EMS-Konfiguration

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

EMS-Konfiguration

EMS-Konfigurationsübersicht

Sie können ONTAP 9 schnell konfigurieren, um wichtige EMS-Ereignisbenachrichtigungen (Event Management System) direkt an eine E-Mail-Adresse, einen Syslog-Server, ein Simple Management Network Protocol (SNMP) traphost oder EINEN REST-API-Server zu senden, sodass Sie sofort über Systemprobleme informiert werden, bei denen eine sofortige Aufmerksamkeit erforderlich ist.

Um die wichtigsten Aktivitäten in Ihrem System zu überwachen, müssen Sie die wichtigen EMS-Ereignisse überwachen.

Da wichtige Ereignisbenachrichtigungen standardmäßig nicht aktiviert sind, müssen Sie das EMS so konfigurieren, dass Benachrichtigungen entweder an eine E-Mail-Adresse, einen Syslog-Server, einen SNMP traphost oder REST API-Server gesendet werden.

Konfigurieren Sie EMS-Ereignisbenachrichtigungen für wichtige Ereignisse, wenn Folgendes zutrifft:

- Sie implementieren eines der folgenden Szenarien:
  - Sie einrichten ein neues System mit ONTAP 9, das nicht über EMS konfiguriert ist.
  - Sie haben ein System, auf dem ONTAP 9 ausgeführt wird und das über kein EMS konfiguriert ist.
  - Sie aktualisieren gerade auf ONTAP 9, das nicht über EMS konfiguriert ist.
  - Sie haben gerade den Übergang von Data ONTAP im 7-Mode zu ONTAP 9 abgeschlossen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.

Den EMS-Veranstaltungskatalog finden Sie unter Weitere Ressourcen auf dieser Seite: "ONTAP 9 Produktbibliothek". Siehe Konvertieren Sie das Routing für ältere Ereignisse in Ereignisbenachrichtigungen Weitere Informationen zur Durchführung der Benachrichtigungsbasierten Modellkonvertierung. Sie können auch auf die verweisen "EMS-Referenz".

Konfigurieren Sie EMS-Ereignisbenachrichtigungen und -Filter mit System Manager

Mit System Manager können Sie konfigurieren, wie das Event Management System (EMS) Ereignisbenachrichtigungen bereitstellt, sodass Sie über Systemprobleme informiert werden können, bei denen Ihre Eingabeaufforderung angezeigt wird.

ONTAP-Version	Die Vorzüge von System Manager:
ONTAP 9.12.1 und höher	Geben Sie das TLS-Protokoll (Transport Layer Security) an, wenn Ereignisse an Remote-Syslog-Server gesendet werden.
ONTAP 9.10.1 und höher	Konfigurieren Sie E-Mail-Adressen, Syslog-Server und Webhook-Anwendungen sowie SNMP-Traphosts.

ONTAP 9.7 auf 9.10.0	Konfigurieren Sie nur SNMP-Trap-Hosts. Sie können ein anderes EMS-Ziel mit der ONTAP CLI konfigurieren. Siehe "EMS-Konfigurationsübersicht".

Sie können folgende Aktionen durchführen:

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

Verwandte Informationen

- "EMS-Ereigniskatalog"
- "Mit der CLI können Sie SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren"

Fügen Sie ein EMS-Ereignisbenachrichtigungs-Ziel hinzu

Sie können mit System Manager angeben, an welche Empfänger von EMS-Nachrichten gesendet werden sollen.

Ab ONTAP 9.12.1 können EMS-Ereignisse über das TLS-Protokoll (Transport Layer Security) an einen bestimmten Port auf einem Remote-Syslog-Server gesendet werden. Weitere Informationen finden Sie im `event notification destination create` Man-Page.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮ Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie Auf + Add .
5. Geben Sie einen Namen, einen EMS-Zieltyp und Filter an.

   ⓘ Bei Bedarf können Sie einen neuen Filter hinzufügen. Klicken Sie auf **Neuen Ereignisfilter hinzufügen**.

