FMCによって管理されるCLIを介したFTD HAのアップグレード

内容

はじめに

このドキュメントでは、コマンドラインインターフェイス(CLI)を使用してCisco Firepower Threat Defense(FTD)デバイスをアップグレードする詳細な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center v7.2.8

- VMWare v7.2.2向けCisco Firepower Threat Defense

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

このドキュメントに関する特定の要件は次のとおりです。

- バージョン7.2以降を実行しているCisco Secure Firewall Threat Defense
- バージョン7.2以降を実行しているCisco Secure Firewall Management Center(FMC)

設定

CLIを使用してFTDデバイスのペアをアップグレードするには、デバイスにアップグレードパッケージファイルが存在している必要があります。CLIを使用して正常にアップグレードするには、前提条件として保留中の導入がないことが不可欠です。

アップグレードの準備

警告：アップグレード順序であるスタンバイ/アクティブを確認して、トラフィックの停止を回避してください。

1. スタンバイとして設定されているデバイスから開始します。

2. クライアントモードでexpertに続けてsudo suと入力し、expertモードでCLIにアクセスします。デバイスのパスワードを確認して権限を引き上げ、エキスパートモードに入ります。

```
Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 1104)
Cisco Firepower Threat Defense for VMware v7.2.2 (build 54)

> expert
admin@firepower:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
root@firepower:/home/admin#
root@firepower:/home/admin# cd
root@firepower:~#
root@firepower:~#
```

フェールオーバーステータスの確認

フェールオーバーステータスを確認して、手順がセカンダリFTDに適用されていることを確認します。セカンダリFTDは、セカンダリおよびスタンバイの準備完了として表示できます。

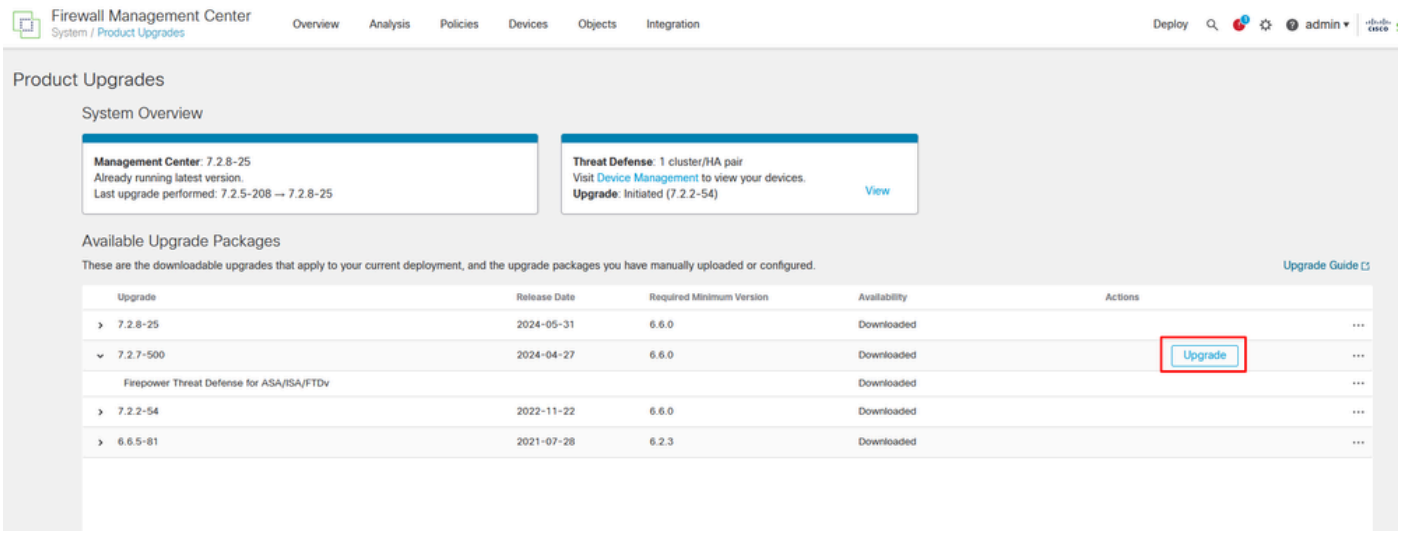
```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

