Configure las notificaciones de eventos de EMS con la CLI

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Configure las notificaciones de eventos de EMS con la CLI

Flujo de trabajo de configuración de EMS de ONTAP

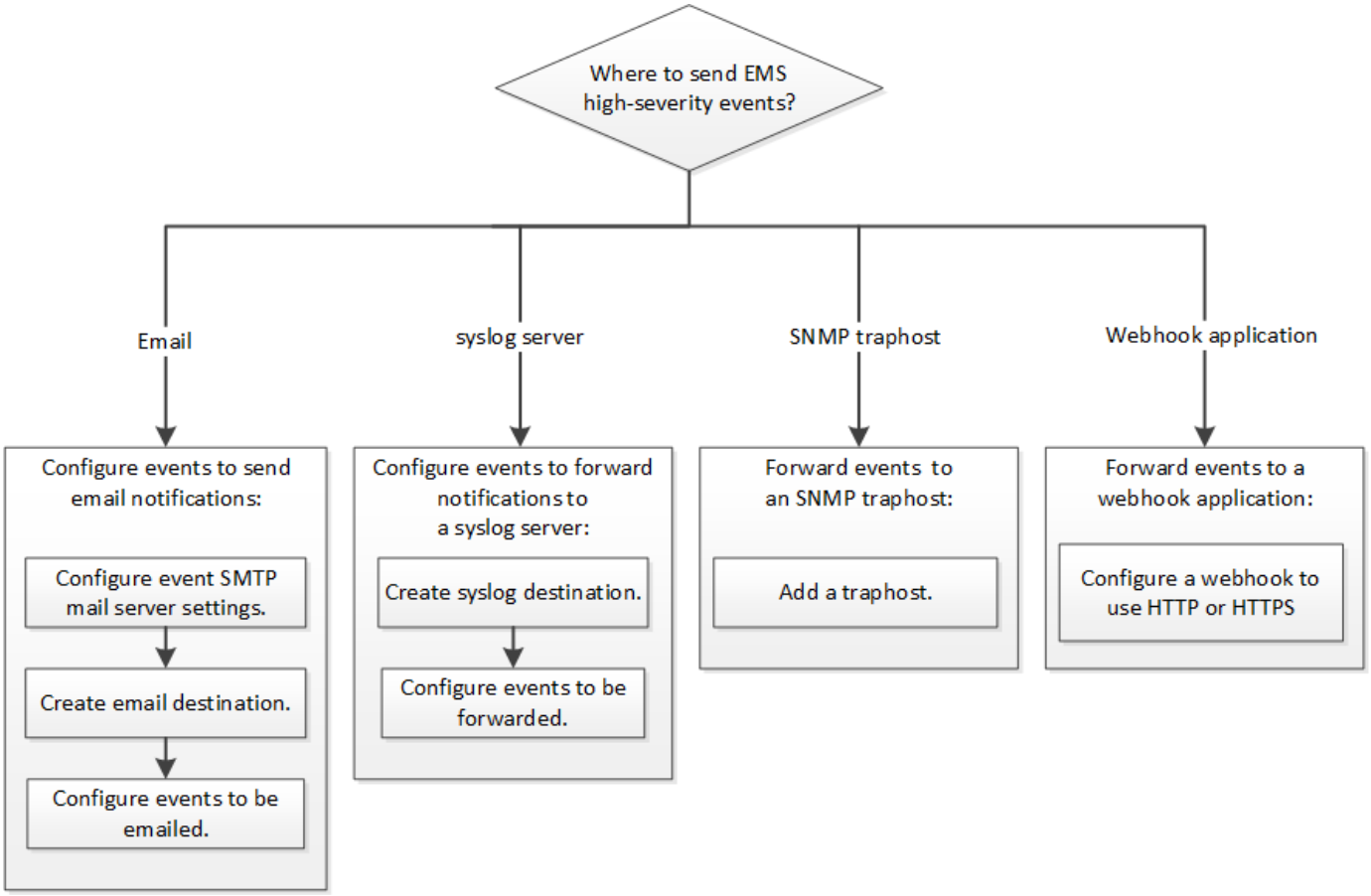
Debe configurar las notificaciones de eventos de EMS importantes para que se envíen como correo electrónico, se reenvíen a un servidor de syslog, se reenvíen a un host de capturas de SNMP o se reenvíen a una aplicación de webhook. Esto le ayuda a evitar interrupciones en el sistema tomando medidas correctivas de forma puntual.

Acerca de esta tarea

Si el entorno ya contiene un servidor de syslog para añadir los eventos registrados de otros sistemas, como servidores y aplicaciones, resulta más fácil utilizar el mismo servidor de syslog para enviar las notificaciones de eventos importantes de sistemas de almacenamiento.

Si el entorno no contiene ningún servidor de syslog, resulta más fácil usar un correo electrónico para enviar las notificaciones de eventos importantes.

