

Atualização do FTD HA Gerenciado pelo FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Carregar Pacote de Atualização](#)

[Etapa 2. Verificar Preparação](#)

[Etapa 3. Atualizar o FTD em alta disponibilidade](#)

[Etapa 4. Switch Ativo Peer \(Opcional\)](#)

[Etapa 5. Implantação final](#)

[Validar](#)

Introdução

Este documento descreve o processo de atualização de um Cisco Secure Firewall Threat Defense em alta disponibilidade gerenciado por um Firewall Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Conceitos e configuração de alta disponibilidade (HA)
- Configuração do Secure Firewall Management Center (FMC)
- Configuração do Cisco Secure Firewall Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas em:

- Virtual Firewall Management Center (FMC), versão 7.2.4
- Virtual Cisco Firewall Threat Defense (FTD), versão 7.0.1

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.

Overview

A forma como o CVP funciona consiste em atualizar um ponto de cada vez. Primeiro, o Standby e, em seguida, o Ative, fazendo um failover antes que o upgrade Ative seja concluído.

Informações de Apoio

O pacote de atualização deve ser baixado de software.cisco.com antes da atualização.

Em cliques de CLI, execute o comando `show high-availability config` no FTD Ativo para verificar o status da Alta Disponibilidade.

```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/0 (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 1285 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(2)5, Mate 9.16(2)5
Serial Number: Ours 9AJJSEGJS2T, Mate 9AVLW3FSSK8
Last Failover at: 00:37:48 UTC Jul 20 2023
```

```
    This host: Secondary - Standby Ready
      Active time: 4585 (sec)
      slot 0: ASAv hw/sw rev (/9.16(2)5) status (Up Sys)
        Interface INSIDE (10.10.153.2): Normal (Monitored)
        Interface diagnostic (0.0.0.0): Normal (Waiting)
        Interface OUTSIDE (10.20.153.2): Normal (Monitored)
      slot 1: snort rev (1.0) status (up)
      slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Primary - Active
      Active time: 60847 (sec)
      Interface INSIDE (10.10.153.1): Normal (Monitored)
      Interface diagnostic (0.0.0.0): Normal (Waiting)
      Interface OUTSIDE (10.20.153.1): Normal (Monitored)
      slot 1: snort rev (1.0) status (up)
      slot 2: diskstatus rev (1.0) status (up)
```

Stateful Failover Logical Update Statistics

```
Link : FAILOVER_LINK GigabitEthernet0/0 (up)
Stateful Obj   xmit   xerr   rcv    rerr
General       9192   0      10774  0
sys cmd       9094   0      9092   0
...
Rule DB B-Sync 0       0       0       0
Rule DB P-Sync 0       0      204     0
Rule DB Delete 0       0       1       0
```

Logical Update Queue Information

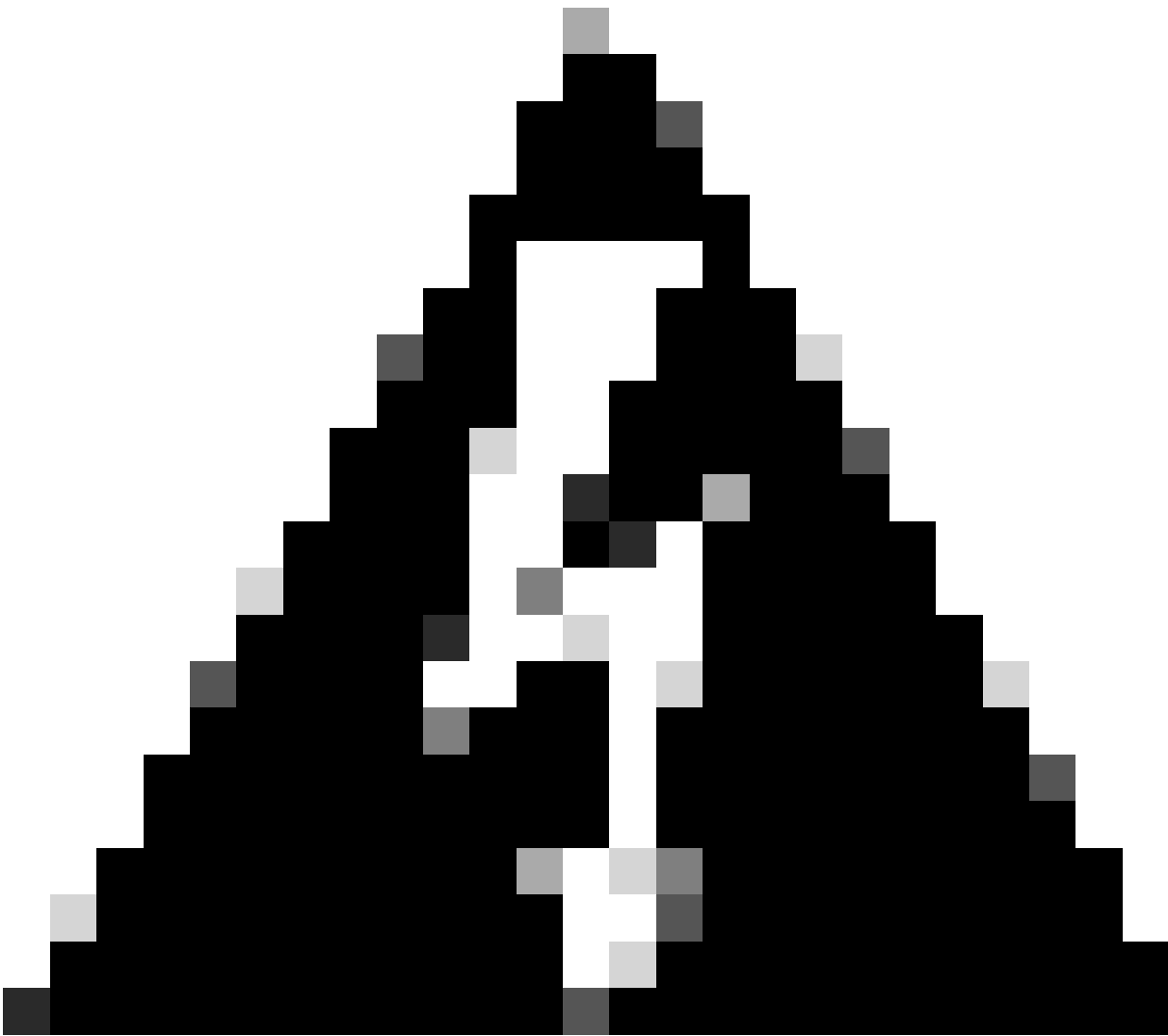
	Cur	Max	Total
Recv Q:	0	9	45336
Xmit Q:	0	11	11572

