NXOS - Apague com segurança o conteúdo do disco

Contents

Introduction

Este documento descreve como limpar com segurança o disco de um switch Cisco Nexus, que utiliza utilitários Linux padrão. Isso é necessário para determinados clientes militares e governamentais que movem equipamentos de uma zona protegida para uma zona não segura ou para qualquer outro cliente que tenha requisitos de conformidade para transferir equipamentos para fora de suas instalações.

Informações de Apoio

Há duas opções que dependem de o switch ter uma unidade SSD ou eUSB:

- O Init-System é usado em switches de modelo mais novos com SSDs. O Init-System usa ATA Secure erase para gravar 0s binários em todos os setores da unidade.
- Para switches de modelo mais antigos com unidades de eUSB, você também pode gravar 0s em todos os setores da unidade, usando o método Zero-Byte Erase.

Os utilitários padrão usados no procedimento documentado usam uma série de comandos que destroem com segurança os dados no disco de armazenamento e, na maioria dos casos, dificultam ou impossibilitam a recuperação dos dados.

Este guia orienta os dois processos com switches Cisco Nexus 3000 Series, switches Cisco Nexus 5000 Series, switches Cisco Nexus 9000 Series, switches Cisco Nexus 7000 Series em mente, mas funciona para a maioria dos outros switches Cisco Nexus, desde que você tenha acesso inicial ao sistema ou básico. Se o switch que você tem ou a versão do software que você está executando não tiver suporte para habilitar o **bash de recursos** para obter acesso ao shell Bash, abra uma Solicitação de Serviço no Cisco TAC para obter assistência na utilização de um plug-in de depuração para este procedimento.

Como determinar o procedimento adequado para você mesmo?

se seu PID retornar um valor de **0**, o sistema está usando um SSD e pode usar o método Init-System para apagar a unidade.

Se o seu PID retornar um valor de **1**, o sistema está usando uma unidade de eUSB e você precisa usar o método 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$
```

Depois que o procedimento anterior for executado, se ainda não estiver claro qual o tipo de unidade no sistema e qual procedimento deve ser usado para limpar com segurança o conteúdo do disco, abra uma solicitação de serviço com o Cisco TAC.

Preparação

Antes de limpar a unidade, você deve ter os seguintes itens:

1. Acesso do console ao switch.
2. Acesso a um servidor TFTP através da interface management0 - que é necessário para fazer backup da configuração atual e, em seguida, restaurar o SO.
3. Um backup da configuração atual e de todos os outros arquivos que você deseja salvar do sistema off-line quando eles forem destruídos neste processo!

Note: É altamente recomendável executar este procedimento em peças que não estão mais em produção ou instaladas em chassis de produção. Os dispositivos ou peças devem ser movidos para um ambiente de não produção antes de executar este procedimento para evitar interrupções involuntárias na rede.

Usar procedimento de inicialização do sistema em switches com SSD

Note: Ao executar esse procedimento em um Supervisor dentro de um switch baseado em modular, é recomendável ter apenas o Supervisor que você planeja para executar o procedimento instalado no sistema.

1. Recarregue ou desligue e ligue o switch enquanto estiver conectado via console.

2. Enquanto o switch estiver inicializando, use CTRL-C para dividir o switch no prompt loader>.

3. No prompt loader>, digite cmdline recovery mode=1. Isso interrompe a inicialização do switch no prompt **(boot)#switch**:

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

4. Inicie o procedimento de inicialização com **boot bootflash:<nxos_filename.bin>**.

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

5. O switch é inicializado no prompt **switch(boot)#**. Nesse prompt de gravação, 0's para todos os blocos na nvram, exceto os blocos de licença, usando **clear nvram** CLI assim como **init system** CLI. **Note**: este teste foi realizado em um N9K-C9372TX-E com um Intel Core i3- CPU @ 2,50GHz e um SSD 110G. O tempo total do sistema de inicialização levou aproximadamente 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. Quando a etapa 5 for concluída, recarregue o switch:

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

Use o procedimento Adicionar em Switches/Supervisores/Controladores do sistema com eUSB

1. Faça login na conta admin do switch através da porta de console.

   Note: Ao executar este procedimento em um Supervisor dentro de um switch baseado em modular, é recomendável ter apenas o Supervisor que você planeja para executar o procedimento instalado no sistema.

2. Ative **o recurso bash-shell** do modo de configuração e digite o prompt Bash com **run bash** (somente N3K/9K). Outros switches Cisco Nexus precisam de um plug-in de depuração para obter acesso ao 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. Obtenha acesso raiz com **sudo su -**

   Note: Essa etapa pode ser ignorada para os switches Cisco Nexus 7000 Series que estão usando um plug-in de depuração para este procedimento.

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

4. Se estiver executando este procedimento em um Controlador de sistema instalado em um

Switch Nexus 9000 Series, você deverá fazer logon remoto no número de slot no qual deseja executar este procedimento. Por exemplo, aqui é feito para a controladora do sistema no slot 29:

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

5. Verifique o tamanho do bloco de cada disco com fdisk -l. Em um N3K-C3064PQ-10X ele tem apenas o tamanho de bloco /dev/sda @ 512 bytes, consulte aqui:

> **Note**: Em alguns switches Cisco Nexus, pode haver mais de um disco. Ele deve ser levado em conta ao executar a operação de adição. Por exemplo, N7K-SUP2 existe /dev/sda, /dev/sdb, /dev/sdc/, /dev/md2, /dev/md3, /dev/md4, /dev/md5 e **/dev/md6**. Você deve executar a operação de adição em cada um deles para concluir o procedimento de exclusão segura corretamente.

> **Note**: Nos switches Cisco Nexus 9000 Series, o Controlador de sistema tem /dev/mtdblock0, /dev/mtdblock1, /dev/mtdblock2, /dev/mtdblock3, /dev/mtdblock4, **/dev/mtdblock5** e **/dev/mtdblock6**. Você deve executar a operação de adição em cada um deles para concluir o procedimento de exclusão segura corretamente.

