Configuração EMS

ONTAP 9

NetApp
January 17, 2025

Índice

Configuração EMS 1
Visão geral da configuração EMS 1
Configurar notificações e filtros de eventos EMS com o System Manager 1
Configure as notificações de eventos EMS com a CLI 4
Atualizar mapeamento de eventos EMS obsoleto 11

Configuração EMS

Visão geral da configuração EMS

Você pode configurar o ONTAP 9 para enviar notificações de eventos importantes do EMS (sistema de gerenciamento de eventos) diretamente para um endereço de e-mail, servidor syslog, traphost de protocolo de rede de gerenciamento simples (SNMP) ou aplicativo webhook para que você seja imediatamente notificado sobre problemas do sistema que exigem atenção imediata.

Como as notificações de eventos importantes não estão habilitadas por padrão, você precisa configurar o EMS para enviar notificações para um endereço de e-mail, um servidor syslog, um traphost SNMP ou um aplicativo webhook.

Reveja as versões específicas da versão do "Referência EMS da ONTAP 9".

Se o mapeamento de eventos do EMS usar conjuntos de comandos ONTAP obsoletos (como destino de eventos, rota de eventos), é recomendável atualizar o mapeamento. "Saiba como atualizar seu mapeamento EMS a partir de comandos ONTAP obsoletos".

Configurar notificações e filtros de eventos EMS com o System Manager

Você pode usar o System Manager para configurar como o sistema de gerenciamento de eventos (EMS) entrega notificações de eventos para que você possa ser notificado sobre problemas do sistema que exigem sua atenção imediata.

Versão de ONTAP	Com o System Manager, você pode…
ONTAP 9.12,1 e posterior	Especifique o protocolo TLS (Transport Layer Security) ao enviar eventos para servidores syslog remotos.
ONTAP 9.10,1 e posterior	Configure endereços de e-mail, servidores syslog e aplicativos de webhook, bem como hosts SNMP.
ONTAP 9 F.7 a 9.10.0	Configurar apenas os hosts SNMP. Você pode configurar outro destino EMS com a CLI do ONTAP. "Visão geral da configuração EMS"Consulte .

Você pode executar os seguintes procedimentos:

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

- [delete-ems-filter]

Informações relacionadas

- "Referência EMS da ONTAP"
- "Usando a CLI para configurar hosts SNMP para receber notificações de eventos"

Adicionar um destino de notificação de evento EMS

Você pode usar o System Manager para especificar para onde deseja que as mensagens EMS sejam enviadas.

A partir do ONTAP 9.12,1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Para obter detalhes, consulte a `event notification destination create` página de manual.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Clique em + Add .
5. Especifique um nome, um tipo de destino EMS e filtros.

   Se necessário, você pode adicionar um novo filtro. Clique em **Adicionar um novo filtro de evento**.

6. Dependendo do tipo de destino EMS selecionado, especifique o seguinte:

Para configurar…	Especificar ou selecionar…
SNMP traphost	• Nome do Traphost
E-mail (Começando com 9.10.1)	• Endereço de e-mail de destino • Servidor de correio • Do endereço de e-mail
Servidor syslog (Começando com 9.10.1)	• Nome do host ou endereço IP do servidor • Porta syslog (começando com 9.12.1) • Transporte syslog (começando com 9.12.1) Selecionar **TCP Encrypted** ativa o protocolo TLS (Transport Layer Security). Se nenhum valor for inserido para **Syslog port**, um padrão será usado com base na seleção **Syslog transport**.

Webhook (Começando com 9.10.1)	• URL do webhook • Autenticação de cliente (selecione esta opção para especificar um certificado de cliente)

Crie um novo filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para definir novos filtros personalizados que especificam as regras para o tratamento de notificações EMS.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Clique em Add .
5. Especifique um nome e selecione se deseja copiar regras de um filtro de evento existente ou adicionar novas regras.
6. Dependendo da sua escolha, execute as seguintes etapas:

Se você escolher…	Em seguida, execute estes passos…
Copiar regras do filtro de eventos existente	1. Selecione um filtro de eventos existente. 2. Modifique as regras existentes. 3. Adicione outras regras, se necessário, clicando em Add .
Adicione novas regras	Especifique o tipo, o padrão de nome, as severidades e o tipo de trap SNMP para cada nova regra.

