Alerts

SANtricity 11.5

NetApp
February 12, 2024

Table of Contents

Alerts

Concepts

How alerts work

Alerts notify administrators about important events that occur on the storage array. Alerts can be sent through email, SNMP traps, and syslog.

The alerts process works as follows:

1. An administrator configures one or more of the following alerting methods in System Manager:
   - **Email** — Messages are sent to email addresses.
   - **SNMP** — SNMP traps are sent to an SNMP server.
   - **Syslog** — Messages are sent to a syslog server.
2. When the storage array's event monitor detects an issue, it writes information about that issue to the event log (available from **Support › Event Log**). For example, issues can include such events as a battery failure, a component moving from Optimal to Offline, or redundancy errors in the controller.
3. If the event monitor determines that the event is "alertable," it then sends a notification using the configured alerting methods (email, SNMP, and/or syslog). All Critical events are considered "alertable," along with some Warning and Informational events.

Alerts configuration

You can configure alerts from the Initial Setup wizard (for email alerts only) or from the Alerts page. To check the current configuration, go to **Settings › Alerts**.

The Alerts tile displays the alerts configuration, which can be one of the following:

- Not configured.
- Configured; at least one alerting method is set up. To determine which alerting methods are configured, point the cursor at the tile.

Alerts information

Alerts can include the following types of information:

- Name of the storage array.
- Event error type related to an event log entry.
- Date and time when the event occurred.
- Brief description of the event.

Syslog alerts follow the RFC 3164 messaging standard.

Alerts terminology

Learn how the alerts terms apply to your storage array.

Component	Description
Event monitor	The event monitor resides on the storage array and runs as a background task. When the event monitor detects anomalies on the storage array, it writes information about the issues to the event log. Issues can include such events as a battery failure, a component moving from Optimal to Offline, or redundancy errors in the controller. If the event monitor determines that the event is "alertable," it then sends a notification using the configured alerting methods (email, SNMP, and/or syslog). All Critical events are considered "alertable," along with some Warning and Informational events.
Mail server	The mail server is used for sending and receiving email alerts. The server uses Simple Mail Transfer Protocol (SMTP).
SNMP	Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and sharing information between devices on IP networks.
SNMP trap	An SNMP trap is a notification sent to an SNMP server. The trap contains information about significant issues with the storage array.
SNMP trap destination	An SNMP trap destination is an IPv4 or IPv6 address of the server running an SNMP service.
Community name	A community name is a string that acts like a password for the network server(s) in a SNMP environment.
MIB file	The management information base (MIB) file defines the data being monitored and managed in the storage array. It must be copied and compiled on the server with the SNMP service application. This MIB file is available with the System Manager software on the Support site.
MIB variables	Management Information Base (MIB) variables can return values such as the storage array name, array location, and a contact person in response to SNMP GetRequests.
Syslog	Syslog is a protocol used by network devices for sending event messages to a logging server.

Component	Description
UDP	User Datagram Protocol (UDP) is a transport layer protocol that specifies a source and destination port number in their packet headers.

How tos

Manage email alerts

Configure mail server and recipients for alerts

To configure email alerts, you must specify a mail server address and the email addresses of the alert recipients. Up to 20 email addresses are allowed.

Before you begin

- The address of the mail server must be available. The address can be an IPv4 or IPv6 address, or a fully qualified domain name.

  To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

- Email address to be used as the alert sender must be available. This is the address that appears in the "From" field of the alert message. A sender address is required in the SMTP protocol; without it, an error results.
- Email address(es) of the alert recipient(s) must be available. The recipient is typically an address for a network administrator or storage administrator. You can enter up to 20 email addresses.

About this task

This task describes how to configure the mail server, enter email addresses for the sender and recipients, and test all the email addresses entered from the Alerts page.

Email alerts can also be configured from the Initial Setup wizard.

Steps

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

   If an email server is not yet configured, the **Email** tab displays "Configure Mail Server."

3. Select **Configure Mail Server**.

   The **Configure Mail Server** dialog box opens.

4. Enter the mail server information, and then click **Save**.
   - Mail server address — Enter a fully qualified domain name, IPv4 address, or IPv6 address of the mail server.

To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

- Email sender address — Enter a valid email address to be used as the sender of the email. This address appears in the "From" field of the email message.
- Include contact information in email — To include the sender's contact information with the alert message, select this option, and then enter a name and phone number. After you click **Save**, the email addresses appear in the **Email** tab of the **Alerts** page.

5. Select **Add Emails**.

   The **Add Emails** dialog box opens.

6. Enter one or more email addresses for the alert recipients, and then click **Add**.

   The email addresses appear on the **Alerts** page.

7. If you want to make sure the email addresses are valid, click **Test All Emails** to send test messages to the recipients.

Result

After you configure email alerts, the event monitor sends email messages to the specified recipients whenever an alertable event occurs.

Edit email addresses for alerts

You can change the email addresses of the recipients who receive email alerts.

Before you begin

The email address you intend to edit must be defined in the Email tab of the Alerts page.

Steps

1. Select **Settings › Alerts**.
2. Select the **Email** tab.
3. From the **Email Address** table, select the address you want to change, and then click the **Edit** (pencil) icon on the far right.

   The row becomes an editable field.

4. Enter a new address, and then click the **Save** (checkmark) icon.

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

Result

The Email tab of the Alerts page displays the updated email addresses.

