



Configure as notificações de eventos EMS com a CLI

ONTAP 9

NetApp
January 17, 2025

Índice

- Configure as notificações de eventos EMS com a CLI 1
 - Fluxo de trabalho de configuração do EMS 1
 - Configurar eventos importantes do EMS para enviar notificações por e-mail 2
 - Configurando eventos importantes do EMS para encaminhar notificações para um servidor syslog 3
 - Configure os hosts SNMP para receber notificações de eventos 4
 - Configure eventos EMS importantes para encaminhar notificações para um aplicativo webhook 4

Configure as notificações de eventos EMS com a CLI

Fluxo de trabalho de configuração do EMS

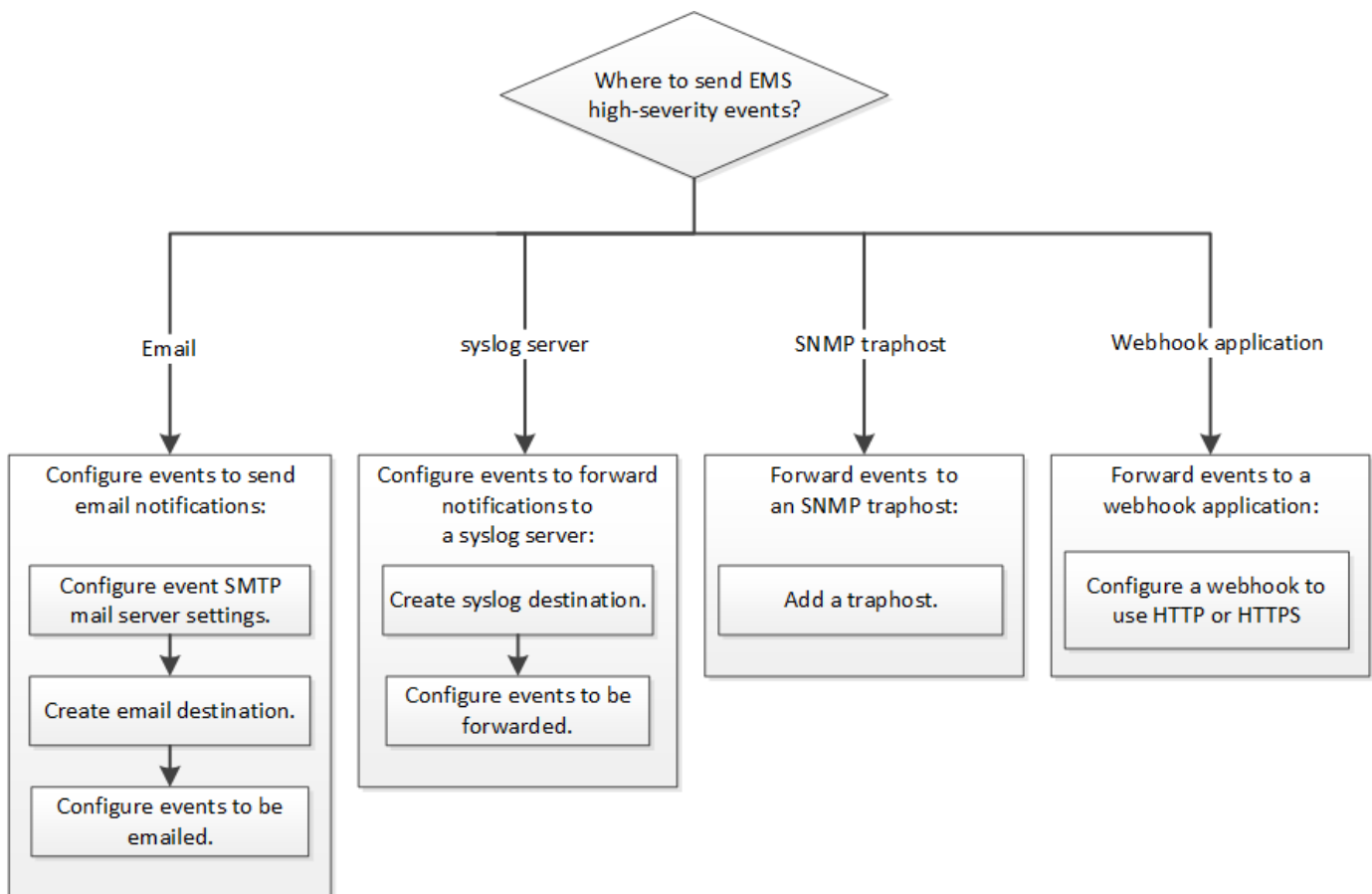
Você deve configurar notificações importantes de eventos EMS para serem enviadas como e-mail, encaminhadas para um servidor syslog, encaminhadas para um trapost SNMP ou encaminhadas para um aplicativo webhook. Isso ajuda você a evitar interrupções no sistema, tomando ações corretivas em tempo hábil.

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 trapost SNMP, talvez queira monitorar esse trapost 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 trapost 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 registrar 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 webhook. 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
```

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.