

Promovendo um FTD HA emparelho em dispositivos de FirePOWER

Índice

[Introdução](#)

[Objetivo](#)

[Componentes do laboratório](#)

[Topologia](#)

[O processo de upgrade FTD HA](#)

[Passo 1: Verifique as condições prévias](#)

[Passo 2: Transfira arquivos pela rede as imagens](#)

[Passo 3: Promova os FXO secundários](#)

[Passo 4: Troque os estados do Failover FTD](#)

[Passo 5: Promova o dispositivo preliminar FXO](#)

[Passo 6: Promova o software FMC](#)

[Passo 7: Promova os pares FTD HA](#)

[Passo 8: Distribua uma política aos pares FTD HA](#)

[Documentos relacionados](#)

Introdução

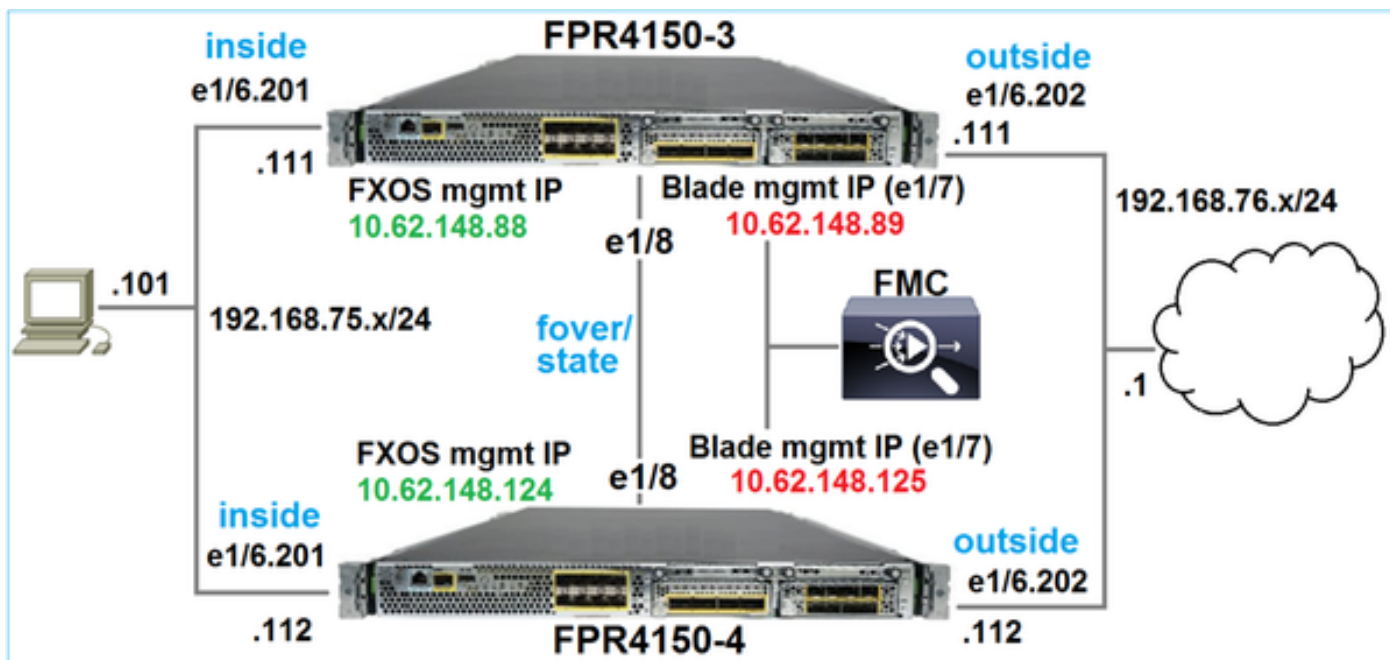
Objetivo

O objetivo deste documento é demonstrar o processo de upgrade da defesa da ameaça de FirePOWER (FTD) na Alta disponibilidade do modo em dispositivos de FirePOWER.