```
firepower#
firepower#
```

アップグレードパッケージのアップロード

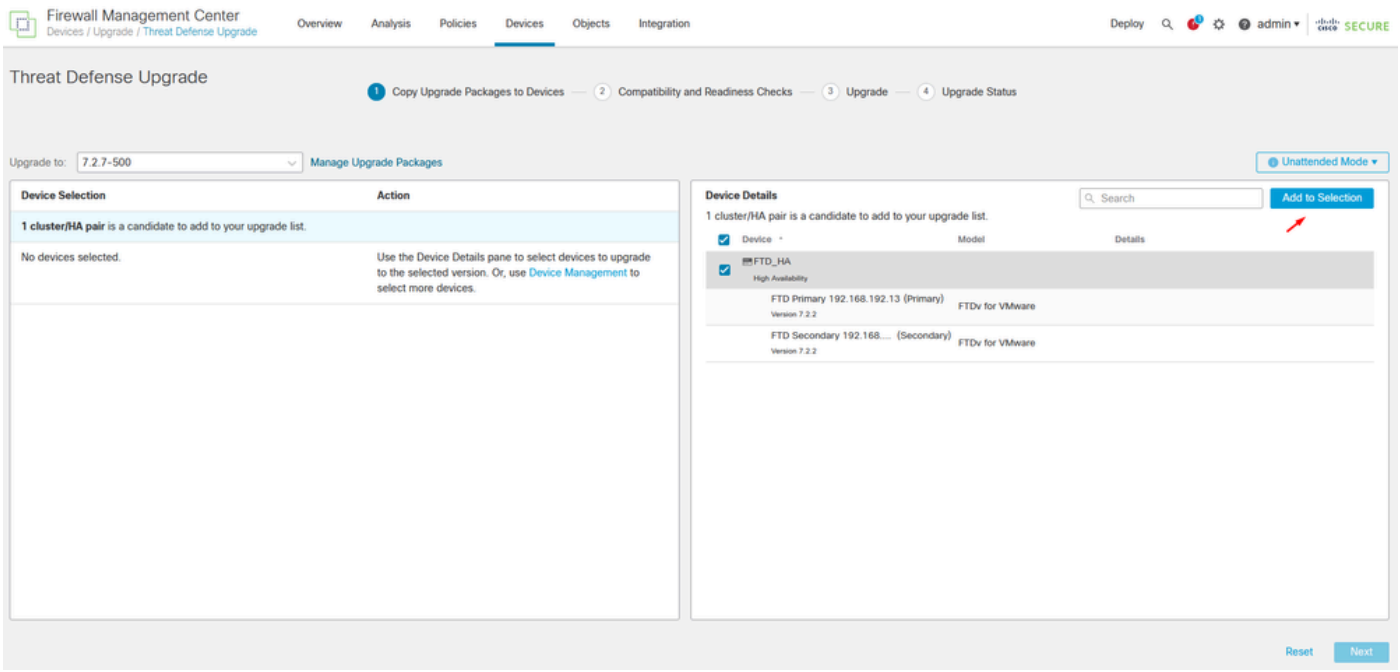
Settings > Updates > Product Updates > Upload local software update packageの順に移動し、FMCを介して両方のデバイスにアップグレードパッケージをアップロードします。software.cisco.comから以前にダウンロードしたパッケージを選択し、Uploadを選択します。

FMCにFirepowerパッケージをアップロードしたら、アップグレードボタンを続行します。



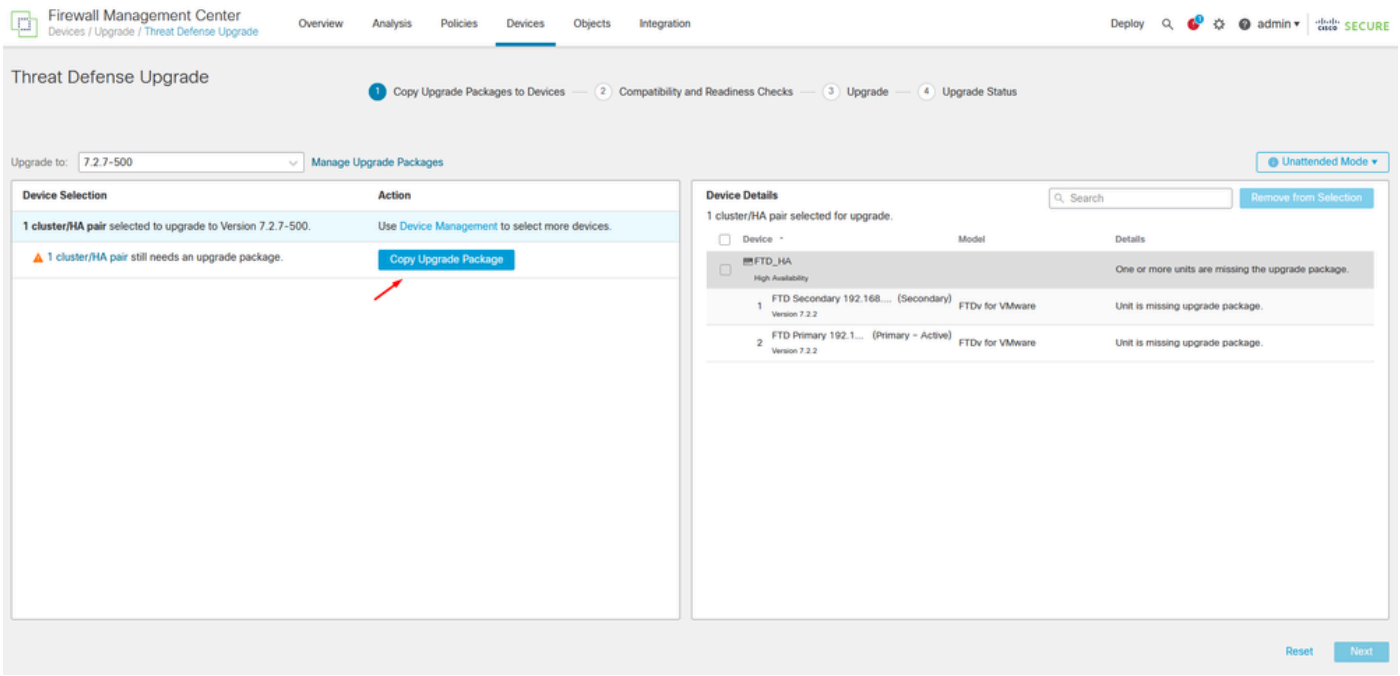
