EMS configuration

ONTAP 9

NetApp
February 24, 2023

Table of Contents

EMS configuration

EMS configuration overview

You can quickly configure ONTAP 9 to send important EMS (Event Management System) event notifications directly to an email address, syslog server, Simple Management Network Protocol (SNMP) traphost, or REST API server so that you are immediately notified of system issues that require prompt attention.

To monitor the most important activities in your system, you must monitor the important EMS events.

Because important event notifications are not enabled by default, you must configure the EMS to send notifications to either an email address, a syslog server, an SNMP traphost, or REST API server.

Configure EMS event notifications for important events if the following are true:

- You are implementing one of the following scenarios:
  - You are setting up a new system running ONTAP 9 that does not have EMS configured.
  - You have an existing system running ONTAP 9 that does not have EMS configured.
  - You are upgrading to ONTAP 9 that does not have EMS configured.
  - You have just completed a transition from Data ONTAP operating in 7-Mode to ONTAP 9.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

You can find the EMS Event Catalog under More Resources on this page: ONTAP 9 Product Library. See Convert the legacy event route-based routing to event notifications for more information on how to perform the notification-based model conversion. You can also refer to the EMS reference.

Configure EMS event notifications and filters with System Manager

You can use System Manager to configure how the Event Management System (EMS) delivers event notifications so that you can be notified of system issues that require your prompt attention.

ONTAP version	With System Manager, you can…
ONTAP 9.12.1 and later	Specify Transport Layer Security (TLS) protocol when sending events to remote syslog servers.
ONTAP 9.10.1 and later	Configure email addresses, syslog servers, and webhook applications, as well as SNMP traphosts.
ONTAP 9.7 to 9.10.0	Configure only SNMP traphosts. You can configure other EMS destination with the ONTAP CLI. See EMS configuration overview.

You can perform the following procedures:

- Add an EMS event notification destination
- Create a new EMS event notification filter
- Edit an EMS event notification destination
- Edit an EMS event notification filter
- Delete an EMS event notification destination
- Delete an EMS event notification filter

Related information

- EMS Event Catalog
- Using the CLI to configure SNMP traphosts to receive event notifications

Add an EMS event notification destination

You can use System Manager to specify to where you want EMS messages sent.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. For details, see the `event notification destination create` man page.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Click + Add .
5. Specify a name, an EMS destination type, and filters.

   ⓘ If needed, you can add a new filter. Click **Add a New Event Filter**.

6. Depending on the EMS destination type you selected, specify the following:

To configure…	Specify or select…
SNMP traphost	• Traphost name
Email (Beginning with 9.10.1)	• Destination email address • Mail server • From email address

Syslog server (Beginning with 9.10.1)	• Host name or IP address of the server • Syslog port (beginning with 9.12.1) • Syslog transport (beginning with 9.12.1) Selecting **TCP Encrypted** enables the Transport Layer Security (TLS) protocol. If no value is entered for **Syslog port**, a default is used based on the **Syslog transport** selection.
Webhook (Beginning with 9.10.1)	• Webhook URL • Client authentication (select this option to specify a client certificate)

Create a new EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to define new customized filters that specify the rules for handling EMS notifications.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Click + Add .
5. Specify a name, and select whether you want to copy rules from an existing event filter or add new rules.
6. Depending on your choice, perform the following steps:

If you choose….	**Then, perform these steps…**
Copy rules from existing event filter	1. Select an existing event filter. 2. Modify the existing rules. 3. Add other rules, if needed, by clicking + Add .
Add new rules	Specify the type, name pattern, severities, and SNMP trap type for each new rule.

Edit an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to change the event notification destination information.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notifications Management** page, select the **Events Destinations** tab.

4. Next to the name of the event destination, click ⋮, then click **Edit**.
5. Modify the event destination information, then click **Save**.

Edit an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to modify customized filters to change how event notifications are handled.

ⓘ You cannot modify system-defined filters.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click ⋮, then click **Edit**.
5. Modify the event filter information, then click **Save**.

Delete an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to delete an EMS event notification destination.

ⓘ You cannot delete SNMP destinations.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click ⋮, then click **Delete**.

Delete an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to delete customized filters.

ⓘ You cannot delete system-defined filters.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click ⋮, then click **Delete**.

