



CLIを使用したEMSイベント通知の設定

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用したEMSイベント通知の設定	1
EMSの設定ワークフロー	1
重要なEMSイベントを設定してEメール通知を送信する	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
イベント通知を受信するためのSNMPトラップホストの設定	3
重要なEMSイベントを設定して通知をWebhookアプリケーションに転送する	4

CLIを使用したEMSイベント通知の設定

EMSの設定ワークフロー

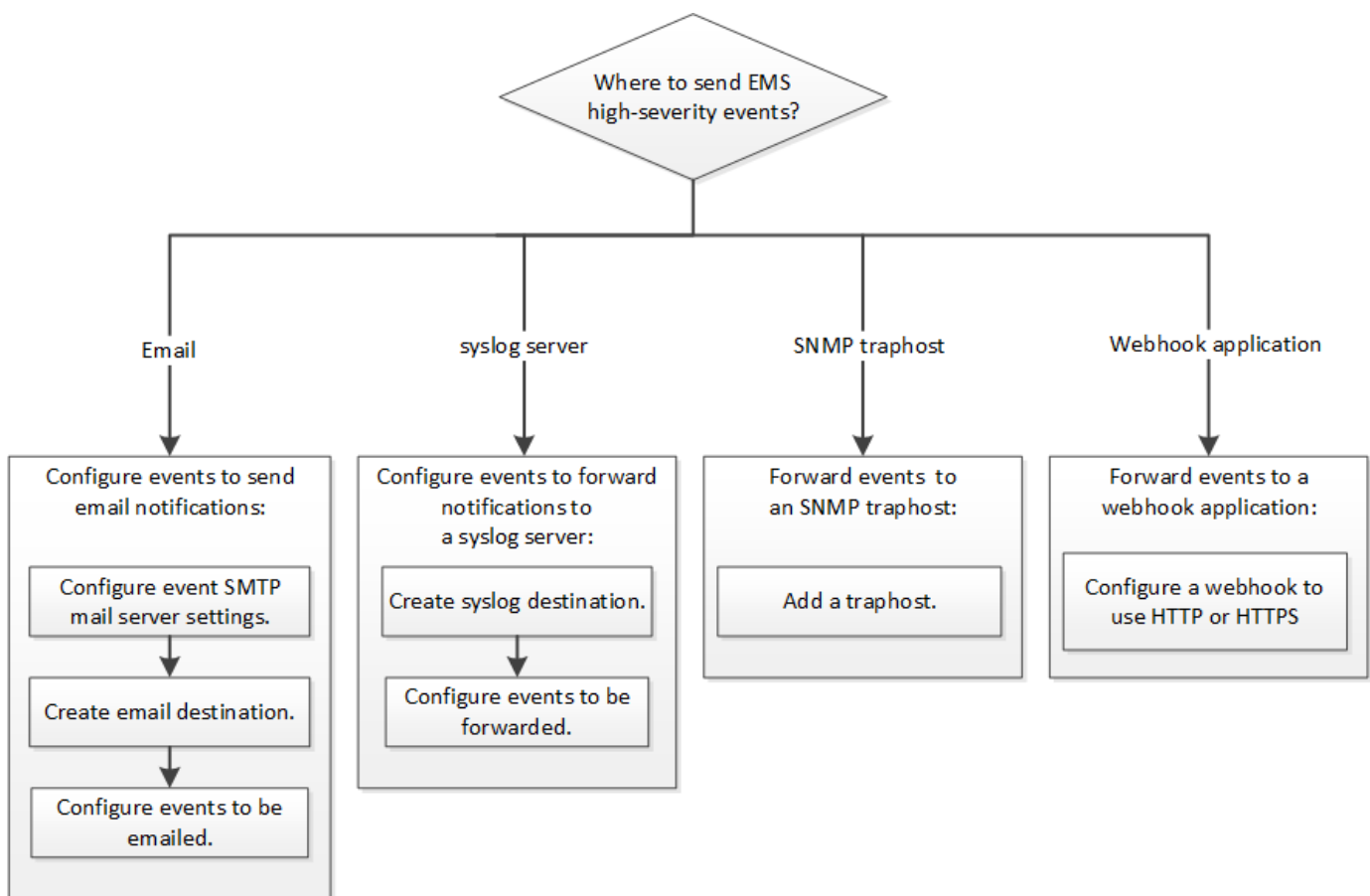
重要なEMSイベント通知がEメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebhookアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

タスクの内容

サーバやアプリケーションなど、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から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メールを使用する方が簡単です。