Se nenhum erro estiver visível, continue com a atualização.

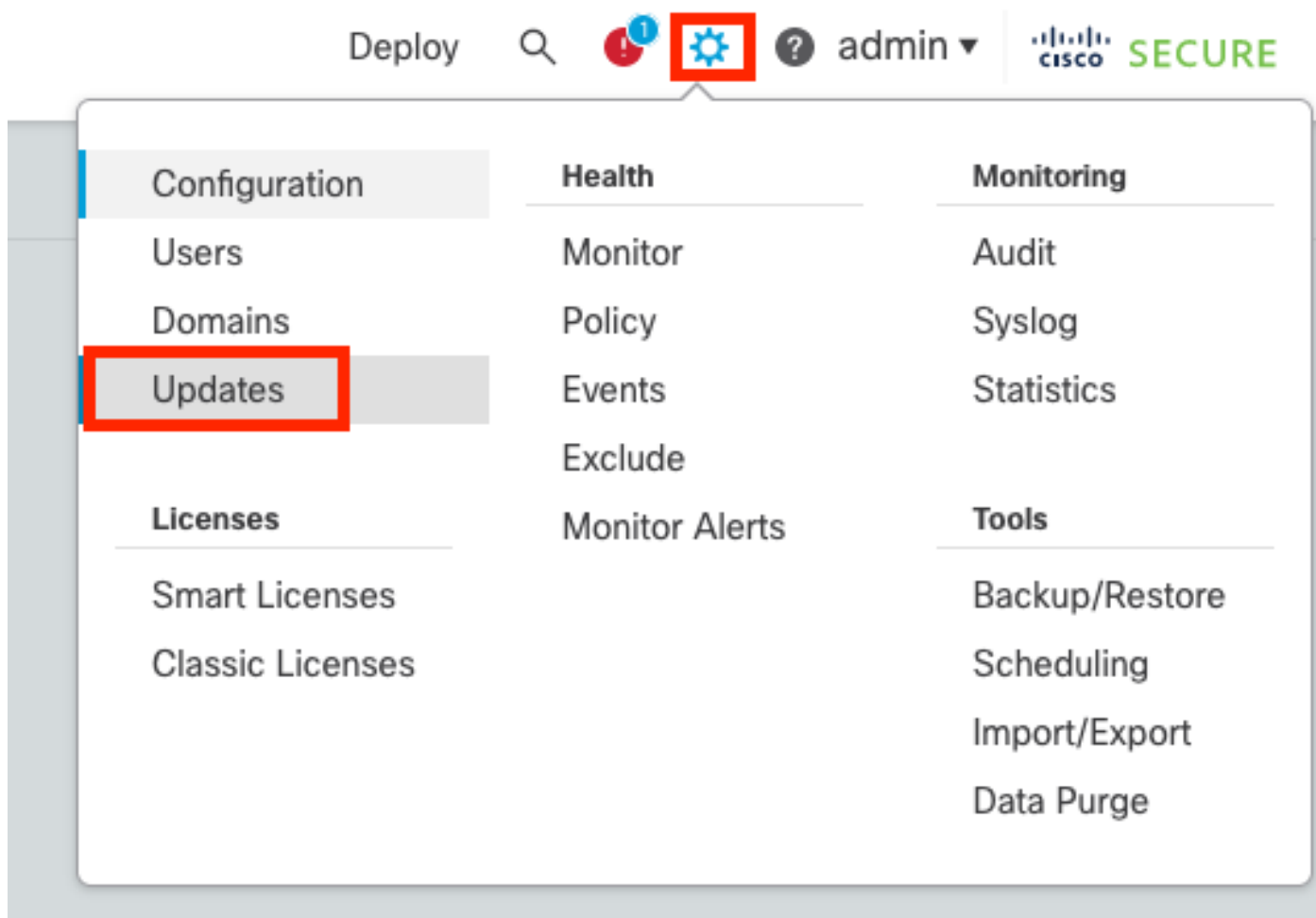
Configurar

Etapa 1. Carregar Pacote de Atualização

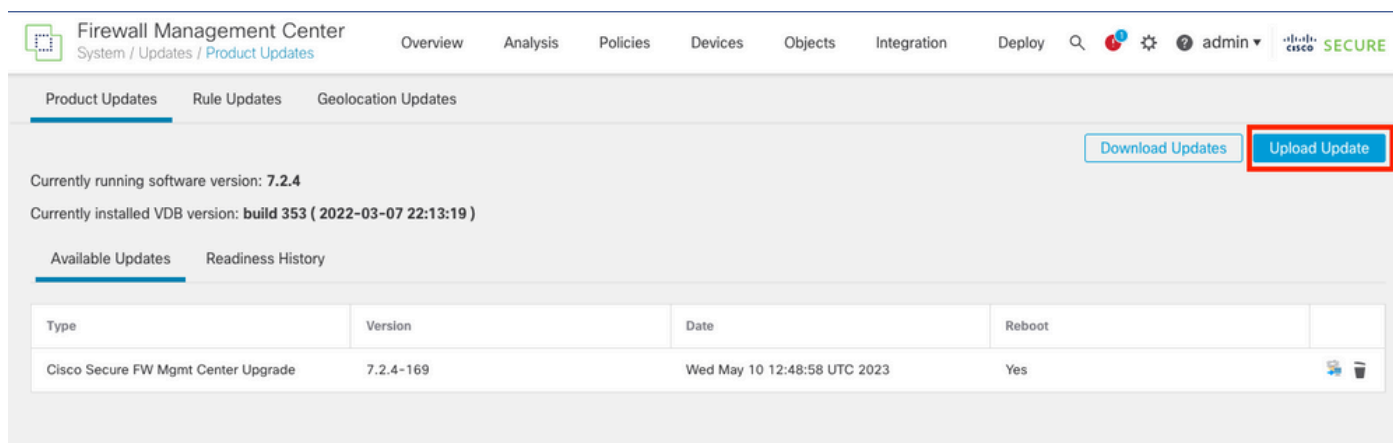
- Carregar o pacote de atualização do FTD no FMC usando a interface gráfica do usuário (GUI).
