升级FTD HA，由FMC管理

目录

简介

本文档介绍由防火墙管理中心管理的具有高可用性的思科安全防火墙威胁防御的升级过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 高可用性(HA)概念和配置
- 安全防火墙管理中心(FMC)配置
- 思科安全防火墙威胁防御(FTD)配置

使用的组件

本文档中的信息基于：

- 虚拟防火墙管理中心(FMC)，版本7.2.4
- 虚拟思科防火墙威胁防御(FTD)，版本7.0.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

FMC的工作方式是一次升级一个对等体。首先选择Standby（备用），然后选择Active（活动），在完成Active（活动）升级之前执行故障切换。

背景信息

升级前必须从software.cisco.com下载升级软件包。

在CLI完成后，在活动FTD中运行show high-availability config命令，检查高可用性状态。

```
> 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
```

如果未显示错误，则继续升级。

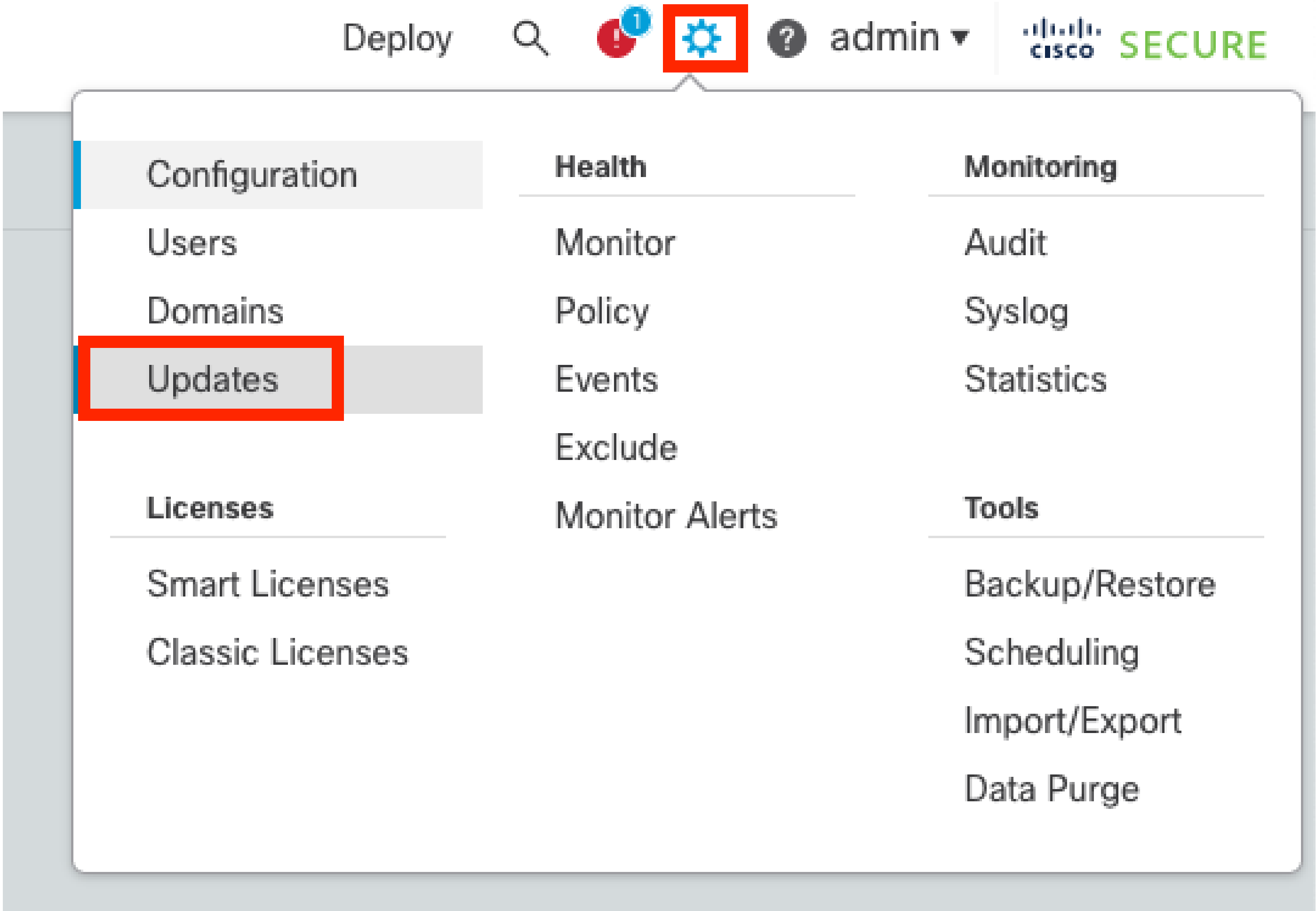
配置

步骤1:上传升级包

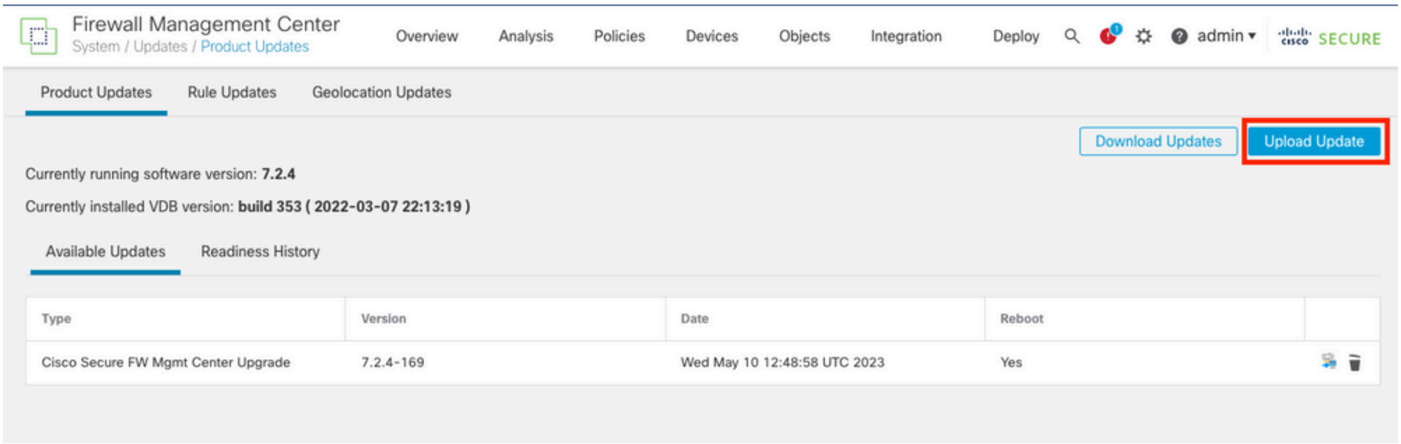
- 使用图形用户界面(GUI)将FTD升级软件包上传到FMC。
  之前必须根据FTD型号和所需版本从思科软件站点下载该软件。

警告：确保FMC版本高于或等于要升级的新FTD版本。

System > Updates



- 选择Upload Update。

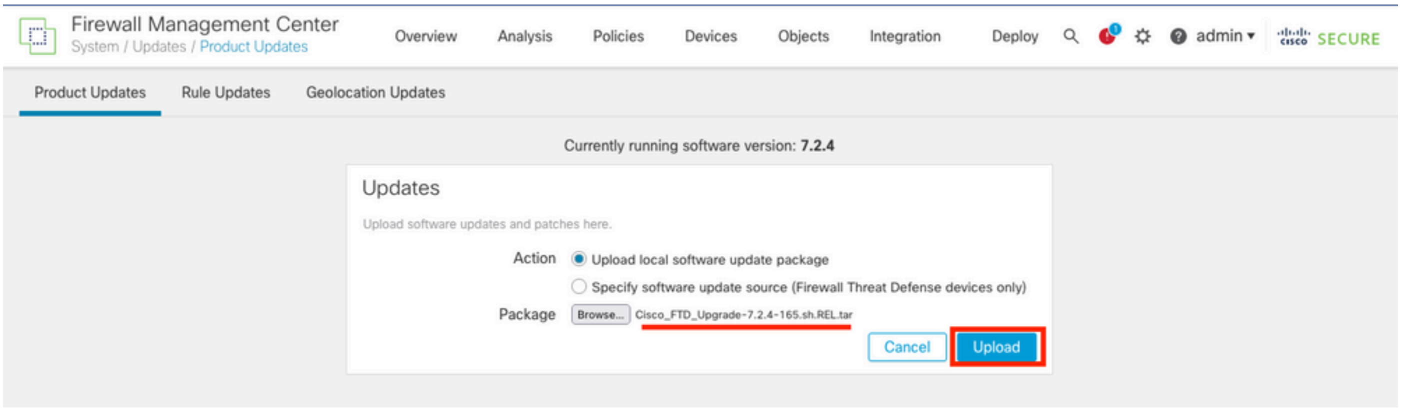


Currently running software version: **7.2.4**

Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

Type	Version	Date	Reboot	
Cisco Secure FW Mgmt Center Upgrade	7.2.4-169	Wed May 10 12:48:58 UTC 2023	Yes	

