EMS配置

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/error-messages/index.html on February 12, 2026. Always check docs.netapp.com for the latest.

目录

EMS配置 1
- 了解ONTAP EMS配置 1
- 使用System Manager配置ONTAP EMS事件通知和筛选器 1
  - 添加 EMS 事件通知目标 1
  - 创建新的 EMS 事件通知筛选器 2
  - 编辑 EMS 事件通知目标 3
  - 编辑 EMS 事件通知筛选器 3
  - 删除 EMS 事件通知目标 3
  - 删除 EMS 事件通知筛选器 4
- 使用 CLI 配置 EMS 事件通知 4
  - ONTAP EMS配置工作流 4
  - 配置重要的ONTAP EMS事件以发送电子邮件通知 5
  - 配置重要的ONTAP EMS事件以将通知转发到系统日志服务器 6
  - 配置ONTAP SNMP陷阱主机以接收事件通知 7
  - 配置重要的ONTAP EMS事件以将通知转发到webhook应用程序 8
- 更新已弃用的 EMS 事件映射 10
  - 了解ONTAP EMS事件映射模型 10
  - 从已弃用的命令更新ONTAP EMS事件映射 14

EMS配置

了解ONTAP EMS配置

您可以将ONTAP 9配置为将重要的EMS (事件管理系统)事件通知直接发送到电子邮件地址、系统日志服务器、简单管理网络协议(SNMP)陷阱主机或webhook应用程序、以便您可以立即收到需要立即引起关注的系统问题的通知。

由于默认情况下不会启用重要事件通知、因此您需要将EMS配置为向电子邮件地址、系统日志服务器、SNMP陷阱主机或webhook应用程序发送通知。

查看特定于版本的 "《ONTAP 9 EMS参考》"。

如果EMS事件映射使用已弃用的ONTAP 命令集(例如事件目标、事件路由)、则建议您更新映射。"了解如何使用已弃用的ONTAP 命令更新EMS映射"(英文)

使用System Manager配置ONTAP EMS事件通知和筛选器

您可以使用 System Manager 配置事件管理系统（ Event Management System ， EMS ）发送事件通知的方式，以便在出现需要及时关注的系统问题时收到通知。

ONTAP 版本	使用 System Manager ，您可以 …
ONTAP 9.12.1及更高版本	将事件发送到远程系统日志服务器时、请指定传输层安全(TLS)协议。
ONTAP 9.10.1 及更高版本	配置电子邮件地址、系统日志服务器和webhook应用程序以及SNMP陷阱主机。
ONTAP 9.10.0 至 9.7	仅配置 SNMP 陷阱主机。 您可以使用 ONTAP 命令行界面配置其他 EMS 目标。 请参见 "EMS配置概述"。

添加 EMS 事件通知目标

您可以使用 System Manager 指定 EMS 消息要发送到的位置。

从ONTAP 9.12.1开始、可以通过传输层安全(Transport Layer Security、TLS)协议将EMS事件发送到远程系统日志服务器上的指定端口。有关的详细信息 `event notification destination create`，请参见"ONTAP命令参考"。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。
4. 单击 + Add 。

5. 指定名称， EMS 目标类型和筛选器。

   如果需要，您可以添加新筛选器。 单击 * 添加新事件筛选器 * 。

6. 根据您选择的 EMS 目标类型，指定以下内容：

配置…	指定或选择…
SNMP 陷阱主机	• TrapHost 名称
email （从 9.10.1 开始）	• 目标电子邮件地址 • 邮件服务器 • 发件人电子邮件地址
系统日志服务器 （从 9.10.1 开始）	• 服务器的主机名或 IP 地址 • 系统日志端口(从9.12.1开始) • 系统日志传输(从9.12.1开始) 选择* TCP加密*将启用传输层安全(TLS)协议。如果没有为*系统日志端口*输入任何值、则会根据*系统日志传输*选项使用默认值。
网络钩 （从 9.10.1 开始）	• webhook URL • 客户端身份验证（选择此选项可指定客户端证书）

创建新的 EMS 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 定义新的自定义筛选器，以指定处理 EMS 通知的规则。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 单击 + Add 。
5. 指定一个名称，然后选择是要从现有事件筛选器复制规则还是添加新规则。
6. 根据您的选择，执行以下步骤：