6. Geben Sie je nach gewähltem EMS-Zieltyp Folgendes an:

So konfigurieren Sie…	… angeben oder auswählen
SNMP traphost	• TrapHost-Name

E-Mail (Ab 9.10.1)	• E-Mail-Adresse des Zielorts • Mailserver • Von E-Mail-Adresse
Syslog-Server (Ab 9.10.1)	• Hostname oder IP-Adresse des Servers • Syslog-Port (beginnend mit 9.12.1) • Syslog-Transport (ab 9.12.1) Durch die Auswahl von **TCP Encrypted** wird das TLS-Protokoll (Transport Layer Security) aktiviert. Wenn für **Syslog-Port** kein Wert eingegeben wird, wird ein Standard basierend auf der Auswahl **Syslog Transport** verwendet.
Webhook (Ab 9.10.1)	• Webhook-URL • Clientauthentifizierung (wählen Sie diese Option, um ein Clientzertifikat anzugeben)

Erstellen Sie einen neuen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager neue benutzerdefinierte Filter definieren, die die Regeln für den Umgang mit EMS-Benachrichtigungen festlegen.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie Auf + Add .
5. Geben Sie einen Namen an, und wählen Sie aus, ob Regeln aus einem vorhandenen Ereignisfilter kopiert oder neue Regeln hinzugefügt werden sollen.
6. Führen Sie je nach Ihrer Wahl die folgenden Schritte aus:

Wenn Sie… auswählen.	Führen Sie dann diese Schritte… aus
Regeln aus vorhandenem Ereignisfilter kopieren	1. Wählen Sie einen vorhandenen Ereignisfilter aus. 2. Ändern Sie die vorhandenen Regeln. 3. Fügen Sie bei Bedarf weitere Regeln hinzu, indem Sie auf klicken + Add .
Neue Regeln hinzufügen	Geben Sie für jede neue Regel Typ, Namensmuster, Schweregrade und SNMP-Trap-Typ an.

Bearbeiten Sie ein EMS-Ereignisbenachrichtigungs-Ziel

Ab ONTAP 9.10.1 können Sie mit System Manager die Zielinformationen für die Ereignisbenachrichtigung ändern.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf ⋮Klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie die Informationen zum Event-Ziel und klicken Sie dann auf **Speichern**.

Bearbeiten Sie einen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager benutzerdefinierte Filter ändern, um die Handhabung von Ereignisbenachrichtigungen zu ändern.

ⓘ Sie können keine systemdefinierten Filter ändern.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf ⋮Klicken Sie dann auf **Bearbeiten**.
5. Ändern Sie die Informationen zum Ereignisfilter und klicken Sie dann auf **Speichern**.

Löschen Sie ein EMS-Ereignisbenachrichtigungs-Ziel

Ab ONTAP 9.10.1 können Sie mit System Manager ein EMS-Ereignisbenachrichtigungs-Ziel löschen.

ⓘ SNMP-Ziele können nicht gelöscht werden.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf ⋮Klicken Sie dann auf **Löschen**.

Löschen Sie einen EMS-Ereignisbenachrichtigungs-Filter

Ab ONTAP 9.10.1 können Sie mit System Manager benutzerdefinierte Filter löschen.

ⓘ Sie können keine systemdefinierten Filter löschen.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf ⋮ Klicken Sie dann auf **Veranstaltungsziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf ⋮ Klicken Sie dann auf **Löschen**.

