CLI로 EMS 이벤트 알림을 설정한다

ONTAP 9

NetApp
September 12, 2024

목차

CLI로 EMS 이벤트 알림을 설정한다

EMS 구성 작업 흐름

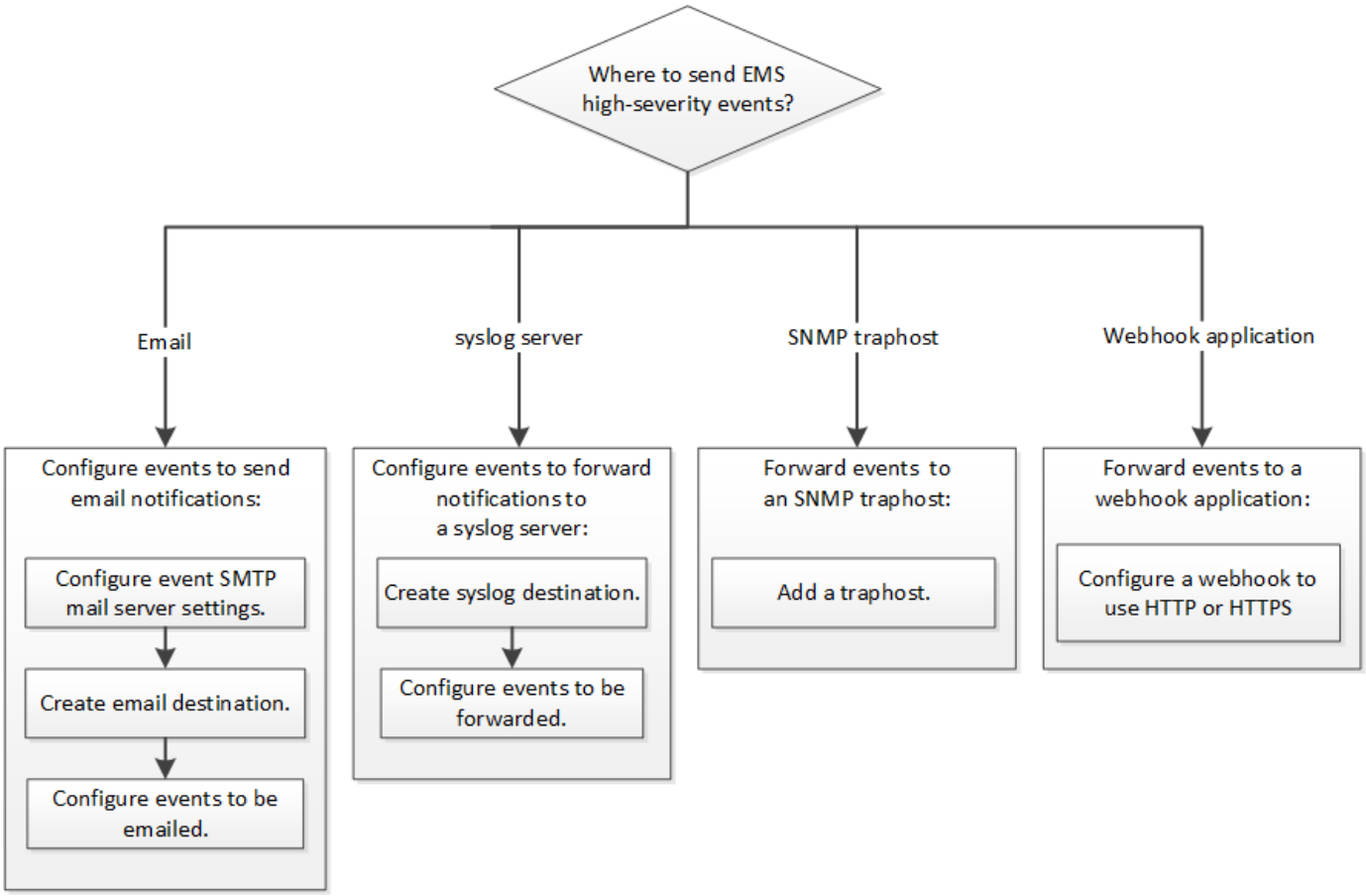
중요한 EMS 이벤트 알림을 e-메일로 보내거나, syslog 서버로 전달하거나, SNMP traphost로 전달하거나, webhook 애플리케이션으로 전달되도록 구성해야 합니다. 이를 통해 적시에 수정 조치를 취함으로써 시스템 중단을 방지할 수 있습니다.

