## Configurare la disponibilità elevata in FMC

## Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Operazioni preliminari
Configurazione
Configura FMC secondario
Configura FMC primario
<u>Verifica</u>

## 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.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	B Devices	Objects	Integration	Deploy Q	📀 🌣 🚱 admin	▼ dialia cisco SECURE
								Reporting
Summary Dashboard (switch dashboard) Provides a summary of activity on the appliance								
Network × Threats Intrusion Events	Status Geo	location QoS	+			Show the Last	1 hour	• II
								Add Widgets
<ul> <li>Unique Applications over Time</li> </ul>	$- \times$	Top Web Applic	ations Seen		- ×	Top Client Application	ns Seen	- ×
No Data			No Dat	a			No Data	
No devices registered.			No devices reg	istered.		No	devices registered.	
Click here to register a device.		C	lick here to regist	ter a device.		Click he	ere to register a device	
Last updated 3 minutes ago		Last updated 3 minute	es ago			Last updated 3 minutes ago		
Traffic by Application Risk	- ×	▶ Top Server App	lications Seen		- ×	Top Operating System	ns Seen	- ×
No Doto								
No Data		1				1		

Passa all'integrazione

Passaggio 3. Fare clic su Altre integrazioni.

Integration	Deploy	Q 📀 🌣 🕜 admin ▼ 👊ulu cisco
SecureX Security Analytics & Other Integrations	Logging	Intelligence Incidents Sources
AMP		Settings
AMP Management Dynamic Analysis Co	onnections	

Passa ad altra integrazione

#### Passaggio 4. Passare alla scheda Alta disponibilità.

Firewall	Managen Other Integra	nent Center ations / Cloud Service:	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 Integration	Manager / Other Integ	ment Center rations / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	03	¢ 6	admin 🗸	cisco SECURE
														Peer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Sm	art Software I	Manager On-Prem						
Select a role for Role For This Firev Standalone (N	r this Manager wall Manager o High Availa	gement Center and ment Center: ability)	specify peer detai	ls to setup hig	gh availability	/.								
O Primary														
<ul> <li>Secondary</li> </ul>														

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.

Cloud Services	Pealms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	Peer Manager
01000 00111000	recuirto	Identity obditees	riigir Availability	courcemen	nost input onent		
Select a role for	this Manag	ement Center and	specify peer detail	s to setup high	n availability.		
Role For This Firew	all Managem	ent Center:					
Standalone (No	High Availal	bility)					
O Primary							
<ul> <li>Secondary</li> </ul>							
Peer Details:							
After Firewall Mana	agement Cen	ter high availability is	configured in virtual c	or cloud environm	nent, each registered l	Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Primary Firewall Ma	anagement C	enter Host:					
10.18.19.31							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register							
† Either host or NAT II	D is required.						



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

## Warning

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





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.



Do you want to register primary peer: 10.18.19.31?





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 M Integration /	Managem Other Integra	nent Center Itions / Peer Manager	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	≎	🛿 admin 🕶	cisco SECU	RE
	Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	re Manager On-Prem							
	Host		Last Mo	lified			S	Status				s	tate			
	10.18.19.31		2023-09	-28 13:53:56			P	ending Registratio	on			•	0		11	

#### Configura FMC primario

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

Passaggio 5. Fare clic su Principale.

Firewall Integration /	Manager Other Integr	nent Center ations / High Availabilit	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	03	¢ 0	) admin 🔻	cisco SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client S	mart Software I	Manager On-Prem						Peer Manager
Select a role for	this Manag	gement Center and	specify peer detai	ils to setup hig	gh availabilit	y.								
Role For This Firew	vall Managen High Availa	nent Center: bility)												
Primary														
Secondary														
Peer Details:														
Configure the seco After Firewall Mana	ndary Mana agement Cer	gement Center with d nter high availability is	etails of the primary configured in virtual	before registrat or cloud enviro	ion. nment, each r	egistered Fire	wall Threat De	fense consumes an	additional Fire	power	MCv De	evice lic	cense.	
Secondary Firewal	Manageme	nt Center Host:												
Registration Key*:														
Unique NAT ID:														
Register † Either host or NAT II	D is required.													

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

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	Peer Manager
Select a role for	this Manag	gement Center and	specify peer detai	ls to setup hig	h availability.		
Role For This Firev	vall Manager o High Availa	nent Center: ability)					
Primary							
Secondary							
Peer Details:							
Configure the sect After Firewall Man Secondary Firewa 10.18.19.32	ondary Mana agement Cei II Manageme	gement Center with d nter high availability is nt Center Host:	letails of the primary s configured in virtual	pefore registrati or cloud enviror	on. Iment, each registereo	d Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Registration Key*:							
cisco123							
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?





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?





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.

	Firewall I Integration /	Managen Other Integra	nent Cent ations / High /	er Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	\$	🛿 admin 🔻	cisco SECURE
															Peer Manager
Cloud	Services	Realms	Identity Sou	urces	High Availability	eStreamer	Host Input	t Client Sr	nart Software I	Manager On-Pre	m				
									5	Switch Peer Ro	oles 🔅 I	Break HA		II Pause Syr	nchronization
				High ava These of Database	ilability operations ar perations include file e files synchronizatio	re in progress. The copy which may t n: 100% of 379MI	e status messa take time to co B transferred	ages and alerts omplete.	on this page are	e temporary. Pleas	se check after high	availabili	ty operat	ions are comple	te. ×
	Summa	ary						S	ystem Statu	S					
	Status		🔺 Ten	nporarily (	degraded- high ava	ilability operation p	ns are in progress.			1	Local Active - Primary (10.18.19.31)		Stan	Remote dby - Seconda (10.18.19.32)	ry
	Synchror	nization					Failed	C	perating Syste	m	7.2.5			7.2.5	
	Active Sy	ystem				10.1	18.19.31	s	oftware Versio	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	18.19.32	Ν	lodel	Secur	e Firewall Manag Center for VMwar	ement e	S Mana	ecure Firewall gement Center VMware	for



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.

Firewall	Manager / Other Integr	ment Center ations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (	\$	🕜 admin	▼ dualte SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client S	mart Software N	lanager On-Prem					Peer Manager
							4	Switch Peer Roles	¢ 1	Break HA		II Pause S	Synchronization
Summ	ary					S	system Status	6					
Status				O F	lealthy			Acti	Local		Stand	Remote	larv
Synchr	onization				OK			(1	0.18.19.31)		(	10.18.19.32)	i di y
Active	System			10.18	.19.31	C	Operating System	n	7.2.5			7.2.5	
Standb	y System			10.18	.19.32	5	Software Version	1	7.2.5-208			7.2.5-208	
						Ν	Model	Secure Fi Cent	rewall Manage er for VMware	ement	Se Manag	ecure Firewa ement Cent VMware	ll er for

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

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		Q 🔮	🔅 🕜 admin 🕶 diada SECURE
				Peer Manager
Cloud Services High Availability eStreamer	Host Input Client			
		Switch	Peer Roles   Break HA	II Pause Synchronization
Summary		System Status		
ourintary		oyotoni otatao	Lord	Domete
Status	Synchronization task is in progress		Standby - Secondary	Active - Primary
Synchronization	📀 ОК		(10.18.19.32)	(10.18.19.31)
Active System	10.18.19.31	Operating System	7.2.5	7.2.5
Standby System	10.18.19.32	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).