

Konfigurieren von hoher Verfügbarkeit auf FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorbereitungen](#)

[Konfigurieren](#)

[Sekundäres FMC konfigurieren](#)

[Primäres FMC konfigurieren](#)

[Verifizierung](#)

Einleitung

Dieses Dokument beschreibt ein Konfigurationsbeispiel für Hochverfügbarkeit (HA) in einem Firewall Management Center (FMC).

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Secure FMC für VMware v7.2.5.

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.

Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Beide FMC-Peers müssen dieselbe Softwareversion, dasselbe Update für Angriffsregeln, dieselbe Schwachstellendatenbank und dasselbe Lightweight Security Package verwenden.
- Beide FMC-Peers müssen dieselbe Kapazität oder Hardwareversion aufweisen.
- Beide FMCs erfordern eine separate Lizenz.

Eine vollständige Liste der Anforderungen finden Sie im [Administrationshandbuch](#).



Warnung: Wenn die aufgelisteten Anforderungen nicht übereinstimmen, kann die HA-Funktion nicht konfiguriert werden.

Dieses Verfahren wird auf allen Hardware-Appliances unterstützt.

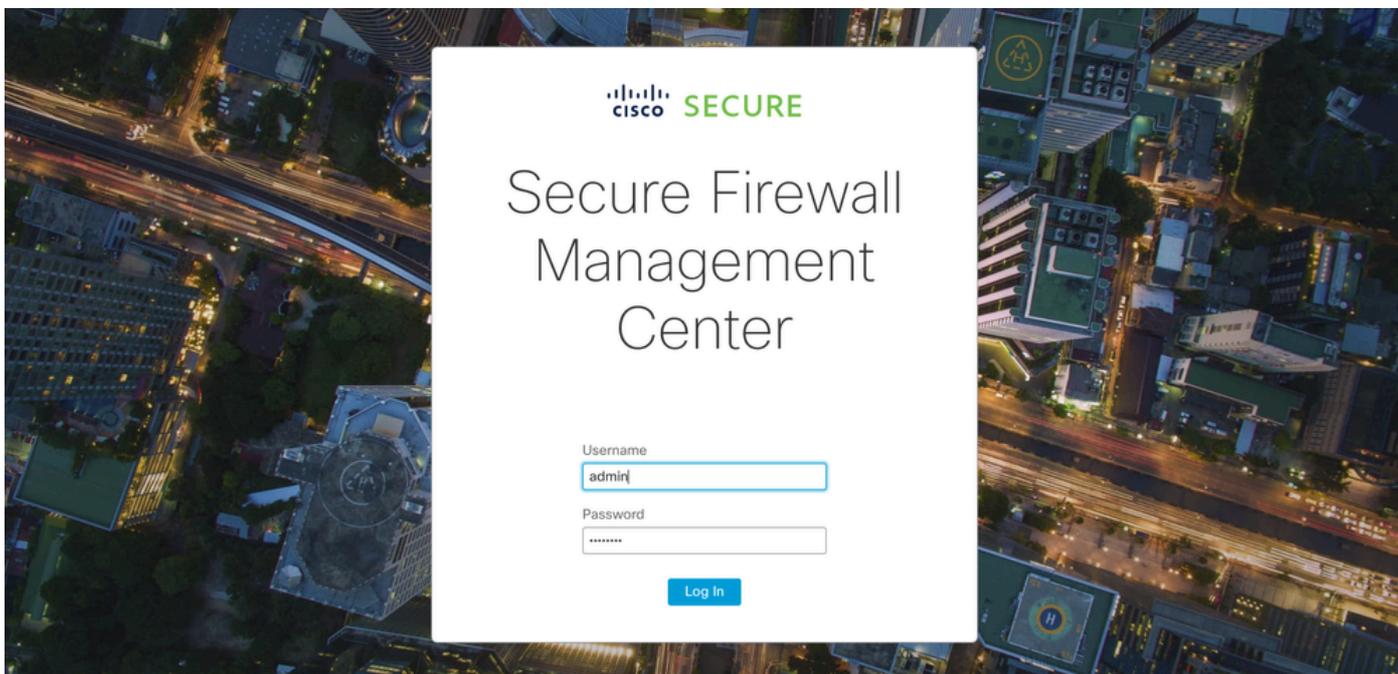
Vorbereitungen

- Administratorzugriff auf beide FMCs gewährleisten
- Gewährleistung der Verbindung zwischen Verwaltungsschnittstellen
- Nehmen Sie sich einen Moment Zeit, um die Softwareversionen zu überprüfen und sicherzustellen, dass alle erforderlichen Upgrades durchgeführt werden.

