



# 管理SNMP警报

## SANtricity 11.8

NetApp  
December 16, 2024

# 目录

管理SNMP警报.....	1
配置SNMP警报.....	1
为SNMP警报添加陷阱目标.....	2
配置SNMP MIB变量.....	3
编辑SNMPv2c陷阱的社区.....	4
编辑SNMPv3陷阱的用户设置.....	4
为SNMPv2c陷阱添加社区.....	5
为SNMPv3陷阱添加用户.....	6
删除SNMPv2c陷阱的社区.....	6
删除SNMPv3陷阱的用户.....	7
删除陷阱目标.....	7

# 管理SNMP警报

## 配置SNMP警报

要配置简单网络管理协议(Simple Network Management Protocol、SNMP)警报、您必须至少确定一台存储阵列的事件监控器可以发送SNMP陷阱的服务器。此配置需要社区名称或用户名以及服务器的IP地址。

### 开始之前

- 必须为网络服务器配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
- 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。

如果您没有 MIB 文件，可以从 NetApp 支持站点获取：

- 转到。"[NetApp 支持](#)"
- 单击\*下载\*选项卡、然后选择\*下载\*。
- 单击\* E系列SANtricity 操作系统控制器软件\*。
- 选择\*下载最新版本\*。
- 登录。
- 接受警告声明和许可协议。
- 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

### 关于此任务

此任务介绍如何识别陷阱目标的SNMP服务器、然后测试您的配置。

### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

首次设置时、SNMP选项卡会显示"Configure Communities/Users"。

3. 选择\*配置社区/用户\*。

此时将打开选择SNMP版本对话框。

4. 为警报选择SNMP版本、可以是\* SNMPv2c\*或\* SNMPv3 \*。

根据您的选择、将打开配置社区对话框或配置SNMPv3用户对话框。

5. 按照SNMPv2c (社区)或SNMPv3 (用户)的相应说明进行操作：

- \* SNMPv2c (社区)—在配置社区对话框中、为网络服务器输入一个或多个社区字符串。社区名称是一个字符串、用于标识一组已知的管理工作站、通常由网络管理员创建。它仅包含可打印的**ASCII**字符。您最多可以添加**256**个社区。完成后、单击\*保存。

- \* SNMPv3 (用户)—在配置**SNMPv3**用户对话框中、单击\*添加、然后输入以下信息：
  - 用户名-输入一个名称以标识用户、该名称最长可达31个字符。
  - 引擎ID-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择\*本地\*。如果您使用的是非标准配置、请选择\*自定义\*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
  - 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
  - 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。完成后、单击\*添加\*、然后单击\*关闭\*。

6. 在选择了SNMP选项卡的警报页面中、单击\*添加陷阱目标\*。

此时将打开添加陷阱目标对话框。

7. 输入一个或多个陷阱目标、选择其关联的社区名称或用户名、然后单击\*添加\*。

- 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
- 社区名称或用户名-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您仅定义了一个、则此名称已显示在此字段中。)
- 发送身份验证失败陷阱-如果要在SNMP请求因社区名称或用户名无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击\*添加\*后、陷阱目标和关联名称将显示在\*警报\*页面的\* SNMP\*选项卡中。

8. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击\*测试陷阱目标\*向配置的地址发送测试陷阱。

## 结果

每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

# 为SNMP警报添加陷阱目标

您最多可以添加10个服务器来发送SNMP陷阱。

## 开始之前

- 要添加的网络服务器必须配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
- 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。

如果您没有 MIB 文件，可以从 NetApp 支持站点获取：

- 转到。 ["NetApp 支持"](#)
- 单击\*下载\*、然后选择\*下载\*。
- 单击\* E系列SANtricity 操作系统控制器软件\*。
- 选择\*下载最新版本\*。
- 登录。

- 接受警告声明和许可协议。
- 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

## 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

表中将显示当前定义的陷阱目标。

3. 选择\*添加陷阱配置\*。

此时将打开添加陷阱目标对话框。

4. 输入一个或多个陷阱目标、选择其关联的社区名称或用户名、然后单击\*添加\*。
  - 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
  - 社区名称或用户名-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您仅定义了一个、则此名称已显示在此字段中。)
  - 发送身份验证失败陷阱-如果要在SNMP请求因社区名称或用户名无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击\*添加\*后、陷阱目标以及关联的社区名称或用户名将显示在表中。
5. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击\*测试陷阱目标\*向配置的地址发送测试陷阱。

## 结果

每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

## 配置SNMP MIB变量

对于SNMP警报、您可以选择配置SNMP陷阱中显示的管理信息库(Management Information Base、MIB)变量。这些变量可以返回存储阵列名称、阵列位置和联系人。