Componentes do laboratório

- 2 x FP4150
- 1 x FS4000
- 1 PC

Topologia



As versões de imagem de software antes de começar a atividade:

- Centro de gerenciamento de FirePOWER (FMC) 6.1.0-330
- FTD 6.1.0-330 preliminares
- FTD 6.1.0-330 secundários
- FXO 2.0.1-37 preliminares
- FXO 2.0.1-37 secundários

Plano de ação

Passo 1: Verifique as condições prévias

Passo 2: Transfira arquivos pela rede as imagens a FMC e a SSP

Passo 3: Promova os FXO secundários 2.0.1-37 - > 2.0.1-86

Passo 4: Troque o Failover FTD (você terá preliminar/apoio, o secundário/Active)

Passo 5: Promova os FXO preliminares 2.0.1-37 - > 2.0.1-86

Passo 6: Promova o FMC 6.1.0-330 - > 6.1.0.1

Passo 7: Promova os pares 6.1.0-330 FTD HA - > 6.1.0.1

Passo 8: Distribua uma política de FMC aos pares FTD HA

O processo de upgrade FTD HA

Passo 1: Verifique as condições prévias

Consulte o guia da compatibilidade FXO para determinar no meio a compatibilidade:

- Vise a versão de software FTD e a versão de software FXO
- Plataforma do HW de FirePOWER e versão de software FXO

<http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#pgfld-136544>

Verifique os Release Note FXO da versão de destino para determinar o caminho de upgrade FXO:

http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos201/release/notes/fxos201_rn.html#pgfld-141076

Consulte os Release Note da versão de destino FTD para determinar o caminho de upgrade FTD:

<http://www.cisco.com/c/en/us/td/docs/security/firepower/601/6012/relnotes/firepower-system-release-notes-version-6012.html#pgfld-378288>

Passo 2: Transfira arquivos pela rede as imagens

Nos 2 FCMs transfere arquivos pela rede as imagens FXO (fxos-k9.2.0.1.86.SPA)

Na transferência de arquivo pela rede FMC a elevação FMC e FTD empacota:

- Para a elevação FMC: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- Para a elevação FTD: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

Passo 3: Promova os FXO secundários

Antes da elevação:

```
FPR4100-4-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.0(1.37)
  Upgrade-Status: Ready
```

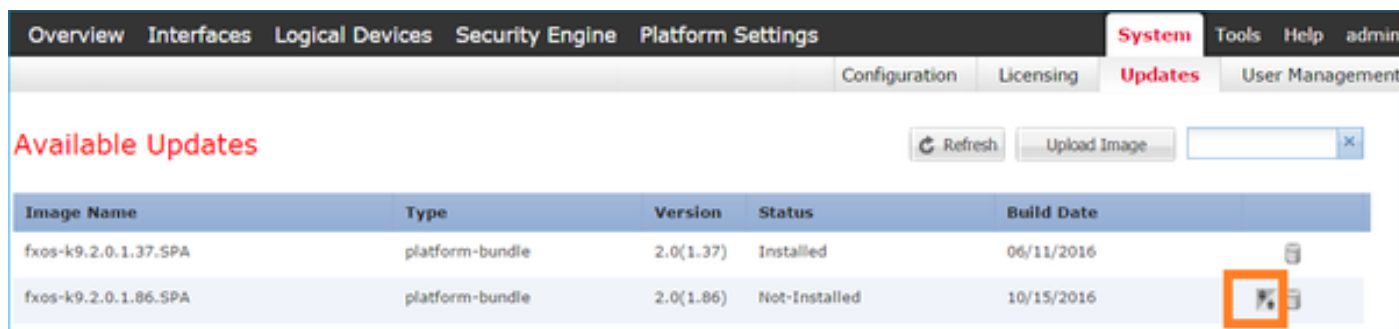
Fabric Interconnect A:

Package-Vers: 2.0(1.37)
Upgrade-Status: Ready

Chassis 1:

Server 1:
Package-Vers: 2.0(1.37)
Upgrade-Status: Ready

Comece a elevação FXO:

