGRID software

NetApp
July 23, 2026

目录

使用 SNMP 监控	1
在 StorageGRID 中使用 SNMP 监控	1
功能	1
SNMP 版本支持	1
限制	2
在 StorageGRID 中配置 SNMP 代理	2
指定基本配置	2
输入团体字符串	3
创建陷阱目的地	4
创建代理地址	6
创建 USM 用户	7
更新 StorageGRID SNMP 代理	8
访问 StorageGRID MIB 文件	10
访问 MIB 文件	10
MIB 文件内容	11
MIB 对象	11

使用 SNMP 监控

在 StorageGRID 中使用 SNMP 监控

如果要使用简单网络管理协议 (SNMP) 监控 StorageGRID，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 节点都运行提供 MIB 的 SNMP 代理或守护程序。StorageGRID MIB 包含警报的表和通知定义。MIB 还包含系统描述信息，例如每个节点的平台和型号。每个 StorageGRID 节点还支持 MIB-II 对象的子集。



如果您想在网格节点上下载 MIB 文件，请参阅 ["访问 MIB 文件"](#)。

最初，在所有节点上禁用 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通知：

陷阱

陷阱是由 SNMP 代理发送的通知，不需要管理系统的确认。陷阱用于通知管理系统 StorageGRID 中发生的事件，例如触发警报。

所有三个版本的 SNMP 均支持陷阱。

通知

Inform 类似于陷阱，但需要管理系统确认。如果 SNMP 代理在一定时间内没有收到确认，它会重新发送 inform，直到收到确认或达到最大重试值。

SNMPv2c 和 SNMPv3 支持 Inform。

在以下情况下会发送陷阱和通知消息：

- 在任何严重程度下都会触发默认或自定义警报。要抑制警报的 SNMP 通知，您必须 ["配置静默"](#) 为警报。警报通知由 ["首选发件人管理节点"](#) 发送。

每个警报都会根据警报的严重性级别映射到三种陷阱类型之一：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"](#)。

SNMP 版本支持

该表提供了每个 SNMP 版本支持内容的高级摘要。

	SNMPv1	SNMPv2c	SNMPv3
查询 (GET 和 GETNEXT)	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 (TRAP 和 INFORM)	仅限陷阱	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	每个陷阱目的地的 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受相同的配置。
- SNMPv3: StorageGRID 不支持传输支持模式 (TSM)。
- SNMPv3: 唯一支持的身份验证协议是 SHA (HMAC-SHA-96)。
- SNMPv3: 唯一支持的隐私协议是 AES。

在 StorageGRID 中配置 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

- 您已使用 ["支持的 Web 浏览器"](#) 登录到网格管理器。
- 您有 ["root 访问权限"](#)。

关于此任务

StorageGRID SNMP 代理支持 SNMPv1、SNMPv2c 和 SNMPv3。您可以为一个或多个版本配置此代理。对于 SNMPv3，仅支持用户安全模型 (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

第一步，启用 StorageGRID SNMP 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. 在基本配置部分输入以下信息。

字段	问题描述
系统联系人	可选。StorageGRID 系统的主要联系人，在 SNMP 消息中返回为 sysContact。 系统联系人通常是一个电子邮件地址。此值适用于 StorageGRID 系统中的所有节点。*系统联系人*最多可包含 255 个字符。
系统位置	可选。StorageGRID 系统的位置，在 SNMP 消息中返回为 sysLocation。 系统位置可以是用于识别 StorageGRID 系统位置的任何信息。例如，您可以使用设施的街道地址。此值适用于 StorageGRID 系统中的所有节点。*系统位置*最多可包含 255 个字符。
启用 SNMP 代理通知	• 如果选中，StorageGRID SNMP 代理将发送陷阱和通知消息。 • 如果未选中，则 SNMP 代理支持只读 MIB 访问，但不发送任何 SNMP 通知。
启用身份验证陷阱	如果选中此选项，则 StorageGRID SNMP 代理会在收到经过不正确身份验证的协议消息时发送身份验证陷阱。

输入团体字符串

如果使用 SNMPv1 或 SNMPv2c，请完成 Community strings 部分。

当管理系统查询 StorageGRID MIB 时，它会发送一个团体字符串。如果团体字符串与此处指定的值之一匹配，则 SNMP 代理将向管理系统发送响应。

步骤

1. 对于*只读社区*，可选择输入一个社区字符串，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"作为团体字符串。如果将此字段留空，SNMP 代理将使用 StorageGRID 系统的网格 ID 作为团体字符串。

每个社区字符串最多可包含 32 个字符，并且不能包含空格字符。

2. 选择*Add another community string*以添加其他字符串。

最多允许五个字符串。

创建陷阱目的地

使用"其他配置"部分中的"陷阱目标"选项卡可为 StorageGRID 陷阱或通知消息定义一个或多个目标。启用 SNMP 代理并选择*保存*后，StorageGRID 会在触发警报时向每个定义的目标发送通知。对于受支持的 MIB-II 实体（例如，ifDown 和 coldStart），也会发送标准通知。