Konfigurieren

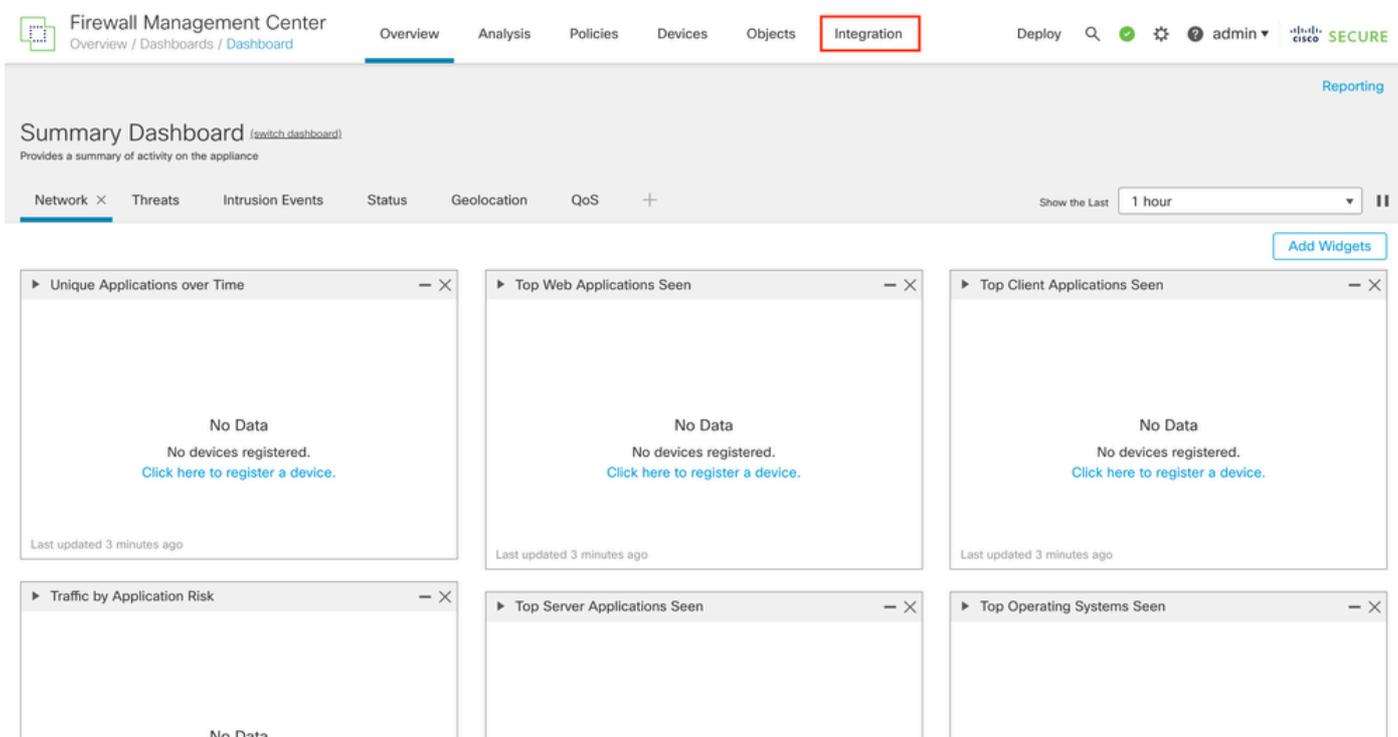
Sekundäres FMC konfigurieren

Schritt 1: Melden Sie sich bei der grafischen Benutzeroberfläche (GUI) des Geräts des FMC an, das die Rolle des sekundären/Standby-Geräts übernehmen soll.



Bei FMC anmelden

Schritt 2: Navigieren Sie zur Registerkarte Integration.



Zur Integration navigieren

Schritt 3: Klicken Sie auf Weitere Integrationen.

SecureX

Security Analytics & Logging

Other Integrations

AMP

AMP Management

Dynamic Analysis Connections

Intelligence

Incidents

Sources

Elements

Settings

Zur anderen Integration navigieren

Schritt 4: Navigieren Sie zur Registerkarte "Hohe Verfügbarkeit".



Firewall Management Center

Integration / Other Integrations / Cloud Services

Overview

Analysis

Policies

Devices

Objects

Integration

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

Navigation zur Hochverfügbarkeit

Schritt 5: Klicken Sie auf Sekundär.