- 浏览先前下载的镜像，然后选择上传。


Firewall Management Center
System / Updates / Product Updates
Overview Analysis Policies Devices Objects Integration Deploy admin SECURE
Product Updates Rule Updates Geolocation Updates

Currently running software version: **7.2.4**

Updates

Upload software updates and patches here.

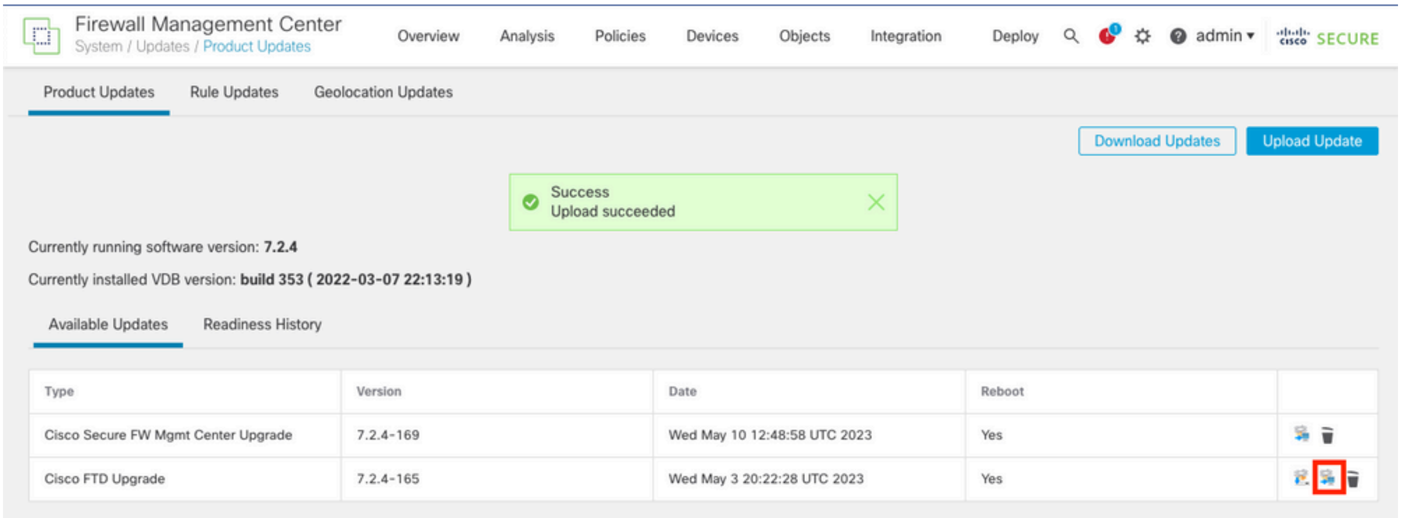
Action ● Upload local software update package
○ Specify software update source (Firewall Threat Defense devices only)

Package Browse... Cisco_FTD_Upgrade-7.2.4-165.sh.REL.tar

第二步：检查就绪性

就绪性检查确认设备是否已准备好继续升级。

- 在正确的升级软件包中选择安装选项。


Firewall Management Center
System / Updates / Product Updates
Overview Analysis Policies Devices Objects Integration Deploy admin SECURE
Product Updates Rule Updates Geolocation Updates
Download Updates
Upload Update

Success
Upload succeeded

Currently running software version: **7.2.4**

Currently installed VDB version: **build 353 (2022-03-07 22:13:19)**

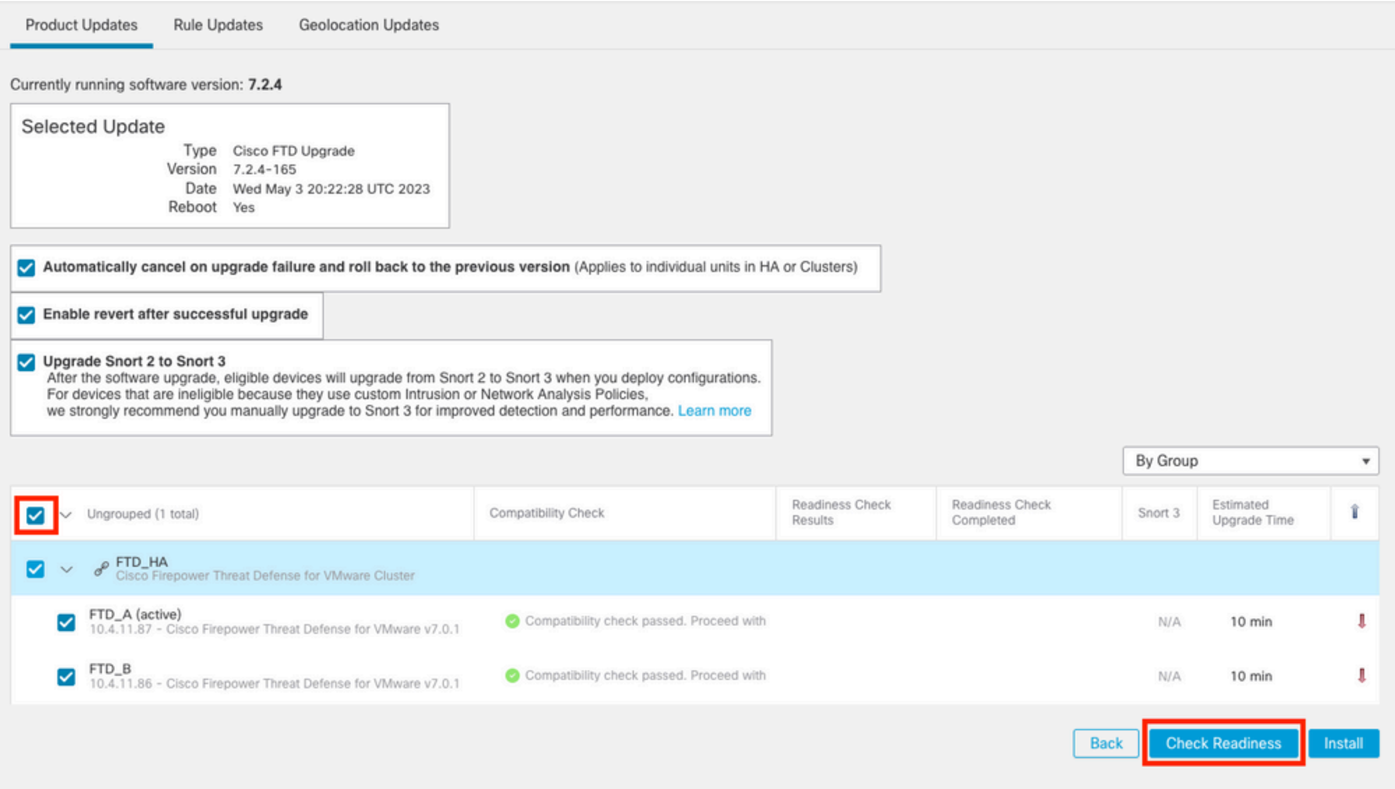
Available Updates
Readiness History

Type	Version	Date	Reboot
Cisco Secure FW Mgmt Center Upgrade	7.2.4-169	Wed May 10 12:48:58 UTC 2023	Yes
Cisco FTD Upgrade	7.2.4-165	Wed May 3 20:22:28 UTC 2023	Yes

