Manage SNMP alerts

SANtricity 11.5

NetApp
February 12, 2024

Table of Contents

Manage SNMP alerts

Configure communities and destinations for 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 and 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).
- A community name must be created, consisting of only printable ASCII characters. The community name, which is a string that acts like a password for the network servers, is typically created by a network administrator. Up to 256 communities can be created.
- 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**.
  - Click **Software**.
  - Find your management software (for example, SANtricity System Manager), and then click **Go!** on the right.
  - Click**View & Download** on the latest version.
  - Click **Continue** at the bottom of the page.
  - Accept the EULA.
  - Scroll down until you see **MIB file for SNMP traps**, 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.

   If a community is not yet configured, the SNMP tab displays "Configure Communities."

3. Select **Configure Communities**.

   The **Configure Communities** dialog box opens.

4. In the **Community Name** field, enter one or more community strings for the network servers, and then click **Save**.

   The **Alerts** page displays "Add Trap Destinations."

5. Select **Add Trap Destinations**.

   The **Add Trap Destinations** dialog box opens.

6. Enter one or more trap destinations, select their associated community names, and then click **Add**.
   - Trap Destination — Enter an IPv4 or IPv6 address of the server running an SNMP service.
   - Community name — From the drop-down, select the community name for this trap destination. (If you defined only one community name, 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. After you click Add, the trap destinations and associated community names appear in the **SNMP** tab of the **Alerts** page.
7. 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.

Result

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

Edit community names for SNMP traps

You can edit community names for SNMP traps, and also associate a different community name to an SNMP trap destination.

Before you begin

A community name must be created, consisting of only printable ASCII characters. The community name, which is a string that acts like a password for the network servers, is created by a network administrator.

Steps

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

   The trap destinations and community names appear in the table.

3. Edit community names as follows:
   - To edit a community name, select **Configure Communities**. Enter the new community name, and then click **Save**. Community names can consist of only printable ASCII characters.
   - To associate a community name to a new trap destination, select the community name from the table, and then click the **Edit** (pencil) icon on the far right. From the **Community Name** drop-down, select a new community name for an SNMP trap destination, and then click the Save (checkmark) icon.

     If you want to cancel changes, select the Cancel (X) icon.

Result

The **SNMP** tab of the **Alerts** page displays the updated communities.

Add community names for SNMP traps

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

Before you begin

The community name(s) must be created. The community name, which is a string that acts like a password for the network servers, is typically created by a network administrator. It consists of only printable ASCII characters.

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**.

Result

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

Remove community name for SNMP traps

You can remove a community name for SNMP 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.

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**.
- Click **Software**.
- Find your management software (for example, SANtricity System Manager), and then click **Go!** on the right.
- Click **View & Download** on the latest version.
- Click **Continue** at the bottom of the page.
- Accept the EULA.
- Scroll down until you see **MIB file for SNMP traps**, 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.

Result

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

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).
- A community name must be created, consisting of only printable ASCII characters. The community name, which is a string that acts like a password for the network servers, is typically created by a network administrator. Up to 256 communities can be created.
- 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**.
  - Click **Software**.
  - Find your management software (for example, SANtricity System Manager), and then click **Go!** on the right.
  - Click **View & Download** on the latest version.
  - Click **Continue** at the bottom of the page.
  - Accept the EULA.
  - Scroll down until you see **MIB file for SNMP traps**, 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, and then click **Add**.
   - Trap Destination — Enter an IPv4 or IPv6 address of the server running an SNMP service.
   - Community name — From the drop-down, select the community name for this trap destination. (If you defined only one community name, 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. After you click Add, the trap destinations and associated community 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.

Result

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

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.

Result

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

Copyright information

Trademark information