# EMSノセツテイ

ONTAP 9

NetApp
April 24, 2024

# 目次

# EMSノセツテイ

## EMS設定の概要

早急な対応が必要なシステムの問題をすぐに通知するように、イベント管理システム（EMS）の重要なイベント通知をEメールアドレス、syslogサーバ、簡易管理ネットワークプロトコル（SNMP）トラップホスト、またはWebhookアプリケーションに直接送信するようにONTAP 9を設定できます。

重要なイベント通知はデフォルトでは有効になっていないため、Eメールアドレス、syslogサーバ、SNMPトラップホスト、またはWebhookアプリケーションのいずれかに通知を送信するようにEMSを設定する必要があります。

のリリース固有のバージョンを確認します "ONTAP 9 EMSリファレンス"。

EMSイベントのマッピングで廃止されたONTAP コマンドセット（イベントの送信先、イベントルートなど）を使用している場合は、マッピングを更新することを推奨します。 "廃止されたONTAP コマンドからEMSマッピングを更新する方法について説明します"。

## System Manager で EMS イベントの通知とフィルタを設定します

System Manager を使用して、早急な対応を要するシステムの問題を通知するために、Event Management System （ EMS ；イベント管理システム）でのイベント通知の配信方法を設定できます。

| ONTAPバージョン | System Manager で実行できる作業 |
|---|---|
| ONTAP 9.12.1以降 | リモートsyslogサーバにイベントを送信するときに、Transport Layer Security（TLS）プロトコルを指定します。 |
| ONTAP 9.10.1 以降 | SNMPトラップホストに加え、Eメールアドレス、syslogサーバ、Webフックアプリケーションを設定します。 |
| ONTAP 9.7 から 9.10.0 | SNMP トラップホストのみを設定する。 ONTAP CLI を使用して他の EMS デスティネーションを設定できます。 を参照してください "EMS設定の概要"。 |

次の手順を実行できます。

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]

- [delete-ems-filter]

関連情報

- "ONTAP EMSリファレンス"
- "CLI を使用して、イベント通知を受信する SNMP トラップホストを設定します"

## EMS イベント通知の送信先を追加します

System Manager を使用して、 EMS メッセージの送信先を指定できます。

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。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. **[Cluster] > [Settings]** の順にクリックします。
2. [*Notifications Management] セクションで、をクリックします ⋮をクリックし、 * イベントの送信先の表示 * をクリックします。
3. [* 通知管理 **]** ページで、 **[** イベントの送信先 *] タブを選択します。
4. をクリックします + Add 。
5. 名前、 EMS デスティネーションタイプ、およびフィルタを指定します。

   ⓘ 必要に応じて、新しいフィルタを追加できます。 [ 新しいイベントフィルタの追加 *] をクリックします。

6. 選択した EMS デスティネーションのタイプに応じて、次の情報を指定します。

| 構成する | 指定または選択 … |
|---|---|
| SNMP トラップホスト | • トラップホスト名 |
| E メール<br><br>（ 9.10.1 以降） | • 送信先 E メールアドレス<br>• メールサーバ<br>• 送信元 E メールアドレス |
| syslog サーバ<br><br>（ 9.10.1 以降） | • サーバのホスト名または IP アドレス<br>• Syslogポート（9.12.1以降）<br>• Syslog転送（9.12.1以降）<br><br>TCP Encrypted を選択すると、**Transport Layer Security（TLS）**プロトコルが有効になります。**syslog**ポート*に値を入力しない場合は、「 Syslog transport *」の選択に基づいてデフォルトが使用されます。 |

| | |
|---|---|
| ウェブフック<br><br>（ 9.10.1 以降） | • webhook URL<br>• クライアント認証（クライアント証明書を指定する場合はこのオプションを選択します） |