Ele deve ser baixado anteriormente do site do Software Cisco com base no modelo do FTD e na versão desejada.
-



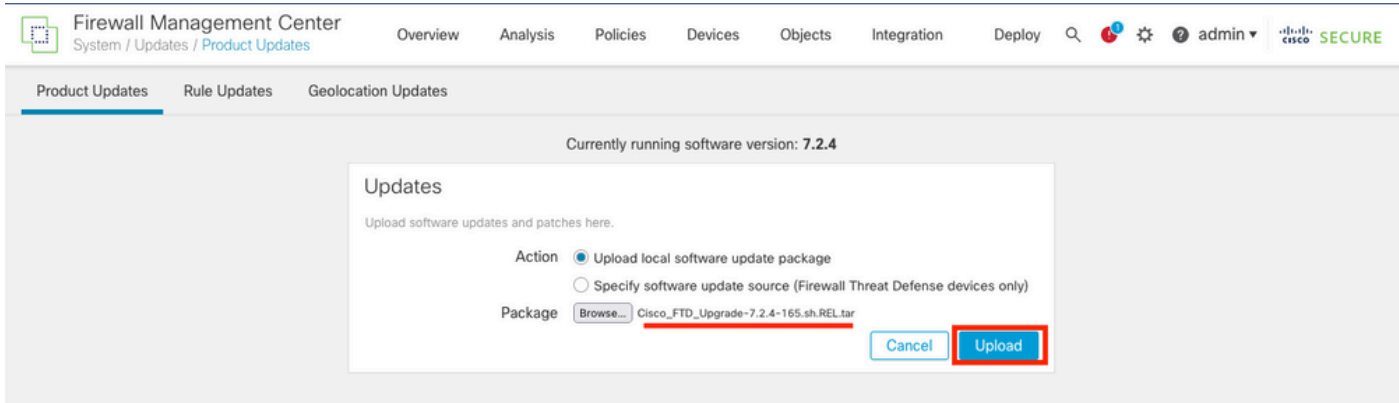
Aviso: verifique se a versão do FMC é superior ou igual à nova versão do FTD a ser atualizada.



- Selecione Upload Update.



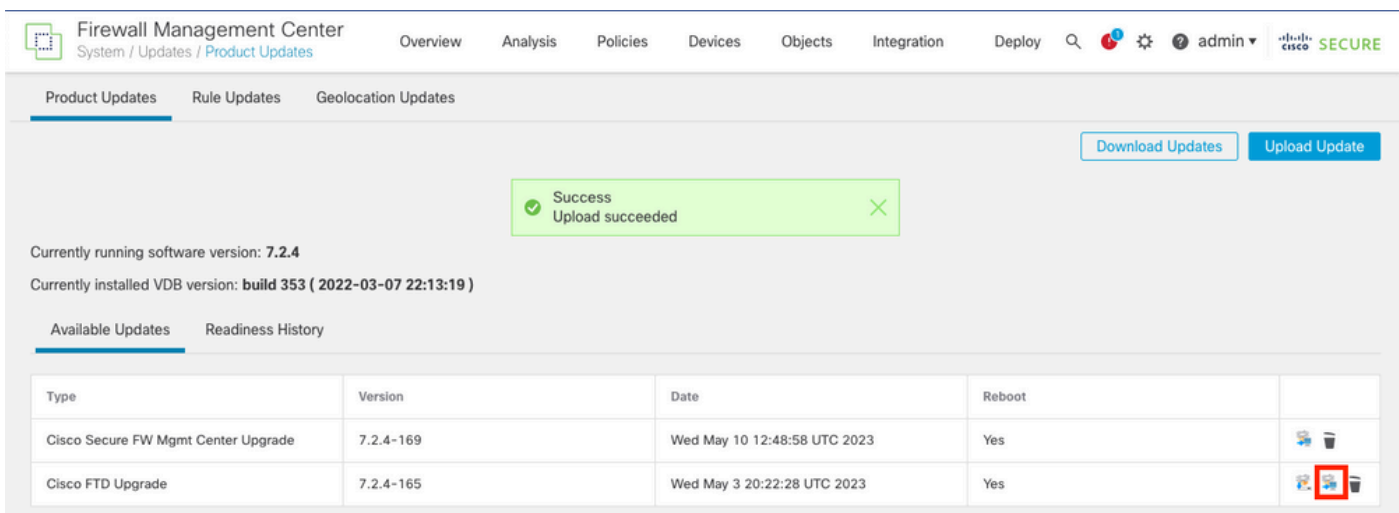
- Procure a imagem baixada anteriormente e selecione Upload.



