



Configure EMS event notifications with the CLI

ONTAP 9

NetApp
April 19, 2022

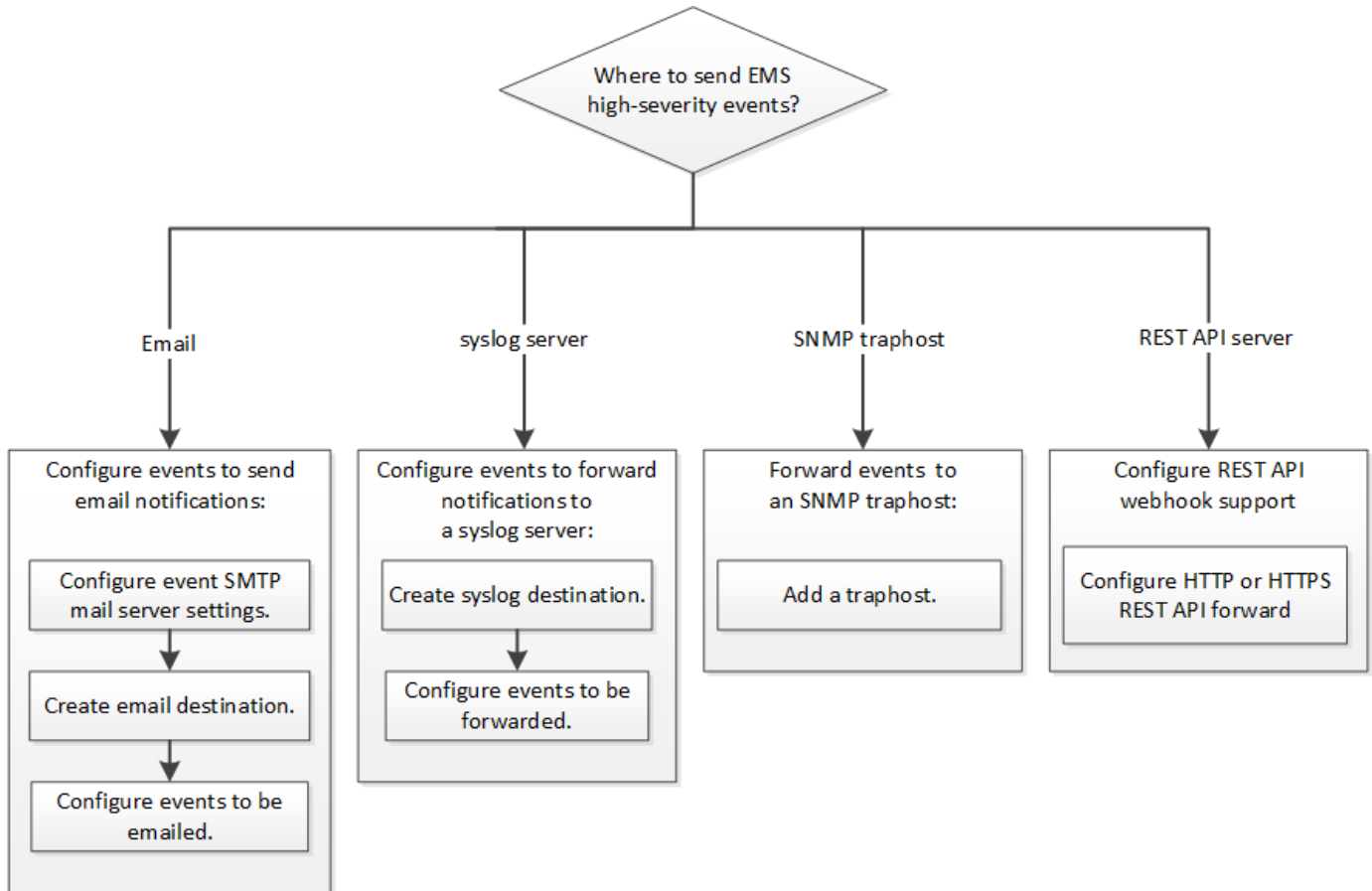
Table of Contents

- Configure EMS event notifications with the CLI 1
 - EMS configuration workflow 1
 - Decide where to send important event notifications 1
 - Configure important EMS events to send email notifications 2
 - Configuring important EMS events to forward notifications to a syslog server 3
 - Configure SNMP traphosts to receive event notifications 3
 - Configure important EMS events to forward notifications to a REST API server 4

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 REST API server. This helps you to avoid system disruptions by taking corrective actions in a timely manner.



Decide where to send important event notifications

Before you configure important EMS event notifications, you need to decide whether to send the notifications to an email address, a syslog server, an SNMP traphost, or REST API server.

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 REST API server | Configure important EMS events to forward notifications to a REST API server |

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 command line.

Steps

1. Create a syslog server destination for important events:

```
event notification destination create -name syslog-ems -syslog syslog-server-address
```

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 REST API server

To receive event notifications on a REST API server, you must configure REST API webhook support.

Before you begin

- You need a server with REST API/webhook support capable of receiving EMS events.
- The REST API server can utilize server-side or client-side security certificates.
- Configuration for certificates is determined by destination. Refer to the following for an overview of certificate configuration based on destination:
 - **http:** - No certificate involved
 - **https:** - The server certificate is verified by the ONTAP system. Optionally, a client certificate can be configured that will be sent by the ONTAP system for the server to verify.
- Client-side certificates require both the private key and certificate available for installation on the source ONTAP system(s).



If you are configuring both a client and server certificate REST API forward, a server-side certificate is required to utilize a client-side certificate. As a result, you must follow the client-side instructions to use both methods of authentication.

Configuring a HTTP Rest API forward

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. Create a new destination `restapi-ems` destination for the filter `important-events`:

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

2. 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
```

Configuring a server certificate HTTPS Rest API forward

About this task

This procedure assumes you have previously generated a server-side private key and public certificate. It also assumes you have the root certificate available to install in ONTAP.

Steps

1. Install the appropriate server private key and public certificates in your REST API server.



Specific instructions depend on the server.

2. Install the server root certificate in ONTAP.

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

The command will query for the public certificate.

3. Create the `restapi-ems` destination for the filter `important-events`.

You must use the HTTPS scheme for the server-side certificate to be utilized.

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

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
```

Configuring a client certificate HTTPS Rest API forward

About this task

The usage of a client certificate is optional and only necessary if client authentication by the server is desired. This procedure assumes you have previously generated a client private key and public certificate.

Steps

1. Install the appropriate root and intermediate certificates, in the Rest API server, to validate your client certificate.
2. Install the client certificate in ONTAP.

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

The command will query for the private key and the public certificate.

3. Create the `restapi-ems` destination for the filter `important-events`.

```
<code>event notification destination create -name restapi-ems -rest-api-url <a  
href="https://&lt;url_to_rest_api_server>" class="bare">https://&lt;url_to_rest_api_server>&lt;/a>;  
-certificate-authority &lt;issuer of the client certificate>; -certificate-serial &lt;serial of the client  
certificate>&lt;/code>
```

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
```

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.