## 新しい **EMS** イベント通知フィルタを作成します

ONTAP 9.10.1 以降の System Manager を使用して、 EMS 通知の処理ルールを指定する、カスタマイズされた新しいフィルタを定義できます。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [ * イベント・フィルタ * ] タブを選択します。
4. をクリックします ＋ Add 。
5. 名前を指定し、既存のイベントフィルタからルールをコピーするか、新しいルールを追加するかを選択します。
6. 選択した手順に応じて、次の手順を実行します。

| 選択した場合 | 次に、次の手順を実行します。 |
|---|---|
| • 既存のイベントフィルタからルールをコピー * | 1. 既存のイベントフィルタを選択します。<br>2. 既存のルールを変更します。<br>3. 必要に応じて、をクリックして他のルールを追加します ＋ Add 。 |
| • 新しいルールを追加 * | 新しいルールごとに、タイプ、名前パターン、重大度、および SNMP トラップのタイプを指定します。 |

## **EMS** イベント通知の送信先を編集します

ONTAP 9.10.1 以降では、 System Manager を使用してイベント通知の送信先情報を変更できます。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [*Notifications Management] セクションで、をクリックします ⋮をクリックし、 * イベントの送信先の表示 * をクリックします。
3. [**Notifications Management]** ページで、 **[*Events Destinations**] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします ⋮をクリックし、 * 編集 * をクリックします。
5. イベントの送信先情報を変更し、 * 保存 * をクリックします。

## EMS イベント通知フィルタを編集します

ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを変更して、イベント通知の処理方法を変更できるようになりました。

システム定義のフィルタは変更できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [ * イベント・フィルタ * ] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします ⋮をクリックし、 * 編集 * をクリックします。
5. イベントフィルタの情報を変更し、 [ 保存（ Save ） ] をクリックします。

## EMS イベント通知の送信先を削除します

ONTAP 9.10.1 以降の場合、 System Manager を使用して EMS イベント通知の送信先を削除できます。

SNMP 送信先は削除できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 **]** ページで、 **[** イベントの送信先 *] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします ⋮をクリックし、*[削除]*をクリックします。

## EMS イベント通知フィルタを削除します

ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを削除できるようになりました。

システム定義のフィルタは削除できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [ * イベント・フィルタ * ] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします ⋮をクリックし、 * 削除 * をクリックします。

# 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

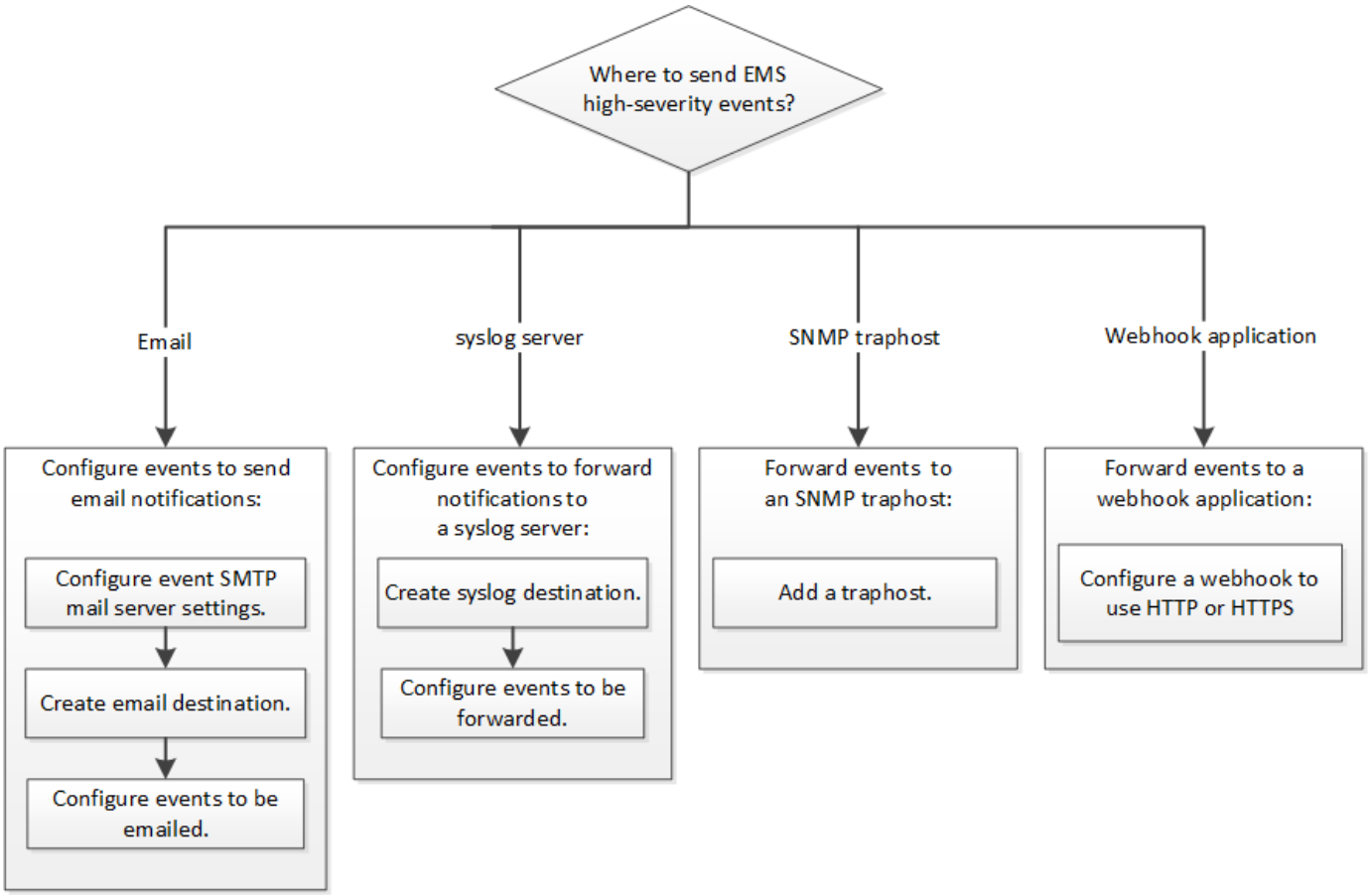
重要なEMSイベント通知は、Eメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebフックアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

