

Atualização do par HA do FTD em dispositivos Firepower

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Tarefa 1. Verificar os pré-requisitos](#)

[Tarefa 2. Carregar as imagens do software](#)

[Tarefa 3. Atualizar o primeiro chassi FXOS](#)

[Tarefa 4. Trocar os estados de failover de FTD](#)

[Tarefa 5. Atualizar o segundo chassi FXOS](#)

[Tarefa 6. Atualizar o software FMC](#)

[Tarefa 7. Atualizar o par HA do FTD](#)

[Tarefa 8. Implantar uma política no par HA do FTD](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de atualização do Firepower Threat Defense (FTD) no modo de alta disponibilidade (HA) nos dispositivos Firepower.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center (FMC)
- FTD
- Dispositivos Firepower (FXOS)

Componentes Utilizados

- 2 FPR4150
- 1 FS4000
- 1 PC

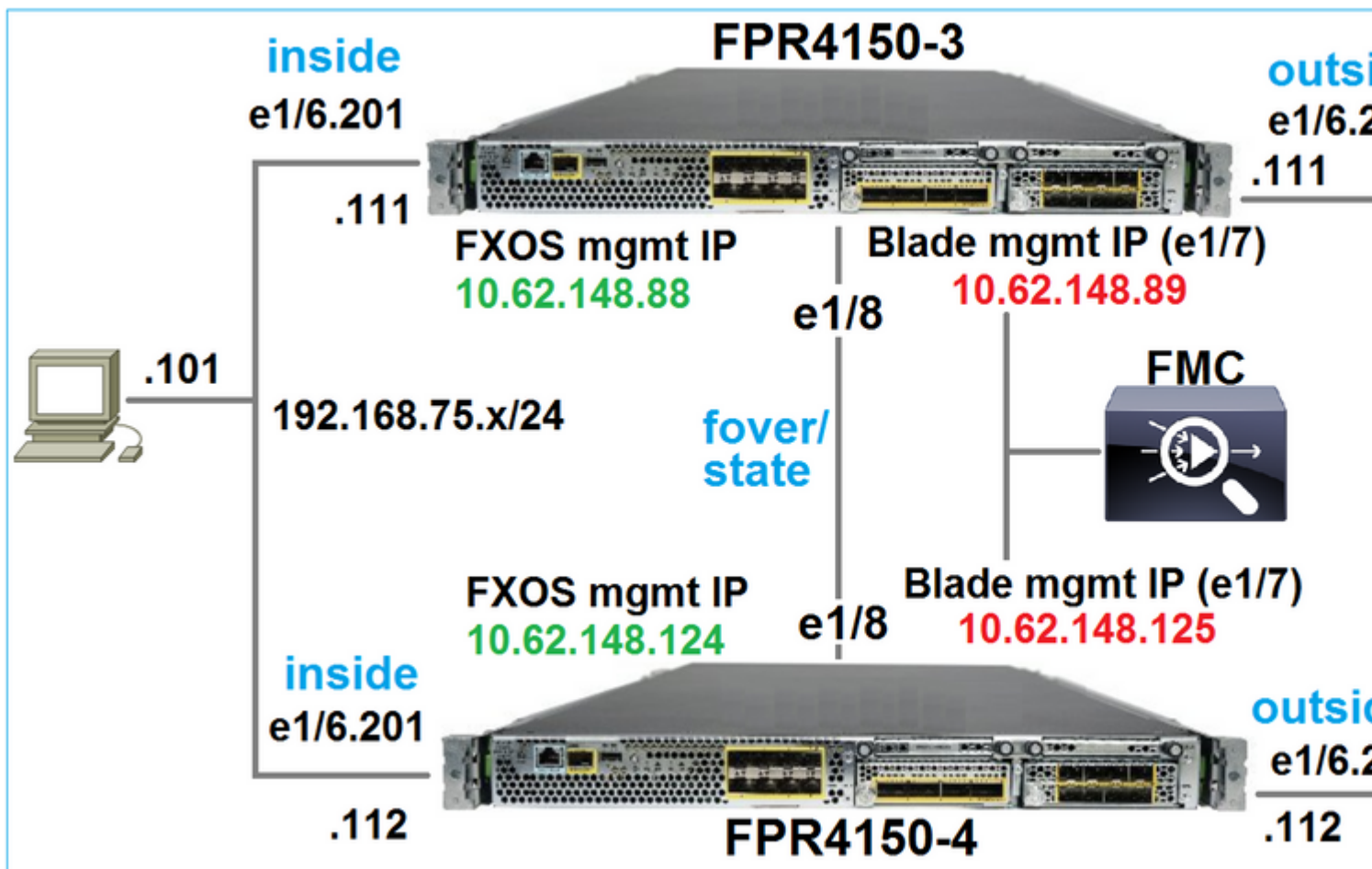
As versões de imagem de software antes da atualização:

