

# Configurazione del clustering sui dispositivi Cisco FirePOWER serie 7000 e 8000

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Aggiunta di un cluster](#)

[Interruzione di un cluster](#)

[Condivisione dello stato](#)

[Risoluzione dei problemi](#)

[Dispositivo non configurato correttamente](#)

[Tutti i membri HA devono avere criteri aggiornati](#)

[Documenti correlati](#)

## Introduzione

Il clustering dei dispositivi fornisce ridondanza della configurazione e delle funzionalità di rete tra due dispositivi o stack. In questo articolo viene descritto come configurare il clustering sui dispositivi Cisco Firepower serie 7000 e 8000.

## Prerequisiti

Prima di tentare di stabilire un cluster, è necessario avere familiarità con le varie funzionalità del clustering. Cisco consiglia di leggere la sezione [Clustering Device](#) del manuale FireSIGHT System User Guide per ulteriori informazioni.

## Requisiti

Entrambi i dispositivi devono avere i seguenti componenti identici:

1. Stessi modelli hardware

**Nota:** Impossibile configurare uno stack e un singolo dispositivo in un cluster. Devono essere in uno stack dello stesso tipo o di due dispositivi singoli simili.

2. Stessi moduli di rete (Netmod) negli stessi slot

**Nota:** Le netmod di stack non vengono prese in considerazione quando vengono controllati i prerequisiti del cluster. Sono considerati uguali a uno slot vuoto.

3. Stesse licenze e devono essere esattamente le stesse. Se un dispositivo dispone di una licenza aggiuntiva, non è possibile formare il cluster.

4. Stesse versioni software

5. Stesse versioni VDB

6. Stessi criteri NAT (se configurati)

## Componenti usati

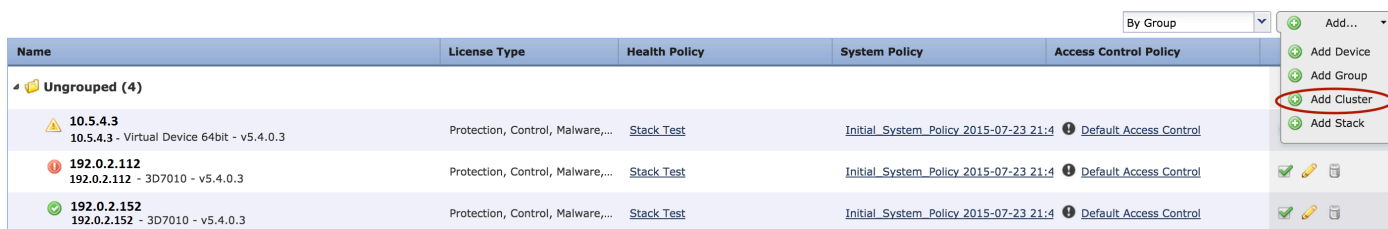
- Due Cisco Firepower 7010 nella versione 5.4.0.4
- FireSIGHT Management Center 5.4.1.3