Editar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para alterar as informações de destino da notificação de eventos.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Ao lado do nome do destino do evento, clique em e, em seguida, clique em **Editar**.
5. Modifique as informações de destino do evento e clique em **Salvar**.

Editar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para modificar filtros personalizados para alterar a forma como as notificações de eventos são tratadas.

Não é possível modificar filtros definidos pelo sistema.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique em e, em seguida, clique em **Editar**.
5. Modifique as informações do filtro de eventos e clique em **Salvar**.

Eliminar um destino de notificação de evento EMS

A partir do ONTAP 9.10,1, pode utilizar o Gestor do sistema para eliminar um destino de notificação de eventos EMS.

Não é possível eliminar destinos SNMP.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **Destinos de eventos**.
4. Ao lado do nome do destino do evento, clique em e, em seguida, clique em **Excluir**.

Eliminar um filtro de notificação de eventos EMS

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para excluir filtros personalizados.

Não é possível eliminar filtros definidos pelo sistema.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção **Gerenciamento de notificações**, clique em **Exibir destinos de eventos**.
3. Na página **Gerenciamento de notificações**, selecione a guia **filtros de eventos**.
4. Ao lado do nome do filtro de evento, clique em e, em seguida, clique em **Eliminar**.

Configure as notificações de eventos EMS com a CLI

Fluxo de trabalho de configuração do EMS

Você deve configurar notificações importantes de eventos EMS para serem enviadas como e-mail, encaminhadas para um servidor syslog, encaminhadas para um traphost SNMP ou encaminhadas para um aplicativo webhook. Isso ajuda você a evitar interrupções no sistema, tomando ações corretivas em tempo hábil.