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が発生していないか監視できます。



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する	重要なEMSイベントを設定してEメール通知を送信する
EMSの重要なイベント通知をsyslogサーバに転送する	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する
EMSのイベント通知をSNMPトラップホストに転送する場合	イベント通知を受信するためのSNMPトラップホストの設定
EMSのイベント通知をWebhookアプリケーションに転送する場合	重要なEMSイベントを設定して通知をWebhookアプリケーションに転送する

重要なEMSイベントを設定してEメール通知を送信する

最も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ついて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。

タスクの内容

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. イベント通知用の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. Eメール通知を送信するための重要なイベントを設定します。

```
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

重大度の高いイベントの通知を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の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。

タスクの内容

イベント通知用のsyslogサーバがまだない場合は、最初に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その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、Transport Layer Security (TLS) プロトコルを使用して、リモートsyslogサーバ上の指定ポートにEMSイベントを送信できます。次の2つの新しいパラメータを使用できます。

tcp-encrypted

にを指定する `syslog-transport`と`tcp-encrypted`、ONTAPは証明書を検証してデスティネーションホストの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`のパラメータは、パラメータの設定によって異なり`syslog-transport`ます。かに設定されて`tcp-encrypted`いる場合、`syslog-transport`の`syslog-port`デフォルト値は6514です。`

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

手順

1. 重要なイベントのsyslogサーバの送信先を作成します。

```
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 `syslog-transport`ます。`

- `udp-unencrypted`-セキュリティなしのUser Datagram Protocol (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伝送制御プロトコル
- `tcp-encrypted`- Transport Layer Security (TLS) を使用したTransmission Control Protocol (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
```

イベント通知を受信するためのSNMPトラップホストの設定

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とSNMPトラップが有効になっている必要があります。



SNMPおよび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。

タスクの内容

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、SNMPトラップホストを追加します。

```
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イベントを設定して通知をWebhookアプリケーションに転送する

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準備

Webhookアプリケーションにイベント通知を転送するように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Webhookアプリケーションが必要です。Webhookはユーザ定義のコールバックルーチンで、実行され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します。Webhookは、宛先URLにHTTP要求を送信することにより、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しているサーバーに、XML形式のイベント通知の詳細とともにHTTP POST要求を送信します。

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を使用できます。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、および認証を提供します。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クライアントとWebhook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または保護されません。設定の詳細については、を参照してください"[Webフックの転送先でHTTPを使用するための設定](#)"。

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WebhookアプリケーションサーバのIDを検証するために使用されます。また、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、両方の当事者によって使用されます。設定の詳細については、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](#)"。

相互認証を使用するHTTPS

Webフ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ことで、HTTPSセキュリティをさらに強化できます。WebhookアプリケーションサーバのIDを検証し、ネットワークトラフィックを保護するONTAPに加えて、WebhookアプリケーションはONTAPクライアントのIDを検証します。この双方向ピア認証は、`_Mutual TLS_`と呼ばれています。設定の詳細については、を参照してください"[相互認証でHTTPSを使用するようにWebhookの宛先を設定する](#)"。

関連情報

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

Webフックの転送先でHTTPを使用するための設定

HTTPを使用してWebフックアプリケーションにイベント通知を転送するようにONTAPを設定できます。これはセキュリティが最も低いオプションですが、設定が最も簡単です。

手順

1. イベントを受信する新しい送信先を作成し `restapi-ems` ます。

```
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. フィルタと `restapi-ems`宛先をリンクする通知を作成し `important-events` ます。

```
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、Webhook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。

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する

- ルート証明書をONTAPにインストールできるようにする

手順

1. Webhookアプリケーションをホストするサーバーに、適切なサーバー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. ONTAPにサーバルート証明書をインストールします。

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

コマンドは証明書を要求します。

3. イベントを受信する送信先を作成し `restapi-ems` ます。

```
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. フィルタと新しい `restapi-ems`宛先をリンクする通知を作成し `important-events` ます。

```
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の宛先を設定する

相互認証を使用してHTTPSを使用してWebhookアプリケーションにイベント通知を転送するように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Webhook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。さらに、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。

開始する前に

ONTAPを設定する前に、次の作業を行う必要があります。

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

手順

1. タスクの最初の2つの手順を実行し["HTTPSを使用するようにWebhookの宛先を設定する"](#)でサーバ証明書をインストールし、ONTAPがサーバのIDを確認できるようにします。
2. Webhookアプリケーションに適切なルート証明書と中間証明書をインストールして、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
```

コマンドは秘密鍵と証明書を要求します。

4. イベントを受信する送信先を作成し `restapi-ems` ます。

```
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. フィルタと新しい `restapi-ems`宛先をリンクする通知を作成し `important-events` ます。

```
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。