Si ya ha reenviado notificaciones de eventos a un host de capturas de SNMP, es posible que desee supervisar dicho host de capturas para buscar eventos importantes.



Opciones

- Configure EMS para que envíe notificaciones de eventos.

Si desea que…	Consulte…
EMS envíe notificaciones de eventos importantes a una dirección de correo electrónico	Configure eventos de EMS importantes para que envíen notificaciones por correo electrónico
EMS reenvíe notificaciones de eventos importantes a un servidor de syslog	Configure eventos de EMS importantes para reenviar notificaciones a un servidor de syslog
EMS reenvíe notificaciones de eventos a un host de capturas de SNMP	Configure los hosts de capturas de SNMP para recibir notificaciones de eventos
Si desea que EMS reenvíe notificaciones de eventos a una aplicación webhook	Configure eventos EMS importantes para reenviar notificaciones a una aplicación webhook

Configure eventos de EMS de ONTAP importantes para que envíen notificaciones por correo electrónico

Para recibir notificaciones por correo electrónico acerca de los eventos más importantes, debe configurar EMS para que envíe mensajes por correo electrónico de los eventos que representan actividades importantes.

Antes de empezar

El DNS debe haberse configurado en el clúster para resolver las direcciones de correo electrónico.

Acerca de esta tarea

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

Pasos

1. Configure las opciones del servidor de correo SMTP de eventos:

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

   Obtenga más información sobre `event config modify` en el "Referencia de comandos del ONTAP".

2. Cree un destino de correo electrónico para las notificaciones de eventos:

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

   Obtenga más información sobre `event notification destination create` en el "Referencia de comandos del ONTAP".

3. Configure los eventos importantes para que envíen notificaciones por correo electrónico:

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

Obtenga más información sobre `event notification create` en el "Referencia de comandos del ONTAP".

Configure eventos de EMS de ONTAP importantes para reenviar notificaciones a un servidor de syslog

Para registrar las notificaciones de los eventos más graves en un servidor de syslog, debe configurar EMS para reenviar las notificaciones de los eventos que representan actividades importantes.

Antes de empezar

El DNS debe haberse configurado en el clúster para resolver el nombre del servidor de syslog.

Acerca de esta tarea

Si el entorno no contiene un servidor de syslog para las notificaciones de eventos, primero debe crear uno. Si el entorno ya contiene un servidor de syslog para registrar eventos de otros sistemas, se recomienda usarlo para las notificaciones de eventos importantes.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la CLI de ONTAP.

A partir de ONTAP 9.12.1, los eventos EMS se pueden enviar a un puerto designado en un servidor de syslog remoto a través del protocolo de seguridad de la capa de transporte (TLS). Hay dos nuevos parámetros disponibles:

`tcp-encrypted`

Cuando `tcp-encrypted` se especifica para `syslog-transport` , ONTAP verifica la identidad del host de destino validando su certificado. El valor predeterminado es `udp-unencrypted`.

`syslog-port`

El `syslog-port` parámetro Valor predeterminado depende del valor `syslog-transport` del parámetro. Si `syslog-transport` se establece en `tcp-encrypted`, `syslog-port` tiene el valor predeterminado 6514.

Pasos

1. Cree un destino de servidor de syslog para los eventos importantes:

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

   A partir de ONTAP 9.12,1, se pueden especificar los siguientes valores para `syslog-transport`:

   - `udp-unencrypted` - Protocolo de datagramas de usuario sin seguridad
   - `tcp-unencrypted` - Protocolo de control de transmisión sin seguridad
   - `tcp-encrypted` - Protocolo de control de transmisión con seguridad de la capa de transporte (TLS)

     El protocolo por defecto es `udp-unencrypted`.

   Obtenga más información sobre `event notification destination create` en el "Referencia de

comandos del ONTAP".

2. Configure los eventos importantes de manera que reenvíen notificaciones al servidor de syslog:

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

   Obtenga más información sobre `event notification create` en el "Referencia de comandos del ONTAP".

Configure los hosts de capturas de SNMP de ONTAP para que reciban notificaciones de eventos

Para recibir notificaciones de eventos en un host de capturas de SNMP, debe configurar un host de capturas.

Antes de empezar

- Se debe habilitar SNMP y las capturas de SNMP en el clúster.

  SNMP y las capturas de SNMP se habilitan de forma predeterminada.

- El DNS debe haberse configurado en el clúster para resolver los nombres de host de capturas.

Acerca de esta tarea

Si no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos (capturas de SNMP), debe añadir uno.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

Paso

1. Si su entorno no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos, añada uno:

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

   Todas las notificaciones de eventos que SNMP admite de forma predeterminada se reenvían al host de capturas de SNMP.

Configure eventos EMS importantes de ONTAP para reenviar notificaciones a una aplicación webhook

Puede configurar ONTAP para reenviar notificaciones de eventos importantes a una aplicación webhook. Los pasos de configuración necesarios dependen del nivel de seguridad que elija.