如果选择… 。	然后，执行以下步骤…

• 从现有事件筛选器复制规则 *	1. 选择现有事件筛选器。 2. 修改现有规则。 3. 如果需要，可通过单击来添加其他规则 + Add 。
• 添加新规则 *	为每个新规则指定类型，名称模式，严重性和 SNMP 陷阱类型。

编辑 EMS 事件通知目标

从 ONTAP 9.10.1 开始，您可以使用 System Manager 更改事件通知目标信息。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。
4. 在事件目标的名称旁边，单击，然后单击 ⋮**Edit**。
5. 修改事件目标信息，然后单击 * 保存 * 。

编辑 EMS 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 修改自定义筛选器以更改事件通知的处理方式。

ⓘ 您不能修改系统定义的筛选器。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 在事件过滤器的名称旁边，单击，然后单击 ⋮**Edit**。
5. 修改事件筛选器信息，然后单击 * 保存 * 。

删除 EMS 事件通知目标

从 ONTAP 9.10.1 开始，您可以使用 System Manager 删除 EMS 事件通知目标。

ⓘ 您不能删除 SNMP 目标。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ⋮，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件目标 * 选项卡。

4. 在事件目标的名称旁边，单击，然后单击 **Delete**。

删除 EMS 事件通知筛选器

从 ONTAP 9.10.1 开始，您可以使用 System Manager 删除自定义筛选器。

您不能删除系统定义的筛选器。

步骤

1. 单击 * 集群 > 设置 * 。
2. 在*Notification Management*部分中，单击 ，然后单击*View Event目的地*。
3. 在 * 通知管理 * 页面上，选择 * 事件筛选器 * 选项卡。
4. 在事件过滤器的名称旁边，单击，然后单击 **Delete**。

相关信息

- "《ONTAP EMS参考》"
- "使用 CLI 配置 SNMP 陷阱主机以接收事件通知"

使用 CLI 配置 EMS 事件通知

ONTAP EMS配置工作流

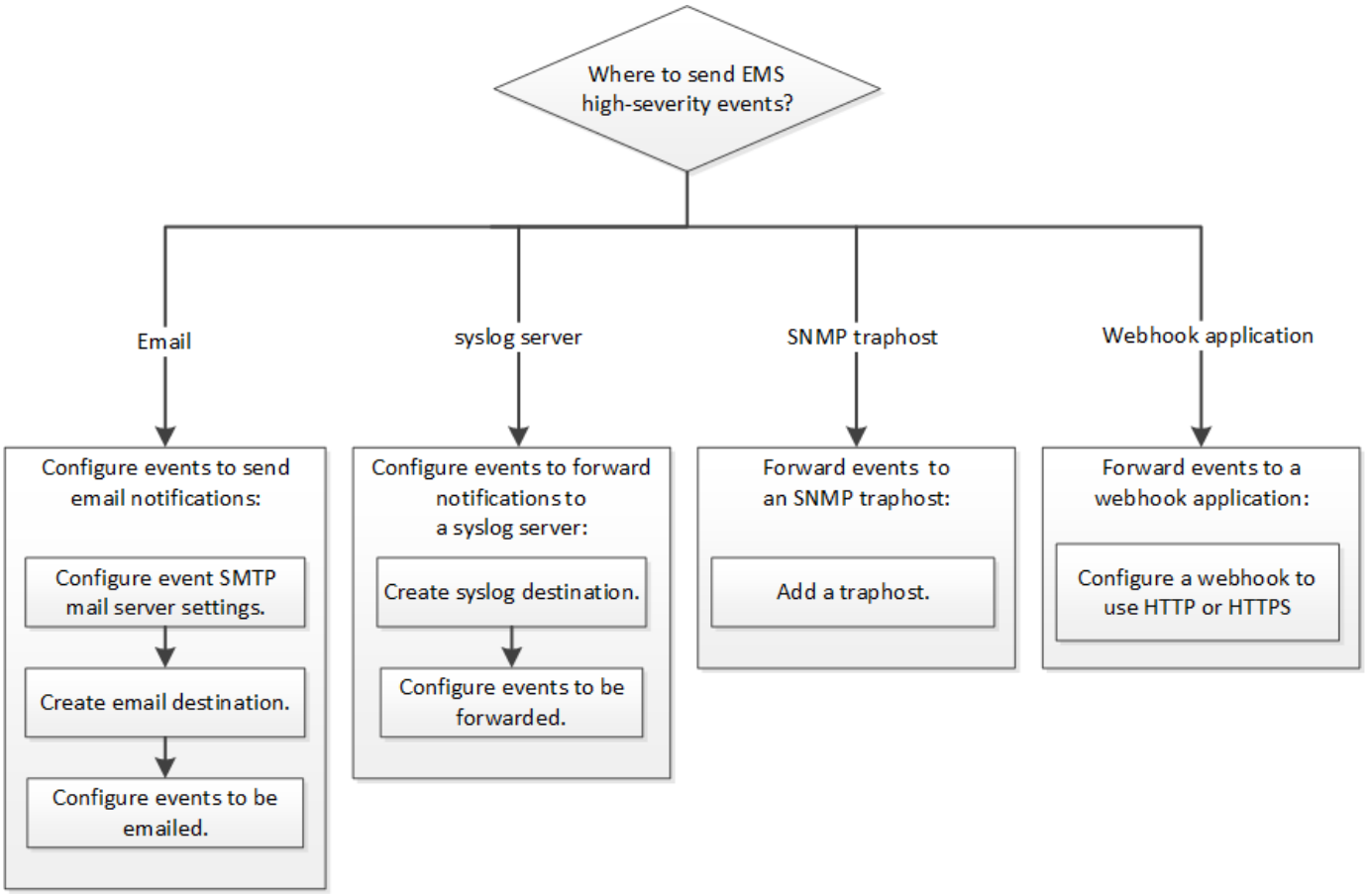
您必须将重要的EMS事件通知配置为以电子邮件形式发送、转发到系统日志服务器、转发到SNMP陷阱主机或转发到webhook应用程序。这有助于您及时采取更正操作，避免系统中断。