Etapa 2. Verificar Preparação

As verificações de prontidão confirmam se os dispositivos estão prontos para continuar com a atualização.

- Selecione a opção Install no pacote de atualização correto.



Selecione a atualização de sua preferência. Nesse caso, a seleção é para:

- Cancelar automaticamente em caso de falha na atualização e reverter para a versão anterior.
- Habilitar reversão após atualização bem-sucedida.
- Atualize Snort 2 para Snort 3.
- Selecione o grupo HA de FTDs e clique em Verificar preparação.

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.2.4

Selected Update

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

Enable revert after successful upgrade

Upgrade Snort 2 to Snort 3

After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom Intrusion or Network Analysis Policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. [Learn more](#)

By Group ▾

<input checked="" type="checkbox"/> Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/> FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with			N/A	10 min	⚠
<input checked="" type="checkbox"/> FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with			N/A	10 min	⚠

O progresso pode ser verificado no centro de mensagens Messages > Tasks.

Policies Devices Objects Integration Deploy 🔍 📢 ⚙️ ? admin ▾ cisco SECURE

Deployments Upgrades 🚨 Health **Tasks** 🏷️ Show Notifications

20+ total 0 waiting 0 running 0 retrying 20+ success 0 failures 🔍 Filter

✔ Remote Readiness Check

Checking Cisco FTD Upgrade 7.2.4-165 on [FTD_HA] 2m 11s ✕

10.4.11.86: Success. OK to upgrade to 7.2.4-165 version.

10.4.11.87: Success. OK to upgrade to 7.2.4-165 version.

Quando a verificação de preparação for concluída no FTD e o resultado for Êxito, a atualização poderá ser feita.

By Group ▾

<input type="checkbox"/> Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input type="checkbox"/> FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	⚠
<input type="checkbox"/> FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	⚠

Etapa 3. Atualizar o FTD em alta disponibilidade

- Selecione o par HA e clique em Instalar.

Firewall Management Center
System / Updates / Upload Update

Overview Analysis Policies Devices Objects Integration Deploy

Product Updates Rule Updates Geolocation Updates

Warnings

- Version 7.2.0 onwards, the Intelligent Application Bypass (IAB) setting is deprecated for ... [See More](#)
- Version 7.2.0 onwards, the port_scan inspector is deprecated for Snort 3 ... [See More](#)

Currently running software version: 7.2.4

Selected Update

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

Enable revert after successful upgrade

Upgrade Snort 2 to Snort 3
After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom Intrusion or Network Analysis Policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. [Learn more](#)

By Group

<input checked="" type="checkbox"/>	Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input checked="" type="checkbox"/>	FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/>	FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	
<input checked="" type="checkbox"/>	FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	

Back Check Readiness **Install**

Aviso para continuar com a atualização, o sistema é reinicializado para concluir a atualização. Selecione OK.

10.88.243.115:43092


Update installation will reboot the system(s). Are you sure you want to continue?

Cancel OK

O progresso pode ser verificado no centro de mensagens Messages > Tasks.

Deployments Upgrades **Health** **Tasks** Show Notifications

20+ total | 0 waiting | 1 running | 0 retrying | 20+ success | 0 failures

 Remote Install

Apply Cisco FTD Upgrade 7.2.4-165 to FTD_HA 8m 57s

FTD_B : Upgrade in progress: (14% done.12 mins to reboot). Updating Operating System...
(300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

firepower: View details.

Se você clicar em firepower: Exibir detalhes, o progresso será mostrado de forma gráfica e os logs de status.log.

Upgrade in Progress



FTD_B

10.4.11.86

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | **Initiated At:** Jul 20, 2023 2:58 PM EDT



14% Completed (12 minutes left)

Upgrade In Progress...

Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

• Upgrade will automatically cancel on failure and roll back to the previous version.

Log Details



```
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/202_disable_syncd.sh... 13 mins
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/400_restrict_rpc.sh... 13 mins
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/500_stop_system.sh... 13 mins
Thu Jul 20 18:57:17 UTC 2023 7% Running script 200_pre/501_recovery.sh... 13 mins rema
Thu Jul 20 18:57:18 UTC 2023 14% Running script 200_pre/505_revert_prep.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 200_pre/999_enable_sync.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 300_os/001_verify_bundle.sh... 12 mins
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/002_set_auto_neg.pl... 12 mins
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/060_fix_fstab.sh... 12 mins re
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/100_install_Fire_Linux_OS_aqui
```

Cancel Upgrade

Close

Observação: a atualização leva cerca de 20 minutos por FTD.

