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

EMSの設定ワークフロー

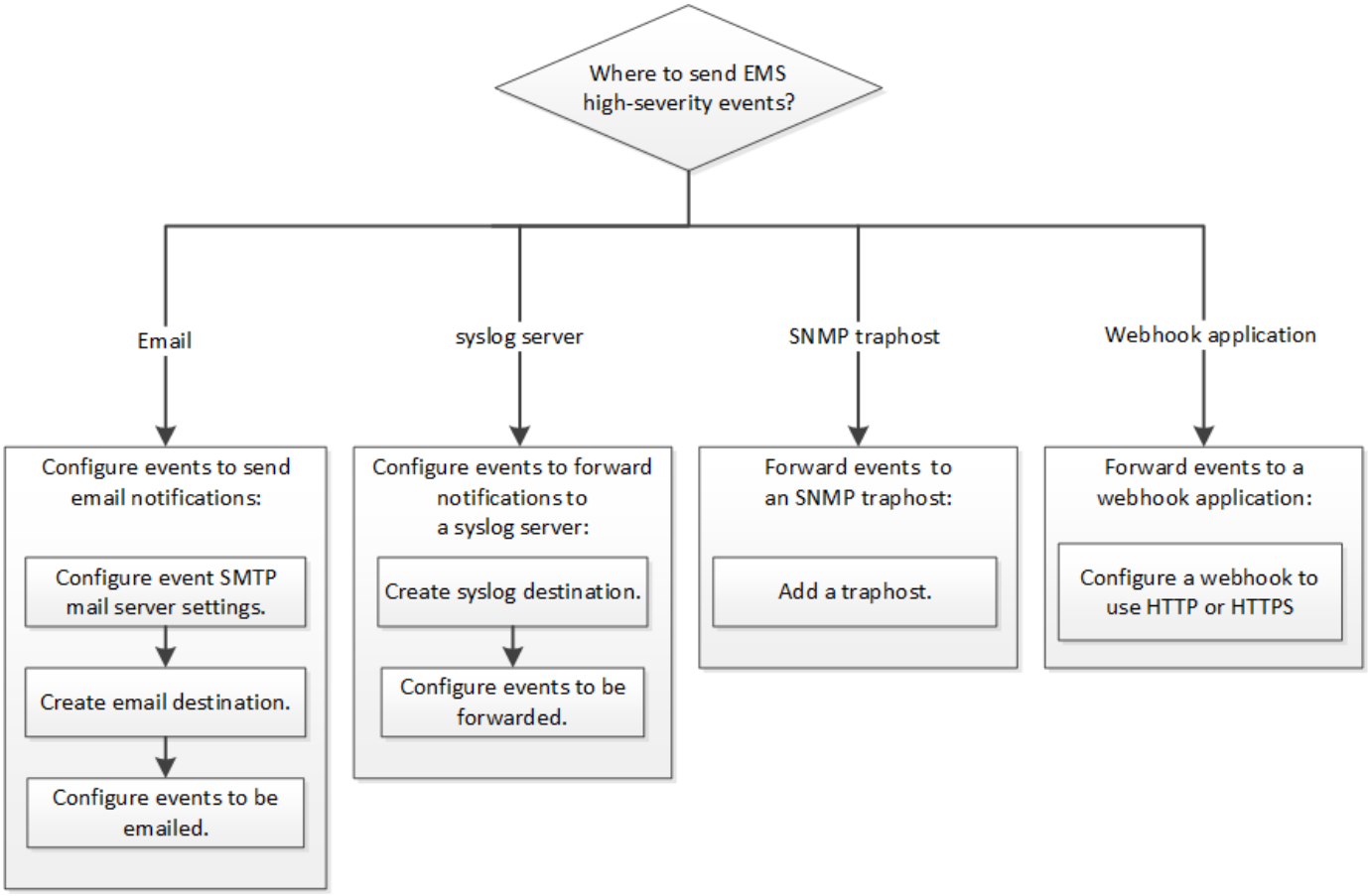
重要なEMSイベント通知は、Eメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebフックアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

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
   ```