选择您喜欢的升级。在本例中，选择用于：

- 升级失败时自动取消并回滚到以前的版本。
- 在成功升级后启用恢复。
- 将Snort 2升级到Snort 3。

- 选择FTD的HA组并单击Check Readiness。



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)

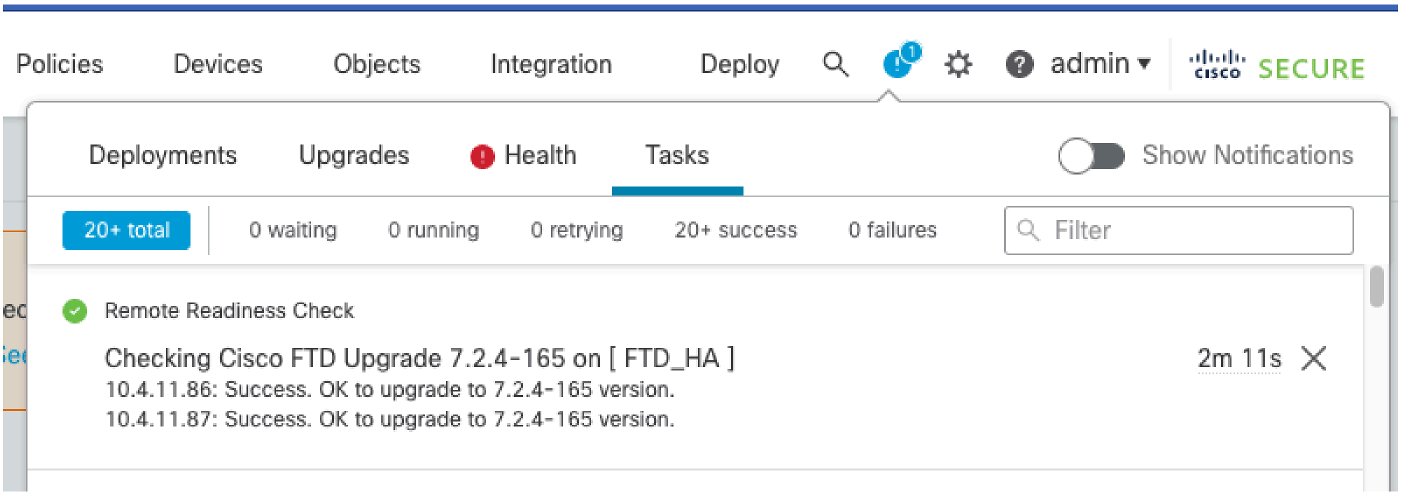
☑ **Enable revert after successful upgrade**

☑ **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

☑ 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					
☑ 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
☑ FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with			N/A	10 min

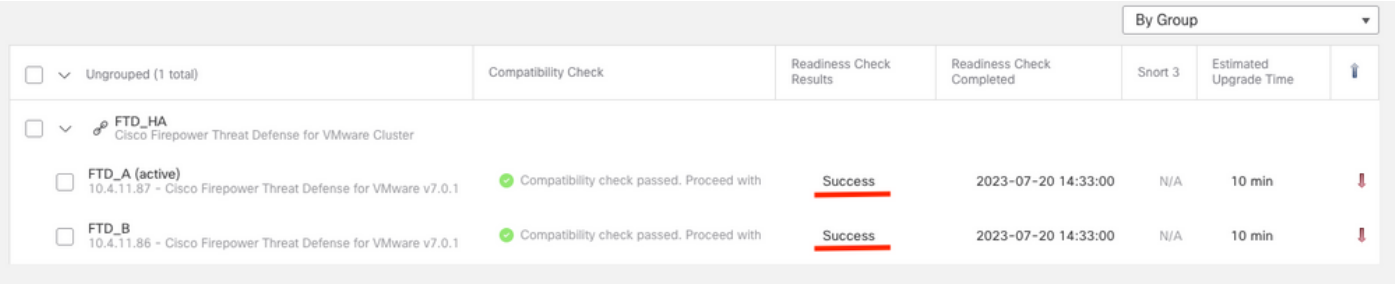
可以在消息中心Messages > Tasks中检查进度。



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.

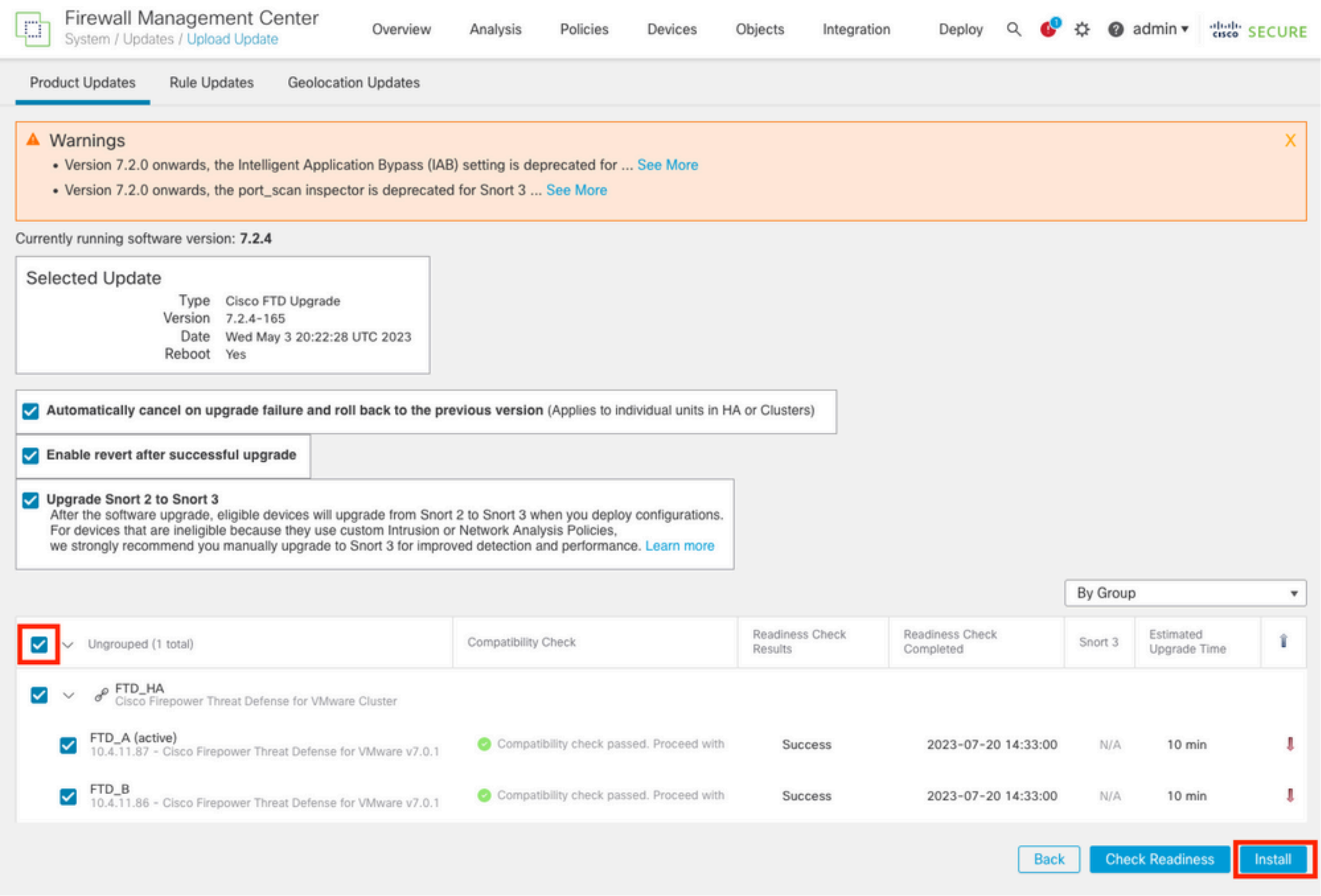
当FTD中的就绪性检查完成且结果为成功时，可以完成升级。


By Group

□ 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					
□ 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
□ 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

第三步：在高可用性中升级FTD

- 选择HA对，然后单击安装。



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)