- FMC 6.1.0-330
- FTD Principal 6.1.0-330
- FTD secundário 6.1.0-330
- FXOS Principal 2.0.1-37
- FXOS secundário 2.0.1-37

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Plano de ação

Tarefa 1: Verificar os pré-requisitos

Tarefa 2: Carregar as imagens no FMC e no SSP

Tarefa 3: Atualizar o primeiro chassi FXOS (2.0.1-37 -> 2.0.1-86)

Tarefa 4: Trocar o failover de FTD

Tarefa 5: Atualizar o segundo chassi FXOS (2.0.1-37 -> 2.0.1-86)

Tarefa 6: Atualizar o FMC (6.1.0-330 -> 6.1.0.1)

Tarefa 7: Atualizar o par FTD HA (6.1.0-330 -> 6.1.0.1)

Tarefa 8: Implantar uma política do FMC para o par HA do FTD

Tarefa 1. Verificar os pré-requisitos

Consulte o Guia de compatibilidade FXOS para determinar a compatibilidade entre:

- Versão do software FTD alvo e versão do software FXOS
- Plataforma de hardware Firepower e versão do software FXOS

[Compatibilidade com FXOS do Cisco Firepower 4100/9300](#)

Observação: esta etapa não se aplica às plataformas FP21xx e anteriores.

Verifique as Notas de Versão do FXOS da versão de destino para determinar o caminho de atualização do FXOS:

[Notas de versão do Cisco Firepower 4100/9300 FXOS, 2.0\(1\)](#)

Observação: esta etapa não se aplica às plataformas FP21xx e anteriores.

Consulte as Notas de Versão da versão de destino do FTD para determinar o caminho de atualização do FTD:

[Notas de versão do sistema Firepower, Versão 6.0.1.2](#)

Tarefa 2. Carregar as imagens do software

Nos dois FCMs, carregue as imagens FXOS (fxos-k9.2.0.1.86.SPA).

No FMC, carregue os pacotes de atualização do FMC e do FTD:

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

Tarefa 3. Atualizar o primeiro chassi FXOS

Observação: caso você atualize o FXOS de 1.1.4.x para 2.x, primeiro desligue o dispositivo lógico de FTD, atualize o FXOS e, em seguida, reative-o.

Observação: esta etapa não se aplica às plataformas FP21xx e anteriores.

Antes da atualização:

```
<#root>
```

```
FPR4100-4-A /system #
```

```
show firmware monitor
```

```
FPRM:
```