步骤

1. 对于*默认陷阱社区*字段，可选择输入要用于 SNMPv1 或 SNMPv2 陷阱目的地的默认社区字符串。

根据需要，您可以在定义特定陷阱目标时提供不同的（"自定义"）社区字符串。

Default trap community 最多可包含 32 个字符，不能包含空格字符。

2. 要添加陷阱目的地，请选择 **Create**。
3. 选择此陷阱目标将使用的 SNMP 版本。
4. 为所选版本填写"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	问题描述
类型	必须是 SNMPv1 的陷阱。
主机	用于接收陷阱的 IPv4 或 IPv6 地址或完全限定域名 (FQDN)。
端口	使用 162，这是 SNMP 陷阱的标准端口，除非必须使用其他值。
协议	使用 UDP，这是标准的 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），或为此陷阱目标输入自定义团体字符串。 自定义社区字符串最多可包含 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	问题描述
类型	目的地是否将用于陷阱或通知。
主机	用于接收陷阱的 IPv4 或 IPv6 地址或 FQDN。
端口	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，这是标准的 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），或为此陷阱目标输入自定义团体字符串。 自定义社区字符串最多可包含 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	问题描述
类型	目的地是否将用于陷阱或通知。
主机	用于接收陷阱的 IPv4 或 IPv6 地址或 FQDN。

字段	问题描述
端口	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，这是标准的 SNMP 陷阱协议，除非您需要使用 TCP。
USM 用户	将用于身份验证的 USM 用户。 • 如果选择 Trap，则仅显示没有权威引擎 ID 的 USM 用户。 • 如果选择 Inform，则仅显示具有权威引擎 ID 的 USM 用户。 • 如果未显示用户： i. 创建并保存陷阱目标。 ii. 转到创建 USM 用户并创建用户。 iii. 返回"陷阱目的地"选项卡，从表中选择已保存的目的地，然后选择*编辑*。 iv. 选择用户。

5. 选择 **Create**。

陷阱目标已创建并添加到表中。

创建代理地址

（可选）使用"其他配置"部分的"代理地址"选项卡指定一个或多个"侦听地址"。这些是 SNMP 代理可以接收查询的 StorageGRID 地址。

如果不配置代理地址，则默认侦听地址为所有 StorageGRID 网络上的 UDP 端口 161。

步骤

1. 选择 **Create**。
2. 输入以下信息。

字段	问题描述
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	问题描述
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：如果您将客户端网络用于不安全的数据，并为客户端网络创建代理地址，请注意 SNMP 流量也将是不安全的。
端口	（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都允许访问这些端口。

3. 选择 **Create**。

已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。



对于 SNMPv3 *trap* 目标，建议为每个管理节点创建一个 USM 用户。如果每个管理节点都没有 USM 用户，则当主管理节点关闭时，您的管理系统可能会停止接收通知。



SNMPv3 *inform* 目标必须具有带引擎 ID 的用户。SNMPv3 *trap* 目标不能有带引擎 ID 的用户。

如果仅使用 SNMPv1 或 SNMPv2c，则这些步骤不适用。

步骤

1. 选择 **Create**。
2. 输入以下信息。

字段	问题描述
用户名	此 USM 用户的唯一名称。 用户名最多可包含 32 个字符，并且不能包含空白字符。创建用户后无法更改用户名。
只读 MIB 访问	如果选中，此用户应具有对 MIB 的只读访问权限。
权威引擎 ID	如果此用户将在通知目标中使用，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 个字节），不带空格。对于将在陷阱目标中选择用于 informs 的 USM 用户，此值是必需的。对于将在陷阱目标中选择用于 traps 的 USM 用户，不允许使用此值。 注意：如果您选择了*只读 MIB 访问权限*，则不会显示此字段，因为具有只读 MIB 访问权限的 USM 用户无法拥有引擎 ID。
安全级别	USM 用户的安全级别： • authPriv：此用户使用身份验证和隐私（加密）进行通信。您必须指定身份验证协议和密码以及隐私协议和密码。 • authNoPriv：此用户通过身份验证进行通信，无需隐私（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，这是唯一受支持的协议（HMAC-SHA-96）。
密码	此用户将用于身份验证的密码。
隐私协议	仅当您选择 authPriv 时才会显示，并始终设置为 AES，这是唯一受支持的隐私协议。
密码	仅在您选择 authPriv 时显示。此用户将用于隐私的密码。

3. 选择 **Create**。

已创建USM用户并将其添加到表中。

4. 完成 SNMP 代理配置后，选择*保存*。

新的SNMP代理配置变为活动状态。

更新 StorageGRID SNMP 代理

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

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到网络管理器。
- 您有 ["root 访问权限"](#)。

关于此任务

有关 SNMP 代理页上每个字段的详细信息，请参阅 ["配置 SNMP 代理"](#)。您必须在页面底部选择 **Save**，以提交您对每个选项卡所做的任何更改。

