# NXOS — 安全擦除磁盘内容

## 目录



## 简介

本文档介绍如何安全擦除使用标准Linux实用程序的Cisco Nexus交换机的磁盘。 这对于某些军事和政府客户将设备从安全区域移动到非安全区域，或者对于任何其他有合规性要求的客户将设备移出其场所而言是必要的。

## 背景信息

有两个选项取决于交换机是具有SSD还是eUSB驱动器：

- Init-System用于带SSD的较新型号交换机。Init-System使用ATA安全擦除将二进制0写入驱动器的所有扇区。
- 对于带eUSB驱动器的旧型号交换机，您也可以使用零字节擦除方法将0写入驱动器的所有扇区。

文档中的标准实用程序使用一系列命令来安全地销毁存储磁盘上的数据，而且在大多数情况下，这些命令会使恢复数据变得困难或不可能。

本指南将引导您完成Cisco Nexus 3000系列交换机、Cisco Nexus 5000系列交换机、Cisco Nexus 9000系列交换机、Cisco Nexus 7000系列交换机和Cisco MDS系列交换机的这两个流程，但适用于大多数其他Cisco Nexus交换机，前提是您有初始系统或bash access。 如果您运行的交换机或软件版本不支持启用**feature bash**以访问Bash外壳，请向Cisco TAC提交服务请求，以获取对此过程使用调试插件的帮助。

## 如何确定适合自己的程序？

如果PID返回值**0**，则系统使用SSD，并且可以使用Init-System方法擦除驱动器。

如果PID返回值**1**，则系统使用eUSB驱动器，您需要使用零字节擦除方法。

```
F340.23.13-C3064PQ-1# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
F340.23.13-C3064PQ-1(config)# feature bash-shell
```

```
F340.23.13-C3064PQ-1(config)#
F340.23.13-C3064PQ-1(config)# exit
F340.23.13-C3064PQ-1# run bash bash-4.2$ cat /sys/block/sda/queue/rotational 1
bash-4.2$
```

执行上述步骤后，如果尚不清楚系统中的驱动器类型以及安全擦除磁盘内容应使用的步骤，请向Cisco TAC提交服务请求。

# 准备

在擦除驱动器之前，您必须具备以下条件：

1. 控制台访问交换机。
2. 通过management0接口访问TFTP服务器 — 备份当前配置和恢复操作系统所必需的。
3. 在此过程中销毁运行配置和要从系统脱机保存的任何其他文件的备份！

**注意：**强烈建议您对不再在生产或安装在生产机箱中的部件执行此程序。在执行此程序之前，应将设备或部件移至非生产环境，以避免任何无意中的网络中断。

# 在带SSD的交换机上使用Init-System程序

**注意：**在基于模块的交换机内的Supervisor上执行此程序时，建议仅将您计划执行此程序的Supervisor安装在系统中。

1. 通过控制台连接时重新加载或重新通电交换机。

2. 当交换机启动时，使用CTRL-C将交换机中断到loader>提示符。

3. 在loader>提示符下，输入cmdline recoverymode=1。 这会在switch(boot)#提示符**下停止交换机**启动：

```
loader > cmdline recoverymode=1
```

4. 以boot bootflash:<nxos_filename.**bin>开始引导过程**。

```
loader > boot bootflash:nxos.7.0.3.I7.8.bin
```

5. 交换机引导至**switch(boot)#提**示符。 在此提示符下，使用clear nvram CLI和init system CLI将0写入nvram中除许可证块**外的**所有块**中。 注意：**本测试在N9K-C9372TX-E上进行，该N9K-C9372TX-E采用2.50GHz的英特尔酷睿i3- CPU和110G SSD。 初始化系统的总时间大约花费8秒：

```
switch(boot)# clear nvram
switch(boot)# init system This command is going to erase your startup-config, licenses as
well as the contents of your bootflash:. Do you want to continue? (y/n) [n] y
```

