NXOS - Sicheres Löschen des Inhalts der Festplatte

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Festplatte eines Cisco Nexus-Switches, der standardmäßige Linux-Dienstprogramme verwendet, sicher löschen. Dies ist erforderlich für bestimmte Militär- und Regierungskunden, die Geräte aus einem sicheren Bereich in einen ungesicherten Bereich verlagern, oder für alle anderen Kunden, die die Compliance-Anforderungen erfüllen, Geräte außerhalb ihres Standorts zu verlagern.

Hintergrundinformationen

Es gibt zwei Optionen, die davon abhängig sind, ob der Switch über ein SSD- oder eUSB-Laufwerk verfügt:

- Init-System wird auf neueren Switch-Modellen mit SSDs verwendet. Init-System verwendet ATA Secure erase zum Schreiben von Binärzahlen in alle Sektoren des Laufwerks.
- Bei älteren Switch-Modellen mit eUSB-Laufwerken können Sie mithilfe der Zero-Byte-Erase-Methode auch 0 s in alle Sektoren des Laufwerks schreiben.

Die in der dokumentierten Prozedur verwendeten Standard-Dienstprogramme verwenden eine Reihe von Befehlen, die die Daten auf der Festplatte sicher zerstören und in den meisten Fällen die Wiederherstellung der Daten erschweren oder unmöglich machen.

Dieser Leitfaden führt Sie durch die beiden Prozesse mit Cisco Nexus Switches der Serie 3000, Cisco Nexus Switches der Serie 5000, Cisco Nexus Switches der Serie 9000, Cisco Nexus Switches der Serie 7000 und Cisco Switches der MDS-Serie. Er eignet sich jedoch für die meisten anderen Cisco Nexus-Switches, vorausgesetzt Sie haben Zugriff auf Init-Systeme oder Bash. Wenn der Switch, den Sie haben, oder die Softwareversion, die Sie ausführen, nicht unterstützt wird, um **Feature-Bash** für den Zugriff auf die Bash-Shell zu aktivieren, öffnen Sie eine Serviceanfrage bei Cisco TAC, um Unterstützung bei der Verwendung eines Debug-Plugins für dieses Verfahren zu erhalten.

Wie bestimmen Sie die geeignete Vorgehensweise für sich

selbst?

Wenn Ihre PID einen Wert von **0** zurückgibt, verwendet das System eine SSD und kann das Laufwerk mithilfe der Init-System-Methode löschen.

Wenn Ihre PID einen Wert von **1** zurückgibt, verwendet das System ein eUSB-Laufwerk und Sie müssen die Zero-Byte-Erase-Methode verwenden.

```
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$
```

Wenn nach der Ausführung des vorhergehenden Verfahrens immer noch nicht klar ist, welcher Laufwerkstyp in Ihrem System vorhanden ist und mit welchem Verfahren der Inhalt der Festplatte sicher gelöscht werden soll, öffnen Sie eine Serviceanfrage bei Cisco TAC.

Vorbereitung

Bevor Sie Ihr Laufwerk löschen, müssen Sie über Folgendes verfügen:

1. Konsolenzugriff auf den Switch.
2. Zugriff auf einen TFTP-Server über die Management0-Schnittstelle. Diese Schnittstelle ist erforderlich, um die aktuelle Konfiguration zu sichern und anschließend das Betriebssystem wiederherzustellen.
3. Eine Sicherung der laufenden Konfiguration und aller anderen Dateien, die Sie im System offline speichern möchten, da sie in diesem Prozess zerstört werden!

Hinweis: Es wird dringend empfohlen, dieses Verfahren für Teile auszuführen, die nicht mehr in der Produktion sind oder in Produktionshallen installiert sind. Die Geräte oder Teile sollten vor der Durchführung dieses Verfahrens in eine nicht produktionsbezogene Umgebung verschoben werden, um unbeabsichtigte Netzwerkunterbrechungen zu vermeiden.

