Configurez les notifications d'événements EMS avec l'interface de ligne de commande

ONTAP 9

NetApp
September 12, 2024

Sommaire

Configurez les notifications d'événements EMS avec l'interface de ligne de commande

Flux de travail de configuration EMS

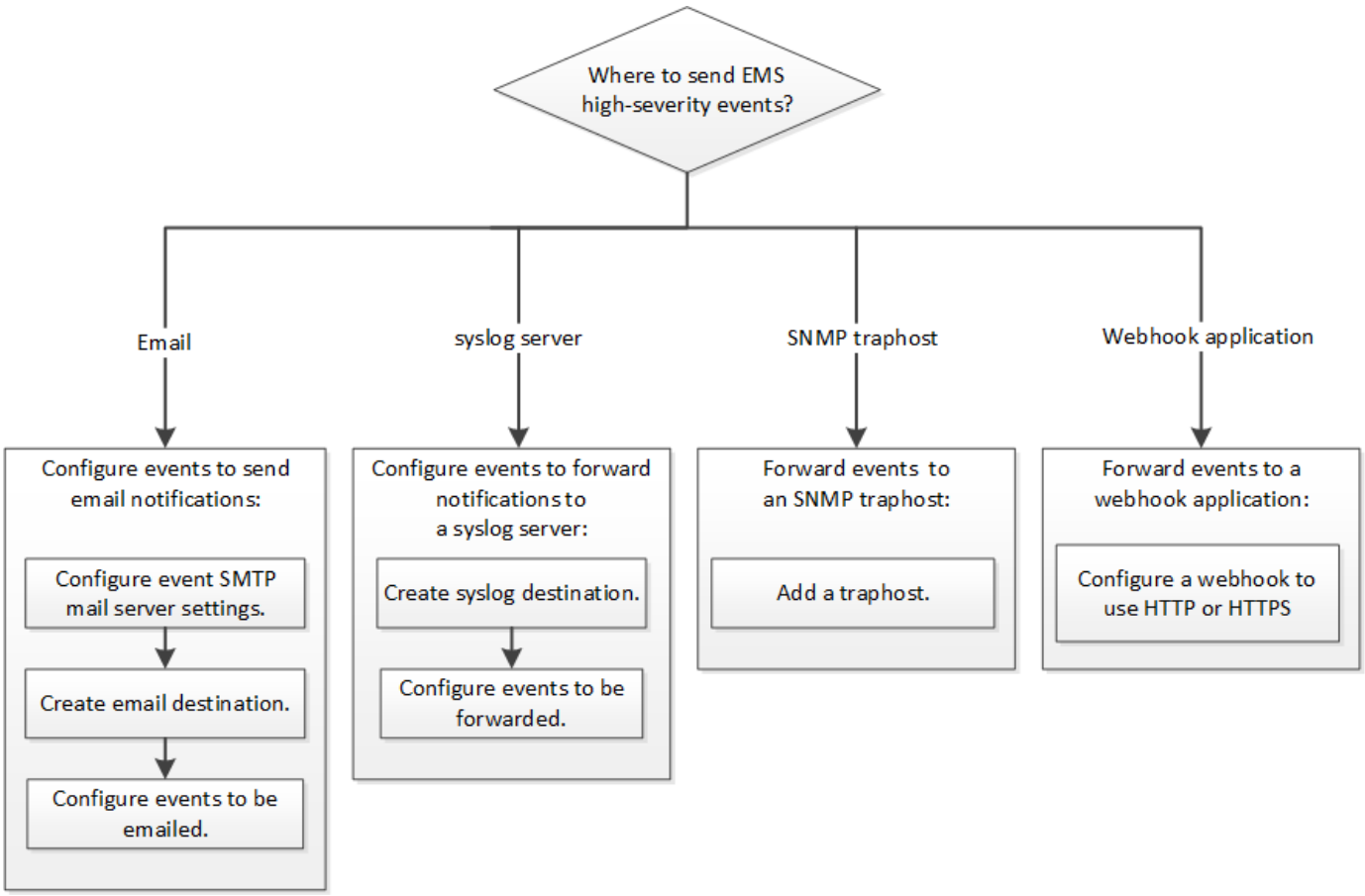
Vous devez configurer les notifications d'événements EMS importantes pour qu'elles soient envoyées par e-mail, envoyées à un serveur syslog, transférées à un hôte de transfert SNMP ou transmises à une application de connexion Web. Cela vous permet d'éviter toute interruption du système en prenant des actions correctives en temps opportun.

Description de la tâche

Si votre environnement contient déjà un serveur syslog permettant d'agréger les événements journaux d'autres systèmes, tels que des serveurs et des applications, il est plus facile d'utiliser ce serveur syslog également pour recevoir des notifications d'événements importantes provenant des systèmes de stockage.

Si votre environnement ne contient pas encore de serveur syslog, il est plus facile d'utiliser le courrier électronique pour les notifications d'événements importantes.