6. 完成步骤5后，重新加载交换机:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

# 在带eUSB的交换机/管理引擎/系统控制器上使用dd程序

1. 通过控制台端口登录到交换机的管理员帐户。

   **注意：**当您在基于模块的交换机内的Supervisor上执行此程序时，建议仅将您计划执行此程序的Supervisor安装在系统中。

2.从配置模**式启用功能**bash-shell，并使用运行bash进入Bash**提示符**（仅限N3K/9K）。 其他Cisco Nexus交换机需要调试插件才能访问Bash)。

```
F340.23.13-C3064PQ-1# config terminal
F340.23.13-C3064PQ-1(config)# feature bash-shell F340.23.13-C3064PQ-1(config)# exit
F340.23.13-C3064PQ-1# run bash
bash-4.2$

N7K-1# load n7000-s2-debug-sh.7.2.1.D1.1.gbin Loading plugin version 7.2(1)D1(1)
################################################################## Warning: debug-plugin is for
engineering internal use only! For security reason, plugin image has been deleted.
################################################################## Successfully loaded debug-
plugin!!! Linux(debug)#
```

3.使用sudo su获得根**访问权 —**

**注意：**对于使用此过程调试插件的Cisco Nexus 7000系列交换机，可跳过此步骤。

```
bash-4.2$ sudo su -
root@F340#
```

4.如果您在安装在Nexus 9000系列交换机中的系统控制器上执行此程序，则必须远程登录到要执行此程序的插槽编号。 例如，此处为插槽29中的系统控制器完成：

```
N9K-EOR# run bash bash-4.2$ sudo su - root@N9K-EOR#rlogin lc29 root@sc29:~#
```

5.使用fdisk -l检验每个磁盘的块大小。 在N3K-C3064PQ-10X上，它只有/dev/sda @ 512字节块大小，请参阅此处：

**注意：**在某些Cisco Nexus交换机上，可能不止一个磁盘。执行dd操作时，必须考虑它。例如，N7K-SUP2有/dev/sda、/dev/sdb、/dev/sdc/、/dev/md2、/dev/md3、/dev/md4、/dev/md5和/dev/md6。您必须对每个操作执行dd操作，以完成安全擦除过程正确。

**注意：**在Cisco Nexus 9000系列交换机上，系统控制器具有/dev/mtdblock0、/dev/mtdblock1、/dev/mtdblock2、/dev/mtdblock3、/dev/mtdblock4、**/dev/mtdblock5**和/dev/mtdblock6。 您必须对其中的每一项执行dd操作，才能正确完成安全擦除过程。

```
root@F340# fdisk -l

Disk /dev/sda: 2055 MB, 2055208960 bytes
64 heads, 62 sectors/track, 1011 cylinders
Units = cylinders of 3968 * 512 = 2031616 bytes
```

```
Disk identifier: 0x8491e758

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1               1           5        9889   83  Linux
/dev/sda2               6          45       79360    5  Extended
/dev/sda3              67        1011     1874880   83  Linux
/dev/sda4              46          66       41664   83  Linux
/dev/sda5               6          26       41633   83  Linux
/dev/sda6              27          45       37665   83  Linux
```

6.将零字节写入磁盘上的每个扇区。

**注意**：本测试是在N3K-C3064PQ-10X上进行的，采用英特尔赛扬CPU P4505 @1.87 GHz和13G eUSB，零字节过程大约需要501秒。

```
root@F340# dd if=/dev/zero of=/dev/sda bs=512
```

**注意**：预期它将看到在此步骤中在某些部分上生成的内核消息。

7.完成第5步后，重新加载交换机、管理引擎或系统控制器:

**注意**：要在Cisco Nexus 9000系列模块化交换机中重新加载系统控制器，请**输入reload module <slot_number>**CLI。

```
bash-4.2$ exit
F340.23.13-C3064PQ-1# exit
F340.23.13-C3064PQ-1# reload
WARNING: There is unsaved configuration!!!
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

# 使用dd将零字节写入I/O模块上的相关分区

1.通过控制台端口登录交换机的管理员帐户。

2.从配置**模式启用**feature bash-shell，并使用运行bash进**入Bash提**示符（仅限N3K/N9K）。 其他Cisco Nexus交换机需要调试插件才能访问Bash)。 如果需要调试插件，请联系Cisco TAC并执行步骤3，而不是步骤2。

**注意**：要从Bash提示符访问LC/FM，请在获得根访问**权后输**入rlogin lc# CLI。现在，将**CLI**中的#替换为要对其执行操作的插槽编号。