关于此任务

如果您的环境已包含用于聚合其他系统（例如服务器和应用程序）中记录的事件的系统日志服务器，则使用该系统日志服务器也可以更方便地从存储系统发出重要事件通知。

如果您的环境尚未包含系统日志服务器，则使用电子邮件发送重要事件通知会更方便。

如果您已将事件通知转发到 SNMP 陷阱主机，则可能需要监控该陷阱主机以查看重要事件。



选项

- 设置 EMS 以发送事件通知。

如果您希望 …	请参见 …
用于向电子邮件地址发送重要事件通知的 EMS	配置重要的 EMS 事件以发送电子邮件通知
用于将重要事件通知转发到系统日志服务器的 EMS	配置重要的 EMS 事件以将通知转发到系统日志服务器
希望 EMS 将事件通知转发到 SNMP 陷阱主机	配置 SNMP 陷阱主机以接收事件通知
希望EMS将事件通知转发到webhook应用程序	配置重要的EMS事件以将通知转发到webhook应用程序

配置重要的ONTAP EMS事件以发送电子邮件通知

要接收最重要事件的电子邮件通知，您必须将 EMS 配置为针对表示重要活动的事件发送电子邮件消息。

开始之前

要解析电子邮件地址，必须在集群上配置 DNS 。

关于此任务

您可以在集群运行时随时通过在 ONTAP 命令行上输入命令来执行此任务。

步骤

1. 配置事件 SMTP 邮件服务器设置：

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

   有关的详细信息 `event config modify`，请参见"ONTAP 命令参考"。

2. 为事件通知创建电子邮件目标：

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

   有关的详细信息 `event notification destination create`，请参见"ONTAP 命令参考"。

3. 配置重要事件以发送电子邮件通知：

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

   有关的详细信息 `event notification create`，请参见"ONTAP 命令参考"。

配置重要的ONTAP EMS事件以将通知转发到系统日志服务器

要在系统日志服务器上记录最严重事件的通知，您必须配置 EMS 以转发用于表示重要活动的事件的通知。

开始之前

要解析系统日志服务器名称，必须在集群上配置 DNS 。

关于此任务

如果您的环境尚未包含用于发送事件通知的系统日志服务器，则必须先创建一个。如果您的环境已包含一个用于记录其他系统中的事件的系统日志服务器，则您可能需要使用该服务器来发送重要事件通知。

