

FTD HA-Upgrade von FMC verwaltet

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Upgrade-Paket hochladen](#)

[Schritt 2: Überprüfungsbereitschaft](#)

[Schritt 3: FTD-Upgrade bei hoher Verfügbarkeit](#)

[Schritt 4: Aktive Peer-Switches \(optional\)](#)

[Schritt 5: Endgültige Bereitstellung](#)

[Validieren](#)

Einleitung

Dieses Dokument beschreibt den Upgrade-Prozess für eine Cisco Secure Firewall Threat Defense in High Availability, die von einem Firewall Management Center verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Hochverfügbarkeitskonzepte und -konfigurationen
- Secure Firewall Management Center (FMC)-Konfiguration
- Konfiguration von Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Das FMC arbeitet, indem jeweils ein Peer-Upgrade durchgeführt wird. Zuerst der Standby-Modus und dann der Active-Modus, sodass ein Failover durchgeführt wird, bevor das Active-Upgrade abgeschlossen wird.

Hintergrundinformationen

Das Upgrade-Paket muss vor dem Upgrade von software.cisco.com heruntergeladen werden.

Führen Sie auf CLI-Aufruf den Befehl `show high-availability config in the Active FTD` aus, um den Status von High Availability zu überprüfen.

```
> 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

Wenn keine Fehler sichtbar sind, fahren Sie mit dem Upgrade fort.

Konfigurieren

Schritt 1: Upgrade-Paket hochladen

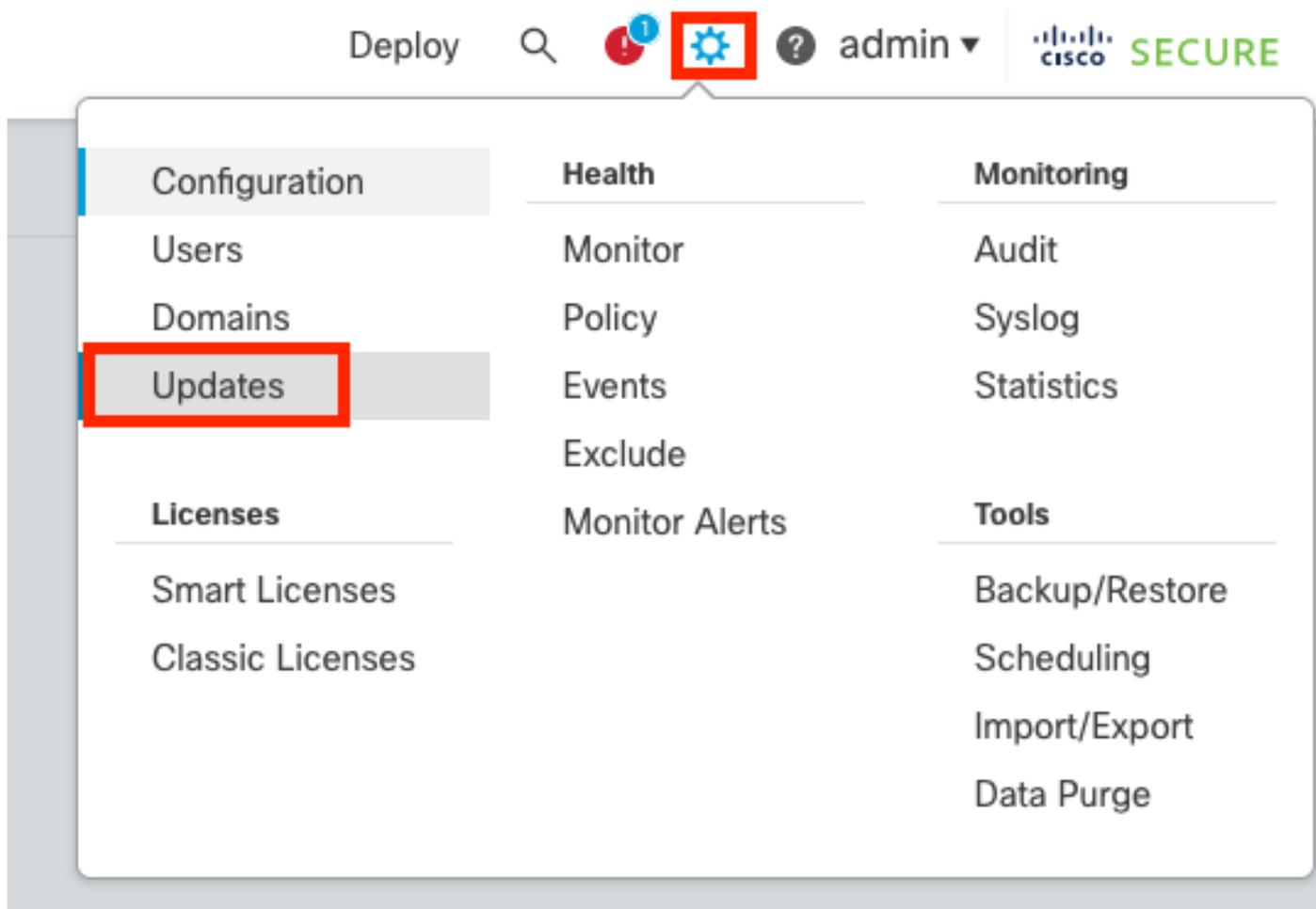
- Laden Sie das FTD-Upgrade-Paket über die grafische Benutzeroberfläche (GUI) in das FMC hoch.
Dieser muss zuvor von der Cisco Software-Website heruntergeladen werden. Hierbei wird das FTD-Modell und die gewünschte Version zugrunde gelegt.



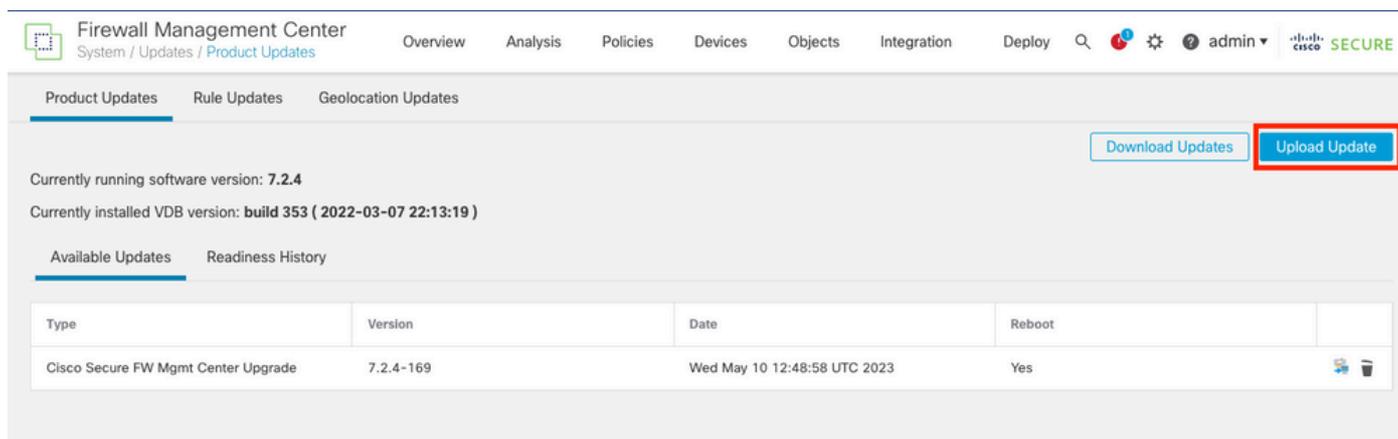
Warnung: Stellen Sie sicher, dass die FMC-Version höher oder gleich der neuen FTD-

Version ist, die aktualisiert werden soll.

System > Updates



- Wählen Sie Update hochladen aus.



- Suchen Sie nach dem zuvor heruntergeladenen Image, und wählen Sie dann Hochladen aus.

Firewall Management Center
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

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 Cisco_FTD_Upgrade-7.2.4-165.sh.REL.tar

Schritt 2: Überprüfungsbereitschaft

Die Bereitschaftsprüfungen bestätigen, ob die Appliances für das Upgrade bereit sind.

- Wählen Sie die Option Install (Installieren) im richtigen Upgrade-Paket aus.

