Configurare le notifiche degli eventi EMS con la CLI

ONTAP 9

NetApp
May 09, 2024

Sommario

Configurare le notifiche degli eventi EMS con la CLI

Workflow di configurazione EMS

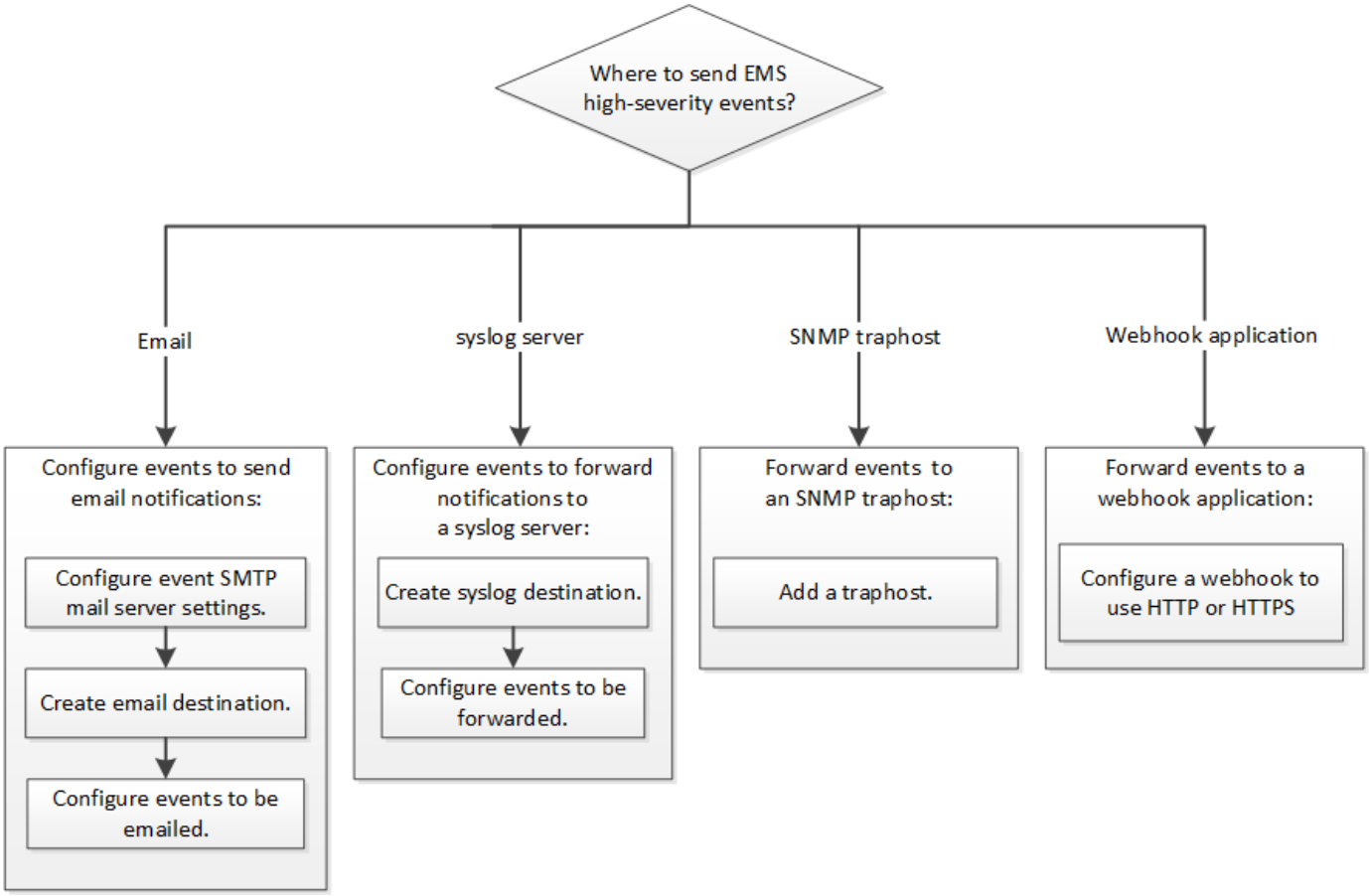
È necessario configurare le notifiche di eventi EMS importanti da inviare come email, inoltrate a un server syslog, inoltrate a un host traphost SNMP o inoltrate a un'applicazione webhook. In questo modo, è possibile evitare interruzioni del sistema adottando azioni correttive in modo tempestivo.