Firewall Management Center

Integration / Other Integrations / High Availability

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

✔

⚙️

❓

admin ▾

cisco SECURE

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

Peer Manager

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

Standalone (No High Availability)

Primary

Secondary

Informationen eingeben und gewünschte Rolle für aktuelles FMC auswählen

Schritt 6: Geben Sie Informationen zum primären/aktiven Peer ein, und klicken Sie auf **Register**.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

Anmerkung: Beachten Sie den Registrierungsschlüssel, da er für das aktive FMC verwendet wird.

Schritt 7. Diese Warnung fordert Sie zur Bestätigung auf, klicken Sie auf **Yes**.

Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



Anmerkung: Stellen Sie sicher, dass kein anderer Task ausgeführt wird, da die GUI neu gestartet wird, während HA erstellt wird.

Schritt 8: Bestätigen Sie, dass Sie den primären Peer registrieren möchten.

Warning

Do you want to register primary peer:
10.18.19.31?

No

Yes



Warnung: Alle Informationen auf den Geräten/Richtlinien/Konfigurationen werden aus dem sekundären FMC entfernt, sobald die HA erstellt wurde.

Schritt 9: Überprüfen Sie, ob der Status des sekundären FMC "Ausstehend" lautet.

Host	Last Modified	Status	State	
10.18.19.31	2023-09-28 13:53:56	Pending Registration	<input type="checkbox"/>	

Primäres FMC konfigurieren

Wiederholen Sie die Schritte 1 bis 4 für das primäre/aktive FMC.

Schritt 5: Klicken Sie auf Primär.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

Schritt 6: Geben Sie die Informationen zum sekundären FMC ein, und klicken Sie auf Registrieren.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

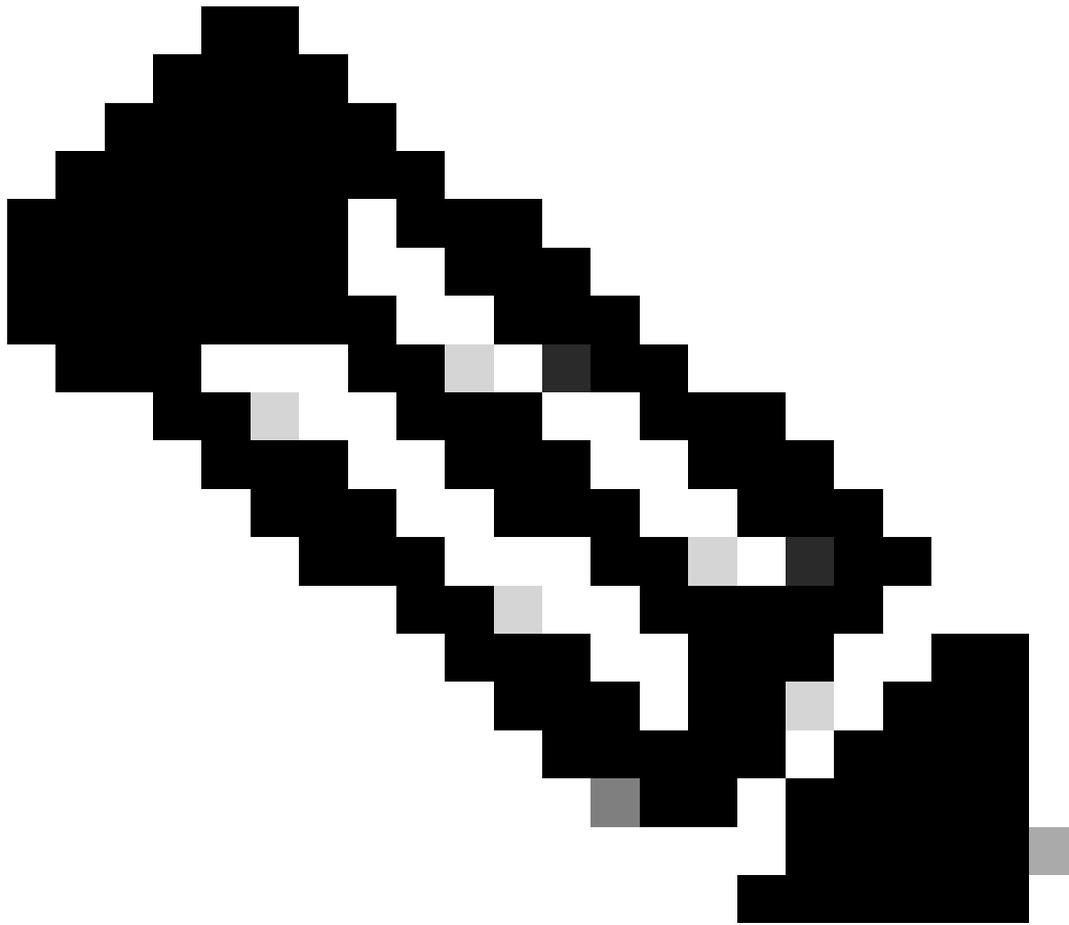
Secondary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.



