# SNMP configuration

## System Manager Classic

NetApp
June 22, 2024

# Table of Contents

# SNMP configuration

## SNMP configuration overview

Using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier, you can configure SNMP at the cluster management level; add communities, security users, and traphosts; and test the SNMP communication.

You should use these procedures if you want to configure SNMP access to a cluster in the following way:

- You are working with clusters running ONTAP 9.
- You want to use best practices, not explore every available option.

> There are a few steps in these procedures for which you must use the command-line interface.

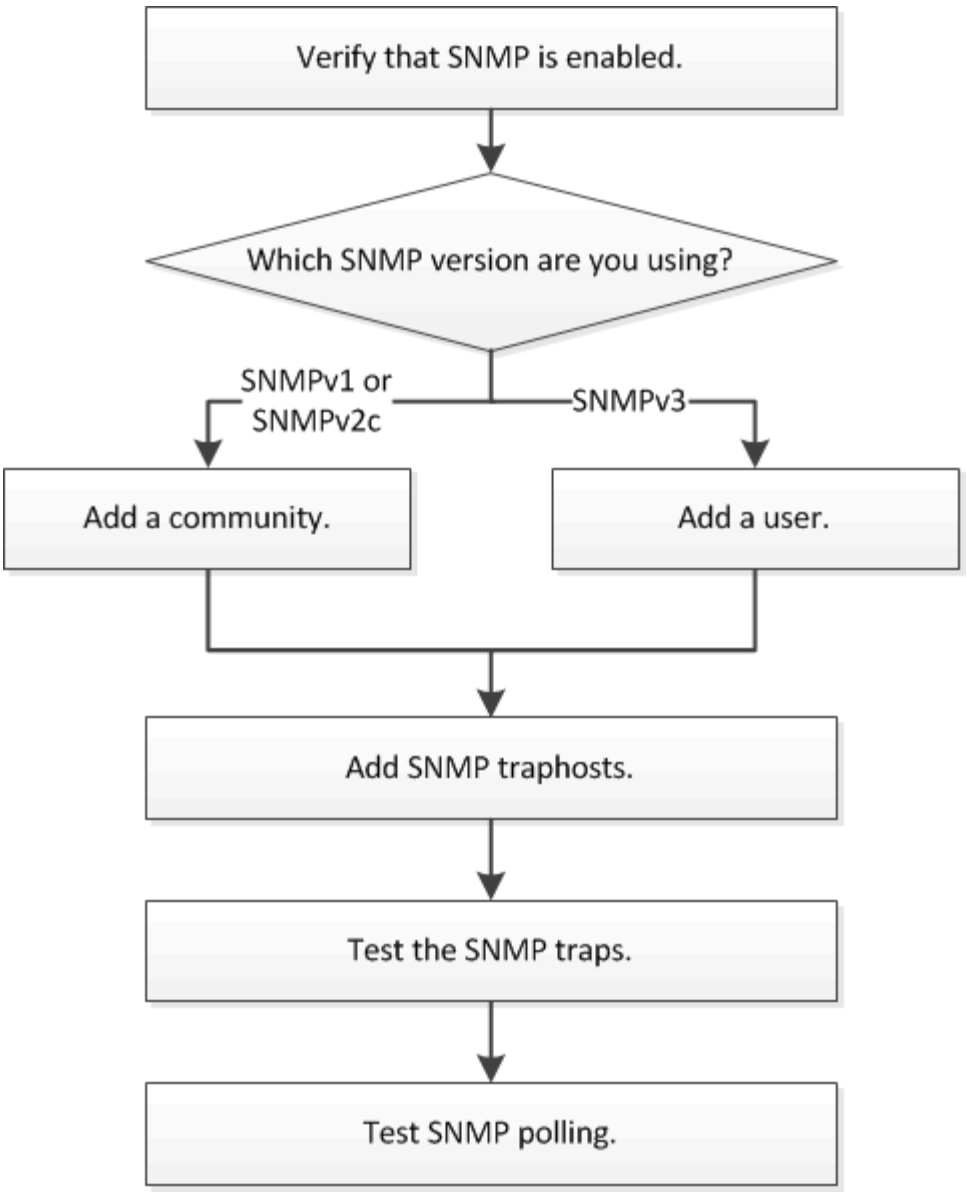
### Other ways to do this in ONTAP

You can configure SNMP access to a cluster using for all ONTAP 9 versions. You should use the appropriate procedure for your version of ONTAP.

| To perform these tasks with… | Refer to… |
| --- | --- |
| The redesigned System Manager (available with ONTAP 9.7 and later) | Manage SNMP on the cluster (cluster administrators only) > Overview |
| The ONTAP command-line interface (CLI) | Commands for managing SNMP |

## SNMP configuration workflow

Configuring SNMP involves enabling SNMP, optionally configuring an SNMPv1 or SNMPv2c community, optionally adding an SNMPv3 user, adding SNMP traphosts, and testing SNMP polling and traps.




## Verify that SNMP is enabled

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to verify whether SNMP is enabled on the cluster.

