



# CLI を使用して EMS イベント通知を設定します ONTAP 9

NetApp  
April 24, 2024

# 目次

CLI を使用して EMS イベント通知を設定します .....	1
EMSの設定ワークフロー .....	1
重要な EMS イベントの通知を E メールで送信するように設定します .....	2
重要な EMS イベントの通知を syslog サーバに転送するための設定 .....	2
SNMP トラップホストでイベント通知を受信するように設定します .....	4
重要なEMSイベントについて、通知をWebフックアプリケーションに転送するように設定します .....	4

# CLI を使用して EMS イベント通知を設定します

## EMSの設定ワークフロー

重要なEMSイベント通知は、Eメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebフックアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

このタスクについて

サーバやアプリケーションなどの他のシステムで記録されたイベントを集約するためにすでに syslog サーバを使用している場合は、ストレージシステムの重要なイベントの通知にもその syslog サーバを使用すると簡単です。

syslog サーバがまだない場合は、重要なイベントの通知に E メールを使用すると便利です。

イベント通知をすでに SNMP トラップホストに転送している場合は、そのトラップホストで重要なイベントについても監視できます。



選択肢

- イベント通知を送信するように EMS を設定します。

状況

参照先

EMS の重要なイベント通知を E メールアドレスに送信します	重要な EMS イベントの通知を E メールで送信するように設定します
EMS の重要なイベント通知を syslog サーバに転送します	重要な EMS イベントの通知を syslog サーバに転送するように設定します
EMS のイベント通知を SNMP トラップホストに転送する	SNMP トラップホストでイベント通知を受信するように設定します
EMS でイベント通知を webhook アプリケーションに転送する場合	重要な EMS イベントについて、通知を Web フック アプリケーションに転送するように設定します

## 重要な EMS イベントの通知を E メールで送信するように設定します

重要なイベントの通知を E メールで受信するには、重要なアクティビティを示すイベントに関する E メールメッセージを送信するように EMS を設定する必要があります。

必要なもの

クラスタで E メールアドレスを解決するように DNS が設定されている必要があります。

このタスクについて

このタスクは、クラスタの実行中であれば、ONTAP コマンドラインでコマンドを入力していつでも実行できます。

手順

1. イベント用の SMTP メールサーバを設定します。

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

2. イベントの通知に使用する E メール送信先を作成します。

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

3. 重要なイベントの通知を E メールで送信するように設定します。

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

## 重要な EMS イベントの通知を syslog サーバに転送するための設定

重大なイベントの通知を syslog サーバに記録するには、重要なアクティビティを示すイ

ベントに関する通知を転送するように EMS を設定する必要があります。

必要なもの

クラスタで syslog サーバ名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知用の syslog サーバがまだない場合は、先に syslog サーバを作成する必要があります。他のシステムのイベントを記録するためにすでに syslog サーバを使用している場合は、重要なイベントの通知にも同じ syslog サーバを使用できます。

このタスクは、クラスタの実行中であれば、ONTAP CLIでコマンドを入力していつでも実行できます。

ONTAP 9.12.1以降では、EMSイベントをTransport Layer Security (TLS) プロトコル経由でリモートsyslogサーバの指定ポートに送信できます。次の2つの新しいパラメータを使用できます。

### **tcp-encrypted**

いつ tcp-encrypted にを指定します syslog-transport`ONTAP は、デスティネーションホストの証明書を検証することで、そのホストのIDを検証します。デフォルト値はです `udp-unencrypted。

### **syslog-port**

デフォルト値 syslog-port パラメータは、の設定によって異なります syslog-transport パラメータ状況 syslog-transport がに設定されます tcp-encrypted、 syslog-port のデフォルト値は6514です。

詳細については、を参照してください event notification destination create のマニュアルページ。

手順

1. 重要なイベントの転送先の syslog サーバを作成します。

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

ONTAP 9.12.1以降では、に次の値を指定できます syslog-transport :

- ° udp-unencrypted -セキュリティなしのユーザデータグラムプロトコル
- ° tcp-unencrypted -セキュリティなしのTransmission Control Protocol
- ° tcp-encrypted - Transport Layer Security (TLS) を使用したTransmission Control Protocol

デフォルトのプロトコルはです udp-unencrypted`。

2. 重要なイベントについて、 syslog サーバに通知を転送するように設定します。

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

# SNMP トラップホストでイベント通知を受信するように設定します

SNMP トラップホストでイベント通知を受信するには、トラップホストを設定する必要があります。

必要なもの

- ・ クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。



SNMP トラップと SNMP トラップはデフォルトで有効になっています。

- ・ クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知（SNMP トラップ）を受信するように設定した SNMP トラップホストがまだない場合は、SNMP トラップホストを追加する必要があります。