Anmerkung: Verwenden Sie denselben Registrierungsschlüssel wie das sekundäre FMC.

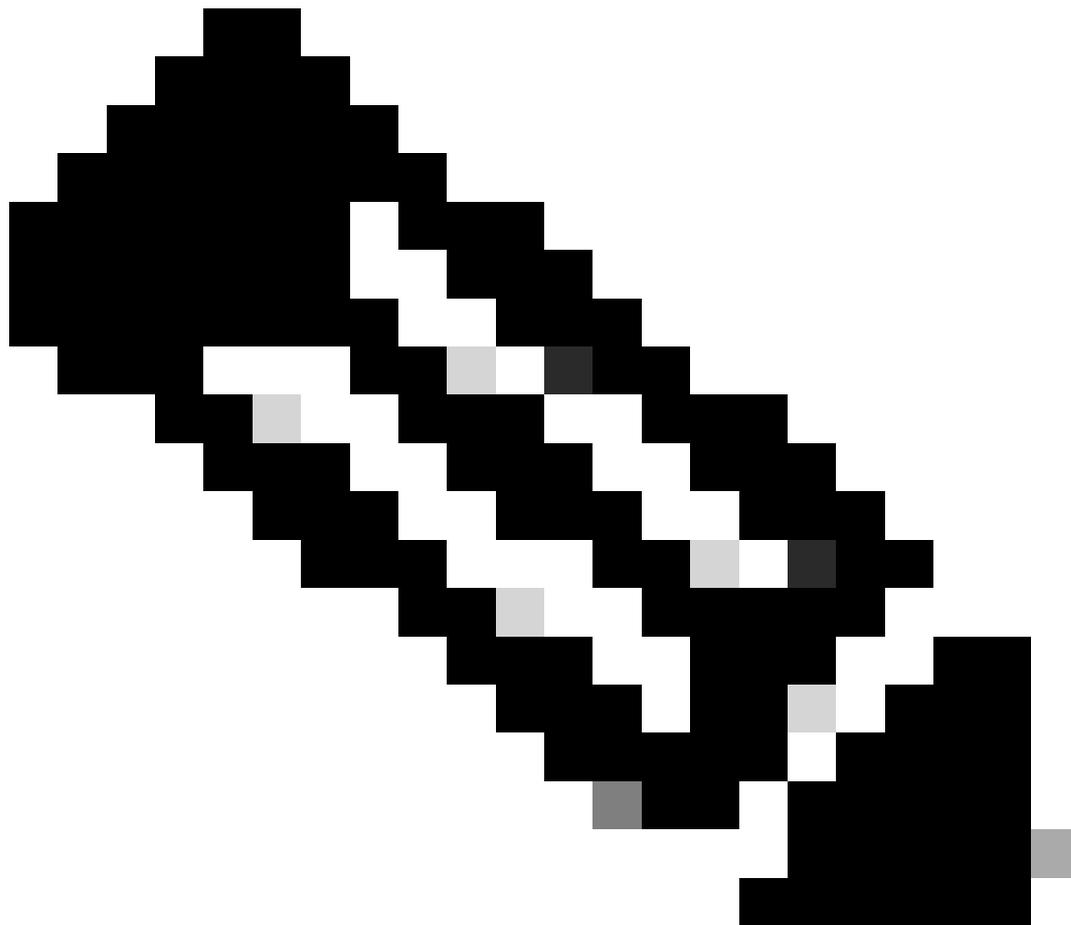
Schritt 7. Diese Warnung fordert Sie zur Bestätigung auf, klicken Sie auf **Yes**.

Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



Anmerkung: Stellen Sie sicher, dass kein anderer Task ausgeführt wird.

Schritt 8: Bestätigen Sie, dass Sie sich für das sekundäre FMC registrieren möchten.

Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer:
10.18.19.32?

No

Yes



Anmerkung: Stellen Sie sicher, dass keine kritischen Informationen zum sekundären FMC vorliegen, da bei Annahme dieser Aufforderung alle Konfigurationen aus dem FMC entfernt werden.

