

Configurare la disponibilità elevata in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Operazioni preliminari](#)

[Configurazione](#)

[Configura FMC secondario](#)

[Configura FMC primario](#)

[Verifica](#)

Introduzione

In questo documento viene descritto un esempio di configurazione dell'alta disponibilità (HA, High Availability) su un centro di gestione dei firewall (FMC, Firewall Management Center).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Secure FMC per VMware v7.2.5.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I requisiti specifici per questo documento includono:

- Entrambi i peer FMC devono trovarsi sulla stessa versione del software, sull'aggiornamento delle regole di intrusione, sul database delle vulnerabilità e sul Lightweight Security Package
- Entrambi i peer FMC devono avere la stessa capacità o versione hardware
- Entrambi i CCP richiedono una licenza separata

Per una serie completa di requisiti, è possibile consultare la [Guida all'amministrazione](#).



Avviso: In caso di mancata corrispondenza tra i requisiti elencati, non è possibile configurare HA.

Questa procedura è supportata su tutti gli accessori hardware.

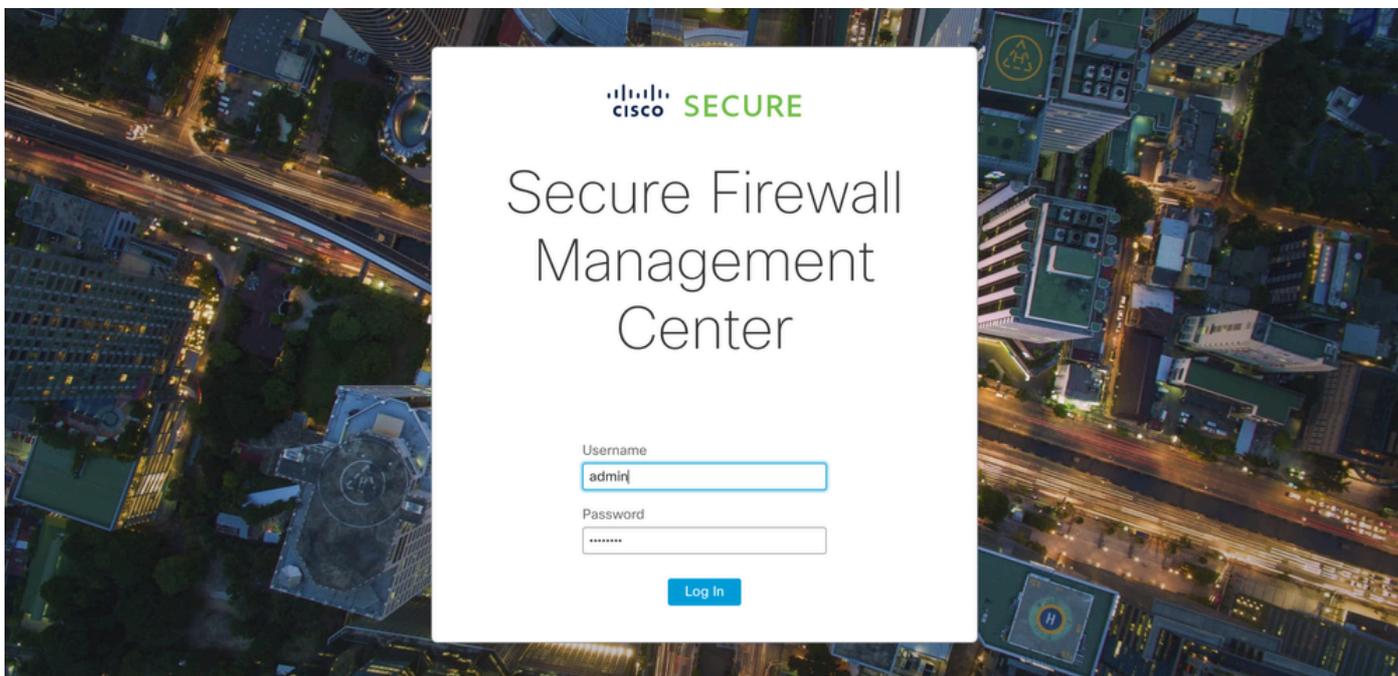
Operazioni preliminari

- Garantire l'accesso degli amministratori a entrambi i CCP
- Connettività tra le interfacce di gestione
- Esaminare le versioni del software e verificare che siano stati eseguiti tutti gli aggiornamenti necessari