Na CLI, o progresso pode ser verificado na pasta de atualização /ngfw/var/log/sf; mova para o modo especialista e digite root access.

```
> 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-7.2.4

root@firepower:/ngfw/var/log/sf# cd Cisco_FTD_Upgrade-7.2.4

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# ls
000_start AQ_UUID DBCheck.log finished_kickstart.flag flags.conf main_upgrade_script.log status.log

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# tail -f status.log
```

```
state:running
ui:Upgrade has begun.
ui: Upgrade in progress: ( 0% done.14 mins to reboot). Checking device readiness... (000_start/000_00_r
...
ui: Upgrade in progress: (64% done. 5 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 (Thu Jul 20 19:05:20 2023):

System will reboot in 5 seconds due to system upgrade.

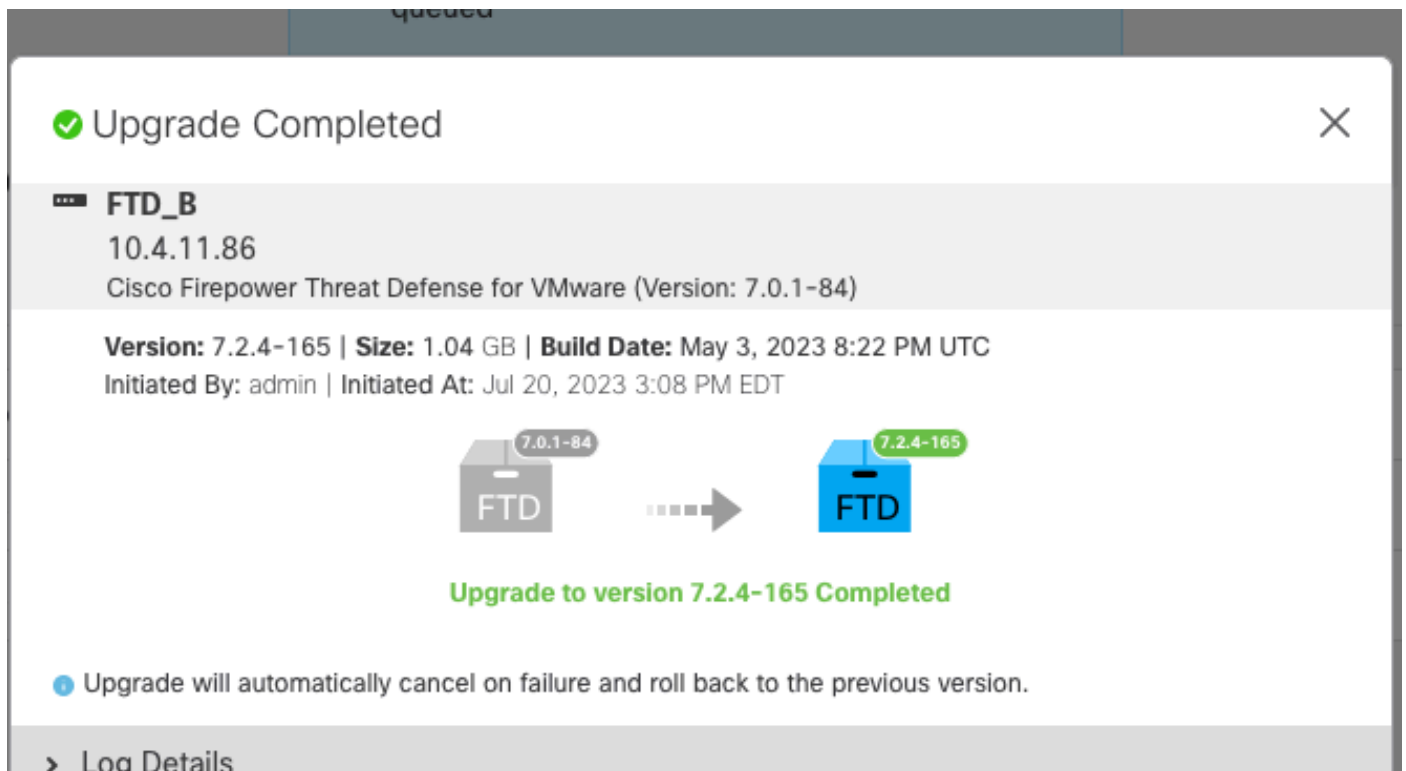
