NXOS - Securely Erase the Contents of the Disk

Contents

Introduction

This document describes how to safely wipe the disk of a Cisco Nexus switch, which utilizes standard Linux utilities. This is necessary for certain military and government customers moving equipment from a secured zone to a non-secured zone, or for any other customer having compliance requirements to shift equipment out of their premise.

Background Information

There are two options that depend upon whether the switch has an SSD or eUSB drive:

- Init-System is used on newer model switches with SSDs. Init-System uses ATA Secure erase to write binary 0s to all sectors of the drive.
- For older model switches with eUSB drives, you can also write 0s to all sectors of the drive, using the Zero-Byte Erase method.

The standard utilities used in the documented procedure use a series of commands that securely destroy the data on the storage disk, and in most cases make it difficult or impossible to recover the data.

This guide walks you through both processes with Cisco Nexus 3000 Series switches, Cisco Nexus 5000 Series switches, Cisco Nexus 9000 Series switches, Cisco Nexus 7000 Series switches, and Cisco MDS Series switches in mind, but works for most other Cisco Nexus switches, provided you have init-system or Bash access. If the switch you have or software release you are running does not have support to enable **feature bash** to gain access to the Bash shell, open a Service Request with Cisco TAC to get assistance with utilizing a debug plugin for this procedure.

How To Determine the Suitable Procedure for Yourself?

if your PID returns a value of **0**, the system is using an SSD and can use the Init-System method to erase the drive.

If your PID returns a value of **1**, the system is using an eUSB drive, and you need to use the Zero-Byte Erase method.

```
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$
```

After the preceding procedure is performed, if it is still not clear which type of drive is in your system and what procedure should be used to securely wipe the contents of the disk, open a Service Request with Cisco TAC.

Preparation

Prior to wiping your drive, you must have these:

1. Console access to the switch.
2. Access to a TFTP server through the management0 interface - that is necessary to back up the current config and then to restore the OS.
3. A back up of the running-config and any other files you want to save from the system offline as they are destroyed in this process!

> **Note**: It is strongly recommended you perform this procedure on parts that are no longer in production or installed in production chassis's. The devices or parts should be moved into a non-production environment prior to performing this procedure to avoid any unintentional network disruptions.

Use Init-System Procedure on Switches with SSD

> **Note**: When performing this procedure on a Supervisor inside of a modular-based switch, it is recommended to only have the Supervisor who you plan on performing the procedure installed in the system.

1. Reload or power cycle the switch while connected via console.

2. While the switch is booting, use CTRL-C to break the switch into loader> prompt.

3. From the loader> prompt, enter cmdline recoverymode=1. This stops the switch booting at the **switch(boot)#** prompt:

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

4. Begin the boot procedure with **boot bootflash:<nxos_filename.bin>**.

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

5. The switch boots to the **switch(boot)#** prompt. At this prompt write, 0's to all blocks in nvram, except the license blocks, using **clear nvram** CLI as well as **init system** CLI. **Note**: this test was carried out on an N9K-C9372TX-E with an Intel Core i3- CPU @ 2.50GHz and a 110G SSD. Total time for init system took ~8 seconds:

```
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. Once step 5 is complete, reload the switch:

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

Use dd Procedure on Switches/Supervisors/System Controllers with eUSB

1. Log in to the admin account of the switch via the console port.

   Note: When you perform this procedure on a Supervisor inside of a modular-based switch, it is recommended to only have the Supervisor which you plan on performing the procedure installed in the system.

2. Enable **feature bash-shell** from config mode and enter the Bash-prompt with **run bash** (N3K/9K only. Other Cisco Nexus switches need a debug plugin to gain access to 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. Gain root access with **sudo su -**

   Note: This step can be skipped for Cisco Nexus 7000 Series switches that are using a debug plugin for this procedure.

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

4. If you are performing this procedure on a System Controller installed in a Nexus 9000 Series Switch, you must remote login to the slot number on which you wish to perform this procedure. For example, here it is done for the System Controller in slot 29:

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

5. Verify the block size of each disk with fdisk -l. On a N3K-C3064PQ-10X it has only /dev/sda @ 512 bytes block size, see here:

> **Note**: On some Cisco Nexus switches there may be more than a single disk. It must be taken into account when you perform the dd operation. For example, N7K-SUP2 there is **/dev/sda**, **/dev/sdb**, **/dev/sdc/**, **/dev/md2**, **/dev/md3**, **/dev/md4**, **/dev/md5**, and **/dev/md6**. You must perform the dd operation on each of these to complete the secure erase procedure correctly.

> **Note**: On Cisco Nexus 9000 Series switches the System Controller has **/dev/mtdblock0**, **/dev/mtdblock1**, **/dev/mtdbloc2**, **/dev/mtdblock3**, **/dev/mtdblock4**, **/dev/mtdblock5**, and **/dev/mtdblock6**. You must perform the dd operatoon on each of these to complete the secure erase procedure correctly.

```
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. Write a zero-byte to every sector on the disk.

> **Note**: This test was carried out on an N3K-C3064PQ-10X with an Intel Celeron CPU P4505 @1.87 GHz and 13G eUSB the Zero-Byte process took ~501 seconds.