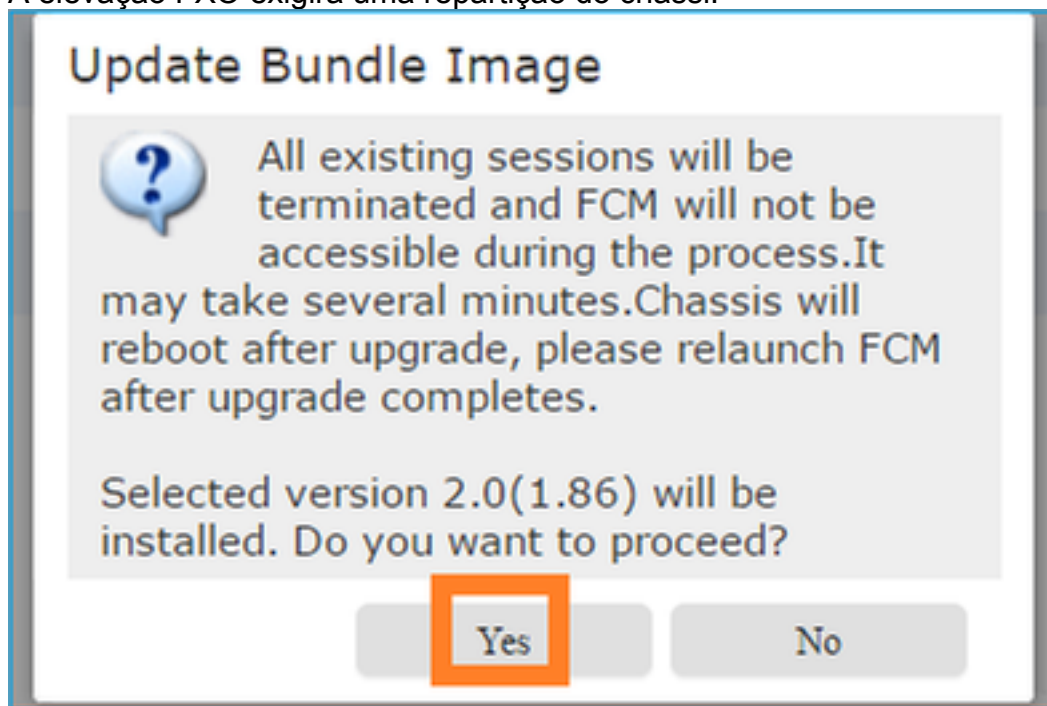


The screenshot shows a web interface with a navigation bar at the top containing 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', 'Platform Settings', 'System', 'Tools', 'Help', and 'admin'. Below the navigation bar, there are tabs for 'Configuration', 'Licensing', 'Updates', and 'User Management'. The 'Updates' tab is active, displaying a section titled 'Available Updates'. This section includes a 'Refresh' button, an 'Upload Image' button, and a search input field. Below this is a table with the following data:

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Installed	06/11/2016
fxos-k9.2.0.1.86.SPA	platform-bundle	2.0(1.86)	Not-Installed	10/15/2016

An orange box highlights the 'Not-Installed' status and the 'fxos-k9.2.0.1.86.SPA' row in the table.

A elevação FXO exigirá uma repartição do chassi:



The screenshot shows a dialog box titled 'Update Bundle Image'. It contains a question mark icon and the following text: 'All existing sessions will be terminated and FCM will not be accessible during the process. It may take several minutes. Chassis will reboot after upgrade, please relaunch FCM after upgrade completes.' Below this text, it says 'Selected version 2.0(1.86) will be installed. Do you want to proceed?'. At the bottom of the dialog, there are two buttons: 'Yes' and 'No'. The 'Yes' button is highlighted with an orange box.

Você pode monitorar a elevação FXO dos FXO CLI. Todos os 3 componentes (FPRM, interconexão da tela e chassi) têm que ser promovidos:

```
FPR4100-4-A# scope system
FPR4100-4-A /system # show firmware monitor
FPRM:
Package-Vers: 2.0(1.37)
Upgrade-Status: Upgrading
```

```
Fabric Interconnect A:  
  Package-Vers: 2.0(1.37)  
  Upgrade-Status: Ready
```

```
Chassis 1:  
  Server 1:  
    Package-Vers: 2.0(1.37)  
    Upgrade-Status: Ready
```

Nota – Poucos minutos após ter começado o processo de upgrade FXO você pôde ser desligado de FXO CLI e de GUI. Você deve poder entrar outra vez após poucos segundos.