您可以在集群运行时随时在ONTAP 命令行界面上输入命令来执行此任务。

从ONTAP 9.12.1开始、可以通过传输层安全(Transport Layer Security、TLS)协议将EMS事件发送到远程系统日志服务器上的指定端口。有两个新参数可用：

`tcp-encrypted`

时间 `tcp-encrypted` 已为指定 `syslog-transport`、ONTAP 通过验证目标主机的证书来验证其身份。默认值为 `udp-unencrypted`。

`syslog-port`

默认值 `syslog-port` 参数取决于的设置 `syslog-transport` 参数。条件 `syslog-transport` 设置为 `tcp-encrypted`， `syslog-port` 具有默认值6514。

步骤

1. 为重要事件创建系统日志服务器目标：

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

   从ONTAP 9.12.1开始、可以为指定以下值 `syslog-transport`：

   - `udp-unencrypted` —无安全性的用户数据报协议
   - `tcp-unencrypted` —传输控制协议无安全性
   - `tcp-encrypted` —传输层安全传输控制协议(TLS)

     默认协议为 `udp-unencrypted`。

   有关的详细信息 `event notification destination create`，请参见"ONTAP 命令参考"。

2. 配置重要事件以将通知转发到系统日志服务器：

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

   有关的详细信息 `event notification create`，请参见"ONTAP 命令参考"。

配置ONTAP SNMP陷阱主机以接收事件通知

要在 SNMP 陷阱主机上接收事件通知，必须配置陷阱主机。

开始之前

- 必须在集群上启用 SNMP 和 SNMP 陷阱。

  默认情况下， SNMP 和 SNMP 陷阱处于启用状态。

- 要解析陷阱主机名称，必须在集群上配置 DNS 。

关于此任务

如果尚未将 SNMP 陷阱主机配置为接收事件通知（ SNMP 陷阱），则必须添加一个。

您可以在集群运行时随时通过在 ONTAP 命令行上输入命令来执行此任务。

步骤

1. 如果您的环境尚未配置 SNMP 陷阱主机以接收事件通知，请添加一个：

   `system snmp traphost add -peer-address snmp_traphost_name`

   默认情况下， SNMP 支持的所有事件通知都会转发到 SNMP 陷阱主机。

配置重要的ONTAP EMS事件以将通知转发到webhook应用程序

您可以将ONTAP 配置为将重要事件通知转发到webhook应用程序。所需的配置步骤取决于您选择的安全性级别。

准备配置EMS事件转发

在配置ONTAP 将事件通知转发到webhook应用程序之前、您应考虑几个概念和要求。

webhook应用程序

您需要一个能够接收ONTAP 事件通知的webhook应用程序。webhook是用户定义的回调例程、用于扩展运行它的远程应用程序或服务器的功能。客户端(在本例中为ONTAP)通过向目标URL发送HTTP请求来调用或激活webhooks。具体而言、ONTAP 会向托管webhook应用程序的服务器发送HTTP POST请求以及XML格式的事件通知详细信息。

安全选项

根据传输层安全(Transport Layer Security、TLS)协议的使用方式、有多个安全选项可用。您选择的选项将确定所需的ONTAP 配置。

TLS是一种加密协议、在互联网上广泛使用。它使用一个或多个公有 密钥证书提供隐私以及数据完整性和身份验证。证书由可信证书颁发机构颁发。

HTTP

您可以使用HTTP传输事件通知。使用此配置时、连接不安全。不会验证ONTAP 客户端和webhook应用程序的身份。此外、网络流量不会加密或受到保护。请参见 "配置webhook目标以使用HTTP" 以获取配置详细信息。

HTTPS

为了提高安全性、您可以在托管webhook例程的服务器上安装证书。ONTAP 使用HTTPS协议来验证webhook应用程序服务器的身份、双方也使用此协议来确保网络流量的隐私和完整性。请参见 "将网络挂机目标配置为使用HTTPS" 以获取配置详细信息。

使用HTTPS进行相互身份验证

您可以通过在发出webbook请求的ONTAP 系统上安装客户端证书来进一步增强HTTPS安全性。除了ONTAP验证webhook应用程序服务器的身份并保护网络流量之外、webhook应用程序还会验证ONTAP 客户端的身份。这种双向对等身份验证称为_mutual tls_.请参见 "配置一个webhook目标以使用HTTPS进行相互身份验证" 以获取配置详细信息。

