



EMS-Konfiguration

ONTAP 9

NetApp
January 08, 2026

Inhalt

EMS-Konfiguration	1
Erfahren Sie mehr über die ONTAP-EMS-Konfiguration	1
Konfigurieren Sie ONTAP EMS-Ereignisbenachrichtigungen und -Filter mit System Manager	1
Fügen Sie ein EMS-Ereignisbenachrichtigungs-Ziel hinzu	1
Erstellen Sie einen neuen EMS-Ereignisbenachrichtigungs-Filter	2
Bearbeiten Sie ein EMS-Ereignisbenachrichtigungs-Ziel	3
Bearbeiten Sie einen EMS-Ereignisbenachrichtigungs-Filter	3
Löschen Sie ein EMS-Ereignisbenachrichtigungs-Ziel	3
Löschen Sie einen EMS-Ereignisbenachrichtigungs-Filter	4
Konfigurieren Sie EMS-Ereignisbenachrichtigungen mit der CLI	4
ONTAP EMS-Konfigurationsworkflow	4
Konfigurieren Sie wichtige ONTAP EMS-Ereignisse, um E-Mail-Benachrichtigungen zu senden	6
Konfigurieren Sie wichtige ONTAP EMS-Ereignisse, um Benachrichtigungen an einen Syslog-Server weiterzuleiten	6
Konfigurieren Sie ONTAP SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen	7
Konfigurieren Sie wichtige ONTAP-EMS-Ereignisse, um Benachrichtigungen an eine Webhook- Anwendung weiterzuleiten	8
Aktualisieren der veralteten EMS-Ereigniszuordnung	11
Erfahren Sie mehr über die ONTAP EMS-Ereigniszuordnungsmodelle	11
Aktualisieren Sie die ONTAP-EMS-Ereigniszuordnung von veralteten Befehlen	15

EMS-Konfiguration

Erfahren Sie mehr über die ONTAP-EMS-Konfiguration

Sie können ONTAP 9 so konfigurieren, dass wichtige EMS (Event Management System)-Ereignisbenachrichtigungen direkt an eine E-Mail-Adresse, Syslog-Server, Simple Management Network Protocol (SNMP) traphost oder Webhook-Anwendung gesendet werden, sodass Sie sofort über Systemprobleme benachrichtigt werden, die eine sofortige Aufmerksamkeit erfordern.

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

Überprüfen Sie die Release-spezifischen Versionen der ["ONTAP 9 EMS-Referenz"](#).

Wenn Ihre EMS-Ereigniszuordnung veraltete ONTAP-Befehlssätze verwendet (z. B. Ereignisziel, Ereignisroute), wird empfohlen, dass Sie Ihre Zuordnung aktualisieren. ["Erfahren Sie, wie Sie Ihre EMS-Zuordnung von veralteten ONTAP-Befehlen aktualisieren können"](#).

Konfigurieren Sie ONTAP 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 9.10.0 bis 9.7	Konfigurieren Sie nur SNMP-Trap-Hosts. Sie können ein anderes EMS-Ziel mit der ONTAP CLI konfigurieren. Siehe "Übersicht über die EMS-Konfiguration" .

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. Erfahren Sie mehr über `event notification destination create` in der ["ONTAP-Befehlsreferenz"](#).

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungsverwaltung** auf , und klicken Sie dann auf **Ereignisziele 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	<ul style="list-style-type: none">• TrapHost-Name
E-Mail (Ab 9.10.1)	<ul style="list-style-type: none">• E-Mail-Adresse des Zielorts• Mailserver• Von E-Mail-Adresse
Syslog-Server (Ab 9.10.1)	<ul style="list-style-type: none">• Hostname oder IP-Adresse des Servers• Syslog-Port (beginnend mit 9.12.1)• Syslog-Transport (ab 9.12.1) <p>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.</p>
Webhook (Ab 9.10.1)	<ul style="list-style-type: none">• 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 , und klicken Sie dann auf **Ereignisziele 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	<ol style="list-style-type: none"> 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 , und klicken Sie dann auf **Ereignisziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf , und 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 , und klicken Sie dann auf **Ereignisziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf , und 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 , und klicken Sie dann auf **Ereignisziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisziele** aus.
4. Klicken Sie neben dem Namen des Ereignisziels auf , und 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 , und klicken Sie dann auf **Ereignisziele anzeigen**.
3. Wählen Sie auf der Seite **Benachrichtigungsverwaltung** die Registerkarte **Ereignisfilter** aus.
4. Klicken Sie neben dem Namen des Ereignisfilters auf , und klicken Sie dann auf **Löschen**.

