



使用**CLI**設定**EMS**事件通知 ONTAP 9

NetApp
January 08, 2026

目錄

使用CLI設定EMS事件通知	1
ONTAP EMS 組態工作流程	1
設定重要的 ONTAP EMS 事件以傳送電子郵件通知	2
設定重要的 ONTAP EMS 事件，將通知轉送到系統記錄伺服器	2
設定 ONTAP SNMP traphosts 以接收事件通知	3
設定重要的 ONTAP EMS 事件，將通知轉寄至 Webhook 應用程式	4
準備設定EMS事件轉送	4
設定Webhook目的地以使用HTTP	5
設定 Webhook 目的地以使用 HTTPS	5
設定Webhook目的地使用HTTPS進行相互驗證	6

使用CLI設定EMS事件通知

ONTAP EMS 組態工作流程

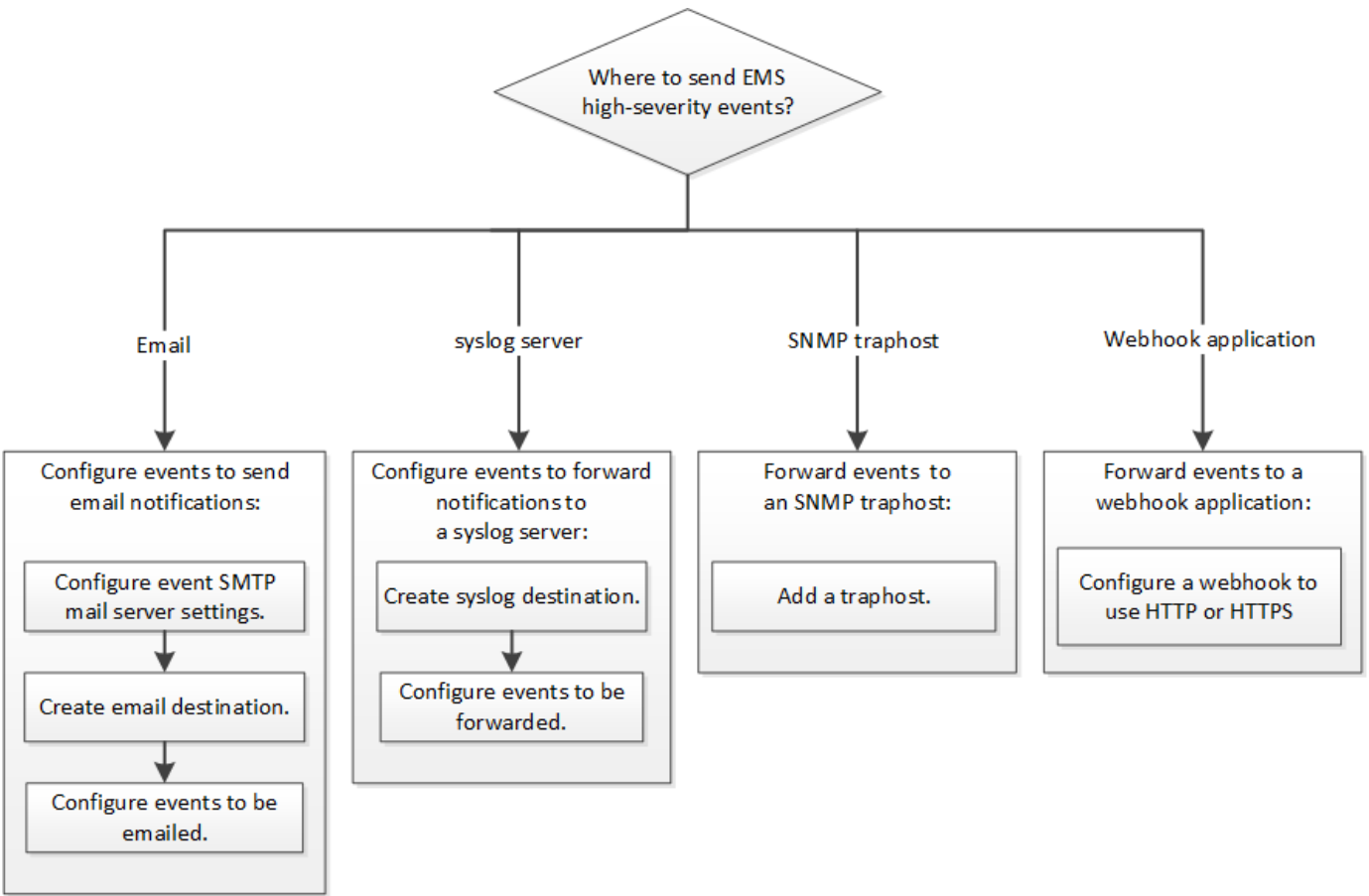
您必須將重要的EMS事件通知設定為以電子郵件傳送、轉送至syslog伺服器、轉送至SNMP traphost、或轉送至Webhook應用程式。這有助於您及時採取修正行動、避免系統中斷。