```
N7K-1# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
N7K-1(config)# feature bash-shell
N7K-1(config)# exit
N7K-1# run bash
```

```
bash-4.3$

N9K-EOR# run bash bash-4.2$ sudo su - root@N9K-EOR#rlogin lc22 root@fm22:~#
```

3.对于使用调试插件的Cisco Nexus交换机，请确保将运行的软件版本的调试插件复制到bootflash中，并将调试插件加载到要为其运行安全擦除过程的模块上：

**注意**：Nexus 7000系列交换机I/O模块有单独的调试插件映像，而Supervisor模块有调试插件映像。将LC映像用于交换机上运行的软件版本。

```
switch# attach module 3 Attaching to module 3 ... To exit type 'exit', to abort type '$.'
module-3# load bootflash:dplug-lc_p476-bin.7.2.1.D1.1.bin Name of debug-plugin from SUP:
'/bootflash/dplug-lc_p476-bin.7.2.1.D1.1.bin' Downloaded debug-plugin to LC: '/tmp/dplug-
lc_p476-bin.7.2.1.D1.1.bin' Loading plugin version 7.2(1)D1(1)
############################################################ Warning: debug-plugin is for
engineering internal use only! ############################################################
Warning: /debug-plugin/.autorun is using deprecated /bin/bash. Please change to /bin/sh
Successfully loaded debug-plugin!!! Linux(debug)#
```

4.接下来，对于Cisco Nexus 7000系列线卡，确定文件系统上装载的位置/logflash/和/mnt/pss。 为此，请使用mount命令查找/mnt/plog(logflash)和/mnt/pss驻留的位置。

**注意**：对于Cisco Nexus 9000系列线卡，对/dev/mmcblk0执行dd操作。

**注意**：对于Cisco Nexus 9000系列交换矩阵模块，对/tmpfs、/dev/root、/dev/zram0、/dev/loop0、/dev/loop1和/unionfs执行dd操作。

```
Linux(debug)# mount | grep plog /dev/mtdblock2 on /mnt/plog type jffs2 (rw,noatime)
Linux(debug)# Linux(debug)# mount | grep pss tmpfs on /mnt/pss type tmpfs
(rw,size=409600k,mode=777) Linux(debug)#
```

5.现在已知/mnt/plog 驻留在/dev/mtdblock2上，/mnt/pss 驻留在/tmpfs上，您可以使用dd命令将零字节写入两者，退出调试插件，然后重新加载模块：

```
Linux(debug)# dd if=/dev/zero of=/dev/mtdblock2 bs=1024 dd: writing '/dev/mtdblock2': No space
left on device 15361+0 records in 15360+0 records out Linux(debug)# Linux(debug)# dd if=dev/zero
of=/tmpfs bs=1024 dd: writing '/tmpfs': No space left on device 23781+0 records in 23780+0
records out Linux(debug)# Linux(debug)# exit
######################################################################## Warning: for security
reason, please delete plugin image on sup.
######################################################################## module-3# exit rlogin:
connection closed. switch# switch# reload module 3 This command will reload module 3.
Proceed[y/n]? [n] y reloading module 3 ... switch#
```

# 恢复交换机并重新安装操作系统

重新通电交换机后，它会在加载程序提示符下启动。

要从loader>提示符中恢复，必须按照以下步骤将交换机TFTP启动：

1. 将IP地址设置（或分配）到交换机的mgmt0接口：

```
loader > set ip <IP_address> <Subnet_Mask>
```

2.如果要启动的TFTP服务器位于不同的子网中，请为交换机分配默认网关：