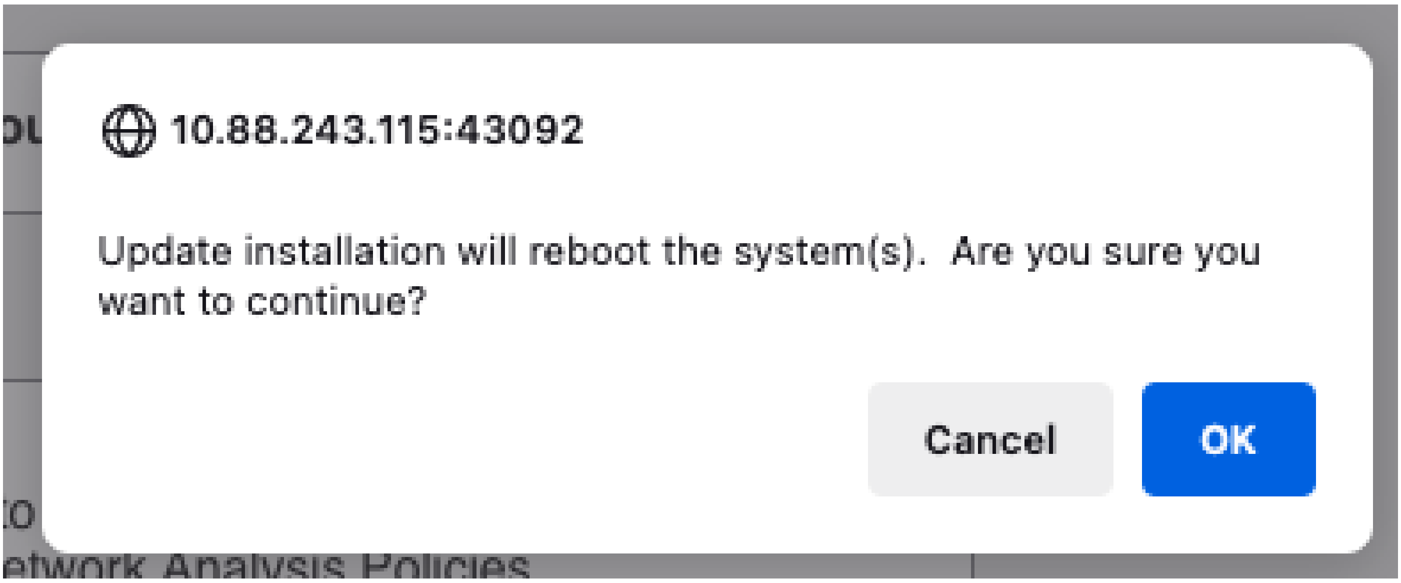
☑ **Enable revert after successful upgrade**

☑ **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

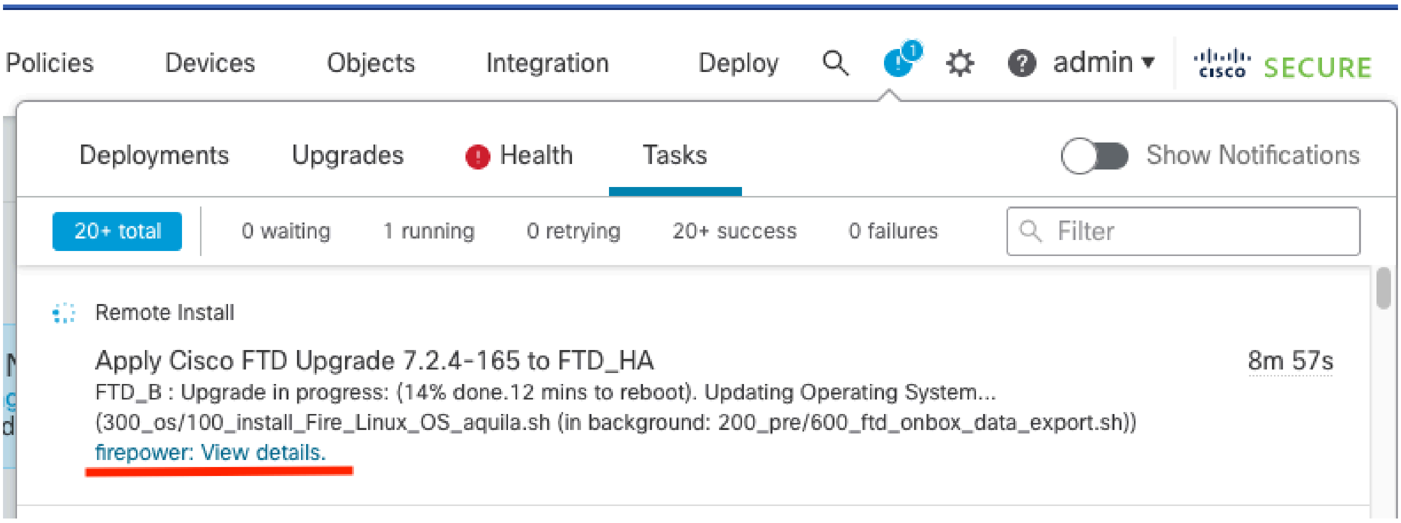
☑ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time
☑ FTD_HA Cisco Firepower Threat Defense for VMware Cluster					
☑ FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed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

警告：要继续升级，系统会重新启动以完成升级。选择“确定”。


10.88.243.115:43092

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

可以在消息中心Messages > Tasks中检查进度。

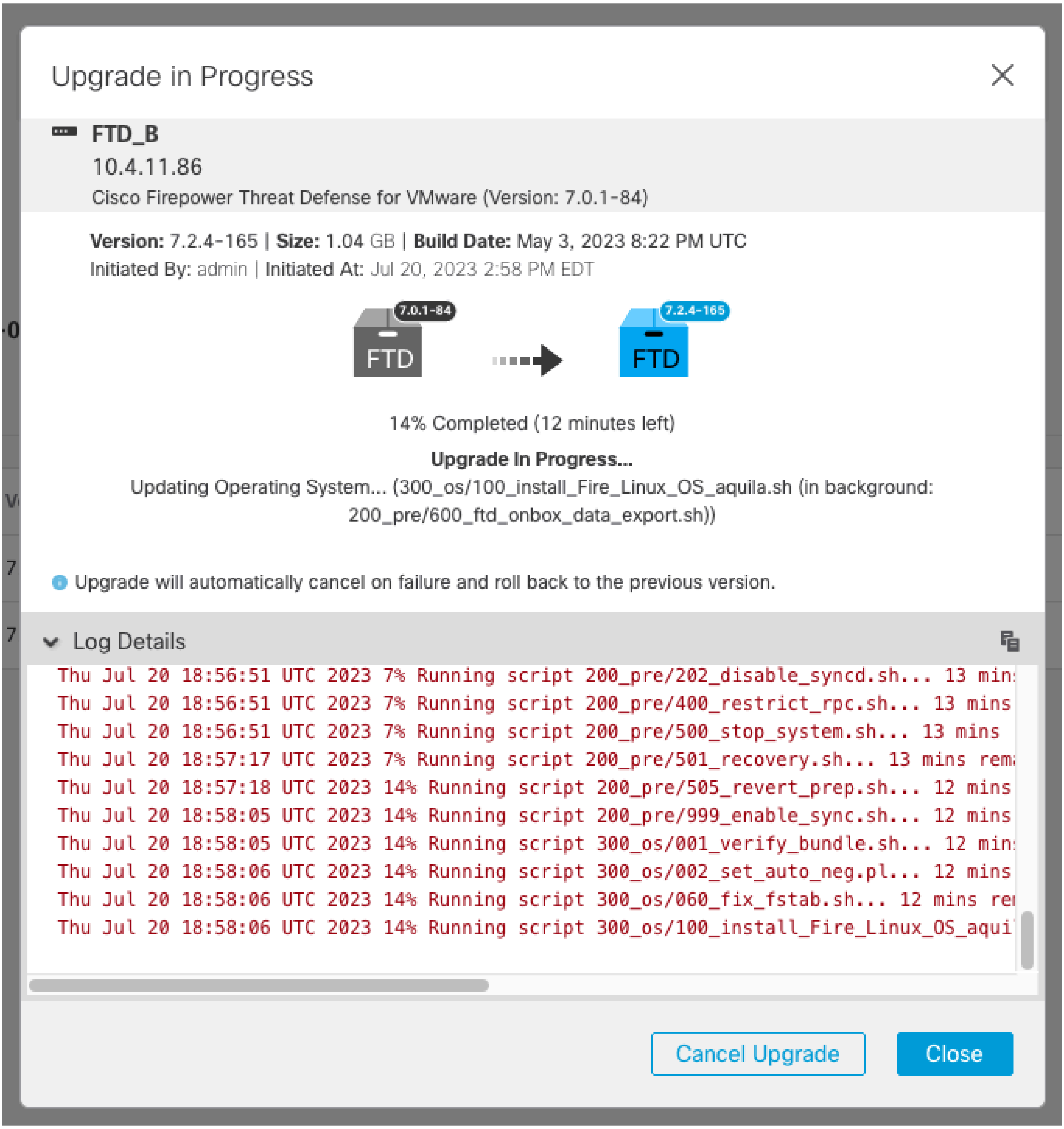


Remote Install

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.