Konfigurieren Sie EMS-Ereignisbenachrichtigungen mit der CLI

EMS-Konfigurationsworkflow

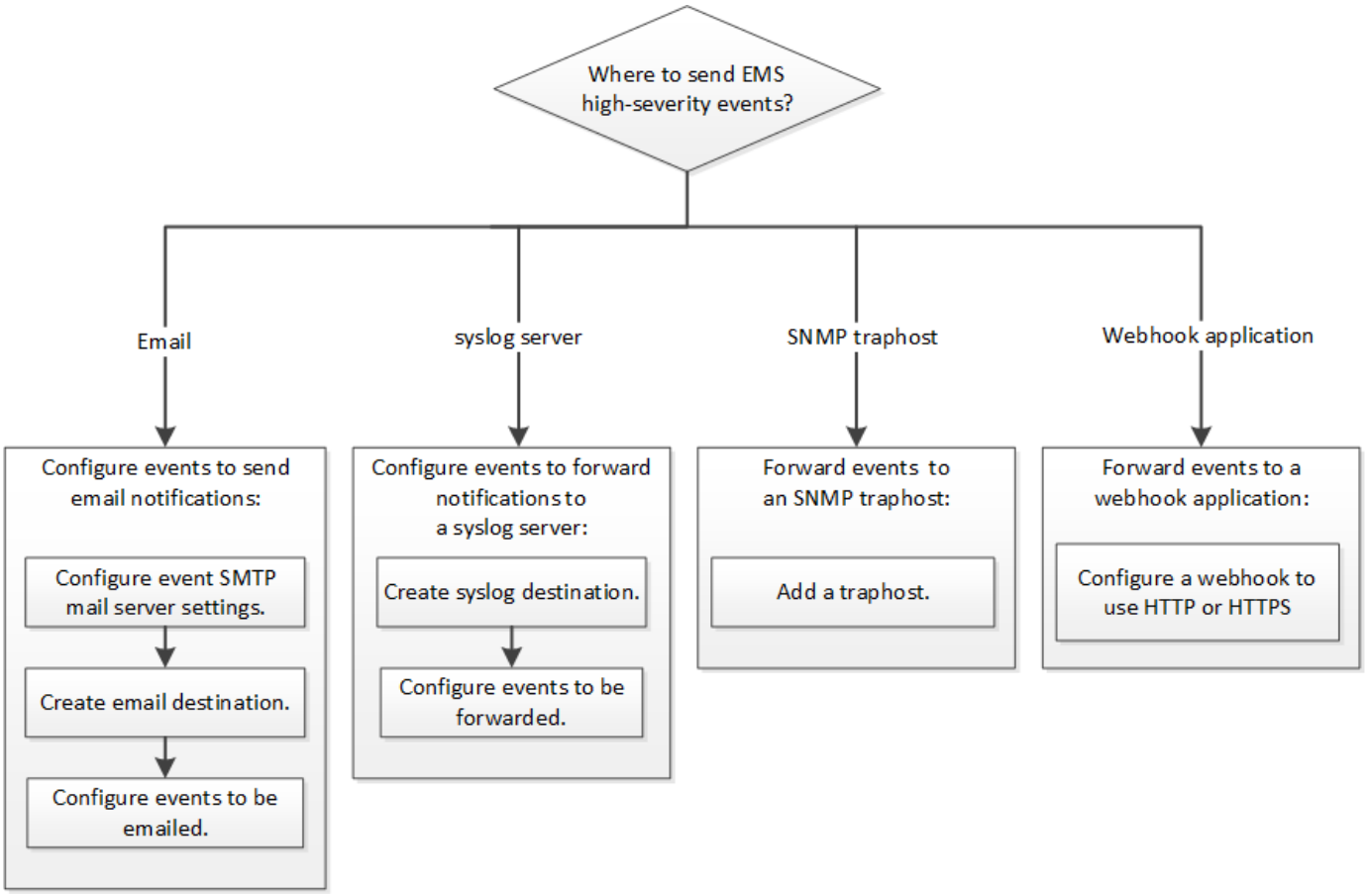
Sie müssen wichtige EMS-Ereignisbenachrichtigungen so konfigurieren, dass sie entweder als E-Mail gesendet, an einen Syslog-Server weitergeleitet, an einen SNMP traphost weitergeleitet oder an eine Webhook-Anwendung weitergeleitet werden. Auf diese Weise können Sie Systemstörungen vermeiden, indem Sie Korrekturmaßnahmen rechtzeitig ergreifen.