```
loader > set gw <GW_IP_Address>
```

3.执行启动过程。 交换机引导至交换机（引导）提示符。

> **注意：**对于使用独立系统/启动映像的交换机，如Cisco Nexus 5000系列交换机、Cisco Nexus 6000系列交换机和Cisco Nexus 7000系列交换机，在此步骤中，您需要启动启动映像。 对于使用单个NXOS映像的交换机，如Cisco Nexus 9000系列交换机和Cisco Nexus 3000系列交换机，在此步骤中，您需要启动单个映像：

```
loader > boot tftp://
```

4.执行clear nvram、Init系统和format bootflash:

> **注意：**对于Cisco Nexus 5000系列交换机和Cisco Nexus 6000系列交换机，在switch(boot)#提示符下**不提供clear nvram**。

```
switch(boot)# clear nvram
switch(boot)# init system
This command is going to erase your startup-config, licenses as well as the contents of your
bootflash:.
Do you want to continue? (y/n) [n] y
Initializing the system ...

<snip>

switch(boot)# format bootflash:
This command is going to erase the contents of your bootflash:.
Do you want to continue? (y/n) [n] y
get_sup_active_slot failed with -1
Unknown card
Formatting bootflash:

<snip>
```

5.重新加载交换机：

```
switch(boot)# reload This command will reboot this supervisor module. (y/n) ? y  (c) Copyright
2011, Cisco Systems. N3000 BIOS v.5.0.0, Tue 06/05/2018, 05:24 PM
```

6.将IP地址设置（或分配）到交换机的mgmt0接口：

```
loader > set ip <IP_address> <Subnet_Mask>
```

7.如果要启动的TFTP服务器位于不同的子网中，请为交换机分配默认网关：

```
loader > set gw <GW_IP_Address>
```

8.重新加载交换机：

> **注意：**在Cisco Nexus 5000系列交换机、Cisco Nexus 6000系列交换机、Cisco Nexus 7000系列交换机管理引擎模块或Cisco Nexus 9000系列交换机管理引擎模块上执行此步骤(8)**不是必需的。** 如果在Cisco Nexus 5000系列交换机、Cisco Nexus 6000系列交换机、Cisco Nexus 7000系列交换机管理引擎模块或Cisco Nexus 9000系列交换机管理引擎模块上执行此步骤，请跳至步骤9。

```
loader> reboot
```

9.执行启动过程。 交换机引导至**switch(boot)提**示符。

> **注意：**对于使用单独系统/启动映像的交换机，如Cisco Nexus 7000系列交换机，在此步骤中，您需要启动启动映像。 对于使用单个NXOS映像的交换机，如Cisco Nexus 9000系列交换机和Cisco Nexus 3000系列交换机，在此步骤中，您需要启动单个映像：

```
loader > boot tftp://<server_IP>/<nxos_image_name>
```

10.对于使用单独系统/启动映像的交换机，如Cisco Nexus 5000系列交换机、Cisco Nexus 6000系列交换机和Cisco Nexus 7000系列交换机，在此步骤中，您需要执行一些其他步骤来启动交换机。您需要配置mgmt 0 IP地址和子网掩码，并定义默认网关。 完成此操作后，您可以将启动和系统映像复制到交换机并加载：

```
switch(boot)# config terminal Enter configuration commands, one per line. End with CNTL/Z.
switch(boot)(config)# interface mgmt 0 switch(boot)(config-if)# ip address 10.122.160.55
255.255.255.128 switch(boot)(config-if)# no shutdown switch(boot)(config-if)# exit
switch(boot)(config)# switch(boot)(config)# ip default-gateway 10.122.160.1
switch(boot)(config)# switch(boot)(config)# exit switch(boot)# switch(boot)# switch(boot)# copy
ftp: bootflash: Enter source filename:
```

11.对于Cisco Nexus 5000系列交换机、Cisco Nexus 6000系列交换机和Cisco Nexus 7000系列交换机管理引擎模块，在**switch(boot)#提示符**下输入**load bootflash:<system_image>**。 这将完成交换机的启动过程。

```
switch(boot)# load bootflash:<system_image>
```

12.成功加载系统映像后，您需要通过设置提示开始按照所需规格配置设备。