Configurazione EMS

ONTAP 9

NetApp
May 09, 2024

Sommario

Configurazione EMS

Panoramica della configurazione EMS

È possibile configurare ONTAP 9 in modo che invii notifiche di eventi EMS (sistema di gestione degli eventi) importanti direttamente a un indirizzo e-mail, a un server syslog, a un traphost SNMP (Simple Management Network Protocol) o a un'applicazione webhook, in modo da ricevere una notifica immediata dei problemi di sistema che richiedono un'attenzione immediata.

Poiché le notifiche di eventi importanti non sono attivate per impostazione predefinita, è necessario configurare EMS in modo che invii le notifiche a un indirizzo e-mail, a un server syslog, a un host trapSNMP o a un'applicazione webhook.

Esaminare le versioni specifiche della release di "Riferimento EMS ONTAP 9".

Se la mappatura degli eventi EMS utilizza set di comandi ONTAP deprecati (come destinazione dell'evento, percorso dell'evento), si consiglia di aggiornare la mappatura. "Scopri come aggiornare la mappatura EMS da comandi ONTAP non aggiornati".

Configurare le notifiche e i filtri degli eventi EMS con System Manager

È possibile utilizzare System Manager per configurare il modo in cui il sistema di gestione degli eventi (EMS) invia le notifiche degli eventi, in modo da poter essere avvisati dei problemi di sistema che richiedono una rapida attenzione.

Versione di ONTAP	Con System Manager, è possibile…
ONTAP 9.12.1 e versioni successive	Specificare il protocollo TLS (Transport Layer Security) quando si inviano eventi ai server syslog remoti.
ONTAP 9.10.1 e versioni successive	Configurare indirizzi e-mail, server syslog, applicazioni webhook e host SNMP.
ONTAP da 9.7 a 9.10.0	Configurare solo i traphost SNMP. È possibile configurare un'altra destinazione EMS con la CLI ONTAP. Vedere "Panoramica della configurazione EMS".

È possibile eseguire le seguenti procedure:

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]

- [delete-ems-filter]

Informazioni correlate

- "Riferimento EMS ONTAP"
- "Utilizzo della CLI per configurare i traphost SNMP in modo che ricevano le notifiche degli eventi"

Aggiungere una destinazione di notifica degli eventi EMS

È possibile utilizzare System Manager per specificare dove si desidera inviare i messaggi EMS.

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

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Fare clic su + Add .
5. Specificare un nome, un tipo di destinazione EMS e i filtri.

   Se necessario, è possibile aggiungere un nuovo filtro. Fare clic su **Aggiungi un nuovo filtro eventi**.

6. A seconda del tipo di destinazione EMS selezionato, specificare quanto segue:

Per configurare…	Specificare o selezionare…
SNMP traphost	• Nome TrapHost
E-mail (A partire da 9.10.1)	• Indirizzo e-mail di destinazione • Server di posta • Da indirizzo e-mail
Server syslog (A partire da 9.10.1)	• Nome host o indirizzo IP del server • Porta syslog (a partire da 9.12.1) • Trasporto syslog (a partire da 9.12.1) Selezionando **TCP Encrypted** si attiva il protocollo TLS (Transport Layer Security). Se non viene immesso alcun valore per **porta Syslog**, viene utilizzato un valore predefinito in base alla selezione **trasporto Syslog**.

Webhook (A partire da 9.10.1)	• URL Webhook • Autenticazione client (selezionare questa opzione per specificare un certificato client)

Creare un nuovo filtro per la notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per definire nuovi filtri personalizzati che specificano le regole per la gestione delle notifiche EMS.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Fare clic su + Add .
5. Specificare un nome e scegliere se si desidera copiare le regole da un filtro eventi esistente o aggiungere nuove regole.
6. A seconda della scelta, attenersi alla seguente procedura:

Se si sceglie….	Quindi, eseguire questi passaggi…
Copia delle regole dal filtro eventi esistente	1. Selezionare un filtro eventi esistente. 2. Modificare le regole esistenti. 3. Aggiungere altre regole, se necessario, facendo clic su + Add .
Aggiungi nuove regole	Specificare il tipo, il modello di nome, le severità e il tipo di trap SNMP per ogni nuova regola.