Configurazione

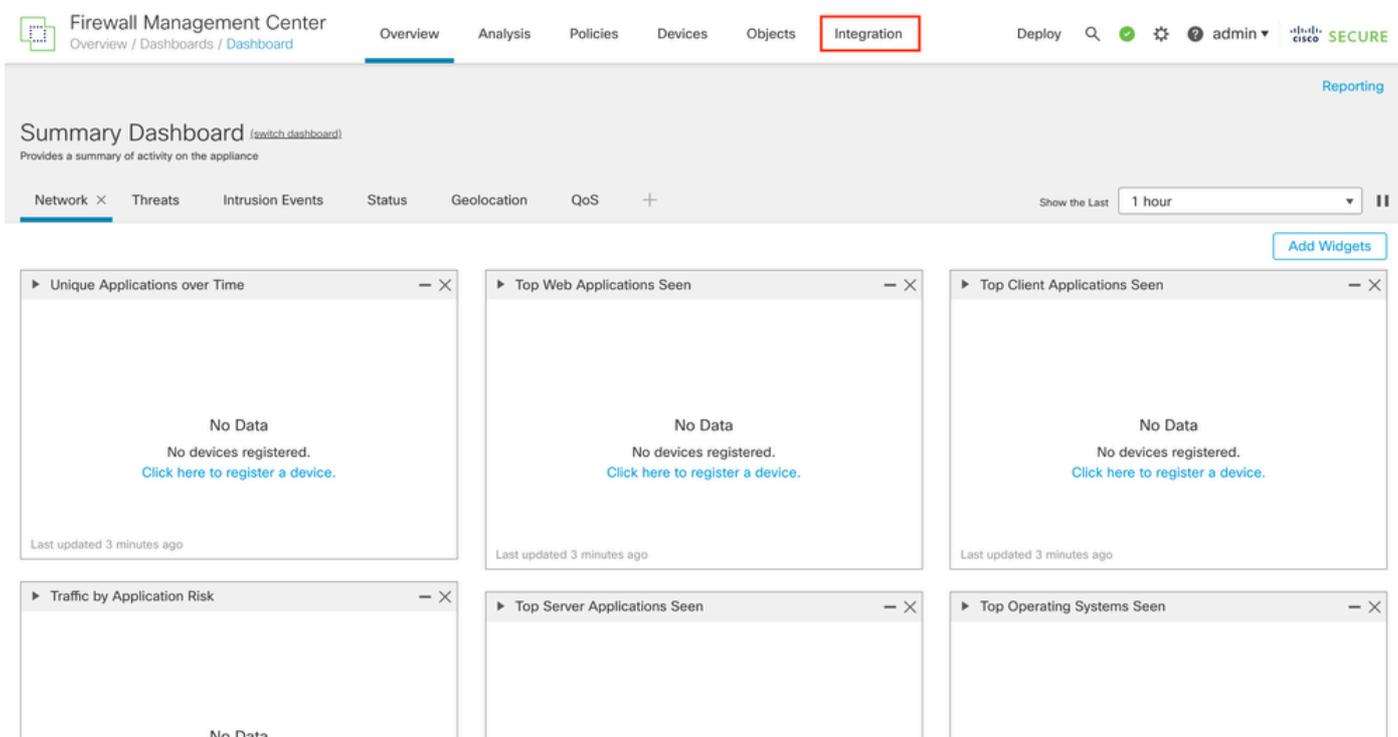
Configura FMC secondario

Passaggio 1. Accedere all'interfaccia utente grafica (GUI) del dispositivo del FMC che assumerà il ruolo di database secondario/standby.



Accedere a FMC

Passaggio 2. Passare alla scheda Integrazione.



Passa all'integrazione

Passaggio 3. Fare clic su Altre integrazioni.

SecureX

Security Analytics & Logging

Other Integrations

AMP

AMP Management

Dynamic Analysis Connections

Intelligence

Incidents

Sources

Elements

Settings

Passa ad altra integrazione

Passaggio 4. Passare alla scheda Alta disponibilità.



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

Passa a Alta disponibilità

Passaggio 5. Fare clic su Secondario.



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

Immettere le informazioni e selezionare il ruolo desiderato per il CCP corrente

Passaggio 6. Immettere le informazioni sul peer primario/attivo e fare clic su **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.

Nota: Prendere nota della chiave di registrazione, in quanto verrà utilizzata sul CCP attivo.

Passaggio 7. Questo avviso richiede di confermare, fare clic su Yes.

Warning

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

No

Yes



Nota: Verificare che non vi siano altre attività in esecuzione mentre è in corso la creazione di HA, la GUI viene riavviata.

Passaggio 8. Confermare che si desidera registrare il peer primario.

Warning

Do you want to register primary peer:
10.18.19.31?

