

NXOS - Hiermee kunt u de inhoud van de schijf goed wissen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Hoe kun je zelf de juiste procedure bepalen?](#)

[Vorbereiding](#)

[Gebruik de systeemprocedure op switches met SSD](#)

[Gebruik de ADD-procedure voor switches/Supervisors/systeemcontrollers met eUSB](#)

[Gebruik dd om Nul-byte naar relevante partities op I/O-module te schrijven](#)

[De switch herstellen en het besturingssysteem opnieuw installeren](#)

Inleiding

Dit document beschrijft hoe de schijf van een Cisco Nexus-switch veilig kan worden gewist met behulp van de standaard Linux-hulpprogramma's. Dit is noodzakelijk voor bepaalde militaire en overheidsambtenaren die apparatuur van een beveiligd gebied naar een niet-beveiligd gebied verplaatsen, of voor andere klanten die voldoen aan de eisen om apparatuur uit hun bedrijfsruimte te verplaatsen.

Achtergrondinformatie

Er zijn twee opties die afhankelijk zijn van of de schakelaar een SSD of eUSB-station heeft:

- Init-System wordt gebruikt op nieuwere modelswitches met SSD's. Het Init-System gebruikt ATA Secure Wase om binaire 0s te schrijven naar alle sectoren van de schijf.
- Voor oudere modelswitches met eUSB-schijven kunt u ook 0s schrijven naar alle sectoren van het station met behulp van de Zero-Byte Erase-methode.

De standaardhulpprogramma's die in de gedocumenteerde procedure worden gebruikt, maken gebruik van een reeks opdrachten die de gegevens op de opslagschijf veilig vernietigen, en in de meeste gevallen het moeilijk of onmogelijk maken de gegevens te herstellen.

Deze gids loopt u door beide processen met Cisco Nexus 3000 Series switches, Cisco Nexus 5000 Series switches, Cisco Nexus 9000 Series switches, Cisco Nexus 7000 Series switches en Cisco MDS Series switches in gedachten, maar werkt voor de meeste andere Cisco Nexus switches, mits u init-systeem of Bash-toegang hebt. Als de schakelaar of de softwarerelease die u hebt uitgevoerd geen steun heeft om **functiebasis** toe te **stellen** om toegang tot de schaal van de Uitgangswaarde te krijgen, open een de Vraag van de Dienst met Cisco TAC om hulp te krijgen bij het gebruiken van een debug plug-in voor deze procedure.

Hoe kun je zelf de juiste procedure bepalen?

als uw PID een waarde van 0 retourneert, gebruikt het systeem een SSD en kan de Init-System methode worden gebruikt om het station te wissen.

Als uw PID een waarde van 1 retourneert, gebruikt het systeem een eUSB-station en moet u de Zero-Byte Erase-methode gebruiken.

```
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$
```

Nadat de vorige procedure is uitgevoerd, als niet duidelijk is welk type schijf in uw systeem staat en welke procedure moet worden gebruikt om de inhoud van de schijf veilig te wissen, opent u een serviceaanvraag bij Cisco TAC.

Vorbereiding

Voordat u het station gaat reinigen, dient u te beschikken over:

1. Console toegang tot de schakelaar.
2. Toegang tot een TFTP-server via de management0 interface - die nodig is om een back-up te maken van de huidige configuratie en vervolgens het OS te herstellen.
3. Een back-up van de in werking stellen-configuratie en andere bestanden die u van het systeem wilt opslaan offline als ze in dit proces worden vernietigd!

Opmerking: Aanbevolen wordt om deze procedure ook uit te voeren voor onderdelen die niet meer in productie zijn of die niet meer in een productiechassis zijn geïnstalleerd. De apparatuur of onderdelen moeten vóór de uitvoering van deze procedure in een niet-productieomgeving worden geplaatst om onbedoelde verstoringen van het netwerk te voorkomen.

Gebruik de systeempcedure op switches met SSD

Opmerking: Wanneer het uitvoeren van deze procedure op een Supervisor binnen van een op modulair gebaseerd schakelaar, wordt het aanbevolen om slechts de Supervisor te hebben die u van plan bent om de procedure uit te voeren in het systeem geïnstalleerd is.