Modificare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare le informazioni di destinazione della notifica degli eventi.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su ⋮, Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni sulla destinazione dell'evento, quindi fare clic su **Salva**.

Modificare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare i filtri personalizzati e

modificare la modalità di gestione delle notifiche degli eventi.

> Non è possibile modificare i filtri definiti dal sistema.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su ⋮, Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni del filtro eventi, quindi fare clic su **Save** (Salva).

Eliminare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare una destinazione di notifica degli eventi EMS.

> Non è possibile eliminare le destinazioni SNMP.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su ⋮, Quindi fare clic su **Delete** (Elimina).

Eliminare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare i filtri personalizzati.

> Non è possibile eliminare i filtri definiti dal sistema.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su ⋮, Quindi fare clic su **Delete** (Elimina).

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

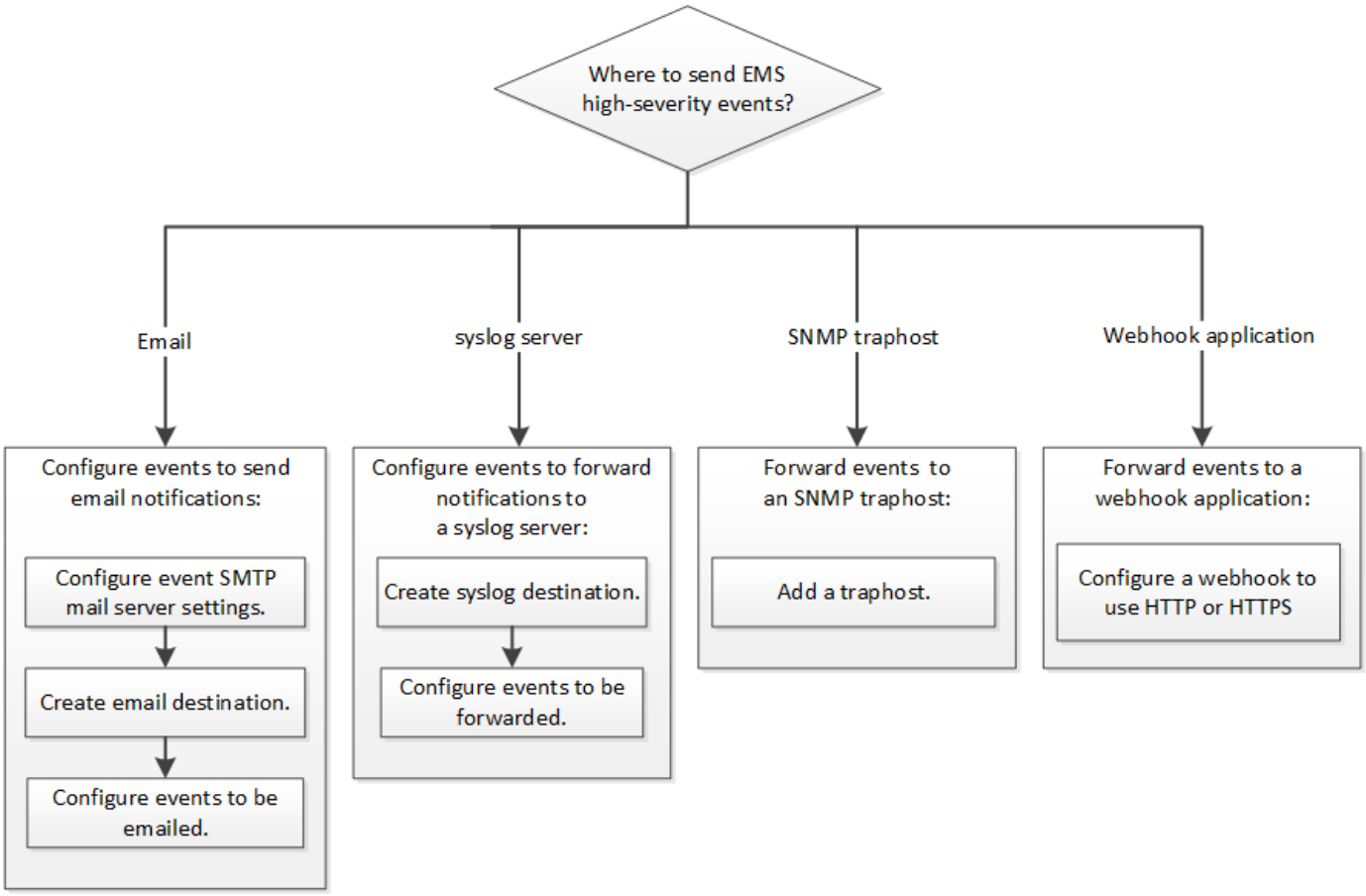
adottando azioni correttive in modo tempestivo.