このタスクは、クラスタの実行中であれば、ONTAP コマンドラインでコマンドを入力していつでも実行できます。

ステップ

1. イベント通知を受信するように設定された SNMP トラップホストがまだない場合は、次のいずれかを追加します。

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

SNMP でデフォルトでサポートされるすべてのイベント通知が SNMP トラップホストに転送されます。

## 重要なEMSイベントについて、通知をWebフックアプリケーションに転送するように設定します

重要なイベント通知をwebhookアプリケーションに転送するようにONTAP を設定できます。必要な設定手順は、選択したセキュリティのレベルによって異なります。

### EMSイベント転送を設定するための準備をします

イベント通知をWebフックアプリケーションに転送するようにONTAP を設定する前に、いくつかの概念と要件を考慮する必要があります。

#### Webhookアプリケーション

ONTAP イベント通知を受信できるWebフックアプリケーションが必要です。webhookは、実行するリモートアプリケーションまたはサーバの機能を拡張するユーザ定義のコールバックルーチンです。webhookは、宛先URLにHTTP要求を送信することによって、クライアント（この場合はONTAP）によって呼び出されるか、アクティブになります。具体的には、ONTAP は、webhookアプリケーションをホストするサーバにHTTP POST要求を送信し、イベント通知の詳細をXML形式で送信します。

## セキュリティオプション

Transport Layer Security (TLS) プロトコルの使用方法に応じて、いくつかのセキュリティオプションがあります。選択するオプションによって、必要なONTAP 設定が決まります。



TLSは、インターネットで広く使用されている暗号化プロトコルです。1つ以上の公開鍵証明書を使用して、プライバシー、データの整合性、および認証を実現します。証明書は、信頼された認証局によって発行されます。

### HTTP

HTTPを使用してイベント通知を転送できます。この設定では、接続はセキュアではありません。ONTAP クライアントおよびWebフックアプリケーションのIDは検証されません。さらに、ネットワークトラフィックは暗号化も保護もされません。を参照してください ["HTTPを使用するようにwebhookの宛先を設定します"](#) をクリックして設定の詳細を確認します

### HTTPS

セキュリティを強化するために、webhookルーチンをホストするサーバーに証明書をインストールできます。HTTPSプロトコルは、ONTAP によって、WebフックアプリケーションサーバーのIDおよびネットワークトラフィックのプライバシーと整合性を確保するために、両当事者によって使用されます。を参照してください ["HTTPSを使用するようにWebhookの宛先を設定する"](#) をクリックして設定の詳細を確認します

### HTTPSを相互認証で使用

Webブック要求を発行するONTAP システムにクライアント証明書をインストールすると、HTTPSセキュリティをさらに強化できます。ONTAP がWebフックアプリケーションサーバーのIDを検証し、ネットワークトラフィックを保護することに加えて、webhookアプリケーションはONTAP クライアントのIDを確認します。この双方向ピア認証は、`_Mutual TLS_`と呼ばれています。を参照してください ["相互認証でHTTPSを使用するようにwebhookの宛先を設定します"](#) をクリックして設定の詳細を確認します

### 関連情報

- ["Transport Layer Security \(TLS\) プロトコルバージョン1.3"](#)

## HTTPを使用するようにwebhookの宛先を設定します

HTTPを使用してイベント通知をWebフックアプリケーションに転送するようにONTAP を設定できます。これは最も安全性の低いオプションですが、設定が最も簡単です。

### 手順

1. 新しい保存先を作成します `restapi-ems` イベントを受信するには：

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

上記のコマンドでは、デスティネーションに\* HTTP \*スキームを使用する必要があります。

2. をリンクする通知を作成します `important-events` でフィルタリングします `restapi-ems` 目的地：

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

## HTTPSを使用するようにWebhookの宛先を設定する

HTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAPを設定できます。ONTAPは、サーバ証明書を使用して、WebフックアプリケーションのIDを確認し、ネットワークトラフィックを保護します。

作業を開始する前に

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAPにインストールできるようにします

手順

1. webhookアプリケーションをホストしているサーバに、適切なサーバ秘密鍵と証明書をインストールします。具体的な設定手順は、サーバによって異なります。
2. サーバのルート証明書をONTAPにインストールします。

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

このコマンドでは証明書を要求します。

3. を作成します restapi-ems イベントの受信先：

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

上記のコマンドでは、デスティネーションに\* HTTPS \*スキームを使用する必要があります。

4. をリンクする通知を作成します important-events 新しいでフィルタリングします restapi-ems 目的地：

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

## 相互認証でHTTPSを使用するようにwebhookの宛先を設定します

相互認証を使用したHTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAPを設定できます。この構成では、2つの証明書があります。ONTAPは、サーバ証明書を使用して、WebフックアプリケーションのIDを確認し、ネットワークトラフィックを保護します。また、webhookをホストするアプリケーションは、クライアント証明書を使用してONTAPクライアントのIDを確認します。

作業を開始する前に

ONTAPを設定する前に、次の作業を実行する必要があります。

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAPにインストールできるようにします
- ONTAPクライアントの秘密鍵と証明書を生成します

手順

1. タスクの最初の2つの手順を実行します ["HTTPSを使用するようにWebhookの宛先を設定する"](#) ONTAPが



サーバの識別情報を確認できるようにサーバ証明書をインストールする。

2. 適切なルート証明書と中間証明書をwebhookアプリケーションにインストールして、クライアント証明書を検証します。
3. ONTAP にクライアント証明書をインストールします。

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

秘密鍵と証明書を入力するよう求められます。

4. を作成します restapi-ems イベントの受信先：

```
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>
```

上記のコマンドでは、デスティネーションに\* HTTPS \*スキームを使用する必要があります。

5. をリンクする通知を作成します important-events 新しいでフィルタリングします restapi-ems 目的地：

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

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。