Über diese Aufgabe

Wenn in Ihrer Umgebung bereits ein Syslog-Server zur Aggregation der protokollierten Ereignisse von anderen Systemen, wie z. B. Servern und Anwendungen, vorhanden ist, ist es einfacher, diesen Syslog-Server auch für wichtige Ereignisbenachrichtigungen von Speichersystemen zu verwenden.

Wenn in Ihrer Umgebung noch kein Syslog-Server vorhanden ist, ist es einfacher, E-Mails für wichtige Ereignisbenachrichtigungen zu verwenden.

Wenn Sie Ereignisbenachrichtigungen bereits an einen SNMP traphost weiterleiten, können Sie diesen traphost bei wichtigen Ereignissen überwachen.



Wahlmöglichkeiten

- Setzen Sie EMS ein, um Ereignisbenachrichtigungen zu senden.

Ihre Situation	Lesen Sie dazu…
Das EMS sendet wichtige Ereignisbenachrichtigungen an eine E-Mail-Adresse	Konfigurieren Sie wichtige EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen
Das EMS sendet wichtige Ereignisbenachrichtigungen an einen Syslog-Server	Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an einen Syslog-Server weiterzuleiten
Wenn Sie möchten, dass der EMS Ereignisbenachrichtigungen an einen SNMP traphost weitergibt	Konfigurieren Sie SNMP-Trap-Hosts für den Empfang von Ereignisbenachrichtigungen
Wenn Sie möchten, dass das EMS Ereignisbenachrichtigungen an eine Webhook-Anwendung weitergibt	Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an eine Webhook-Anwendung weiterzuleiten

Konfigurieren Sie wichtige EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen

Um E-Mail-Benachrichtigungen über die wichtigsten Ereignisse zu erhalten, müssen Sie

das EMS so konfigurieren, dass E-Mail-Nachrichten für Ereignisse gesendet werden, die wichtige Aktivitäten signalisieren.

Was Sie benötigen

DNS muss auf dem Cluster konfiguriert sein, um die E-Mail-Adressen zu lösen.

Über diese Aufgabe

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in die ONTAP-Befehlszeile eingeben.

Schritte

1. Konfigurieren Sie die Einstellungen des SMTP-E-Mail-Servers für den Event:

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

2. E-Mail-Ziel für Ereignisbenachrichtigungen erstellen:

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

3. Konfigurieren Sie die wichtigen Ereignisse zum Senden von E-Mail-Benachrichtigungen:

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

Konfigurieren wichtiger EMS-Ereignisse zur Weiterleitung von Benachrichtigungen an einen Syslog-Server

Um Benachrichtigungen über die schwersten Ereignisse auf einem Syslog-Server zu protokollieren, müssen Sie das EMS so konfigurieren, dass Benachrichtigungen für Ereignisse, die wichtige Aktivitäten signalisieren, weitergesendet werden.

Was Sie benötigen

DNS muss auf dem Cluster konfiguriert werden, um den syslog-Servernamen aufzulösen.

Über diese Aufgabe

Wenn in Ihrer Umgebung kein Syslog-Server für Ereignisbenachrichtigungen vorhanden ist, müssen Sie zuerst einen erstellen. Falls Ihre Umgebung bereits einen Syslog-Server zum Protokollieren von Ereignissen aus anderen Systemen enthält, sollten Sie diesen Server möglicherweise für wichtige Ereignisbenachrichtigungen verwenden.

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in der ONTAP-CLI eingeben.

Ab ONTAP 9.12.1 können EMS-Ereignisse über das TLS-Protokoll (Transport Layer Security) an einen bestimmten Port auf einem Remote-Syslog-Server gesendet werden. Es sind zwei neue Parameter verfügbar:

`tcp-encrypted`

Wenn `tcp-encrypted` Wird für das angegeben `syslog-transport`, ONTAP überprüft die Identität des Ziel-Host durch die Validierung seines Zertifikats. Der Standardwert ist `udp-unencrypted`.

`syslog-port`

Der Standardwert `syslog-port` Parameter hängt von der Einstellung für das ab `syslog-transport` Parameter. Wenn `syslog-transport` Ist auf festgelegt `tcp-encrypted`, `syslog-port` Hat den Standardwert 6514.