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
```

# 廃止された **EMS** イベントマッピングを更新します

## **EMS** イベントのマッピングモデル

ONTAP 9.0 よりも前のバージョンでは、 EMS イベントはイベント名のパターンマッチングに基づいてイベントデスティネーションにのみマッピングできました。ONTAP コマンドセット (`event destination`、 `event route`）は、最新バージョンのONTAP でも引き続きこのモデルを使用できますが、ONTAP 9.0以降では廃止されています。

ONTAP 9.0以降ではONTAP 、拡張性に優れたイベントフィルタモデルを使用して、を使用して複数のフィールドに対してパターンマッチングを実行することを推奨します `event filter`、 `event notification`` および `event notification destination` コマンドセット。

廃止されたコマンドを使用してEMSマッピングが設定されている場合は、を使用するようにマッピングを更新する必要があります `event filter`、 `event notification``および `event notification destination` コマンドセット。

イベントの送信先には、次の 2 種類があります。

1. * システムで生成される送信先 * ：システムで生成される 5 つのイベントの送信先があります（デフォルトで作成）。
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     システムで生成される宛先の一部は、特別な目的に使用されます。たとえば、 ASUP デスティネーションは、 callhome.* イベントを ONTAP の AutoSupport モジュールにルーティングして AutoSupport メッセージを生成します。

2. ユーザが作成した送信先：を使用して手動で作成します `event destination create` コマンドを実行します