```
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. Escreva um byte zero em cada setor no disco.

> **Note**: Este teste foi realizado em um N3K-C3064PQ-10X com uma CPU Intel Celeron P4505 @1,87 GHz e 13G eUSB o processo de byte zero levou aproximadamente 501 segundos.

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

> **Note**: Espera-se que as mensagens do kernel sejam geradas nesta etapa em algumas partes.

7. Quando a etapa cinco for concluída, recarregue o switch, o supervisor ou o controlador do sistema:

> **Note**: Para recarregar a controladora do sistema em um switch modular Cisco Nexus 9000

Series, insira a CLI **do módulo de recarga <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
```

Use dd para gravar Zero-byte em partições relevantes no módulo de E/S

1. Faça login na conta admin do switch através da porta de console.

2. Ative **o recurso bash-shell** do modo de configuração e insira o Bash-prompt com **run bash** (somente N3K/N9K). Outros switches Cisco Nexus precisam de um plug-in de depuração para obter acesso ao Bash). Se você precisar de um plug-in de depuração, entre em contato com o Cisco TAC e siga a etapa 3 em vez da etapa 2.

> **Note**: Para acessar o LC/FM do prompt de base, insira **rlogin lc#** CLI depois de obter acesso de raiz. Agora substitua o **#** na CLI pelo número de slot no qual você deseja executar a operação.

```
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 os Switches Cisco Nexus que usam o plug-in de depuração, certifique-se de que o plug-in de depuração para a versão do software em execução seja copiado para o flash de inicialização e carregue o plug-in de depuração no módulo para o qual você deseja executar o procedimento de exclusão segura para:

> **Note**: Há uma imagem de plug-in de depuração separada a ser usada para os módulos de I/O dos Switches Nexus 7000 Series, ao contrário da imagem do plug-in de depuração disponibilizada para os módulos do Supervisor. Use a imagem LC para a versão de software que é executada no 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. Em seguida, para as placas de linha Cisco Nexus 7000 Series, determine onde **/logflash/** e **/mnt/pss** está montado no sistema de arquivos. Para fazer isso, use o comando mount para descobrir onde **/mnt/plog** (logflash) e **/mnt/pss** residem.