Weitere Informationen finden Sie im `event notification destination create` Man-Page.

Schritte

1. Erstellen eines Syslog-Serverziels für wichtige Ereignisse:

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

   Ab ONTAP 9.12.1 können für folgende Werte angegeben werden `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol ohne Sicherheit
   - `tcp-unencrypted` - Transmission Control Protocol ohne Sicherheit
   - `tcp-encrypted` - Transmission Control Protocol mit Transport Layer Security (TLS)

   Das Standardprotokoll ist `udp-unencrypted`.

2. Konfigurieren Sie die wichtigen Ereignisse, um Benachrichtigungen an den Syslog-Server weiterzuleiten:

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

Konfigurieren Sie SNMP-Trap-Hosts für den Empfang von Ereignisbenachrichtigungen

Um Ereignisbenachrichtigungen auf einem SNMP traphost zu erhalten, müssen Sie einen traphost konfigurieren.

Was Sie benötigen

- SNMP- und SNMP-Traps müssen auf dem Cluster aktiviert sein.

  SNMP- und SNMP-Traps sind standardmäßig aktiviert.

- DNS muss auf dem Cluster konfiguriert werden, um die traphost-Namen zu lösen.

Über diese Aufgabe

Wenn Sie noch keinen SNMP traphost für den Empfang von Ereignisbenachrichtigungen (SNMP Traps) konfiguriert haben, müssen Sie einen hinzufügen.

Sie können diese Aufgabe jederzeit ausführen, wenn das Cluster ausgeführt wird, indem Sie die Befehle in die ONTAP-Befehlszeile eingeben.

Schritt

1. Wenn in Ihrer Umgebung noch kein SNMP traphost für den Empfang von Ereignisbenachrichtigungen konfiguriert ist, fügen Sie eine hinzu:

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

Alle Ereignisbenachrichtigungen, die standardmäßig von SNMP unterstützt werden, werden an den SNMP traphost weitergeleitet.

Konfigurieren Sie wichtige EMS-Ereignisse, um Benachrichtigungen an eine Webhook-Anwendung weiterzuleiten

Sie können ONTAP so konfigurieren, dass wichtige Ereignisbenachrichtigungen an eine Webhook-Anwendung weitergesendet werden. Die erforderlichen Konfigurationsschritte hängen vom gewählten Sicherheitsniveau ab.

Bereiten Sie sich auf die Konfiguration der EMS-Ereignisweiterleitung vor

Es gibt verschiedene Konzepte und Anforderungen, die Sie berücksichtigen sollten, bevor Sie ONTAP konfigurieren, um Ereignisbenachrichtigungen an eine Webhook-Anwendung weiterzuleiten.

Webhook-Anwendung

Sie benötigen eine Webhook-Anwendung, die die ONTAP-Ereignisbenachrichtigungen erhalten kann. Ein Webhook ist eine benutzerdefinierte Callback-Routine, die die Fähigkeit der Remote-Anwendung oder des Servers erweitert, auf dem sie ausgeführt wird. Webhooks werden vom Client (in diesem Fall ONTAP) aufgerufen oder aktiviert, indem eine HTTP-Anfrage an die Ziel-URL gesendet wird. Insbesondere sendet ONTAP eine HTTP-POST-Anfrage an den Server, der die Webhook-Anwendung hostet, sowie die in XML formatierten Ereignisbenachrichtigungen.

Sicherheitsoptionen

Je nach Verwendung des TLS-Protokolls (Transport Layer Security) stehen verschiedene Sicherheitsoptionen zur Verfügung. Die von Ihnen gewählte Option bestimmt die erforderliche ONTAP-Konfiguration.

ⓘ TLS ist ein kryptografisches Protokoll, das im Internet weit verbreitet ist. Sie bietet Datenschutz sowie Datenintegrität und Authentifizierung unter Verwendung eines oder mehrerer Public-Key-Zertifikate. Die Zertifikate werden von vertrauenswürdigen Zertifizierungsstellen ausgestellt.

