SNMP配置工作流

System Manager Classic

NetApp
September 05, 2025

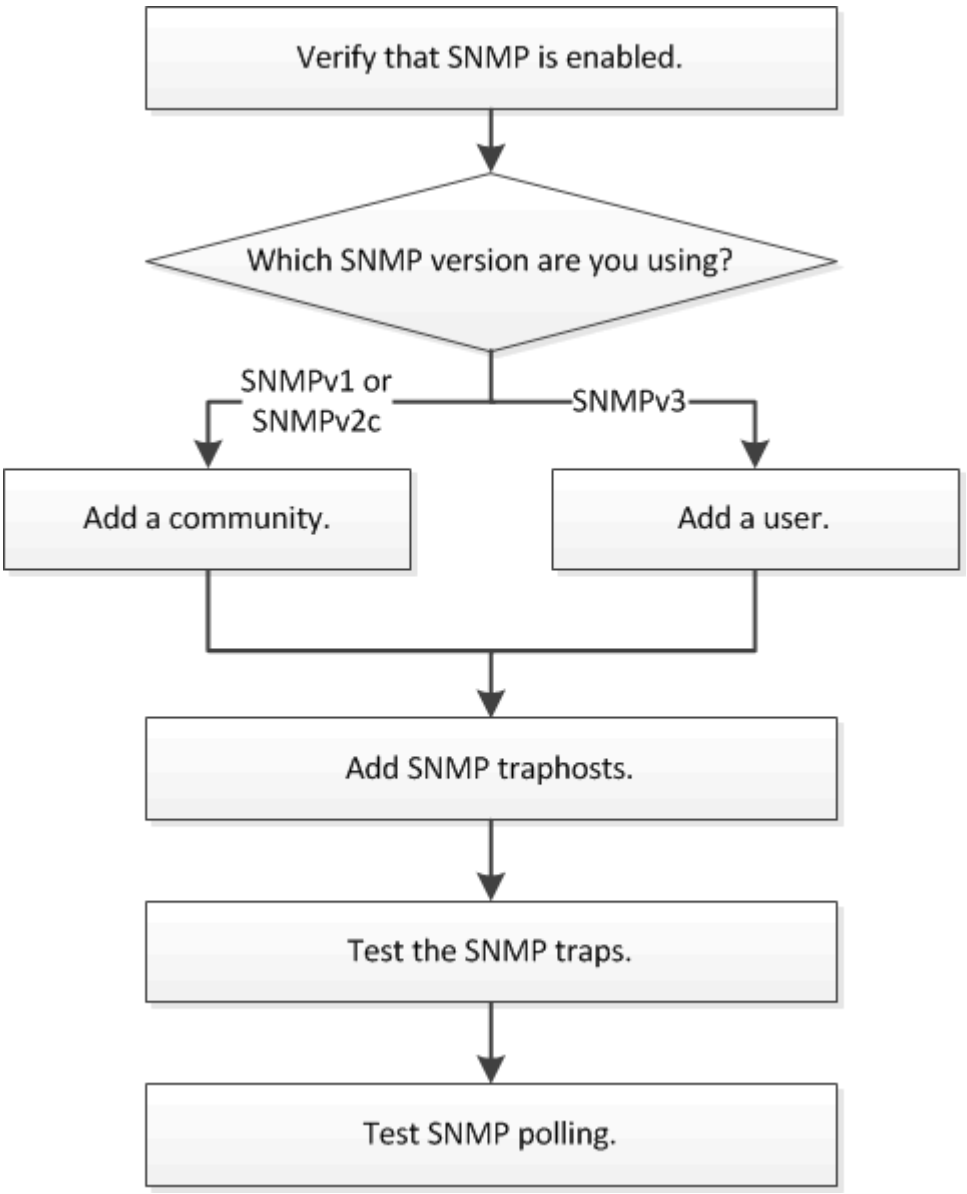
This PDF was generated from https://docs.netapp.com/zh-cn/ontap-system-manager-classic/snmp-config/task_verifying_snmp_is_enabled.html on September 05, 2025. Always check docs.netapp.com for the latest.