Verwandte Informationen

- ["ONTAP EMS-Referenz"](#)
- ["Mit der CLI können Sie SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren"](#)

Konfigurieren Sie EMS-Ereignisbenachrichtigungen mit der CLI

ONTAP 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.

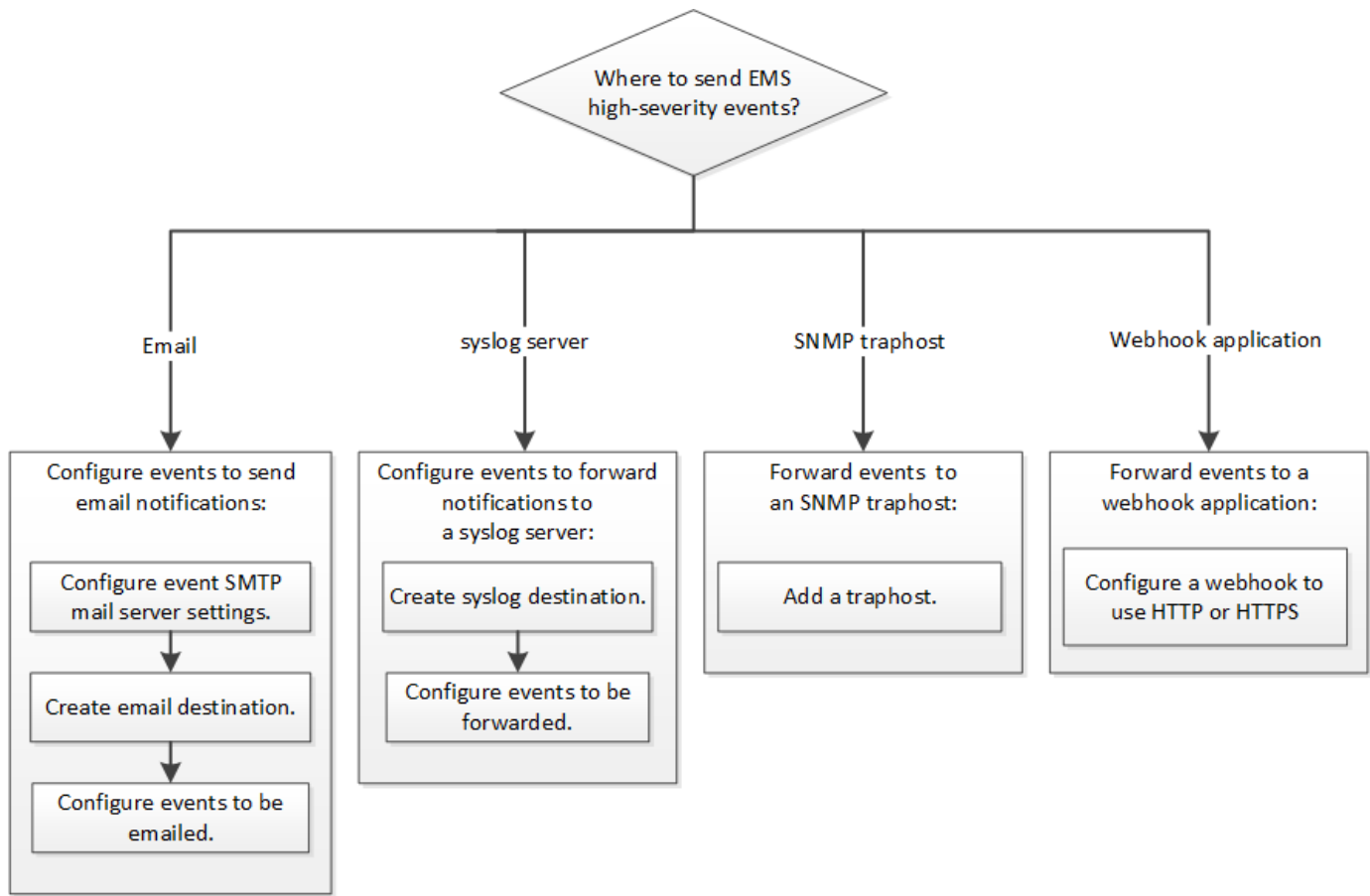
Über diese Aufgabe

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 ONTAP EMS-Ereignisse, um E-Mail-Benachrichtigungen zu senden

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.

Bevor Sie beginnen

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
```

Erfahren Sie mehr über `event config modify` in der ["ONTAP-Befehlsreferenz"](#).

2. E-Mail-Ziel für Ereignisbenachrichtigungen erstellen:

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

Erfahren Sie mehr über `event notification destination create` in der ["ONTAP-Befehlsreferenz"](#).

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

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

Erfahren Sie mehr über `event notification create` in der ["ONTAP-Befehlsreferenz"](#).

Konfigurieren Sie wichtige ONTAP EMS-Ereignisse, um Benachrichtigungen an einen Syslog-Server weiterzuleiten

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.

Bevor Sie beginnen

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` für den angegeben wird `syslog-transport`, überprüft ONTAP die Identität des Zielhosts durch Validierung seines Zertifikats. Der Standardwert ist `udp-unencrypted`.

syslog-port

Der Standardwertparameter `syslog-port` hängt von der Einstellung für den `syslog-transport` Parameter ab. Wenn `syslog-transport` auf `tcp-encrypted`, gesetzt ist, `syslog-port` hat den Standardwert 6514.

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 folgende Werte angegeben werden für `syslog-transport`:

- `udp-unencrypted` - Benutzer-Datagramm-Protokoll ohne Sicherheit
- `tcp-unencrypted` - Transmission Control Protocol ohne Sicherheit
- `tcp-encrypted` - Transmission Control Protocol mit Transport Layer Security (TLS)

Das Standardprotokoll ist `udp-unencrypted`.

Erfahren Sie mehr über `event notification destination create` in der ["ONTAP-Befehlsreferenz"](#).

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

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

Erfahren Sie mehr über `event notification create` in der ["ONTAP-Befehlsreferenz"](#).

Konfigurieren Sie ONTAP SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen

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

Bevor Sie beginnen

- 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 ONTAP-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. ["Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTP"](#)Die Konfigurationsdetails finden Sie unter.

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. ["Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS"](#)Die Konfigurationsdetails finden Sie unter.

HTTPS mit gegenseitiger Authentifizierung

Sie können die HTTPS-Sicherheit weiter erhöhen, indem Sie ein Clientzertifikat beim ONTAP-System installieren, das die Webhook-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. ["Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung"](#)Die Konfigurationsdetails finden Sie unter.

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`, um die Ereignisse zu empfangen:

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

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

Erfahren Sie mehr über `event notification destination create` in der ["ONTAP-Befehlsreferenz"](#).

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

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

Erfahren Sie mehr über `event notification create` in der ["ONTAP-Befehlsreferenz"](#).

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 das `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 `important-events` Filter mit dem neuen `restapi-ems` Ziel verknüpft:

```
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 der Aufgabe aus "[Konfigurieren Sie ein Webhook-Ziel für die Verwendung von HTTPS](#)", um das Serverzertifikat zu installieren, 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 das `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 `important-events` Filter mit dem neuen `restapi-ems` Ziel verknüpft:

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

Verwandte Informationen

- ["Sicherheitszertifikat installieren"](#)

Aktualisieren der veralteten EMS-Ereigniszuordnung

Erfahren Sie mehr über die ONTAP EMS-Ereigniszuordnungsmodelle

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

Beginnend mit ONTAP 9.0, ist die beste Praxis für ONTAP EMS-Ereigniszielzuordnung, das skalierbarere Ereignisfiltermodell `event filter event notification event notification destination` zu verwenden, in dem Musterabgleich auf mehreren Feldern erfolgt, mit den, und Befehlssätzen.

