Configure EMS event notifications with the CLI

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/error-messages/config-workflow-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Configure EMS event notifications with the CLI . . . 1
- ONTAP EMS configuration workflow . . . 1
- Configure important ONTAP EMS events to send email notifications . . . 2
- Configure important ONTAP EMS events to forward notifications to a syslog server . . . 3
- Configure ONTAP SNMP traphosts to receive event notifications . . . 4
- Configure important ONTAP EMS events to forward notifications to a webhook application . . . 4
  - Prepare to configure EMS event forwarding . . . 4
  - Configure a webhook destination to use HTTP . . . 5
  - Configure a webhook destination to use HTTPS . . . 5
  - Configure a webhook destination to use HTTPS with mutual authentication . . . 6

Configure EMS event notifications with the CLI

ONTAP EMS configuration workflow

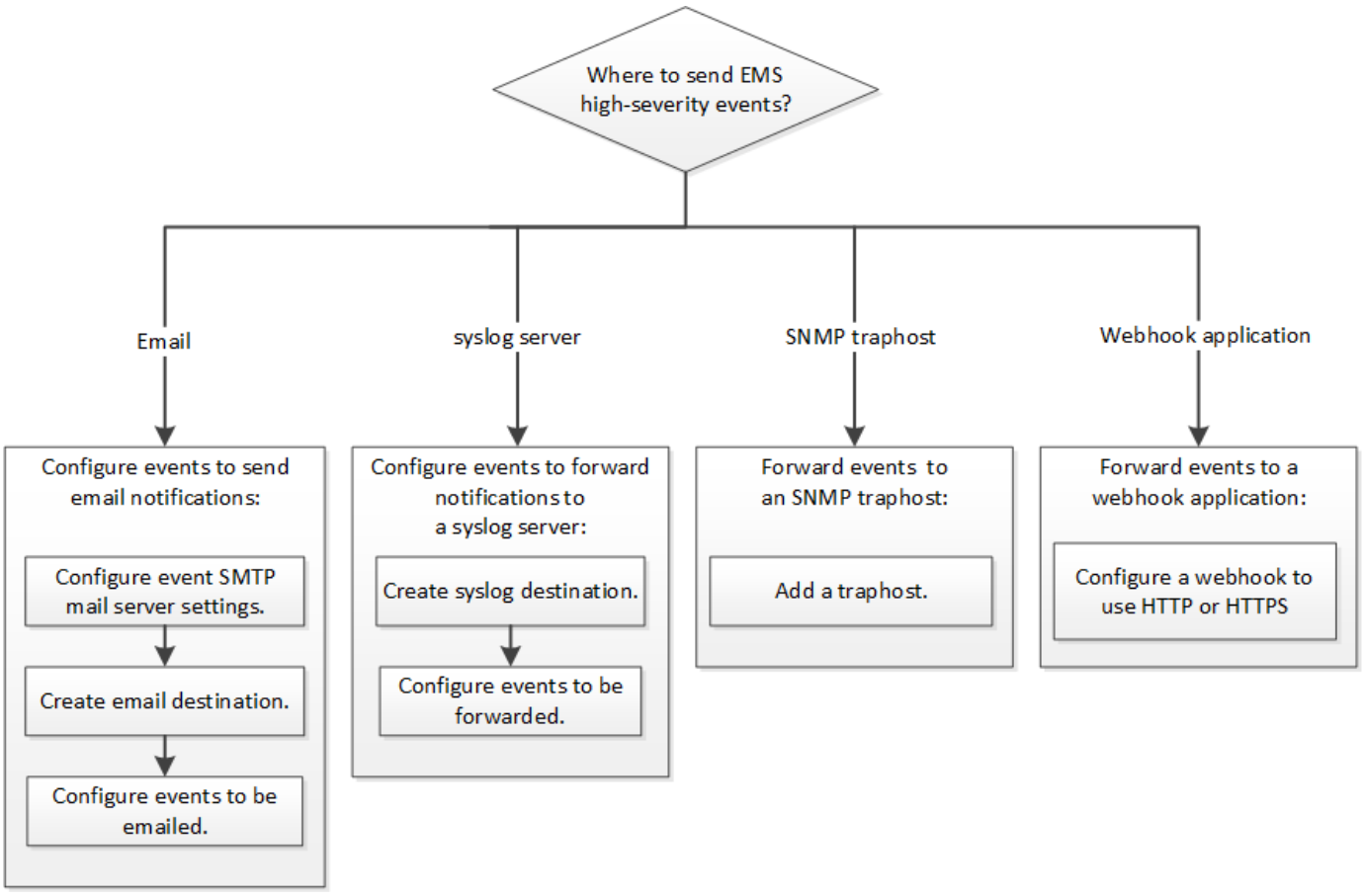
You must configure important EMS event notifications to be sent either as email, forwarded to a syslog server, forwarded to an SNMP traphost, or forwarded to a webhook application. This helps you to avoid system disruptions by taking corrective actions in a timely manner.

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 ONTAP 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.

Before you begin

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
   ```

   Learn more about `event config modify` in the ONTAP command reference.

2. Create an email destination for event notifications:

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

   Learn more about `event notification destination create` in the ONTAP command reference.

3. Configure the important events to send email notifications:

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

   Learn more about `event notification create` in the ONTAP command reference.

Configure important ONTAP 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.

Before you begin

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.

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`.

   Learn more about `event notification destination create` in the ONTAP command reference.

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

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

   Learn more about `event notification create` in the ONTAP command reference.

Configure ONTAP SNMP traphosts to receive event notifications

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

Before you begin

- 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 ONTAP 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.

   Learn more about `event notification destination create` in the ONTAP command reference.

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

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

   Learn more about `event notification create` in the ONTAP command reference.

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
   ```

Related information

- security certificate install

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.