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

> **Note**: It is expected to see Kernel messages generated at this step on some parts.

7. Once step five is complete, reload the switch, Supervisor, or System controller:

> **Note**: In order to reload the System Controller in a Cisco Nexus 9000 Series modular switch, enter the **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
```

Use dd to write Zero-byte to Relevant Partitions on I/O Module

1. Log in to the admin account of the switch via the console port.

2. Enable **feature bash-shell** from config mode and enter the Bash-prompt with **run bash** (N3K/N9K only). Other Cisco Nexus switches need a debug plugin to gain access to Bash). If you require a debug plugin, contact Cisco TAC and follow step 3 instead of step 2.

> **Note**: In order to access the LC/FM from Bash-prompt, enter **rlogin lc#** CLI once you have gained root access. Now replace the **#** in the CLI with the slot number you wish to perform the operation on.

```
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. For Cisco Nexus Switches that use debug plugin, ensure the debug plugin for the software version running is copied to bootflash, and load the debug plugin on the module for which you wish to run the secure erase procedure for:

> **Note**: There is a separate debug plugin image to be used for Nexus 7000 Series Switches I/O modules as opposed to the debug plugin image made available for Supervisor modules. Use LC image for the software release that runs on the switch.

```
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. Next, for Cisco Nexus 7000 Series Line Cards, determine where **/logflash/** and **/mnt/pss** is mounted on the filesystem. In order to do this, use the mount command to find where **/mnt/plog** (logflash) and **/mnt/pss** resides.

> **Note**: For Cisco Nexus 9000 Series Line Cards, perform the dd operation on **/dev/mmcblk0**.

> **Note**: For Cisco Nexus 9000 Series Fabric Modules, perform the dd operation

on **/tmpfs**, **/dev/root**, **/dev/zram0**, **/dev/loop0**, **/dev/loop1**, and **/unionfs**.

```
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. Now that it is known that **/mnt/plog** resides on **/dev/mtdblock2** and **/mnt/pss** resides on **/tmpfs**, you write Zero-Byte to both using dd command, exit from the debug plugin, and reload the module:

```
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#
```

Recover the Switch and Reinstall the OS

After power-cycling the switch, it boots up in the loader prompt.

In order to recover from the loader> prompt, the switch must be TFTP booted according to the following steps:

1. Set (or Assign) an IP address to mgmt0 interface on the switch:

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

2. If the TFTP server from which you are booting is in a different subnet, assign a default gateway to the switch:

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

3. Perform the boot process. The switch boots to the switch(boot) prompt.

> **Note**: For switches that use separate system/kickstart images, like Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, and Cisco Nexus 7000 Series switches, at this step you need to boot the kickstart image. For switches that use a single NXOS image, like Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches, at this step you need to boot the single image:

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

4. Perform clear nvram, Init system, and format bootflash:

> **Note**: For Cisco Nexus 5000 Series switches and Cisco Nexus 6000 Series switches, clear

nvram is not available at **switch(boot)#** prompt.

```
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. Reload the switch:

```
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 <snip>
```

6. Set (or Assign) an IP address to mgmt0 interface on the switch:

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

7. If the TFTP server from which you are booting is in a different subnet, assign a default gateway to the switch:

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

8. Reload the switch:

> **Note**: This step (8) is **NOT** required when this procedure is performed on Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, Cisco Nexus 7000 Series switches Supervisor modules, or Cisco Nexus 9000 Series switches Supervisor module. Skip to step 9 if you perform this procedure on a Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, Cisco Nexus 7000 Series switch Supervisor module, or Cisco Nexus 9000 Series switches Supervisor module.

```
loader> reboot
```

9. Perform the boot process. The switch boots to the **switch(boot)** prompt.

> **Note**: For switches that use separate system/kickstart images, like Cisco Nexus 7000 Series switches, at this step you need to boot the kickstart image. For switches that use a single NXOS image, like Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches, at this step you need to boot the single image:

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

10. For switches that use separate system/kickstart images, like the Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, and Cisco Nexus 7000 Series switches, at this step you need to take some additional steps to boot the switch. You need to configure the mgmt 0 IP address and subnet mask as well as define the default gateway. Once this is complete, you may copy the kickstart and system image to the switch and load it:

```
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: <Kickstart image file name> Enter hostname for the ftp
server: <IP address of FTP server> Enter username: <Username> Connected to x.x.x.x. 220 CALO
Fileserver 331 Please specify the password. Password: <Password> 230 Login successful. <snip>
221 Goodbye. Copy complete, now saving to disk (please wait)... switch(boot)# switch(boot)# copy
ftp: bootflash: Enter source filename: <System image file name> Enter hostname for the ftp
server: <IP address of FTP server> Enter username: <Username> Connected to x.x.x.x. 220 CALO
Fileserver 331 Please specify the password. Password: <Password> 230 Login successful. <snip>
221 Goodbye. switch(boot)#
```

11. For Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, and Cisco Nexus 7000 Series switch Supervisor modules, from the **switch(boot)#** prompt, enter **load bootflash:<system_image>**. This finishes the boot process of the switch.

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

12. Once the system image loads successfully you need to go through the setup prompt to begin configuring the device to your desired specifications.