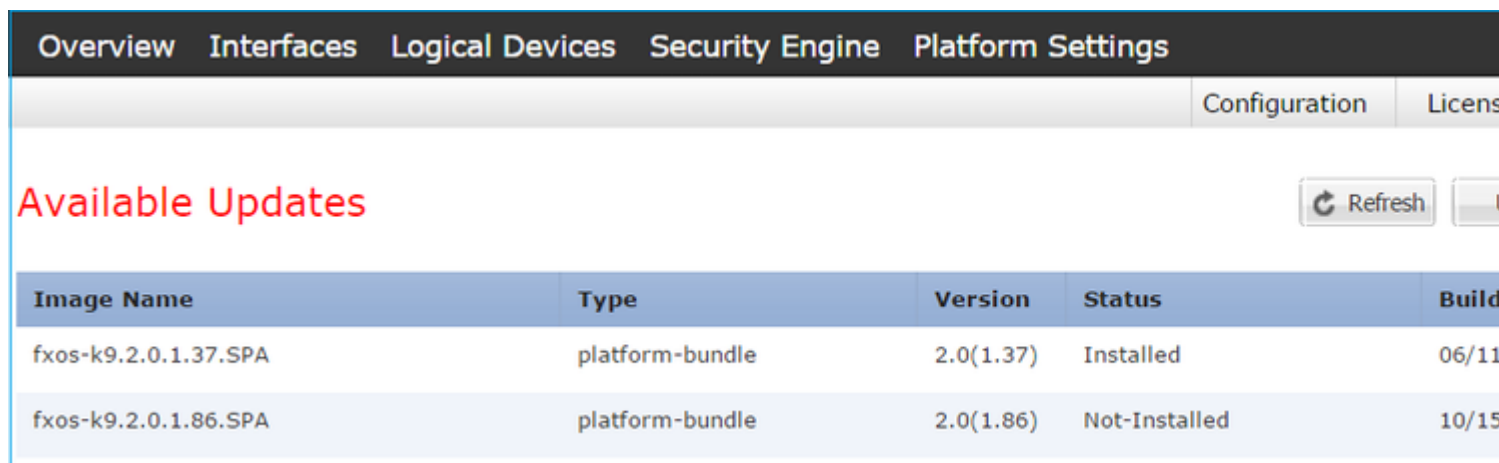
```
Package-Vers: 2.0(1.37)
```

```
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

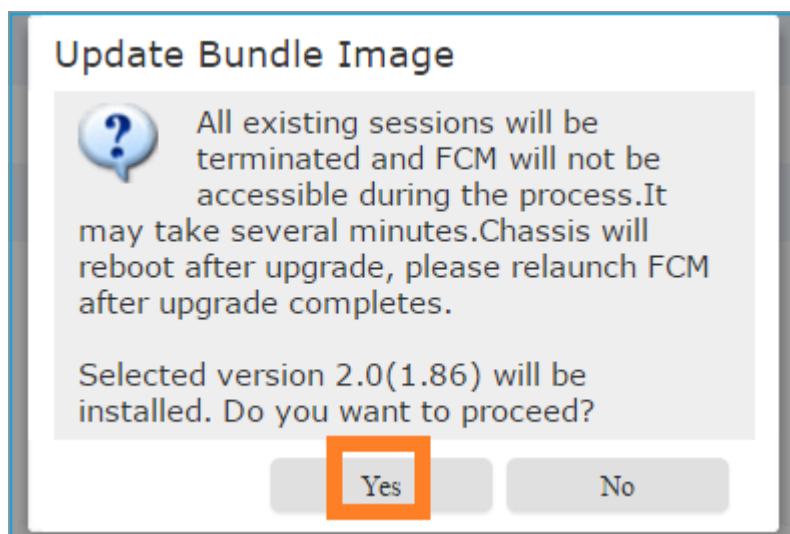
Inicie a atualização do FXOS:



The screenshot shows the 'Available Updates' section of the FXOS configuration interface. The interface has a navigation bar with 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. Below the navigation bar, there are tabs for 'Configuration' and 'Licenses'. The 'Available Updates' section features a red heading and a 'Refresh' button. A table lists the available updates:

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

A atualização do FXOS requer uma reinicialização do chassi:



Você pode monitorar a atualização FXOS a partir da CLI FXOS. Todos os três componentes (FPRM, interconexão de estrutura e chassi) devem ser atualizados:

```
<#root>  
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
```

Observação: alguns minutos após iniciar o processo de atualização do FXOS, você será desconectado da CLI do FXOS e da GUI. Você deve conseguir fazer login novamente após alguns minutos.

Após aproximadamente cinco minutos, a atualização do componente FPRM é concluída:

```
<#root>
```

```
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 aproximadamente 10 minutos, e como parte do processo de atualização do FXOS, o dispositivo Firepower reinicia:

```
<#root>
```

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

```
...
```

Restarting system.