이 작업에 대해

환경에 서버 및 애플리케이션과 같은 다른 시스템에서 기록된 이벤트를 집계하기 위한 syslog 서버가 이미 포함되어 있는 경우, 해당 syslog 서버를 사용하여 스토리지 시스템의 중요한 이벤트 알림도 쉽게 확인할 수 있습니다.

환경에 syslog 서버가 아직 포함되어 있지 않은 경우 중요한 이벤트 알림에 e-메일을 사용하는 것이 더 쉽습니다.

이벤트 알림을 SNMP traaphost에 이미 전달하는 경우 해당 traaphost에서 중요한 이벤트를 모니터링할 수 있습니다.



선택

- 이벤트 알림을 보내도록 EMS를 설정합니다.

원하는 작업	참조 항목…
EMS는 중요한 이벤트 알림을 이메일 주소로 전송합니다	e-메일 알림을 보내도록 중요한 EMS 이벤트를 구성합니다

중요한 이벤트 알림을 syslog 서버로 전달하는 EMS입니다	syslog 서버로 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다
EMS에서 이벤트 알림을 SNMP traaphost로 전달하도록 하려는 경우	이벤트 알림을 수신하도록 SNMP traaphosts를 구성합니다
EMS에서 이벤트 알림을 Webhook 애플리케이션으로 전달하려는 경우	Webhook 애플리케이션에 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다

e-메일 알림을 보내도록 중요한 EMS 이벤트를 구성합니다

가장 중요한 이벤트의 이메일 알림을 수신하려면 중요한 활동을 나타내는 이벤트에 대한 이메일 메시지를 보내도록 EMS를 구성해야 합니다.

필요한 것

클러스터에서 DNS를 구성하여 이메일 주소를 확인해야 합니다.

이 작업에 대해

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 이벤트 SMTP 메일 서버 설정을 구성합니다.

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

2. 이벤트 알림을 위한 e-메일 대상 생성:

   '이벤트 알림 대상 create-name storage-admins-email@your_domain'으로 이메일을 보냅니다

3. e-메일 알림을 보내도록 중요한 이벤트를 구성합니다.

   이벤트 알림 create-filter-name important-events-destinations storage-admins입니다

syslog 서버로 알림을 전달하도록 중요한 EMS 이벤트 구성

syslog 서버에서 가장 심각한 이벤트의 알림을 기록하려면 중요한 활동을 나타내는 이벤트에 대한 알림을 전달하도록 EMS를 구성해야 합니다.

필요한 것

syslog 서버 이름을 확인하기 위해 클러스터에 DNS를 구성해야 합니다.

이 작업에 대해

환경에 이벤트 알림에 대한 syslog 서버가 아직 포함되어 있지 않은 경우 먼저 syslog 서버를 생성해야 합니다. 사용자 환경에 다른 시스템의 이벤트를 로깅하기 위한 syslog 서버가 이미 포함되어 있는 경우 중요한 이벤트 알림에 이 서버를 사용할 수 있습니다.

ONTAP CLI에서 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

ONTAP 9.12.1부터 EMS 이벤트는 TLS(Transport Layer Security) 프로토콜을 통해 원격 syslog 서버의 지정된 포트로 전송될 수 있습니다. 두 가지 새로운 매개 변수를 사용할 수 있습니다.