如果单击firepower：查看详细信息，则会以图形方式显示进度以及status.log的日志。



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 min
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 min
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
```

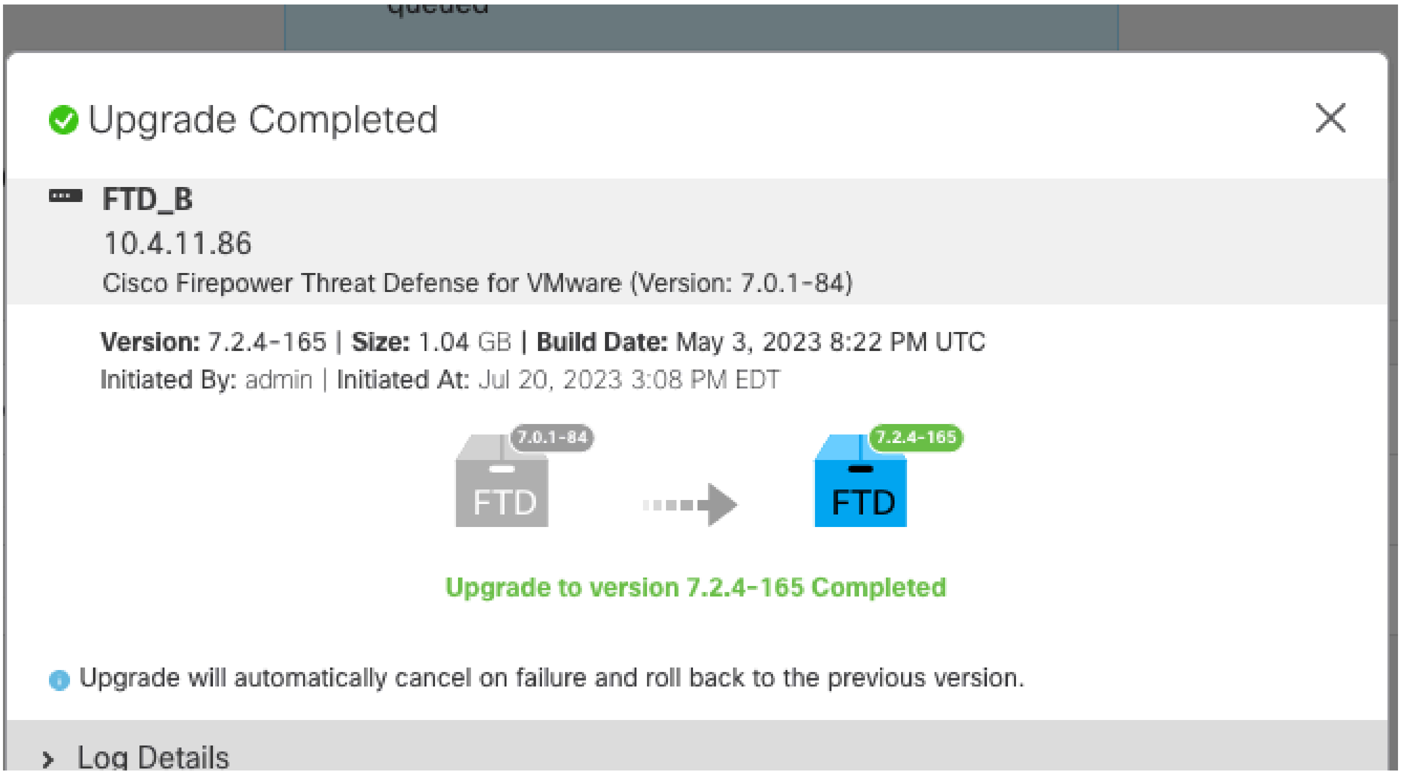
注意：每FTD升级大约需要20分钟。

在CLI中，可以在升级文件夹/ngfw/var/log/sf中检查进度；转到expert模式并输入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.l

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!
```

升级状态在GUI上标记为已完成，并显示后续步骤。



Upgrade Completed

FTD_B

10.4.11.86

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

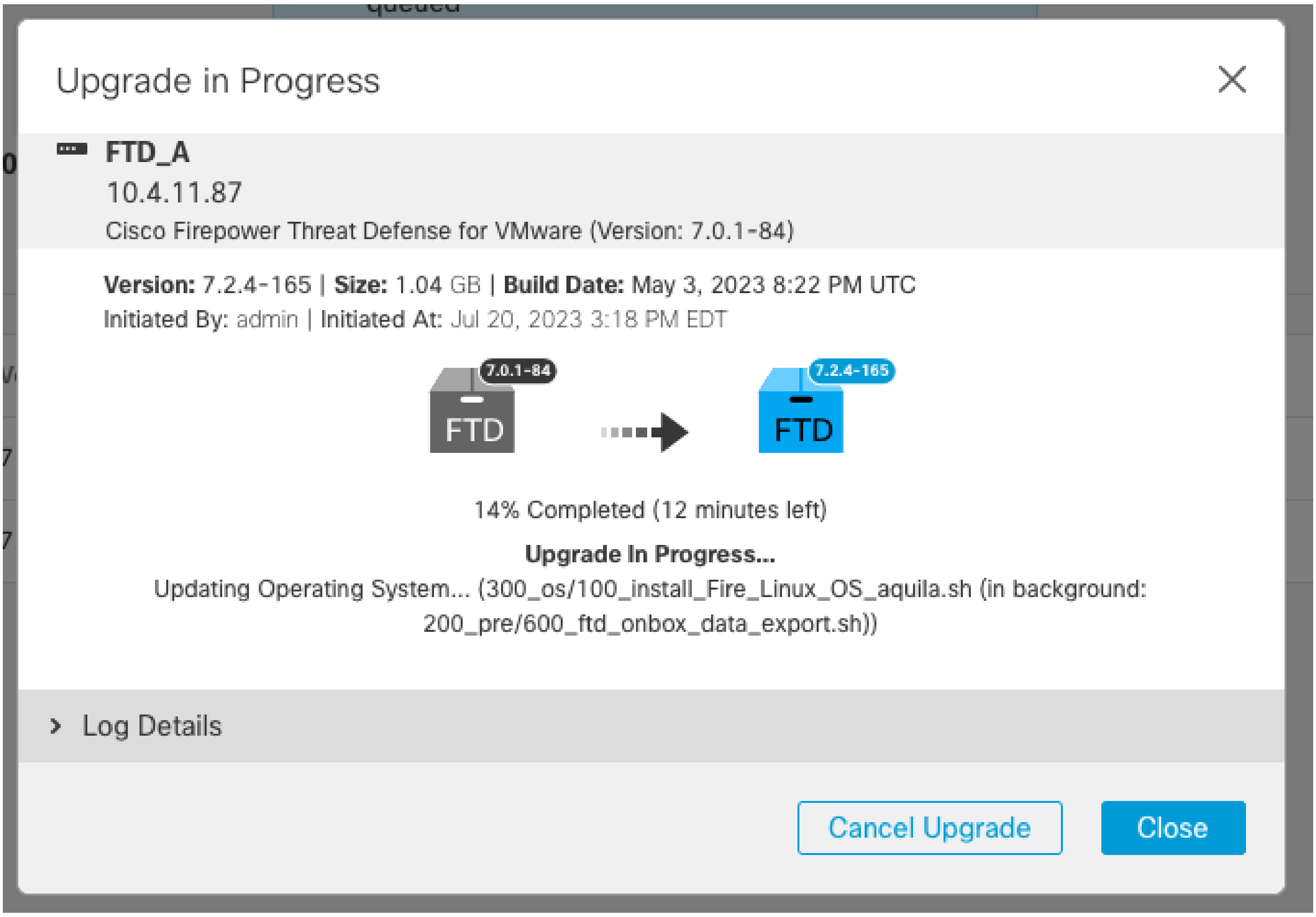
Version: 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

Initiated By: admin | Initiated At: Jul 20, 2023 3:08 PM EDT

Upgrade to version 7.2.4-165 Completed

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

在备用设备中完成升级后，它将在主用设备中启动。



Upgrade in Progress

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 3:18 PM EDT

14% Completed (12 minutes left)

Upgrade In Progress...