步骤

1. 选择*配置* > 监控 > **SNMP代理**。

此时将显示 SNMP 代理页面。

2. 要禁用所有网格节点上的 SNMP 代理，请清除*启用 SNMP*复选框，然后选择*保存*。

如果重新启用 SNMP 代理，则保留所有以前的 SNMP 配置设置。

3. (可选) 更新基本配置部分中的信息：

- 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消息。

清除此复选框后，SNMP 代理将支持只读 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 代理在接收到经过不正确身份验证的协议消息时是否发送身份验证陷阱。

4. 如果您使用 SNMPv1 或 SNMPv2c，则可以在社区字符串部分更新或添加*只读社区*。

5. 要更新陷阱目标，请在"其他配置"部分中选择"陷阱目标"选项卡。

使用此选项卡可定义 StorageGRID 陷阱或通知消息的一个或多个目标。启用 SNMP 代理并选择*保存*后，StorageGRID 会在触发警报时向每个定义的目标发送通知。对于受支持的 MIB-II 实体（例如 ifDown 和 coldStart），也会发送标准通知。

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，则必须首先确保任何现有的陷阱目标使用自定义团体字符串。

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

6. 要更新代理地址，请在"其他配置"部分中选择"代理地址"选项卡。

使用此选项卡可指定一个或多个"监听地址"。这些是 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"](#)。

- 要添加代理地址，请选择*创建*。
- 要编辑代理地址，请选择单选按钮，然后选择 **Edit**。
- 要删除代理地址，请选择单选按钮，然后选择*删除*。
- 要提交更改，请选择页面底部的*保存*。

7. 要更新 USM 用户，请在其他配置部分中选择 USM 用户选项卡。

使用此选项卡可定义有权查询 MIB 或接收陷阱和通知的 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*创建*。
- 要编辑 USM 用户，请选择单选按钮，然后选择*编辑*。

无法更改现有 USM 用户的用户名。如果需要更改用户名，则必须删除该用户并创建一个新用户。



如果您添加或删除用户的权威引擎 ID，并且该用户当前被选为目标，则必须编辑或删除目标。否则，保存 SNMP 代理配置时会出现验证错误。

- 要删除 USM 用户，请选择单选按钮，然后选择*删除*。



如果您删除的用户当前被选为陷阱目标，则必须编辑或删除目标。否则，保存 SNMP 代理配置时会出现验证错误。

- 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*保存*。

访问 StorageGRID MIB 文件

MIB 文件包含有关网格中节点的托管资源和服务属性的定义和信息。您可以访问定义 StorageGRID 对象和通知的 MIB 文件。这些文件对于监控网格非常有用。

有关 SNMP 和 MIB 文件的详细信息，请参见["使用 SNMP 监控"](#)。

访问 MIB 文件

按照下面的步骤访问 MIB 文件。

步骤

1. 选择*配置* > 监控 > **SNMP代理**。
2. 在 SNMP 代理页上，选择要下载的文件：
 - **NETAPP-STORAGEGRID-MIB.txt**：定义在所有管理节点上可访问的警报表和通知（陷阱）。
 - **ES-NETAPP-06-MIB.mib**：定义基于 E-Series 设备的对象和通知。

◦ **MIB_1_10.zip**: 定义具有 BMC 接口的设备的对象和通知。



您还可以访问任何 StorageGRID 节点上以下位置的 MIB 文件：
`/usr/share/snmp/mibs`

3. 从 MIB 文件中提取 StorageGRID OID:

a. 获取 StorageGRID MIB 根的 OID:

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

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

b. 在整个树中对 StorageGRID OID 执行 Grep 操作 (使用 `paste` 连接行):

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



该 `snmptranslate` 命令有许多选项, 可用于探索 MIB。此命令可在任何 StorageGRID 节点上使用。

MIB 文件内容

所有对象都在 StorageGRID OID 下。

对象名称	对象ID (OID)	问题描述
		NetApp StorageGRID 实体的 MIB 模块。

MIB 对象

对象名称	对象ID (OID)	类型	访问	MIB 模块	问题描述
activeAlertCount		Integer32	只读	NETAPP-STORAGEGRID-MIB	activeAlertTable 中的活动警报数。
activeAlertTable		ActiveAlertEntry 的序列	不可访问	NETAPP-STORAGEGRID-MIB	StorageGRID 中活动警报的表格。
activeAlertEntry		序列	不可访问	NETAPP-STORAGEGRID-MIB	单个 StorageGRID 警报, 按警报 ID 编制索引。
activeAlertId		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的 ID。仅在当前活动警报集中唯一。

对象名称	对象ID (OID)	类型	访问	MIB 模块	问题描述
activeAlertName		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的名称。
activeAlertInstance		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	生成警报的实体的名称，通常是节点名称。
activeAlertSeverity		八位字节字符串	只读	NETAPP-STORAGEGRID-MIB	警报的严重程度。
activeAlertStartTime		日期和时间	只读	NETAPP-STORAGEGRID-MIB	触发警报的时间。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。