HTTP

Sie können HTTP für die Übertragung von Ereignisbenachrichtigungen verwenden. Bei dieser Konfiguration ist die Verbindung nicht sicher. Die Identitäten des ONTAP-Clients und der Webhook-Anwendung werden nicht überprüft. Darüber hinaus ist der Netzwerkverkehr weder verschlüsselt noch geschützt. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP" Für die Konfigurationsdetails.

HTTPS

Für zusätzliche Sicherheit können Sie ein Zertifikat auf dem Server installieren, der die Webhook-Routine hostet. Das HTTPS-Protokoll wird von ONTAP verwendet, um die Identität des Webhook-Anwendungsservers sowie von beiden Parteien zu überprüfen, um die Privatsphäre und Integrität des Netzwerkdatenverkehrs zu gewährleisten. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS" Für die Konfigurationsdetails.

HTTPS mit gegenseitiger Authentifizierung

Sie können die HTTPS-Sicherheit weiter erhöhen, indem Sie ein Clientzertifikat beim ONTAP-System installieren, das die Webbook-Anfragen ausgibt. Zusätzlich zur ONTAP, die die Identität des Webhook-Anwendungsservers überprüft und den Netzwerkverkehr schützt, überprüft die Webhook-Anwendung die

Identität des ONTAP-Clients. Diese Zweiwege-Peer-Authentifizierung wird als *Mutual TLS* bezeichnet. Siehe "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung" Für die Konfigurationsdetails.

Verwandte Informationen

- "Das TLS-Protokoll (Transport Layer Security) Version 1.3"

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTP an eine Webhook-Anwendung weitergesendet werden. Dies ist die am wenigsten sichere Option, aber die einfachste Einrichtung.

Schritte

1. Erstellen Sie ein neues Ziel `restapi-ems` So erhalten Sie die Ereignisse:

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

   Im obigen Befehl müssen Sie das **HTTP**-Schema für das Ziel verwenden.

2. Erstellen Sie eine Benachrichtigung, die den verknüpft `important-events` Mit dem filtern `restapi-ems` Ziel:

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

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTPS an eine Webhook-Anwendung weitergesendet werden. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr zu sichern.

Bevor Sie beginnen

- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver
- Lassen Sie das Root-Zertifikat zur Installation in ONTAP zur Verfügung

Schritte

1. Installieren Sie den entsprechenden Server-privaten Schlüssel und die entsprechenden Zertifikate auf dem Server, der Ihre Webhook-Anwendung hostet. Die spezifischen Konfigurationsschritte hängen vom Server ab.
2. Installieren Sie das Server-Root-Zertifikat in ONTAP:

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

   Der Befehl fragt nach dem Zertifikat.

3. Erstellen Sie die `restapi-ems` Ziel für den Empfang der Ereignisse:

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

   Im obigen Befehl müssen Sie das Schema **HTTPS** für das Ziel verwenden.

4. Erstellen Sie die Benachrichtigung, die den verbindet `important-events` Mit dem neuen Filter filtern `restapi-ems` Ziel:

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

Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung

Sie können ONTAP so konfigurieren, dass Ereignisbenachrichtigungen mithilfe von HTTPS mit gegenseitiger Authentifizierung an eine Webhook-Anwendung weitergesendet werden. Mit dieser Konfiguration gibt es zwei Zertifikate. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr zu sichern. Darüber hinaus verwendet die Anwendung, die den Webhook hostet, das Clientzertifikat, um die Identität des ONTAP-Clients zu bestätigen.

Bevor Sie beginnen

Vor dem Konfigurieren von ONTAP müssen Sie Folgendes ausführen:

- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver
- Lassen Sie das Root-Zertifikat zur Installation in ONTAP zur Verfügung
- Generieren Sie einen privaten Schlüssel und ein Zertifikat für den ONTAP-Client

Schritte

1. Führen Sie die ersten beiden Schritte in der Aufgabe aus "Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS" So installieren Sie das Serverzertifikat, damit ONTAP die Identität des Servers überprüfen kann.
2. Installieren Sie die entsprechenden Root- und Zwischenzertifikate in der Webhook-Anwendung, um das Clientzertifikat zu validieren.
3. Installieren Sie das Client-Zertifikat in ONTAP:

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

   Der Befehl fragt nach dem privaten Schlüssel und dem Zertifikat.