Init-System-Verfahren für Switches mit SSD verwenden

Hinweis: Bei der Durchführung dieses Verfahrens auf einem Supervisor innerhalb eines modulbasierten Switches wird empfohlen, nur den Supervisor zu haben, den Sie für die Durchführung der Prozedur planen, der im System installiert ist.

1. Laden Sie den Switch neu, oder schalten Sie ihn ein, während er über die Konsole verbunden ist.

2. Während der Switch hochfährt, brechen Sie mit STRG-C den Switch in die Ladeprogramm-Eingabeaufforderung> auf.

3. Geben Sie in der Eingabeaufforderung loader> cmdline restore ymode=1 ein. Dadurch wird das Booten des Switches an der **switch(boot)#**-Eingabeaufforderung beendet:

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

4. Beginnen Sie die Bootprozedur mit **boot bootflash:<nxos_filename.bin>**.

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

5. Der Switch startet mit der **switch(boot)#**-Eingabeaufforderung. Geben Sie bei dieser Eingabeaufforderung 0 an alle Blöcke in nvram, mit Ausnahme der Lizenzblöcke, unter Verwendung der **clear nvram** CLI sowie der **init system** CLI. **Hinweis:** Dieser Test wurde mit einer N9K-C9372TX-E mit einer Intel Core i3-CPU bei 2,50 GHz und einer 110-G-SSD durchgeführt. Die Gesamtzeit für das Init-System betrug ~8 Sekunden:

```
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. Laden Sie nach Abschluss von Schritt 5 den Switch neu:

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

Verfahren für Hinzufügen von Switches/Supervisoren/System-Controllern mit eUSB verwenden

1. Melden Sie sich über den Konsolenport beim Administratorkonto des Switches an.

   Hinweis: Wenn Sie dieses Verfahren auf einem Supervisor in einem modulbasierten Switch ausführen, wird empfohlen, nur den Supervisor zu verwenden, den Sie zur Ausführung des Vorgangs im System installieren möchten.

2. Aktivieren Sie **feature bash-shell** aus dem Konfigurationsmodus, und geben Sie die Bash-Prompt mit **Run bash ein** (nur N3K/9K). Andere Cisco Nexus Switches benötigen ein Debug-Plugin, um Zugriff auf Bash zu erhalten).

```
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. Root-Zugriff mit **sudo su -**

   Hinweis: Dieser Schritt kann bei Cisco Nexus Switches der Serie 7000 übersprungen werden, die für dieses Verfahren ein Debug-Plug-in verwenden.

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

4. Wenn Sie dieses Verfahren auf einem System-Controller ausführen, der auf einem Nexus Switch der Serie 9000 installiert ist, müssen Sie sich remote an die Steckplatznummer anmelden, auf der Sie dieses Verfahren ausführen möchten. Beispiel: Dies wird für den System-Controller in Steckplatz 29 durchgeführt:

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

5. Überprüfen Sie die Blockgröße jedes Datenträgers mit fdisk -l. Auf einem N3K-C3064PQ-10X hat es nur /dev/sda bei 512 Byte Blockgröße, siehe hier:

> **Hinweis:** Bei einigen Cisco Nexus-Switches kann es mehr als eine Festplatte geben. Sie muss bei der Durchführung des TT-Vorgangs berücksichtigt werden. N7K-SUP2 umfasst beispielsweise /dev/sda, /dev/sdb, /dev/sdc/, /dev/md2, /dev/md3, /dev/md4, **/dev/md5** und **/dev/md6.** Sie müssen für jeden dieser Schritte den Befehl dd ausführen, um die sichere Löschoperation ordnungsgemäß abzuschließen.