Após o minuto ~5 a elevação componente FPRM termina:

```
FPR4100-4-A /system # show firmware monitor  
FPRM:  
  Package-Vers: 2.0(1.86)  
  Upgrade-Status: Ready
```

```
Fabric Interconnect A:  
  Package-Vers: 2.0(1.37)  
  Upgrade-Status: Upgrading
```

```
Chassis 1:  
  Server 1:  
    Package-Vers: 2.0(1.37)  
    Upgrade-Status: Upgrading
```

Após ~10 minutos e como parte do processo de upgrade FXO o dispositivo secundário de FirePOWER reinicia:

```
Please stand by while rebooting the system...  
...  
Restarting system.
```

Após o reinício os resumos do processo de upgrade:

```
FPR4100-4-A /system # show firmware monitor  
FPRM:  
  Package-Vers: 2.0(1.86)  
  Upgrade-Status: Ready
```

```
Fabric Interconnect A:  
  Package-Vers: 2.0(1.37)  
  Upgrade-Status: Upgrading
```

```
Chassis 1:
```

```
Server 1:  
  Package-Vers: 2.0(1.37)  
  Upgrade-Status: Upgrading
```

Após um total do minuto ~30 a elevação FXO termina:

```
FPR4100-4-A /system # show firmware monitor  
FPRM:
```

```
  Package-Vers: 2.0(1.86)  
  Upgrade-Status: Ready
```

```
Fabric Interconnect A:
```

```
  Package-Vers: 2.0(1.86)  
  Upgrade-Status: Ready
```

```
Chassis 1:
```

```
  Server 1:  
    Package-Vers: 2.0(1.86),2.0(1.37)  
    Upgrade-Status: Ready
```

Passo 4: Troque os estados do Failover FTD

Antes de trocar os estados do failver certifique-se de que o módulo FTD no chassi secundário está inteiramente ACIMA:

```
FPR4100-4-A# connect module 1 console  
Firepower-module1>connect ftd  
Connecting to ftd console... enter exit to return to bootCLI
```

```
> show high-availability config
```

```
Failover On  
Failover unit Secondary  
Failover LAN Interface: FOVER Ethernet1/8 (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 1041 maximum  
MAC Address Move Notification Interval not set  
failover replication http  
Version: Ours 9.6(2), Mate 9.6(2)  
Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U  
Last Failover at: 15:08:47 UTC Dec 17 2016  
  This host: Secondary - Standby Ready  
    Active time: 0 (sec)  
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys)  
      Interface inside (192.168.75.112): Normal (Monitored)  
      Interface outside (192.168.76.112): Normal (Monitored)  
      Interface diagnostic (0.0.0.0): Normal (Waiting)  
    slot 1: snort rev (1.0) status (up)  
    slot 2: diskstatus rev (1.0) status (up)
```

Other host: Primary - Active

```
Active time: 5163 (sec)
Interface inside (192.168.75.111): Normal (Monitored)
Interface outside (192.168.76.111): Normal (Monitored)
Interface diagnostic (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 : FOVER Ethernet1/8 (up)
Stateful Obj   xmit      xerr      rcv        rerr
General        65         0         68         4
sys cmd        65         0         65         0
...
```

Troque os estados do Failover FTD. Do FTD ativo CLI:

```
> no failover active
    Switching to Standby
>
```

Nota - Neste momento você pôde ter o pacote ~1 de tráfego de trânsito FTD deixado cair

Passo 5: Promova o dispositivo preliminar FXO

Similar à elevação de etapa 2 o dispositivo FXO onde o FTD preliminar é instalado - esta etapa pode tomar ~30 minutos ou mais para terminar.

Passo 6: Promova o software FMC

Promova o FMC, nesta encenação de 6.1.0-330 a 6.1.0.1.