アップグレードボタン

アップグレードウィザードでFTD HAデバイスを選択してから、デバイスを選択し、Add to Selectionをクリックする必要があります。



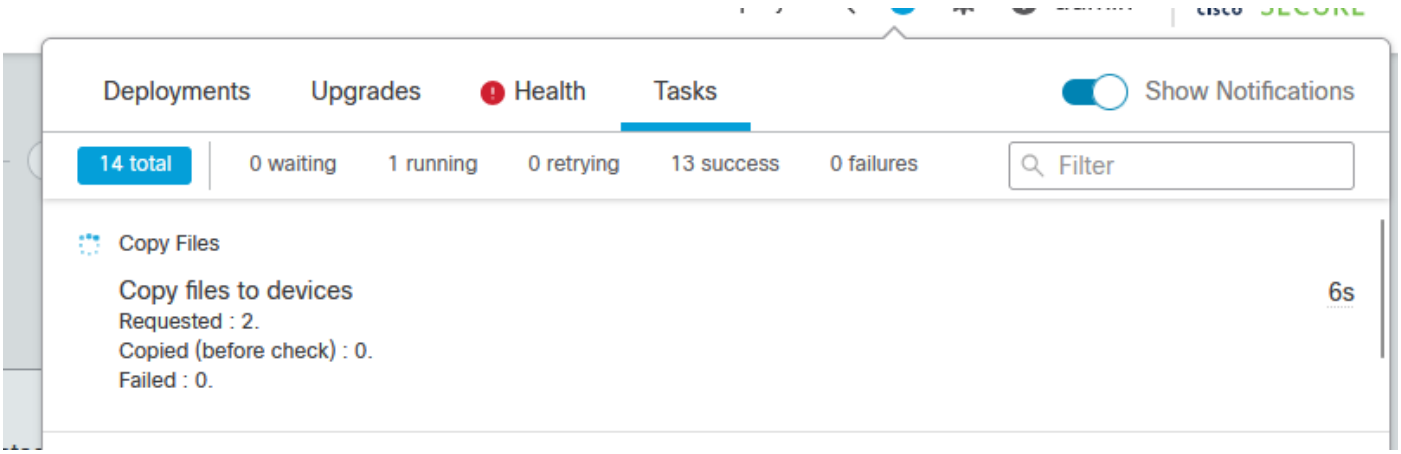
選択範囲に追加

その後、デバイスにアップグレードパッケージをコピーすると、アップグレードパッケージを続行するためのメッセージが表示されます。



アップグレードパッケージのコピーボタン

通知タスクでは、デバイスにファイルをコピーするジョブを見つけることができます。タスクが完了すると、タスクは完了し、成功します。



デバイスへのファイルのコピー

パッケージが次のパスのデバイスにアップロードされていることを確認できます。