Broadcast message from root@firepower (Thu Jul 20 19:05:25 2023):

System will reboot now due to system upgrade.

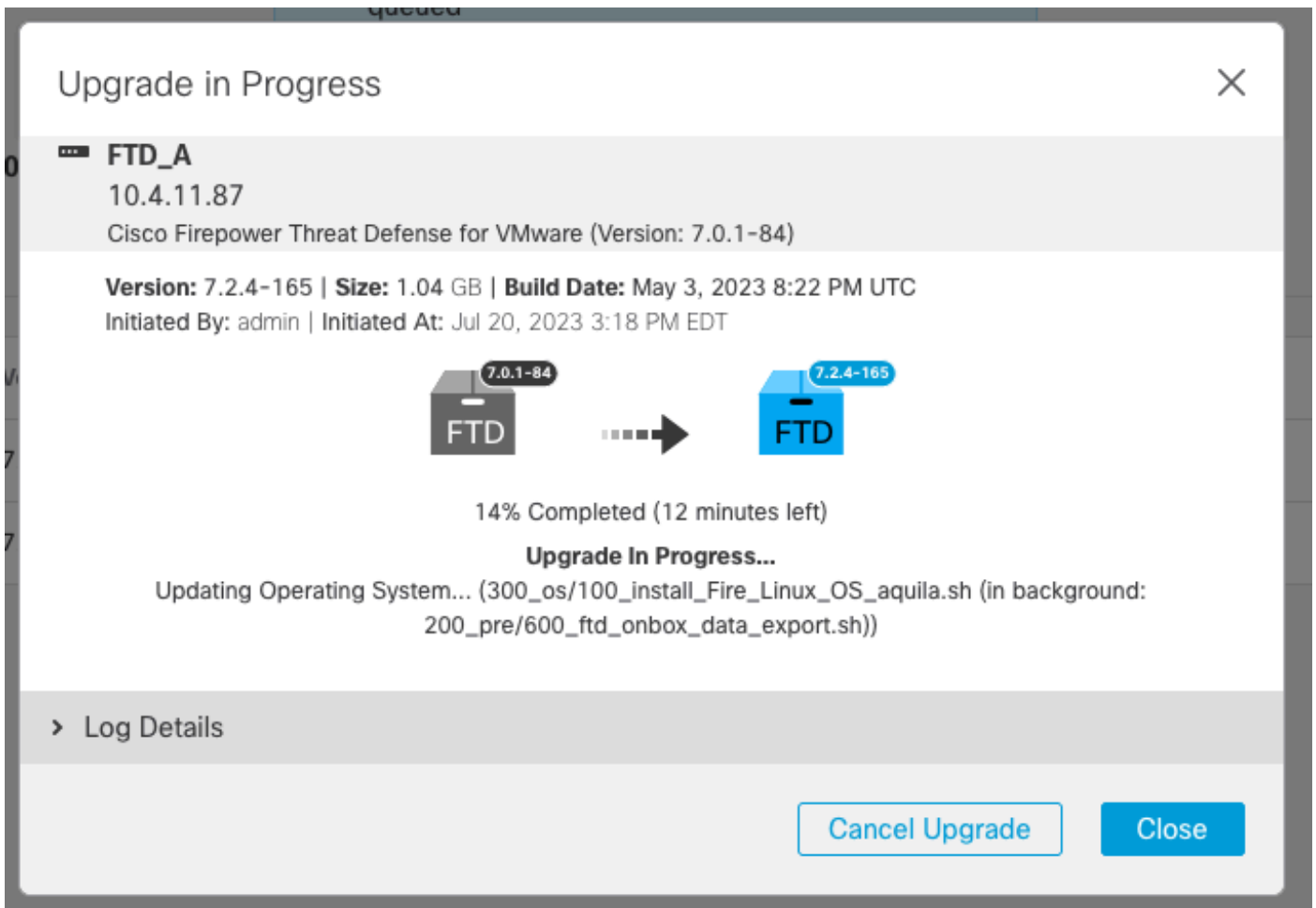
Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

The system is going down for reboot NOW!

O status da atualização é marcado como concluído na GUI e mostra as próximas etapas.



Após a conclusão do upgrade no dispositivo em standby, ele é iniciado no dispositivo ativo.



Na CLI, vá para LINA (system support diagnostic-cli) e verifique o estado de failover no FTD de standby usando o comando show failover state.

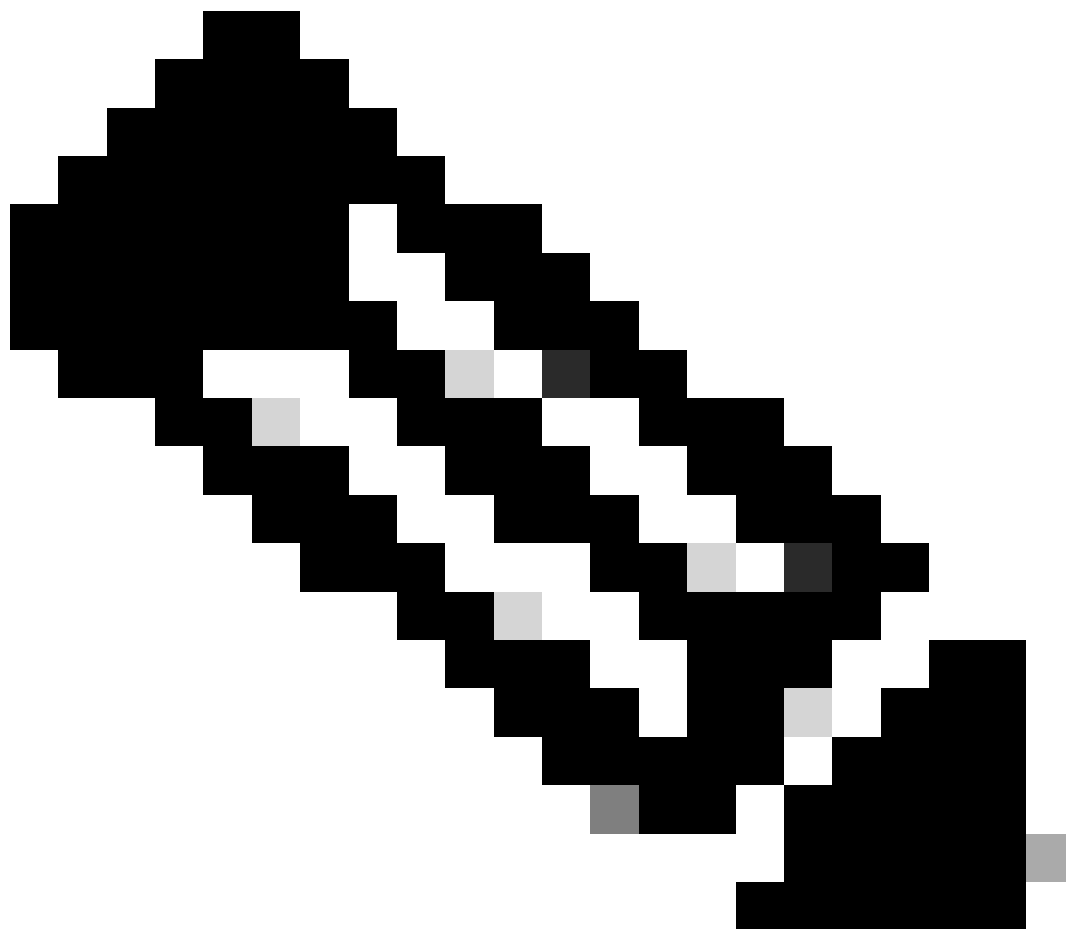
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password:
firepower# show failover state

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

====Configuration State====
Sync Done - STANDBY
====Communication State====
Mac set

firepower#
Switching to Active
```



