透過FMC管理的CLI升級FTD HA

目錄

簡介

本檔案介紹透過指令行介面(CLI)升級Cisco Firepower威脅防禦(FTD)裝置的詳細程式。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全防火牆管理中心7.2.8版

- VMWare v7.2.2的Cisco Firepower威脅防禦

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔的特定要求包括：

- 運行版本7.2或更高版本的思科安全防火牆威脅防禦
- 運行版本7.2或更高版本的Cisco Secure Firewall Management Center

設定

透過CLI升級一對FTD裝置時，裝置上必須存在升級套件檔案。透過CLI成功升級的前提條件是沒有待處理的部署。

準備升級

警告：檢查升級順序，選擇備用/活動，以避免任何流量中斷。

1. 從配置為「備用」的裝置開始。

2. 在clish模式下輸入expert(後跟sudo su)以在expert模式下訪問CLI。確認裝置密碼以提升許可權並

進入專家模式。

```
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:~#
```

檢查容錯移轉狀態

驗證容錯移轉狀態，以確保這些步驟已套用到次要FTD（可以顯示為「次要和待命就緒」）。

```
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#
```

上傳升級套件

導航到設定>更新>產品更新>上傳本地軟體更新包，透過FMC將升級包上傳到兩個裝置。從
software.cisco.com選擇先前下載的軟體套件，然後選擇Upload。

在FMC上上傳Firepower資料包後,請繼續執行Upgrade按鈕。

升級按鈕

在升級嚮導中,您需要選擇FTD HA裝置,然後選擇裝置,然後再按一下Add to Selection。

新增至選取範圍

然後,您可以在裝置上複製升級包,系統會顯示一條消息,以繼續升級包。
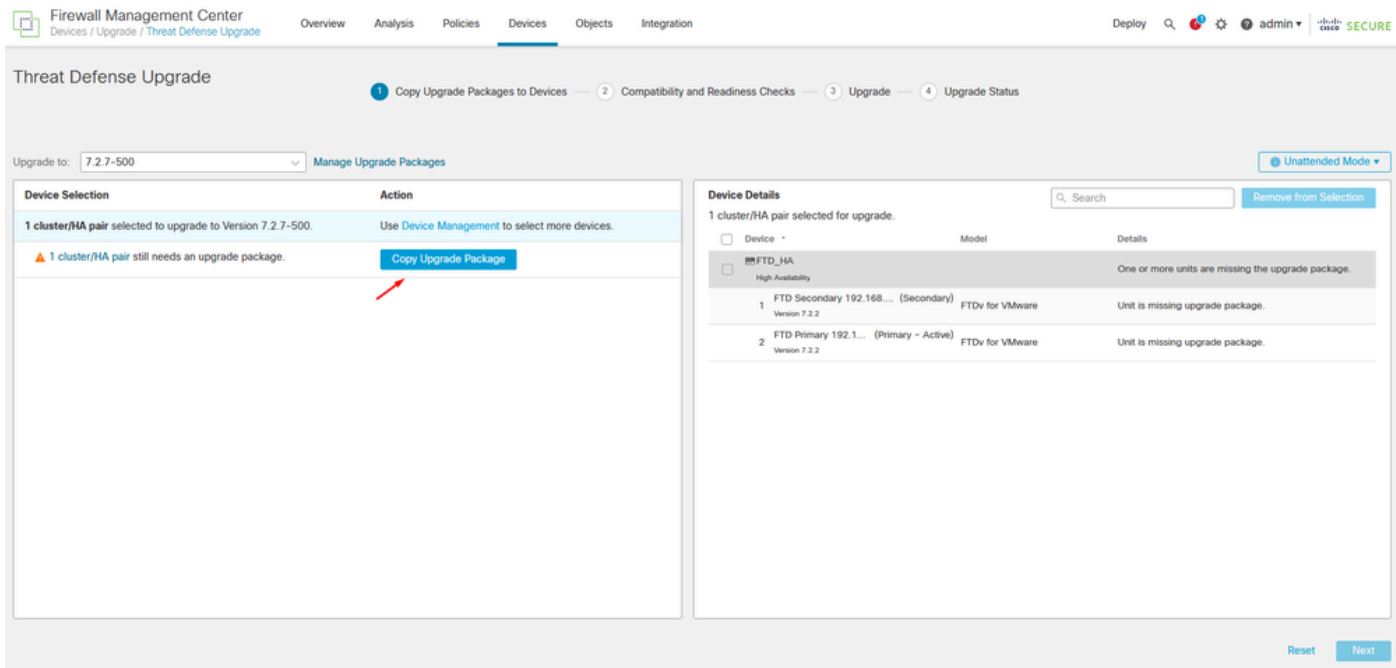
複製升級包按鈕

在「通知」任務中，您可以找到將檔案複製到裝置的工作。任務完成後，即會完成並成功。
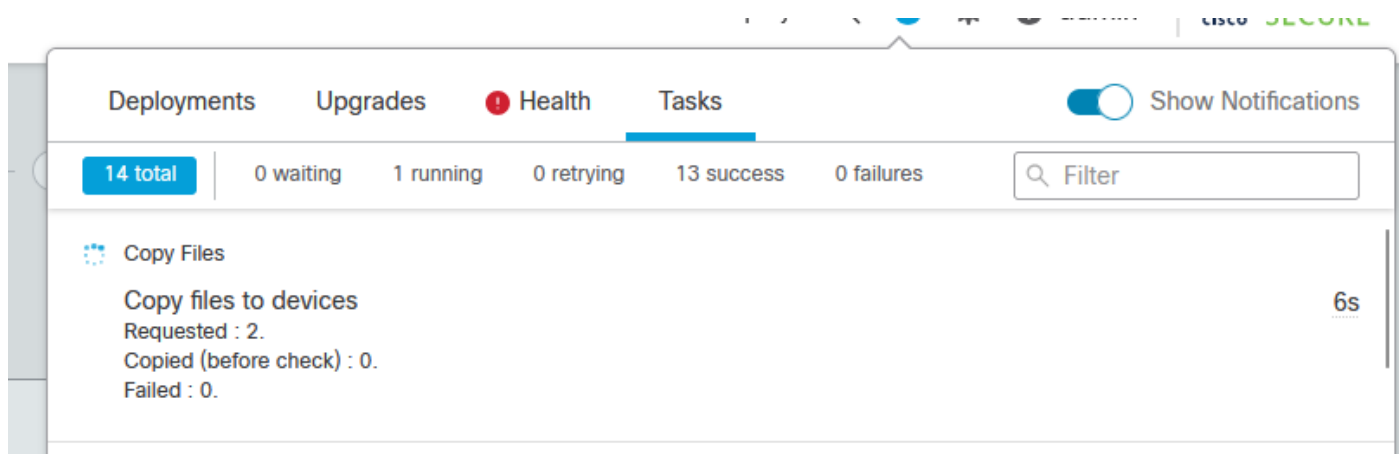
將檔案複製到裝置的任務

您可以驗證封裝是否已上傳到此路徑上的裝置：

```
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#
```

準備程度檢查

使用命令從輔助裝置上的CLI執行就緒性檢查：

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

以下是範例：

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/C
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 line
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.s
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/s
root@firepower:/ngfw/var/sf/updates#
```

透過以下路徑監控就緒性檢查流程：

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_kick
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_nun
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#
```

如果就緒性檢查失敗，請與Cisco TAC聯絡。

升級安裝

在次要FTD上繼續升級安裝。瀏覽至包含升級檔案的資料夾，然後執行安裝指令：

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

執行升級後，將會出現如下所示的輸出：

```
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/Statusi
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.REl
[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_st
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_sta
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
```

在FMC上，有一個任務在輔助裝置上運行升級：
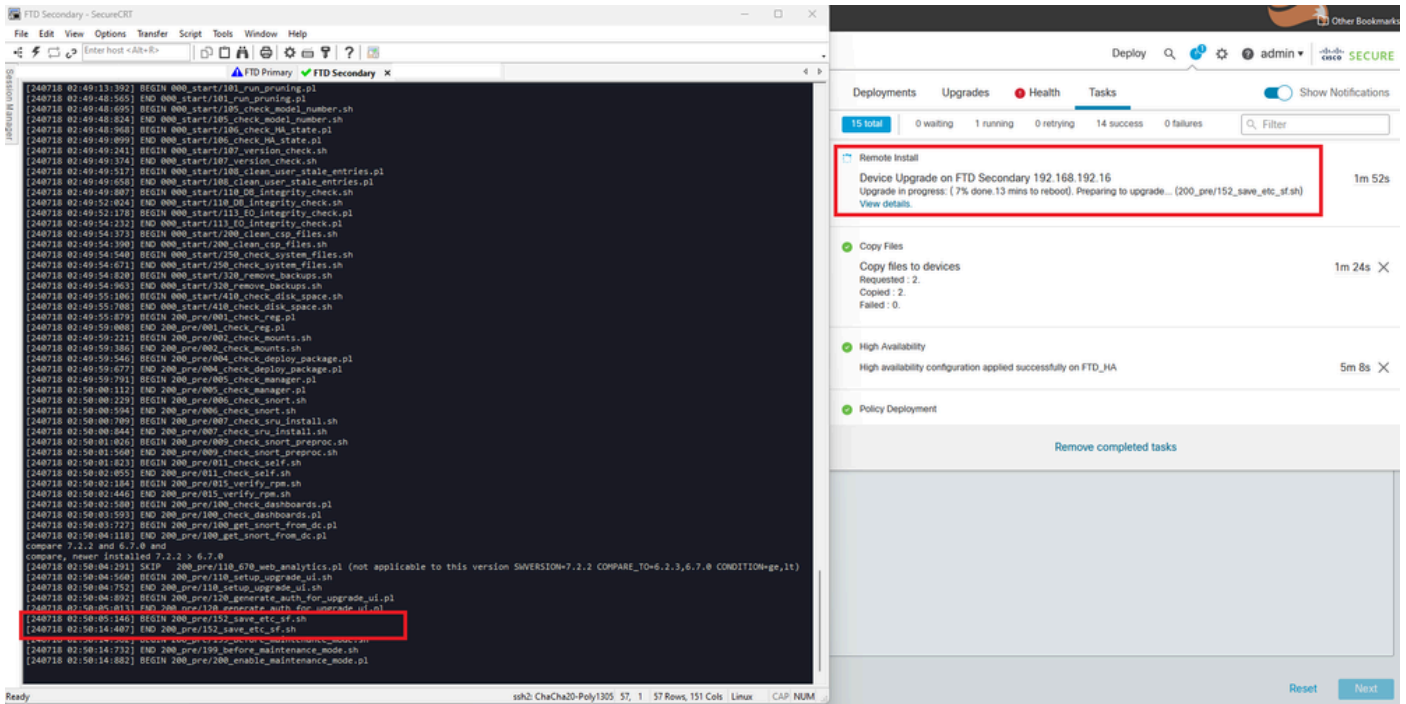
在FMC上執行的作業

使用以下路徑監控升級狀態：

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

以下是輸出範例：

```
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_Linu
```

輔助裝置上的升級完成後，您將看到以下消息：

```
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_stat
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volum
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!
```

從備用裝置升級完成後，裝置將重新啟動。裝置啟動後，請檢查故障切換狀態以確保所有裝置都保持初始配置狀態。

在作用中FTD上，您可以找到：

```
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#
```

在待命FTD上，您會發現：

```
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#
```

將會出現一則訊息，顯示版本不同。

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

使用命令failover active on Standby Device透過CLI手動執行故障切換。現在，備用裝置變為活動狀態。

警告：此時，在發生故障切換時，資料流將短暫中斷。

```
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#
```

故障切換完成後,您可以繼續升級其他裝置。使用與文檔開始部分描述的步驟相同的步驟,適用於以前處於活動狀態而現在處於備用狀態的裝置。

現在兩個裝置都已升級。您可以透過Lina端的show version命令進行檢視。對於主裝置:

```
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#
```

對於輔助裝置:

```
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#
```

此時，您可以像開始時一樣從FMC切換裝置。

驗證

成功升級兩個裝置後，使用show version命令驗證FMC和兩個FTD上的狀態。

```
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
---------------------------------------------------
```

在FMC上，您可以看到版本更新，並準備切換至您最初的狀態。

來自FMC的交換對等體