

Configuración del clustering en los dispositivos Cisco FirePOWER series 7000 y 8000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Adición de un clúster](#)

[Romper un clúster](#)

[Compartir el estado](#)

[Resolución de problemas](#)

[El dispositivo no está configurado correctamente](#)

[Todos los miembros de HA deben tener políticas actualizadas](#)

[Documentos Relacionados](#)

Introducción

La agrupación en clúster de dispositivos proporciona redundancia de configuración y funcionalidad de red entre dos dispositivos o pilas. En este artículo se describe cómo configurar la agrupación en clústeres en los dispositivos Cisco Firepower series 7000 y 8000.

Prerequisites

Antes de intentar establecer un clúster, debe estar familiarizado con diversas características de la agrupación en clúster. Cisco recomienda leer la sección [Dispositivo de agrupamiento](#) de la Guía del Usuario del Sistema FireSIGHT para obtener más información.

Requirements

Ambos dispositivos deben tener los siguientes componentes idénticos:

1. Mismos modelos de hardware

Nota: No se puede configurar una pila y un solo dispositivo en un clúster. Deben estar en la pila del mismo tipo o en dos dispositivos individuales similares.

2. Mismos módulos de red (Netmod) en las mismas ranuras

Nota: Los netmods de apilamiento no se tienen en cuenta cuando se comprueban los requisitos previos del clúster. Se consideran como una ranura vacía.

3. Las mismas licencias y deben ser exactamente iguales. Si un dispositivo tiene una licencia adicional, el clúster no se puede formar.

4. Mismas versiones de software

5. Mismas versiones de VDB

6. Misma política NAT (si está configurada)

Componentes Utilizados

- Dos Cisco Firepower 7010 en la versión 5.4.0.4
- FireSIGHT Management Center 5.4.1.3

Nota: La información de este documento se creó a partir de los dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

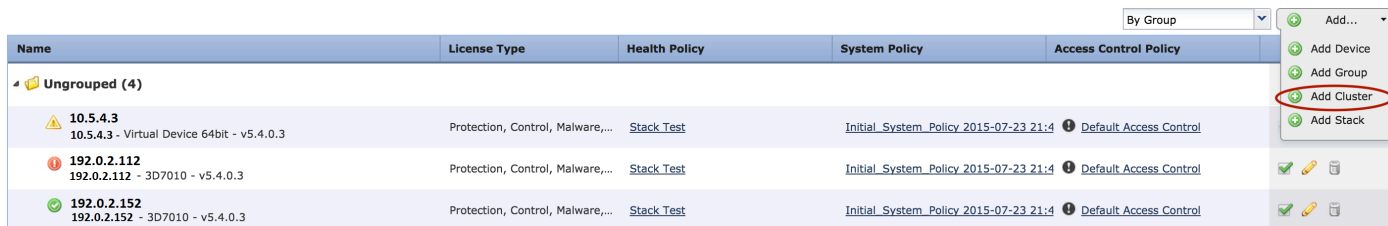
Configuración

Adición de un clúster

1. Vaya a **Device > Device Management** .

2. Seleccione los dispositivos que desea agrupar en clúster. En la parte superior derecha de la página, seleccione la lista desplegable **Agregar**.