Após a reinicialização, o processo de atualização recomeça:

```
<#root>
```

```
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 de aproximadamente 30 minutos, a atualização do FXOS é concluída:

```
<#root>
```

```
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
```

Tarefa 4. Trocar os estados de failover de FTD

Observação: esta etapa não se aplica às plataformas FP21xx e anteriores.

Antes de trocar os estados de failover, verifique se o módulo FTD no chassi está totalmente ATIVO:

```
<#root>
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 de failover de FTD. Na CLI do FTD Ativo:


```
<#root>
>
no failover active
```

```
Switching to Standby
```

```
>
```

Tarefa 5. Atualizar o segundo chassi FXOS

Semelhante à Tarefa 2, atualize o dispositivo FXOS onde o novo FTD de espera está instalado. Isso pode levar aproximadamente 30 minutos ou mais para ser concluído.

Observação: esta etapa não se aplica às plataformas FP21xx e anteriores.

Tarefa 6. Atualizar o software FMC

Atualize o FMC, neste cenário de 6.1.0-330 para 6.1.0.1.

Tarefa 7. Atualizar o par HA do FTD

Antes da atualização:

```
<#root>
>
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

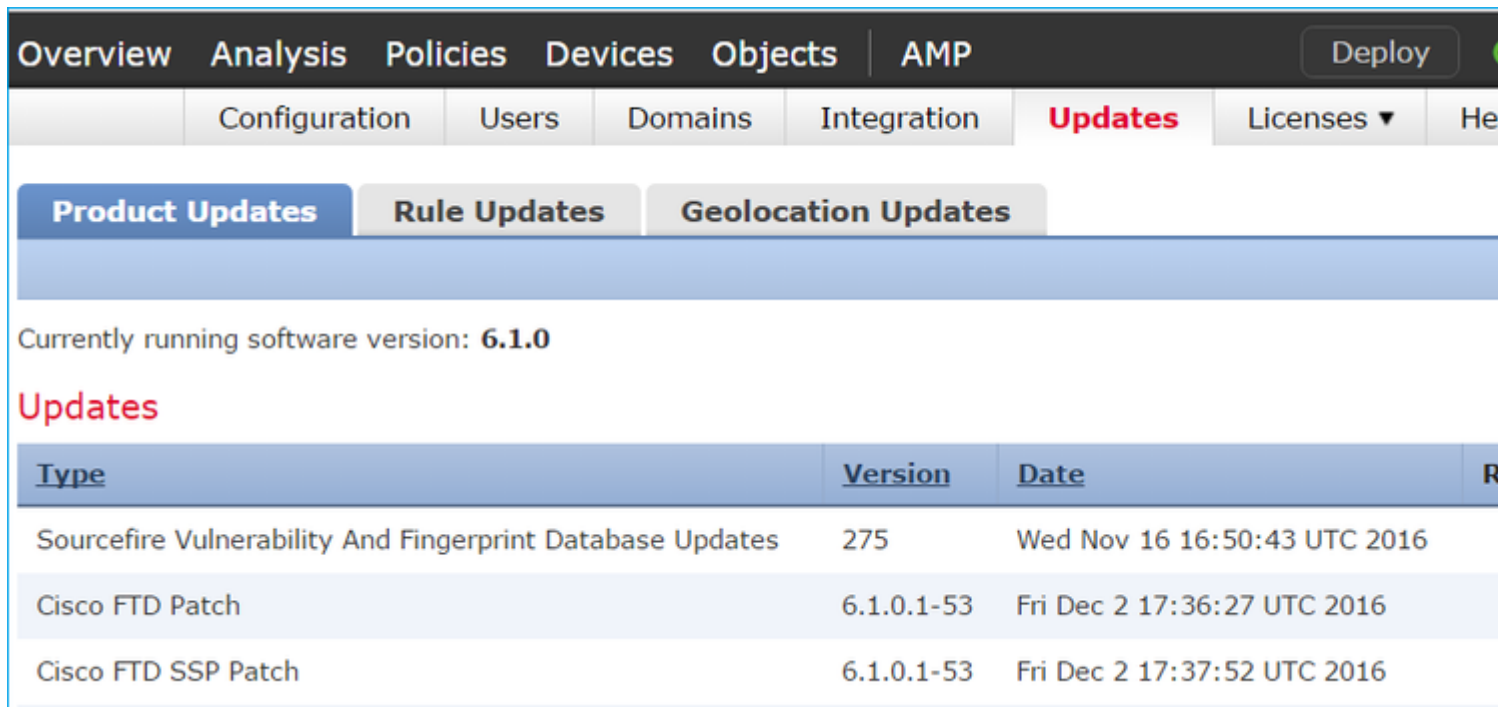
```
Active time: 1724 (sec)
Interface inside (192.168.75.111): Normal (Monitored)
Interface outside (192.168.76.111): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