Wenn Ihre EMS-Zuordnung mit den veralteten Befehlen konfiguriert ist, sollten Sie Ihre Zuordnung aktualisieren, um die `event filter event notification event notification destination` Befehlssätze, und zu verwenden. Erfahren Sie mehr über `event` in der ["ONTAP-Befehlsreferenz"](#).

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 `event destination create` Befehl erstellt.

```
cluster-1::event*> destination show
```

Name	Mail Dest.	SNMP Dest.	Syslog Dest.	Hide
------	------------	------------	--------------	------

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 über den `event route add-destinations` Befehl individuell einem Ziel zugeordnet.

```
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.*
```

Time	Severity	Destinations	Freq	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.

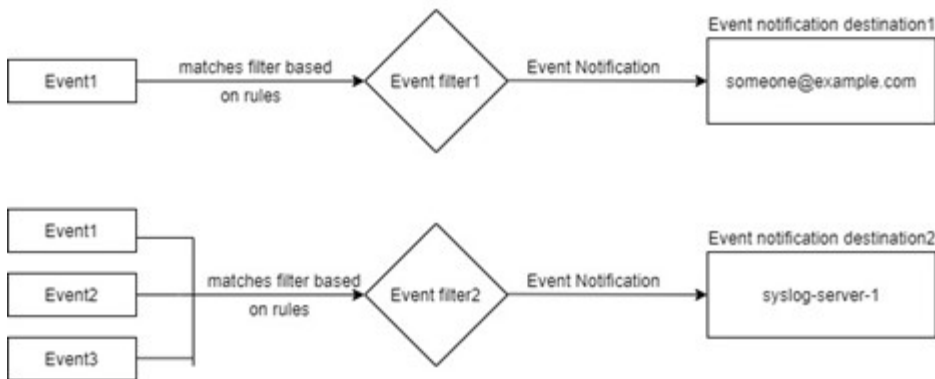
Der neue, besser skalierbare EMS-Mechanismus für Ereignisbenachrichtigungen basiert auf Ereignisfiltern und Zielorten für Ereignisbenachrichtigungen. Detaillierte Informationen zum neuen Benachrichtigungsmechanismus für Ereignisse finden Sie in dem folgenden KB-Artikel:

- ["Übersicht über das Event Management System für ONTAP 9"](#)

Legacy routing based model



Event notification based model



Aktualisieren Sie die ONTAP-EMS-Ereigniszuordnung von veralteten Befehlen

Wenn Ihre EMS-Ereigniszuordnung derzeit mit den veralteten ONTAP-Befehlssätzen (event destination, event route) konfiguriert ist, sollten Sie dieses Verfahren befolgen, um Ihre Zuordnung zu aktualisieren, um die event filter event notification event notification destination Befehlssätze , und zu verwenden.

Schritte

1. Führen Sie mit dem event destination show Befehl alle Event-Ziele im System auf.

```
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 zugeordnet werden `event route show -destinations <destination name>`, mit dem Befehl.

```
cluster-1::event*> route show -destinations test
```

Time	Severity	Destinations	Freq	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 ein entsprechendes `event filter`, das alle diese Teilmengen von Ereignissen enthält. Wenn Sie beispielsweise nur die `raid.aggr.*`-Ereignisse einbeziehen möchten, verwenden Sie `message-name` beim Erstellen des Filters einen Platzhalter für den Parameter. Sie können auch Filter für einzelne Ereignisse erstellen.

Erfahren Sie mehr über `event filter` in der ["ONTAP-Befehlsreferenz"](#).



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 eines event notification destination für jeden event destination Endpunkt (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.
```

Erfahren Sie mehr über event notification destination und event destination in der ["ONTAP-Befehlsreferenz"](#).

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 alle event destination, die eine event route Zuordnung haben.



Ereignisse, die an SNMP-Ziele weitergeleitet werden snmp-traphost, sollten dem Ziel für die Ereignisbenachrichtigung zugeordnet werden. 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?: -
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.