在SD-WAN cEdge路由器上执行安全出厂重置

目录

简介

本文档介绍运行Cisco IOS® XE的Cisco Catalyst SD-WAN边缘路由器的安全出厂重置过程。

背景

出厂重置将设备恢复至其原始制造状态，通常作为停用、重新部署或安全补救工作流程的一部分需要。

⚠ 警告：本文仅推荐`factory-reset all secure`选项，该选项执行与NIST SP 800-88 Rev. 1一致的数据清理。此方法使存储介质上的数据不可恢复，并提供已永久删除敏感数据的最高级别保证。

适用范围

运行Cisco IOS XE的以下平台支持`factory-reset all secure`命令：

- Cisco Catalyst 8200系列边缘平台
- Cisco Catalyst 8300系列边缘平台
- Cisco Catalyst 8500系列边缘平台
- Cisco ASR 1000系列聚合服务路由器(US)
- 思科ISR 4000系列集成多业务路由器
- Cisco ISR 1000系列集成多业务路由器

注意：`all secure`选项只能在独立设备上使用。通过检查`factory-reset`，验证您的平台和Cisco IOS XE版本是否支持`secure`关键字？在特权执行模式下运行。

先决条件

在执行安全出厂重置之前，请确保满足以下前提条件：

- 备份配置：在重置之前，从SD-WAN Manager(vManage)导出并安全地存储所有设备配置、模板和策略。
- 备份软件映像：在执行重置之前，请确保将Cisco IOS XE软件映像的副本加载到bootflash中。当`secure`选项在大多数平台上将引导镜像保留在闪存中时，某些平台将bootflash完全清理为安全擦除的一部分。作为应急方案，请务必在USB驱动器或可访问的TFTP服务器上提供Cisco IOS XE映像，以确保恢复不受平台行为的影响。
- 不间断电源：确保设备在整个重置过程中都使用不间断电源。在清理过程中断电可能导致设备无法恢复。
- 完成所有ISSU步骤：如果任何服务中软件升级(ISSU)操作处于待定或正在进行中，请在启动出厂重置之前完成这些操作。
- 版本HSEC许可证：在执行出厂重置之前，必须从设备中释放HSEC许可证。 按照“返回HSECK9许可证”部分所述，返回HSECK9许可证，网址为：在思科边缘路由器上配置HSECK9许可证
- 从SD-WAN交换矩阵删除：在vManage中使设备证书无效，并在执行重置之前从控制器重叠中删除设备。
- 控制台访问:确保您拥有对设备的物理控制台访问权限。重置后，设备进入ROMMON模式，并且VTY会话不可用。

提示：在执行出厂重置之前，请确认Cisco IOS XE映像已加载到bootflash 中，并且USB或TFTP上有恢复副本可用。虽然`secure`选项在大多数平台上保留引导映像，但某些平台会在

进程中完全清理Bootflash。

清除的内容

`factory-reset all secure`命令会永久从设备中移除此数据：

分类	已清除的数据
软件	所有Cisco IOS XE软件映像(当前引导映像保留在大多数平台的闪存中；但是，在某些平台上，bootflash被完全清理)
配置	启动配置，运行配置
日志和诊断	崩溃信息、系统日志、OBFL（板载故障记录）
安全材料	与FIPS相关的密钥和凭证、用户配置的PKI密钥和证书
存储	可移动存储(SATA、SSD、USB)上的所有用户数据
许可	所有设备许可证（需要重新注册）
ROMMON	用户添加的ROMMON环境变量

注意：在安全恢复出厂设置后，将保留以下项:

- SUDI（安全唯一设备标识符）证书和关联的PKI密钥
- 配置寄存器值
- 当前引导映像(保留在大多数平台的闪存中；在某些平台上，bootflash已完全清理 — 始终保留USB/TFTP恢复)