No

Yes



Avviso: Tutte le informazioni su Dispositivi/Criteri/Configurazione verranno rimosse dal FMC secondario dopo la creazione di HA.

Passaggio 9. Verificare che lo stato del CCP secondario sia in sospeso.

Firewall Management Center
Integration / Other Integrations / Peer Manager

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

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

Configura FMC primario

Ripetere i passaggi da 1 a 4 sul CCP primario/attivo.

Passaggio 5. Fare clic su Principale.

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.

Passaggio 6. Immettere le informazioni relative al CCP secondario e fare clic su Registra.

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.



Nota: Utilizzare la stessa chiave di registrazione utilizzata come CCP secondario.

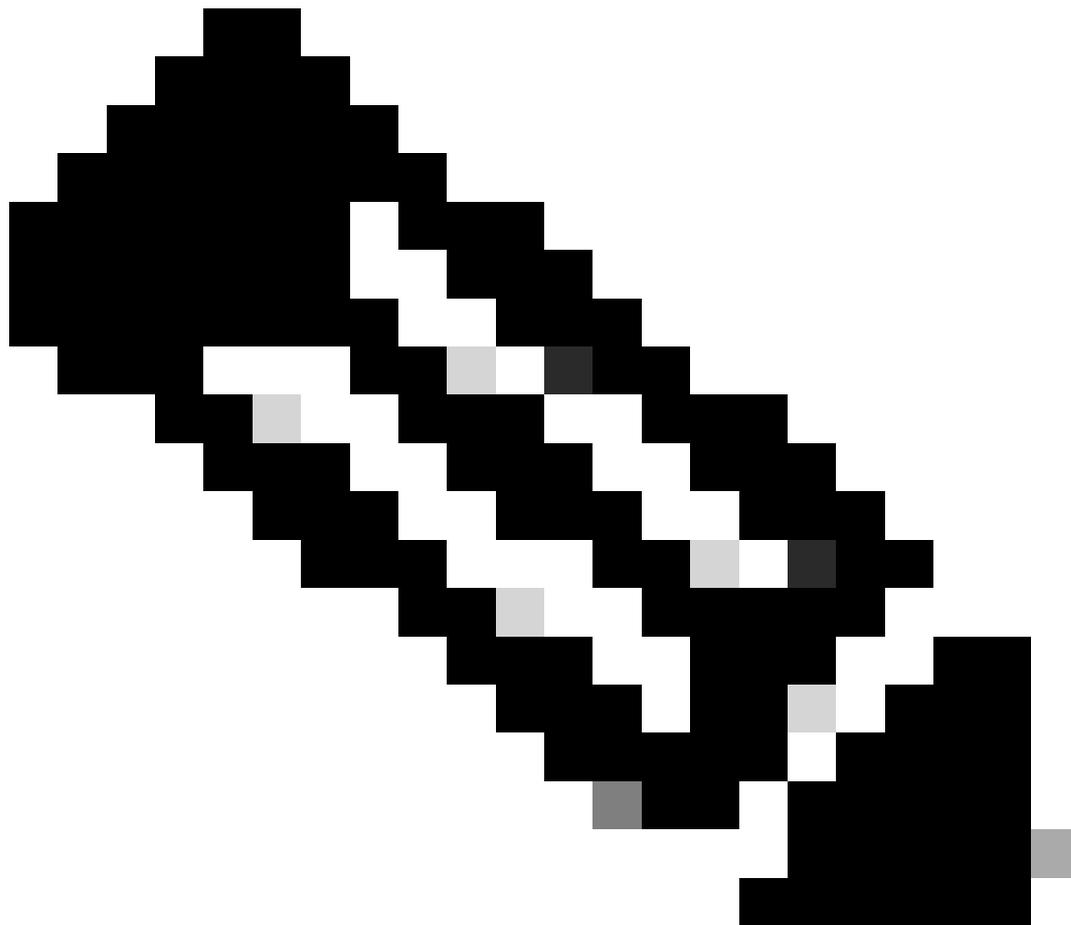
Passaggio 7. Questo avviso richiede di confermare, fare clic su **Yes**.

Warning

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

No

Yes



Nota: Verificare che non siano in esecuzione altre attività.

Passaggio 8. Confermare la registrazione per il CCP secondario.

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



Nota: Accertarsi che il CCP secondario non contenga informazioni critiche, in quanto l'accettazione di questa richiesta comporta la rimozione di tutte le configurazioni dal CCP.