Configure EMS event notifications with the CLI

EMS configuration workflow

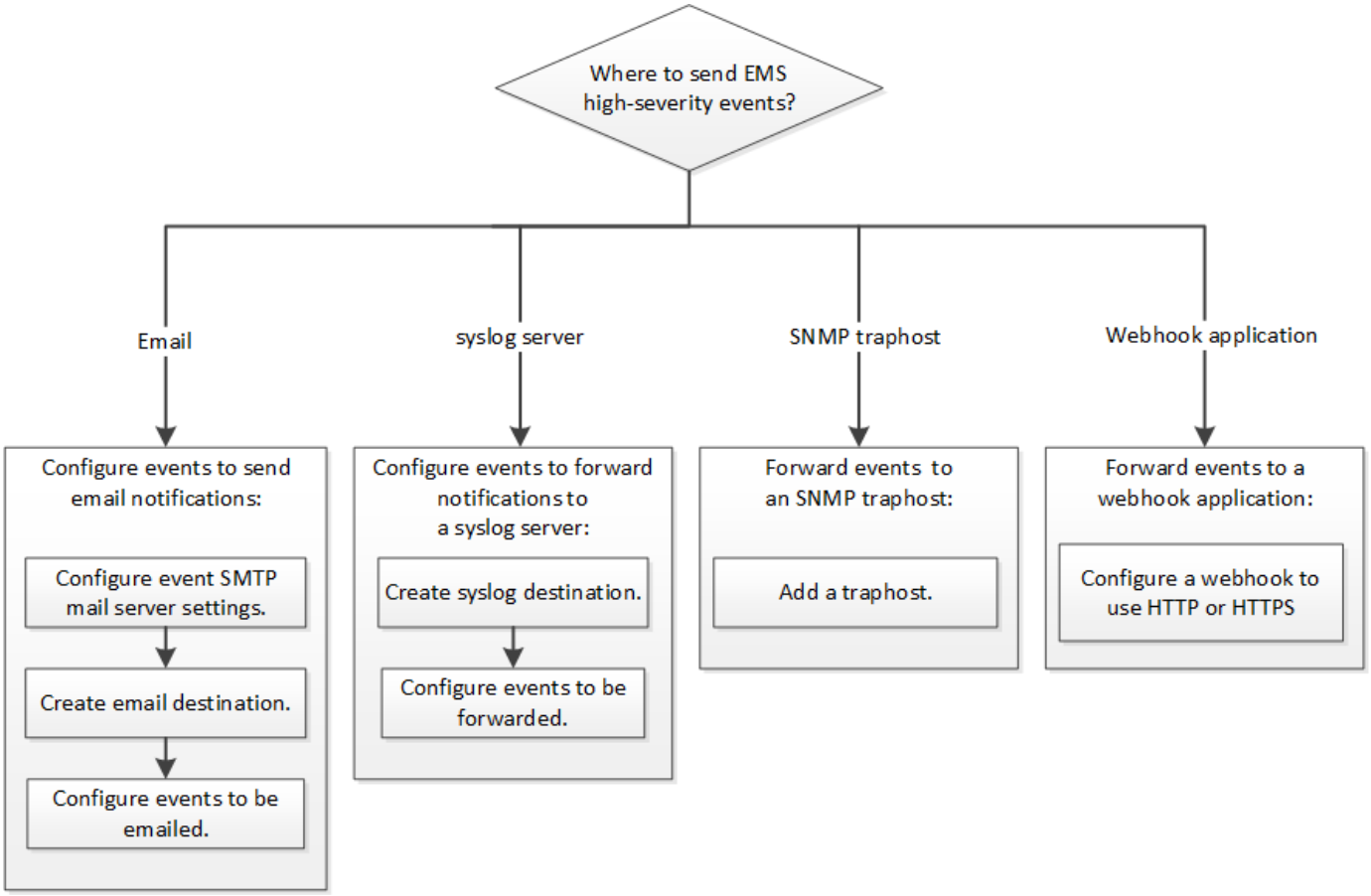
You must configure important EMS event notifications to be sent either as email, forwarded to a syslog server, forwarded to an SNMP traphost, or forwarded to a webhook application. This helps you to avoid system disruptions by taking corrective actions in a timely manner.

About this task

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for important events.



Choices

- Set EMS to send event notifications.

If you want…	Refer to this…
The EMS to send important event notifications to an email address	Configure important EMS events to send email notifications

The EMS to forward important event notifications to a syslog server	Configure important EMS events to forward notifications to a syslog server
If you want the EMS to forward event notifications to an SNMP traphost	Configure SNMP traphosts to receive event notifications
If you want the EMS to forward event notifications to a webhook application	Configure important EMS events to forward notifications to a webhook application

Configure important EMS events to send email notifications

To receive email notifications of the most important events, you must configure the EMS to send email messages for events that signal important activity.

What you'll need

DNS must be configured on the cluster to resolve the email addresses.

About this task

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

Steps

1. Configure the event SMTP mail server settings:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. Create an email destination for event notifications:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Configure the important events to send email notifications:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Configuring important EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

What you'll need

DNS must be configured on the cluster to resolve the syslog server name.

About this task

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP CLI.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. Two new parameters are available:

`tcp-encrypted`

When `tcp-encrypted` is specified for the `syslog-transport`, ONTAP verifies the identity of the destination host by validating its certificate. The default value is `udp-unencrypted`.