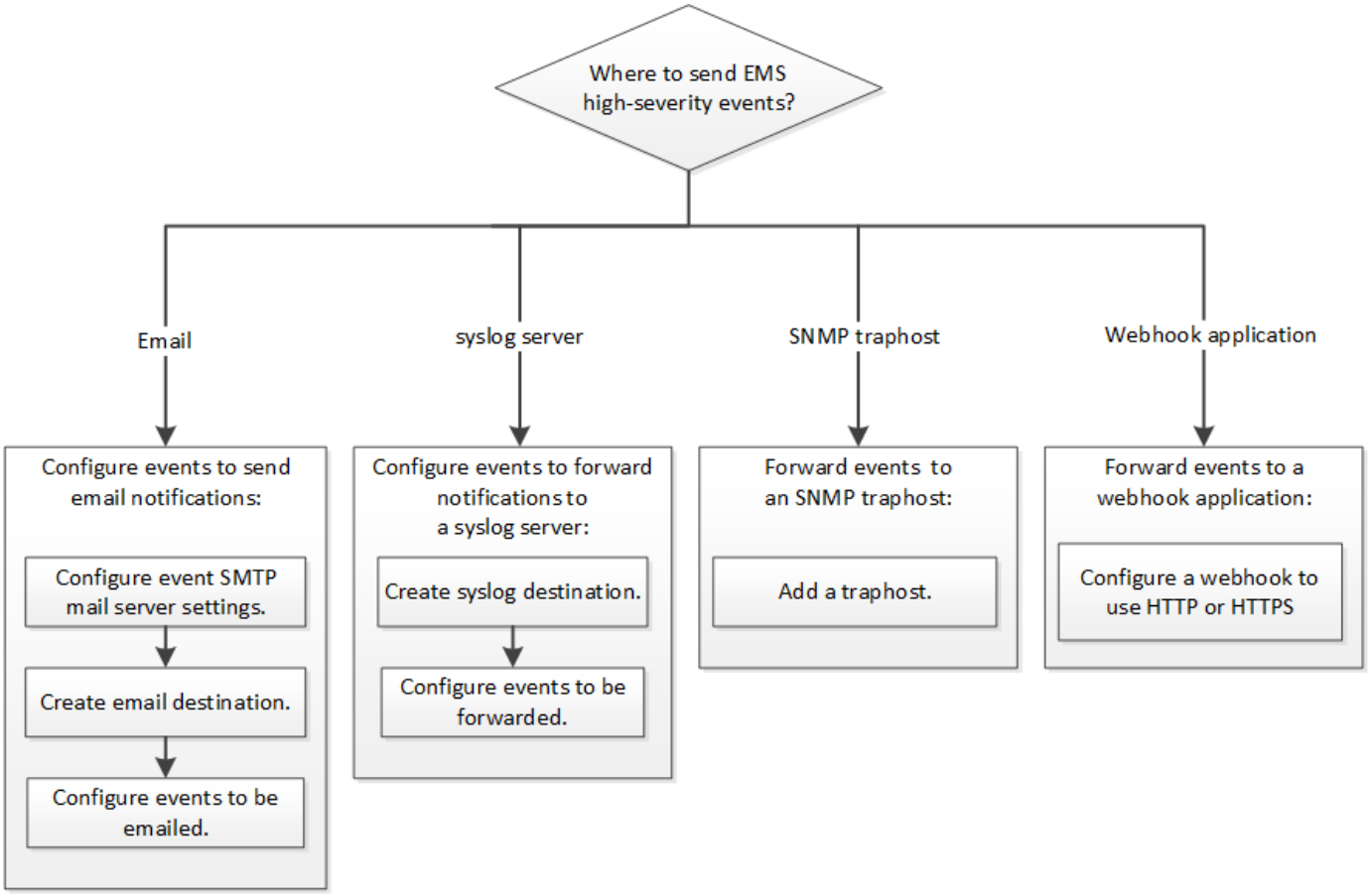
Sobre esta tarefa

Se o seu ambiente já contém um servidor syslog para agregar os eventos registrados de outros sistemas,

como servidores e aplicativos, então é mais fácil usar esse servidor syslog também para notificações de eventos importantes de sistemas de armazenamento.

Se o seu ambiente ainda não contém um servidor syslog, é mais fácil usar e-mail para notificações de eventos importantes.

Se você já encaminhar notificações de eventos para um traphost SNMP, talvez queira monitorar esse traphost para eventos importantes.



Opções

- Defina EMS para enviar notificações de eventos.

Se você quiser…	Consulte isto…
O EMS para enviar notificações de eventos importantes para um endereço de e-mail	Configurar eventos importantes do EMS para enviar notificações por e-mail
O EMS para encaminhar notificações de eventos importantes para um servidor syslog	Configure eventos importantes do EMS para encaminhar notificações para um servidor syslog
Se você quiser que o EMS encaminhe notificações de eventos para um traphost SNMP	Configure os hosts SNMP para receber notificações de eventos

Se você quiser que o EMS encaminhe notificações de eventos para um aplicativo webhook	Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook

Configurar eventos importantes do EMS para enviar notificações por e-mail

Para receber notificações por e-mail dos eventos mais importantes, você deve configurar o EMS para enviar mensagens de e-mail para eventos que sinalizem atividade importante.

O que você vai precisar

O DNS deve ser configurado no cluster para resolver os endereços de e-mail.

Sobre esta tarefa

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

Passos

1. Configure as definições do servidor de correio SMTP de eventos:

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

2. Criar um destino de e-mail para notificações de eventos:

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

3. Configure os eventos importantes para enviar notificações por e-mail:

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

Configurando eventos importantes do EMS para encaminhar notificações para um servidor syslog

Para Registrar notificações dos eventos mais graves em um servidor syslog, você deve configurar o EMS para encaminhar notificações de eventos que sinalizam atividade importante.

O que você vai precisar

O DNS deve ser configurado no cluster para resolver o nome do servidor syslog.

Sobre esta tarefa

Se o seu ambiente ainda não contiver um servidor syslog para notificações de eventos, você deve primeiro criar um. Se o seu ambiente já contiver um servidor syslog para registar eventos de outros sistemas, talvez você queira usá-lo para notificações de eventos importantes.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na CLI

do ONTAP.

A partir do ONTAP 9.12,1, os eventos EMS podem ser enviados para uma porta designada em um servidor syslog remoto através do protocolo TLS (Transport Layer Security). Dois novos parâmetros estão disponíveis:

`tcp-encrypted`

Quando `tcp-encrypted` for especificado para o `syslog-transport`, o ONTAP verifica a identidade do host de destino validando seu certificado. O valor padrão é `udp-unencrypted`.