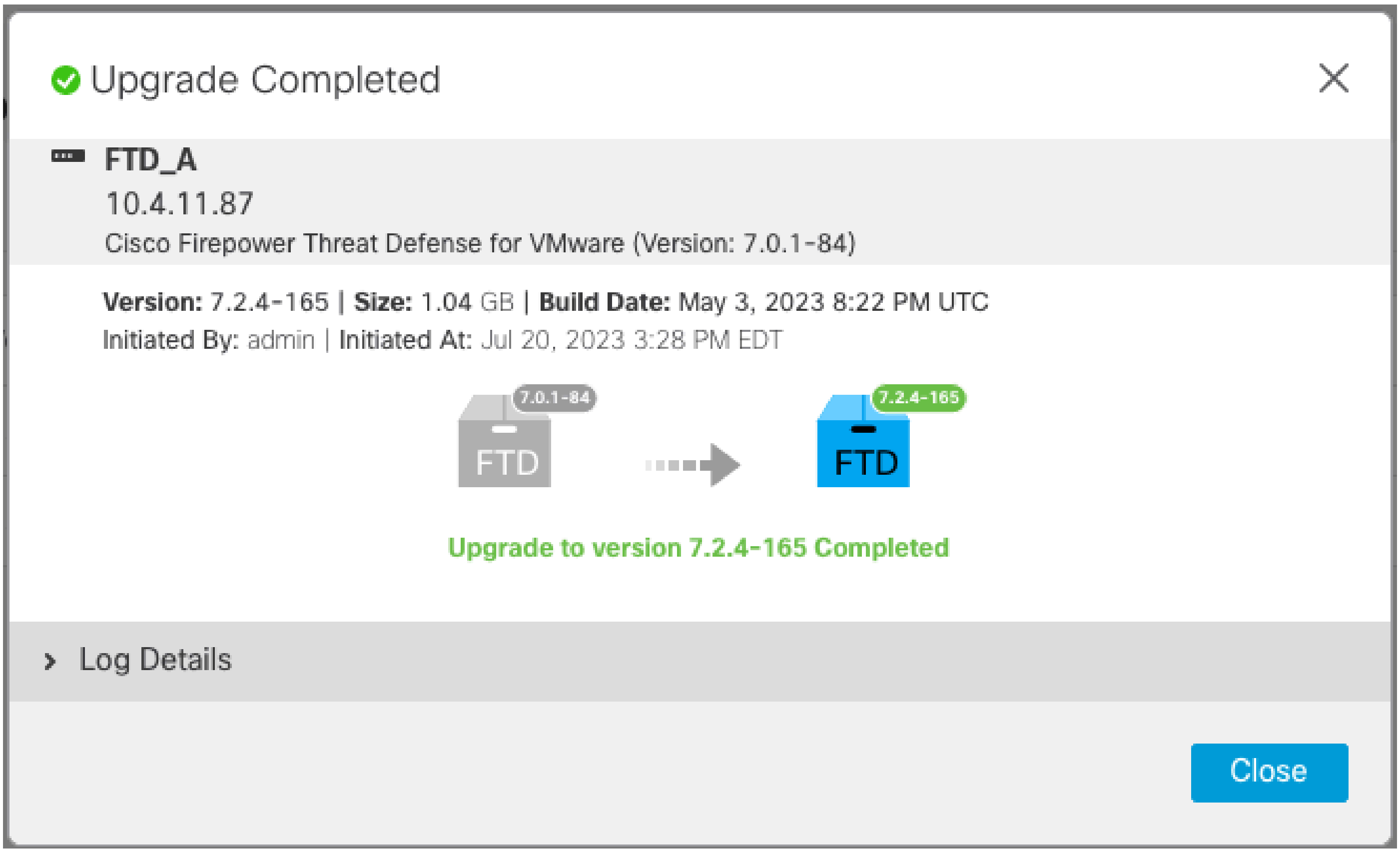
Updating Operating System... (300_os/100_install_Fire_Linux_OS_aquila.sh (in background: 200_pre/600_ftd_onbox_data_export.sh))

在CLI中，转到LINA (system support diagnostic-cli)并使用命令show failover state检查备用FTD上的故障切换状态。

```
> 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

               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#
        Switching to Active
```

