NXOS — 安全擦除磁碟內容

目錄

簡介

本文說明如何安全擦除Cisco Nexus交換機的磁碟，該交換機使用標準Linux實用程式。 對於某些軍方和政府客戶將裝置從安全區域移動到非安全區域，或者對於具有合規要求的任何其他客戶將裝置移出其場所而言，這是必要的。

背景資訊

有兩種選項取決於交換機是SSD還是eUSB驅動器：

- Init-System用於帶SSD的較新型號交換機。Init-System使用ATA安全擦除將二進位制0寫入驅動器的所有扇區。
- 對於帶有eUSB驅動器的舊型號交換機，還可以使用零位元組擦除方法向驅動器的所有扇區寫入0。

記錄在案的過程中使用的標準實用程式使用一系列命令，它們可以安全地銷毀儲存磁碟上的資料，而且在多數情況下，會使恢複資料變得困難或不可能。

本指南將帶您瞭解Cisco Nexus 3000系列交換機、Cisco Nexus 5000系列交換機、Cisco Nexus 9000系列交換機、Cisco Nexus 7000系列交換機和Cisco MDS系列交換機的兩個流程，但是適用於大多數其他Cisco Nexus交換機（前提是您具有init-system或Bash訪問許可權）。 如果您運行的交換機或軟體版本不支援啟用**feature bash**來訪問Bash外殼，請通過Cisco TAC開啟服務請求，以獲得使用用於此過程的調試外掛的幫助。

如何為自己確定合適的程式？

如果PID返回值**0**，則系統使用固態硬碟，並且可以使用Init-System方法擦除驅動器。

如果PID返回值**1**，則系統正在使用eUSB驅動器，並且您需要使用零位元組擦除方法。

```
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$
```

執行上述步驟之後，如果仍然不清楚系統中是哪種型別的驅動器，以及應該使用什麼步驟安全擦除磁碟內容，請通過Cisco TAC開啟服務請求。

準備

在擦拭驅動器之前，必須具備以下條件：

1. 通過控制檯訪問交換機。
2. 通過management0介面訪問TFTP伺服器 — 這是備份當前配置然後恢復作業系統所必需的。
3. 備份運行配置以及要在系統離線時儲存的任何其他檔案，因為這些檔案在此過程中已銷毀！

附註：強烈建議對不再生產或安裝在生產機箱中的部件執行此過程。在執行此過程之前，裝置或部件應移動到非生產環境中，以避免任何無意的網路中斷。

在帶有SSD的交換機上使用Init-System過程

附註：在基於模組的交換機內部的Supervisor上執行此過程時，建議僅將您計畫執行此過程的Supervisor安裝在系統中。

1. 通過控制檯連線時，重新載入或重新啟動交換機。

2. 當交換機啟動時，使用CTRL-C將交換機中斷到loader>提示符下。

3. 在loader>提示符下，輸入cmdline recoverymode=1。 這會在**switch(boot)#**提示時停止交換器開機：

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

4. 使用**boot bootflash:<nxos_filename.bin>**開始引導過程。

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

5. 交換器開機至**switch(boot)#提**示。 在此提示符下，使用**clear nvram** CLI和**init system** CLI將0寫入nvram中的所有塊（許可證塊除外）。 **附註**：此測試是在搭載Intel Core i3-CPU(2.50GHz)和110G SSD的N9K-C9372TX-E上進行的。 init系統的總時間大約為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. 完成步驟5後，重新載入switch:

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

在帶有eUSB的交換機/管理引擎/系統控制器上使用dd過程

1. 通過控制檯埠登入交換機的管理員帳戶。

   附註：在基於模組化的交換機內部的Supervisor上執行此過程時，建議僅將計畫執行此過程的Supervisor安裝在系統中。

2.在配置模式下啟用**feature bash-shell**，並使用**run bash**（僅限N3K/9K）進入Bash-prompt。 其他Cisco Nexus switch需要調試外掛才能訪問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獲取根**訪問許可權 —**

   附註：對此過程使用調試外掛的Cisco Nexus 7000系列交換機可以跳過此步驟。

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

4.如果要在安裝在Nexus 9000系列交換機中的系統控制器上執行此過程，則必須遠端登入到要在其中執行此過程的插槽編號。 例如，在此處對插槽29中的系統控制器進行操作：

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

5.使用fdisk -l驗證每個磁碟的塊大小。 在N3K-C3064PQ-10X上，它只有/dev/sda @ 512位元組塊大小，請參閱此處：

   附註：在一些Cisco Nexus交換機上，可能不止一個磁碟。執行DD操作時必須考慮這一點。例如，N7K-SUP2上有/dev/sda、/dev/sdb、/dev/sdc/、/dev/md2、/dev/md3、/dev/md4、/dev/md5和**/dev/md6**。必須對這些選項分別執行dd操作才能正確完成安全擦除過程。