關於這項工作

如果您的環境已包含syslog伺服器、可用來彙總來自其他系統（例如同服務器和應用程式）的記錄事件、那麼使用syslog伺服器也能更輕鬆地從儲存系統發出重要的事件通知。

如果您的環境尚未包含syslog伺服器、則使用電子郵件進行重要事件通知會更容易。

如果您已將事件通知轉送到SNMP traphost、則可能需要監控該traphost是否有重要事件。



選擇

- 設定EMS以傳送事件通知。

如果您需要...	請參閱此...
將重要事件通知傳送至電子郵件地址的EMS	設定重要的EMS事件以傳送電子郵件通知

EMS可將重要事件通知轉送至syslog伺服器	設定重要的EMS事件、將通知轉送到syslog伺服器
如果您想要EMS將事件通知轉送到SNMP traphost	設定SNMP traphosts以接收事件通知
如果您想要EMS將事件通知轉送到Webhook應用程式	設定重要的EMS事件、將通知轉送到Webhook應用程式

設定重要的 ONTAP EMS 事件以傳送電子郵件通知

若要接收最重要事件的電子郵件通知、您必須將EMS設定為針對重要活動的事件傳送電子郵件訊息。

開始之前

必須在叢集上設定DNS、才能解析電子郵件地址。

關於這項工作

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 設定事件的SMTP郵件伺服器設定：

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

如"[指令參考資料ONTAP](#)"需詳細 `event config modify` 資訊，請參閱。

2. 建立事件通知的電子郵件目的地：

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

如"[指令參考資料ONTAP](#)"需詳細 `event notification destination create` 資訊，請參閱。

3. 設定重要事件以傳送電子郵件通知：

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

如"[指令參考資料ONTAP](#)"需詳細 `event notification create` 資訊，請參閱。

設定重要的 ONTAP EMS 事件，將通知轉送到系統記錄伺服器

若要在syslog伺服器上記錄最嚴重事件的通知、您必須將EMS設定為轉送重要活動訊號的事件通知。

開始之前

必須在叢集上設定DNS、才能解析syslog伺服器名稱。

關於這項工作

如果您的環境尚未包含用於事件通知的syslog伺服器、您必須先建立一個。如果您的環境中已包含用於記錄其他系統事件的syslog伺服器、您可能會想要使用該伺服器來處理重要的事件通知。

您可以在ONTAP 叢集執行時、在CLI輸入命令來執行此工作。

從S應9.12.1開始ONTAP、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。有兩個新參數可供使用：

tcp-encrypted

何時 tcp-encrypted 為指定 syslog-transport、ONTAP 驗證目的地主機的憑證來驗證其身分。預設值為 udp-unencrypted。

syslog-port

預設值 syslog-port 參數取決於的設定 syslog-transport 參數。如果 syslog-transport 設為 tcp-encrypted、syslog-port 預設值為6514。

步驟

1. 建立重要事件的syslog伺服器目的地：

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

從ONTAP 功能變數9.12.1開始、可以指定下列值 syslog-transport：

- udp-unencrypted 無安全性的使用者資料包傳輸協定
- tcp-unencrypted 無安全性的傳輸控制傳輸協定
- tcp-encrypted -傳輸層安全性（TLS）的傳輸控制傳輸協定

預設傳輸協定為 udp-unencrypted。

如"[指令參考資料ONTAP](#)"需詳細 `event notification destination create` 資訊，請參閱。

2. 設定重要事件以將通知轉送到syslog伺服器：

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

如"[指令參考資料ONTAP](#)"需詳細 `event notification create` 資訊，請參閱。

設定 ONTAP SNMP traphosts 以接收事件通知

若要在SNMP traphost上接收事件通知、您必須設定traphost。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。



SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。

關於這項工作

如果您尚未設定SNMP traphost來接收事件通知（SNMP設陷）、則必須新增一個。

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 如果您的環境尚未設定SNMP traphost來接收事件通知、請新增一個：

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

SNMP預設支援的所有事件通知都會轉送到SNMP traphost。

設定重要的 ONTAP EMS 事件，將通知轉寄至 Webhook 應用程式

您可以設定ONTAP 將重要事件通知轉送至Webhook應用程式。所需的組態步驟取決於您選擇的安全性層級。

準備設定EMS事件轉送

在設定ONTAP 將事件通知轉送到Webhook應用程式之前、您應該考慮幾個概念和要求。

Webhook應用程式

您需要能夠接收ONTAP 不必要事件通知的Webhook應用程式。Webhook是使用者定義的回撥例行工作、可延伸執行遠端應用程式或伺服器的功能。Webhooks是由用戶端呼叫或啟動（本例ONTAP 為示例）、方法是將HTTP要求傳送至目的地URL。具體而言ONTAP 、將HTTP POST要求傳送至裝載Webhook應用程式的伺服器、以及以XML格式設定的事件通知詳細資料。

