NXOS - Effacer en toute sécurité le contenu du disque

Contenu

Introduction

Ce document décrit comment essuyer en toute sécurité le disque d'un commutateur Cisco Nexus, qui utilise des utilitaires Linux standard. Cela est nécessaire pour certains clients militaires et gouvernementaux qui déplacent de l'équipement d'une zone sécurisée vers une zone non sécurisée, ou pour tout autre client qui a des exigences de conformité pour déplacer l'équipement hors de leur site.

Informations générales

Il existe deux options qui dépendent du fait que le commutateur possède un disque SSD ou un lecteur eUSB :

- Init-System est utilisé sur les commutateurs de modèles plus récents avec des disques SSD. Init-System utilise l'effacement sécurisé ATA pour écrire des 0 binaires sur tous les secteurs du lecteur.
- Pour les anciens modèles de commutateurs dotés de lecteurs eUSB, vous pouvez également écrire des 0 dans tous les secteurs du lecteur, à l'aide de la méthode d'effacement automatique des octets.

Les utilitaires standard utilisés dans la procédure documentée utilisent une série de commandes qui détruisent en toute sécurité les données sur le disque de stockage et, dans la plupart des cas, rendent difficile ou impossible la récupération des données.

Ce guide vous guide dans les deux processus avec les commutateurs Cisco Nexus 3000, les commutateurs Cisco Nexus 5000, les commutateurs Cisco Nexus 9000, les commutateurs Cisco Nexus 7000 et les commutateurs Cisco MDS en tête, mais il fonctionne pour la plupart des autres commutateurs Cisco Nexus, à condition que vous ayez un accès système intégré ou Bash. Si le commutateur que vous utilisez ou la version logicielle que vous utilisez ne prend pas en charge l'activation de **feature bash** pour accéder au shell Bash, ouvrez une demande de service avec le TAC Cisco pour obtenir de l'aide sur l'utilisation d'un plug-in de débogage pour cette procédure.

Comment déterminer la procédure appropriée pour vous-même ?

si votre PID renvoie une valeur de **0**, le système utilise un SSD et peut utiliser la méthode Init-System pour effacer le lecteur.

Si votre PID renvoie une valeur de **1**, le système utilise un lecteur eUSB et vous devez utiliser la méthode d'effacement automatique de octets.

```
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$
```

Après avoir effectué la procédure précédente, s'il n'est toujours pas clair quel type de lecteur se trouve dans votre système et quelle procédure doit être utilisée pour effacer le contenu du disque en toute sécurité, ouvrez une demande de service avec le TAC Cisco.

Préparation

Avant d'effacer votre lecteur, vous devez disposer des éléments suivants :

1. Accès console au commutateur.
2. Accès à un serveur TFTP via l'interface management0, nécessaire pour sauvegarder la configuration actuelle, puis pour restaurer le système d'exploitation.
3. Une sauvegarde de la configuration en cours et de tous les autres fichiers que vous voulez enregistrer hors connexion du système lors de leur destruction dans ce processus !

Note: Il est fortement recommandé d'effectuer cette procédure sur les pièces qui ne sont plus en production ou installées dans les châssis de production. Les périphériques ou les pièces doivent être déplacés dans un environnement de non-production avant d'exécuter cette procédure afin d'éviter toute interruption involontaire du réseau.

Utilisation de la procédure Init-System sur les commutateurs avec SSD

Note: Lors de l'exécution de cette procédure sur un superviseur à l'intérieur d'un commutateur modulaire, il est recommandé de n'avoir que le superviseur que vous prévoyez d'installer dans le système.

1. Rechargez ou mettez le commutateur hors tension puis sous tension lorsqu'il est connecté via la console.

2. Pendant le démarrage du commutateur, utilisez CTRL-C pour diviser le commutateur en chargeur>.

3. Àpartir de l'invite loader>, entrez cmdline recovery ymode=1. Ceci arrête le démarrage du commutateur à l'invite **switch(boot)#** :