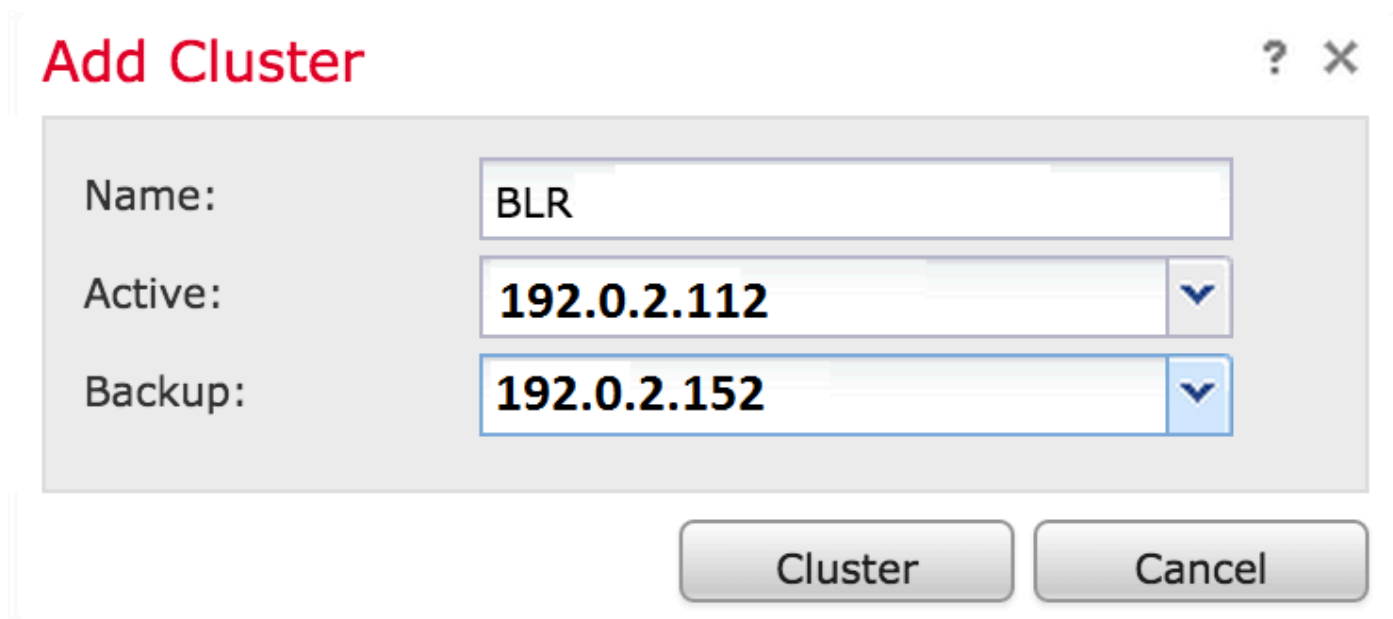
3. Seleccione **Agregar clúster**.



| 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. Aparece la ventana emergente **Agregar clúster**. Verá la siguiente pantalla. Proporcione las direcciones IP de los dispositivos Active y Backup.



Add Cluster ? X

Name:

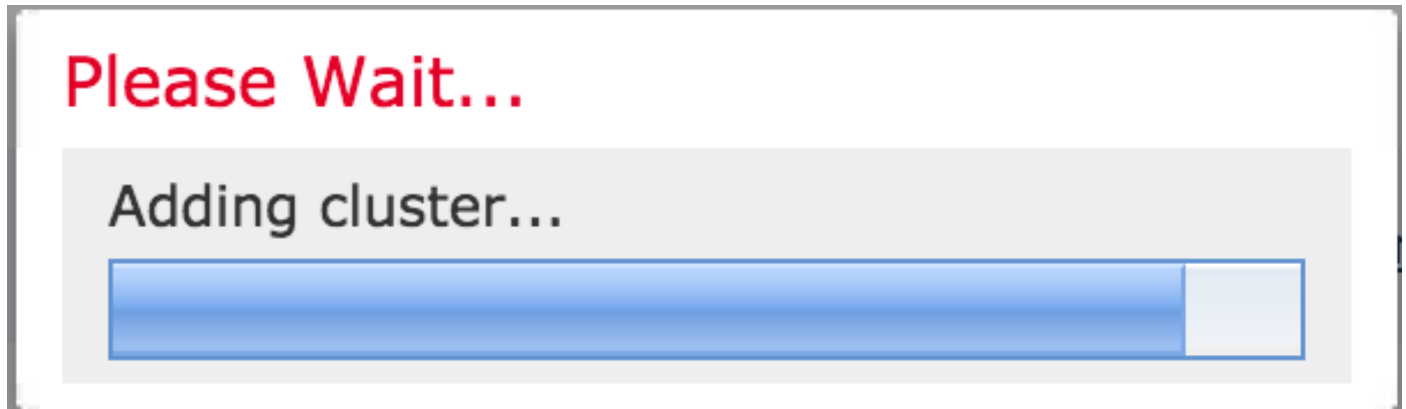
Active: ▼

Backup: ▼

Cluster Cancel

5. Haga clic en el botón **Clúster**. Si se cumplen todos los requisitos previos, verá la ventana de

estado **Agregar clúster** durante un máximo de 10 minutos.