目录

SNMP配置工作流 1
验证是否已启用 SNMP 1
添加 SNMP 社区 2
添加 SNMPv3 安全用户 2
添加 SNMP 陷阱主机： 3
测试 SNMP 陷阱 4
测试 SNMP 轮询 4

SNMP配置工作流

配置 SNMP 包括启用 SNMP ，配置 SNMPv1 或 SNMPv2c 社区（可选），添加 SNMPv3 用户，添加 SNMP 陷阱主机以及测试 SNMP 轮询和陷阱。



验证是否已启用 SNMP

您可以在 ONTAP 9.7 或更早版本中使用 ONTAP System Manager *classic* 界面来验证集群上是否启用了 SNMP 。

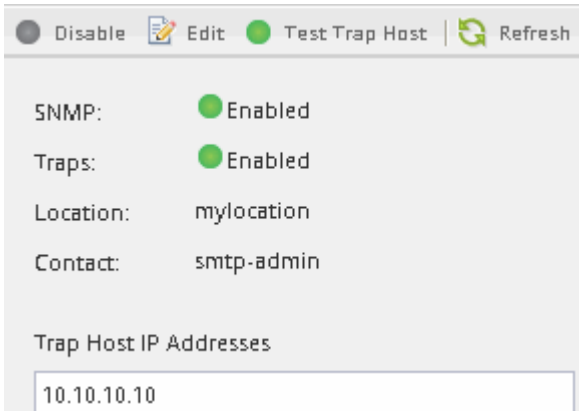
关于此任务

在所有版本的 ONTAP 中，默认情况下会在集群级别启用 SNMPv3 ，默认情况下会禁用 SNMPv1 和 SNMPv2c 。创建 SNMP 社区时， SNMPv1 和 SNMPv2c 将处于启用状态。

默认情况下， SNMP 在数据 LIF 上处于禁用状态。有关在数据 LIF 上启用 SNMP 的信息，请参见 "网络管理"。

步骤

1. 单击切槽图标。
2. 在 * 设置 * 窗格中，导航到 * SNMP * 窗口。



您可以查看集群的当前 SNMP 状态。

如果未启用 SNMP ，请单击 * 启用 * 。

添加 **SNMP** 社区

您可以将 ONTAP System Manager *classic* 界面与 ONTAP 9.7 或更早版本结合使用，将社区添加到运行 SNMPv1 或 SNMPv2c 的集群的管理 Storage Virtual Machine （ SVM ）中。System Manager 使用 SNMP 协议 SNMPv1 和 SNMPv2c 以及 SNMP 社区来发现存储系统。

关于此任务

此操作步骤用于向集群的管理 SVM 添加 SNMP 社区。中介绍了用于向数据 SVM 添加 SNMP 社区的操作步骤 "网络管理"。

在新安装的 ONTAP 中， SNMPv1 和 SNMPv2c 默认处于禁用状态。创建 SNMP 社区时， SNMPv1 和 SNMPv2c 将处于启用状态。

步骤

1. 在 SNMP 窗口中，单击 * 编辑 * 以打开 * 编辑 SNMP 设置 * 对话框。
2. 在 * 常规 * 选项卡中，指定 ONTAP 系统的联系人和位置。
3. 单击 * 添加 * ，输入社区名称，然后单击 * 社区名称 * 窗格中的 * 确定 * 。

   您可以添加多个社区名称。团体名称最多可以包含32个字符、并且不能包含以下特殊字符： , / : " ' |

4. 添加完社区名称后，单击 * 编辑 SNMP 设置 * 对话框中的 * 确定 * 。

添加 **SNMPv3** 安全用户

您可以在 ONTAP 9.7 或更早版本中使用 ONTAP System Manager *classic* 界面在集群级别

添加 SNMPv3 用户。

SNMPv3 用户可以使用您指定的身份验证和隐私设置从陷阱主机（ SNMP 管理器）运行 SNMP 实用程序。SNMPv3 通过使用密码短语和加密提供高级安全性。