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

4. Commencez la procédure de démarrage avec **boot bootflash:<nxos_filename.bin>**.

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

5. Le commutateur démarre à l'invite **switch(boot)#**. À cette invite, écrivez des 0 à tous les blocs dans nvram, à l'exception des blocs de licence, en utilisant **clear nvram** CLI ainsi que **init system** CLI. **Note**: ce test a été effectué sur un N9K-C9372TX-E avec un processeur Intel Core i3- à 2,50 GHz et un disque SSD 110 G. La durée totale du système d'initialisation a pris environ 8 secondes :

```
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. Une fois l'étape 5 terminée, rechargez le commutateur :

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

Utiliser la procédure dd sur les commutateurs/superviseurs/contrôleurs système avec eUSB

1. Connectez-vous au compte d'administration du commutateur via le port de console.

   Note: Lorsque vous exécutez cette procédure sur un superviseur à l'intérieur d'un commutateur modulaire, il est recommandé de n'installer que le superviseur que vous prévoyez d'installer dans le système.

2. Activez **feature bash-shell** à partir du mode de configuration et entrez l'invite Bash avec **run bash** (N3K/9K uniquement). D'autres commutateurs Cisco Nexus ont besoin d'un plug-in de débogage pour accéder à 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. Obtenir l'accès racine avec **sudo su -**

   Note: Cette étape peut être ignorée pour les commutateurs Cisco Nexus 7000 qui utilisent un plug-in de débogage pour cette procédure.

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

4. Si vous exécutez cette procédure sur un contrôleur système installé dans un commutateur Nexus 9000, vous devez vous connecter à distance au numéro de logement sur lequel vous souhaitez effectuer cette procédure. Par exemple, ici, cela est fait pour le contrôleur système dans le logement 29 :

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

5. Vérifiez la taille de bloc de chaque disque avec fdisk -l. Sur un N3K-C3064PQ-10X, il n'a que /dev/sda @ taille de bloc de 512 octets, voir ici :

> **Note**: Sur certains commutateurs Cisco Nexus, il peut y avoir plusieurs disques. Il doit être pris en compte lorsque vous effectuez l'opération dd. Par exemple, N7K-SUP2 contient /dev/sda, /dev/sdb, /dev/sdc/, /dev/md2, /dev/md3, /dev/md4, /dev/md5 et **/dev/md6**. Vous devez effectuer l'opération dd sur chacune de ces opérations pour terminer correctement la procédure d'effacement sécurisé.

> **Note**: Sur les commutateurs de la gamme Cisco Nexus 9000, le contrôleur système dispose de /dev/mtdblock0, /dev/mtdblock1, /dev/mtdbloc2, /dev/mtdblock3, /dev/mtdblock4, **/dev/mtdblock5** et **/dev/mtdblock6**. Vous devez exécuter l'opération dd sur chacune de ces opérations pour effectuer correctement la procédure d'effacement sécurisé.

```
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. Écrivez un octet zéro dans chaque secteur du disque.

> **Note**: Ce test a été effectué sur un N3K-C3064PQ-10X avec un processeur Intel Celeron P4505 à 1,87 GHz et 13G eUSB, le processus Zero-Byte a pris ~501 secondes.

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

> **Note**: Il est prévu que les messages du noyau générés à cette étape apparaissent sur certaines parties.

7. Une fois l'étape 5 terminée, rechargez le commutateur, le superviseur ou le contrôleur système

:

> **Note**: Afin de recharger le contrôleur système dans un commutateur modulaire de la gamme Cisco Nexus 9000, entrez l'interface de ligne de commande **du module de rechargement <slot_number>**.

```
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
```

Utiliser dd pour écrire des octets nuls sur les partitions pertinentes sur le module E/S

1. Connectez-vous au compte d'administration du commutateur via le port de console.

2. Activez **feature bash-shell** à partir du mode de configuration et entrez l'invite Bash avec **run bash** (N3K/N9K uniquement). D'autres commutateurs Cisco Nexus ont besoin d'un plug-in de débogage pour accéder à Bash). Si vous avez besoin d'un plug-in de débogage, contactez le TAC Cisco et suivez l'étape 3 au lieu de l'étape 2.

> **Note**: Afin d'accéder à LC/FM à partir de Bash-prompt, entrez **rlogin lc#**CLI une fois que vous avez obtenu l'accès racine. Remplacez maintenant le **#** dans l'interface de ligne de commande par le numéro de logement sur lequel vous souhaitez effectuer l'opération.

```
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. Pour les commutateurs Cisco Nexus qui utilisent le plug-in de débogage, assurez-vous que le plug-in de débogage de la version logicielle en cours d'exécution est copié sur bootflash et chargez le plug-in de débogage sur le module pour lequel vous souhaitez exécuter la procédure d'effacement sécurisé pour :

> **Note**: Il existe une image de plug-in de débogage distincte à utiliser pour les modules d'E/S des commutateurs Nexus 7000, par opposition à l'image de plug-in de débogage disponible pour les modules Supervisor. Utilisez l'image LC pour la version logicielle qui s'exécute sur le commutateur.

```
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. Ensuite, pour les cartes de ligne Cisco Nexus 7000, déterminez où **/logflash/** et/**mnt/pss** est monté sur le système de fichiers. Pour ce faire, utilisez la commande mount pour trouver où **/mnt/plog** (logflash) et **/mnt/pss** résident.