步骤:安全出厂重置

警告：此过程是不可逆的。启动后，永久销毁上表中列出的所有数据。继续之前，请确保所有备份都已验证。

步骤 1：通过控制台访问设备

通过物理控制台连接连接到设备。在重置过程中，SSH/VTY访问丢失。

步骤 2：进入特权执行模式

```
Device> enable
Device#
```

步骤 3：执行安全出厂重置

运行以下命令以启动安全出厂重置：

```
Device# factory-reset all secure
```

系统提示确认：

```
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
```

检查:在确认提示符下，最后一次验证以下内容：

- 已备份所有配置
- Cisco IOS XE恢复映像在USB或TFTP上可用
- 设备已从SD-WAN重叠中删除

键入y或按Enter确认并继续。

步骤 4：等待清理完成

设备对所有存储介质执行数据清理。此过程可能需要较长的时间，具体取决于存储容量。请勿在此操作期间中断电源。

完成后，设备会自动重新加载并进入ROMMON模式。

步骤 5：恢复ROMMON环境变量

重置后，可以清除包括MAC_ADDRESS和SERIAL_NUMBER在内的环境变量。执行ROMMON重置以恢复它们：

```
rommon 1> reset
```

注意：出厂重置后，波特率环境变量返回其默认值(9600)。如果您的控制台会话配置不同的波特率，您可以将终端仿真器设置调整为9600波特以重新获得控制台访问。

步骤 6：启动Cisco IOS XE软件映像

在大多数平台上，secure选项将引导映像保留在闪存中。使用dir bootflash:来自ROMMON。如果映像可用，请直接启动：

```
rommon 2> boot bootflash:<image-filename>.bin
```

平台特定的行为：在某些硬件平台上，安全清理过程会完全擦除bootflash，包括启动映像。在这些情况下，通过USB或TFTP恢复。

选项A — USB恢复：

```
rommon 2> boot usbflash0:<image-filename>.bin
```

选项B - TFTP恢复：

设置所需的ROMMON环境变量，然后启动传输：

```
rommon 2> IP_ADDRESS=

rommon 3> IP_SUBNET_MASK=

rommon 4> DEFAULT_GATEWAY=

rommon 5> TFTP_SERVER=

rommon 6> TFTP_FILE=

     .bin
rommon 7> tftpboot
```

> 验证通过管理接口或直连网段与TFTP服务器的连接是否可用。ROMMON不支持路由协议，因此TFTP服务器必须通过配置的默认网关访问。
>
> 在启动出厂重置之前始终在USB或可访问TFTP服务器上暂存恢复映像，以便解决此行为。

Post-Reset:重新注册到SD-WAN交换矩阵

使用干净的Cisco IOS XE映像恢复设备后，使用标准的SD-WAN自注册程序将设备重新引入交换矩阵：

1. 引导程序配置：应用初始引导程序配置（系统IP、站点ID、组织名称、vBond地址）。 有关过程，请参阅使用CLI生成引导程序文件。
2. 证书安装：按照证书颁发机构（Symantec/DigiCert、Cisco PKI或Enterprise CA）的要求安装设备证书和根CA链。
3. 控制连接：验证已建立到vManage、vSmart和vBond的DTLS/TLS控制连接。
4. 模板推送：在vManage中，将适当的设备模板或配置组附加到设备。
5. 验证：确认BFD会话、OMP路由和数据平面隧道运行正常。

注意：重新加入后，必须通过CLI手动重新应用HSEC（高安全性）许可证以恢复加密吞吐量。如Managing HSEC Licenses in Cisco Catalyst SD-WAN中所述，SD-WAN Manager(vManage)不支持在设备上重新安装HSEC许可证。要激活许可证，需要在物理路由器上重新加载设备。有关手动CLI过程，请参阅在思科边缘路由器上配置HSECK9许可证。

故障排除

控制台在重置后无响应

如果控制台在出厂重置完成后显示无响应，波特率可能已恢复为默认值(9600)。 将终端仿真器调整为9600波特并重新连接。

设备未进入ROMMON

如果设备在重置完成后未进入ROMMON，请验证配置寄存器设置正确。在大多数情况下，当不存在可引导映像时，电源循环会强制设备进入ROMMON。

ROMMON中缺少环境变量

如果在重置后缺少MAC_ADDRESS或SERIAL_NUMBER变量，请在ROMMON中发出reset命令以从硬件存储恢复出厂默认的环境变量。

常见问题解答

问:为什么建议使用“secure”选项而不是标准的“all”或“3-pass”选项？

A：factory-reset all secure选项执行可用的最彻底的数据清理，与NIST SP 800-88 Rev. 1保持一致。它使数据不可恢复并将当前启动映像保留在闪存中，简化了恢复。相比，3遍选项执行三遍覆盖模式（零、一、随机），这大约需要三倍时间，而且会擦除启动映像，需要从USB或TFTP重新加载完整映像。建议使用secure选项，因为它提供了最彻底的清理，并且恢复操作开销最低。