注意：在升级过程中，会自动进行故障切换。在活动FTD重新启动并完成升级之前。

升级完成后，需要重新启动：



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

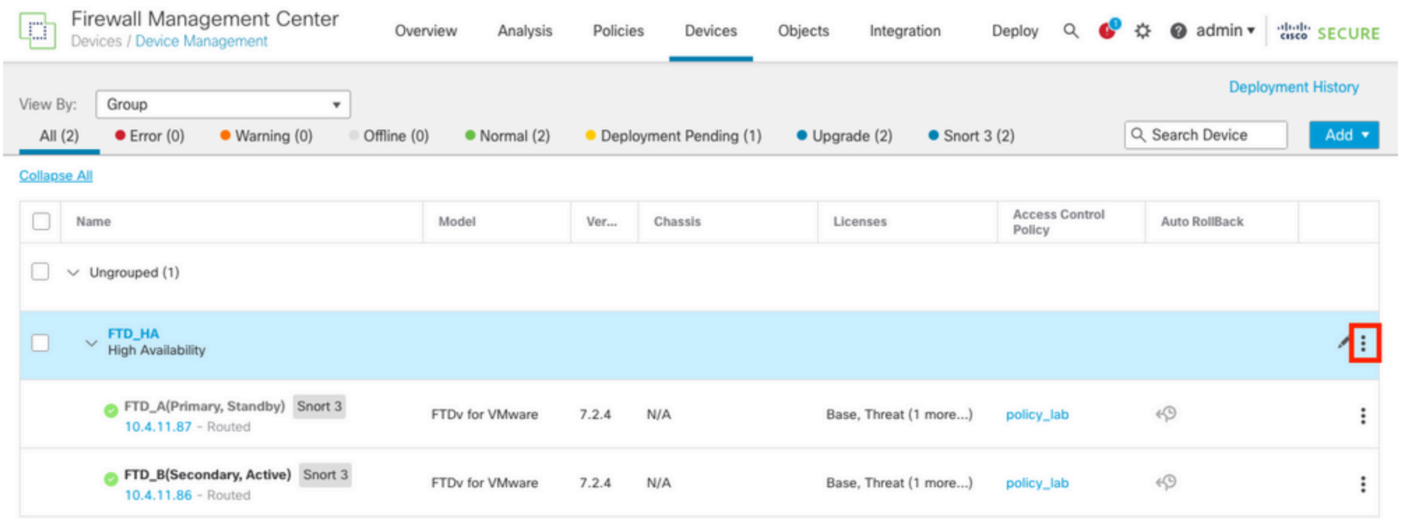
Upgrade to version 7.2.4-165 Completed

第四步：交换活动对等体（可选）

注意：如果辅助设备处于活动状态，则不会对操作产生任何影响。
将主设备设置为主用设备，将辅助设备设置为备用设备，这是帮助跟踪可能发生的任何故障转移的最佳实践。

在这种情况下，FTD主用现在为备用，可以使用手动故障切换将其重新设置为主用。

- 导航到编辑符号旁边的三个点。

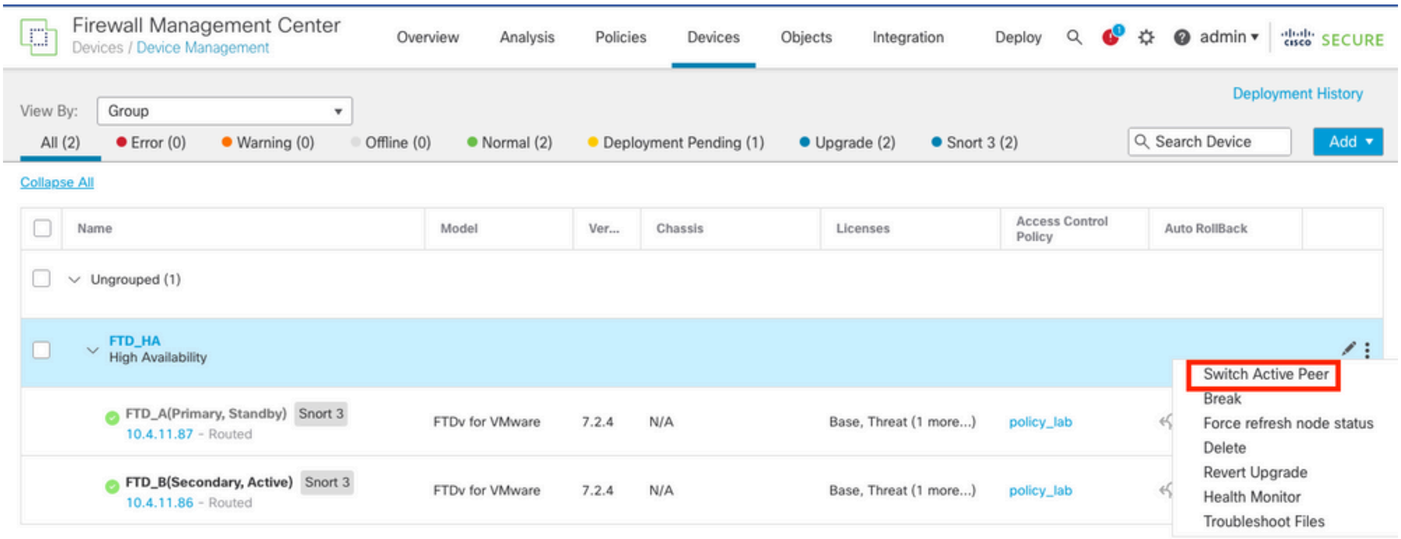


View By: Group

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

	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
□	Ungrouped (1)						
□	FTD_HA High Availability						
	✓ FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
	✓ FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	

- 选择Switch Active Peer。

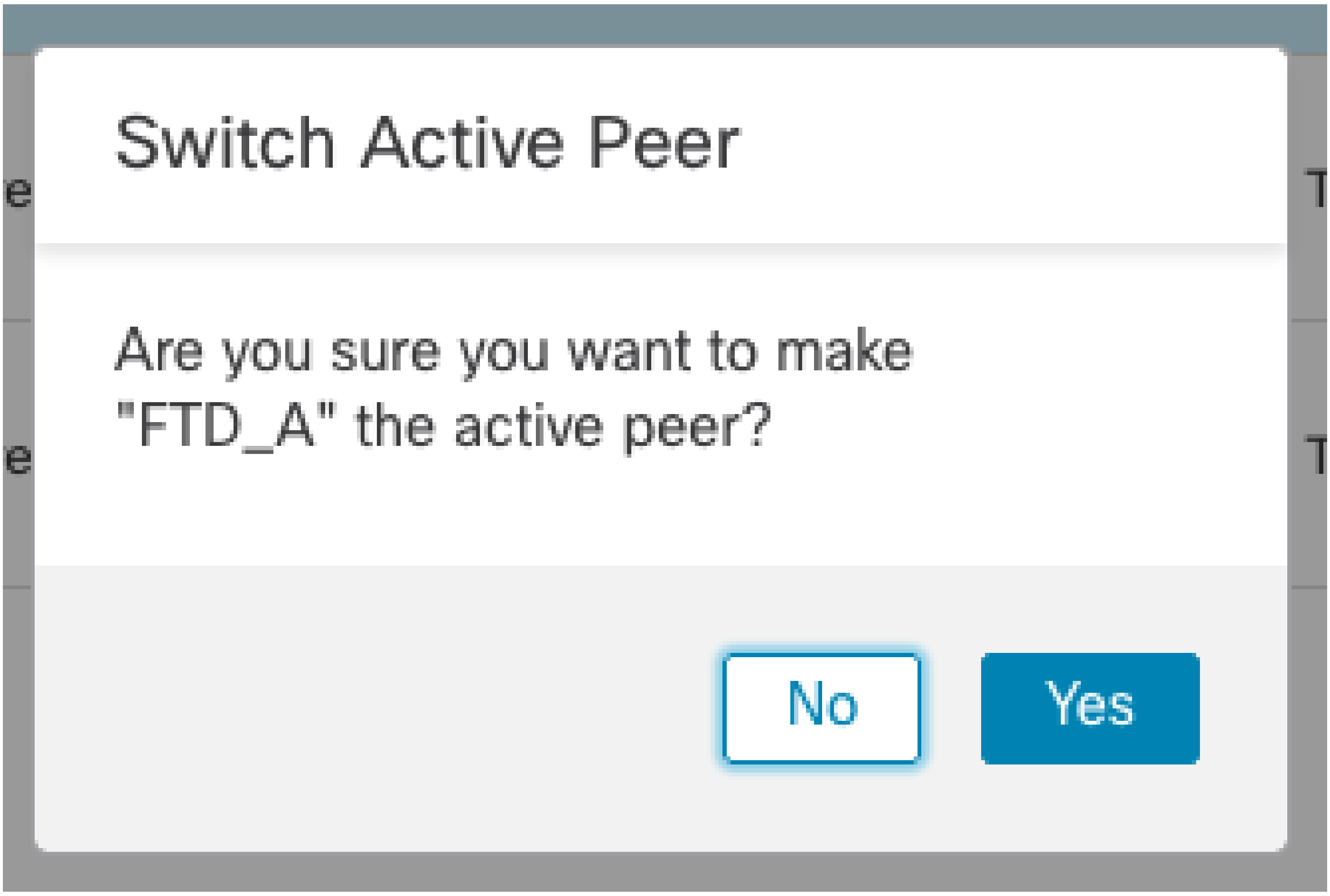


View By: Group

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

	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
□	Ungrouped (1)						
□	FTD_HA High Availability						
	✓ FTD_A(Primary, Standby) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
	✓ FTD_B(Secondary, Active) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	