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
```

...

No menu **Sistema > Atualizações** do FMC, inicie o processo de atualização do FTD HA:



Overview Analysis Policies Devices Objects | AMP Deploy

Configuration Users Domains Integration **Updates** Licenses ▾ He

Product Updates Rule Updates Geolocation Updates

Currently running software version: **6.1.0**

Updates

Type	Version	Date	R
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016	
Cisco FTD Patch	6.1.0.1-53	Fri Dec 2 17:36:27 UTC 2016	
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016	

▼ **Ungrouped (1 total)**

▼ 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 12:21:09
<input checked="" type="checkbox"/> FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Health Policy Initial Health 12:21:09

Primeiro, o FTD Principal/Standby é atualizado:

O módulo FTD em standby é reinicializado com a nova imagem:

Você pode verificar o status do FTD no modo BootCLI do FXOS:

```

<#root>
FPR4100-3-A#
connect module 1 console
Firepower-module1>
show services status

Services currently running:
Feature | Instance ID | State | Up Since
-----|-----|-----|-----
ftd | 001_JAD201200R4WLYCW06 |
  
```

RUNNING

| :00:00:33

A CLI do FTD secundário/ativo mostra uma mensagem de aviso devido a uma incompatibilidade de versão de software entre os módulos do FTD:

<#root>

firepower#

*****WARNING****WARNING****WARNING*****

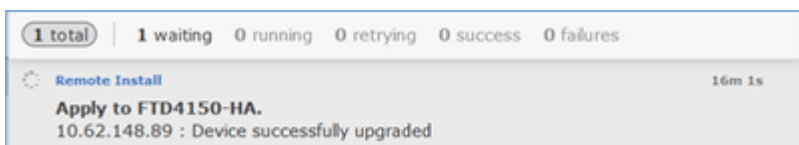
Mate version 9.6(2) is not identical with ours 9.6(2)4

*****WARNING****WARNING****WARNING*****

Beginning configuration replication: Sending to mate.

End Configuration Replication to mate

O FMC mostra que o dispositivo FTD foi atualizado com êxito:

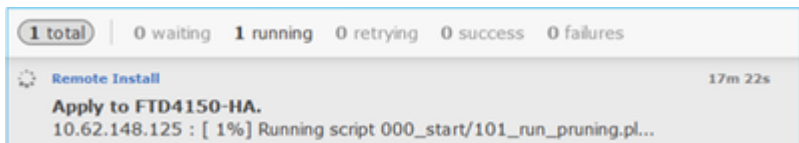


1 total | 1 waiting 0 running 0 retrying 0 success 0 failures

Remote Install 16m 1s

Apply to FTD4150-HA.
10.62.148.89 : Device successfully upgraded

A atualização do segundo módulo FTD inicia-se:

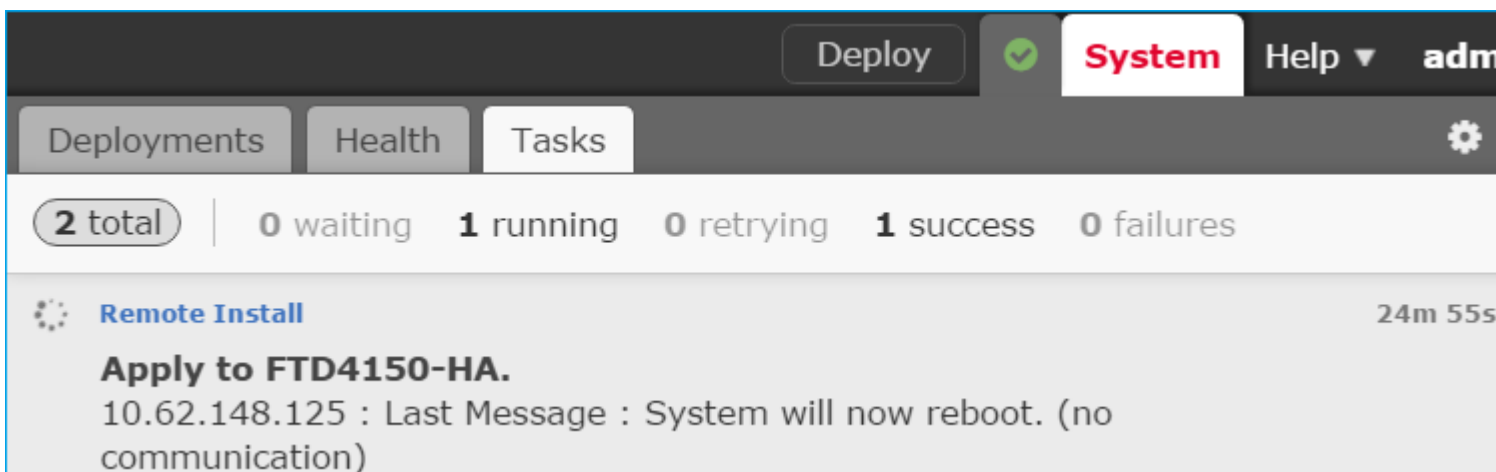


1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 17m 22s

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

No final do processo, o FTD inicializa com a nova imagem:



Deploy System Help adm

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)

Em segundo plano, o FMC usa o usuário interno **enable_1**, troca os estados de failover do FTD e remove temporariamente a configuração de failover do FTD:

<#root>