Prepare la configuración del reenvío de eventos EMS

Hay varios conceptos y requisitos que debe tener en cuenta antes de configurar ONTAP para reenviar notificaciones de eventos a una aplicación webhook.

Aplicación Webhook

Necesita una aplicación de webhook capaz de recibir las notificaciones de eventos de ONTAP. Un webhook es una rutina de devolución de llamada definida por el usuario que amplía la capacidad de la aplicación remota o el servidor donde se ejecuta. El cliente llama o activa a los enlaces web (en este caso ONTAP) enviando una solicitud HTTP a la dirección URL de destino. Específicamente, ONTAP envía una solicitud HTTP POST al servidor que aloja la aplicación webhook junto con los detalles de notificación de eventos formateados en XML.

Opciones de seguridad

Hay varias opciones de seguridad disponibles en función de cómo se utilice el protocolo de seguridad de la capa de transporte (TLS). La opción que elija determina la configuración de ONTAP que requiere.

TLS es un protocolo criptográfico que se utiliza ampliamente en Internet. Proporciona privacidad, así como integridad de datos y autenticación mediante uno o varios certificados de clave pública. Los certificados son emitidos por autoridades de certificados de confianza.

HTTP

Es posible utilizar HTTP para transportar las notificaciones de eventos. Con esta configuración, la conexión no es segura. Las identidades del cliente ONTAP y de la aplicación webhook no se verifican. Además, el tráfico de red no está cifrado ni protegido. Consulte "Configure un destino de webhook para utilizar HTTP" para obtener información detallada sobre la configuración.

HTTPS

Para mayor seguridad, puede instalar un certificado en el servidor que aloja la rutina de webhook. ONTAP utiliza el protocolo HTTPS para verificar la identidad del servidor de aplicaciones webhook, así como de ambas partes, para garantizar la privacidad e integridad del tráfico de red. Consulte "Configure un destino de webhook para utilizar HTTPS" para obtener información detallada sobre la configuración.

HTTPS con autenticación mutua

Puede mejorar aún más la seguridad HTTPS mediante la instalación de un certificado de cliente en el sistema ONTAP que emite las solicitudes webbook. Además ONTAP de verificar la identidad del servidor de aplicaciones webhook y proteger el tráfico de red, la aplicación webhook verifica la identidad del cliente ONTAP. Esta autenticación de par bidireccional se conoce como *Mutual TLS*. Consulte "Configure un destino de webhook para utilizar HTTPS con autenticación mutua" para obtener información detallada sobre la configuración.

Información relacionada

- "Protocolo de seguridad de la capa de transporte (TLS) versión 1.3"

Configure un destino de webhook para utilizar HTTP

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTP. Esta es la opción menos segura pero la más sencilla de configurar.

Pasos

1. Cree un nuevo destino `restapi-ems` para recibir los eventos:

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

   En el comando anterior, debe usar el esquema **HTTP** para el destino.

   Obtenga más información sobre `event notification destination create` en el "Referencia de comandos del ONTAP".

2. Cree una notificación que vincule el `important-events` filtro con el `restapi-ems` destino:

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

   Obtenga más información sobre `event notification create` en el "Referencia de comandos del ONTAP".

Configure un destino de webhook para utilizar HTTPS

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red.

Antes de empezar

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP

Pasos

1. Instale la clave privada y los certificados del servidor adecuados en el servidor que aloja la aplicación webhook. Los pasos de configuración específicos dependen del servidor.
2. Instale el certificado raíz de servidor en ONTAP:

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

   El comando solicitará el certificado.

3. Cree el `restapi-ems` destino para recibir los eventos:

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

   En el comando anterior, debe usar el esquema **HTTPS** para el destino.

4. Cree la notificación que enlaza el `important-events` filtro con el nuevo `restapi-ems` destino:

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

Configure un destino de webhook para utilizar HTTPS con autenticación mutua

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS con autenticación mutua. Con esta configuración hay dos certificados. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red. Además, la aplicación que aloja el webhook utiliza el certificado de cliente para confirmar la identidad del cliente ONTAP.

Antes de empezar

Debe hacer lo siguiente antes de configurar ONTAP:

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP
- Genere una clave privada y un certificado para el cliente ONTAP

Pasos

1. Realice los dos primeros pasos de la tarea "Configure un destino de webhook para utilizar HTTPS" para instalar el certificado de servidor para que ONTAP pueda verificar la identidad del servidor.
2. Instale los certificados raíz e intermedios adecuados en la aplicación webhook para validar el certificado de cliente.
3. Instale el certificado de cliente en ONTAP:

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

   El comando solicitará la clave privada y el certificado.

4. Cree el `restapi-ems` destino para recibir los eventos:

   ```
   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>
   ```

   En el comando anterior, debe utilizar el esquema **HTTPS** para el destino.

5. Cree la notificación que enlaza el `important-events` filtro con el nuevo `restapi-ems` destino:

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

Información relacionada

- "instalación del certificado de seguridad"