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`

Aggiornare la mappatura degli eventi EMS obsoleta

Modelli di mappatura degli eventi EMS

Prima di ONTAP 9.0, gli eventi EMS potevano essere mappati solo alle destinazioni degli eventi in base alla corrispondenza del modello di nome dell'evento. Il comando ONTAP viene impostato (`event destination`, `event route`) Che utilizzano questo modello continuano a essere disponibili nelle ultime versioni di ONTAP, ma sono state deprecate a partire da ONTAP 9.0.

A partire da ONTAP 9.0, la Best practice per il mapping della destinazione degli eventi EMS di ONTAP consiste nell'utilizzare il modello di filtro eventi più scalabile in cui la corrispondenza dei modelli viene eseguita su più campi, utilizzando l' `event filter`, `event notification`, e. `event notification destination` set di comandi.

Se la mappatura EMS è configurata utilizzando i comandi non aggiornati, aggiornare la mappatura per utilizzare `event filter`, `event notification`, e. `event notification destination` set di comandi.

Esistono due tipi di destinazioni degli eventi:

1. **Destinazioni generate dal sistema**: Esistono cinque destinazioni di eventi generate dal sistema (create per impostazione predefinita)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Alcune destinazioni generate dal sistema sono destinate a scopi speciali. Ad esempio, la destinazione asup instrada gli eventi callhome.* al modulo AutoSupport in ONTAP per generare messaggi AutoSupport.
2. **Destinazioni create dall'utente**: Vengono create manualmente utilizzando `event destination create` comando.

```
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.
```