`tcp-encrypted`

시기 `tcp-encrypted` 에 대해 지정됩니다 `syslog-transport`, ONTAP 는 해당 인증서를 검증하여 대상 호스트의 ID를 확인합니다. 기본값은 입니다 `udp-unencrypted`.

`syslog-port`

기본값입니다 `syslog-port` 매개 변수는 의 설정에 따라 다릅니다 `syslog-transport` 매개 변수. If(경우 `syslog-transport` 가 로 설정되어 있습니다 `tcp-encrypted`, `syslog-port` 기본값은 6514입니다.

자세한 내용은 를 참조하십시오 `event notification destination create` Man 페이지.

단계

1. 중요한 이벤트에 대한 syslog 서버 대상을 생성합니다.

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

   ONTAP 9.12.1부터 에 대해 다음 값을 지정할 수 있습니다 `syslog-transport`:

   - `udp-unencrypted` 보안 기능이 없는 사용자 데이터그램 프로토콜
   - `tcp-unencrypted` 보안 기능이 없는 전송 제어 프로토콜
   - `tcp-encrypted` 전송 계층 보안(TLS)이 있는 전송 제어 프로토콜

   기본 프로토콜은 입니다 `udp-unencrypted`.

2. syslog 서버로 알림을 전달할 중요 이벤트를 구성합니다.

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

이벤트 알림을 수신하도록 **SNMP traaphosts**를 구성합니다

SNMP traaphost에서 이벤트 알림을 수신하려면 traphost를 구성해야 합니다.

필요한 것

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

  SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.

이 작업에 대해

이벤트 알림(SNMP 트랩)을 받도록 구성된 SNMP 트랩 호스트가 아직 없는 경우 이를 추가해야 합니다.

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 환경에 이벤트 알림을 수신하도록 구성된 SNMP traaphost가 아직 없는 경우 다음 중 하나를 추가하십시오.

   'System snmp traphost add-peer-address_snmp_traphost_name_'

   기본적으로 SNMP에서 지원하는 모든 이벤트 알림은 SNMP traphost로 전달됩니다.

Webhook 애플리케이션에 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다

중요한 이벤트 알림을 Webhook 애플리케이션에 전달하도록 ONTAP를 구성할 수 있습니다. 필요한 구성 단계는 선택한 보안 수준에 따라 다릅니다.

EMS 이벤트 전달을 구성할 준비를 합니다

이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성하기 전에 고려해야 할 몇 가지 개념과 요구 사항이 있습니다.

Webhook 응용 프로그램

ONTAP 이벤트 알림을 받을 수 있는 웹 후크 응용 프로그램이 필요합니다. Webhook은 사용자가 정의한 콜백 루틴으로, 이 루틴이 실행되는 원격 응용 프로그램 또는 서버의 기능을 확장합니다. Webhook는 대상 URL로 HTTP 요청을 전송하여 클라이언트(이 경우 ONTAP)에 의해 호출되거나 활성화됩니다. 특히 ONTAP는 웹 후크 응용 프로그램을 호스팅하는 서버에 HTTP POST 요청을 보내고 XML로 포맷된 이벤트 알림 세부 정보를 보냅니다.

보안 옵션

TLS(Transport Layer Security) 프로토콜을 사용하는 방법에 따라 몇 가지 보안 옵션을 사용할 수 있습니다. 선택한 옵션에 따라 필요한 ONTAP 구성이 결정됩니다.

> TLS는 인터넷에서 널리 사용되는 암호화 프로토콜입니다. 하나 이상의 공개 키 인증서를 사용하여 개인 정보 보호와 데이터 무결성 및 인증을 제공합니다. 인증서는 신뢰할 수 있는 인증 기관에서 발급합니다.