```
root@firepower:/ngfw/var/sf/updates#
root@firepower:/ngfw/var/sf/updates# ls -l
total 2181772
-rw-r--r-- 1 root root 1110405120 Jul 18 01:08 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar
-rw-r--r-- 1 root root        815 Jul 18 01:23 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar.METADATA
-rw-r--r-- 1 root root 1123706880 Jul 18 02:36 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
-rw-r--r-- 1 root root        854 Jul 18 02:37 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar.METADATA
root@firepower:/ngfw/var/sf/updates#
```

準備チェック

次のコマンドを使用して、セカンダリデバイスのCLIから準備状況チェックを実行します。

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
```

ランダム データの例は次のとおりです。

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
ARGV[0] = --detach
ARGV[1] = --readiness-check
ARGV[2] = /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
[Readiness-Info]filename : /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar  at /usr/local/sf/lib
This was not run through the SF::System APIs at /usr/local/sf/lib/perl/5.24.4/SF/System/Wrappers.pm lin
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.sh at /usr/local/
root@firepower:/ngfw/var/sf/updates#
```

次のパスで準備状況の確認プロセスを監視します。

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness# cat upgrade_readiness_status
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 0%  MESSAGE:Running script 000_start/000_00_run_cli_kic
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 5%  MESSAGE:Running script 000_start/000_check_platform_
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:10%  MESSAGE:Running script 000_start/100_start_messages
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:14%  MESSAGE:Running script 000_start/101_run_pruning.pl
TIMESTAMP:Thu Jul 18 02:43:41 UTC 2024 PERCENT:19%  MESSAGE:Running script 000_start/105_check_model_nu
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:24%  MESSAGE:Running script 000_start/106_check_HA_state
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:29%  MESSAGE:Running script 000_start/107_version_check.
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:33%  MESSAGE:Running script 000_start/108_clean_user_sta
TIMESTAMP:Thu Jul 18 02:43:43 UTC 2024 PERCENT:38%  MESSAGE:Running script 000_start/110_DB_integrity_c
TIMESTAMP:Thu Jul 18 02:43:47 UTC 2024 PERCENT:43%  MESSAGE:Running script 000_start/113_EO_integrity_c
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:48%  MESSAGE:Running script 000_start/250_check_system_f
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:52%  MESSAGE:Running script 000_start/410_check_disk_spa
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:57%  MESSAGE:Running script 200_pre/001_check_reg.pl...
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:62%  MESSAGE:Running script 200_pre/002_check_mounts.sh.
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:67%  MESSAGE:Running script 200_pre/004_check_deploy_pac
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:71%  MESSAGE:Running script 200_pre/005_check_manager.pl
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:76%  MESSAGE:Running script 200_pre/006_check_snort.sh..
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:81%  MESSAGE:Running script 200_pre/007_check_sru_instal
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:86%  MESSAGE:Running script 200_pre/009_check_snort_prep
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:90%  MESSAGE:Running script 200_pre/011_check_self.sh...
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:95%  MESSAGE:Running script 200_pre/015_verify_rpm.sh...
TIMESTAMP:Thu Jul 18 02:44:00 UTC 2024 PERCENT:100%  MESSAGE:Readiness Check completed successfully.
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness#
```