`syslog-port`

The default value `syslog-port` parameter depends on the setting for the `syslog-transport` parameter. If `syslog-transport` is set to `tcp-encrypted`, `syslog-port` has the default value 6514.

For details, see the `event notification destination create` man page.

Steps

1. Create a syslog server destination for important events:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   Beginning with ONTAP 9.12.1, the following values can be specified for `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol with no security
   - `tcp-unencrypted` - Transmission Control Protocol with no security
   - `tcp-encrypted` - Transmission Control Protocol with Transport Layer Security (TLS)

   The default protocol is `udp-unencrypted`.

2. Configure the important events to forward notifications to the syslog server:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Configure SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

What you'll need

- SNMP and SNMP traps must be enabled on the cluster.

  SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command

line.

Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

Configure important EMS events to forward notifications to a webhook application

You can configure ONTAP to forward important event notifications to a webhook application. The configuration steps needed depend on the level of security you choose.

Prepare to configure EMS event forwarding

There are several concepts and requirements you should consider before configuring ONTAP to forward event notifications to a webhook application.

Webhook application

You need a webhook application capable of receiving the ONTAP event notifications. A webhook is a user-defined callback routine that extends the capability of the remote application or server where it runs. Webhooks are called or activated by the client (in this case ONTAP) by sending an HTTP request to the destination URL. Specifically, ONTAP sends an HTTP POST request to the server hosting the webhook application along with the event notification details formatted in XML.

Security options

There are several security options available depending on how the Transport Layer Security (TLS) protocol is used. The option you choose determines the required ONTAP configuration.

TLS is a cryptographic protocol that is widely used on the internet. It provides privacy as well as data integrity and authentication using one or more public key certificates. The certificates are issued by trusted certificate authorities.

HTTP

You can use HTTP to transport the event notifications. With this configuration, the connection is not secure. The identities of the ONTAP client and webhook application are not verified. Further, the network traffic is not encrypted or protected. See Configure a webhook destination to use HTTP for the configuration details.

HTTPS

For additional security, you can install a certificate at the server hosting the webhook routine. The HTTPS protocol is used by ONTAP to verify the identity of the webhook application server as well as by both parties to ensure the privacy and integrity of the network traffic. See Configure a webhook destination to use HTTPS for the configuration details.

HTTPS with mutual authentication

You can further enhance the HTTPS security by installing a client certificate at the ONTAP system issuing the webbook requests. In addition to ONTAP verifying the identity of the webhook application server and protecting the network traffic, the webhook application verifies the identity of the ONTAP client. This two-

way peer authentication is known as *Mutual TLS*. See Configure a webhook destination to use HTTPS with mutual authentication for the configuration details.

Related information

- The Transport Layer Security (TLS) Protocol Version 1.3

Configure a webhook destination to use HTTP

You can configure ONTAP to forward event notifications to a webhook application using HTTP. This is the least secure option but the simplest to set up.

Steps

1. Create a new destination `restapi-ems` to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   In the above command, you must use the **HTTP** scheme for the destination.

2. Create a notification linking the `important-events` filter with the `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure a webhook destination to use HTTPS

You can configure ONTAP to forward event notifications to a webhook application using HTTPS. ONTAP uses the server certificate to confirm the identity of the webhook application as well as secure the network traffic.

Before you begin

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP

Steps

1. Install the appropriate server private key and certificates at the server hosting your webhook application. The specific configuration steps are dependent on the server.
2. Install the server root certificate in ONTAP:

   ```
   security certificate install -type server-ca
   ```

   The command will ask for the certificate.

3. Create the `restapi-ems` destination to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   In the above command, you must use the **HTTPS** scheme for the destination.

4. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ```

```
ems
```

Configure a webhook destination to use HTTPS with mutual authentication

You can configure ONTAP to forward event notifications to a webhook application using HTTPS with mutual authentication. With this configuration there are two certificates. ONTAP uses the server certificate to confirm the identity of the webhook application and secure the network traffic. In addition, the application hosting the webhook uses the client certificate to confirm the identity of the ONTAP client.

Before you begin

You must do the following before configuring ONTAP:

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP
- Generate a private key and certificate for the ONTAP client

Steps

1. Perform the first two steps in the task Configure a webhook destination to use HTTPS to install the server certificate so that ONTAP can verify the identity of the server.
2. Install the appropriate root and intermediate certificates at the webhook application to validate the client certificate.
3. Install the client certificate in ONTAP:

   ```
   security certificate install -type client
   ```

   The command will ask for the private key and certificate.

4. Create the `restapi-ems` destination to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   In the above command, you must use the **HTTPS** scheme for destination.

5. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Update deprecated EMS event mapping

EMS event mapping models

Prior to ONTAP 9.0, EMS events could only be mapped to event destinations based on event name pattern matching. The ONTAP command sets (`event destination`, `event route`) that use this model continue to be available in the latest versions of ONTAP, but they have been deprecated starting with ONTAP 9.0.

Beginning with ONTAP 9.0, the best practice for ONTAP EMS event destination mapping is to use the more scalable event filter model in which pattern matching is done on multiple fields, using the `event filter`, `event notification`, and `event notification destination` command sets.

If your EMS mapping is configured using the deprecated commands, you should update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

There are two types of event destinations:

1. **System-generated destinations**: There are five system-generated event destinations (created by default)
    - `allevents`
    - `asup`
    - `criticals`
    - `pager`
    - `traphost`

    Some of the system-generated destinations are for special purpose. For example, the asup destination routes callhome.* events to the AutoSupport module in ONTAP to generate AutoSupport messages.
2. **User-created destinations**: These are manually created using the `event destination create` command.

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

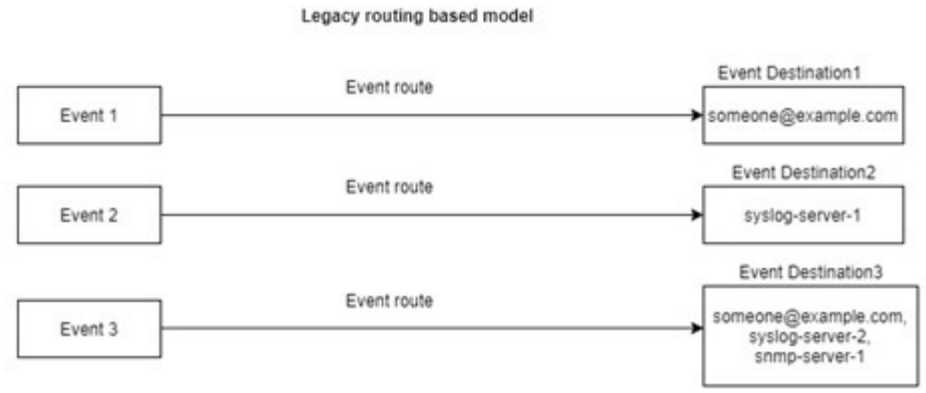
In the deprecated model, EMS events are individually mapped to a destination using the `event route add-destinations` command.

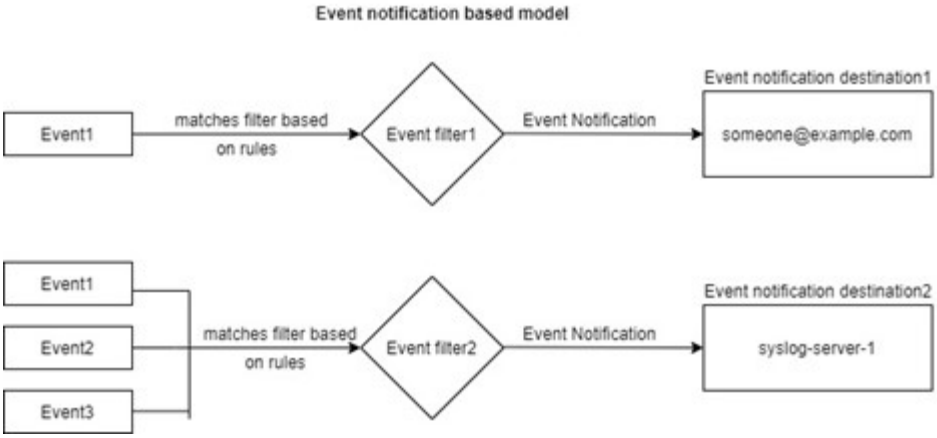
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

The new, more scalable EMS event notifications mechanism is based on event filters and event notification destinations. Refer to the following KB article for detailed information on the new event notification mechanism:

- Overview of Event Management System for ONTAP 9





Update EMS event mapping from deprecated ONTAP commands

If your EMS event mapping is currently configured using the deprecated ONTAP command sets (`event destination`, `event route`), you should follow this procedure to update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

Steps

1. List all the event destinations in the system using the `event destination show` command.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. For each destination, list the events being mapped to it using the `event route show -destinations <destination name>` command.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Create a corresponding `event filter` which includes all these subsets of events. For example, if you want to include only the `raid.aggr.*` events, use a wildcard for the `message-name` parameter when creating the filter. You can also create filters for single events.

You can create up to 50 event filters.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Create an `event notification destination` for each of the `event destination` endpoints (i.e., SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Create an event notification by mapping the event filter to the event notification destination.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. Repeat steps 1-5 for each `event destination` that has an `event route` mapping.

Events routed to SNMP destinations should be mapped to the `snmp-traphost` event notification destination. The SNMP traphost destination uses the system configured SNMP traphost.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

Copyright information

Trademark information