Si vous transférez déjà des notifications d'événement à un Traphost SNMP, il se peut que vous souhaitiez surveiller ce Traphost pour les événements importants.



Choix

- Configurez EMS pour envoyer des notifications d'événement.

Les fonctions que vous recherchez…	Reportez-vous à ceci…
L'EMS doit envoyer des notifications d'événements importantes à une adresse e-mail	Configurez les événements EMS importants pour envoyer des notifications par e-mail
L'EMS doit transmettre des notifications d'événements importantes à un serveur syslog	Configurez les événements EMS importants pour transférer des notifications à un serveur syslog
Si vous souhaitez que l'EMS envoie des notifications d'événement à un Traphost SNMP	Configurez les Traphosts SNMP pour recevoir des notifications d'événement
Si vous souhaitez que l'EMS envoie des notifications d'événement à une application de connexion Web	Configurez les événements EMS importants pour transférer les notifications vers une application webhook

Configurez les événements EMS importants pour envoyer des notifications par e-mail

Pour recevoir des notifications par e-mail des événements les plus importants, vous devez configurer l'EMS pour qu'il envoie des e-mails pour les événements qui signalent une activité importante.

Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre les adresses e-mail.

Description de la tâche

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

Étapes

1. Configurez les paramètres du serveur de messagerie SMTP d'événement :

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

2. Créer une destination e-mail pour les notifications d'événements :

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

3. Configurez les événements importants pour envoyer des notifications par e-mail :

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

Configuration des événements EMS importants pour transférer des notifications à un serveur syslog

Pour enregistrer les notifications des événements les plus graves sur un serveur syslog, vous devez configurer l'EMS pour transférer les notifications des événements qui signalent une activité importante.

Ce dont vous avez besoin

Le DNS doit être configuré sur le cluster pour résoudre le nom du serveur syslog.

Description de la tâche

Si votre environnement ne contient pas encore de serveur syslog pour les notifications d'événements, vous devez d'abord en créer un. Si votre environnement contient déjà un serveur syslog pour la journalisation des événements à partir d'autres systèmes, vous pouvez l'utiliser pour les notifications d'événements importantes.

Vous pouvez effectuer cette tâche à n'importe quel moment du cluster en entrant les commandes sur l'interface de ligne de commandes de ONTAP.

Depuis ONTAP 9.12.1, les événements EMS peuvent être envoyés vers un port désigné sur un serveur syslog distant via le protocole TLS (transport Layer Security). Deux nouveaux paramètres sont disponibles :

`tcp-encrypted`

Quand `tcp-encrypted` est spécifié pour le `syslog-transport`, ONTAP vérifie l'identité de l'hôte de destination en validant son certificat. La valeur par défaut est `udp-unencrypted`.

`syslog-port`

La valeur par défaut `syslog-port` le paramètre dépend du réglage de l' `syslog-transport` paramètre. Si `syslog-transport` est défini sur `tcp-encrypted`, `syslog-port` a la valeur par défaut 6514.

Pour plus d'informations, reportez-vous à la `event notification destination create` page de manuel.

Étapes

1. Créer une destination de serveur syslog pour les événements importants :

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

   À partir de ONTAP 9.12.1, les valeurs suivantes peuvent être spécifiées pour `syslog-transport`:

   - `udp-unencrypted` - Protocole de datagramme utilisateur sans sécurité
   - `tcp-unencrypted` - Protocole de contrôle de transmission sans sécurité
   - `tcp-encrypted` - Protocole de contrôle de transmission avec TLS (transport Layer Security)

   Le protocole par défaut est `udp-unencrypted`.

2. Configurez les événements importants pour transférer des notifications au serveur syslog :

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

Configurez les Traphosts SNMP pour recevoir des notifications d'événement

Pour recevoir des notifications d'événements sur un Traphost SNMP, vous devez configurer un Traphost.

Ce dont vous avez besoin

- Les traps SNMP doivent être activés sur le cluster.

  Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour résoudre les noms de Traphost.

Description de la tâche

Si aucun Traphost SNMP n'est déjà configuré pour recevoir des notifications d'événements (traps SNMP), vous devez en ajouter un.

Vous pouvez effectuer cette tâche à tout moment du cluster en entrant les commandes sur la ligne de commande ONTAP.

Étape

1. Si votre environnement ne dispose pas déjà d'un Traphost SNMP configuré pour recevoir des notifications d'événement, ajoutez-en un :

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

   Toutes les notifications d'événements prises en charge par SNMP par défaut sont transmises au Traphost SNMP.

Configurez les événements EMS importants pour transférer les notifications vers une application webhook

Vous pouvez configurer ONTAP pour transférer des notifications d'événements importantes vers une application de connexion Web. Les étapes de configuration nécessaires dépendent du niveau de sécurité que vous choisissez.

Préparez-vous à configurer le transfert d'événements EMS

Vous devez tenir compte de plusieurs concepts et exigences avant de configurer ONTAP pour transférer les notifications d'événements vers une application webhook.