Firewall Management Center
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

Product Updates Rule Updates Geolocation Updates

✔ 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	

Wählen Sie das gewünschte Upgrade aus. In diesem Fall ist die Auswahl für:

- Bei fehlgeschlagener Aktualisierung automatisch abbrechen und auf die vorherige Version zurücksetzen.
- Aktivieren Sie nach erfolgreicher Aktualisierung die Option "Wiederherstellen".
- Aktualisieren Sie Snort 2 auf Snort 3.
- Wählen Sie die HA-Gruppe von FTDs aus, und klicken Sie auf Check Readiness.

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	
<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			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	⬇

Der Fortschritt kann im Nachrichtencenter Nachrichten > Tasks überprüft werden.

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.

Wenn die Bereitschaftsprüfung in FTD abgeschlossen ist und das Ergebnis "Success" lautet, kann das Upgrade durchgeführt werden.

By Group ▾

<input type="checkbox"/>	Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input type="checkbox"/>	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	⬇

Schritt 3: FTD-Upgrade bei hoher Verfügbarkeit

- Wählen Sie das HA-Paar aus, und klicken Sie auf Installieren.

Firewall Management Center
System / Updates / Upload Update

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin **SECURE**

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	⬇️

Warnung: Wenn Sie mit dem Upgrade fortfahren möchten, startet das System neu, um das Upgrade abzuschließen. Wählen Sie OK aus.

 **10.88.243.115:43092**

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

Der Fortschritt kann im Nachrichtencenter Nachrichten > Tasks überprüft werden.

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.](#)

Wenn Sie auf `firepower: Details` anzeigen klicken, wird der Fortschritt grafisch dargestellt und die Protokolle von `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 rem
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

Hinweis: Die Aktualisierung dauert ca. 20 Minuten pro FTD.

Auf CLI kann der Fortschritt im Upgrade-Ordner `/ngfw/var/log/sf` überprüft werden. Wechseln Sie in den Expertenmodus, und wechseln Sie in den Root-Zugriff.

