FDMで管理される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、Firepower Device Manager(FDM)で管理されるハイアベイラビリティのCisco Secure Firewall Threat Defense(FTD)のアップグレードプロセス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を推奨しています。

- ハイアベイラビリティ(HA)の概念と設定
- Cisco Secure Firepower Device Manager(FDM)の設定
- Cisco Secure Firewall Threat Defense(FTD)の設定

使用するコンポーネント

このドキュメントの情報は、仮想Cisco FTDバージョン7.2.8に基づいています。

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。

概要

FDMが動作する方法は、ピアを1つずつアップグレードすることです。アクティブアップグレードを開始する前に、まずスタンバイ、次にアクティブの順にフェールオーバーを実行します。

背景説明

アップグレードパッケージは、アップグレードの前にsoftware.cisco.comからダウンロードする必要があります。

CLIクリックで、アクティブFTDのshow high-availability設定コマンドを実行して、HAのステータスを確認します。

```
> show high-availability config

Failover On

Failover unit Primary

Failover LAN Interface: failover-link GigabitEthernet0/2 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(3)53, Mate 9.18(3)53

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 11:57:26 UTC Oct 8 2024

        This host: Primary - Active

                Active time: 507441 (sec)

                slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)

                  Interface diagnostic (0.0.0.0): Normal (Waiting)

                  Interface inside (192.168.45.1): Normal (Waiting)

                  Interface outside (192.168.1.10): Normal (Waiting)

                slot 1: snort rev (1.0)  status (up)

                slot 2: diskstatus rev (1.0)  status (up)

        Other host: Secondary - Standby Ready
```

```
Active time: 8 (sec)

  Interface diagnostic (0.0.0.0): Normal (Waiting)

  Interface inside (0.0.0.0): Normal (Waiting)

  Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0)  status (up)

slot 2: diskstatus rev (1.0)  status (up)
```

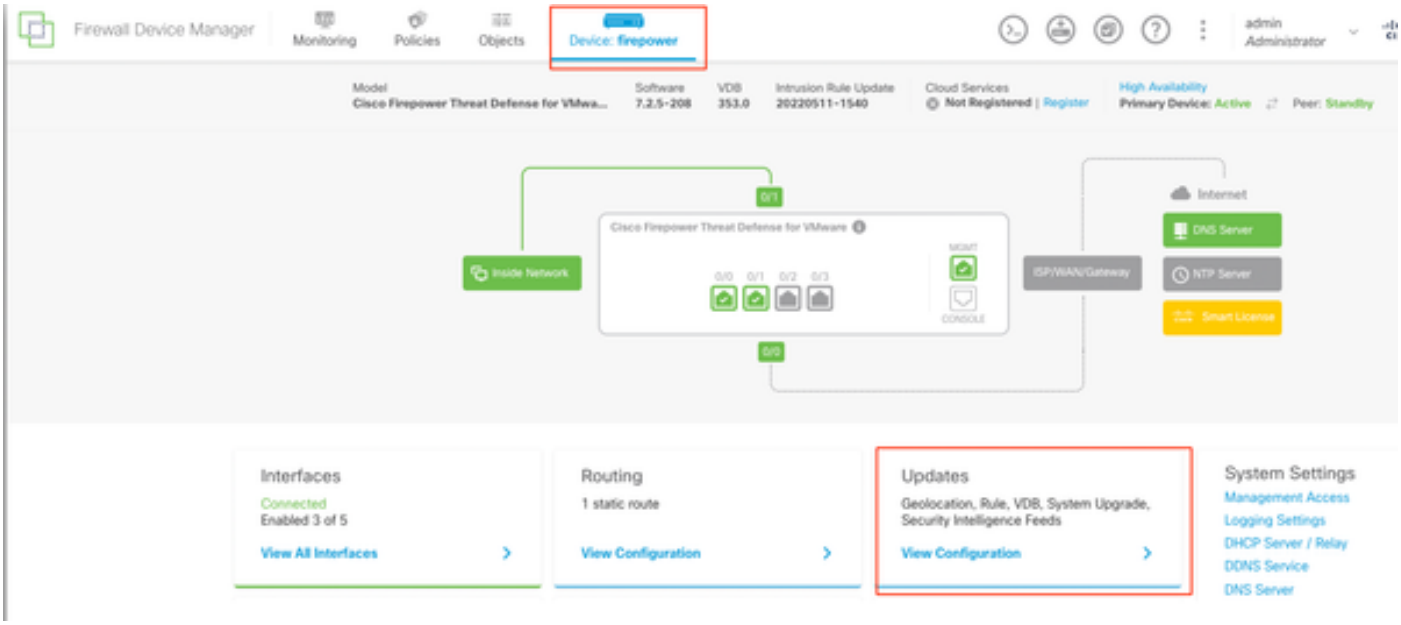
エラーが表示されない場合は、アップグレードに進みます。

設定

ステップ 1：アップグレードパッケージのアップロード

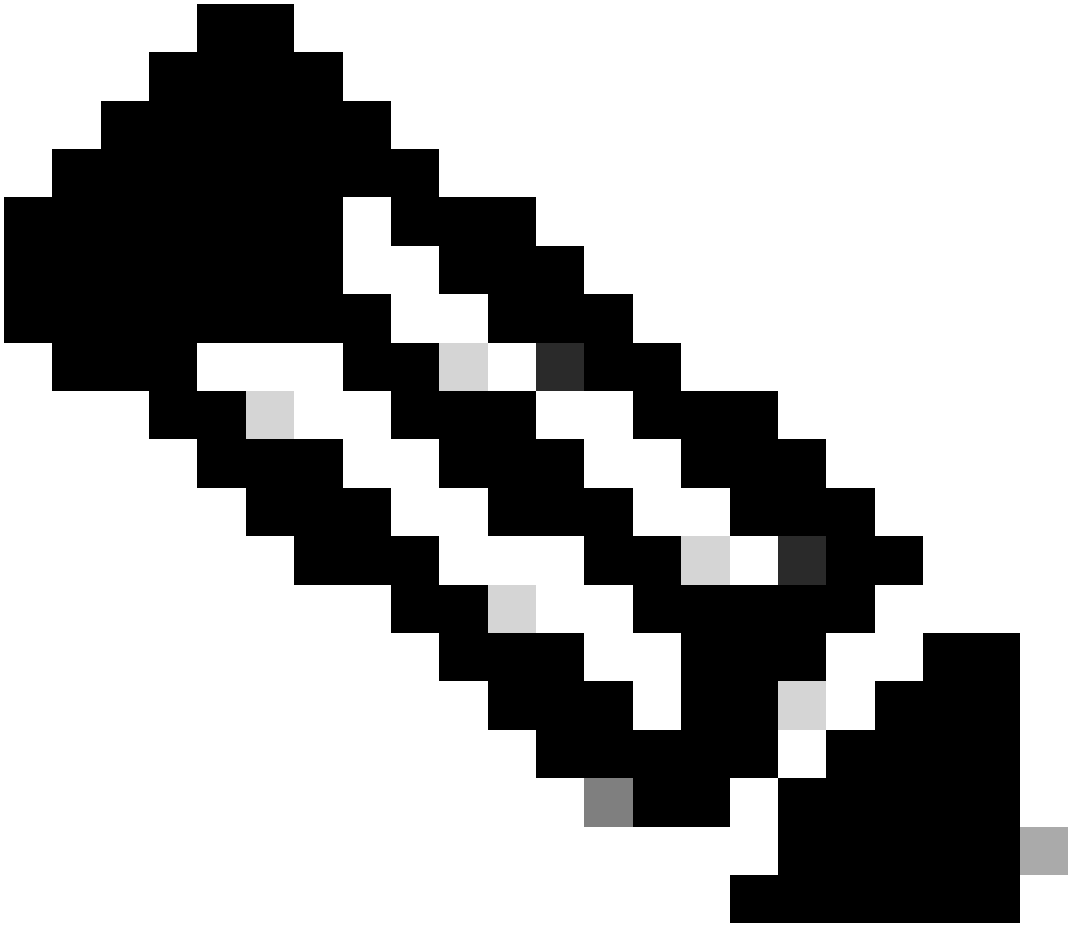
- GUIを使用してFDMにFTDアップグレードパッケージをアップロードします。

このファイルは、FTDモデルと必要なバージョンに基づいて、シスコのソフトウェアサイトから事前にダウンロードしておく必要があります。Device > Updates > System Upgradeの順に移動します。

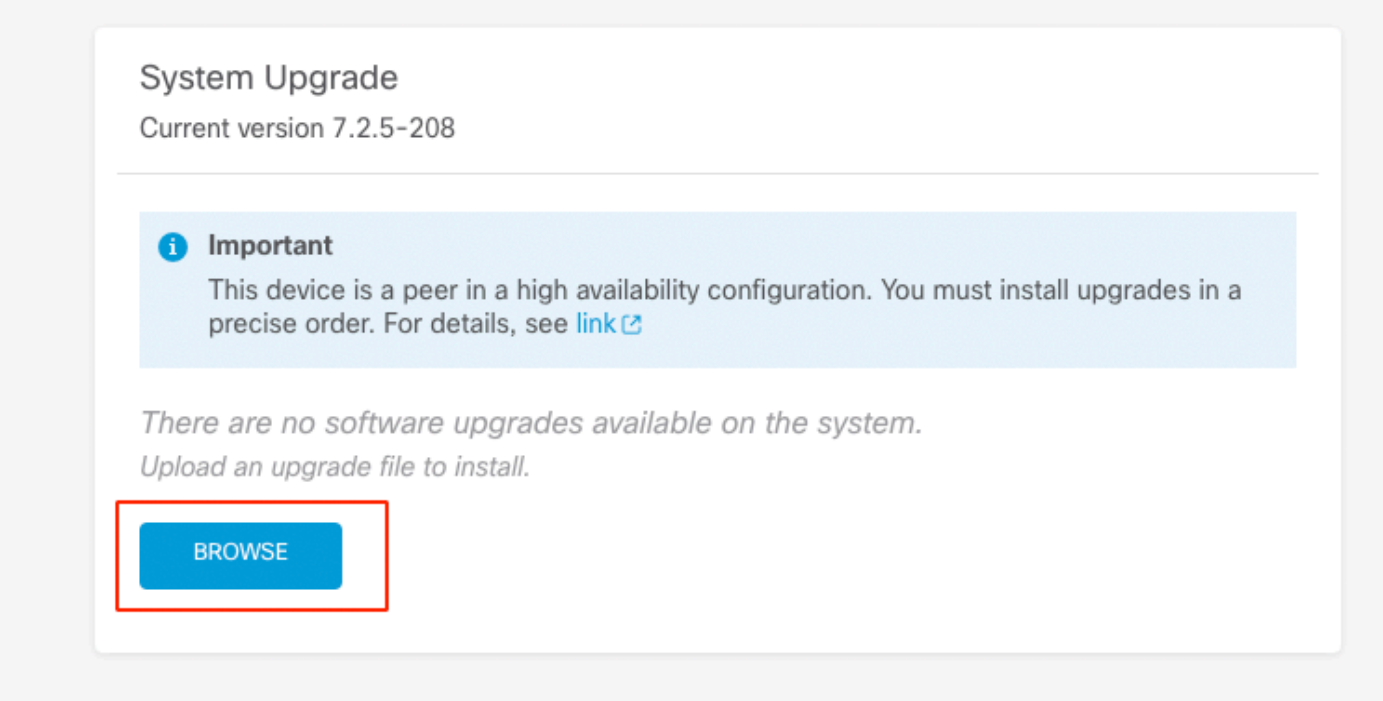


アップデート

- 以前にダウンロードしたイメージを参照し、Uploadを選択します。



注：アクティブとスタンバイの両方のノードにイメージをアップロードします。

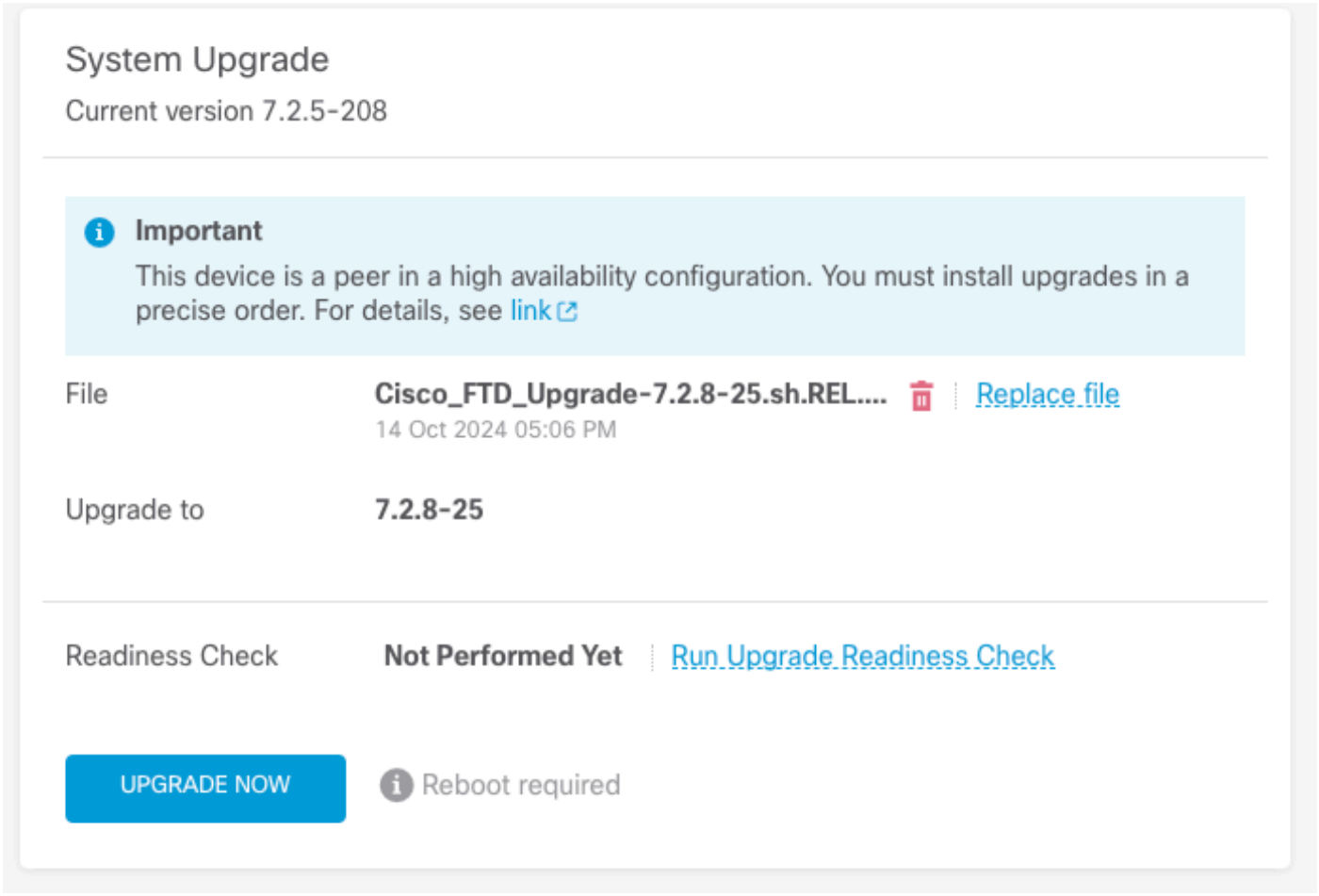


準備状況の確認の実行

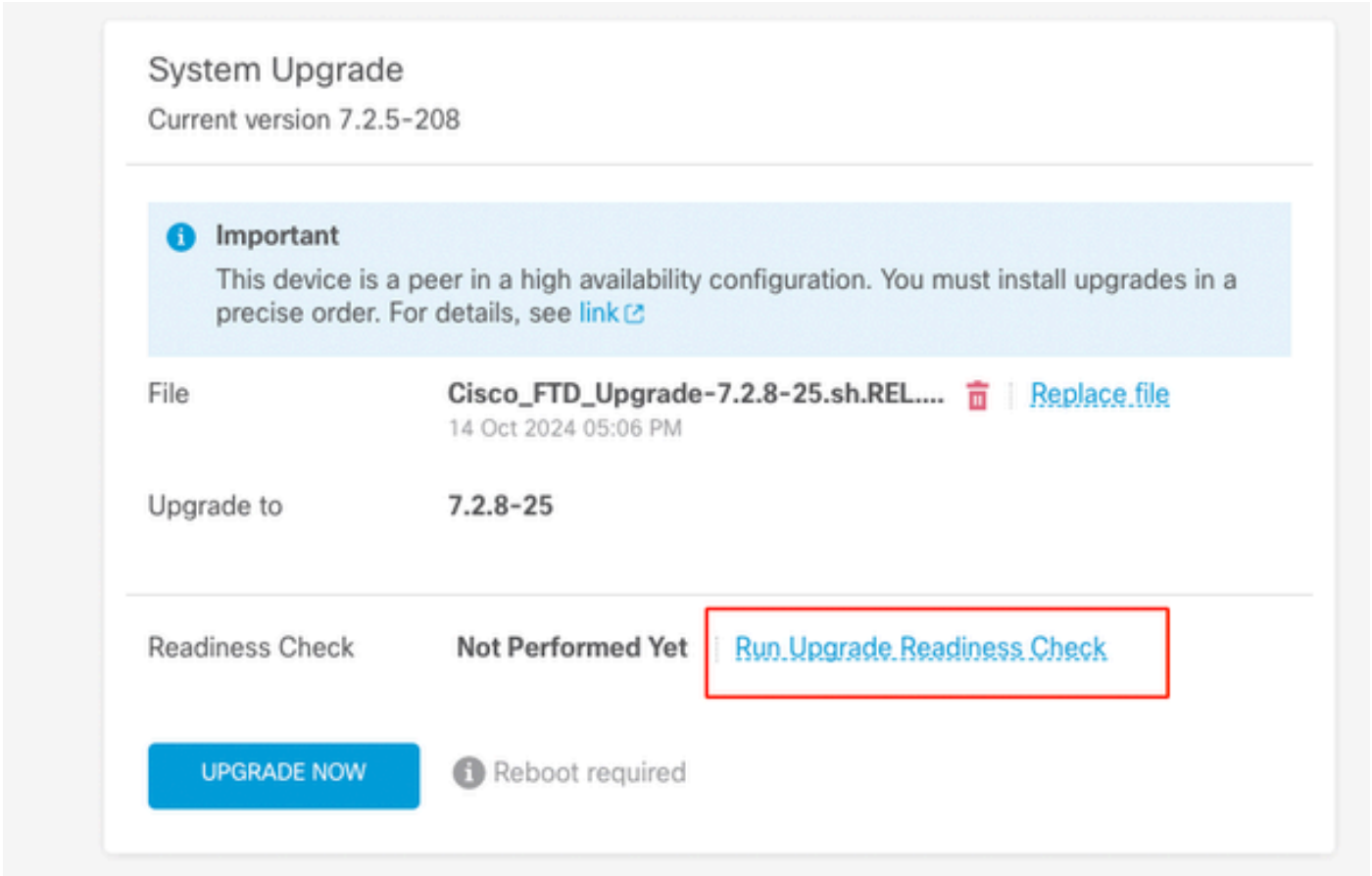
ステップ 2：準備状況の確認

準備状況のチェックにより、アプライアンスがアップグレードを続行する準備ができているかどうかが確認されます。

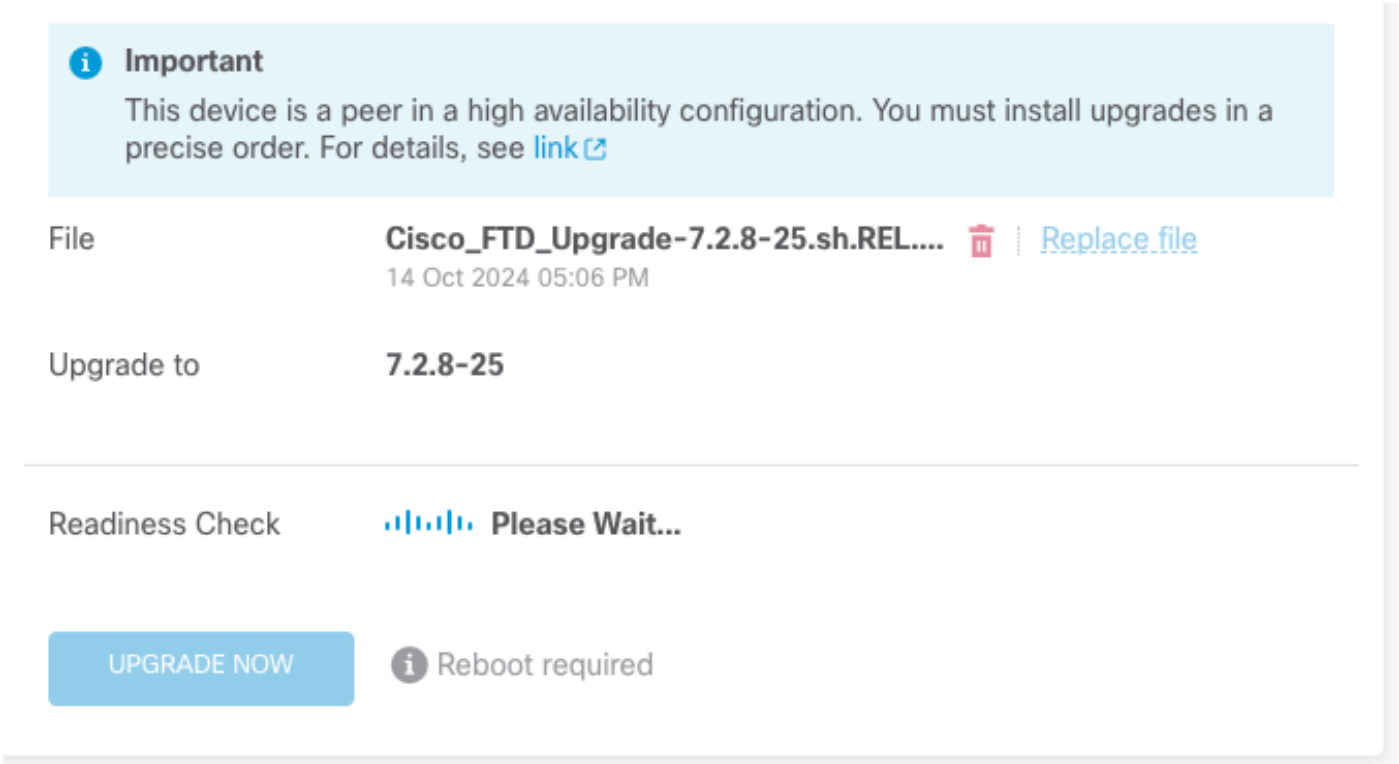
- Run Upgrade Readiness Checkの順に選択します。


System Upgrade
Current version 7.2.5-208
Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link
File
Cisco_FTD_Upgrade-7.2.8-25.sh.REL....
Replace file
14 Oct 2024 05:06 PM
Upgrade to
7.2.8-25
Readiness Check
Not Performed Yet
Run Upgrade Readiness Check
UPGRADE NOW
Reboot required

準備状況の確認の実行

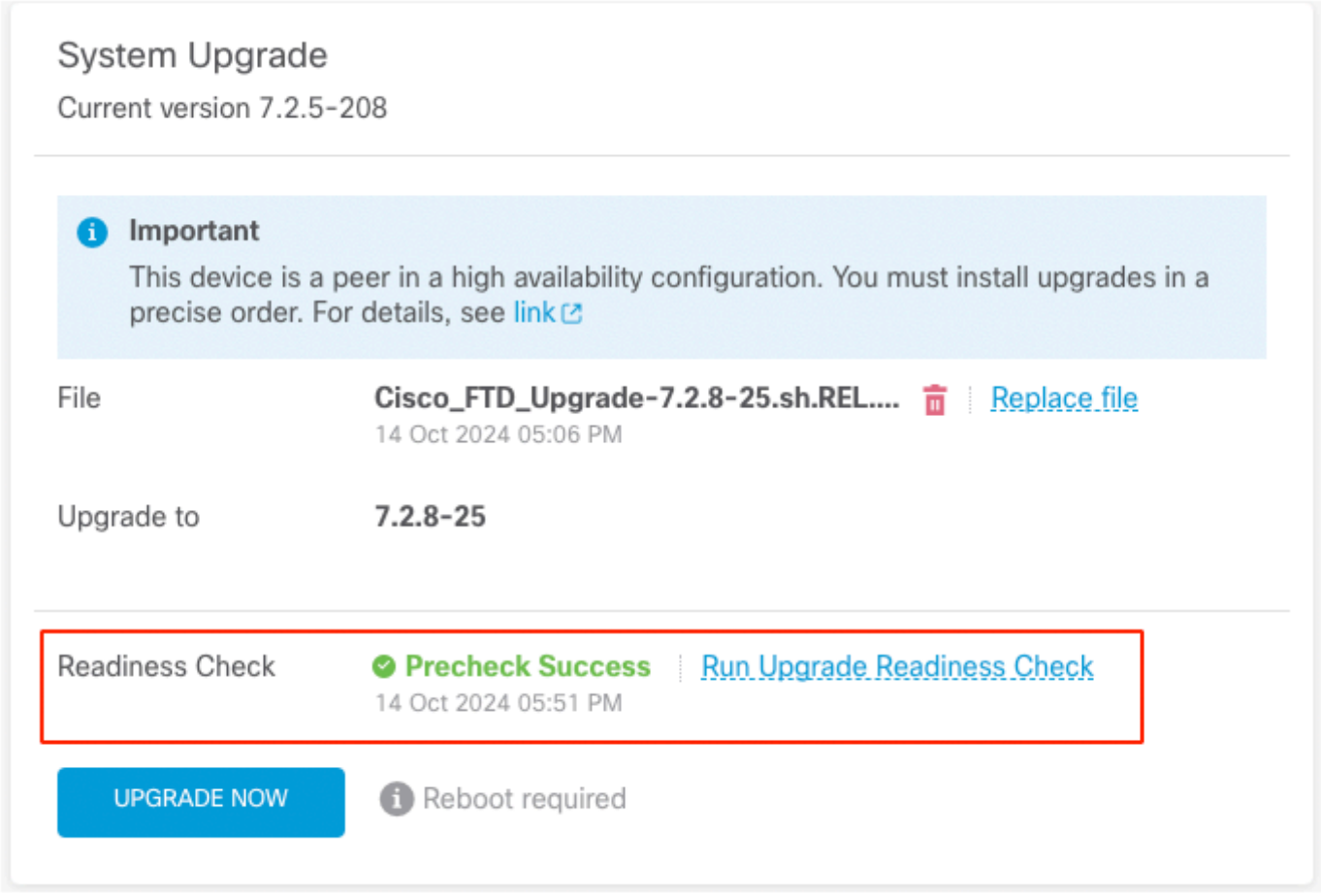

System Upgrade
Current version 7.2.5-208
Important
This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link
File
Cisco_FTD_Upgrade-7.2.8-25.sh.REL....
Replace file
14 Oct 2024 05:06 PM
Upgrade to
7.2.8-25
Readiness Check
Not Performed Yet
Run Upgrade Readiness Check
UPGRADE NOW
Reboot required

準備状況の確認の実行



準備状況の確認の実行

System > Upgradeの順に移動して、進行状況を確認できます。

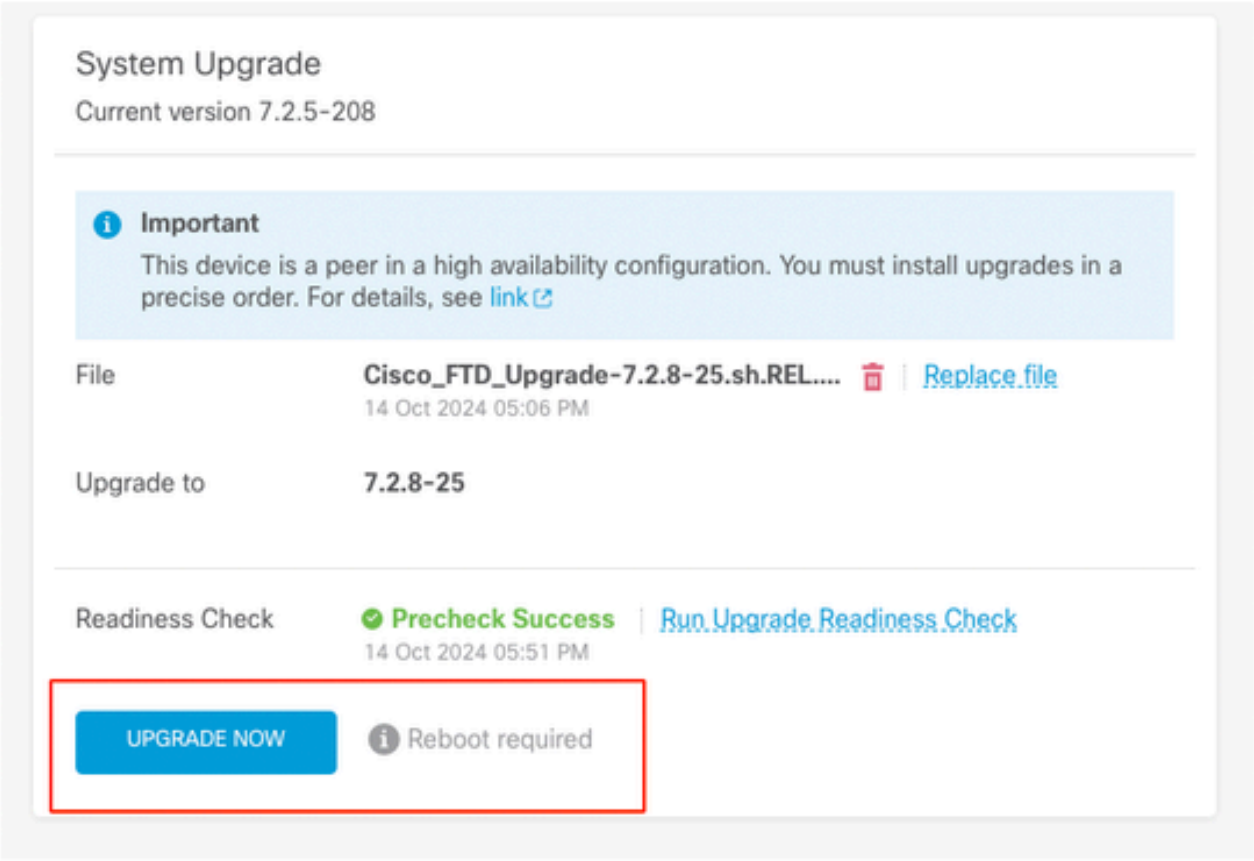


準備状況の確認の実行

アップグレードは、両方のFTDで準備状況のチェックが完了し、結果がSuccessのときに実行できます。

ステップ 3：HAでのFTDのアップグレード

- Standby FDM を選択し、Upgrade Nowをクリックします。

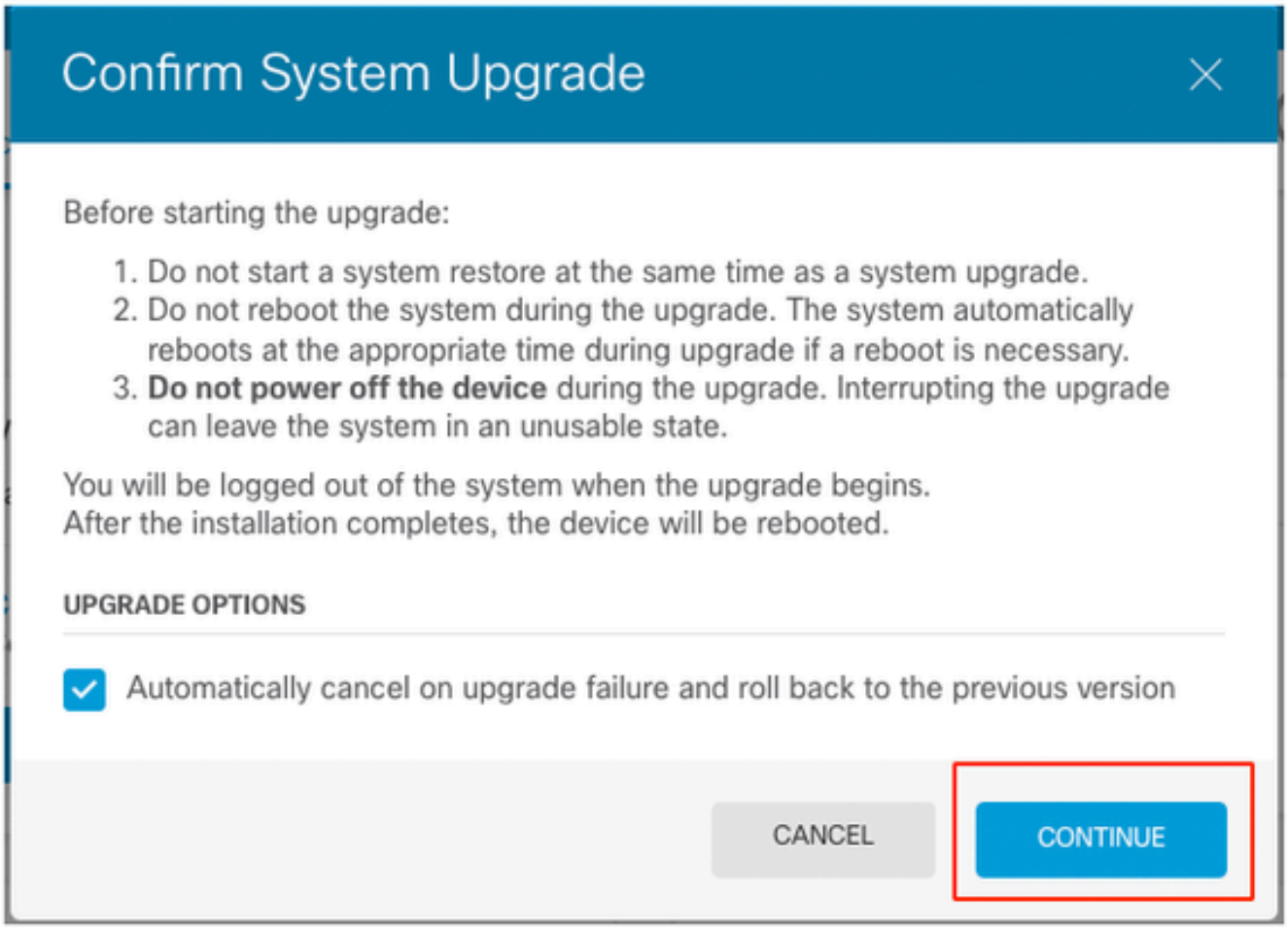


今すぐアップグレード

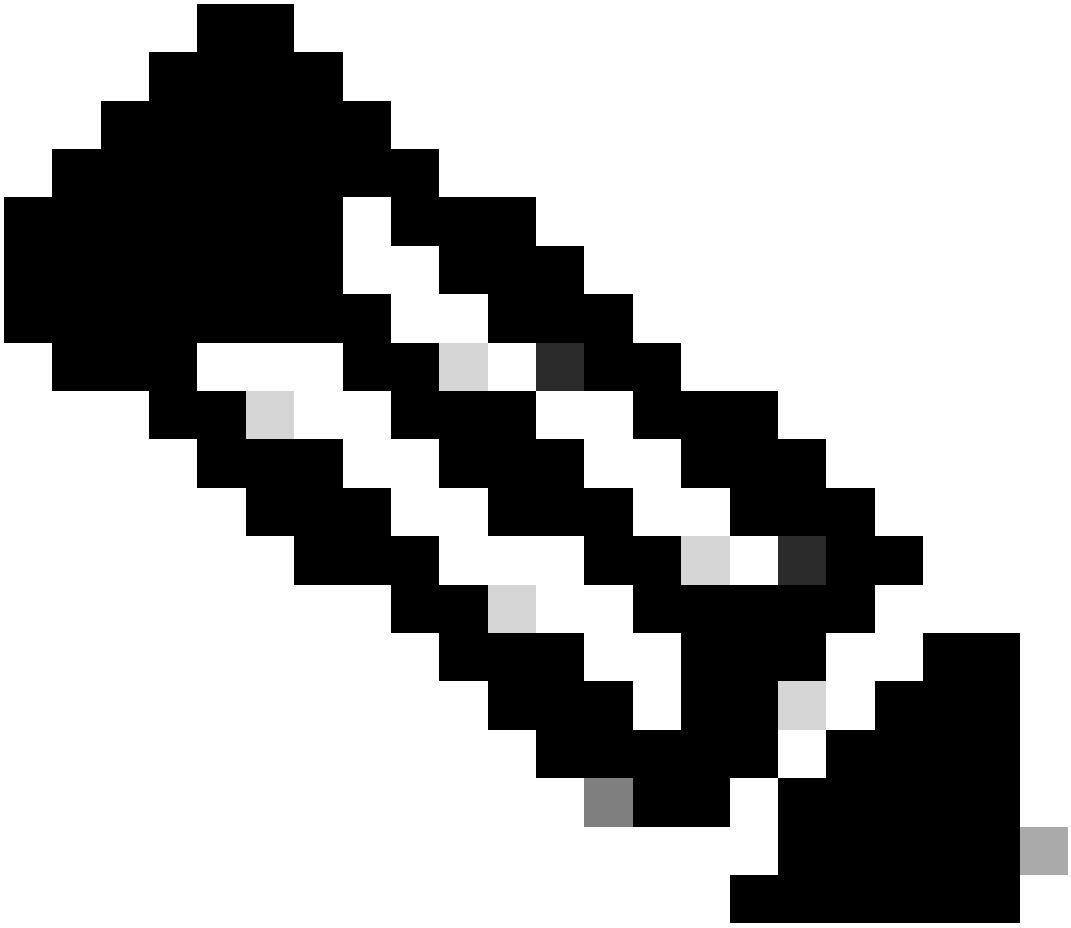
アップグレードを開始する前：

1. システムのアップグレードと同時にシステムの復元を開始しないでください。
2. アップグレード中にシステムをリブートしないでください。リブートが必要な場合、システムはアップグレード中の適切なタイミングで自動的にリブートします。
3. アップグレード中にデバイスの電源をオフにしないでください。アップグレードを中断すると、システムが使用できなくなる可能性があります。

アップグレードの開始時にシステムからログアウトされます。
インストールが完了すると、デバイスがリブートされます。


Confirm System Upgrade
Before starting the upgrade:
1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. Do not power off the device during the upgrade. Interrupting the upgrade can leave the system in an unusable state.
You will be logged out of the system when the upgrade begins.
After the installation completes, the device will be rebooted.
UPGRADE OPTIONS
Automatically cancel on upgrade failure and roll back to the previous version
CANCEL
CONTINUE

[Continue]



注：アップグレードにはFTDあたり約20分かかります。

CLIでは、アップグレードフォルダ/ngfw/var/log/sfで進行状況を確認できます。expert モードに移行し、enterroot accessを入力します。

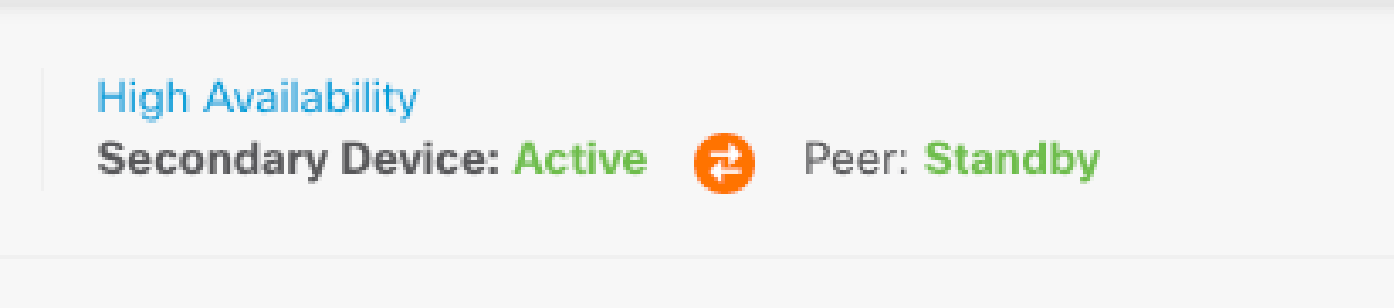
```
> expert

admin@firepower:~$ sudo su

Password:

root@firepower:/home/admin# cd /ngfw/var/log/sf



root@firepower:/ngfw/var/log/sf# ls

Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf

ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
ui: Upgrade complete
ui: The system will now reboot.
ui: System will now reboot.

Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
System will reboot now due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
The system is going down for reboot NOW!
```

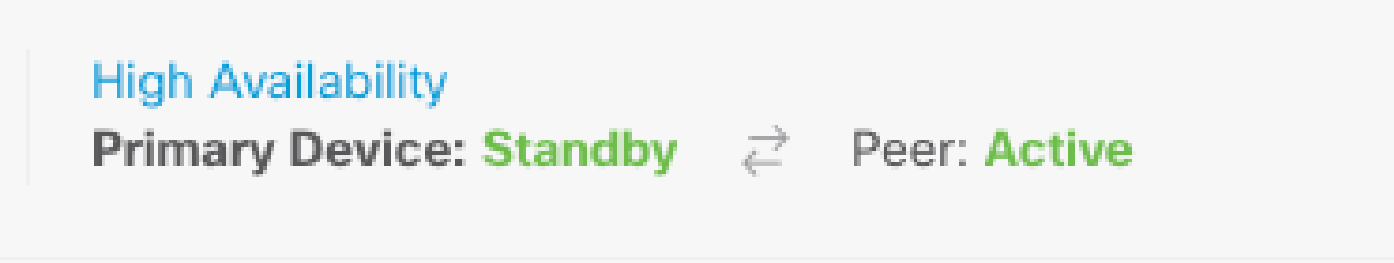
2台目のユニットをアップグレードします。

このデバイスをアクティブにするには、ロールを切り替えます。Device> High Availabilityの順に選択し、歯車メニューからSwitch Modeを選択します。ユニットのステータスがアクティブに変わるのを待ち、トラフィックが正常に流れていることを確認します。その後、ログアウトします。

アップグレード：前の手順を繰り返して、新しいスタンバイにログインし、パッケージをアップロードし、デバイスをアップグレードし、進行状況を監視し、成功を確認します。



ハイ アベイラビリティ



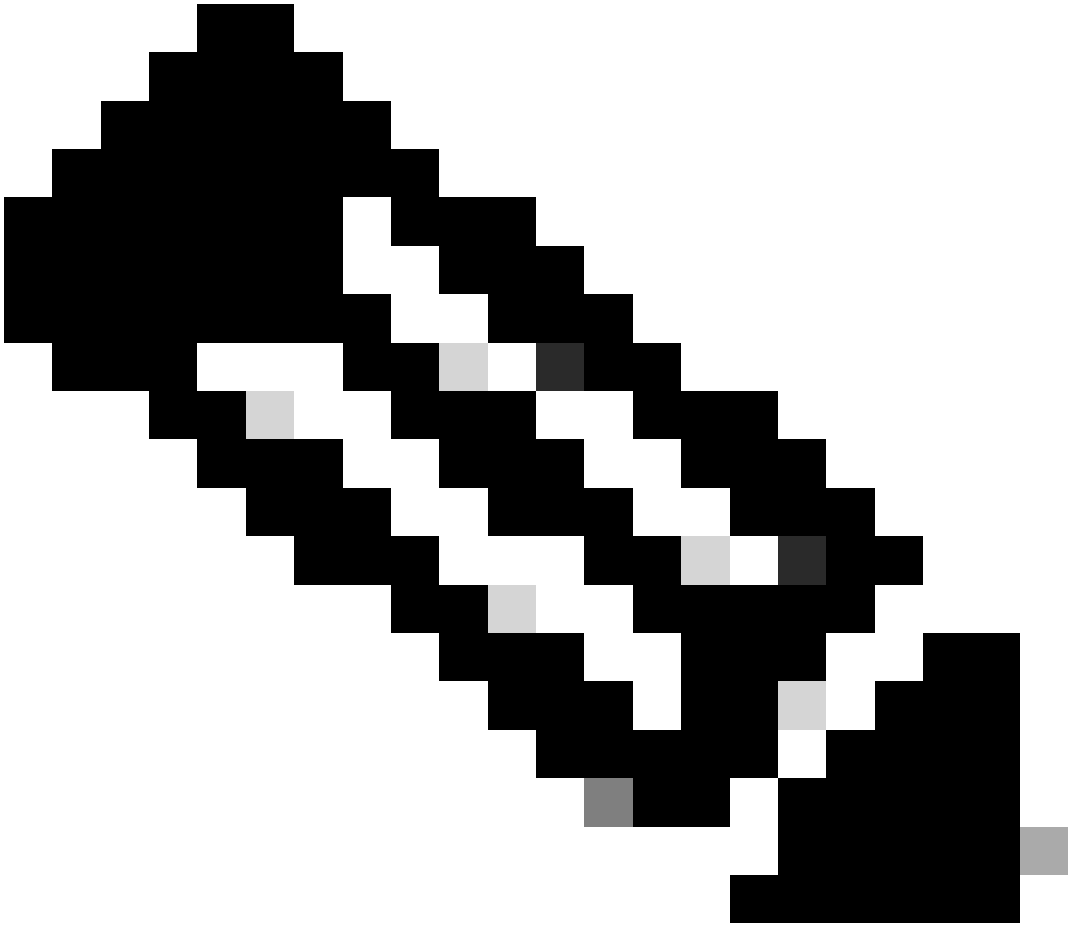
ハイ アベイラビリティ

CLIで、LINA(system support diagnostic-cli)に移動し、commandshow failover stateコマンドを使用してスタンバイFTDのフェールオーバー状態を確認します。

```
> system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.



primary_ha> enable

Password:

primary_ha# 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


primary_ha#
```

ステップ 4：スイッチアクティブピア（オプション）

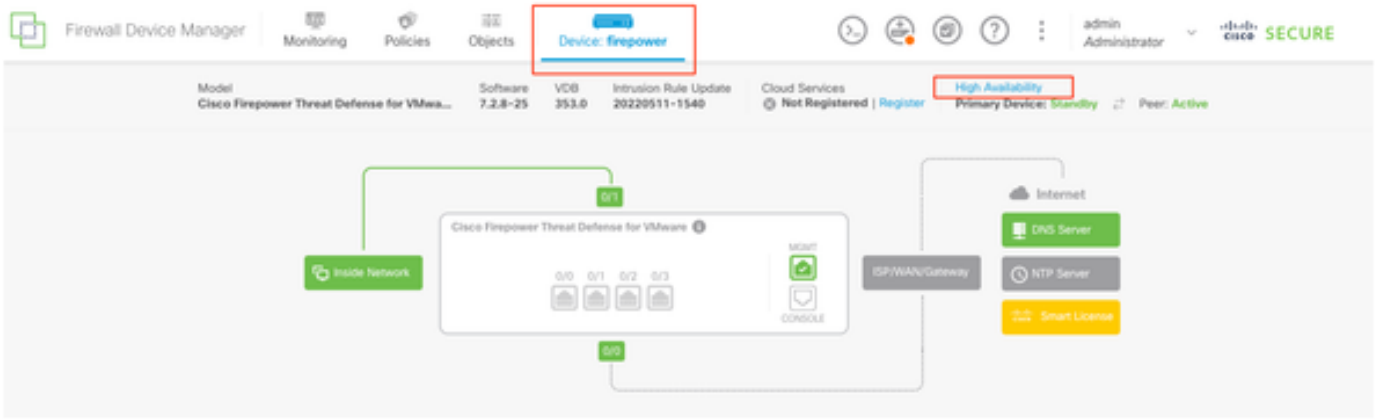


注：セカンダリデバイスがアクティブの場合、操作に影響はありません。

プライマリデバイスをアクティブに、セカンダリデバイスをスタンバイにすることは、発生する可能性のあるフェールオーバーの追跡に役立つベストプラクティスです。

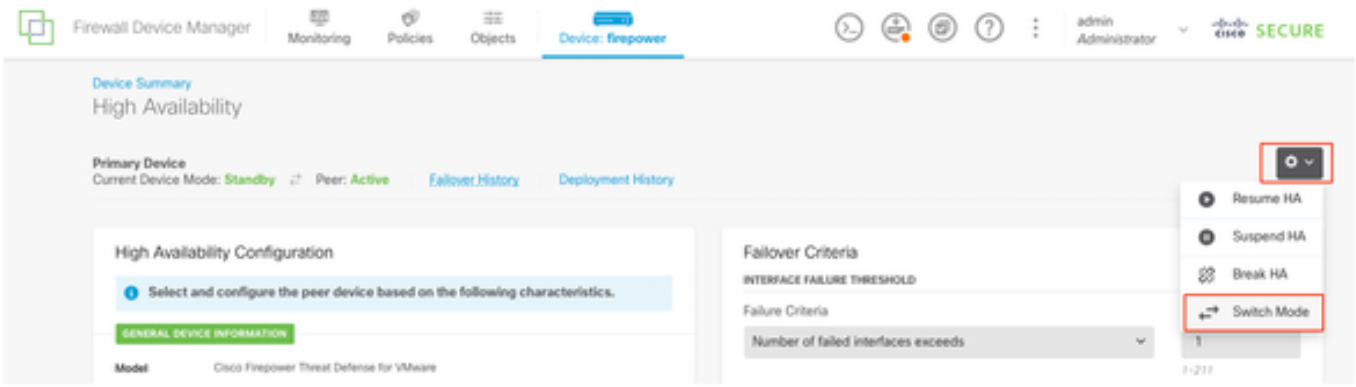
この場合、FTDのアクティブはスタンバイになり、手動フェールオーバーを使用してアクティブに戻すことができます。

- Devices > High Availabilityの順に選択します。



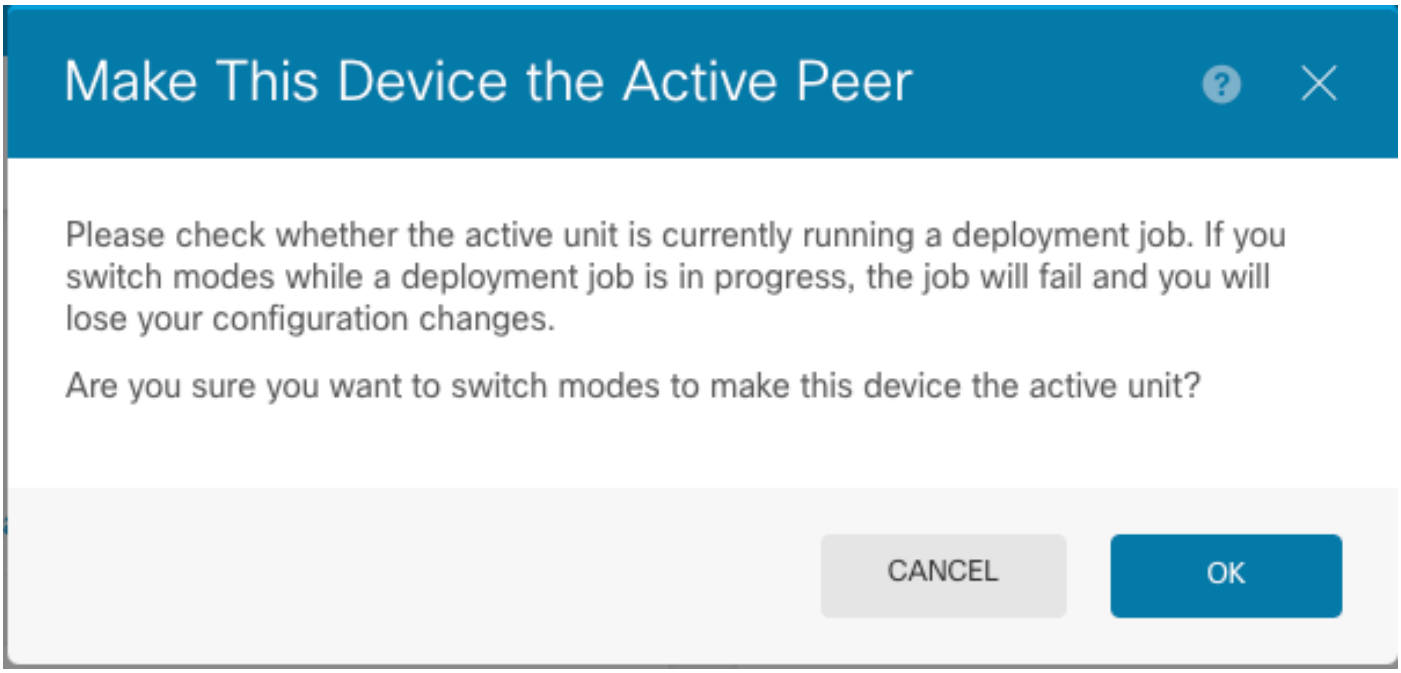
ハイ アベイラビリティ

- Switch Modeを選択します。



スイッチ モード

- OKを選択して、フェールオーバーを確認します。



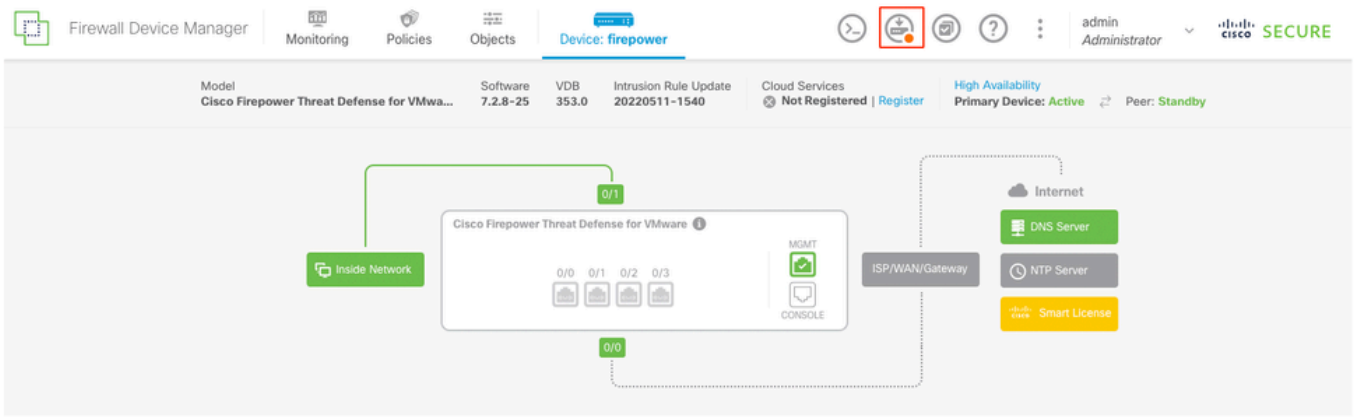
アクティブピア

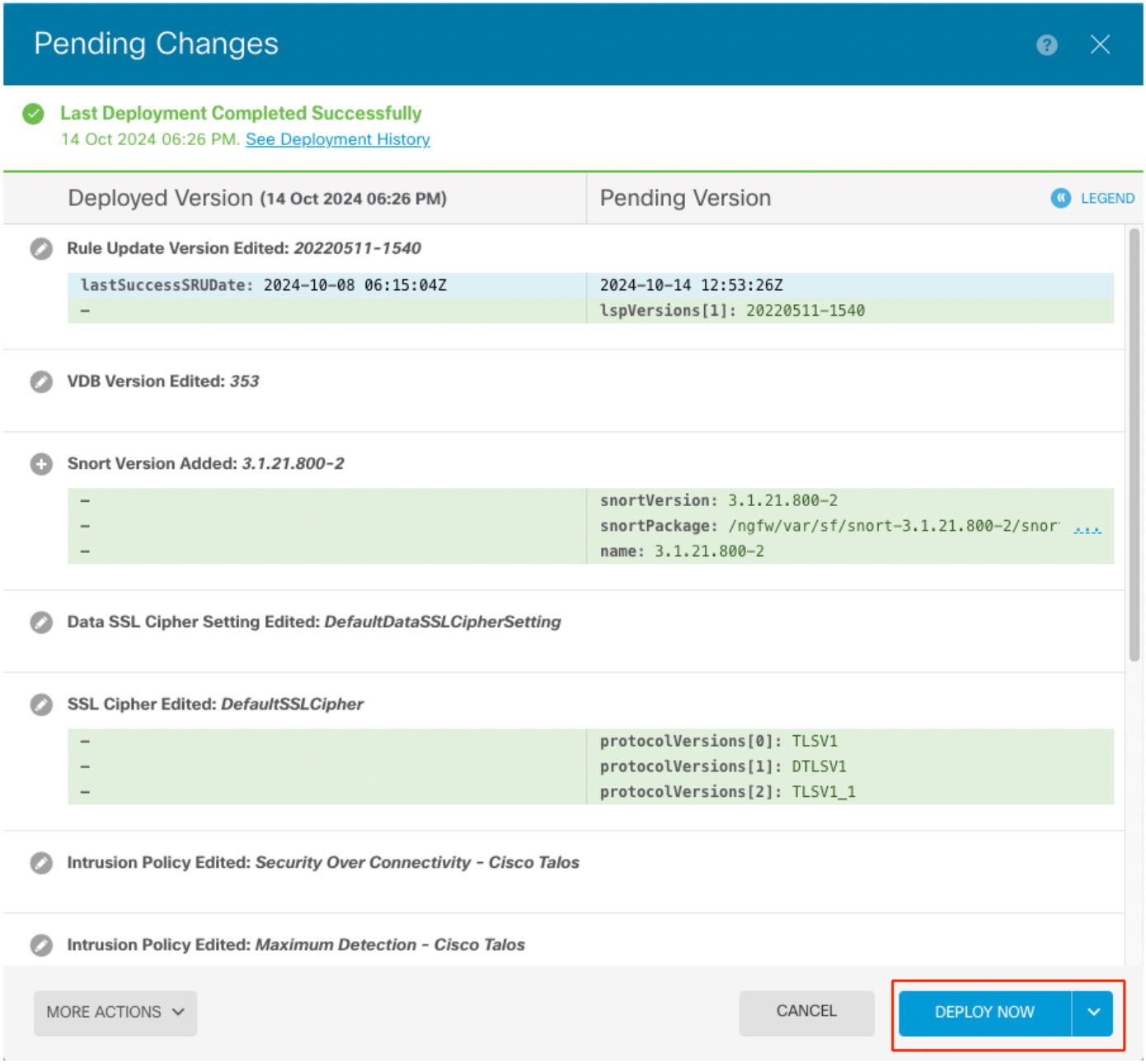
アップグレードおよびフェールオーバー終了時のHAステータスの検証

デバイス

ステップ 5：最終展開

- Deploymentタブの下にあるDEPLOY NOWをクリックして、ポリシーをデバイスに展開します。





ポリシーの導入

検証

HAステータスとアップグレードが完了したことを検証するには、ステータスを確認する必要があります。
プライマリ：アクティブ
セカンダリ：スタンバイ準備完了

両方とも、最近変更されたバージョン（この例では7.2.8）の下にあります。

フェールオーバー

- CLIクリックで、commandsshow failover stateandshow failoversコマンドを使用してフェールオーバー状態をチェックすると、詳細が表示されます。

Cisco Firepower Extensible Operating System(FX-OS)v2.12.1（ビルド73）
Cisco Firepower Threat Defense for VMware v7.2.8（ビルド25）

```
> show failover state

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

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

> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
Last Failover at: 14:13:56 UTC Oct 15 2024
        This host: Primary - Active
                Active time: 580 (sec)
                slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (192.168.45.1): Normal (Waiting)
                  Interface outside (192.168.1.10): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 91512 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)


Stateful Failover Logical Update Statistics
        Link : failover-link GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         11797      0          76877      0
```

sys cmd	11574	0	11484	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx	0	0	0	0
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device-ID	0	0	0	0
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

```
Logical Update Queue Information

                Cur     Max     Total

Recv Q:         0       31      123591

Xmit Q:         0       1       12100
```

両方のFTDが同じバージョンにあり、HAステータスが正常であれば、アップグレードは完了です。

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。