1. Herladen of inschakelen van de schakelaar terwijl deze via de console is aangesloten.
2. Wanneer de schakelaar start, gebruik CTRL-C om de schakelaar in de herinnering van het Lader> te breken.
3. Voer in de Password-prompt in (cd) Dit stopt de switchingstart bij de **schakelaar(start)#**prompt:

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

4. Begin de laarprocedure met **bootflitser:<nxos_filename.bin>**.

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

5. De schakelaar start op de **schakelaar (start)#**prompt. Bij deze prompt schrijft 0 naar alle blokken in nvram, behalve de licentieblokken, met **behulp van een duidelijk nvram CLI en een CLI-systeem**. **Opmerking:** deze test werd uitgevoerd op een N9K-C9372TX-E met een Intel Core i3-CPU bij 2,50 GHz en een 110G SSD. Totale tijd voor inbraaksysteem:

```
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. Nadat stap 5 is voltooid, laadt u de schakelaar opnieuw:

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

Gebruik de ADD-procedure voor switches/Supervisors/systeemcontrollers met eUSB

1. Meld u aan bij de beheerder van de schakelaar via de console poort.

Opmerking: Wanneer u deze procedure op een supervisor binnen van een op modulaair gebaseerde schakelaar uitvoert, wordt het aanbevolen om slechts de supervisor te hebben die u van plan bent om de procedure uit te voeren in het systeem geïnstalleerd.

2. Schakel terug in vanaf de **basis-shell** van de configuratiewijze en voer de Bash-prompt in met **loopbasis** (alleen N3K/9K). Andere Cisco Nexus switches hebben een debug plug-in nodig om toegang tot Bash te krijgen).

```
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 toegang met **sudo su -**

Opmerking: Deze stap kan voor Cisco Nexus 7000 Series switches worden overgeslagen die een debug plug-in voor deze procedure gebruiken.

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

4. Als u deze procedure toepast op een systeemcontroller die in een Nexus 9000 Series-switch is geïnstalleerd, moet u externe inloggen naar het nummer van de sleuf waarop u deze procedure

wilt uitvoeren. Bijvoorbeeld, hier wordt het gedaan voor de Systemcontroller in sleuf 29:

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

5. Controleer de blok grootte van elke schijf met `fdisk-l`. Op een N3K-C3064PQ-10X heeft het alleen `/dev/sda @ 512 bytes` blok size, zie hier:

Opmerking: Op sommige Cisco Nexus-switches kan er meer dan één schijf zijn. Hiermee moet rekening worden gehouden bij het uitvoeren van de `dd`-operatie. Bijvoorbeeld N7K-SUP2 is `/dev/sda`, `/dev/sdb`, `/dev/sdc`, `/dev/md2`, `/dev/md3`, `/dev/md4`, `/dev/md5` en `/dev/md6`. U moet de `dd` uitvoeren op elk van deze apparaten om de beveiligde wisseringsprocedure correct te voltooien.

Opmerking: Op Cisco Nexus 9000 Series-switches heeft de systeemcontroller `beschikt/dev/mtblok0`, `/dev/mtdblock1`, `/dev/mtbloc2`, `/dev/mtdblock3`, `/dev/mtdblock4`, `/dev/mtdblock5` en `/dev/mtdblock tdblok 6`. U moet de `dd`-handeling op elk van deze apparaten uitvoeren om de beveiligde wisprocedure correct te voltooien.

```
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. Schrijf een nulbyte aan elke sector op de schijf.

Opmerking: Deze test werd uitgevoerd op een N3K-C3064PQ-10X met een Intel Celeron CPU P4505 @1,87 GHz en 13G eUSB, het proces van Zero-Byte duurde ~501 seconden.

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

Opmerking: Verwacht wordt dat Kernel berichten op sommige onderdelen bij deze stap gegenereerd zullen worden.

7. Zodra stap 5 is voltooid, laadt u de schakelaar, supervisor of systeemcontroller opnieuw:

Opmerking: Om de systeemcontroller in een Cisco Nexus 9000 Series modulaire switch te herladen, voert u de module `<sleuf_number>CLI` in.

```
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
```

Gebruik dd om Nul-byte naar relevante partities op I/O-module te schrijven

1. Meld u aan bij de beheeraccount van de schakelaar via de console-poort.

2. Schakel **terug** in **vanaf** de **basis-shell** van de configuratiemodus en voer de Bash-prompt in met **run bash** (alleen N3K/N9K). Andere Cisco Nexus switches hebben een debug plug-in nodig om toegang tot Bash te krijgen). Als u een debug plug-in nodig hebt, neemt u contact op met Cisco TAC en volgt u stap 3 in plaats van stap 2.

Opmerking: Voer vanuit de Bash-prompt **rlogin lc#** CLI in om toegang tot de LC/FM te krijgen nadat u worteltoegang hebt verkregen. Vervang nu de **#** in de CLI met het nummer van de sleuf waarop u de handeling wilt uitvoeren.