Add email addresses for alerts

You can add up to 20 recipients for email alerts.

Steps

1. Select **Settings › Alerts**.
2. Select the **Email** tab.
3. Select **Add Emails**.

   The Add Emails dialog box opens.

4. In the empty field, enter a new email address. If you want to add more than one address, select **Add another email** to open another field.
5. Click **Add**.

Result

The Email tab of the Alerts page displays the new email addresses.

Delete email addresses for alerts

You can delete the email addresses of the recipients who receive email alerts.

Steps

1. Select **Settings › Alerts**.
2. Select the **Email** tab.
3. From the **Email Address** table, select the email address you want to delete.

   The **Delete** button in the upper right of the table becomes available for selection.

4. Click **Delete**.

   The **Confirm Delete Email** dialog box opens.

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

Result

Alerts are no longer sent to this email address.

Edit mail server for alerts

You can change the mail server address and email sender address used for email alerts.

Before you begin

The address of the mail server you are changing must be available. The address can be an IPv4 or IPv6 address, or a fully qualified domain name.

> To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

Steps

1. Select **Settings › Alerts**.
2. Select the **Email** tab.
3. Select **Configure Mail Server**.

The **Configure Mail Server** dialog opens.

4. Edit the mail server address, sender information, and contact information.
   - Mail server address — Edit the fully qualified domain name, IPv4 address, or IPv6 address of the mail server.

     To use a fully qualified domain name, you must configure a DNS server on both controllers. You can configure a DNS server from the Hardware page.

   - Email sender address — Edit the email address to be used as the sender of the email. This address appears in the "From" field of the email message.
   - Include contact information in email — To edit the sender's contact information, select this option, and then edit the name and phone number.
5. Click **Save**.

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.

Manage syslog alerts

Configure syslog server for alerts

To configure syslog alerts, you must enter a syslog server address and a UDP port. Up to five syslog servers are allowed.

Before you begin

- The syslog server address must be available. This address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- UDP port number of the syslog server must be available. This port is typically 514.

About this task

This task describes how to enter the address and port for the syslog server, and then test the address you entered.

Steps

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

   If a syslog server is not yet defined, the **Alerts** page displays "Add Syslog Servers."

3. Click **Add Syslog Servers**.

   The **Add Syslog Server** dialog box opens.

4. Enter information for one or more syslog servers (maximum of five), and then click **Add**.
   - Server Address — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - UDP Port — Typically, the UDP port for syslog is 514. The table displays the configured syslog servers.
5. To send a test alert to the server addresses, select **Test All Syslog Servers**.

Result

The event monitor sends alerts to the syslog server whenever an alertable event occurs.

Edit syslog servers for alerts

You can edit the server address used for receiving syslog alerts.

Steps

1. Select **Settings › Alerts**.
2. Select the **Syslog** tab.
3. From the table, select a syslog server address, and then click the **Edit** (pencil) icon from on the far right.

   The row becomes an editable field.

4. Edit the server address and UDP port number, and then click the **Save** (checkmark) icon.

Result

The updated server address appears in the table.

Add syslog servers for alerts

You can add a maximum of five servers for syslog alerts.

Before you begin

- The syslog server address must be available. This address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- The UDP port number of the syslog server must be available. This port is typically 514.

Steps

1. Select **Settings › Alerts**.
2. Select the **Syslog** tab.
3. Select **Add Syslog Servers**.

   The **Add Syslog Server** dialog box opens.

4. Select **Add another syslog server**.
5. Enter information for the syslog server, and then click **Add**.
   - Syslog Server Address — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.

- UDP Port — Typically, the UDP port for syslog is 514.

> You can configure up to five syslog servers.

Result

The syslog server addresses appear in the table.

Delete syslog servers for alerts

You can delete a syslog server so it no longer receives alerts.

Steps

1. Select **Settings › Alerts**.
2. Select the **Syslog** tab.
3. Select a syslog server address, and then click **Remove** from the top right.

   The **Confirm Delete Syslog Server** dialog box opens.
4. Confirm the operation, and then click **Delete**.

Result

The server you removed no longer receives alerts from the event monitor.

FAQs

What if alerts are disabled?

If you want administrators to receive notifications about important events that occur in the storage array, you must configure an alerting method.

For storage arrays managed with SANtricity System Manager, you configure alerts from the Alerts page. Alert notifications can be sent through email, SNMP traps, or syslog messages. In addition, email alerts can be configured from the Initial Setup Wizard.

How do I configure SNMP or syslog alerts?

In addition to email alerts, you can configure alerts to be sent by Simple Network Management Protocol (SNMP) traps or by syslog messages.

To configure SNMP or syslog alerts, go to **Settings › Alerts**.

Why are timestamps inconsistent between the array and alerts?

When the storage array sends alerts, it does not correct for the time zone of the target server or host that receives the alerts. Instead, the storage array uses the local time (GMT) to create the timestamp used for the alert record. As a result, you might see inconsistencies between the timestamps for the storage array and the server or host receiving an alert.

Because the storage array does not correct for time zone when sending alerts, the timestamp on the alerts is GMT-relative, which has a time-zone offset of zero. To calculate a timestamp appropriate to your local time zone, you should determine your hour offset from GMT, and then add or subtract that value from the timestamps.

To avoid this issue, configure Network Time Protocol (NTP) on your storage array controllers. NTP ensures that the controllers are always synced to the correct time.

Copyright information

Trademark information