**Nota:** 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.

## Configurazione

### Aggiunta di un cluster

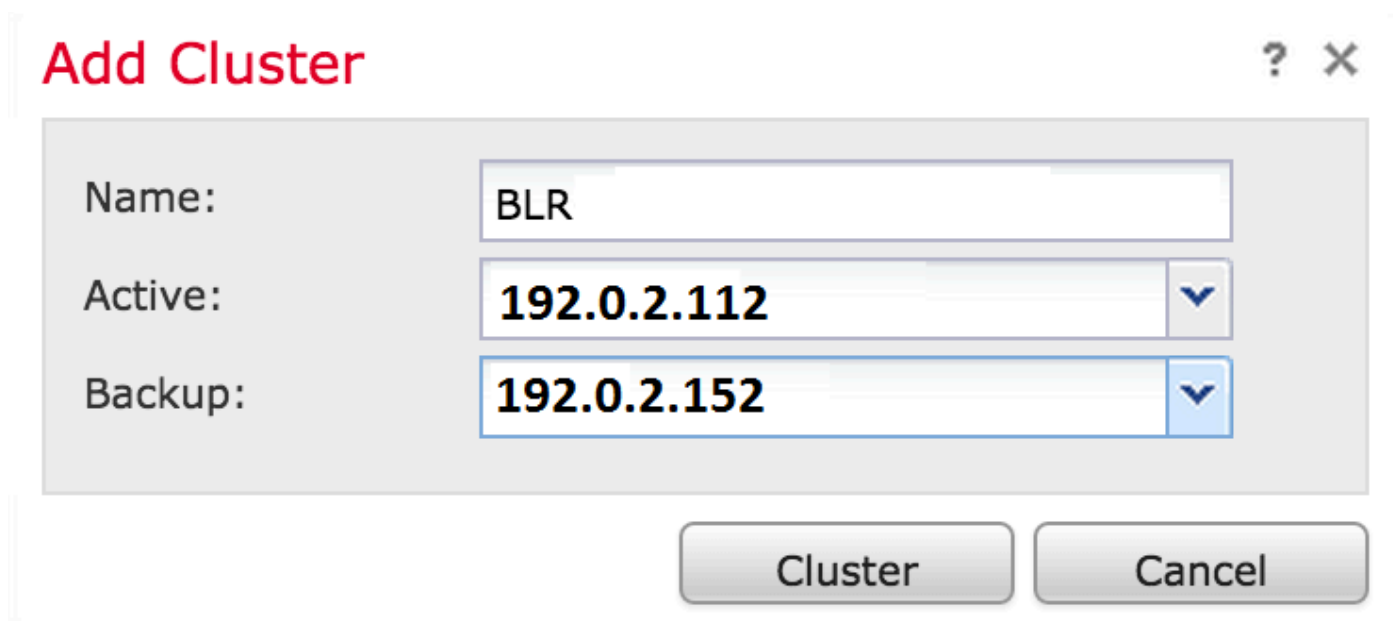
1. Selezionare **Device > Device Management**.
2. Selezionare i dispositivi da raggruppare. Nella parte superiore destra della pagina, selezionare l'elenco a discesa **Aggiungi**.
3. Selezionare **Aggiungi cluster**.



Name	License Type	Health Policy	System Policy	Access Control Policy
Ungrouped (4)				
10.5.4.3 10.5.4.3 - Virtual Device 64bit - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial_System_Policy_2015-07-23_21:4	Default Access Control
192.0.2.112 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial_System_Policy_2015-07-23_21:4	Default Access Control
192.0.2.152 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial_System_Policy_2015-07-23_21:4	Default Access Control

By Group [v]  
Add...  
Add Device  
Add Group  
Add Cluster  
Add Stack

4. Viene visualizzata la finestra popup **Aggiungi cluster**. Verrà visualizzata la seguente schermata. Specificare gli indirizzi IP dei dispositivi attivi e di backup.



**Add Cluster** ? X

Name:

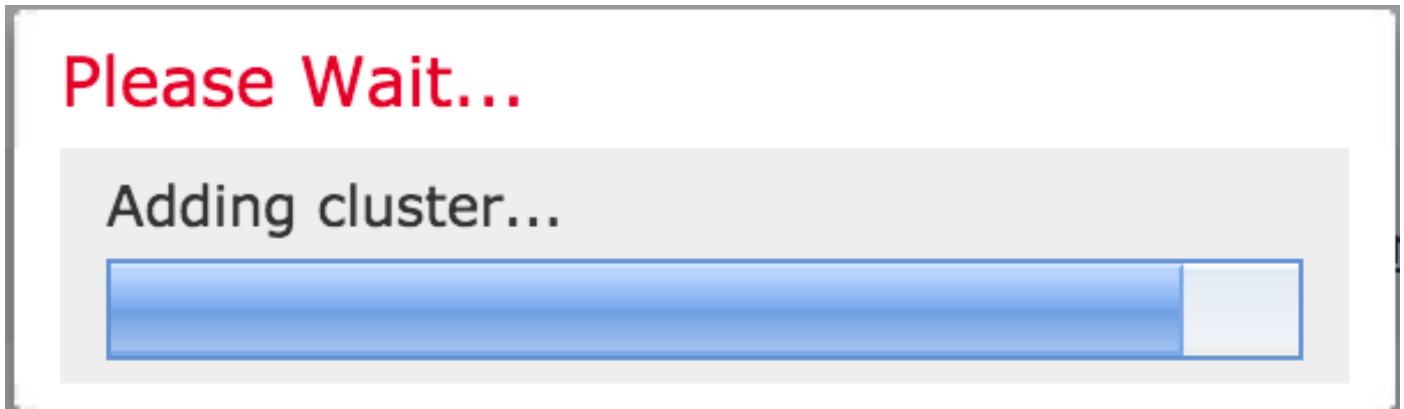
Active:  ▼

Backup:  ▼











Cluster Cancel

5. Fare clic sul pulsante **Cluster**. Se vengono soddisfatti tutti i prerequisiti, verrà visualizzata la









finestra di stato **Aggiunta cluster** per un massimo di 10 minuti.



