NXOS – ディスクの内容を安全に消去する

内容

概要

このドキュメントでは、標準のLinuxユーティリティを使用するCisco Nexusスイッチのディスクを安全にワイプする方法について説明します。 これは、特定の軍事および政府顧客が機器を安全なゾーンから非安全なゾーンに移動したり、コンプライアンス要件を持つ他の顧客が機器を構外に移動するために必要です。

背景説明

スイッチにSSDドライブとeUSBドライブのどちらが搭載されているかによって、次の2つのオプションがあります。

- Init-Systemは、SSDを搭載した新しいモデルスイッチで使用されます。Init-Systemは、ATA Secure eraseを使用して、ドライブのすべてのセクタにバイナリ0を書き込みます。
- eUSBドライブを搭載した旧型のスイッチでは、ゼロバイト消去方式を使用して、ドライブのすべてのセクタに0を書き込むこともできます。

ドキュメント化された手順で使用される標準ユーティリティでは、ストレージ・ディスク上のデータを安全に破棄する一連のコマンドを使用します。ほとんどの場合、データのリカバリが困難または不可能になります。

このガイドでは、Cisco Nexus 3000シリーズスイッチ、Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 9000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチ、およびCisco MDSシリーズスイッチの両方のプロセスについて説明します。ただし、initシステムまたはCisco Nexusスイッチがを使用しているのbashアクセス 実行しているスイッチまたはソフトウェアリリースが**feature bash**を有効にしてBashシェルにアクセスできない場合は、Cisco TACでサービスリクエストをオープンし、この手順のデバッグプラグインの使用に関するサポートを受けてください。

自分に適した手順を決定する方法

PIDが0の値を返す場合、システムはSSDを使用し、Init-System方式を使用してドライブを消去できます。

PIDが1の値を返す場合、システムは**eUSBドライブを使用**しており、ゼロバイト消去方式を使用する必要があります。

```
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$
```

上記の手順を実行した後で、システム内のドライブのタイプと、ディスクの内容を安全に消去するために使用する手順が不明な場合は、Cisco TACでサービスリクエストをオープンしてください。

準備

ドライブをワイプする前に、次の情報が必要です。

1. スイッチへのコンソールアクセス。
2. management0インターフェイスを介してTFTPサーバにアクセスします。これは、現在の設定をバックアップし、OSを復元するために必要です。
3. 実行コンフィギュレーションのバックアップと、システムからオフラインで保存するファイルは、このプロセスで破棄されます。

注：この手順は、実稼働していない部品や実稼働シャーシに取り付けられている部品に対して実行することを強くお勧めします。この手順を実行する前に、デバイスまたは部品を非実稼働環境に移動して、意図しないネットワークの中断を回避する必要があります。

SSD搭載スイッチでのInit-System手順の使用

注：この手順をモジュラベースのスイッチ内のスーパーバイザで実行する場合は、この手順を実行する予定のスーパーバイザだけをシステムにインストールすることをお勧めします。

1. コンソール経由で接続している間、スイッチをリロードまたは電源の再投入を行います。
2. スイッチのブート中に、Ctrl+Cを使用してスイッチをloader>プロンプトに分割します。
3. loader>プロンプトで、cmdline recoverymode=1と入力します。 これにより、スイッチのブートが**switch(boot)#プロンプトで停止**されます。

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

4. **boot bootflash:<nxos_filename.bin>**でブート手順を開始します。

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

5. スイッチが**switch(boot)#プロンプトで起動**します。 このプロンプトで、**clear nvram** CLIおよびinit system CLIを使用して、ライセンスブロックを除くnvram内のすべてのブロックに