4. Erstellen Sie die `restapi-ems` Ziel für den Empfang der Ereignisse:

   ```
   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>
   ```

   Im obigen Befehl müssen Sie das Schema **HTTPS** für das Ziel verwenden.

5. Erstellen Sie die Benachrichtigung, die den verbindet `important-events` Mit dem neuen Filter filtern `restapi-ems` Ziel:

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

Aktualisieren der veralteten EMS-Ereigniszuordnung

EMS-Modelle für die Ereigniszuordnung

Vor ONTAP 9.0 konnten EMS-Ereignisse basierend auf dem Abgleich von Ereignisnamen nur Ereigniszielen zugeordnet werden. Die ONTAP-Befehle werden eingestellt (`event destination`, `event route`), die dieses Modell verwenden, ist weiterhin in den neuesten Versionen von ONTAP verfügbar, aber sie sind seit ONTAP 9.0 veraltet.

Seit ONTAP 9.0 empfiehlt sich die Verwendung des skalierbareren Ereignisfiltermodells für ONTAP EMS, in dem die Musteranpassung für mehrere Felder mit dem durchgeführt wird `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Wenn Ihre EMS-Zuordnung mit den veralteten Befehlen konfiguriert ist, sollten Sie Ihre Zuordnung aktualisieren, um die zu verwenden `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Es gibt zwei Arten von Ereigniszielen:

1. **Systemgenerierte Ziele**: Es gibt fünf vom System generierte Ereignisziele (standardmäßig erstellt)
    - `allevents`
    - `asup`
    - `criticals`
    - `pager`
    - `traphost`

      Einige der vom System generierten Ziele sind für besondere Zwecke. Zum Beispiel leitet das Asup-Zielgerät Callhome.* Ereignisse an das AutoSupport-Modul in ONTAP weiter, um AutoSupport-Nachrichten zu generieren.
2. **Vom Benutzer erstellte Ziele**: Diese werden manuell mit dem erstellt `event destination create` Befehl.

```
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.
```