Application Webhook

Vous avez besoin d'une application webhook capable de recevoir les notifications d'événements ONTAP. Un webhook est une routine de rappel définie par l'utilisateur qui étend la capacité de l'application ou du serveur distant où il s'exécute. Les patères sont appelés ou activés par le client (dans ce cas ONTAP) en envoyant une requête HTTP à l'URL de destination. Plus précisément, ONTAP envoie une requête HTTP POST au serveur hébergeant l'application webhook avec les détails de notification d'événement formatés en XML.

Options de sécurité

Plusieurs options de sécurité sont disponibles en fonction de l'utilisation du protocole TLS (transport Layer Security). L'option choisie détermine la configuration ONTAP requise.

> TLS est un protocole cryptographique largement utilisé sur Internet. Il assure la confidentialité ainsi que l'intégrité et l'authentification des données à l'aide d'un ou de plusieurs certificats de clé publique. Les certificats sont émis par les autorités de certification de confiance.

HTTP

Vous pouvez utiliser HTTP pour transporter les notifications d'événement. Avec cette configuration, la connexion n'est pas sécurisée. Les identités du client ONTAP et de l'application webhook ne sont pas vérifiées. En outre, le trafic réseau n'est pas chiffré ni protégé. Voir "Configurez une destination de connexion Web pour utiliser HTTP" pour en savoir plus sur la configuration.

HTTPS

Pour plus de sécurité, vous pouvez installer un certificat sur le serveur hébergeant la routine webhook. Le protocole HTTPS est utilisé par ONTAP pour vérifier l'identité du serveur d'application webhook ainsi que par les deux parties pour assurer la confidentialité et l'intégrité du trafic réseau. Voir "Configurez une destination Webhook pour utiliser HTTPS" pour en savoir plus sur la configuration.

HTTPS avec authentification mutuelle

Vous pouvez améliorer encore la sécurité HTTPS en installant un certificat client sur le système ONTAP émettant les requêtes webbook. En plus de la vérification par ONTAP de l'identité du serveur d'applications webhook et de la protection du trafic réseau, l'application webhook vérifie l'identité du client ONTAP. Cette authentification bidirectionnelle par poste est appelée *Mutual TLS*. Voir "Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle" pour en savoir plus sur la configuration.

Informations associées

- "Protocole TLS (transport Layer Security) version 1.3"

Configurez une destination de connexion Web pour utiliser HTTP

Vous pouvez configurer ONTAP pour transférer des notifications d'événements vers une application de webhook à l'aide de HTTP. Il s'agit de l'option la moins sécurisée, mais la plus simple à configurer.

Étapes

1. Créer une nouvelle destination `restapi-ems` pour recevoir les événements :

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

   Dans la commande ci-dessus, vous devez utiliser le schéma **HTTP** pour la destination.

2. Créez une notification reliant le `important-events` filtrer avec le `restapi-ems` destination :

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

Configurez une destination Webhook pour utiliser HTTPS

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application de connexion Internet à l'aide de HTTPS. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau.

Avant de commencer

- Générez une clé privée et un certificat pour le serveur d'applications webhook
- Disponibilité du certificat racine pour l'installation dans ONTAP

Étapes

1. Installez la clé privée du serveur et les certificats appropriés sur le serveur hébergeant votre application webhook. Les étapes de configuration spécifiques dépendent du serveur.
2. Installez le certificat racine du serveur dans ONTAP :

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

   La commande demande le certificat.

3. Créer le `restapi-ems` destination pour recevoir les événements :

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

   Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

4. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

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

Configurez une destination de connexion Web pour utiliser HTTPS avec authentification mutuelle

Vous pouvez configurer ONTAP pour transférer les notifications d'événements vers une application webhook en utilisant HTTPS avec authentification mutuelle. Avec cette configuration, il y a deux certificats. ONTAP utilise le certificat de serveur pour confirmer l'identité de l'application webhook et sécuriser le trafic réseau. De plus, l'application hébergeant le webhook utilise le certificat client pour confirmer l'identité du client ONTAP.

Avant de commencer

Vous devez effectuer les opérations suivantes avant de configurer ONTAP :

- Générez une clé privée et un certificat pour le serveur d'applications webhook
- Disponibilité du certificat racine pour l'installation dans ONTAP
- Générez une clé privée et un certificat pour le client ONTAP

Étapes

1. Effectuez les deux premières étapes de la tâche "Configurez une destination Webhook pour utiliser HTTPS" Pour installer le certificat de serveur afin que ONTAP puisse vérifier l'identité du serveur.
2. Installez les certificats racine et intermédiaire appropriés sur l'application webhook pour valider le certificat

client.

3. Installez le certificat client dans ONTAP :

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

   La commande demande la clé privée et le certificat.

4. Créer le `restapi-ems` destination pour recevoir les événements :

   ```
   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>
   ```

   Dans la commande ci-dessus, vous devez utiliser le schéma **HTTPS** pour la destination.

5. Créez la notification qui lie le `important-events` filtrer avec le nouveau `restapi-ems` destination :

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