使用 CLI 配置 EMS 事件通知

ONTAP 9

NetApp
April 24, 2024

目录

使用 CLI 配置 EMS 事件通知

EMS配置工作流

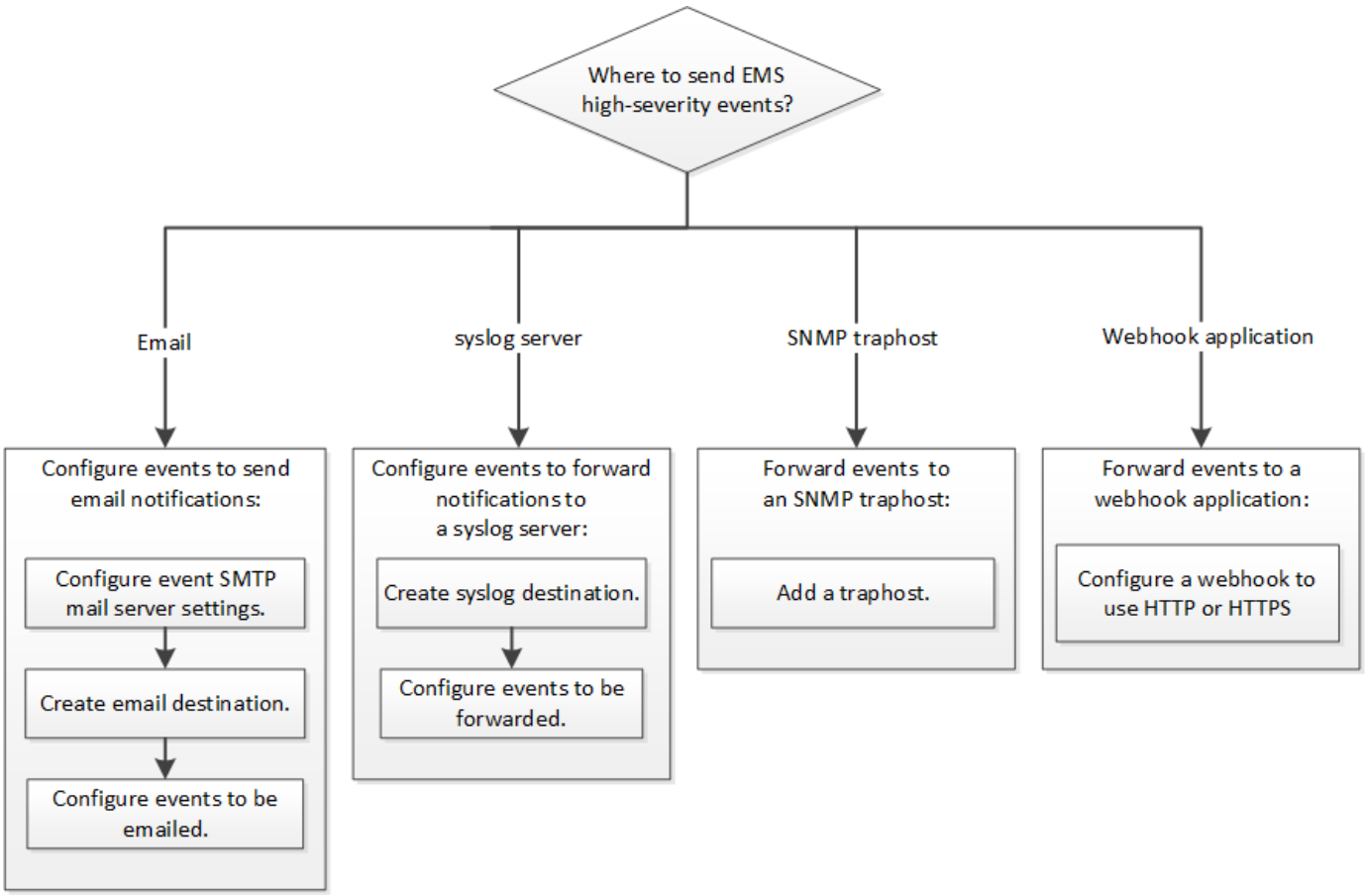
您必须将重要的EMS事件通知配置为以电子邮件形式发送、转发到系统日志服务器、转发到SNMP陷阱主机或转发到webhook应用程序。这有助于您及时采取更正操作，避免系统中断。

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 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。

您需要的内容

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
   ```

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
   ```

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
   ```

配置重要的 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。

您需要的内容

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。

有关详细信息，请参见 `event notification destination create` 手册页。

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`。

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`*

配置 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。

您需要的内容

- 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。

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
   ```

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
   ```