Passo 7: Promova os pares FTD HA

Antes da elevação:

> show high-availability config

Failover On

Failover unit Primary

Failover LAN Interface: FOVER Ethernet1/8 (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 1041 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.6(2), Mate 9.6(2)

Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW

Last Failover at: 15:51:08 UTC Dec 17 2016

This host: Primary - Standby Ready

Active time: 0 (sec)

slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys)

Interface inside (192.168.75.112): Normal (Monitored)

Interface outside (192.168.76.112): Normal (Monitored)

Interface diagnostic (0.0.0.0): Normal (Waiting)

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

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

Other host: Secondary - Active

Active time: 1724 (sec)

Interface inside (192.168.75.111): Normal (Monitored)

Interface outside (192.168.76.111): Normal (Monitored)

Interface diagnostic (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 : FOVER Ethernet1/8 (up)

Stateful Obj	xmit	xerr	rcv	rerr
General	6	0	9	0
sys cmd	6	0	6	0

...

Do menu do sistema > das atualizações FMC inicie o processo de upgrade FTD HA:

Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016		No
Cisco FTD Patch	6.1.0.1-53	Fri Dec 2 17:36:27 UTC 2016		Yes
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016		Yes

Opcionalmente você pode lançar a verificação da prontidão da elevação FTD que inclui uma verificação de integridade FTD DB:

Overview Analysis Policies Devices Objects AMP Deploy System Help admin

Configuration Users Domains Integration **Updates** Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.1.0

Selected Update

Type Cisco FTD SSP Patch
 Version 6.1.0.1-53
 Date Fri Dec 2 17:37:52 UTC 2016
 Release Notes
 Reboot Yes

By Group

▼ Ungrouped (1 total)

<input checked="" type="checkbox"/>	▼ FTD4150-HA Cisco Firepower 4150 Threat Defense Cluster		
<input checked="" type="checkbox"/>	FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09	X ✓
<input checked="" type="checkbox"/>	FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09	X ✓

Launch Readiness Check Install Cancel

A verificação tomou ~5 minutos e foi bem sucedida:

Deployments Health **Tasks** Settings ?

1 total | 0 waiting 0 running 0 retrying 1 success 0 failures

✓ **Remote Install** 5m 2s X

Apply to FTD4150-HA.
 Readiness Check To 10.62.148.125 Success

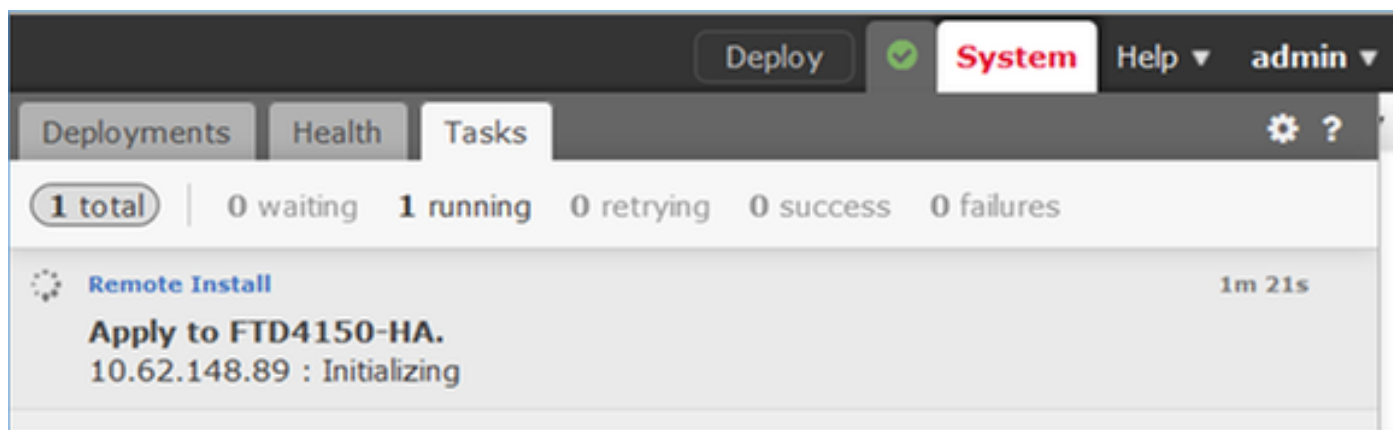
Inicie o processo de instalação:

▼ Ungrouped (1 total)

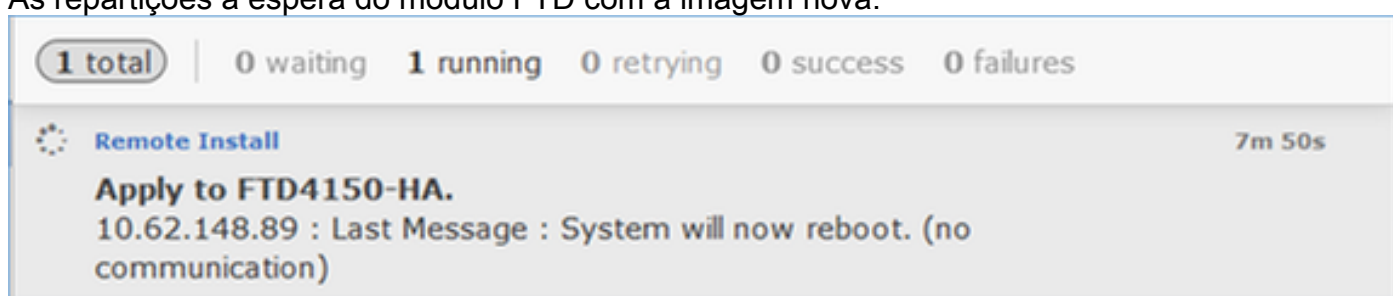
<input checked="" type="checkbox"/>	▼ FTD4150-HA Cisco Firepower 4150 Threat Defense Cluster		
<input checked="" type="checkbox"/>	FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09	X ✓
<input checked="" type="checkbox"/>	FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 12:21:09	X ✓

Launch Readiness Check Install Cancel

FTD primeiramente preliminar/à espera é promovido:



As repartições à espera do módulo FTD com a imagem nova:



Você pode verificar o estado FTD do modo FXO BootCLI:

```
FPR4100-3-A# connect module 1 console
Firepower-module1> show services status
Services currently running:
Feature | Instance ID | State | Up Since
-----|-----|-----|-----
ftd | 001_JAD201200R4WLYCWO6 | RUNNING | :00:00:33
```

FTD secundário/ativo CLI mostra um mensagem de advertência devido à má combinação da versão de software entre os módulos FTD:

```
firepower#
*****WARNING****WARNING****WARNING*****
Mate version 9.6(2) is not identical with ours 9.6(2)4
*****WARNING****WARNING****WARNING*****
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
```

O FMC mostra que o dispositivo FTD esteve promovido com sucesso:

1 total | 1 waiting 0 running 0 retrying 0 success 0 failures

Remote Install 16m 1s

Apply to FTD4150-HA.
10.62.148.89 : Device successfully upgraded

A elevação do segundo módulo FTD começa:

1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 17m 22s

Apply to FTD4150-HA.
10.62.148.125 : [1%] Running script 000_start/101_run_pruning.pl...

No fim do processo o FTD secundário carreg com a imagem nova:

Deploy ✔ **System** Help ▾ admin

Deployments Health **Tasks** ⚙ ?

2 total | 0 waiting 1 running 0 retrying 1 success 0 failures

Remote Install 24m 55s

Apply to FTD4150-HA.
10.62.148.125 : Last Message : System will now reboot. (no communication)

No fundo o FMC, usando o usuário interno “enable_1”, troca os estados do Failover FTD e remove temporariamente a configuração de failover do FTD secundário:

```
firepower# show logging
Dec 17 2016 16:40:14: %ASA-5-111008: User 'enable_1' executed the 'no failover active' command.
Dec 17 2016 16:40:14: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'no failover active'
Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'clear configure failover' command.
Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'clear configure failover'
Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'copy /noconfirm running-config disk0:/modified-config.cfg' command.
Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'copy /noconfirm running-config disk0:/modified-config.cfg'

firepower#
      Switching to Standby

firepower#
```