```
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. Voor Cisco Nexus-switches die plug-in gebruiken, dient u te waarborgen dat de stekker voor de softwarerelease niet wordt gekopieerd naar bootflitser en de stekker voor het reinigen van de stekker op de module waarvoor u de beveiligde wisseprocedure wilt uitvoeren:

Opmerking: Er is een afzonderlijk debug plug-in beeld dat moet worden gebruikt voor Nexus 7000 Series switches I/O-modules in vergelijking met de debug plug-in afbeelding die beschikbaar is voor Supervisor modules. Gebruik het LC-beeld voor de softwarerelease die op de schakelaar draait.

```
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. Bepaal vervolgens voor Cisco Nexus 7000 Series lijnkaarten waar **/flitser/** en **/mnt/pss** op het bestandssysteem is gemonteerd. Om dit te doen, gebruik de bergopdracht om te vinden waar **/mnt/plog** (logflitser) en **/mnt/pss** verblijft.

Opmerking: Voer voor Cisco Nexus 9000 Series lijnkaarten de DD-handeling uit op `dev/mme10`.

Opmerking: Voer voor Cisco Nexus 9000 Series fabric-modules de DD-handeling uit op `/TCP/dev/root`, `/dev/zram0`, `/dev/loop0`, `/dev/loop1` en `/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. Nu bekend is dat `/mnt/plog` op `dev/mtdblock2` en `/mnt/pss` op `/tmpfs` verblijft, schrijft u Zero-Byte aan zowel de hand van dd-opdracht, de uitgang van de debug-stekker en het opnieuw laden van de 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#
```

De switch herstellen en het besturingssysteem opnieuw installeren

Nadat u de schakelaar op het apparaat hebt aangezet, start de machine op in de vraag.

Om te herstellen van de `loader>`-prompt moet de schakelaar TFTP volgens de volgende stappen worden gestart:

1. Stel een IP-adres in (of wijs dit toe) op een GMT0-interface in de switch:

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

2. Als de TFTP-server waarvan u start in een andere vorm is, moet u een standaardgateway aan de switch toewijzen:

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

3. Start het laarsproces uit. De schakelaar start op de schakelaar (start).

Opmerking: Voor switches die afzonderlijke systeem/kickstart-afbeeldingen gebruiken, zoals Cisco Nexus 5000 Series-switches, Cisco Nexus 6000 Series-switches en Cisco Nexus 7000 Series-switches, moet u in deze stap het kickstart-beeld opstarten. Voor switches die één NXOS-afbeelding gebruiken, zoals Cisco Nexus 9000 Series-switches en Cisco Nexus 3000 Series-switches, moet u bij deze stap het enkele beeld starten:

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

4. Voer duidelijke informatie-, informatie- en signaaluitvoer uit:

Opmerking: Voor Cisco Nexus 5000 Series-switches en Cisco Nexus 6000 Series-switches is duidelijk nvram niet beschikbaar bij **switch(start)#**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. Herladen van de schakelaar:

```
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. Stel een IP-adres in (of wijs dit toe) op een GMT0-interface in de switch:

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

7. Als de TFTP-server waarvan u start in een andere vorm is, moet u een standaardgateway aan de switch toewijzen:

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

8. Herladen van de schakelaar:

Opmerking: Deze stap (8) is **NIET** vereist wanneer deze procedure wordt uitgevoerd op Cisco Nexus 5000 Series switches, Cisco Nexus 6000 Series switches, Cisco Nexus 7000 Series switches voor supervisor modules of Cisco Nexus 9000 Series switches voor supervisor module. Naar stap 9 als u deze procedure op een Cisco Nexus 5000 Series-switches, Cisco Nexus 6000 Series-switches, Cisco Nexus 7000 Series supervisor-module of Cisco Nexus 9000 Series supervisor-modules uitvoert.

```
loader> reboot
```

9. Start het laarsproces uit. De schakelaar start op de **schakelaar(de laars)** herinnering.

Opmerking: Voor switches die afzonderlijke systeem/kickstart-afbeeldingen gebruiken, zoals Cisco Nexus 7000 Series-switches, moet u bij deze stap het kickstart-beeld opstarten. Voor switches die één NXOS-afbeelding gebruiken, zoals Cisco Nexus 9000 Series-switches en Cisco Nexus 3000 Series-switches, moet u bij deze stap het enkele beeld starten:

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

10. Voor switches die afzonderlijke systeem/kickstart-afbeeldingen gebruiken, zoals Cisco Nexus 5000 Series-switches, Cisco Nexus 6000 Series-switches en Cisco Nexus 7000 Series-switches, moet u bij deze stap enkele extra stappen ondernemen om de switch te starten. U moet het IP-adres en het subnetmasker van GIGIT configureren en de standaardgateway definiëren. Nadat dit is voltooid, kunt u de kickstart en het systeembeeld naar de schakelaar kopiëren en deze 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. Voor Cisco Nexus 5000 Series-switches, voeren Cisco Nexus 6000 Series-switches en Cisco Nexus 7000 Series Supervisor-modules via de **switch(start)#** prompt in **load-flitser:<system_image>**. Hiermee wordt het laarsproces van de switch voltooid.

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

12. Zodra het systeembeeld met succes is geladen, moet u de setup-melding doorlopen om het apparaat aan uw gewenste specificaties te configureren.