> **Note**: Pour les cartes de ligne de la gamme Cisco Nexus 9000, effectuez l'opération dd sur **/dev/mmcblk0**.

> **Note**: Pour les modules de fabric de la gamme Cisco Nexus 9000, exécutez l'opération dd sur /tmpfs, /dev/root, /dev/zram0, **/dev/loop0**, **/dev/loop1** et **/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. Maintenant qu'il est connu que **/mnt/plog** réside sur **/dev/mtdblock2** et **/mnt/pss** réside sur **/tmpfs**, vous écrivez Zero-Byte aux deux à l'aide de la commande dd, quittez le plug-in de débogage et rechargez le 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#
```

Récupérer le commutateur et réinstaller le système d'exploitation

Après avoir mis le commutateur hors tension, il démarre à l'invite du chargeur.

Afin de récupérer à partir de l'invite loader**>**, le commutateur doit être amorcé TFTP selon les étapes suivantes :

1. Définissez (ou Affectez) une adresse IP à l'interface mgmt0 sur le commutateur :

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

2. Si le serveur TFTP à partir duquel vous démarrez se trouve dans un sous-réseau différent, affectez une passerelle par défaut au commutateur :

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

3. Exécutez le processus de démarrage. Le commutateur démarre à l’invite switch(boot).

> **Note**: Pour les commutateurs qui utilisent des images système/démarrage séparées, telles que les commutateurs Cisco Nexus 5000, les commutateurs Cisco Nexus 6000 et les commutateurs Cisco Nexus 7000, vous devez à cette étape démarrer l'image de démarrage. Pour les commutateurs qui utilisent une seule image NXOS, comme les commutateurs Cisco Nexus 9000 et les commutateurs Cisco Nexus 3000, à cette étape, vous devez démarrer l'image unique :

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

4. Exécuter la commande clear nvram, Init system et formater bootflash:

> **Note**: Pour les commutateurs Cisco Nexus 5000 et Cisco Nexus 6000, la commande clear nvram n'est pas disponible à l'invite **switch(boot)#**.

```
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. Recharger le commutateur :

```
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. Définissez (ou Affectez) une adresse IP à l'interface mgmt0 sur le commutateur :

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

7. Si le serveur TFTP à partir duquel vous démarrez se trouve dans un sous-réseau différent, affectez une passerelle par défaut au commutateur :

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

8. Recharger le commutateur :

Note: Cette étape (8) n'est **PAS** requise lorsque cette procédure est exécutée sur les commutateurs de la gamme Cisco Nexus 5000, les commutateurs de la gamme Cisco Nexus 6000, les modules Supervisor des commutateurs de la gamme Cisco Nexus 7000 ou le module Supervisor des commutateurs de la gamme Cisco Nexus 9000. Passez à l'étape 9 si vous exécutez cette procédure sur un commutateur Cisco Nexus 5000, un commutateur Cisco Nexus 6000, un module de supervision de commutateur Cisco Nexus 7000 ou un module de supervision de commutateurs Cisco Nexus 9000.

```
loader> reboot
```

9. Exécutez le processus de démarrage. Le commutateur démarre à l'invite **switch(boot)**.

Note: Pour les commutateurs qui utilisent des images système/démarrage séparées, comme les commutateurs Cisco Nexus 7000, à cette étape, vous devez démarrer l'image de démarrage. Pour les commutateurs qui utilisent une seule image NXOS, comme les commutateurs Cisco Nexus 9000 et les commutateurs Cisco Nexus 3000, à cette étape, vous devez démarrer l'image unique :

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

10. Pour les commutateurs qui utilisent des images système/démarrage séparées, telles que les commutateurs Cisco Nexus 5000, les commutateurs Cisco Nexus 6000 et les commutateurs Cisco Nexus 7000, vous devez à cette étape prendre des mesures supplémentaires pour démarrer le commutateur. Vous devez configurer l'adresse IP et le masque de sous-réseau de gestion 0, ainsi que définir la passerelle par défaut. Une fois cette opération terminée, vous pouvez copier l'image système et de démarrage sur le commutateur et la charger :

```
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. Pour les commutateurs Cisco Nexus 5000, les commutateurs Cisco Nexus 6000 et les modules Supervisor de commutation Cisco Nexus 7000, à partir de l'**invite switch(boot)#**, entrez **load bootflash:<system_image>**. Ceci termine le processus de démarrage du commutateur.

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

12. Une fois que l'image système s'est correctement chargée, vous devez passer par l'invite de configuration pour commencer à configurer le périphérique conformément aux spécifications souhaitées.