0を書き込みます。 **注：**このテストは、Intel Core i3- CPU @ 2.50GHzおよび110G SSDを搭載したN9K-C9372TX-Eで実施されました。 init systemの合計時間は最大8秒かかりました。

```
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. ステップ5が完了したら、switch:

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

eUSBを使用したスイッチ/スーパーバイザ/システムコントローラでの追加手順

1. コンソールポート経由でスイッチのadminアカウントにログインします。

注：この手順をモジュラベースのスイッチ内のスーパーバイザで実行する場合は、その手順を実行する予定のスーパーバイザだけをシステムにインストールすることをお勧めします。

2.設定モードから機能bash-shellを有効にし、run bashでBashプロンプトを入力します(N3K/9Kのみ)。 他のCisco Nexusスイッチは、Bashにアクセスするためにデバッグプラグインが必要です)。

```
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. sudo suを使用してルートアクセスを取得します。

注：この手順でデバッグプラグインを使用しているCisco Nexus 7000シリーズスイッチでは、この手順をスキップできます。

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

4. Nexus 9000シリーズスイッチにインストールされたシステムコントローラでこの手順を実行する場合は、この手順を実行するスロット番号にリモートログインする必要があります。 たとえば、スロット29のシステムコントローラに対して次のように行われます。

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

5.各ディスクのブロックサイズをfdisk -lで確認します。 N3K-C3064PQ-10Xでは、ブロックサイ

ズが/dev/sda @ 512バイトしかありません。次を参照してください。

注：一部のCisco Nexusスイッチでは、複数のディスクが存在する場合があります。dd操作を実行する際には、この点を考慮する必要があります。たとえば、N7K-SUP2には、/dev/sda、/dev/sdb、/dev/sdc/、/dev/md2、/dev/md3、/dev/md4、/dev/md5、**/dev/md6**があり、これらをそれぞれ消去する必要があります手順を正しく説明します。

注：Cisco Nexus 9000シリーズスイッチでは、システムコントローラに/dev/mtdblock0、/dev/mtdblock1、/dev/mtdbloc2、/dev/mtdblock3、/dev/mtdblock4、/**dev/mtdblock5**、/**dev/mtdblock6があります。** セキュアな消去手順を正しく実行するには、これらの各ノードでdd操作を実行する必要があります。

```
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.ディスク上のすべてのセクタに0バイトを書き込みます。

注：このテストは、インテルCeleron CPU P4505 @1.87 GHzと13G eUSBを搭載したN3K-C3064PQ-10Xでゼロバイト処理に約501秒かかりました。

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

注：一部の部分では、このステップで生成されたカーネルメッセージが表示されます。

7.ステップ5が完了したら、スイッチ、スーパーバイザ、またはシステムコントローラをリロードします。

注：Cisco Nexus 9000シリーズモジュラスイッチでシステムコントローラをリロードするには、**reload module <slot_number>のCLIを入力**します。

```
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
```

ddを使用して、I/Oモジュールの関連パーティションに0バイトを書き込む

1.コンソールポート経由でスイッチのadminアカウントにログインします。

2.設定モードから機能bash-shellを有効にし、run bashでbash-promptを入力します（N3K/N9Kのみ）。 他のCisco Nexusスイッチは、Bashにアクセスするためにデバッグプラグインが必要です)。 デバッグプラグインが必要な場合は、Cisco TACに連絡し、ステップ2ではなくステップ3に従ってください。

> **注：**BashプロンプトからLC/FMにアクセスするには、rootアクセス権を取得した後でrlogin lc# CLIと入力します。ここで、CLIの#を、操作を実行するスロット番号に置き換えます。

```
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.デバッグプラグインを使用するCisco Nexusスイッチの場合、実行しているソフトウェアバージョンのデバッグプラグインがブートフラッシュにコピーされていることを確認し、次の場合に安全な消去手順を実行するモジュールにデバッグプラグインをロードします。