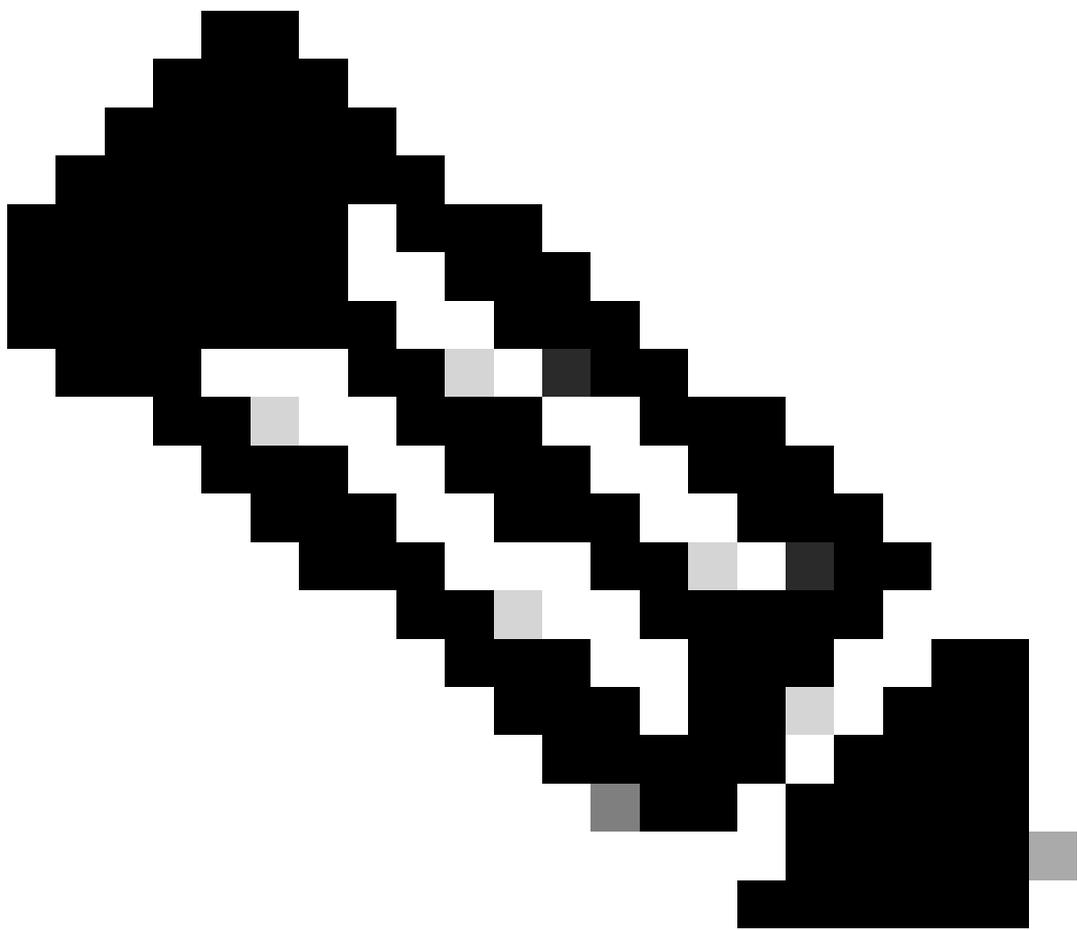
Synchronisierung zwischen primärem und sekundärem Start Die Dauer hängt von der Konfiguration und den Geräten ab. Dieser Vorgang kann von beiden Einheiten aus überwacht werden.

[Switch Peer Roles](#) [Break HA](#) [Pause Synchronization](#)

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 379MB transferred

Summary	
Status	▲ Temporarily degraded- high availability operations are in progress.
Synchronization	▲ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Active - Primary (10.18.19.31)	Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware



Anmerkung: Erwarten Sie während der Synchronisierung den Status Failed (Fehlgeschlagen) und Temporarily degraded (Temporär). Dieser Status wird angezeigt, bis der Prozess abgeschlossen ist.

Verifizierung

Nach Abschluss der Synchronisierung lautet die erwartete Ausgabe Status fehlerfrei und Synchronisierung OK.

Firewall Management Center
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem Peer Manager

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	🟢 Healthy
Synchronization	🟢 OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Active - Primary (10.18.19.31)	Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Die primäre und sekundäre Synchronisierung wird fortgesetzt. das ist normal.

Firewall Management Center
Integration / Other Integrations / High Availability

Devices Integration 🔍 ⚙️ 👤 admin | cisco SECURE

Cloud Services **High Availability** eStreamer Host Input Client Peer Manager

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	🟢 Synchronization task is in progress
Synchronization	🟢 OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Standby - Secondary (10.18.19.32)	Active - Primary (10.18.19.31)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Nehmen Sie sich einen Moment Zeit, um zu überprüfen, ob Ihre Geräte sowohl in der primären als auch in der sekundären Anzeige korrekt sind.

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.