`syslog-port`

O parâmetro valor padrão `syslog-port` depende da configuração do `syslog-transport` parâmetro. Se `syslog-transport` estiver definido como `tcp-encrypted`, `syslog-port` tem o valor padrão 6514.

Para obter detalhes, consulte a `event notification destination create` página de manual.

Passos

1. Crie um destino de servidor syslog para 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, os seguintes valores podem ser especificados para `syslog-transport`:

   - `udp-unencrypted` - Protocolo de datagrama de usuário sem segurança
   - `tcp-unencrypted` - Protocolo de Controle de transmissão sem segurança
   - `tcp-encrypted` - Protocolo de Controle de transmissão com Transport Layer Security (TLS)

   O protocolo predefinido é `udp-unencrypted`.

2. Configure os eventos importantes para encaminhar notificações para o servidor syslog:

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

Configure os hosts SNMP para receber notificações de eventos

Para receber notificações de eventos em um traphost SNMP, você deve configurar um traphost.

O que você vai precisar

- Os traps SNMP e SNMP devem estar ativados no cluster.

  As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do traphost.

Sobre esta tarefa

Se você ainda não tiver um traphost SNMP configurado para receber notificações de eventos (traps SNMP), você deve adicionar um.

Você pode executar essa tarefa sempre que o cluster estiver sendo executado inserindo os comandos na linha de comando ONTAP.

Passo

1. Se o seu ambiente ainda não tiver um traphost SNMP configurado para receber notificações de eventos, adicione uma:

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

   Todas as notificações de eventos que são suportadas por SNMP por padrão são encaminhadas para o traphost SNMP.

Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook

Você pode configurar o ONTAP para encaminhar notificações de eventos importantes para um aplicativo webhook. As etapas de configuração necessárias dependem do nível de segurança escolhido.

Prepare-se para configurar o encaminhamento de eventos EMS

Há vários conceitos e requisitos que você deve considerar antes de configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook.

Aplicação webhook

Você precisa de um aplicativo webhook capaz de receber as notificações de eventos do ONTAP. Um webhook é uma rotina de retorno de chamada definida pelo usuário que estende a capacidade do aplicativo ou servidor remoto onde ele é executado. Webhooks são chamados ou ativados pelo cliente (neste caso ONTAP) enviando uma solicitação HTTP para o URL de destino. Especificamente, o ONTAP envia uma solicitação HTTP POST para o servidor que hospeda o aplicativo webhook junto com os detalhes de notificação de evento formatados em XML.

Opções de segurança

Existem várias opções de segurança disponíveis, dependendo de como o protocolo TLS (Transport Layer Security) é usado. A opção escolhida determina a configuração necessária do ONTAP.

> TLS é um protocolo criptográfico amplamente utilizado na internet. Ele fornece privacidade, bem como integridade de dados e autenticação usando um ou mais certificados de chave pública. Os certificados são emitidos por autoridades de certificação confiáveis.

HTTP

Você pode usar HTTP para transportar as notificações de eventos. Com esta configuração, a conexão não é segura. As identidades do cliente ONTAP e da aplicação webhook não são verificadas. Além disso, o tráfego de rede não é criptografado ou protegido. "Configure um destino de webhook para usar HTTP"Consulte para obter os detalhes de configuração.

HTTPS

Para segurança adicional, você pode instalar um certificado no servidor que hospeda a rotina do webhook. O protocolo HTTPS é usado pelo ONTAP para verificar a identidade do servidor de aplicativos webhook, bem como por ambas as partes para garantir a privacidade e integridade do tráfego de rede. "Configure um

destino de webhook para usar HTTPS"Consulte para obter os detalhes de configuração.

HTTPS com autenticação mútua

Você pode aprimorar ainda mais a segurança HTTPS instalando um certificado de cliente no sistema ONTAP que emite as solicitações de webbook. Além de o ONTAP verificar a identidade do servidor de aplicativos webhook e proteger o tráfego de rede, o aplicativo webhook verifica a identidade do cliente ONTAP. Essa autenticação de dois sentidos é conhecida como *Mutual TLS*. "Configure um destino de webhook para usar HTTPS com autenticação mútua"Consulte para obter os detalhes de configuração.