```
> 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.

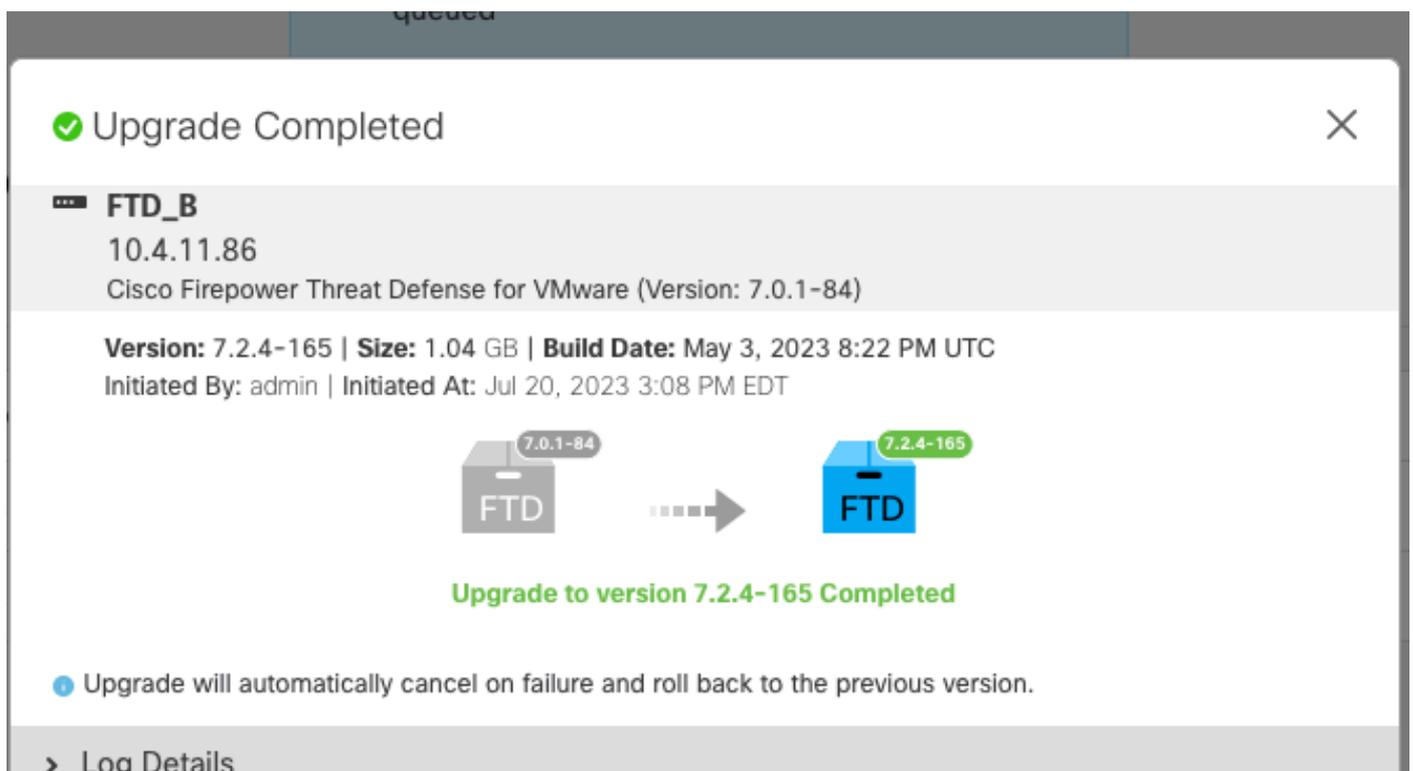
Broadcast message from root@firepower (Thu Jul 20 19:05:25 2023):