6. Una vez que el clúster se ha creado correctamente, encontrará los dispositivos actualizados en la página **Administración de dispositivos**.

| BLR-Cluster 3D7010 Cluster | | | | ✓ ✎ 🗑️ 📄 | |
|---|----------------------------------|------------|---------------------------------------|--------------------------|---|
| ✓ 192.0.2.112 (active) 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 | 🔗 |

7. Puede cambiar el par activo en un clúster haciendo clic en la flecha giratoria además del icono del lápiz.

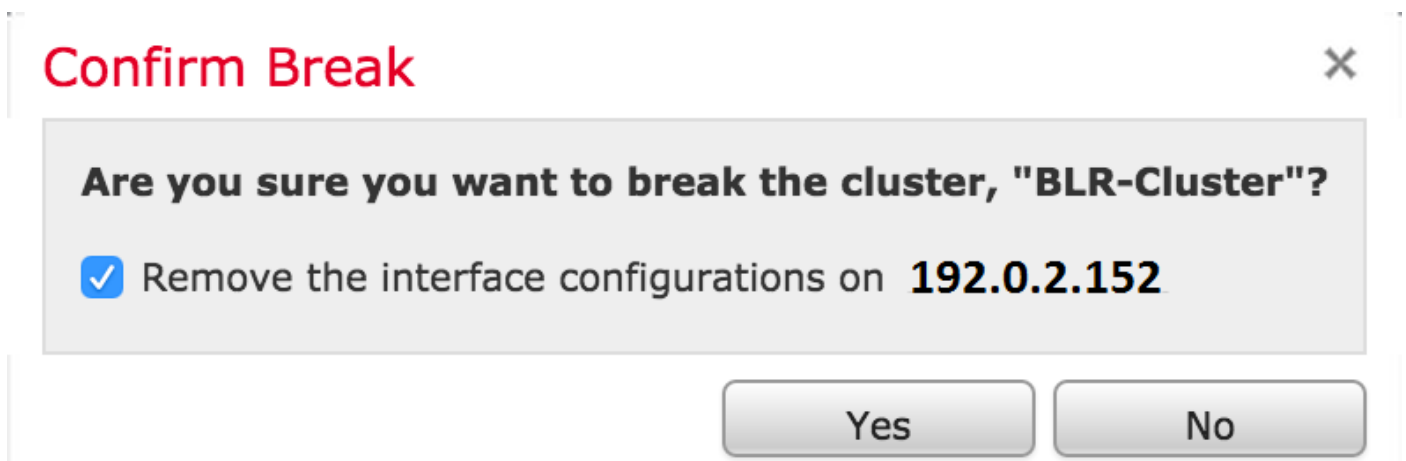
| BLR-Cluster 3D7010 Cluster | | | | ✓ ✎ 🗑️ 📄 | |
|---|----------------------------------|------------|---------------------------------------|--------------------------|---|
| ✓ 192.0.2.112 (active) 192.0.2.112 - 3D7010 - v5.4.0.3 | Protection, Control, Malware,... | Stack Test | Initial_System_Policy 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 | 🔗 |

Romper un clúster

Puede romper un clúster haciendo clic en la opción Romper clúster además del icono de papelera de reciclaje.

| BLR-Cluster 3D7010 Cluster | | | | ✓ ✎ 🗑️ 📄 | |
|---|----------------------------------|------------|---------------------------------------|--------------------------|---|
| ✓ 192.0.2.112 (active) 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 | 🔗 |

Después de hacer clic en el icono de papelera de reciclaje, se le pedirá que quite la configuración de la interfaz del dispositivo de copia de seguridad. Seleccione **Yes** o **No**.



También puede eliminar un clúster y anular el registro de los dispositivos del centro de administración haciendo clic en la **papelera de reciclaje**.