> **Note**: Para placas de linha Cisco Nexus 9000 Series, execute a operação dd em **/dev/mcblk0**.

> **Note**: Para os módulos de estrutura Cisco Nexus 9000 Series, execute a operação dd em /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. Agora que se sabe que **/mnt/plog** reside em **/dev/mtdblock2** e **/mnt/pss** reside em **/tmpfs**, você escreve Zero-Byte para ambos usando o comando dd, sai do plug-in de depuração e recarrega o 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#
```

Recupere o switch e reinstale o sistema operacional

Depois de ligar e desligar o switch, ele é inicializado no prompt do carregador.

Para se recuperar do prompt loader**>**, o switch deve ser inicializado pelo TFTP de acordo com as seguintes etapas:

1. Defina (ou Atribua) um endereço IP para a interface mgmt0 no switch:

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

2. Se o servidor TFTP do qual você está inicializando estiver em uma sub-rede diferente, atribua um gateway padrão ao switch:

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

3. Execute o processo de inicialização. O switch é inicializado no prompt do switch (boot).

> **Note**: Para os switches que usam imagens separadas de sistema/início, como os switches Cisco Nexus 5000 Series, os switches Cisco Nexus 6000 Series e os switches Cisco Nexus

7000 Series, nesta etapa você precisa inicializar a imagem de início rápido. Para switches que usam uma única imagem NXOS, como switches Cisco Nexus 9000 Series e switches Cisco Nexus 3000 Series, nesta etapa você precisa inicializar a imagem única:

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

4. Execute nvram nítida, sistema de inicialização e format bootflash:

Note: Para os switches Cisco Nexus 5000 Series e os switches Cisco Nexus 6000 Series, a nvram clara não está disponível no 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. Recarregue o 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. Defina (ou Atribua) um endereço IP para a interface mgmt0 no switch:

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

7. Se o servidor TFTP do qual você está inicializando estiver em uma sub-rede diferente, atribua um gateway padrão ao switch:

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

8. Recarregue o switch:

Note: Esta etapa (8) **NÃO** é necessária quando este procedimento é executado nos switches Cisco Nexus 5000 Series, nos switches Cisco Nexus 6000 Series, nos módulos Supervisor dos switches Cisco Nexus 7000 Series ou no módulo Supervisor dos switches Cisco Nexus 9000 Series. Vá para a etapa 9 se você executar este procedimento em um switch Cisco Nexus 5000 Series, em switches Cisco Nexus 6000 Series, no módulo supervisor do switch Cisco Nexus 7000 Series ou no módulo supervisor de switches Cisco

Nexus 9000 Series.

```
loader> reboot
```

9. Execute o processo de inicialização. O switch é inicializado no prompt **switch(boot)**.

> **Note**: Para switches que usam imagens separadas de sistema/início de linha, como os switches Cisco Nexus 7000 Series, nesta etapa você precisa inicializar a imagem de início de linha. Para switches que usam uma única imagem NXOS, como switches Cisco Nexus 9000 Series e switches Cisco Nexus 3000 Series, nesta etapa você precisa inicializar a imagem única:

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

10. Para switches que usam imagens de início/sistema separadas, como os switches Cisco Nexus 5000 Series, os switches Cisco Nexus 6000 Series e os switches Cisco Nexus 7000 Series, nesta etapa você precisa executar algumas etapas adicionais para inicializar o switch. Você precisa configurar o endereço IP e a máscara de sub-rede do mgmt 0, bem como definir o gateway padrão. Quando isso estiver concluído, você poderá copiar o kickstart e a imagem do sistema para o switch e carregá-lo:

```
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 os switches Cisco Nexus 5000 Series, os switches Cisco Nexus 6000 Series e os módulos supervisores do switch Cisco Nexus 7000 Series, do prompt **switch(boot)#**, insira **load bootflash:<system_image>**. Isso conclui o processo de inicialização do switch.

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

12. Quando a imagem do sistema for carregada com êxito, você precisará passar pelo prompt de configuração para começar a configurar o dispositivo de acordo com as especificações desejadas.