A proposito di questa attività

Se l'ambiente in uso contiene già un server syslog per l'aggregazione degli eventi registrati da altri sistemi, come server e applicazioni, è più semplice utilizzare tale server syslog anche per le notifiche di eventi importanti provenienti dai sistemi storage.

Se l'ambiente non contiene già un server syslog, è più semplice utilizzare l'e-mail per le notifiche di eventi importanti.

Se si inoltrano già notifiche di eventi a un host trapSNMP, potrebbe essere necessario monitorare tale host per rilevare eventi importanti.



Scelte

- Impostare EMS per l'invio delle notifiche degli eventi.

Se vuoi…	Fare riferimento a…
EMS per inviare notifiche di eventi importanti a un indirizzo e-mail	Configurare eventi EMS importanti per l'invio di notifiche e-mail
EMS per inoltrare notifiche di eventi importanti a un server syslog	Configurare eventi EMS importanti per inoltrare le notifiche a un server syslog
Se si desidera che EMS inoltri le notifiche degli eventi a un host trapSNMP	Configurare i traphost SNMP per ricevere le notifiche degli eventi
Se si desidera che EMS inoltri le notifiche degli eventi a un'applicazione webhook	Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook

Configurare eventi EMS importanti per l'invio di notifiche e-mail

Per ricevere notifiche via email degli eventi più importanti, è necessario configurare il servizio EMS in modo che invii messaggi di posta elettronica per gli eventi che segnalano attività importanti.

Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere gli indirizzi e-mail.

A proposito di questa attività

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

Fasi

1. Configurare le impostazioni del server di posta SMTP dell'evento:

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

2. Creare una destinazione email per le notifiche degli eventi:

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

3. Configurare gli eventi importanti per l'invio di notifiche e-mail:

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

Configurazione di eventi EMS importanti per inoltrare le notifiche a un server syslog

Per registrare le notifiche degli eventi più gravi su un server syslog, è necessario configurare EMS in modo che inoltri le notifiche per gli eventi che segnalano attività importanti.

Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere il nome del server syslog.

A proposito di questa attività

Se l'ambiente non contiene già un server syslog per le notifiche degli eventi, è necessario crearne uno. Se l'ambiente in uso contiene già un server syslog per la registrazione degli eventi da altri sistemi, è possibile utilizzare tale server per le notifiche di eventi importanti.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nell'interfaccia utente di ONTAP.

A partire da ONTAP 9.12.1, gli eventi EMS possono essere inviati a una porta designata su un server syslog remoto tramite il protocollo TLS (Transport Layer Security). Sono disponibili due nuovi parametri:

`tcp-encrypted`

Quando `tcp-encrypted` è specificato per `syslog-transport`, ONTAP verifica l'identità dell'host di destinazione convalidandone il certificato. Il valore predefinito è `udp-unencrypted`.

`syslog-port`

Il valore predefinito `syslog-port` il parametro dipende dall'impostazione di `syslog-transport` parametro. Se `syslog-transport` è impostato su `tcp-encrypted`, `syslog-port` ha il valore predefinito 6514.

Per ulteriori informazioni, vedere `event notification destination create` pagina man.

Fasi

1. Creare una destinazione del server syslog per eventi importanti:

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

   A partire da ONTAP 9.12.1, è possibile specificare i seguenti valori per `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol senza sicurezza
   - `tcp-unencrypted` – Transmission Control Protocol senza sicurezza
   - `tcp-encrypted` - Transmission Control Protocol con Transport Layer Security (TLS)

   Il protocollo predefinito è `udp-unencrypted`.

2. Configurare gli eventi importanti per inoltrare le notifiche al server syslog:

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

Configurare i traphost SNMP per ricevere le notifiche degli eventi

Per ricevere le notifiche degli eventi su un host trapSNMP, è necessario configurare un host traphost.

Di cosa hai bisogno

- I trap SNMP e SNMP devono essere attivati sul cluster.

  I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.

A proposito di questa attività

Se non si dispone già di un host trapSNMP configurato per ricevere notifiche di eventi (trap SNMP), è necessario aggiungerne uno.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

Fase

1. Se l'ambiente non dispone già di un host trapSNMP configurato per ricevere le notifiche degli eventi, aggiungerne uno:

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

   Tutte le notifiche degli eventi supportate da SNMP per impostazione predefinita vengono inoltrate all'host principale SNMP.

Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook

È possibile configurare ONTAP per inoltrare notifiche di eventi importanti a un'applicazione webhook. I passaggi necessari per la configurazione dipendono dal livello di sicurezza scelto.

Prepararsi a configurare l'inoltro degli eventi EMS

Prima di configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook, è necessario prendere in considerazione diversi concetti e requisiti.

Applicazione Webhook

È necessaria un'applicazione webhook in grado di ricevere le notifiche degli eventi ONTAP. Un webhook è una routine di callback definita dall'utente che estende le funzionalità dell'applicazione o del server remoto in cui viene eseguito. I webhook vengono chiamati o attivati dal client (in questo caso ONTAP) inviando una richiesta HTTP all'URL di destinazione. In particolare, ONTAP invia una richiesta HTTP POST al server che ospita l'applicazione webhook insieme ai dettagli della notifica degli eventi formattati in XML.

Opzioni di sicurezza

Sono disponibili diverse opzioni di sicurezza a seconda di come viene utilizzato il protocollo TLS (Transport Layer Security). L'opzione scelta determina la configurazione ONTAP richiesta.

> TLS è un protocollo crittografico ampiamente utilizzato su Internet. Fornisce privacy, integrità dei dati e autenticazione utilizzando uno o più certificati a chiave pubblica. I certificati vengono emessi da autorità di certificazione attendibili.

HTTP

È possibile utilizzare HTTP per trasportare le notifiche degli eventi. Con questa configurazione, la connessione non è sicura. Le identità del client ONTAP e dell'applicazione webhook non vengono verificate. Inoltre, il traffico di rete non viene crittografato o protetto. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTP" per informazioni dettagliate sulla configurazione.

HTTPS

Per una maggiore sicurezza, è possibile installare un certificato sul server che ospita la routine webhook. Il protocollo HTTPS viene utilizzato da ONTAP per verificare l'identità del server applicazioni webhook e da entrambe le parti per garantire la privacy e l'integrità del traffico di rete. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTPS" per informazioni dettagliate sulla configurazione.

HTTPS con autenticazione reciproca

È possibile migliorare ulteriormente la protezione HTTPS installando un certificato client sul sistema ONTAP che invia le richieste del manuale. Oltre a verificare l'identità del server dell'applicazione webhook e a proteggere il traffico di rete, ONTAP verifica l'identità del client ONTAP. Questa autenticazione peer bidirezionale è nota come *Mutual TLS*. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca" per informazioni dettagliate sulla configurazione.

Informazioni correlate

- "Il protocollo TLS (Transport Layer Security) versione 1.3"

Configurare una destinazione webhook per l'utilizzo di HTTP

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTP. Si tratta dell'opzione meno sicura, ma la più semplice da configurare.

Fasi

1. Creare una nuova destinazione `restapi-ems` per ricevere gli eventi:

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

   Nel comando precedente, è necessario utilizzare lo schema **HTTP** per la destinazione.

2. Creare una notifica che colleghi `important-events` filtrare con `restapi-ems` destinazione:

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

Configurare una destinazione webhook per l'utilizzo di HTTPS

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete.

Prima di iniziare

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP

Fasi

1. Installare la chiave privata del server e i certificati appropriati sul server che ospita l'applicazione webhook. Le specifiche fasi di configurazione dipendono dal server.
2. Installare il certificato root del server in ONTAP:

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

   Il comando chiederà il certificato.

3. Creare il `restapi-ems` destinazione per ricevere gli eventi:

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

   Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

4. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

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

Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca

È possibile configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS con autenticazione reciproca. Con questa configurazione sono disponibili due certificati. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete. Inoltre, l'applicazione che ospita il webhook utilizza il certificato client per confermare l'identità del client ONTAP.

Prima di iniziare

Prima di configurare ONTAP, è necessario effettuare le seguenti operazioni:

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP
- Generare una chiave privata e un certificato per il client ONTAP

Fasi

1. Eseguire le prime due fasi dell'attività "Configurare una destinazione webhook per l'utilizzo di HTTPS" Per installare il certificato del server in modo che ONTAP possa verificare l'identità del server.

2. Installare i certificati root e intermedi appropriati nell'applicazione webhook per convalidare il certificato client.
3. Installare il certificato client in ONTAP:

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

   Il comando richiede la chiave privata e il certificato.

4. Creare il `restapi-ems` destinazione per ricevere gli eventi:

   ```
   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>
   ```

   Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

5. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

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