6. Una volta creato il cluster, le periferiche aggiornate saranno disponibili nella pagina **Gestione periferiche**.

BLR-Cluster 3D7010 Cluster				   
 <b>192.0.2.112</b> (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	
 <b>192.0.2.152</b> 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	

7. È possibile cambiare il peer attivo in un cluster facendo clic sulla freccia di rotazione accanto all'icona a forma di matita.

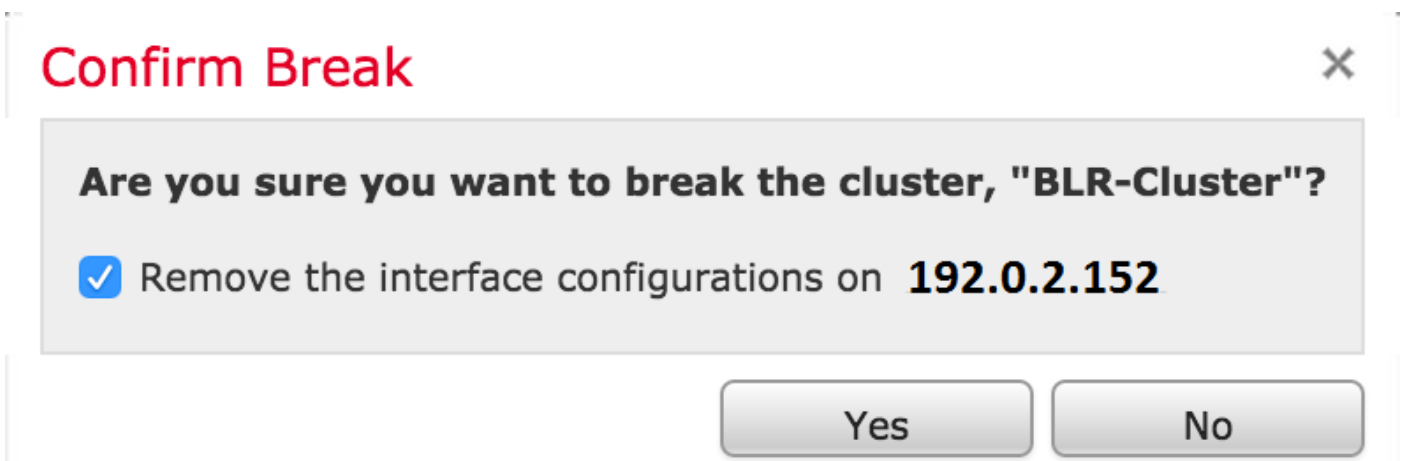
BLR-Cluster 3D7010 Cluster				   
 <b>192.0.2.112</b> (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	
 <b>192.0.2.152</b> 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	

## Interruzione di un cluster

È possibile interrompere un cluster facendo clic sull'opzione **Interrompi cluster** accanto all'icona **Cestino**.

BLR-Cluster 3D7010 Cluster				   
 <b>192.0.2.112</b> (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	
 <b>192.0.2.152</b> 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>  <a href="#">Default Access Control</a>	

Dopo aver fatto clic sull'icona del **Cestino**, verrà richiesto di rimuovere la configurazione dell'interfaccia dal dispositivo di backup. Selezionare **Sì** o **No**.



È inoltre possibile eliminare un cluster e annullare la registrazione dei dispositivi dal centro di gestione facendo clic sul **Cestino**.

Se il dispositivo ha perso l'accesso al Management Center, è possibile interrompere il clustering utilizzando il seguente comando della CLI:

```
> configure clustering disable
```

## Condivisione dello stato

La condivisione dello stato in cluster consente ai dispositivi o agli stack in cluster di sincronizzare gli stati, in modo che se uno dei dispositivi o degli stack si guasta, l'altro peer può subentrare senza alcuna interruzione nel flusso del traffico.

**Nota:** Prima di configurare la condivisione dello stato cluster, è necessario configurare e abilitare le interfacce di collegamento ad alta disponibilità (HA, High Availability) su entrambi i dispositivi o sui dispositivi principali in stack del cluster.