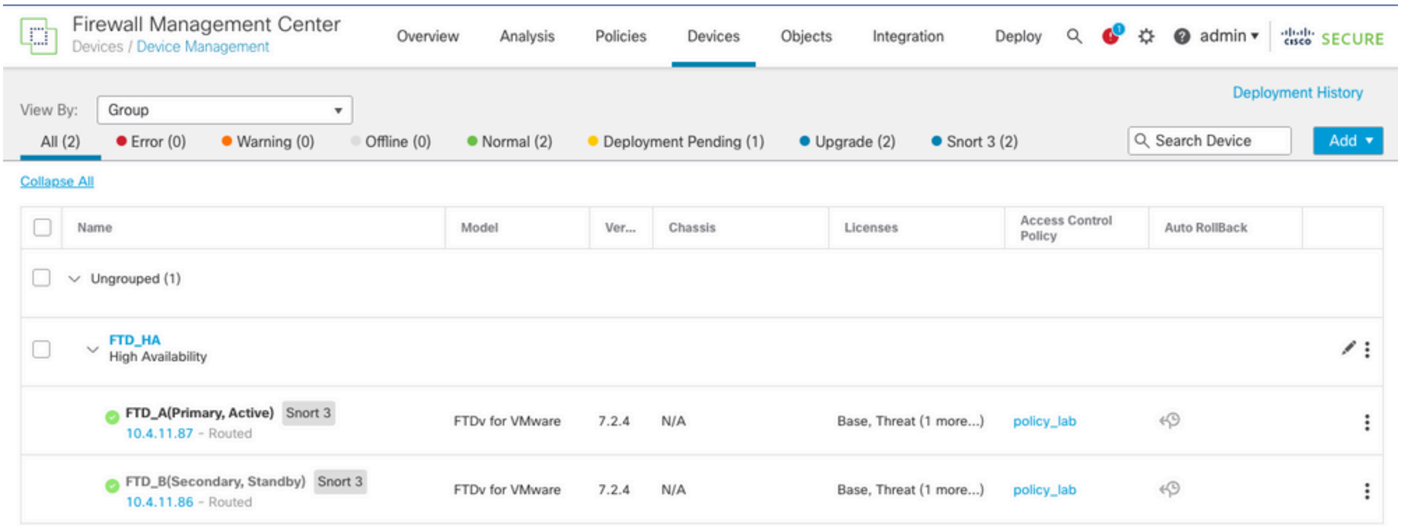
- 选择YES以确认故障切换。



Switch Active Peer

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

在升级结束时验证高可用性状态，完成故障切换。
Devices > Device Management

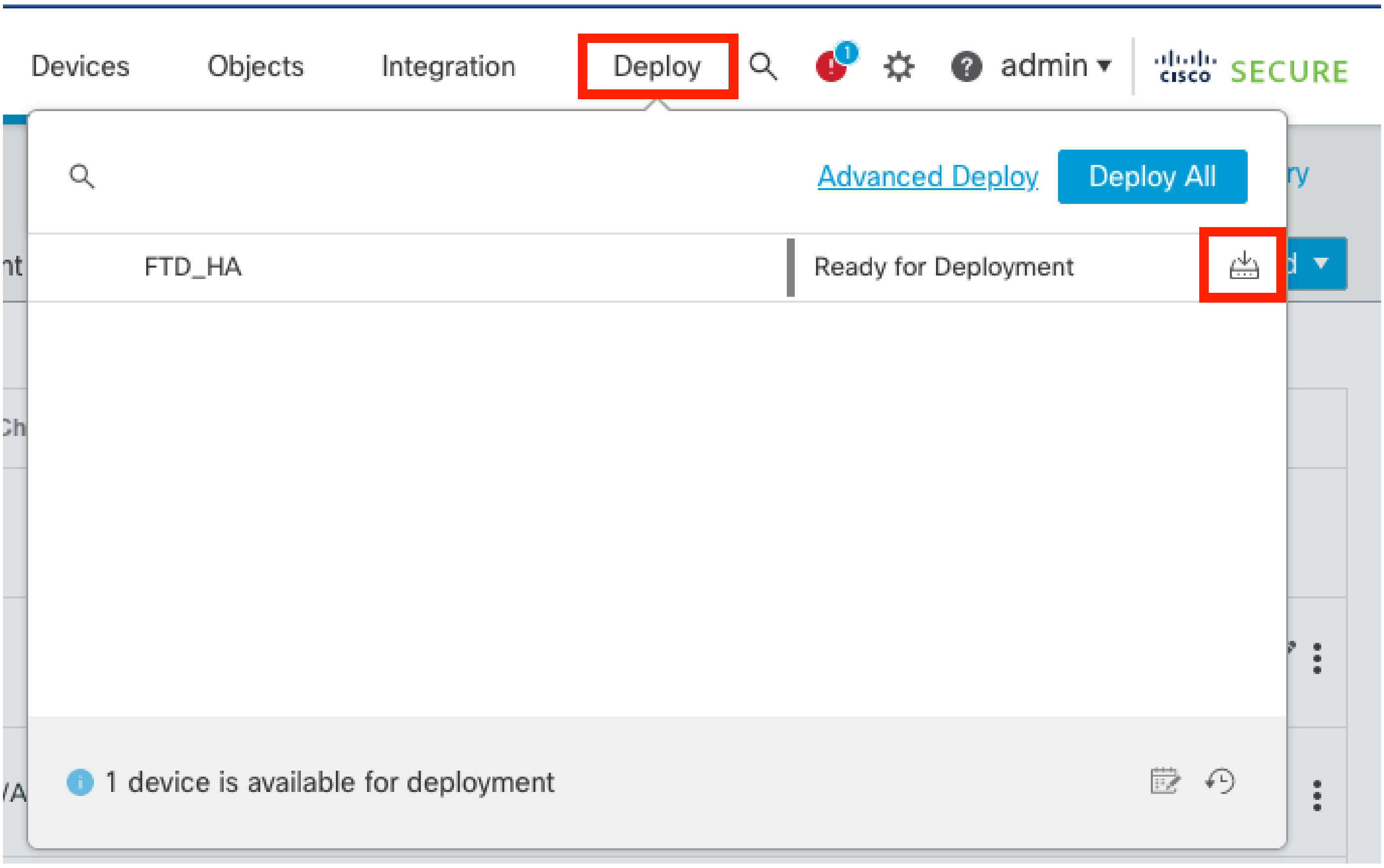


View By: Group

□	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
□	Ungrouped (1)						
□	FTD_HA High Availability						
	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	
	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	

第五步：最终部署

- 将策略部署到设备Deploy > Deploy to this device。



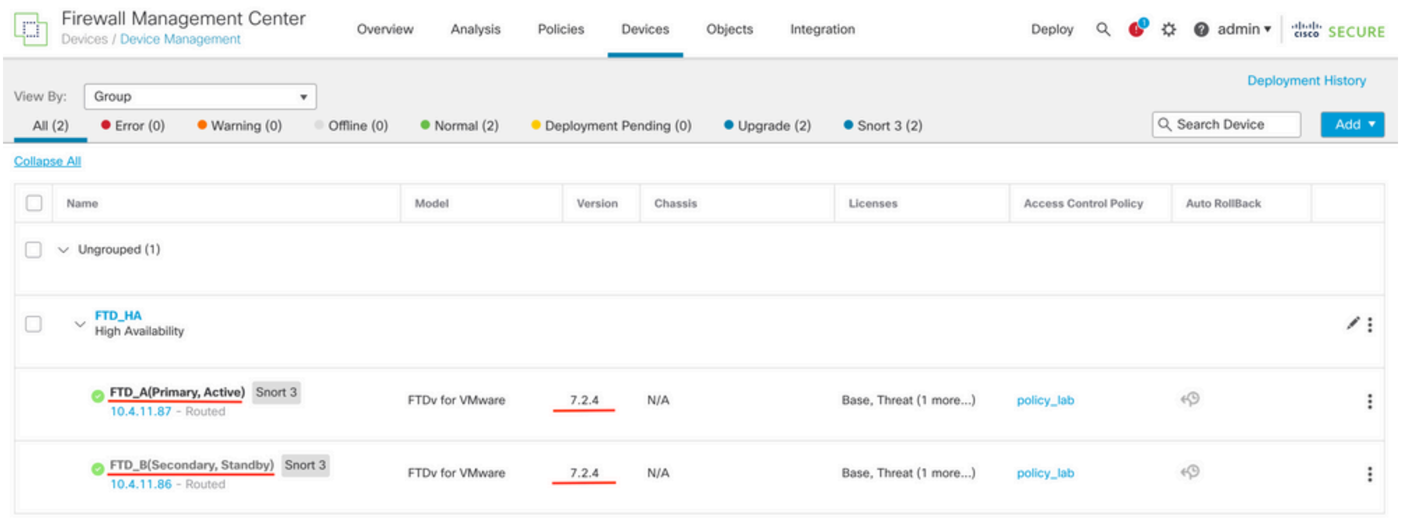
FTD_HA | Ready for Deployment

1 device is available for deployment

验证

要验证高可用性状态并完成升级，您需要确认以下状态：
主要：活动
辅助：备用就绪
这两个版本都是最近更改的版本（本例中为7.2.4）。

- 在FMC GUI中，导航到Devices > Device Management。



View By: Group

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

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
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	
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	

- 有关更多详细信息，请通过CLI单击，使用命令show failover state和show failover检查故障切换状态。

```
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
```

如果两个FTD处于同一版本并且高可用性状态正常，则升级完成。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。