相关信息

- "传输层安全(TLS)协议版本1.3"

配置webhook目标以使用HTTP

您可以将ONTAP 配置为使用HTTP将事件通知转发到webhook应用程序。这是最不安全的选项、但设置最简单。

步骤

1. 创建新目标 `restapi-ems` 要接收事件、请执行以下操作：

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

在上述命令中、必须对目标使用* HTTP *方案。

有关的详细信息 `event notification destination create`，请参见"ONTAP 命令参考"。

2. 创建一个通知以链接 `important-events` 使用进行筛选 `restapi-ems` 目标：

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

有关的详细信息 `event notification create`，请参见"ONTAP 命令参考"。

将网络挂机目标配置为使用**HTTPS**

您可以将ONTAP配置为使用HTTPS将事件通知转发到webhook应用程序。ONTAP 使用服务器证书来确认webhook应用程序的身份并保护网络流量。

开始之前

- 为webhook应用程序服务器生成专用密钥和证书
- 准备好可在ONTAP 中安装的根证书

步骤

1. 在托管webhook应用程序的服务器上安装相应的服务器专用密钥和证书。具体的配置步骤取决于服务器。
2. 在ONTAP 中安装服务器根证书：

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

命令将要求提供证书。

3. 创建 `restapi-ems` 接收事件的目标：

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

在上述命令中，必须对目标使用*HTTPS*方案。

4. 创建用于链接的通知 `important-events` 使用新进行筛选 `restapi-ems` 目标：

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

配置一个**webhook**目标以使用**HTTPS**进行相互身份验证

您可以将ONTAP 配置为使用HTTPS并通过相互身份验证将事件通知转发到webhook应用程序。在此配置中、有两个证书。ONTAP 使用服务器证书确认webhook应用程序的身份并保护网络流量。此外、托管webhook的应用程序使用客户端证书来确认ONTAP 客户端的身份。

开始之前

在配置ONTAP 之前、必须执行以下操作：

- 为webhook应用程序服务器生成专用密钥和证书
- 准备好可在ONTAP 中安装的根证书
- 为ONTAP 客户端生成专用密钥和证书

步骤

1. 执行任务中的前两个步骤 "将网络挂机目标配置为使用HTTPS" 安装服务器证书、以便ONTAP 可以验证服务器的身份。
2. 在webhook应用程序中安装相应的根证书和中间证书以验证客户端证书。
3. 在ONTAP 中安装客户端证书：

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

   命令将要求提供私钥和证书。

4. 创建 `restapi-ems` 接收事件的目标：

   ```
   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、必须对目标使用* HTTPS *方案。

5. 创建用于链接的通知 `important-events` 使用新进行筛选 `restapi-ems` 目标：

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

相关信息

- "安全证书安装"

更新已弃用的 EMS 事件映射

了解ONTAP EMS事件映射模型

在 ONTAP 9.0 之前的版本中，只能根据事件名称模式匹配将 EMS 事件映射到事件目标。ONTAP命令集 (`event destination， event route`)使用此模型的版本在最新版本的ONTAP中仍然可用、但从ONTAP 9.0开始已弃用。

从ONTAP 9.0开始、ONTAP EMS事件目标映射的最佳实践是使用可扩展性更强的事件筛选器模型、在该模型中、可以使用对多个字段执行模式匹配 `event filter， event notification`，和 `event notification destination` 命令集。

如果使用弃用的命令配置了EMS映射，则应更新映射以使用 `event filter、 event notification`和 `event notification destination`命令集。有关的详细信息 `event`，请参见"ONTAP 命令参考"。

事件目标有两种类型：

1. * 系统生成的目标 * ：系统生成的事件目标有五个（默认为创建）
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     系统生成的某些目标用于特殊目的。例如， asup 目标会将 CallHome.* 事件路由到 ONTAP 中的 AutoSupport 模块，以生成 AutoSupport 消息。
2. 用户创建的目标：这些目标是使用手动创建的 `event destination create` 命令：