System will reboot now due to system upgrade.

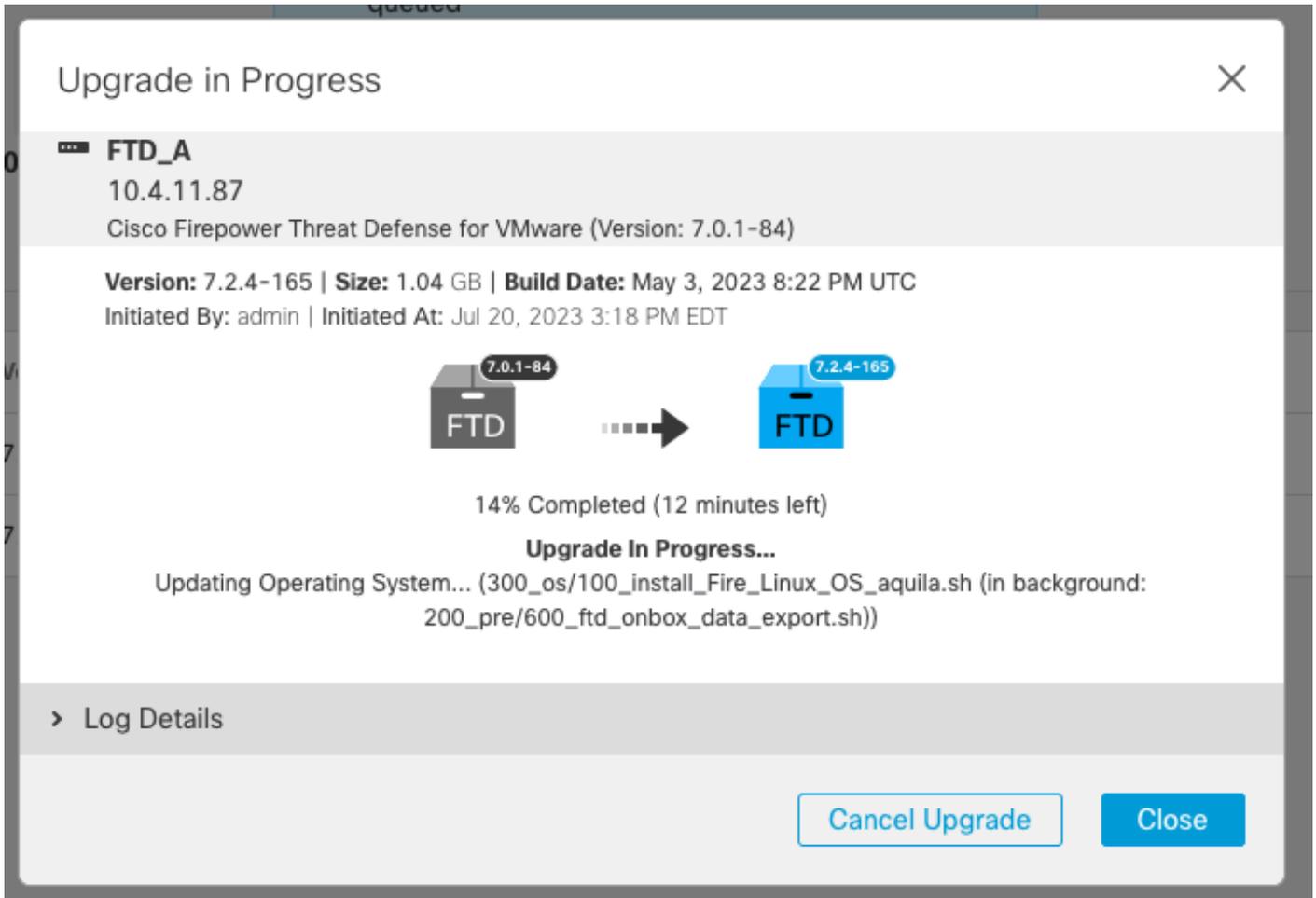
Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

The system is going down for reboot NOW!

Der Upgrade-Status wird in der GUI als abgeschlossen markiert und zeigt die nächsten Schritte an.



Wenn das Upgrade im Standby-Gerät abgeschlossen ist, wird es im aktiven Gerät gestartet.



Wechseln Sie auf der CLI zu LINA (system support diagnostic-CLI), und überprüfen Sie den Failover-Status auf der Standby-FTD mit dem Befehl `show failover state`.

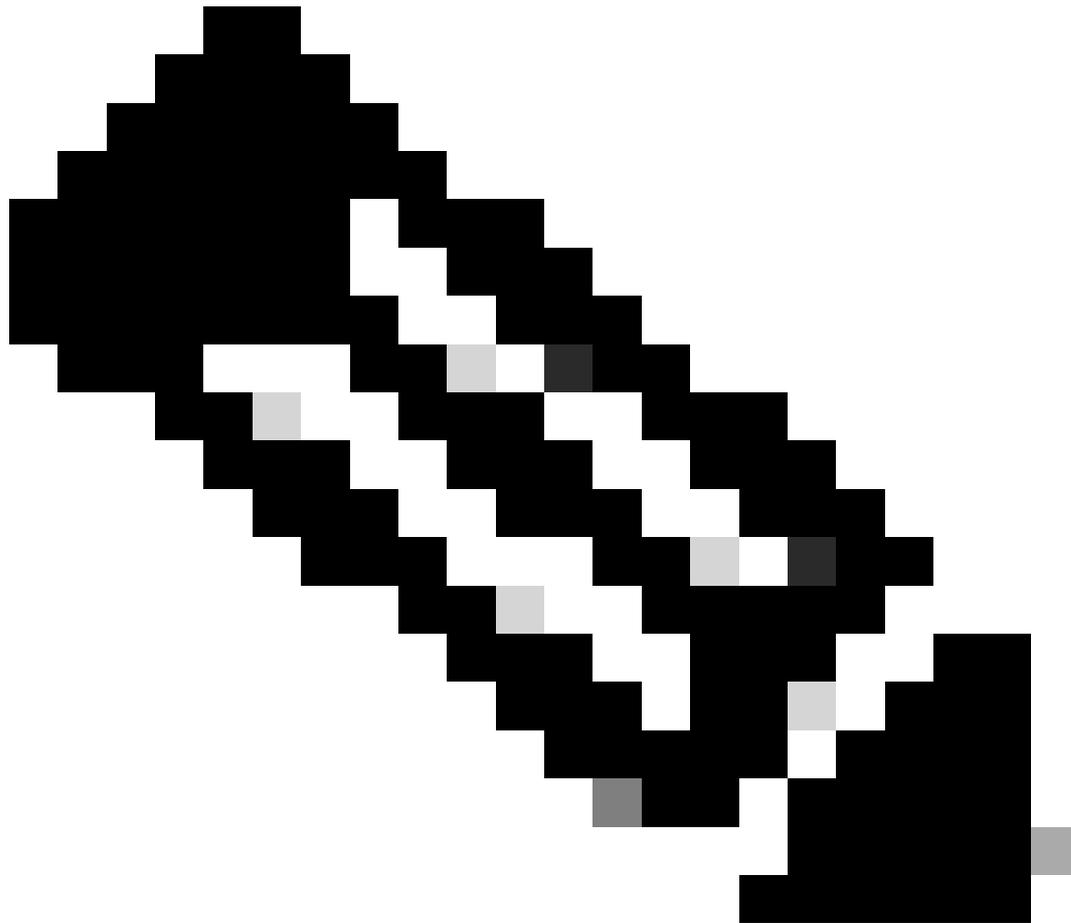
```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

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
```