安全選項

視傳輸層安全性（TLS）傳輸協定的使用方式而定、有多種安全選項可供選擇。您選擇的選項會決定所需ONTAP 的功能組態。



TLS是一種在網際網路上廣泛使用的密碼編譯傳輸協定。它使用一或多個公開金鑰憑證來提供隱私、資料完整性和驗證。這些憑證由信任的憑證授權單位核發。

HTTP

您可以使用HTTP來傳輸事件通知。使用此組態時、連線不安全。不驗證不驗證ONTAP 客戶端和Webhook應用程式的身分。此外、網路流量並未加密或受到保護。請參閱 ["設定Webhook目的地以使用HTTP"](#) 以取得組態詳細資料。

HTTPS

為了提高安全性、您可以在裝載Webhook例行工作的伺服器上安裝憑證。驗證Webhook應用程式伺服器及雙方身分的HTTPS傳輸協定、ONTAP 以確保網路流量的隱私性和完整性。請參閱 ["設定 Webhook 目的地以使用 HTTPS"](#) 以取得組態詳細資料。

HTTPS搭配相互驗證

您可以在ONTAP 發出Webhook要求的系統上安裝用戶端憑證、進一步強化HTTPS安全性。除了驗證Webhook應用程式伺服器的身分、並保護網路流量之外、Webhook應用程式還會驗證該客戶端的身分。ONTAP 這種雙向對等驗證稱為「相互TLS」。請參閱 ["設定Webhook目的地使用HTTPS進行相互驗證"](#) 以取得組態詳細資料。

相關資訊

- ["傳輸層安全性 \(TLS\) 傳輸協定1.3版"](#)

設定Webhook目的地以使用HTTP

您可以設定ONTAP 使用HTTP將事件通知轉送至Webhook應用程式。這是最不安全的選項、但設定起來最簡單。

步驟

1. 建立新目的地 `restapi-ems` 若要接收事件：

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

在上述命令中、您必須使用* HTTP配置作為目的地。

如["指令參考資料ONTAP"](#)需詳細 `event notification destination create` 資訊，請參閱。

2. 建立連結的通知 `important-events` 使用篩選 `restapi-ems` 目的地：

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

如["指令參考資料ONTAP"](#)需詳細 `event notification create` 資訊，請參閱。

設定 Webhook 目的地以使用 HTTPS

您可以設定 ONTAP 、使用 HTTPS 將事件通知轉寄至 Webhook 應用程式。使用伺服器憑證來確認Webhook應用程式的身分識別、以及保護網路流量。ONTAP

開始之前

- 為Webhook應用程式伺服器產生私密金鑰和憑證
- 讓root憑證可安裝在ONTAP 整個過程中

步驟

1. 在裝載Webhook應用程式的伺服器上安裝適當的伺服器私密金鑰和憑證。具體的組態步驟取決於伺服器。
2. 將伺服器根憑證安裝在ONTAP

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

命令會要求提供憑證。

3. 建立 restapi-ems 接收事件的目的地：

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

在上述命令中、您必須使用* HTTPS *配置作為目的地。

4. 建立連結的通知 important-events 使用新的篩選器 restapi-ems 目的地：

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

設定Webhook目的地使用HTTPS進行相互驗證

您可以設定ONTAP 將事件通知轉送至Webhook應用程式、使用HTTPS搭配相互驗證。使用此組態有兩個憑證。使用伺服器憑證來確認Webhook應用程式的身分、並保護網路流量。ONTAP此外、裝載Webhook的應用程式會使用用戶端憑證來確認ONTAP 該客戶端的身分。

開始之前

您必須先執行下列步驟、才能設定ONTAP 使用功能：

- 為Webhook應用程式伺服器產生私密金鑰和憑證
- 讓root憑證可安裝在ONTAP 整個過程中
- 為ONTAP 該驗證用戶端產生私密金鑰和憑證

步驟

1. 執行工作的前兩個步驟 **"設定 Webhook 目的地以使用 HTTPS"** 安裝伺服器憑證、ONTAP 以便驗證伺服器的身分。
2. 在Webhook應用程式中安裝適當的根和中繼憑證、以驗證用戶端憑證。
3. 將用戶端憑證安裝ONTAP 在下列項目中：

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

命令會要求提供私密金鑰和憑證。

4. 建立 restapi-ems 接收事件的目的地：

```
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>
```

在上述命令中、您必須使用* HTTPS *配置作為目的地。

5. 建立連結的通知 important-events 使用新的篩選器 restapi-ems 目的地：


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

相關資訊

- ["安全性憑證安裝"](#)

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。