NXOS - Cancellazione sicura del contenuto del disco

Sommario

Introduzione

In questo documento viene descritto come cancellare il contenuto del disco di uno switch Cisco Nexus, che utilizza utilità Linux standard. Ciò è necessario per alcuni clienti militari e governativi che spostano le apparecchiature da una zona protetta a una zona non protetta o per qualsiasi altro cliente che abbia requisiti di conformità per spostare le apparecchiature dalla propria sede.

Premesse

Sono disponibili due opzioni a seconda che lo switch disponga di un'unità SSD o eUSB:

- Init-System viene utilizzato sugli switch con SSD più recenti. Init-System utilizza ATA Secure erase per scrivere 0 binari in tutti i settori dell'unità.
- Per gli switch di modelli precedenti con unità eUSB, è inoltre possibile scrivere 0 in tutti i settori dell'unità, utilizzando il metodo Zero-Byte Erase.

Le utilità standard utilizzate nella procedura documentata utilizzano una serie di comandi che distruggono in modo sicuro i dati sul disco di storage e nella maggior parte dei casi rendono difficile o impossibile il recupero dei dati.

La presente guida illustra entrambi i processi con gli switch Cisco Nexus serie 3000, Cisco Nexus serie 5000, Cisco Nexus serie 9000, Cisco Nexus serie 7000 e Cisco MDS, ma è valida per la maggior parte degli altri switch Cisco Nexus, a condizione che si disponga di un accesso init-system o Bash. Se lo switch o la versione software in esecuzione non sono supportati per abilitare **feature bash** per accedere alla shell Bash, aprire una richiesta di servizio con Cisco TAC per ottenere assistenza nell'utilizzo di un plug-in di debug per questa procedura.

Come determinare la procedura adatta per se stessi?

se il PID restituisce il valore **0**, il sistema utilizza un'unità SSD e può utilizzare il metodo Init-System per cancellare l'unità.

Se il PID restituisce il valore **1**, il sistema utilizza un'unità eUSB ed è necessario utilizzare il metodo Zero-Byte Erase.

```
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$
```

Dopo aver eseguito la procedura precedente, se non è ancora chiaro quale tipo di unità è presente nel sistema e quale procedura utilizzare per cancellare in modo sicuro il contenuto del disco, aprire una richiesta di servizio con Cisco TAC.

Preparazione

Prima di cancellare il contenuto dell'unità, è necessario disporre dei seguenti elementi:

1. Accesso da console allo switch.
2. Accesso a un server TFTP tramite l'interfaccia management0, necessaria per eseguire il backup della configurazione corrente e ripristinare il sistema operativo.
3. Una copia di backup di running-config e di tutti gli altri file che si desidera salvare dal sistema in modalità offline.

Nota: Si consiglia vivamente di eseguire questa procedura su parti non più in produzione o installate nello chassis di produzione. Prima di eseguire questa procedura, è necessario spostare i dispositivi o le parti in un ambiente non di produzione per evitare interruzioni non intenzionali della rete.

Procedura di utilizzo di Init-System sugli switch con SSD

Nota: Quando si esegue questa procedura su un Supervisor all'interno di uno switch modulare, si consiglia di lasciare installato nel sistema solo il Supervisor che si intende eseguire.

1. Ricaricare o spegnere e riaccendere lo switch mentre è collegato tramite la console.

2. Durante l'avvio dello switch, utilizzare CTRL-C per visualizzare il prompt dello switch in loader>.

3. Dal prompt loader>, immettere cmdline recoverymode=1. In questo modo, l'avvio dello switch viene interrotto al prompt **switch(boot)#**:

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

4. Avviare la procedura di avvio con **boot bootflash:<nxos_filename.bin>**.

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

5. Lo switch viene avviato al prompt **switch(boot)#**. A questo prompt, 0 su tutti i blocchi nella nvram, ad eccezione dei blocchi di licenza, usando **clear nvram** CLI e **init system** CLI. **Nota:** questo test è stato eseguito su un N9K-C9372TX-E con una CPU Intel Core i3- a 2,50 GHz e un SSD 110G. Tempo totale per il sistema di inizializzazione impiegato circa 8 secondi:

```
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. Al termine del passaggio 5, ricaricare lo switch:

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

Uso della procedura Add su switch/supervisori/controller di sistema con eUSB

1. Accedere all'account admin dello switch tramite la porta della console.

   Nota: Quando si esegue questa procedura su un Supervisor all'interno di uno switch modulare, si consiglia di installare solo il Supervisor per il quale si intende eseguire la procedura.

2. Abilitare **feature bash-shell** dalla modalità di configurazione e immettere il prompt Bash con **run bash** (solo N3K/9K). per altri switch Cisco Nexus, è necessario un plug-in di debug per poter accedere 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. Ottenere l'accesso alla radice con **sudo su -**

   Nota: Questo passaggio può essere ignorato per gli switch Cisco Nexus serie 7000 che usano un plug-in di debug per questa procedura.

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

4. Se si esegue questa procedura su un controller di sistema installato in uno switch Nexus serie 9000, è necessario effettuare il login remoto al numero di slot sul quale si desidera eseguire questa procedura. Ad esempio, qui viene fatto per il Controller di sistema nello slot 29:

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

5. Verificare le dimensioni del blocco di ciascun disco con fdisk -l. Su un N3K-C3064PQ-10X ha solo /dev/sda @ 512 byte, vedere qui:

> **Nota:** Su alcuni switch Cisco Nexus potrebbero essere presenti più dischi. È necessario tenerne conto quando si esegue l'operazione di aggiunta. Ad esempio, N7K-SUP2 contiene /dev/sda, /dev/sdb, /dev/sdc/, /dev/md2, /dev/md3, /dev/md4, /dev/md5, e **/dev/md6**. Per completare correttamente la procedura di cancellazione sicura è necessario eseguire l'operazione dd su ognuna di esse.

> **Nota:** Sugli switch Cisco Nexus serie 9000, il controller di sistema dispone di /dev/mtdblock0, /dev/mtdblock1, /dev/mtdbloc2, /dev/mtdblock3, /dev/mtdblock4, **/dev/mtdblock5** e **/dev/mtdblock6**. Per completare correttamente la procedura di cancellazione sicura, è necessario eseguire l'operazione Add su ognuna di esse.

```
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. Scrivere un byte zero in ogni settore del disco.

> **Nota:** Questo test è stato eseguito su un N3K-C3064PQ-10X con una CPU Intel Celeron P4505 a 1,87 GHz e 13G eUSB. Il processo Zero-Byte ha richiesto circa 501 secondi.

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

> **Nota:** In questa fase è prevista la visualizzazione dei messaggi del kernel su alcune parti.

7. Una volta completato il passaggio cinque, ricaricare lo switch, il Supervisor o il controller di sistema:

> **Nota:** Per ricaricare il controller di sistema in uno switch modulare Cisco Nexus serie 9000, usare il comando **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
```

Utilizzare Add per scrivere zero byte nelle partizioni rilevanti sul modulo di I/O

1. Accedere all'account admin dello switch tramite la porta della console.

2. Abilitare **feature bash-shell** dalla modalità di configurazione e immettere il prompt Bash con **run bash** (solo N3K/N9K). per altri switch Cisco Nexus, è necessario un plug-in di debug per poter accedere a Bash). Se è necessario un plug-in di debug, contattare Cisco TAC e seguire il passaggio 3 anziché il passaggio 2.

> **Nota:** Per accedere al comando LC/FM dal prompt di Bash, immettere **rlogin lc#** CLI dopo aver ottenuto l'accesso alla directory principale. A questo punto, sostituire **#** nella CLI con il numero di slot su cui si desidera eseguire l'operazione.

```
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. Per gli switch Cisco Nexus che usano il plug-in di debug, verificare che il plug-in di debug per la versione software in esecuzione sia copiato su bootflash, quindi caricare il plug-in di debug sul modulo per cui si desidera eseguire la procedura di cancellazione sicura per:

> **Nota:** È disponibile un'immagine del plug-in di debug separata da utilizzare per i moduli di I/O degli switch Nexus serie 7000 rispetto all'immagine del plug-in di debug disponibile per i moduli Supervisor. Usare l'immagine LC per la versione software in esecuzione sullo 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. Quindi, per le schede di linea Cisco Nexus serie 7000, determinare dove **/logflash/** e **/mnt/pss** è montato sul file system. A tale scopo, utilizzare il comando mount per trovare dove risiedono **/mnt/plog** (logflash) e **/mnt/pss**.