```
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.
```

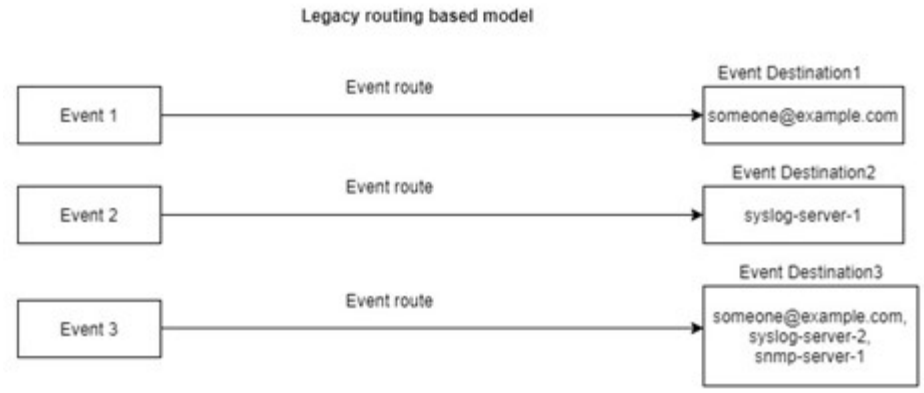
在已弃用的模型中、EMS事件会使用单独映射到目标 `event route add-destinations` 命令：

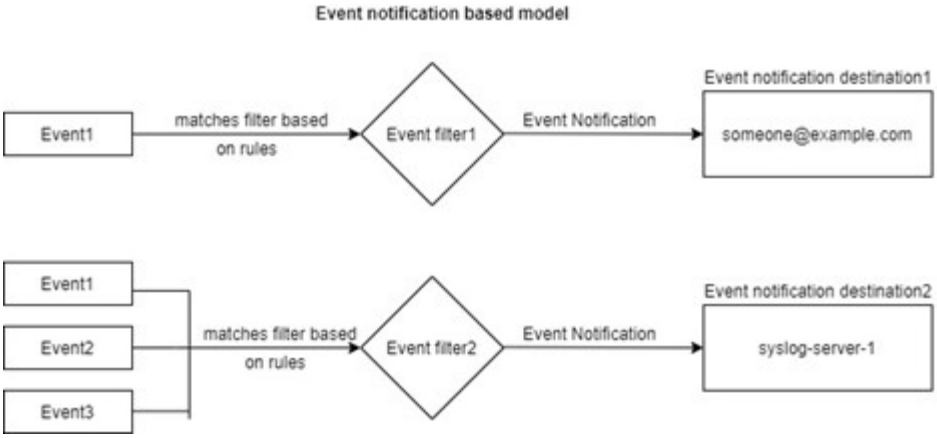
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

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.
```

更具可扩展性的新 EMS 事件通知机制基于事件筛选器和事件通知目标。有关新事件通知机制的详细信息，请参见以下知识库文章：

- "ONTAP 9 事件管理系统概述"





从已弃用的命令更新ONTAP EMS事件映射

当前使用已弃用的ONTAP命令集配置EMS事件映射时 (`event destination`， `event route`)、则应按照此操作步骤更新映射以使用 `event filter`， `event notification`，和 `event notification destination` 命令集。

步骤

1. 使用列出系统中的所有事件目标 `event destination show` 命令：

```
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. 对于每个目标、使用列出要映射到它的事件 `event route show -destinations <destination name>` 命令：

```
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. 创建相应的 `event filter` 其中包括所有这些事件子集。 例如、如果要仅包含 `raid.aggr.*`事件、请使用通配符作为 `message-name` 参数。您还可以为单个事件创建筛选器。

   有关的详细信息 `event filter`，请参见"ONTAP 命令参考"。

   您最多可以创建 50 个事件筛选器。

```
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. 创建 `event notification destination` 对于每个 `event destination` 端点(即SMP/SNMP/系统日志)

```
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.
```

有关和的 `event destination`详细信息 `event notification destination`，请参见"ONTAP 命令参考"。

5. 通过将事件筛选器映射到事件通知目标来创建事件通知。

```
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. 对每个重复步骤1-5 `event destination` 具有 `event route` 映射。

> 路由到SNMP目标的事件应映射到 `snmp-traphost` 事件通知目标。SNMP 陷阱主机目标使用系统配置的 SNMP 陷阱主机。

```
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?: -
```

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。