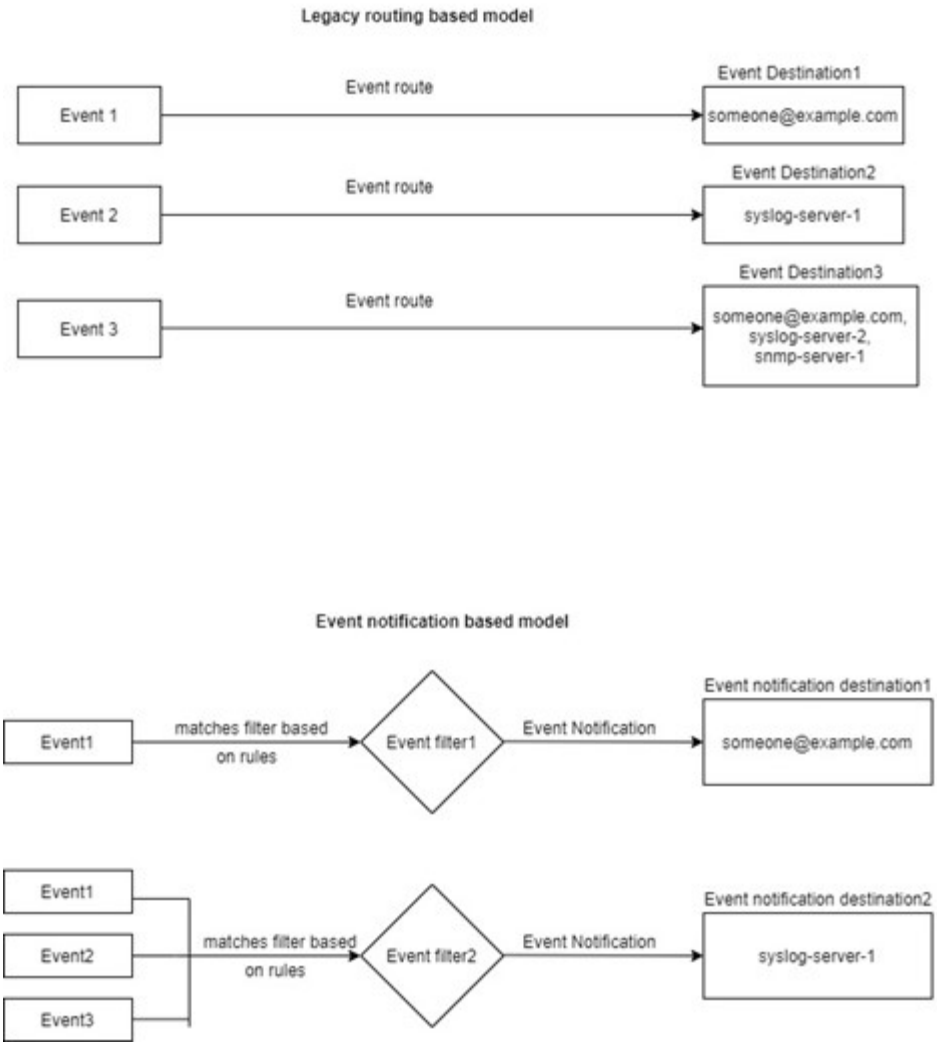
Nel modello obsoleto, gli eventi EMS vengono mappati singolarmente a una destinazione utilizzando `event route add-destinations` comando.

```
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.
```

Il nuovo meccanismo di notifica degli eventi EMS, più scalabile, si basa sui filtri degli eventi e sulle destinazioni di notifica degli eventi. Fare riferimento al seguente articolo della Knowledge base per informazioni dettagliate sul nuovo meccanismo di notifica degli eventi:

- "Panoramica del sistema di gestione degli eventi per ONTAP 9"



Aggiornare la mappatura degli eventi EMS dai comandi ONTAP non aggiornati

Se la mappatura degli eventi EMS è attualmente configurata utilizzando i set di comandi ONTAP deprecati (`event destination`, `event route`), seguire questa procedura per aggiornare la mappatura per utilizzare `event filter`, `event notification`, e. `event notification destination` set di comandi.

Fasi

1. Elencare tutte le destinazioni degli eventi nel sistema utilizzando `event destination show` comando.

```
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. Per ciascuna destinazione, elencare gli eventi associati utilizzando `event route show -destinations <destination name>` comando.

```
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. Creare un corrispondente `event filter` che include tutti questi sottoinsiemi di eventi. Ad esempio, se si desidera includere solo il `raid.aggr.*` eventi, utilizzare un carattere jolly per `message-name` quando si crea il filtro. È inoltre possibile creare filtri per singoli eventi.

> È possibile creare fino a 50 filtri per eventi.

```
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. Creare un `event notification destination` per ciascuno di `event destination` Endpoint (ad esempio, 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. Creare una notifica degli eventi mappando il filtro degli eventi alla destinazione di notifica degli eventi.

```
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. Ripetere i punti 1-5 per ciascuno `event destination` questo ha un `event route` mappatura.

Gli eventi instradati alle destinazioni SNMP devono essere mappati a. `snmp-traphost` destinazione della notifica degli eventi. La destinazione SNMP traphost utilizza l'host SNMP traphost configurato dal sistema.

```
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?: -
```