Informações relacionadas

- "O protocolo TLS (Transport Layer Security) versão 1,3"

Configure um destino de webhook para usar HTTP

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo webhook usando HTTP. Esta é a opção menos segura, mas a mais simples de configurar.

Passos

1. Crie um novo destino `restapi-ems` para receber os eventos:

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

   No comando acima, você deve usar o esquema **HTTP** para o destino.

2. Crie uma notificação vinculando o `important-events` filtro ao `restapi-ems` destino:

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

Configure um destino de webhook para usar HTTPS

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook, bem como proteger o tráfego de rede.

Antes de começar

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP

Passos

1. Instale a chave privada do servidor e os certificados apropriados no servidor que hospeda seu aplicativo webhook. As etapas de configuração específicas dependem do servidor.
2. Instale o certificado raiz do servidor no ONTAP:

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

   O comando pedirá o certificado.

3. Crie o `restapi-ems` destino para receber os eventos:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   ```

```
https://<webhook-application>
```

No comando acima, você deve usar o esquema **HTTPS** para o destino.

4. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

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

Configure um destino de webhook para usar HTTPS com autenticação mútua

Você pode configurar o ONTAP para encaminhar notificações de eventos para um aplicativo de webhook usando HTTPS com autenticação mútua. Com esta configuração existem dois certificados. O ONTAP usa o certificado do servidor para confirmar a identidade do aplicativo webhook e proteger o tráfego de rede. Além disso, o aplicativo que hospeda o webhook usa o certificado de cliente para confirmar a identidade do cliente ONTAP.

Antes de começar

Você deve fazer o seguinte antes de configurar o ONTAP:

- Gerar uma chave privada e um certificado para o servidor de aplicativos webhook
- Tenha o certificado raiz disponível para instalação no ONTAP
- Gerar uma chave privada e um certificado para o cliente ONTAP

Passos

1. Execute as duas primeiras etapas da tarefa "Configure um destino de webhook para usar HTTPS" para instalar o certificado do servidor para que o ONTAP possa verificar a identidade do servidor.
2. Instale os certificados raiz e intermediários apropriados no aplicativo webhook para validar o certificado do cliente.
3. Instale o certificado de cliente no ONTAP:

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

O comando pedirá a chave privada e o certificado.

4. Crie o `restapi-ems` destino para receber os 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>
```

No comando acima, você deve usar o esquema **HTTPS** para destino.

5. Crie a notificação que vincula o `important-events` filtro ao novo `restapi-ems` destino:

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

Atualizar mapeamento de eventos EMS obsoleto

Modelos de mapeamento de eventos EMS

Antes do ONTAP 9.0, os eventos EMS só podiam ser mapeados para destinos de eventos com base na correspondência do padrão de nomes de eventos. Os conjuntos de comandos ONTAP (`event destination`, `event route`) que utilizam este modelo continuam a estar disponíveis nas versões mais recentes do ONTAP, mas foram obsoletos a partir do ONTAP 9.0.

A partir do ONTAP 9.0, a melhor prática para o mapeamento de destino de eventos do ONTAP EMS é usar o modelo de filtro de eventos mais dimensionável no qual a correspondência de padrões é feita em vários campos, usando os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Se o mapeamento EMS estiver configurado usando os comandos obsoletos, você deverá atualizar o mapeamento para usar os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Existem dois tipos de destinos de eventos:

1. **Destinos gerados pelo sistema**: Existem cinco destinos de eventos gerados pelo sistema (criados por padrão)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Alguns dos destinos gerados pelo sistema são para fins especiais. Por exemplo, o destino asup encaminha os eventos callhome.* para o módulo AutoSupport no ONTAP para gerar mensagens AutoSupport.
2. **Destinos criados pelo usuário**: Estes são criados manualmente usando o `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.
```