Observação: o failover ocorre automaticamente como parte do upgrade. Antes que o FTD ativo seja reinicializado e conclua a atualização.

Quando o upgrade for concluído, será necessário reinicializar:

✔ Upgrade Completed



FTD_A

10.4.11.87

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | **Initiated At:** Jul 20, 2023 3:28 PM EDT



Upgrade to version 7.2.4-165 Completed

> Log Details

Close

Etapa 4. Switch Ativo Peer (Opcional)



Observação: se o dispositivo secundário estiver ativo, ele não terá nenhum impacto operacional.

Ter o dispositivo primário como ativo e secundário como em espera é uma prática recomendada que ajuda a rastrear qualquer failover que possa ocorrer.

Nesse caso, o FTD Ativo agora está em Espera, um failover manual pode ser usado para redefini-lo como Ativo.

- Navegue até os três pontos ao lado do sinal de edição.

View By: Deployment History
 All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) 🔍 Search Device Add

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
●	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮
●	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮

- Seleccione Switch Ative Peer.

View By: Deployment History
 All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) 🔍 Search Device Add

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
●	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	<div style="border: 1px solid gray; padding: 5px; width: fit-content;"> Switch Active Peer Break Force refresh node status Delete Revert Upgrade Health Monitor Troubleshoot Files </div>
●	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	

- Seleccione YES para confirmar o failover.

Switch Active Peer

Are you sure you want to make "FTD_A" the active peer?

No

Yes

Validação do status de Alta Disponibilidade no final da atualização e failover concluída.
Dispositivos > Gerenciamento de dispositivos

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (1) Upgrade (2) Snort 3 (2)

