NXOS: borre de forma segura el contenido del disco

Contenido

Introducción

Este documento describe cómo borrar de forma segura el disco de un switch Cisco Nexus, que utiliza utilidades estándar de Linux. Esto es necesario para que algunos clientes militares y gubernamentales que mueven equipos de una zona protegida a una zona no protegida, o para cualquier otro cliente que tenga requisitos de cumplimiento, se desplacen los equipos de sus instalaciones.

Antecedentes

Hay dos opciones que dependen de si el switch tiene una unidad SSD o eUSB:

- Init-System se utiliza en switches de modelos más recientes con SSD. Init-System utiliza ATA Secure erase para escribir 0 binarios en todos los sectores de la unidad.
- En el caso de los switches modelo más antiguos con unidades eUSB, también puede escribir 0 en todos los sectores de la unidad mediante el método de eliminación de bytes cero.

Las utilidades estándar utilizadas en el procedimiento documentado utilizan una serie de comandos que destruyen de forma segura los datos en el disco de almacenamiento y, en la mayoría de los casos, dificultan o hacen imposible la recuperación de los datos.

Esta guía le guía a través de ambos procesos con los switches Nexus de Cisco serie 3000, los switches Nexus de Cisco serie 5000, los switches Nexus de Cisco serie 9000, los switches Nexus de Cisco serie 7000 y los switches Cisco serie MDS en mente, pero funciona para la mayoría de los otros switches Nexus de Cisco, siempre que disponga de acceso en el sistema informático o Bash. Si el switch que tiene o la versión de software que está ejecutando no tiene soporte para habilitar **bash de funciones** para obtener acceso al shell Bash, abra una Solicitud de servicio con Cisco TAC para obtener ayuda con el uso de un complemento de depuración para este procedimiento.

¿Cómo determinar el procedimiento adecuado para usted mismo?

si su PID devuelve un valor de **0**, el sistema utiliza una SSD y puede utilizar el método Init-System para borrar la unidad.

Si su PID devuelve un valor de **1**, el sistema está utilizando una unidad eUSB y necesita utilizar el método Zero-Byte Erase (Borrado de Bytes Cero).

```
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$
```

Después de realizar el procedimiento anterior, si todavía no está claro qué tipo de unidad se encuentra en su sistema y qué procedimiento se debe utilizar para borrar de forma segura el contenido del disco, abra una solicitud de servicio con el TAC de Cisco.

Preparación

Antes de borrar la unidad, debe tener lo siguiente:

1. Acceso de consola al switch.
2. Acceso a un servidor TFTP a través de la interfaz management0 - que es necesario para realizar una copia de seguridad de la configuración actual y luego restaurar el sistema operativo.
3. Una copia de seguridad de running-config y de cualquier otro archivo que desee guardar del sistema sin conexión, ya que se destruirán en este proceso.

Nota: Se recomienda encarecidamente que realice este procedimiento en las partes que ya no están en producción o instaladas en los chasis de producción. Los dispositivos o las piezas deben moverse a un entorno de no producción antes de realizar este procedimiento para evitar cualquier interrupción involuntaria de la red.

Utilice el procedimiento de inicialización en switches con SSD

Nota: Al realizar este procedimiento en un Supervisor dentro de un switch basado en módulos, se recomienda que sólo tenga instalado el Supervisor que planea realizar el procedimiento en el sistema.

1. Recargue o apague el switch mientras se conecta a través de la consola.

2. Mientras se inicia el switch, utilice CTRL-C para interrumpir el switch en loader> prompt.

3. Desde el mensaje loader>, ingrese cmdline recovery ymode=1. Esto detiene el arranque del switch en el mensaje **switch(boot)#**:

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

4. Inicie el procedimiento de inicio con **boot bootflash:<nxos_filename.bin>**.

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

5. El switch se inicia en el mensaje **switch(boot)#**. En este mensaje, escriba 0 a todos los bloques en nvram, excepto los bloques de licencia, usando **clear nvram** CLI así como **init system** CLI. **Nota:** esta prueba se llevó a cabo en un N9K-C9372TX-E con una CPU Intel Core i3- a 2,50 GHz y una SSD de 110 G. El tiempo total para el sistema de inicialización tardó unos 8 segundos:

```
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. Una vez completado el paso 5, recargue el switch:

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

Utilice el procedimiento dd en switches/supervisores/controladores del sistema con eUSB

1. Inicie sesión en la cuenta de administración del switch a través del puerto de la consola.

   Nota: Cuando realiza este procedimiento en un Supervisor dentro de un switch basado en módulos, se recomienda tener solamente el Supervisor que planea realizar el procedimiento instalado en el sistema.

2. Habilite **feature bash-shell** del modo de configuración e ingrese el mensaje Bash con **run bash** (sólo N3K/9K. Otros switches Cisco Nexus necesitan un complemento de depuración para obtener acceso a 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. Obtenga acceso raíz con **sudo su -**

   Nota: Este paso se puede omitir para los switches Nexus de Cisco serie 7000 que utilizan un complemento de depuración para este procedimiento.

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

4. Si está realizando este procedimiento en un controlador de sistema instalado en un switch

Nexus serie 9000, debe iniciar sesión de forma remota en el número de ranura en el que desea realizar este procedimiento. Por ejemplo, aquí se hace para el controlador del sistema en la ranura 29:

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

5. Verifique el tamaño de bloque de cada disco con fdisk -l. En un N3K-C3064PQ-10X sólo tiene /dev/sda @ 512 bytes de tamaño de bloque, vea aquí:

> **Nota:** En algunos switches Cisco Nexus puede haber más de un disco. Debe tenerse en cuenta al realizar la operación dd. Por ejemplo, N7K-SUP2 hay /dev/sda, /dev/sdb, /dev/sdc/, /dev/md2, /dev/md3, /dev/md4, /dev/md5, y /dev/md6. Debe realizar la operación dd en cada uno de estos para completar correctamente el procedimiento de borrado seguro.

> **Nota:** En los switches Nexus de Cisco serie 9000, el controlador del sistema tiene /dev/mtdblock0, /dev/mtdblock1, /dev/mtdbloc2, /dev/mtdblock3, /dev/mtdblock4, /dev/mtdblock5, y /dev/mtdblock6. Debe realizar la operación dd en cada uno de estos para completar correctamente el procedimiento de borrado seguro.

```
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. Escriba un byte cero en cada sector del disco.

> **Nota:** Esta prueba se llevó a cabo en un N3K-C3064PQ-10X con una CPU Intel Celeron P4505 a 1,87 GHz y 13G eUSB, el proceso de byte cero tardó unos 501 segundos.

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

> **Nota:** Se espera ver mensajes del núcleo generados en este paso en algunas partes.

7. Una vez completado el paso cinco, recargue el switch, el supervisor o el controlador del sistema:

> **Nota:** Para recargar el controlador del sistema en un switch modular Cisco Nexus serie 9000, ingrese el **módulo de recarga <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
```

Utilice dd para escribir el byte cero en las particiones relevantes del módulo de E/S

1. Inicie sesión en la cuenta de administración del switch a través del puerto de la consola.

2. Habilite **feature bash-shell** del modo de configuración e ingrese el mensaje Bash con **run bash** (sólo N3K/N9K). Otros switches Cisco Nexus necesitan un complemento de depuración para obtener acceso a Bash). Si necesita un complemento de depuración, póngase en contacto con Cisco TAC y siga el paso 3 en lugar del paso 2.

> **Nota:** Para acceder a la LC/FM desde Bash-prompt, ingrese **rlogin lc#** CLI una vez que haya obtenido acceso root. Ahora reemplace **#** en la CLI por el número de ranura en el que desea realizar la operación.

```
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. Para los switches Nexus de Cisco que utilizan el plugin de depuración, asegúrese de que el plugin de depuración para la versión de software en ejecución se copie en bootflash y cargue el plugin de depuración en el módulo para el cual desea ejecutar el procedimiento de borrado seguro para:

> **Nota:** Hay una imagen de complemento de depuración independiente que se utilizará para los módulos de E/S de los switches Nexus serie 7000, en lugar de la imagen del complemento de depuración que se pone a disposición de los módulos de Supervisor. Utilice la imagen LC para la versión de software que se ejecuta en el 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. A continuación, para las tarjetas de línea Cisco Nexus serie 7000, determine dónde **/logflash/** y **/mnt/pss** se montan en el sistema de archivos. Para hacer esto, utilice el comando mount para encontrar dónde residen **/mnt/plog** (logflash) y **/mnt/pss**.