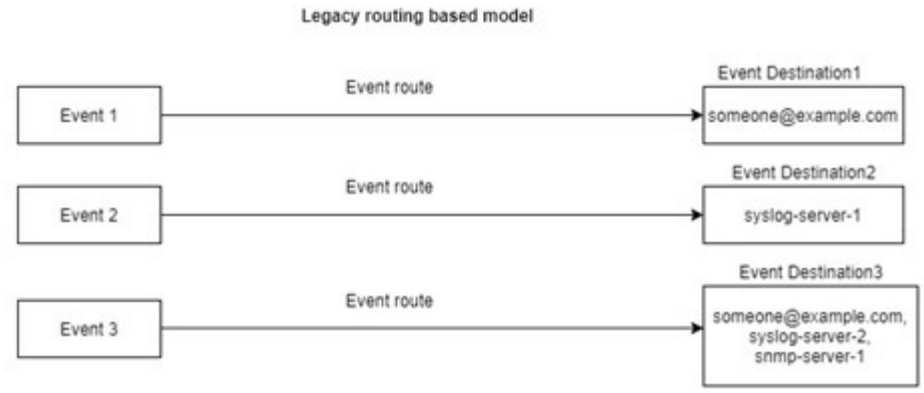
No modelo obsoleto, os eventos EMS são mapeados individualmente para um destino usando o `event route add-destinations` comando.

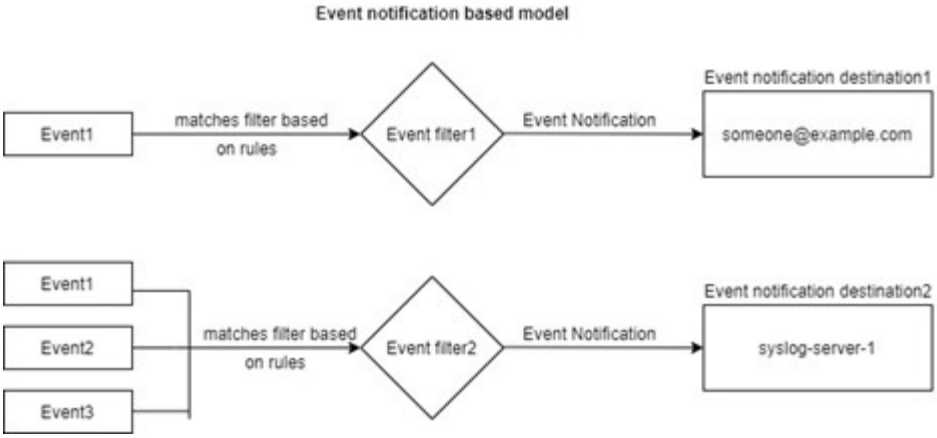
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

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.
```

O novo e mais escalável mecanismo de notificações de eventos EMS baseia-se em filtros de eventos e destinos de notificação de eventos. Consulte o seguinte artigo da KB para obter informações detalhadas sobre o novo mecanismo de notificação de eventos:

- "Visão geral do sistema de gerenciamento de eventos para ONTAP 9"





Atualize o mapeamento de eventos do EMS a partir de comandos ONTAP obsoletos

Se o mapeamento de eventos do EMS estiver configurado atualmente usando os conjuntos de comandos ONTAP obsoletos (`event destination`, `event route`), siga este procedimento para atualizar o mapeamento para usar os `event filter` conjuntos de comandos , `event notification` e `event notification destination` .

Passos

1. Liste todos os destinos de eventos no sistema usando o `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. Para cada destino, liste os eventos que estão sendo mapeados usando o `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. Crie um correspondente `event filter` que inclua todos esses subconjuntos de eventos. Por exemplo, se você quiser incluir apenas os `raid.aggr.`eventos *, use um caractere curinga para o `message-name` parâmetro ao criar o filtro. Você também pode criar filtros para eventos individuais.

Você pode criar até 50 filtros de eventos.

```
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. Criar um `event notification destination` para cada um `event destination` dos endpoints (ou seja, 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. Crie uma notificação de evento mapeando o filtro de evento para o destino de notificação de evento.

```
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. Repita as etapas 1-5 para cada `event destination` um que tenha um `event route` mapeamento.

Os eventos roteados para destinos SNMP devem ser mapeados para o `snmp-traphost` destino de notificação de eventos. O destino SNMP traphost usa o sistema SNMP traphost configurado.

```
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?: -
```

Informações sobre direitos autorais

Informações sobre marcas comerciais