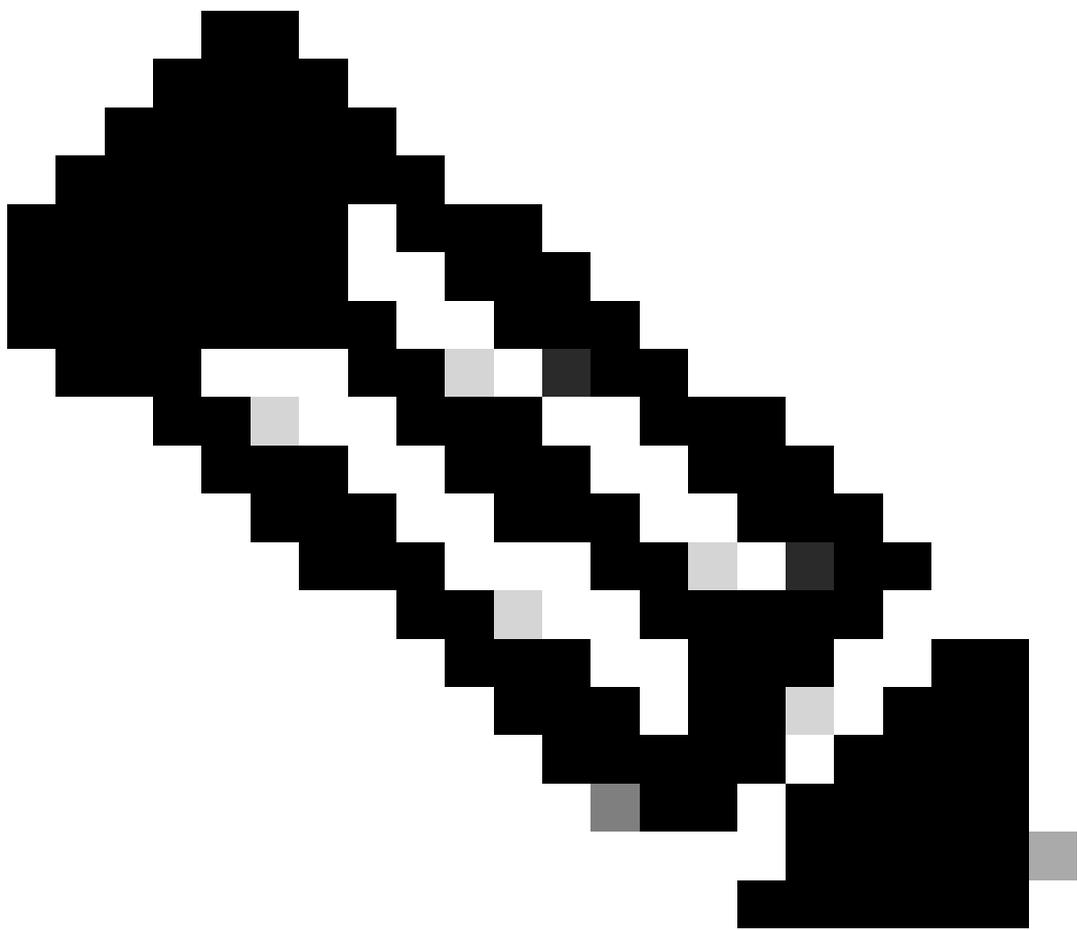
Sincronizzazione tra gli avvii primario e secondario; la durata dipende dalla configurazione e dai dispositivi. Questo processo può essere monitorato da entrambe le unità.

[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 |



Nota: Durante la sincronizzazione, lo stato previsto sarà Non riuscito e Temporaneamente danneggiato. Questo stato viene visualizzato fino al completamento del processo.

Verifica

Una volta completata la sincronizzazione, l'output previsto sarà Stato integro e Sincronizzazione OK.

The screenshot shows the Firewall Management Center interface for High Availability. The status is 'Healthy' and 'Synchronization' is 'OK'. The local system is at 10.18.19.31 and the standby system is at 10.18.19.32. The system status table shows the local system as 'Active - Primary' and the remote system as 'Standby - Secondary'. Both have an operating system of 7.2.5 and software version of 7.2.5-208. The model is 'Secure Firewall Management Center for VMware'.

| 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 |

La sincronizzazione principale e secondaria continua; si tratta di un comportamento normale.

The screenshot shows the Firewall Management Center interface for High Availability. The status is 'Synchronization task is in progress' and 'Synchronization' is 'OK'. The local system is at 10.18.19.31 and the standby system is at 10.18.19.32. The system status table shows the local system as 'Standby - Secondary' and the remote system as 'Active - Primary'. Both have an operating system of 7.2.5 and software version of 7.2.5-208. The model is 'Secure Firewall Management Center for VMware'.

| 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 |

È importante verificare che i dispositivi siano visualizzati correttamente sia sul dispositivo principale che su quello secondario.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).