Manage SNMP alerts

SANtricity 11.8

NetApp
April 05, 2024

Table of Contents

Manage SNMP alerts

Configure SNMP alerts

To configure Simple Network Management Protocol (SNMP) alerts, you must identify at least one server where the storage array's event monitor can send SNMP traps. The configuration requires a community name or user name, and an IP address for the server.

Before you begin

- A network server must be configured with an SNMP service application. You need the network address of this server (either an IPv4 or an IPv6 address), so the event monitor can send trap messages to that address. You can use more than one server (up to 10 servers are allowed).
- The management information base (MIB) file has been copied and compiled on the server with the SNMP service application. This MIB file defines the data being monitored and managed.

  If you do not have the MIB file, you can obtain it from the NetApp Support site:

  - Go to NetApp Support.
  - Click the **Downloads** tab, and then select **Downloads**.
  - Click **E-Series SANtricity OS Controller Software**.
  - Select **Download Latest Release**.
  - Log in.
  - Accept the Caution statement and license agreement.
  - Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

About this task

This task describes how to identify the SNMP server for trap destinations, and then test your configuration.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   On first-time setup, the SNMP tab displays "Configure Communities/Users."

3. Select **Configure Communities/Users**.

   The Select SNMP version dialog box opens.

4. Select the SNMP version for the alerts, either **SNMPv2c** or **SNMPv3**.

   Depending on your selection, the Configure Communities dialog box or the Configure SNMPv3 Users dialog box opens.

5. Follow the appropriate instructions for SNMPv2c (communities) or SNMPv3 (users):
   - **SNMPv2c (communities)** — In the Configure Communities dialog, enter one or more community strings for the network servers. A community name is a string that identifies a known set of management stations, and is typically created by a network administrator. It consists of only printable

ASCII characters. You can add up to 256 communities. When you are done, click **Save**.

- **SNMPv3 (users)** — In the Configure SNMPv3 Users dialog, click **Add**, and then enter the following information:
  - **User name** — Enter a name to identify the user, which can be up to 31 characters long.
  - **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
  - **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
  - **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long. When you are done, click **Add**, and then click **Close**.

6. From the Alerts page with the SNMP tab selected, click **Add Trap Destinations**.

   The Add Trap Destinations dialog box opens.

7. Enter one or more trap destinations, select their associated community names or user names, and then click **Add**.
   - **Trap Destination** — Enter an IPv4 or IPv6 address of the server running an SNMP service.
   - **Community name or User name** — From the drop-down, select the community name (SNMPv2c) or user name (SNMPv3) for this trap destination. (If you defined only one, the name already appears in this field.)
   - **Send Authentication Failure Trap** — Select this option (the checkbox) if you want to alert the trap destination whenever an SNMP request is rejected because of an unrecognized community name or user name. After you click **Add**, the trap destinations and associated names appear in the **SNMP** tab of the **Alerts** page.
8. To make sure a trap is valid, select a trap destination from the table, and then click **Test Trap Destination** to send a test trap to the configured address.

Results

The event monitor sends SNMP traps to the server(s) whenever an alertable event occurs.

Add trap destinations for SNMP alerts

You can add up to 10 servers for sending SNMP traps.

Before you begin

- The network server you want to add must be configured with an SNMP service application. You need the network address of this server (either an IPv4 or an IPv6 address), so the event monitor can send trap messages to that address. You can use more than one server (up to 10 servers are allowed).
- The management information base (MIB) file has been copied and compiled on the server with the SNMP service application. This MIB file defines the data being monitored and managed.

  If you do not have the MIB file, you can obtain it from the NetApp Support site:

- Go to NetApp Support.
- Click **Downloads**, and then select **Downloads**.
- Click **E-Series SANtricity OS Controller Software**.
- Select **Download Latest Release**.
- Log in.
- Accept the Caution statement and license agreement.
- Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The currently defined trap destinations appear in the table.

3. Select **Add Trap Desinations**.

   The Add Trap Destinations dialog box opens.

4. Enter one or more trap destinations, select their associated community names or user names, and then click **Add**.
   - **Trap Destination** — Enter an IPv4 or IPv6 address of the server running an SNMP service.
   - **Community name or User name** — From the drop-down, select the community name (SNMPv2c) or user name (SNMPv3) for this trap destination. (If you defined only one, the name already appears in this field.)
   - **Send Authentication Failure Trap** — Select this option (the checkbox) if you want to alert the trap destination whenever an SNMP request is rejected because of an unrecognized community name or user name. After you click **Add**, the trap destinations and associated community names or user names appear in the table.
5. To make sure a trap is valid, select a trap destination from the table, and then click **Test Trap Destination** to send a test trap to the configured address.

Results

The event monitor sends SNMP traps to the server(s) whenever an alertable event occurs.

Configure SNMP MIB variables

For SNMP alerts, you can optionally configure Management Information Base (MIB) variables that appear in SNMP traps. These variables can return the storage array name, array location, and a contact person.