问:安全工厂重置需要多长时间？

A：持续时间因设备总存储容量而异。对于具有标准闪存(8-32 GB)的设备，此过程通常在15-45分钟内完成。具有较大的SSD或SATA存储的设备可能需要较长时间。重要信息：在此过程中请勿中断电源。规划一个维护窗口，考虑重置以及映像重新加载和重新加入时间。

问:重置后，设备是否保留其身份（序列号、SUDI）？

A：Yes.安全唯一设备标识符(SUDI)证书及其关联的PKI密钥存储在硬件保护存储（TAm/ACT2芯片）中，并且不通过出厂重置进行清除的。设备序列号也保存在硬件中。这意味着重置后，可以使用设备的原始标识将该设备重新注册到SD-WAN交换矩阵。

问:在执行重置之前，是否需要从SD-WAN Manager中删除设备？

A：Yes.强烈建议在执行出厂重置之前，使设备证书无效并从SD-WAN重叠中删除该设备。这可确保从控制器基础设施中完全删除，vManage设备资产中无陈旧条目，无孤立控制连接或隧道状态。从vManage:导航到Configuration > Certificates >选择设备> Invalidate，然后选择Send to Controllers。然后，从设备列表中删除设备。

问:出厂重置后HSEC许可证会发生什么情况？

A：HSEC（高安全性）许可证在出厂重置期间被删除。如果没有它，设备就会以受限的加密吞吐量运行。HSEC许可证必须在工厂重置之前发布，以便之后可以重复使用：

1. 重置前：通过许可证智能授权发布许可证，返回本地联机，并从智能许可证中心删除产品实例。
2. 重新注册后：通过CLI手动重新应用HSEC许可证。如Managing HSEC Licenses in Cisco Catalyst SD-WAN中所述，SD-WAN Manager(vManage)不支持重新安装HSEC许可证。
3. 重新加载：要激活许可证，需要在物理路由器上重新加载。
4. 通过`show license summary`和`show license authorization`进行验证。

有关完整过程，请参阅在思科边缘路由器上配置HSECK9许可证和在Cisco Catalyst SD-WAN中管理HSEC许可证。

问:是否可以远程执行安全出厂重置（通过SSH/VTY）？

A：虽然从技术上来说，命令可以通过SSH/VTY会话发出，但强烈建议不允许使用。设备立即开始清理，远程会话终止。重置后，设备进入ROMMON模式，在该模式下，没有IP连接可用，没有可能的VTY访问，并且需要控制台访问才能恢复映像。在启动出厂重置之前，始终确保物理控制台访问可用。

问:安全出厂重置是否适用于安全补救方案？

A：Yes.当设备在可疑危害后必须恢复为已知良好的状态时，建议使用安全出厂重置。这可确保所有攻击者植入的密钥、后门或持久性机制被永久删除，不保留任何残留的配置或凭证数据，并确保设备可以重新登录。对于与安全相关的出厂重置，请确保在重新登录期间生成新的凭证（密码、密钥、证书），并确保不将任何预危害备份配置恢复到设备中。

问:为什么不使用“请求平台软件sdwan软件重置”或“请求平台软件sdwan配置重置”？

A：这些命令的作用不同，并且不提供与出厂重置安全级别相同的清理级别。`request platform software sdwan software reset`命令重置SD-WAN软件重叠，但不擦除底层的Cisco IOS XE配置、密钥、证书或存储 — 设备保留其基本OS状态。`request platform software sdwan config reset`命令仅重置SD-WAN配置，但将Cisco IOS XE映像、本地凭证、SSH密钥和所有其他数据保留在磁盘上。这两个命令都不会对存储介质执行数据清理。如果目标是将设备恢复为完全干净的状态（特别是在安全事件之后），则这些命令不足，因为残余数据（密钥、凭证、日志、攻击者植入的文件）可以保留在闪存或SSD中。当必须保证设备在存储级别干净时，请使用`factory-reset all secure`。

参考

- Cisco Trustworthy Systems — 出厂重置指南
- 在思科边缘路由器上配置HSECK9许可证
- 在Cisco Catalyst SD-WAN中管理HSEC许可证
- 使用CLI生成Bootstrap文件 — SD-WAN入门指南
- 使用vManage GUI或CLI升级SD-WAN控制器

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。