```
cluster-1::event*> destination show
                                                                      Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
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.
```

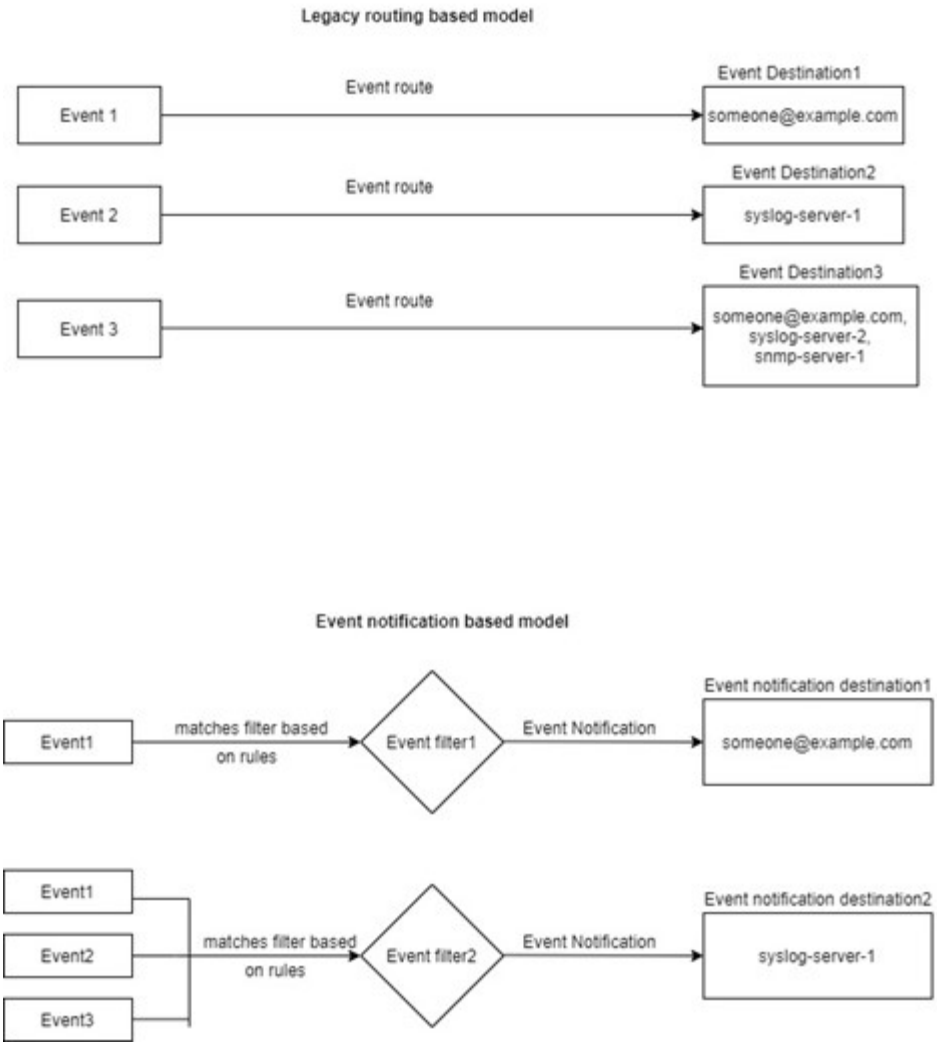
廃止されたモデルでは、EMSイベントはを使用して個別にデスティネーションにマッピングされます `event route add-destinations` コマンドを実行します

```
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.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
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.
```

拡張性に優れた新しい EMS イベント通知メカニズムは、イベントフィルタとイベント通知の送信先に基づいています。新しいイベント通知メカニズムの詳細については、次の技術情報アーティクルを参照してください。

- "ONTAP 9 のイベント管理システムの概要"




## 廃止された **ONTAP** コマンドから **EMS** イベントマッピングを更新します

廃止されたONTAP コマンドセットを使用してEMSイベントマッピングが設定されている場合 (`event destination`、 `event route`を使用するには、この手順 に従ってマッピングを更新する必要があります `event filter`、 `event notification`および `event notification destination` コマンドセット。

手順

1. を使用して、システム内のすべてのイベントの送信先を一覧表示します `event destination show` コマンドを実行します

```
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. 各送信先について、を使用してマッピングされているイベントを一覧表示します `event route show -destinations <destination name>` コマンドを実行します

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                           Severity       Destinations   Threshd
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. 対応するを作成します `event filter` これには、これらすべてのイベントのサブセットが含まれます。たとえば、のみを含める場合などです `raid.aggr.*`イベントの場合は、にワイルドカードを使用します `message-name` フィルタ作成時のパラメータ。単一のイベントに対するフィルタを作成することもできます。

> 最大 50 個のイベントフィルタを作成できます。

```
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. を作成します `event notification destination` をクリックします `event destination` エンドポイント（SMTP、SNMP、syslogなど）

```
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.
```

5. イベントフィルタをイベント通知の送信先にマッピングして、イベント通知を作成します。

```
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. それぞれについて、手順1 ~ 5を繰り返します `event destination` が搭載されています `event route`

マッピング：

> SNMPの送信先にルーティングされたイベントは、にマッピングする必要があります `snmp-traphost` イベント通知の送信先。SNMP トラップホストの送信先では、システムで設定された SNMP トラップホストを使用します。

```
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?: -
```