Hinweis: Das Failover erfolgt automatisch im Rahmen des Upgrades. Bevor Active FTD neu startet und das Upgrade abschließt.

Nach Abschluss des Upgrades ist ein Neustart erforderlich:

✔ 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

Schritt 4: Aktive Peer-Switches (optional)



Hinweis: Wenn das sekundäre Gerät aktiv ist, hat es keine Auswirkungen auf den Betrieb.

Primäres Gerät als aktives und sekundäres als Standby-Gerät zu verwenden, ist eine Best Practice, die bei der Verfolgung eines möglichen Failovers hilft.

In diesem Fall ist "FTD Active" jetzt "Standby", und es kann ein manueller Failover verwendet werden, um den Status wieder auf "Active" zu setzen.

- Navigieren Sie zu den drei Punkten neben dem Bearbeitungszeichen.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

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	↶	⋮

- Wählen Sie Switch Active Peer aus.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

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	↶	⋮

Switch Active Peer
 Break
 Force refresh node status
 Delete
 Revert Upgrade
 Health Monitor
 Troubleshoot Files

- Wählen Sie JA aus, um den Failover zu bestätigen.

Switch Active Peer

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

No

Yes

Validierung des Hochverfügbarkeitsstatus am Ende von Upgrade und Failover abgeschlossen.
Geräte > Gerätemanagement

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 🚫 ⚙️ 👤 admin 🔒

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (1) Upgrade (2) Snort 3 (2) 🔍 Search Device Add