**Attenzione:** L'attivazione della condivisione dello stato rallenta le prestazioni del sistema.

Per abilitare la condivisione dello stato su un collegamento HA, eseguire la procedura seguente:

1. Passare a **Dispositivi > Gestione dispositivi**. Selezionare il cluster e modificarlo.
2. Selezionare la scheda **Interfacce**.
3. Selezionare il collegamento che si desidera impostare come collegamento HA.
4. Fare clic su **modifica** (icona matita). Viene visualizzata la finestra **Modifica interfaccia**.

### Edit Interface



None	Passive	Inline	Switched	Routed	HA Link
Enabled:	<input checked="" type="checkbox"/>				
Mode:	Autonegotiation				▼
MDI/MDIX:	Auto-MDIX				▼
MTU:	9922				
				Save	Cancel

5. Dopo aver abilitato il collegamento e configurato le altre opzioni, fare clic su **Salva**.
6. Passare alla scheda **Cluster**. Nella sezione destra della pagina verrà visualizzata una sezione

denominata **Condivisione di stati**.

## State Sharing



<b>Enabled:</b>	No
<b>Statistics:</b>	
<b>HA Link</b>	<input type="radio"/> (s1p3)
<b>Minimum Flow Lifetime:</b>	1000 ms
<b>Minimum Sync. Interval:</b>	100 ms
<b>Maximum HTTP URL Length:</b>	32

7. Fare clic sull'**icona della matita** per modificare le opzioni di condivisione dello stato.

8. Assicurarsi che l'opzione **Abilitato** sia selezionata.

9. Facoltativamente, è possibile modificare Durata flusso, Intervallo sincronizzazione e Lunghezza massima URL HTTP.

Condivisione dello stato attivata. È possibile controllare le statistiche del traffico facendo clic sull'icona della lente di ingrandimento accanto a Statistiche. Verranno visualizzate le statistiche del traffico per entrambi i dispositivi come mostrato di seguito.

### State Sharing Statistics



	Active Peer	Backup Peer
<b>Device</b>	10.122.144.203 <input type="button" value="v"/>	10.122.144.204 <input type="button" value="v"/>
<b>Messages Received (Unicast)</b>	0	0
<b>Packets Received</b>	0	0
<b>Total Bytes Received</b>	0	0
<b>Protocol Bytes Received</b>	0	0
<b>Messages Sent</b>	0	0
<b>Packets Sent</b>	0	0
<b>Bytes Sent</b>	0	0
<b>TX Errors</b>	0	0
<b>TX Overruns</b>	0	0
<b>Recent Logs</b>	<a href="#">View</a>	<a href="#">View</a>

Refresh

Close


Quando la condivisione dello stato è abilitata e un'interfaccia sul membro Attivo non è attiva, tutte le connessioni TCP vengono trasferite al dispositivo di standby che è diventato Attivo.

## Risoluzione dei problemi

### Dispositivo non configurato correttamente

Se uno dei [prerequisiti](#) non viene soddisfatto, viene visualizzato il seguente messaggio di errore:

**Error**



Device **192.0.2.152** is not properly configured to be a part of the cluster for **192.0.2.112** - check SW versions, HW, licensing, and applied NAT policy

OK

In Management Center passare a **Dispositivi > Gestione dispositivi** e verificare se entrambi i dispositivi dispongono delle stesse versioni software, modelli hardware, licenze e policy.

In alternativa, su un dispositivo è possibile eseguire il comando seguente per verificare il criterio di controllo dell'accesso applicato e la versione hardware e software:

```
> show summary
-----[ Device ]-----
Model                : Virtual Device 64bit (69) Version 5.4.0.4 (Build 55)
UUID                 : 4dfa9fca-30f4-11e5-9eb3-b150a60d4996
VDB version          : 252
-----

-----[ policy info ]-----
Access Control Policy : Default Access Control
Intrusion Policy      : Initial Inline Policy
.
.
.
Output Truncated
.
```

Per verificare il criterio NAT, eseguire il comando seguente sul dispositivo:

```
> show nat config
```

**Nota:** Le licenze possono essere controllate solo nel Management Center, in quanto sono archiviate solo nel Management Center.

## Tutti i membri HA devono avere criteri aggiornati

Di seguito è riportato un altro possibile errore

### Error



All members of an HA config must have up-to-date policies deployed to them. The following devices are out of date: **192.0.2.112**

OK

Questo errore si verifica quando i criteri di controllo di accesso non sono aggiornati. Riapplicare i criteri e ripetere il tentativo di configurazione del cluster.

## Documenti correlati

- [Dispositivo di clustering - Guida per l'utente del sistema FireSIGHT](#)