```
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'  
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#
```

Nesse caso, a atualização do FTD inteiro (ambas as unidades) levou aproximadamente 30 minutos.

Verificação

Este exemplo mostra a verificação FTD CLI do dispositivo FTD principal:

```
<#root>
```

```
>
```

```
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
```

```
...
>
```

Este exemplo mostra a verificação de FTD CLI do dispositivo FTD secundário/em standby:

```
<#root>
```

```
>
```

```
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

```
...  
>
```

Tarefa 8. Implantar uma política no par HA do FTD

Após a conclusão da atualização, você precisa implantar uma política no par HA. Isso é mostrado na interface do usuário do FMC:

The screenshot shows the FMC System page with a 'Deploy' button and a green checkmark. The 'System' tab is active, and the 'Deployments' section shows a summary of 2 total deployments, with 2 success and 0 failures. A specific deployment, 'Remote Install', is highlighted with a green checkmark and a timer of 28m 14s. A message box with an orange border states: 'Apply to FTD4150-HA. Please reapply policies to your managed devices.'

Implante as políticas:

The 'Deploy Policies' window shows the configuration for device FTD4150-HA. The version is 2016-12-17 06:08 PM. The device configuration is listed as follows:

- NGFW Settings: FTD4150
- Access Control Policy: FTD4150
- Intrusion Policy: Balanced Security and Connectivity
- DNS Policy: Default DNS Policy
- Prefilter Policy: Default Prefilter Policy (checked)
- Network Discovery
- Device Configuration ([Details](#))

Verificação

O par HA FTD atualizado, conforme visto na interface do usuário do FMC:

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 	

O par HA FTD atualizado como visto na interface do usuário do FCM:

Overview Interfaces **Logical Devices** Security Engine Platform Settings

FTD4150-3 Standalone Status: ok

Application	Version	Management IP	Gateway	Management
FTD	6.1.0.1.53	10.62.148.89	10.62.148.1	Ethernet1/7
Ports:		Attributes:		
Data Interfaces:	Ethernet1/6 Ethernet1/8	Cluster Operational Status : not-applicable		
		Firepower Management IP : 10.62.148.89		
		Management URL : https://fs4k		
		UUID : 13fbc60-c378		

Informações Relacionadas

- [Cisco Firepower NGFW](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.