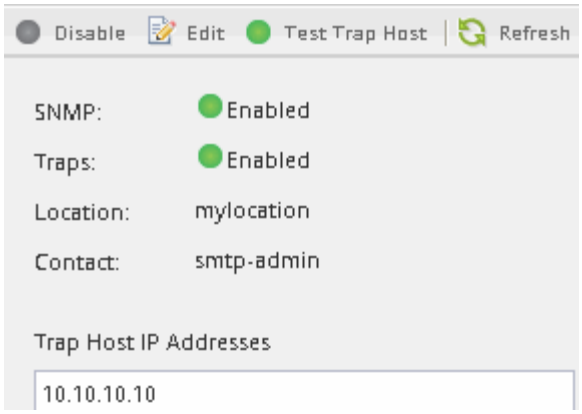
### About this task

In all versions of ONTAP, SNMPv3 is enabled by default at the cluster level and SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

SNMP is disabled by default on data LIFs. For information about enabling SNMP on data LIFs, see Network management.

### Steps

1. Click the groove icon.
2. In the **Setup** pane, navigate to the **SNMP** window.




You can view the current SNMP status for the cluster.

If SNMP is not enabled, click **Enable**.

## Add an SNMP community

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add a community to the administrative storage virtual machine (SVM) for a cluster that is running SNMPv1 or SNMPv2c. System Manager uses SNMP protocols SNMPv1 and SNMPv2c, and an SNMP community to discover storage systems.

### About this task

This procedure is for adding an SNMP community to the administrative SVM for the cluster. The procedure for adding an SNMP community to a data SVM is described in Network management.

In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

### Steps

1. In the SNMP window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **General** tab, specify the contact personnel and location for the ONTAP system.
3. Click **Add**, enter a community name, and then click **OK** in the **Community Names** pane.

   You can add multiple community names. A community name can be a maximum of 32 characters and must not contain the following special characters: `, / : " ' |`

4. When you finish adding community names, click **OK** in the **Edit SNMP Settings** dialog box.

## Add an SNMPv3 security user

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add an SNMPv3 user at the cluster level.

The SNMPv3 user can run SNMP utilities from the traphost (SNMP manager) using the authentication and privacy settings that you specify. SNMPv3 offers advanced security by using passphrases and encryption.

### About this task

When you add an SNMPv3 user at the cluster level, that user can access the cluster through all the LIFs that have the “mgmt” firewall policy applied.

**Steps**

1. In the SNMP window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **SNMPv3** tab, click **Add** to open the **Add SNMPv3 User** dialog box.
3. Enter the following values:

   a. Enter an SNMPv3 user name.

      A security user name must not exceed 31 characters and must not contain the following special characters:

      `, / : " ' |`

   b. For Engine ID, select the default value `Local Engine ID`.

      The Engine ID is used to generate authentication and encryption keys for SNMPv3 messages.

   c. Select an authentication protocol and enter an authentication password.

      A password must contain a minimum of eight characters.

   d. Optional: Select a privacy protocol and enter a password for it.

4. Click **OK** in the **Add SNMPv3 User** dialog box.

   You can add multiple security user names, clicking **OK** after each addition. For example, if you use SNMP to monitor different applications that require different privileges, you might need to add an SNMPv3 user for each monitoring or management function.

5. When you finish adding user names, click **OK** in the **Edit SNMP Settings** dialog box.

## Add an SNMP traphost

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add a traphost (SNMP manager) to receive SNMP notifications (SNMP trap protocol data units) when traps are generated in the cluster.

**Before you begin**

IPv6 must be enabled on the cluster if you configure SNMP traphosts that have IPv6 addresses.

**About this task**

SNMP and SNMP traps are enabled by default. The NetApp Technical Report TR-4220 on SNMP support contains lists of all default events that are supported by SNMP traps.

NetApp Technical Report 4220: SNMP Support in Data ONTAP

**Steps**

1. In the SNMP window, click **EDIT** to open the **Edit SNMP Settings** dialog box.
2. In the **Trap Hosts** tab, verify that the **Enable traps** check box is selected and click **Add**.

3. Enter the traphost IP address, and then click **OK** in the **Trap Hosts** pane.

   The IP address of an SNMP traphost can be IPv4 or IPv6.

4. To add another traphost, repeat Step 2 and Step 3.
5. When you finish adding traphosts, click **OK** in the **Edit SNMP Settings** dialog box.

## Test SNMP traps

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to test SNMP traps. Because communication with a traphost is not automatically validated when you add it, you should verify that the SNMP traphost can correctly receive traps.

**Steps**

1. Navigate to the **SNMP** screen.
2. Click **Test Trap Host** to generate a trap from the cluster in which you added a traphost.
3. From the traphost location, verify that the trap was received.

   Use whatever software you ordinarily use to manage the SNMP traphost.

## Test SNMP polling

After you configure SNMP, you should verify that you can poll the cluster.

**About this task**

To poll a cluster, you need to use a third-party command such as `snmpwalk`.

**Steps**

1. Send an SNMP command to poll the cluster from a different cluster.

   For systems running SNMPv1, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

   In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
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
```

For systems running SNMPv2c, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
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
```

For systems running SNMPv3, use the CLI command `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
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
```

## Copyright information



## Trademark information