> **注：**Nexus 7000シリーズスイッチのI/Oモジュールには、スーパーバイザモジュールで使用できるデバッグプラグインイメージとは異なる、別のデバッグプラグインイメージが用意されています。スイッチで稼働するソフトウェアリリースには、LCイメージを使用します。

```
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.次に、Cisco Nexus 7000シリーズラインカードの場合は、ファイルシステム上の/logflash/および/mnt/pssのマウント先を決定します。 これを行うには、mountコマンドを使用して、/mnt/plog (logflash)および/mnt/pssの場所を検索します。

> **注：**Cisco Nexus 9000シリーズラインカードの場合は、/dev/mmcblk0でdd操作を実行します。

> **注：**Cisco Nexus 9000シリーズファブリックモジュールの場合は、/tmpfs、/dev/root、/dev/zram0、/dev/loop0、/dev/loop1、/unionfsでdd操作を実行します。

```
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. /mnt/plogが/dev/mtdblock2に、**/mnt/pssが/tmpfsに存在することが判明したのでは、ddコマンドを使用して両方に0バイトを書き込み、デバッグプラグインを終了し、モジュールをリロードします。**

```
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#
```

スイッチを回復してOSを再インストールする

スイッチの電源を再投入した後、ローダプロンプトで起動します。

loader>プロンプトから回復するには、次の手順に従ってスイッチをTFTPブートする必要があります。

1. スイッチのmgmt0インターフェイスにIPアドレスを設定（または割り当て）します。

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

2.ブート元のTFTPサーバが別のサブネットにある場合は、スイッチにデフォルトゲートウェイを割り当てます。

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

3.ブートプロセスを実行します。 スイッチがブートして、switch(boot)プロンプトが表示されます。

> **注：**Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 6000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチなど、別のシステム/キックスタートイメージを使用するスイッチの場合は、この手順でキックスタートイメージをブートする必要があります。 Cisco Nexus 9000シリーズスイッチやCisco Nexus 3000シリーズスイッチなど、単一のNXOSイメージを使用するスイッチの場合は、この手順で単一のイメージをブートする必要があります。

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

4. clear nvram、Init system、およびformat bootflash:

> **注：**Cisco Nexus 5000シリーズスイッチおよびCisco Nexus 6000シリーズスイッチの場合、**switch(boot)#プロンプトでclear nvram is not available**.

```
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.スイッチをリロードします。

```
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.スイッチのmgmt0インターフェイスにIPアドレスを設定（または割り当て）します。

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

7.ブート元のTFTPサーバが別のサブネットにある場合は、スイッチにデフォルトゲートウェイを割り当てます。

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

8.スイッチをリロードします。

> **注**：この手順(8)は、Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 6000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチのスーパーバイザモジュール、またはCisco Nexus 9000シリーズスイッチのスーパーバイザモジュールで実行する場合は必要ありません。 Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 6000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチスーパーバイザモジュール、またはCisco Nexus 9000シリーズスイッチスーパーバイザモジュールでこの手順を実行する場合は、ステップ9に進みます。

```
loader> reboot
```

9.ブートプロセスを実行します。 スイッチが**switch(boot)プロンプトにブート**します。

> **注**：Cisco Nexus 7000シリーズスイッチなど、別のシステム/キックスタートイメージを使用するスイッチの場合は、この手順でキックスタートイメージをブートする必要があります。 Cisco Nexus 9000シリーズスイッチやCisco Nexus 3000シリーズスイッチなど、単一のNXOSイメージを使用するスイッチの場合は、この手順で単一のイメージをブートする必要があります。

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

10. Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 6000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチなど、別のシステム/キックスタートイメージを使用するスイッチの場合は、この手順でスイッチをブートするためにいくつかの追加手順を実行する必要があります。 mgmt 0のIPアドレスとサブネットマスクを設定し、デフォルトゲートウェイを定義する必要があります。 これが完了したら、キックスタートイメージとシステムイメージをスイッチにコピーしてロードできます。

```
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. Cisco Nexus 5000シリーズスイッチ、Cisco Nexus 6000シリーズスイッチ、およびCisco Nexus 7000シリーズスイッチスーパーバイザモジュールの**switch(boot)#**プロンプトから、**load bootflash:<system_image>**と入力します。 これで、スイッチのブートプロセスが終了します。

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

12.システムイメージが正常にロードされたら、セットアッププロンプトに従って、デバイスの設定を目的の仕様に合わせる必要があります。