关于此任务

在集群级别添加 SNMPv3 用户时，该用户可以通过应用了 `mGMT` 防火墙策略的所有 LIF 访问集群。

步骤

1. 在 SNMP 窗口中，单击 * 编辑 * 以打开 * 编辑 SNMP 设置 * 对话框。
2. 在 * SNMPv3 * 选项卡中，单击 * 添加 * 以打开 * 添加 SNMPv3 用户 * 对话框。
3. 输入以下值：

   a. 输入 SNMPv3 用户名。

      安全用户名不能超过 31 个字符，并且不能包含以下特殊字符：

      `, / : " ' |`

   b. 对于引擎ID、选择默认值 `Local Engine ID`。

      引擎 ID 用于为 SNMPv3 消息生成身份验证和加密密钥。

   c. 选择身份验证协议并输入身份验证密码。

      密码必须至少包含八个字符。

   d. 可选：选择一个隐私协议并为其输入密码。

4. 单击 * 添加 SNMPv3 用户 * 对话框中的 * 确定 * 。

   您可以添加多个安全用户名，每次添加后单击 * 确定 * 。例如，如果您使用 SNMP 监控需要不同权限的不同应用程序，则可能需要为每个监控或管理功能添加一个 SNMPv3 用户。

5. 添加完用户名后，单击 * 编辑 SNMP 设置 * 对话框中的 * 确定 * 。

添加 **SNMP** 陷阱主机：

您可以将ONTAP系统管理器_classic_界面与ONTAP 9.7或更早版本结合使用、以添加陷阱主机(SNMP管理器)、以便在集群中生成陷阱时接收SNMP通知(SNMP陷阱协议数据单元)。

开始之前

如果您配置的 SNMP 陷阱主机具有 IPv6 地址，则必须在集群上启用 IPv6 。

关于此任务

默认情况下， SNMP 和 SNMP 陷阱处于启用状态。有关 SNMP 支持的 NetApp 技术报告 TR-4220 列出了 SNMP 陷阱支持的所有默认事件。

"NetApp 技术报告 4220： Data ONTAP 中的 SNMP 支持"

步骤

1. 在 SNMP 窗口中，单击 * 编辑 * 以打开 * 编辑 SNMP 设置 * 对话框。
2. 在 * 陷阱主机 * 选项卡中，确认已选中 * 启用陷阱 * 复选框，然后单击 * 添加 * 。
3. 【第 3 步 - 输入 -traphost-ip]] 输入陷阱主机 IP 地址，然后在 * 陷阱主机 * 窗格中单击 * 确定 * 。

   SNMP 陷阱主机的 IP 地址可以是 IPv4 或 IPv6 。

4. 要添加另一个陷阱主机，请重复 步骤2. 和 步骤3.。
5. 添加陷阱主机后，单击 * 编辑 SNMP 设置 * 对话框中的 * 确定 * 。

测试 SNMP 陷阱

您可以将 ONTAP System Manager *classic* 界面与 ONTAP 9.7 或更早版本结合使用来测试 SNMP 陷阱。由于添加陷阱主机时不会自动验证与该主机的通信，因此您应验证 SNMP 陷阱主机是否可以正确接收陷阱。

步骤

1. 导航到 * SNMP * 屏幕。
2. 单击 * 测试陷阱主机 * 可从添加陷阱主机的集群生成陷阱。
3. 从陷阱主机位置验证是否已收到陷阱。

   使用您通常使用的任何软件管理 SNMP 陷阱主机。

测试 SNMP 轮询

配置 SNMP 后，您应验证是否可以轮询集群。

关于此任务

要轮询集群、您需要使用第三方命令、例如 `snmpwalk`。

步骤

1. 发送 SNMP 命令以从其他集群轮询集群。

   对于运行SNMPv1的系统、请使用命令行界面命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 发现MIB (管理信息库)的内容。

   在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123 。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

对于运行SNMPv2c的系统、请使用命令行界面命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 发现MIB (管理信息库)的内容。

在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123 。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

对于运行SNMPv3的系统、请使用命令行界面命令 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` 发现MIB (管理信息库)的内容。

在此示例中，要轮询的集群管理 LIF 的 IP 地址为 10.11.12.123 。命令将显示从 MIB 请求的信息：

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

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。