> **Nota:** Per le schede di linea Cisco Nexus serie 9000, eseguire l'operazione Add su **/dev/mmcblk0**.

Nota: Per i moduli fabric Cisco Nexus serie 9000, eseguire l'operazione dd su /tmpfs, /dev/root, /dev/zram0, **/dev/loop0**, **/dev/loop1** e **/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. Ora che è noto che **/mnt/plog** risiede su **/dev/mtdblock2** e **/mnt/pss** risiede su **/tmpfs**, è possibile scrivere Zero-Byte su entrambi usando il comando dd, uscire dal plug-in di debug e ricaricare il modulo:

```
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#
```

Ripristino dello switch e reinstallazione del sistema operativo

Dopo aver spento e riacceso lo switch, l'avvio avviene nel prompt del caricatore.

Per eseguire il ripristino dal prompt loader**>**, lo switch deve essere avviato con il protocollo TFTP nel modo seguente:

1. Impostare (o assegnare) un indirizzo IP all'interfaccia mgmt0 sullo switch:

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

2. Se il server TFTP da cui si sta eseguendo l'avvio si trova in una subnet diversa, assegnare un gateway predefinito allo switch:

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

3. Eseguire il processo di avvio. Lo switch viene avviato al prompt switch(boot).

Nota: Per gli switch che usano immagini di sistema/kickstart separate, come gli switch Cisco Nexus serie 5000, Cisco Nexus serie 6000 e Cisco Nexus serie 7000, in questo passaggio è necessario avviare l'immagine kickstart. Per gli switch che usano una singola immagine NXOS, come gli switch Cisco Nexus serie 9000 e Cisco Nexus serie 3000, a questo punto è necessario avviare la singola immagine:

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

4. Eseguire clear nvram, Init system e format bootflash:

Nota: Sugli switch Cisco Nexus serie 5000 e Cisco Nexus serie 6000, la cancellazione della nvram non è disponibile al prompt **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. Ricaricare lo 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. Impostare (o assegnare) un indirizzo IP all'interfaccia mgmt0 sullo switch:

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

7. Se il server TFTP da cui si sta eseguendo l'avvio si trova in una subnet diversa, assegnare un gateway predefinito allo switch:

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

8. Ricaricare lo switch:

Nota: Questo passaggio (8) **NON** è richiesto quando la procedura viene eseguita su switch Cisco Nexus serie 5000, switch Cisco Nexus serie 6000, switch Cisco Nexus serie 7000, moduli Supervisor o switch Cisco Nexus serie 9000, modulo Supervisor. Andare al passaggio 9 se si esegue questa procedura su uno switch Cisco Nexus serie 5000, su uno switch Cisco Nexus serie 6000, su uno switch Cisco Nexus serie 7000, sul modulo Supervisor o su uno switch Cisco Nexus serie 9000.

```
loader> reboot
```

9. Eseguire il processo di avvio. Lo switch viene avviato al prompt **dello switch (avvio)**.

Nota: Per gli switch che usano immagini di sistema/kickstart separate, come gli switch Cisco Nexus serie 7000, in questa fase è necessario avviare l'immagine kickstart. Per gli switch

che usano una singola immagine NXOS, come gli switch Cisco Nexus serie 9000 e Cisco Nexus serie 3000, a questo punto è necessario avviare la singola immagine:

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

10. Per gli switch che usano immagini di sistema/kickstart separate, come gli switch Cisco Nexus serie 5000, Cisco Nexus serie 6000 e Cisco Nexus serie 7000, in questa fase è necessario eseguire alcuni passaggi aggiuntivi per avviare lo switch. È necessario configurare l'indirizzo IP e la subnet mask di gestione 0, nonché definire il gateway predefinito. Al termine, è possibile copiare la kickstart e l'immagine del sistema sullo switch e caricarla:

```
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. Per gli switch Cisco Nexus serie 5000, Cisco Nexus serie 6000 e i moduli Supervisor dello switch Cisco Nexus serie 7000, dal prompt **switch(boot)#**, immettere **load bootflash:<system_image>**. Il processo di avvio dello switch è terminato.

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

12. Una volta caricata correttamente l'immagine del sistema, è necessario passare attraverso il prompt di installazione per iniziare a configurare il dispositivo secondo le specifiche desiderate.