> **Hinweis:** Auf Cisco Nexus Switches der Serie 9000 verfügt der System-Controller über **/dev/mtdblock0**, **/dev/mtdblock1**, **/dev/mtdbloc2**, **/dev/mtdblock3**, **/dev/mtdblock4, /dev/mtdblock5 und /dev/mv tdblock6.** Sie müssen für jeden dieser Schritte den Befehl dd ausführen, um die sichere Löschoperation ordnungsgemäß abzuschließen.

```
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. Schreiben Sie ein Nullbyte auf jeden Sektor auf der Festplatte.

> **Hinweis:** Dieser Test wurde mit einem N3K-C3064PQ-10X mit Intel Celeron CPU P4505 bei 1,87 GHz und 13G eUSB durchgeführt. Der Zero-Byte-Prozess dauerte ca. 501 Sekunden.

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

> **Hinweis:** Es wird erwartet, dass bei diesem Schritt Kernel-Meldungen für einige Teile generiert werden.

7. Laden Sie nach Abschluss von Schritt 5 den Switch, den Supervisor oder den System-

Controller neu:

> **Hinweis:** Um den System-Controller in einem modularen Switch der Cisco Nexus Serie 9000 neu zu laden, geben Sie das **Reload-Modul <slot_number>** CLI ein.

```
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
```

Schreiben von 0 Byte auf relevante Partitionen im E/A-Modul mithilfe von dd

1. Melden Sie sich über den Konsolenport beim Administratorkonto des Switches an.

2. Aktivieren Sie **Feature-Bash-Shell** aus dem Konfigurationsmodus, und geben Sie die Bash-Eingabeaufforderung mit **Run Bash ein** (nur N3K/N9K). Andere Cisco Nexus Switches benötigen ein Debug-Plugin, um Zugriff auf Bash zu erhalten). Wenn Sie ein Debug-Plug-in benötigen, wenden Sie sich an das Cisco TAC und befolgen Sie Schritt 3 statt Schritt 2.

> **Hinweis:** Um von der Bash-Eingabeaufforderung aus auf den LC/FM zuzugreifen, geben Sie **rlogin lc#** CLI ein, sobald Sie den Root-Zugriff erhalten haben. Ersetzen Sie jetzt die **#** in der CLI durch die Steckplatznummer, unter der Sie den Vorgang durchführen möchten.

```
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. Bei Cisco Nexus-Switches, die Debug-Plug-Ins verwenden, stellen Sie sicher, dass das Debug-Plug-In für die ausgeführte Softwareversion in Bootflash kopiert wird, und laden Sie das Debug-Plug-In auf das Modul, für das Sie die sichere Löschprozedur für:

> **Hinweis:** Für die E/A-Module der Nexus 7000-Serie ist ein separates Debug-Plugin-Image erforderlich, im Gegensatz zum Debug-Plug-In-Image, das für Supervisor-Module verfügbar ist. Verwenden Sie LC-Image für die Softwareversion, die auf dem Switch ausgeführt wird.

```
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. Als Nächstes bestimmen Sie bei Line Cards der Cisco Nexus Serie 7000, wo **/logflash/**und **/mnt/pss** auf das Dateisystem gemountet ist. Verwenden Sie dazu den Mount-Befehl, um zu finden, wo sich **/mnt/plog** (logflash) und **/mnt/pss** befindet.

> **Hinweis:** Führen Sie bei Cisco Nexus Line Cards der Serie 9000 den dd-Vorgang unter **/dev/mmcblk0 aus**.

> **Hinweis:** Führen Sie bei Cisco Nexus Fabric-Modulen der Serie 9000 den dd-Vorgang für **/tmpfs**, **/dev/root**, **/dev/zram0**, **/dev/loop0**, **/dev/loop1 und /unionfs durch.**

```
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. Da jetzt bekannt ist, dass **/mnt/plog** sich auf **/dev/mtdblock2** und **/mnt/pss** auf **/tmpfs** befindet, schreiben Sie Zero-Byte mit dem Befehl dd, beenden das Debug-Plug-in und laden das Modul neu:

```
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#
```

Stellen Sie den Switch wieder her, und installieren Sie das Betriebssystem neu.

Nachdem der Switch aus- und wieder eingeschaltet wurde, wird er über die Ladeaufforderung gestartet.