Before you begin

The MIB file must be copied and compiled on the server with the SNMP service application.

If you do not have a MIB file, you can obtain it as follows:

- Go to NetApp Support.

- Click **Downloads**, and then select **Downloads**.
- Click **E-Series SANtricity OS Controller Software**.
- Select **Download Latest Release**.
- Log in.
- Accept the Caution statement and license agreement.
- Scroll down until you see the MIB file for your controller type, and then click the link to download the file.

About this task

This task describes how to define MIB variables for SNMP traps. These variables can return the following values in response to SNMP GetRequests:

- `sysName` (name for the storage array)
- `sysLocation` (location of the storage array)
- `sysContact` (name of an administrator)

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.
3. Select **Configure SNMP MIB Variables**.

   The Configure SNMP MIB Variables dialog box opens.

4. Enter one or more of the following values, and then click **Save**.
   - **Name** — The value for the MIB variable `sysName`. For example, enter a name for the storage array.
   - **Location** — The value for the MIB variable `sysLocation`. For example, enter a location of the storage array.
   - **Contact** — The value for the MIB variable `sysContact`. For example, enter an administrator responsible for the storage array.

Results

These values appear in SNMP trap messages for storage array alerts.

Edit communities for SNMPv2c traps

You can edit community names for SNMPv2c traps.

Before you begin

A community name must be created.

Steps

1. Select **Setting › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and community names appear in the table.

3. Select **Configure Communities**.

4. Enter the new community name, and then click **Save**. Community names can consist of only printable ASCII characters.

Results

The SNMP tab of the Alerts page displays the updated community name.

Edit user settings for SNMPv3 traps

You can edit user definitions for SNMPv3 traps.

Before you begin

A user must be created for the SNMPv3 trap.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and user names appear in the table.

3. To edit a user definition, select the user in the table and then click **Configure Users**.
4. In the dialog, click **View/Edit Settings**.
5. Edit the following information:
   - **User name** — Change the name that identifies the user, which can be up to 31 characters long.
   - **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
   - **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
   - **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long.

Results

The SNMP tab of the Alerts page displays the updated settings.

Add communities for SNMPv2c traps

You can add up to 256 community names for SNMPv2c traps.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and community names appear in the table.

3. Select **Configure Communities**.

   The Configure Communities dialog box opens.

4. Select **Add another community**.
5. Enter the new community name, and then click **Save**.

Results

The new community name appears in the SNMP tab of the Alerts page.

Add users for SNMPv3 traps

You can add up to 256 users for SNMPv3 traps.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and user names appear in the table.

3. Select **Configure Users**.

   The Configure SNMPv3 Users dialog box opens.

4. Select **Add**.
5. Enter the following information, and then click **Add**.
   - **User name** — Enter a name to identify the user, which can be up to 31 characters long.
   - **Engine ID** — Select the Engine ID, which is used to generate authentication and encryption keys for messages, and must be unique on the administrative domain. In most cases, you should select **Local**. If you have a non-standard configuration, select **Custom**; another field appears where you must enter the authoritative engine ID as a hexadecimal string, with an even number of characters between 10 and 32 characters long.
   - **Authentication credentials** — Select an authentication protocol, which ensures the identity of users. Next, enter an authentication password, which is required when the authentication protocol is set or changed. The password must be between 8 and 128 characters long.
   - **Privacy credentials** — Select a privacy protocol, which is used to encrypt the contents of messages. Next, enter a privacy password, which is required when the privacy protocol is set or changed. The password must be between 8 and 128 characters long.

Remove communities for SNMPv2c traps

You can remove a community name for SNMPv2c traps.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and community names appear on the **Alerts** page.

3. Select **Configure Communities**.

   The Configure Communities dialog box opens.

4. Select the community name you want to delete, and then click the **Remove** (X) icon on the far right.

   If trap destinations are associated with this community name, the Confirm Remove Community dialog box shows the affected trap destination addresses.

5. Confirm the operation, and then click **Remove**.

Results

The community name and its associated trap destination are removed from the Alerts page.

Remove users for SNMPv3 traps

You can remove a user for SNMPv3 traps.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destinations and user names appear on the Alerts page.

3. Select **Configure Users**.

   The Configure SNMPv3 Users dialog box opens.

4. Select the user name you want to delete, and then click **Delete**.
5. Confirm the operation, and then click **Delete**.

Results

The user name and its associated trap destination are removed from the Alerts page.

Delete trap destinations

You can delete a trap destination address so that the storage array's event monitor no longer sends SNMP traps to that address.

Steps

1. Select **Settings › Alerts**.
2. Select the **SNMP** tab.

   The trap destination addresses appear in the table.

3. Select a trap destination, and then click **Delete** in the upper right of the page.
4. Confirm the operation, and then click **Delete**.

   The destination address no longer appears on the Alerts page.

Results

The deleted trap destination no longer receives SNMP traps from the storage array's event monitor.

Copyright information

Trademark information