準備状況のチェックに失敗した場合は、Cisco TACにお問い合わせください。

アップグレードインストール

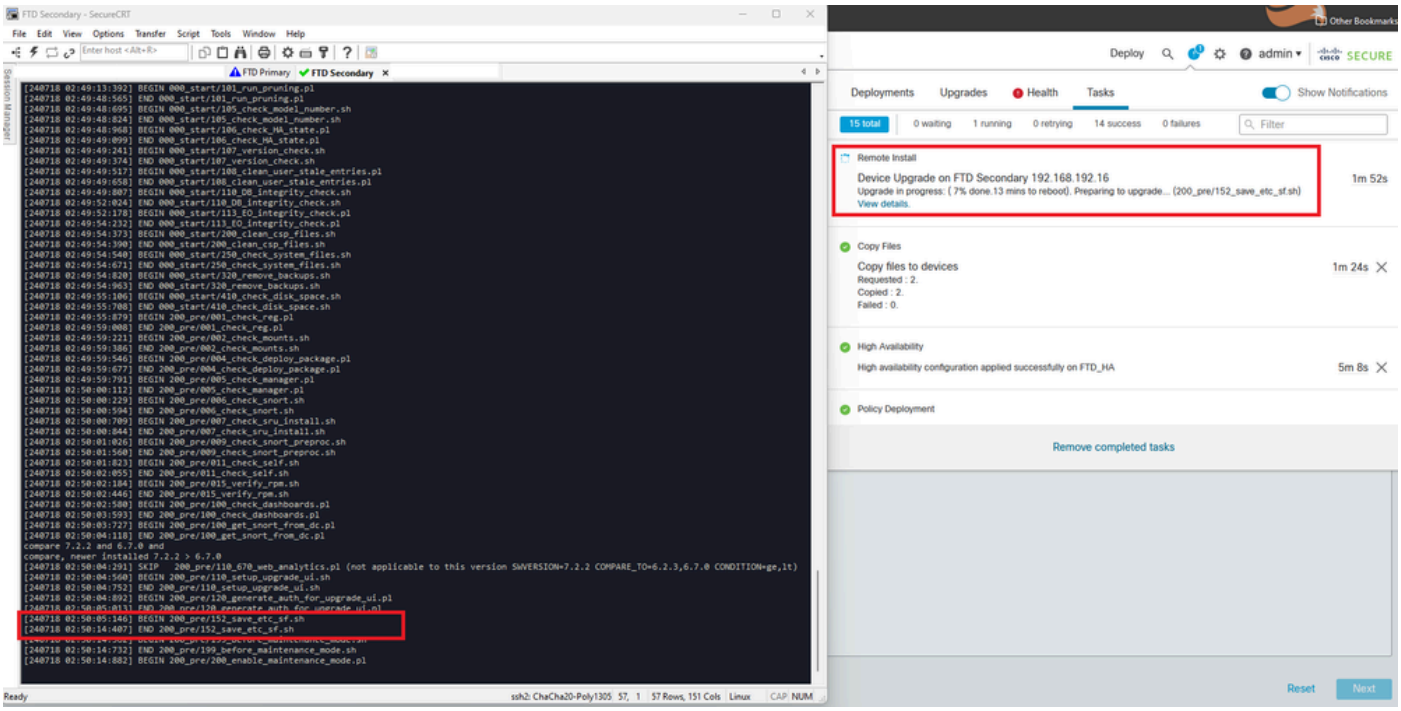
セカンダリFTDでアップグレードインストールを続行します。アップグレードファイルを含むフォルダに移動し、インストールコマンドを実行します。

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach <FTD_Upgrade_Package.sh.REL.tar>
```

アップグレードが実行されると、次の例のような出力が表示されます。

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
ARGV[0] = Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
updated absolute bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr/local/sf/lib/per
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value $in_container in string eq at /usr/local/sf/lib/perl/5.24.4/SF/Update/Status
Verifying archive integrity... All good.
Uncompressing Cisco FTD Upgrade / Sat Apr 27 04:09:29 UTC 2024.....................................
Entering is_fmc_managed
Device is FMC Managed
[240718 02:48:13:868] Found original ftd upgrade file /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.RE
[240718 02:48:16:990] MAIN_UPGRADE_SCRIPT_START
[240718 02:48:17:006] ########################################
[240718 02:48:17:007] # UPGRADE  STARTING
[240718 02:48:17:008] ########################################
compare 7.2.2 and 6.2.3 and
compare, newer installed 7.2.2 > 6.2.3
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/var/sf/sync/updates_status_logs
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/var/sf/sync/updates_s
Link to JSON upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json created i
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/var/sf/sync/updates_st
Link to log upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log created in
[240718 02:48:17:229] BEGIN 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:421] END 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:525] BEGIN 000_start/000_00_run_troubleshoot.sh
```

FMCで、セカンダリデバイスのアップグレードを実行するタスクがあります。



FMCで実行中のタスク

次のパスを使用して、アップグレードステータスを監視します。

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-X.X.X# tail -f upgrade_status.log
```

出力例を次に示します。

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7# tail -f upgrade_status.log
TIMESTAMP:Thu Jul 18 02:50:25 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/202_disable_syncd.sh
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/400_restrict_rpc.sh.
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/500_stop_system.sh..
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/501_recovery.sh... T
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/505_revert_prep.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/999_enable_sync.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/001_verify_bundle.sh.
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/002_set_auto_neg.pl..
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/060_fix_fstab.sh... T
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/100_install_Fire_Linux
```

セカンダリデバイスのアップグレードが完了すると、次のメッセージが表示されます。

```
240718 13:40:58:872] Attempting to remove upgrade lock
[240718 13:40:58:873] Success, removed upgrade lock
Upgrade lock /ngfw/tmp/upgrade.lock removed successfully.
[240718 13:40:58:882]
[240718 13:40:58:883] ############################################################
[240718 13:40:58:885] # UPGRADE  COMPLETE  #
```

```
[240718 13:40:58:887] ###########################################################
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/Volume/root/ngfw/var/sf/sync/updates_st
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/Volu
Link to JSON upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_statu
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volume
Link to log upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_statu
Process 10677 exited.I am going away.
RC: 0
Update package reports success: almost finished...
Scheduling a reboot to occur in 5 seconds...
Process 12153 exited.I am going away.
root@firepower:/ngfw/var/sf/updates#
Broadcast message from root@firepower (Thu Jul 18 13:41:05 2024):

The system is going down for reboot NOW!
```

スタンバイデバイスからのアップグレードが完了した後、デバイスはリブートされます。デバイスが起動したら、フェールオーバーステータスをチェックして、すべてが最初に設定された状態のままであることを確認します。

アクティブFTDでは、次の項目を確認できます。

```
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             13:24:46 UTC Jul 18 2024

====Configuration State===
        Sync Done
====Communication State===
        Mac set

firepower#
```

スタンバイFTDでは、次のように表示されます。

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Skipped - STANDBY
====Communication State===
```

```
        Mac set

firepower#
```

バージョンが異なることを示すメッセージが表示されます。

```
firepower#
************WARNING****WARNING****WARNING*******************************
   Mate version 9.18(4)201 is not identical with ours 9.18(2)200
************WARNING****WARNING****WARNING*******************************
```

CLIを使用して、スタンバイデバイスでコマンドfailover activeを使用し、フェールオーバーを手動で実行します。ここで、スタンバイデバイスがアクティブになります。

警告：この時点で、フェールオーバーの発生時に一時的なトラフィックの中断が発生し

ています。

```
firepower#
firepower# failover active

        Switching to Active
firepower#
firepower#
firepower# sh fail
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Active         None
Other host -   Primary
               Standby Ready  None

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

firepower#
```

フェールオーバーが完了したら、他のデバイスのアップグレードに進むことができます。以前はアクティブで、現在はスタンバイになっているデバイスに対して、このドキュメントの冒頭で説明した同じ手順を使用します。

これで、両方のデバイスがアップグレードされました。回線側でコマンドshow versionを使用すると確認できます。プライマリデバイス：

```
firepower#
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Standby Ready  None
Other host -   Secondary
               Active         None

====Configuration State===
        Sync Skipped - STANDBY
====Communication State===
        Mac set

firepower#
```

セカンダリデバイスについて：

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Active         None
Other host -   Primary
               Standby Ready  Comm Failure             14:03:06 UTC Jul 18 2024

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

firepower#
```

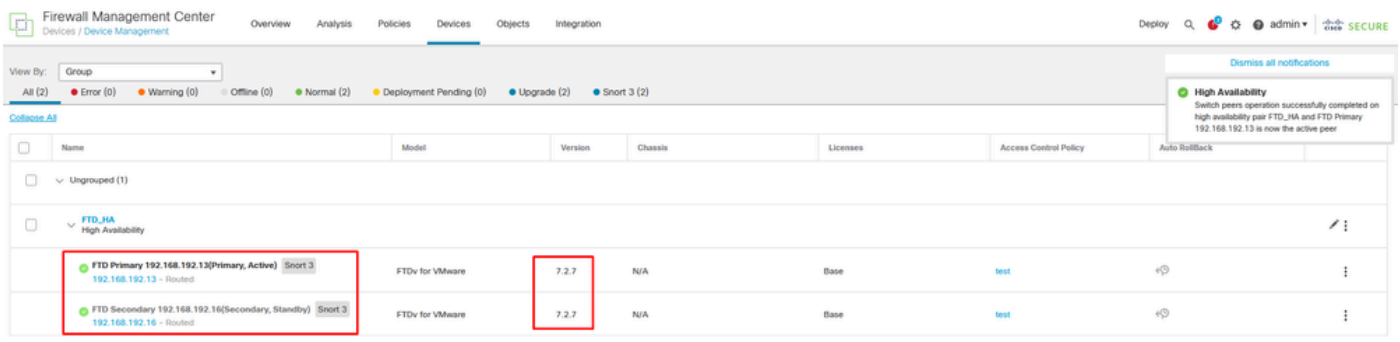
この時点で、FMCからデバイスを最初と同じように切り替えることができます。

確認

両方のデバイスのアップグレードが成功したら、show versionコマンドを使用してFMCと両方のFTDのステータスを確認します。

```
firepower# show version
-------------------[ firepower ]---------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.2.7 (Build 500)
UUID                      : 0edf9f22-78e6-11ea-8ed0-e0e5abf334e2
LSP version               : lsp-rel-20240306-2015
VDB version               : 353
-----------------------------------------------------
```

FMCでバージョンの更新が確認でき、最初の設定と同様にスイッチオーバーできます。



FMCからのスイッチドピア

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。