HTTP

HTTP를 사용하여 이벤트 알림을 전송할 수 있습니다. 이 구성에서는 연결이 안전하지 않습니다. ONTAP 클라이언트 및 웹 후크 응용 프로그램의 ID가 확인되지 않습니다. 또한 네트워크 트래픽은 암호화되거나 보호되지 않습니다. 을 참조하십시오 "HTTP를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

HTTPS

추가 보안을 위해 Webhook 루틴을 호스팅하는 서버에 인증서를 설치할 수 있습니다. ONTAP는 HTTPS 프로토콜을 사용하여 웹 후크 응용 프로그램 서버의 ID와 네트워크 트래픽의 개인 정보 보호와 무결성을 보장합니다. 을 참조하십시오 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

상호 인증을 사용하는 **HTTPS**

웹북 요청을 실행하는 ONTAP 시스템에 클라이언트 인증서를 설치하여 HTTPS 보안을 강화할 수 있습니다. webhook 응용 프로그램 서버의 ID를 확인하고 네트워크 트래픽을 보호하는 ONTAP 외에도 webhook 응용 프로그램은 ONTAP 클라이언트의 ID를 확인합니다. 이 양방향 피어 인증을 _Mutual TLS_라고 합니다. 을

참조하십시오 "상호 인증과 함께 HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

관련 정보

- "TLS(Transport Layer Security) 프로토콜 버전 1.3"

HTTP를 사용하도록 웹 후크 대상을 구성합니다

HTTP를 사용하여 웹 후크 응용 프로그램에 이벤트 알림을 전달하도록 ONTAP를 구성할 수 있습니다. 이 옵션은 가장 안전하지는 않지만 가장 간단한 설치 방법입니다.

단계

1. 이벤트를 수신할 새 대상 'restapi-EMS'를 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\http://<webhook-application>`

   위 명령에서 대상에 대해 * HTTP * 체계를 사용해야 합니다.

2. 중요 이벤트 필터를 "restapi-EMS" 대상으로 연결하는 알림 생성:

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

HTTPS를 사용하도록 웹 후크 대상을 구성합니다

HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성할 수 있습니다. ONTAP는 서버 인증서를 사용하여 웹 후크 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다.

시작하기 전에

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다

단계

1. 웹 후크 응용 프로그램을 호스팅하는 서버에 적절한 서버 개인 키와 인증서를 설치합니다. 특정 구성 단계는 서버에 따라 다릅니다.
2. ONTAP에 서버 루트 인증서 설치:

   보안 인증서설치형 server-ca

   명령이 인증서를 요청합니다.

3. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\https://<webhook-application>`

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

4. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

상호 인증과 함께 **HTTPS**를 사용하도록 웹 후크 대상을 구성합니다

상호 인증을 사용하여 HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램에 전달하도록 ONTAP를 구성할 수 있습니다. 이 구성에는 두 개의 인증서가 있습니다. ONTAP는 서버 인증서를 사용하여 webhook 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다. 또한 webhook를 호스팅하는 응용 프로그램은 클라이언트 인증서를 사용하여 ONTAP 클라이언트의 ID를 확인합니다.

시작하기 전에

ONTAP를 구성하기 전에 다음을 수행해야 합니다.

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다
- ONTAP 클라이언트에 대한 개인 키와 인증서를 생성합니다

단계

1. 작업의 처음 두 단계를 수행합니다 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" ONTAP가 서버의 ID를 확인할 수 있도록 서버 인증서를 설치합니다.
2. 웹 후크 응용 프로그램에 적절한 루트 및 중간 인증서를 설치하여 클라이언트 인증서를 확인합니다.
3. ONTAP에 클라이언트 인증서 설치:

   보안 인증서 설치형 클라이언트

   명령에서 개인 키와 인증서를 요청합니다.

4. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   '이벤트 알림 대상 create-name restapi-EMS-REST-API-URL\https://<webhook-application> - certificate-authority <클라이언트 인증서 발급자> - certificate-serial <클라이언트 인증서 직렬>'

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

5. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS