

Aggiornamento di FTD HA tramite CLI gestito da FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Preparazione per l'aggiornamento](#)

[Controlla stato failover](#)

[Carica il pacchetto di aggiornamento](#)

[Verifica preparazione](#)

[Installazione aggiornamento](#)

[Verifica](#)

Introduzione

Questo documento descrive una procedura dettagliata per aggiornare i dispositivi Cisco Firepower Threat Defense (FTD) tramite l'interfaccia della riga di comando (CLI).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Management Center v7.2.8
- Cisco Firepower Threat Defense per VMWare v7.2.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I requisiti specifici per questo documento includono:

- Cisco Secure Firewall Threat Defense con versione 7.2 o superiore
- Cisco Secure Firewall Management Center con versione 7.2 o superiore

Configurazione

L'aggiornamento di una coppia di dispositivi FTD tramite CLI richiede che il file del pacchetto di aggiornamento sia presente sul dispositivo. È essenziale non avere distribuzioni in sospeso come prerequisito per un aggiornamento corretto tramite CLI.

Preparazione per l'aggiornamento



Avvertenza: controllare l'ordine di aggiornamento Standby/Attivo per evitare interruzioni del traffico.

1. Iniziare con il dispositivo configurato come Standby.
2. Accedere alla CLI in modalità expert immettendo expert seguito da sudo su in modalità clish. Confermare la password del dispositivo per elevare i privilegi e accedere alla modalità Expert.

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:~#
```

Controlla stato failover

Verificare lo stato di failover per assicurarsi che i passi vengano applicati all'FTD secondario, che può essere visualizzato come Secondario e Pronto per standby.

```
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#
```

Carica il pacchetto di aggiornamento

Caricare il pacchetto di aggiornamento su entrambi i dispositivi tramite FMC selezionando Impostazioni > Aggiornamenti > Aggiornamenti prodotti > Carica pacchetto di aggiornamento software locale. Selezionare il pacchetto scaricato in precedenza da software.cisco.com e selezionare Upload.

Una volta caricato il pacchetto Firepower sul FMC, continuare con il pulsante Aggiorna.

Firewall Management Center
System / Product Upgrades

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco

Product Upgrades

System Overview

Management Center: 7.2.8-25
Already running latest version.
Last upgrade performed: 7.2.5-208 → 7.2.8-25

Threat Defense: 1 cluster/HA pair
Visit [Device Management](#) to view your devices.
Upgrade: Initiated (7.2.2-54) [View](#)

Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.2.8-25	2024-05-31	6.6.0	Downloaded	...
▼ 7.2.7-500	2024-04-27	6.6.0	Downloaded	Upgrade ...
Firepower Threat Defense for ASA/ISA/FTDv				...
> 7.2.2-54	2022-11-22	6.6.0	Downloaded	...
> 6.6.5-81	2021-07-28	6.2.3	Downloaded	...

Pulsante Aggiorna

Nell'aggiornamento guidato è necessario selezionare i dispositivi FTD HA, quindi selezionare i dispositivi e fare clic su Aggiungi alla selezione.

Firewall Management Center
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco **SECURE**

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 [Manage Upgrade Packages](#) [Unattended Mode](#)

Device Selection **Action**

1 cluster/HA pair is a candidate to add to your upgrade list.

No devices selected. Use the Device Details pane to select devices to upgrade to the selected version. Or, use [Device Management](#) to select more devices.

Device Details

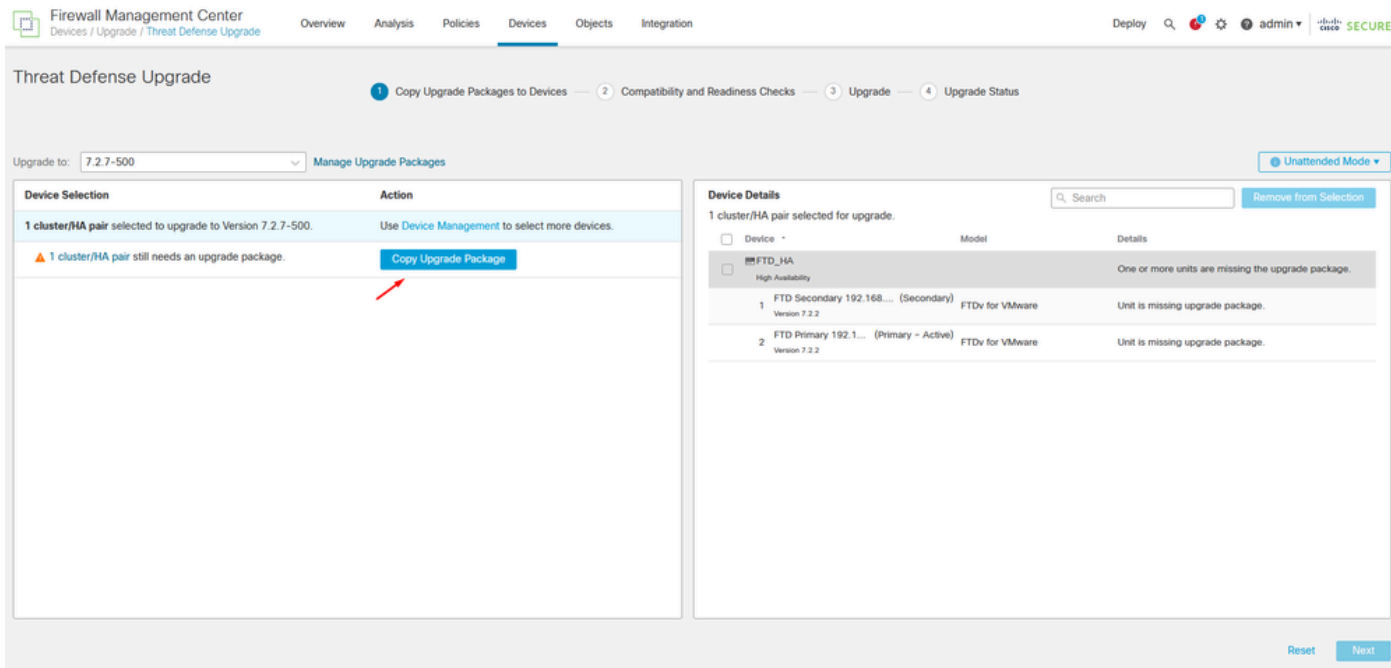
1 cluster/HA pair is a candidate to add to your upgrade list. [Add to Selection](#)

Device	Model	Details
<input checked="" type="checkbox"/> FTD_HA		High Availability
	FTD Primary 192.168.192.13 (Primary)	FTDv for VMware Version 7.2.2
	FTD Secondary 192.168.192.14 (Secondary)	FTDv for VMware Version 7.2.2

[Reset](#) [Next](#)

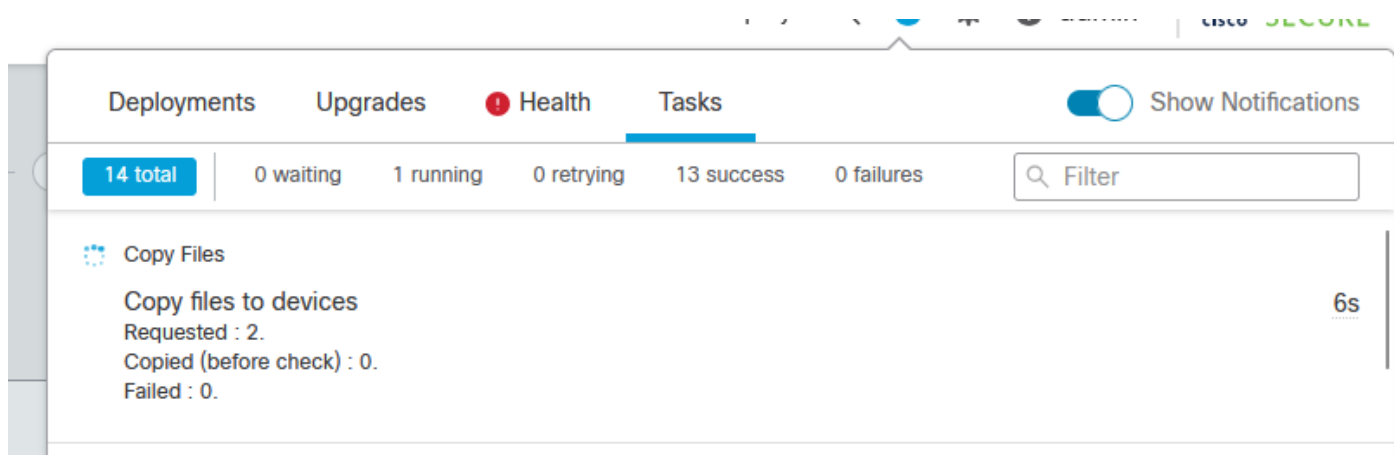
Aggiungi alla selezione

Quindi, è possibile copiare il pacchetto di aggiornamento sui dispositivi; viene visualizzato un messaggio per continuare l'aggiornamento dei pacchetti.



Pulsante Copia pacchetto di aggiornamento

Nell'attività Notifica è possibile trovare il processo di copia dei file nel dispositivo Al termine dell'attività, l'operazione è stata completata e completata correttamente.



Attività Copia di file nei dispositivi

È possibile verificare che il pacchetto sia caricato nei dispositivi sul seguente percorso:

```

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#

```

Verifica preparazione

Eseguire il controllo di fattibilità dalla CLI sul dispositivo secondario utilizzando il comando:

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

Di seguito è riportato un esempio:

```
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 line
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 1
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#
```

Monitora il processo di verifica preparazione nel percorso seguente:

```
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_E0_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#
```

Se il controllo della preparazione non riesce, contattare Cisco TAC.

Installazione aggiornamento

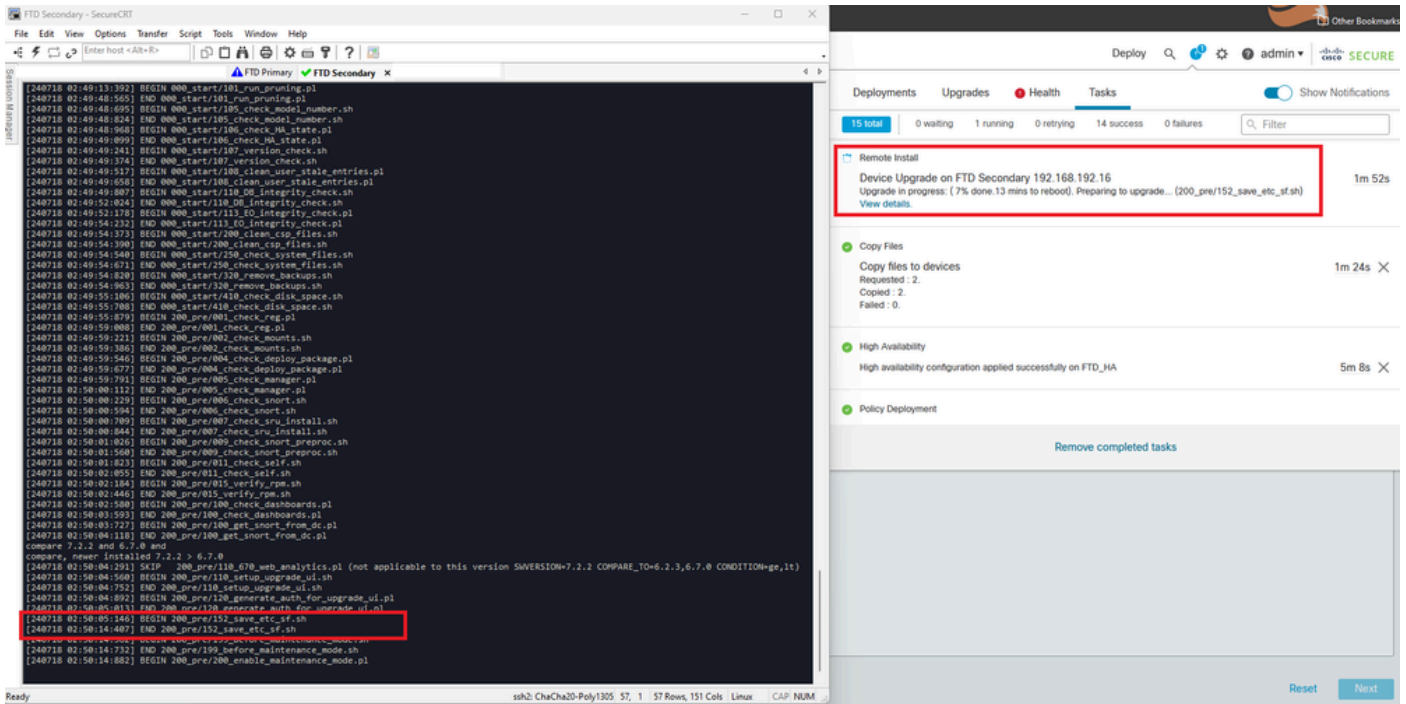
Procedere con l'installazione di aggiornamento sull'FTD secondario. Passare alla cartella contenente il file di aggiornamento ed eseguire il comando di installazione:

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

Una volta eseguito l'aggiornamento, verrà generato un output simile al seguente:

```
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 1
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
```

Nel FMC è presente un'operazione che esegue l'aggiornamento sul dispositivo secondario:



Attività in esecuzione in FMC

Monitorare lo stato dell'aggiornamento utilizzando il seguente percorso:

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

Di seguito è riportato un esempio dell'output:

```
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
```

Al termine dell'aggiornamento sul dispositivo secondario, viene visualizzato questo messaggio:

```
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_status
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json]
Link to JSON upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log]
Link to log upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log
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!
```

Al termine dell'aggiornamento dal dispositivo in standby, il dispositivo verrà riavviato. Dopo l'accensione dei dispositivi, controllare lo stato del failover per verificare che la configurazione iniziale non sia cambiata.

Sul FTD attivo è possibile trovare:

```
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#
```

In Standby FTD, è possibile trovare quanto segue:

```
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#

Verrà visualizzato un messaggio che indica che le versioni non sono uguali.

firepower#

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

Eeguire il failover manualmente tramite CLI utilizzando il comando failover attivo sul dispositivo di standby. A questo punto, il dispositivo di standby diventa attivo.



Avviso: a questo punto si verifica una breve interruzione del traffico quando si verifica il

failover.

```
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#
```

Una volta completato il failover, è possibile procedere con l'aggiornamento dell'altro dispositivo. Eseguire la stessa procedura descritta all'inizio del documento per la periferica che in precedenza era attiva e che ora è in standby.

Ora entrambi i dispositivi sono aggiornati. Per visualizzarlo, usare il comando show version sul lato Lina. Per il dispositivo principale:

```
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#
```

Per il dispositivo secondario:

```

firepower#
firepower# sh failover state

This host - State           Last Failure Reason   Date/Time
           - 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#

```

A questo punto è possibile passare da FMC ai dispositivi come all'inizio.

Verifica

Dopo aver aggiornato correttamente entrambi i dispositivi, verificare lo stato nel FMC e su entrambi gli FTD utilizzando il comando show version.

```

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
-----

```

Nel FMC è possibile visualizzare l'aggiornamento della versione ed è possibile passare alla versione precedente.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD Primary 192.168.192.13(Primary, Active) Snort 3 192.168.192.13 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	⊕
FTD Secondary 192.168.192.16(Secondary, Standby) Snort 3 192.168.192.16 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	⊕

Peer commutati da FMC

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).