Um den Switch von der Loader>-Eingabeaufforderung wiederherzustellen, muss er wie folgt über TFTP gestartet werden:

1. Legen Sie auf dem Switch eine IP-Adresse für die mgmt0-Schnittstelle fest (oder weisen Sie sie zu):

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

2. Wenn sich der TFTP-Server, von dem aus Sie starten, in einem anderen Subnetz befindet, weisen Sie dem Switch ein Standard-Gateway zu:

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

3. Führen Sie den Bootvorgang durch. Der Switch startet mit der Switch(boot)-Eingabeaufforderung.

> **Hinweis:** Für Switches, die separate System-/Kickstart-Images verwenden, wie Cisco Nexus Switches der Serie 5000, Cisco Nexus Switches der Serie 6000 und Cisco Nexus Switches der Serie 7000, müssen Sie in diesem Schritt das Kickstart-Image booten. Für Switches, die ein einzelnes NXOS-Image verwenden, z. B. Cisco Nexus Switches der Serie 9000 und Cisco Nexus Switches der Serie 3000, müssen Sie in diesem Schritt das einzelne Image booten:

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

4. Führen Sie einen Clear nvram, ein Init-System und ein Format für Bootflash durch:

> **Hinweis:** Bei Cisco Nexus Switches der Serie 5000 und Cisco Nexus Switches der Serie 6000 ist kein leeres nvram bei **Switch(boot)#** verfügbar.

```
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. Laden Sie den Switch neu:

```
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. Legen Sie auf dem Switch eine IP-Adresse für die mgmt0-Schnittstelle fest (oder weisen Sie sie zu):

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

7. Wenn sich der TFTP-Server, von dem aus Sie starten, in einem anderen Subnetz befindet, weisen Sie dem Switch ein Standard-Gateway zu:

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

8. Laden Sie den Switch neu:

> **Hinweis:** Dieser Schritt (8) ist **NICHT** erforderlich, wenn dieses Verfahren für Cisco Nexus Switches der Serie 5000, Cisco Nexus Switches der Serie 6000, Cisco Nexus Switches der Serie 7000 Supervisor-Module oder Cisco Nexus Switches der Serie 9000 durchgeführt wird. Fahren Sie mit Schritt 9 fort, wenn Sie dieses Verfahren für ein Supervisor-Modul für Cisco Nexus Switches der Serie 5000, Cisco Nexus Switches der Serie 6000, Cisco Nexus Switches der Serie 7000 oder Cisco Nexus Switches der Serie 9000 ausführen.

```
loader> reboot
```

9. Führen Sie den Bootvorgang durch. Der Switch startet mit der **Switch(boot)**-Eingabeaufforderung.

> **Hinweis:** Bei Switches, die separate System-/Kickstart-Images verwenden, wie z. B. Switches der Cisco Nexus 7000-Serie, müssen Sie in diesem Schritt das Kickstart-Image booten. Für Switches, die ein einzelnes NXOS-Image verwenden, z. B. Cisco Nexus Switches der Serie 9000 und Cisco Nexus Switches der Serie 3000, müssen Sie in diesem Schritt das einzelne Image booten:

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

10. Für Switches, die separate System-/Kickstart-Images verwenden, wie die Cisco Nexus Switches der Serie 5000, die Cisco Nexus Switches der Serie 6000 und die Cisco Nexus Switches der Serie 7000, müssen Sie in diesem Schritt einige zusätzliche Schritte zum Booten des Switches ausführen. Sie müssen die mgmt 0-IP-Adresse und die Subnetzmaske konfigurieren und das Standard-Gateway definieren. Nach Abschluss dieses Vorgangs können Sie das Kickstart- und System-Image auf den Switch kopieren und ihn laden:

```
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. Geben Sie für Cisco Nexus Switches der Serie 5000, Cisco Nexus Switches der Serie 6000 und Cisco Nexus Switches der Serie 7000 Supervisor-Module über die **Switch(boot)#**-Eingabeaufforderung **Load Bootflash ein:<system_image>**. Damit ist der Startvorgang für den Switch abgeschlossen.

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

12. Sobald das System-Image erfolgreich geladen wurde, müssen Sie die Setup-Eingabeaufforderung durchlaufen, um mit der Konfiguration des Geräts gemäß den gewünschten Spezifikationen zu beginnen.