   附註：在Cisco Nexus 9000系列交換機上，系統控制器具有/dev/mtdblock0、/dev/mtdblock1、/dev/mtdbloc2、/dev/mtdblock3、/dev/mtdblock4、/dev/mtdblock5和**/dev/mtdblock6**。 您必須對其中每一項執行dd操作才能正確完成安全擦除過程。

```
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.將零位元組寫入磁碟上的每個扇區。

附註：該測試是在採用英特爾賽揚CPU P4505 @1.87 GHz和13G eUSB的N3K-C3064PQ-10X上進行的，零位元組處理耗時約501秒。

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

附註：預期在某些部分會看到在此步驟中生成的核心消息。

7.完成步驟5後，重新載入交換器、Supervisor或系統控制器:

附註：要在Cisco Nexus 9000系列模組化交換機中重新載入系統控制器，請輸入**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將零位元組寫入I/O模組上的相關分割槽

1.通過控制檯埠登入交換機的管理員帳戶。

2.在配置模式下啟用**feature bash-shell**，並使用**run bash**（僅限N3K/N9K）進入Bash-prompt。 其他Cisco Nexus switch需要調試外掛才能訪問Bash)。 如果您需要調試外掛，請聯絡Cisco TAC並按照步驟3而不是步驟2操作。

附註：若要從Bash-prompt存取LC/FM，請在取得root存取權後輸入**rlogin lc#CLI。**現在用您要對其執行操作的插槽編號替換CLI中的**#**。

```
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.對於使用debug外掛的Cisco Nexus交換機，請確保將運行的軟體版本的調試外掛複製到bootflash，並在要為其運行安全擦除過程的模組上載入調試外掛：

附註：與Supervisor模組可用的調試外掛映像不同，Nexus 7000系列交換機I/O模組可使用單獨的調試外掛映像。在交換器上執行的軟體版本使用LC映像。

```
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.接下來，對於Cisco Nexus 7000系列線卡，確定**/logflash/**和**/mnt/pss**在檔案系統中的安裝位置。為此，請使用mount命令查詢**/mnt/plog(logflash**)和**/mnt/pss駐留**位置。

附註：對於Cisco Nexus 9000系列線卡，請對/**dev**/mmcblk**0執行dd操作**。

附註：對於Cisco Nexus 9000系列交換矩陣模組，請對/tmpfs、/dev/root、/dev/zram0、**/dev/loop0**、/dev/loop1和**/unionfs**執行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.現在已知**/mnt/plog**駐留在**/dev/mtdblock2**上，而**/mnt/pss**駐留在**/tmpfs**上，因此您可以使用dd命令將零位元組寫入到兩者中，退出debug外掛，然後重新載入模組：

```
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#
```

恢復交換機並重新安裝作業系統

重新通電後，switch會在載入器提示中啟動。

若要從loader>提示中復原，必須按照以下步驟將交換器啟動TFTP:

1. 為交換機上的mgmt0介面設定（或分配）IP地址：

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

2.如果要從中啟動的TFTP伺服器位於不同的子網中，請為交換機分配預設網關：

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

3.執行引導過程。 交換器開機至交換器（開機）提示。

> **附註**：對於使用單獨系統/kickstart映像的交換機（如Cisco Nexus 5000系列交換機、Cisco Nexus 6000系列交換機和Cisco Nexus 7000系列交換機），在此步驟需要啟動kickstart映像。 對於使用單個NXOS映像的交換機（如Cisco Nexus 9000系列交換機和Cisco Nexus 3000系列交換機），在此步驟需要引導單個映像：

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

4.執行clear nvram、Init system和format bootflash:

> **附註**：對於Cisco Nexus 5000系列交換機和Cisco Nexus 6000系列交換機，**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.重新載入交換器：

```
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.為交換機上的mgmt0介面設定（或分配）IP地址：

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

7.如果要從其引導的TFTP伺服器位於不同的子網中，請為交換機分配預設網關：

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

8.重新載入交換器：

> **附註**：在Cisco Nexus 5000系列交換機、Cisco Nexus 6000系列交換機、Cisco Nexus 7000系列交換機Supervisor模組或Cisco Nexus 9000系列交換機Supervisor模組上執行此過程**時，不需要執行此步驟**(8)。 如果您在Cisco Nexus 5000系列交換機、Cisco Nexus 6000系列交換機、Cisco Nexus 7000系列交換機管理引擎模組或Cisco Nexus 9000系列交換機管理引擎模組上執行此步驟，請跳至步驟9。

```
loader> reboot
```

9.執行引導過程。 交換器開機至**switch(boot)提**示符。

> **附註**：對於使用單獨系統/kickstart映像的交換機（如Cisco Nexus 7000系列交換機），在此步驟需要引導kickstart映像。 對於使用單個NXOS映像的交換機（如Cisco Nexus 9000系列交換機和Cisco Nexus 3000系列交換機），在此步驟需要引導單個映像：

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

10.對於使用單獨系統/啟動映像的交換機，如Cisco Nexus 5000系列交換機、Cisco Nexus 6000系列交換機和Cisco Nexus 7000系列交換機，在此步驟中，您需要執行一些額外的步驟來啟動交換機。 您需要配置管理0 IP地址和子網掩碼以及定義預設網關。 完成後，您可以將kickstart和系統映像複製到switch並載入：

```
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.對於Cisco Nexus 5000系列交換機、Cisco Nexus 6000系列交換機和Cisco Nexus 7000系列交換機管理引擎模組，在**switch(boot)#**提示符下，輸入**load bootflash:<system_image>**。 這將完成交換機的啟動過程。

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

12.系統映像成功載入後，您需要通過設定提示開始按照所需的規格配置裝置。