> **Nota:** Para tarjetas de línea Cisco Nexus serie 9000, realice la operación dd en **/dev/mmcblk0**.

> **Nota:** Para los módulos de fabric de Cisco Nexus serie 9000, realice la operación dd en /tmpfs, /dev/root, /dev/zram0, **/dev/loop0**, **/dev/loop1** y **/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. Ahora que se sabe que **/mnt/plog** reside en **/dev/mtdblock2** y **/mnt/pss** reside en **/tmpfs**, usted escribe Zero-Byte en ambos usando el comando dd, salga del plugin de debug y recargue el módulo:

```
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#
```

Recuperación del switch y reinstalación del sistema operativo

Después de apagar y encender el switch, se inicia en el indicador del cargador.

Para recuperarse de la indicación loader>, el switch debe arrancar TFTP según los siguientes pasos:

1. Establezca (o asigne) una dirección IP a la interfaz mgmt0 en el switch:

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

2. Si el servidor TFTP desde el que se inicia está en una subred diferente, asigne un gateway predeterminado al switch:

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

3. Realice el proceso de arranque. El switch se inicia en el mensaje switch(boot).

> **Nota:** Para los switches que utilizan imágenes de inicio/sistema independientes, como los switches Nexus de Cisco serie 5000, los switches Nexus de Cisco serie 6000 y los switches

Nexus de Cisco serie 7000, en este paso debe iniciar la imagen de inicio. Para los switches que utilizan una única imagen NXOS, como los switches Nexus de Cisco serie 9000 y los switches Nexus de Cisco serie 3000, en este paso debe iniciar la única imagen:

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

4. Ejecute clear nvram, Init system y format bootflash:

Nota: Para los switches Nexus de Cisco serie 5000 y los switches Nexus de Cisco serie 6000, clear nvram no está disponible en el mensaje **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. Cargue nuevamente el 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
```

6. Establezca (o asigne) una dirección IP a la interfaz mgmt0 en el switch:

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

7. Si el servidor TFTP desde el que se inicia está en una subred diferente, asigne un gateway predeterminado al switch:

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

8. Cargue nuevamente el switch:

Nota: Este paso (8) **NO** es necesario cuando se realiza este procedimiento en switches Nexus de Cisco serie 5000, switches Nexus de Cisco serie 6000, módulos Supervisor de switches Nexus de Cisco serie 7000 o módulo Supervisor de switches Nexus de Cisco serie 9000. Vaya al paso 9 si realiza este procedimiento en switches Nexus de Cisco serie 5000, switches Nexus de Cisco serie 6000, módulo supervisor de switches Nexus de Cisco serie 7000 o módulo supervisor de switches Nexus de Cisco serie 9000.

```
loader> reboot
```

9. Realice el proceso de arranque. El switch se inicia en el mensaje **switch(boot)**.

> **Nota:** Para los switches que utilizan imágenes de inicio/sistema independientes, como los switches Nexus de Cisco serie 7000, en este paso debe iniciar la imagen de inicio rápido. Para los switches que utilizan una única imagen NXOS, como los switches Nexus de Cisco serie 9000 y los switches Nexus de Cisco serie 3000, en este paso debe iniciar la única imagen:

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

10. En el caso de switches que utilizan imágenes de inicio/sistema independientes, como los switches Nexus de Cisco serie 5000, los switches Nexus de Cisco serie 6000 y los switches Nexus de Cisco serie 7000, en este paso debe dar algunos pasos adicionales para iniciar el switch. Debe configurar la dirección IP y la máscara de subred del mgmt 0, así como definir el gateway predeterminado. Una vez que esto se complete, puede copiar el inicio rápido y la imagen del sistema en el switch y cargarla:

```
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. Para los switches Nexus de Cisco serie 5000, los switches Nexus de Cisco serie 6000 y los módulos Supervisor del switch Nexus de Cisco serie 7000, desde la indicación **switch(boot)#**, introduzca **load bootflash:<system_image>**. Esto finaliza el proceso de arranque del switch.

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

12. Una vez que la imagen del sistema se carga correctamente, debe pasar por el mensaje de configuración para comenzar a configurar el dispositivo según las especificaciones que desee.