Nota - Neste momento você pôde ver a queda de pacote de informação ~1 devido à troca do estado do Failover

Neste caso a elevação inteira FTD (ambas as unidades) tomou ~30 minutos:

Verificação

Verificação FTD CLI do dispositivo preliminar FTD:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (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 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2)4, Mate 9.6(2)4
Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW
Last Failover at: 16:40:14 UTC Dec 17 2016
  This host: Primary - Active
    Active time: 1159 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
      Interface inside (192.168.75.111): Normal (Monitored)
      Interface outside (192.168.76.111): Normal (Monitored)
      Interface diagnostic (0.0.0.0): 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: 0 (sec)
    slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
      Interface inside (192.168.75.112): Normal (Monitored)
      Interface outside (192.168.76.112): Normal (Monitored)
      Interface diagnostic (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 : FOVER Ethernet1/8 (up)
  Stateful Obj   xmit      xerr      rcv      rerr
  General        68         0         67         0
...
>
```

Do dispositivo secundário FTD:

```

> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/8 (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 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(2)4, Mate 9.6(2)4
Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U
Last Failover at: 16:52:43 UTC Dec 17 2016
This host: Secondary - Standby Ready
  Active time: 0 (sec)
  slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys)
    Interface inside (192.168.75.112): Normal (Monitored)
    Interface outside (192.168.76.112): Normal (Monitored)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
  slot 1: snort rev (1.0) status (up)
  slot 2: diskstatus rev (1.0) status (up)
Other host: Primary - Active
  Active time: 1169 (sec)
  Interface inside (192.168.75.111): Normal (Monitored)
  Interface outside (192.168.76.111): Normal (Monitored)
  Interface diagnostic (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 : FOVER Ethernet1/8 (up)
Stateful Obj   xmit      xerr      rcv        rerr
General        38         0         41         0
... >

```

Passo 8: Distribua uma política aos pares FTD HA

Depois que a elevação é terminada há uma necessidade de distribuir uma política aos pares HA. Isto é mostrado no FMC UI:

Deploy System Help ▾ admin

Deployments Health Tasks ⚙️ ?

2 total | 0 waiting 0 running 0 retrying 2 success 0 failures

✓ Remote Install 28m 14s ✕

**Apply to FTD4150-HA.
Please reapply policies to your managed devices.**

Distribua as políticas:

Deploy Policies Version: 2016-12-17 06:08 PM

<input checked="" type="checkbox"/>	Device
<input checked="" type="checkbox"/>	FTD4150-HA <ul style="list-style-type: none"><input type="checkbox"/> NGFW Settings: FTD4150<input type="checkbox"/> Access Control Policy: FTD4150<input type="checkbox"/> Intrusion Policy: Balanced Security and Connectivity<input type="checkbox"/> DNS Policy: Default DNS Policy<input checked="" type="checkbox"/> Prefilter Policy: Default Prefilter Policy<input type="checkbox"/> Network Discovery<input type="checkbox"/> Device Configuration (Details)

Verificação

Os pares promovidos FTD HA como ela vista do FMC UI:

Overview Analysis Policies **Devices** Objects AMP

Device Management NAT VPN QoS Platform Settings

Name	Group
<ul style="list-style-type: none"> Ungrouped (1) <ul style="list-style-type: none"> FTD4150-HA <ul style="list-style-type: none"> Cisco Firepower 4150 Threat Defense High Availability <ul style="list-style-type: none"> FTD4150-3(Primary, Active) <ul style="list-style-type: none"> 10.62.148.89 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed FTD4150-4(Secondary, Standby) <ul style="list-style-type: none"> 10.62.148.125 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed 	

Os pares promovidos FTD HA como ele visto do FCM UI:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD4150-3 Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.1.53	10.62.148.89	10.62.148.1	Ethernet1/7	online

Ports:

Data Interfaces: Ethernet1/6 Ethernet1/8

Attributes:

Cluster Operational Status: not-applicable
 Firepower Management IP: 10.62.148.89
 Management URL : https://fs4k
 UUID : 13fcb60-c378

Documentos relacionados

[Cisco FirePOWER NGFW](#)