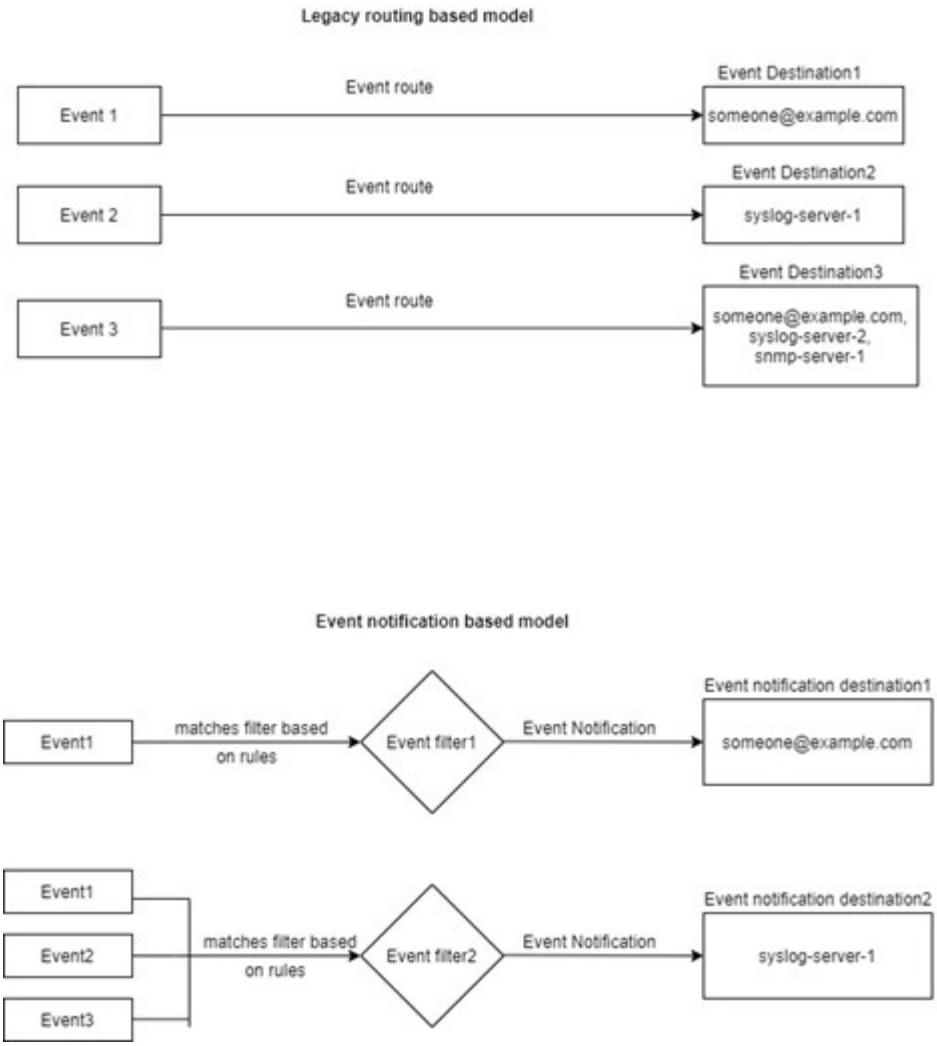
Im veralteten Modell werden EMS-Ereignisse individuell einem Ziel über zugeordnet `event route add-destinations` Befehl.

```
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.
```

Der neue, besser skalierbare EMS-Mechanismus für Ereignisbenachrichtigungen basiert auf Ereignisfiltern und Zielorten für Ereignisbenachrichtigungen. Detaillierte Informationen zum neuen Benachrichtigungsmechanismus für Ereignisse finden Sie in dem folgenden KB-Artikel:

- "Übersicht über das Event Management System für ONTAP 9"



Aktualisieren der EMS-Ereigniszuordnung aus veralteten ONTAP Befehlen

Wenn Ihre EMS-Ereigniszuordnung derzeit mit den veraltet ONTAP-Befehlssätzen konfiguriert ist (`event destination`, `event route`Sie sollten dieses Verfahren befolgen, um Ihr Mapping zu aktualisieren, um das zu verwenden `event filter`, `event notification`, und `event notification destination` Befehlssätze.

Schritte

1. Listen Sie alle Event-Ziele im System mithilfe von auf `event destination show` Befehl.

```
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. Führen Sie für jedes Ziel die Ereignisse auf, die ihm mithilfe des zugeordnet sind `event route show -destinations <destination name>` Befehl.

```
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. Erstellen Sie eine entsprechende `event filter` Welches all diese Teilmengen von Ereignissen enthält. Beispiel: Wenn Sie nur die einschließen möchten `raid.aggr.*` Ereignisse, verwenden Sie einen Platzhalter für die `message-name` Parameter beim Erstellen des Filters. Sie können auch Filter für einzelne Ereignisse erstellen.

> Sie können bis zu 50 Ereignisfilter erstellen.

```
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. Erstellen Sie ein `event notification destination` Für jede der `event destination` Endpunkte (z. B. 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. Erstellen Sie eine Ereignisbenachrichtigung, indem Sie den Ereignisfilter dem Ziel der Ereignisbenachrichtigung zuordnen.

```
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. Wiederholen Sie die Schritte 1-5 für jede einzelne `event destination` Das ist ein `event route` Zuordnung:

> An SNMP-Ziele weitergeleitete Ereignisse sollten dem zugeordnet werden `snmp-traphost` Ziel der Ereignisbenachrichtigung Das SNMP traphost-Ziel verwendet das System konfigurierte SNMP traphost.

```
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?: -
```