Si su dispositivo ha perdido acceso al Management Center, puede interrumpir la agrupación en clúster mediante el siguiente comando de la CLI:

```
> configure clustering disable
```

Compartir el estado

El uso compartido de estado agrupado permite que los dispositivos agrupados o las pilas agrupadas sincronicen los estados, de modo que si uno de los dispositivos o la pila falla, el otro par puede asumir el control sin interrumpir el flujo de tráfico.

Nota: Debe configurar y habilitar las interfaces de enlace de alta disponibilidad (HA) en ambos dispositivos o en los dispositivos apilados principales del clúster antes de configurar el uso compartido de estado en clúster.

Precaución: La habilitación del uso compartido de estado ralentiza el rendimiento del sistema.

Para habilitar el uso compartido de estado en un link HA, siga estos pasos:

1. Vaya a **Dispositivos > Administración de dispositivos**. Seleccione el clúster y edite.
2. Seleccione la pestaña **Interfaces**.
3. Seleccione el enlace que desea realizar como enlace HA.
4. Haga clic en **editar** (icono del lápiz). Aparece la ventana **Editar interfaz**.

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. Después de habilitar el enlace y configurar otras opciones, haga clic en **Guardar**.

6. Ahora navegue a la pestaña **Clúster**. Verá una sección llamada **Compartir estado** a la sección derecha de la página.

State Sharing

| | |
|---------------------------------|--|
| Enabled: | No |
| Statistics: |  |
| HA Link |  (s1p3) |
| Minimum Flow Lifetime: | 1000 ms |
| Minimum Sync. Interval: | 100 ms |
| Maximum HTTP URL Length: | 32 |



7. Haga clic en el **icono del lápiz** para editar las opciones de uso compartido de estado.

8. Asegúrese de que la opción **Enabled** esté marcada.

9. Opcionalmente, puede cambiar la duración del flujo, el intervalo de sincronización y la longitud máxima de URL HTTP.

El uso compartido de estados está ahora habilitado. Puede comprobar las estadísticas del tráfico haciendo clic en el icono de lupa situado junto a Estadísticas. Verá las estadísticas de tráfico para ambos dispositivos como se muestra a continuación.

State Sharing Statistics ? x

| | Active Peer | Backup Peer |
|------------------------------------|--|--|
| Device | 10.122.144.203  | 10.122.144.204  |
| Messages Received (Unicast) | 0 | 0 |
| Packets Received | 0 | 0 |
| Total Bytes Received | 0 | 0 |
| Protocol Bytes Received | 0 | 0 |
| Messages Sent | 0 | 0 |
| Packets Sent | 0 | 0 |
| Bytes Sent | 0 | 0 |
| TX Errors | 0 | 0 |
| TX Overruns | 0 | 0 |
| Recent Logs | View | View |

Refresh

Close

Cuando se habilita el uso compartido de estado y se desactiva una interfaz en el miembro activo, todas las conexiones TCP se transfieren al dispositivo en espera que ahora se ha convertido en activo.

Resolución de problemas

El dispositivo no está configurado correctamente

Si uno de los [requisitos previos](#) no se cumple, aparece el siguiente mensaje de error:

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

En el Management Center, navegue hasta **Devices > Device Management** y verifique si ambos dispositivos tienen las mismas versiones de software, modelos de hardware, licencias y políticas.

Alternativamente, en un dispositivo, puede ejecutar el siguiente comando para verificar la política de control de acceso aplicada y la versión de hardware y 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
.
```

Para verificar la política NAT, ejecute el siguiente comando en el dispositivo:

> `show nat config`

Nota: Las licencias sólo se pueden comprobar en el Management Center, ya que las licencias se almacenan sólo en el Management Center.

Todos los miembros de HA deben tener políticas actualizadas

Otro error que puede encontrar es el siguiente

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

Este error se produce cuando las políticas de control de acceso no están actualizadas. Vuelva a aplicar las políticas y repita la configuración del clúster.

Documentos Relacionados

- [Dispositivo de clustering: guía del usuario del sistema FireSIGHT](#)