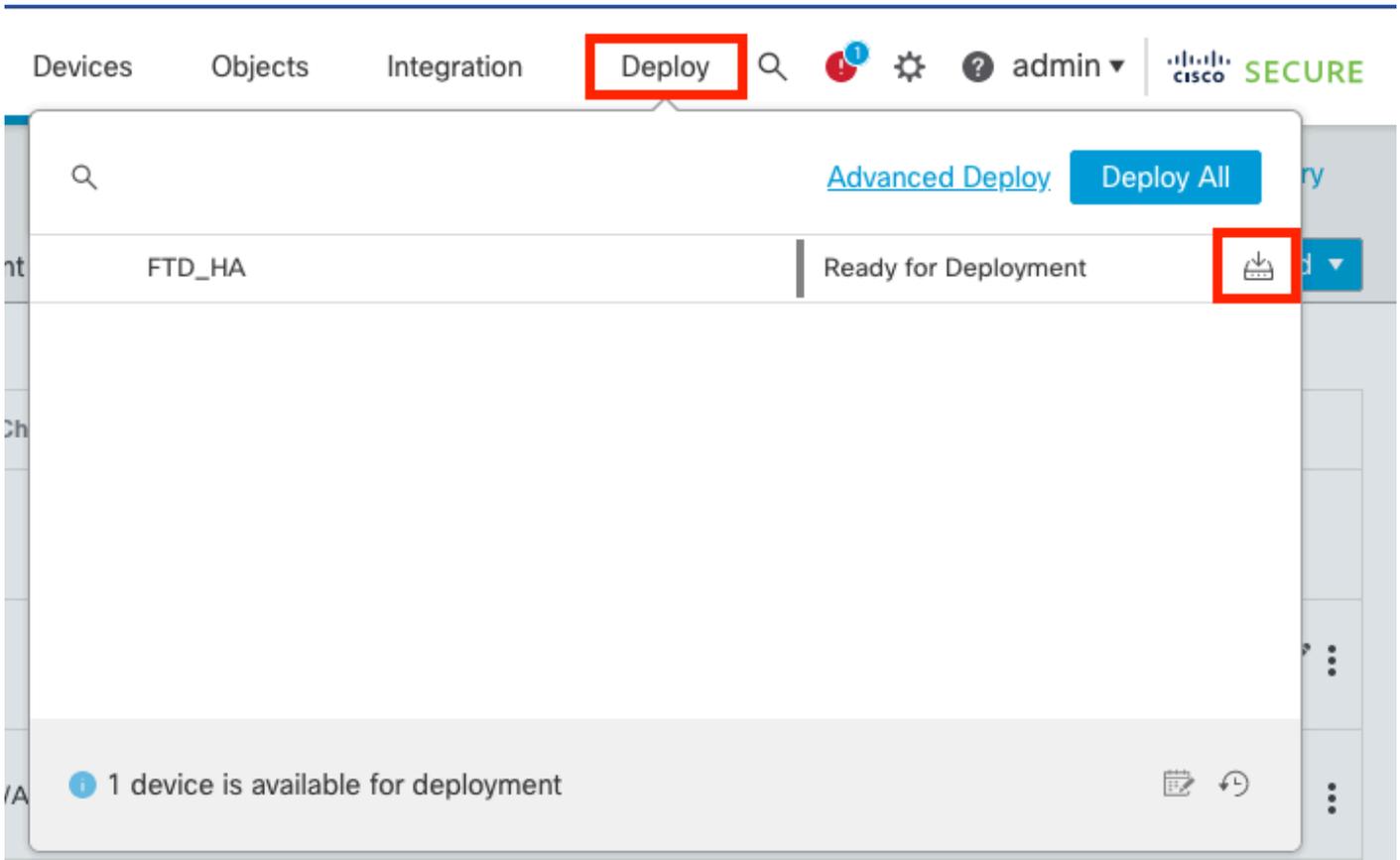
Deployment History

[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) 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) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺	⋮

Schritt 5: Endgültige Bereitstellung

- Bereitstellen einer Richtlinie auf Geräten Bereitstellen > Auf diesem Gerät bereitstellen.



Validieren

Um zu bestätigen, dass der Status für die Hochverfügbarkeit und das Upgrade abgeschlossen sind, müssen Sie den Status bestätigen:

Primär: Aktiv

Sekundär: Standby-fähig

Beide befinden sich unter der Version, die die kürzlich geänderte Version ist (in diesem Beispiel 7.2.4).

- Navigieren Sie in der FMC-GUI zu Geräte > Geräteverwaltung.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy Search Settings Help admin

View By: Group

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

Deployment History

Search Device Add

Collapse All

<input type="checkbox"/>	Name	Model	Version	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	<u>7.2.4</u>	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮
<input checked="" type="checkbox"/>	FTD_B(Secundary, Standby) Snort 3 10.4.11.86 - Routed	FTDv for VMware	<u>7.2.4</u>	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮

- Überprüfen Sie den Failover-Status über den CLI-Befehl show failover state (Failover-Status anzeigen) und show failover (Failover anzeigen), um detailliertere Informationen zu erhalten.

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

Wenn beide FTDs dieselbe Version verwenden und der Status für hohe Verfügbarkeit fehlerfrei ist, ist das Upgrade abgeschlossen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.