Deployment History

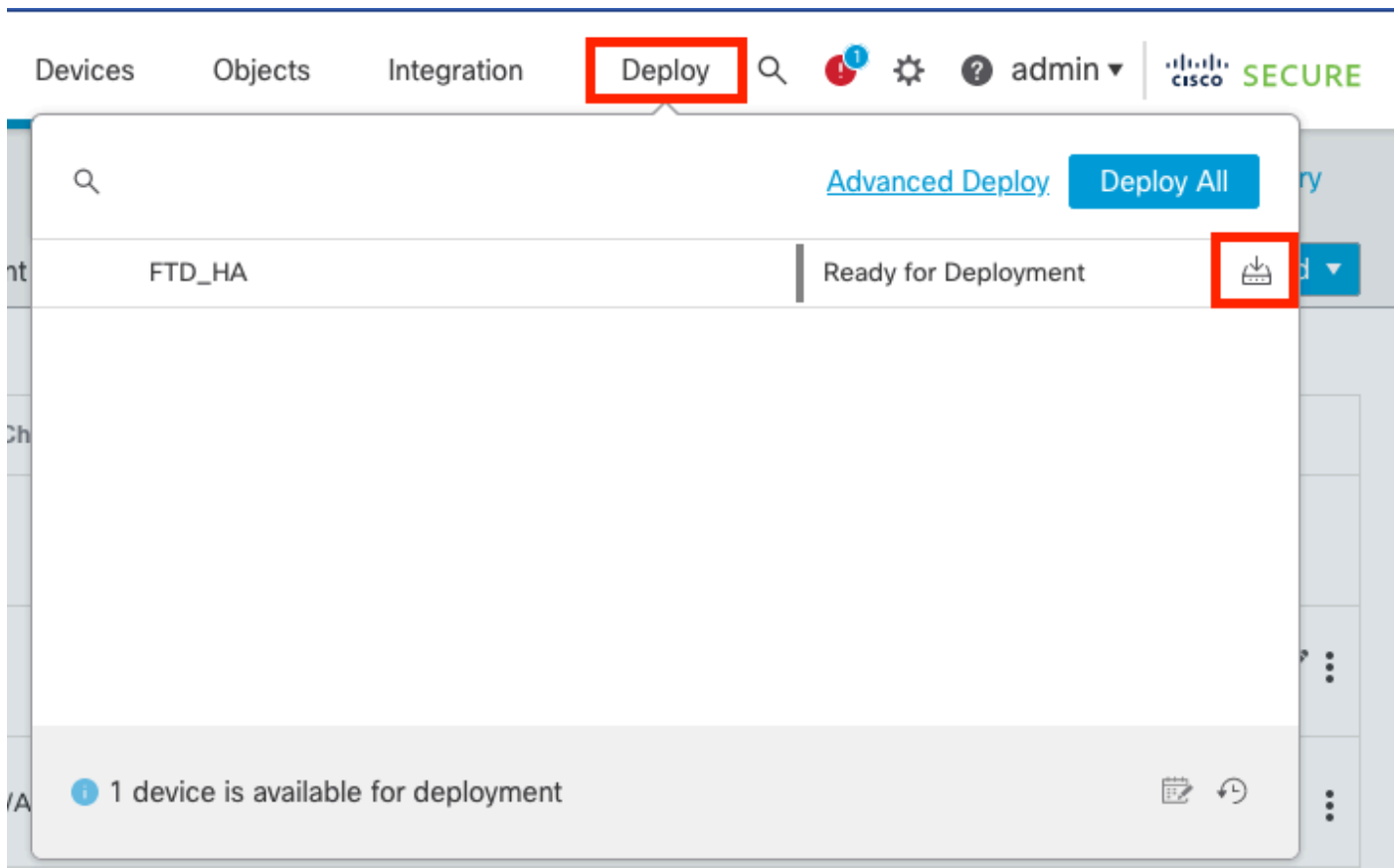
Search Device Add

Collapse All

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
<input checked="" type="checkbox"/>	FTD_A(Primary, Active) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺	⋮
<input checked="" type="checkbox"/>	FTD_B(Secondary, Standby) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺	⋮

Etapa 5. Implantação final

- Implante uma política nos dispositivos Implantar > Implantar neste dispositivo.



Validar

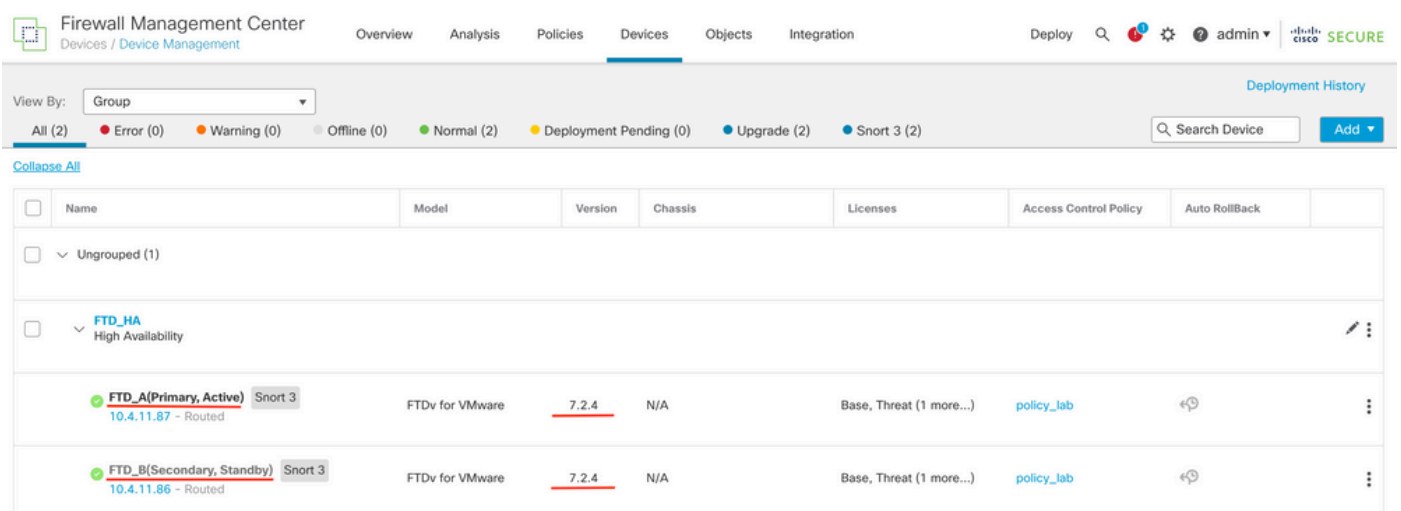
Para validar se o status de alta disponibilidade e a atualização foram concluídos, é necessário confirmar o status:

Primário: Ativo

Secundário: pronto para espera

Ambos estão na versão que foi alterada recentemente (7.2.4 neste exemplo).

- Na GUI do FMC, navegue até Devices > Device Management.



- Em cliques de CLI, verifique o estado de failover usando os comandos `show failover state` e

show failover para obter informações mais detalhadas.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)
Cisco Firepower Threat Defense for VMware v7.2.4 (build 165)

> show failover state

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

====Configuration State====

====Communication State====

Mac set

> show failover

Failover On

Failover unit Primary

Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/0 (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 1285 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(3)39, Mate 9.18(3)39

Serial Number: Ours 9AVLW3FSSK8, Mate 9AJJSEGJS2T

Last Failover at: 19:56:41 UTC Jul 20 2023

This host: Primary - Active

Active time: 181629 (sec)

slot 0: ASAv hw/sw rev (/9.18(3)39) status (Up Sys)

Interface INSIDE (10.10.153.1): Normal (Monitored)

Interface OUTSIDE (10.20.153.1): 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: 2390 (sec)

Interface INSIDE (10.10.153.2): Normal (Monitored)

Interface OUTSIDE (10.20.153.2): 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 : FAILOVER_LINK GigabitEthernet0/0 (up)

Stateful Obj	xmit	xerr	rcv	rerr
--------------	------	------	-----	------

General	29336	0	24445	0
---------	-------	---	-------	---

sys cmd	24418	0	24393	0
---------	-------	---	-------	---

...

Logical Update Queue Information

	Cur	Max	Total
--	-----	-----	-------

Recv Q:	0	11	25331
---------	---	----	-------

Xmit Q:	0	1	127887
---------	---	---	--------

Se ambos os FTDs estiverem na mesma versão e o status de alta disponibilidade estiver íntegro, a atualização estará concluída.

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.