### 开始之前

必须使用SNMP服务应用程序在服务器上复制和编译MIB文件。

如果您没有MIB文件、可以按如下所示获取它：

- 转到。 ["NetApp 支持"](#)
- 单击\*下载\*、然后选择\*下载\*。
- 单击\* E系列SANtricity 操作系统控制器软件\*。
- 选择\*下载最新版本\*。
- 登录。
- 接受警告声明和许可协议。
- 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

### 关于此任务

此任务介绍如何为SNMP陷阱定义MIB变量。这些变量可返回以下值以响应SNMP GetRequests：

- sysName(存储阵列的名称)
- sysLocation(存储阵列的位置)
- sysContact(管理员的名称)

#### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。
3. 选择\*配置SNMP MIB变量\*。

此时将打开配置SNMP MIB变量对话框。

4. 输入以下一个或多个值、然后单击\*保存\*。
  - **Name**-- MIB变量的值 sysName。例如、输入存储阵列的名称。
  - **Location**-- MIB变量的值 sysLocation。例如、输入存储阵列的位置。
  - **联系人**-- MIB变量的值 sysContact。例如、输入负责存储阵列的管理员。

#### 结果

这些值显示在存储阵列警报的SNMP陷阱消息中。

## 编辑SNMPv2c陷阱的社区

您可以编辑SNMPv2c陷阱的社区名称。

#### 开始之前

必须创建社区名称。

#### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和社区名称将显示在表中。

3. 选择\*配置社区\*。
4. 输入新的社区名称、然后单击\*保存\*。团体名称只能包含可打印的ASCII字符。

#### 结果

警报页面的SNMP选项卡会显示更新后的社区名称。

## 编辑SNMPv3陷阱的用户设置

您可以编辑SNMPv3陷阱的用户定义。

#### 开始之前

必须为SNMPv3陷阱创建用户。

#### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和用户名显示在表中。

3. 要编辑用户定义、请在表中选择用户、然后单击\*配置用户\*。
4. 在对话框中、单击\*查看/编辑设置\*。
5. 编辑以下信息：
  - 用户名-更改标识用户的名称、该名称最长可达31个字符。
  - 引擎ID-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择\*本地\*。如果您使用的是非标准配置、请选择\*自定义\*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
  - 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
  - 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。

#### 结果

警报页面的SNMP选项卡会显示更新后的设置。

## 为SNMPv2c陷阱添加社区

您最多可以为SNMPv2c陷阱添加256个社区名称。

#### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和社区名称将显示在表中。

3. 选择\*配置社区\*。

此时将打开配置社区对话框。

4. 选择\*添加其他社区\*。
5. 输入新的社区名称、然后单击\*保存\*。

#### 结果

新社区名称将显示在警报页面的SNMP选项卡中。

## 为SNMPv3陷阱添加用户

对于SNMPv3陷阱、您最多可以添加256个用户。

### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和用户名显示在表中。

3. 选择\*配置用户\*。

此时将打开配置SNMPv3用户对话框。

4. 选择 \* 添加 \*。
5. 输入以下信息、然后单击\*添加\*。
  - 用户名-输入一个名称以标识用户、该名称最长可达31个字符。
  - 引擎ID-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择\*本地\*。如果您使用的是非标准配置、请选择\*自定义\*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
  - 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
  - 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。

## 删除SNMPv2c陷阱的社区

您可以删除SNMPv2c陷阱的社区名称。

### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和社区名称将显示在\*警报\*页面上。

3. 选择\*配置社区\*。

此时将打开配置社区对话框。

4. 选择要删除的社区名称、然后单击最右侧的\*删除\*(X)图标。

如果陷阱目标与此社区名称关联、则确认删除社区对话框将显示受影响的陷阱目标地址。

5. 确认此操作、然后单击\*删除\*。

### 结果



社区名称及其关联的陷阱目标将从警报页面中删除。

## 删除SNMPv3陷阱的用户

您可以删除SNMPv3陷阱的用户。

### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标和用户名显示在警报页面上。

3. 选择\*配置用户\*。

此时将打开配置SNMPv3用户对话框。

4. 选择要删除的用户名、然后单击\*删除\*。
5. 确认此操作、然后单击\*删除\*。

### 结果

用户名及其关联的陷阱目标将从警报页面中删除。

## 删除陷阱目标

您可以删除陷阱目标地址、以便存储阵列的事件监控器不再向该地址发送SNMP陷阱。

### 步骤

1. 选择菜单：设置[警报]。
2. 选择\*SNMP\*选项卡。

陷阱目标地址将显示在表中。

3. 选择陷阱目标、然后单击页面右上角的\*删除\*。
4. 确认此操作、然后单击\*删除\*。

目标地址不再显示在警报页面上。

### 结果

已删除的陷阱目标不再从存储阵列的事件监控器接收SNMP陷阱。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

## 商标信息

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