

# 在Cisco FirePOWER 7000和8000系列设备上配置集群

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[添加集群](#)

[中断集群](#)

[共享状态](#)

[故障排除](#)

[设备配置不正确](#)

[所有HA成员必须具有最新策略](#)

[相关文档](#)

## 简介

设备集群在两台设备或堆栈之间提供配置和网络功能的冗余。本文介绍如何在Cisco Firepower 7000和8000系列设备上配置集群。

## 先决条件

在尝试建立集群之前，必须熟悉集群的各种功能。Cisco建议您阅读《FireSIGHT系统[用户指南](#)》的“集群设备”部分以了解详细信息。

## 要求

两台设备必须具有以下相同的组件：

1. 相同的硬件型号  
**注意：**不能在集群中配置堆栈和单台设备。它们必须位于同一类型或两个相似单一设备的堆栈中。
2. 在完全相同的插槽中使用相同的网络模块（网络模块）  
**注意：**检查集群的必备条件时，不考虑堆叠网络模块。它们被视为与空插槽相同。
3. 相同的许可证，它们必须完全相同。如果一台设备有额外的许可证，则无法形成集群。
4. 相同的软件版本
5. 相同的VDB版本
6. 相同的NAT策略（如果已配置）

## 使用的组件

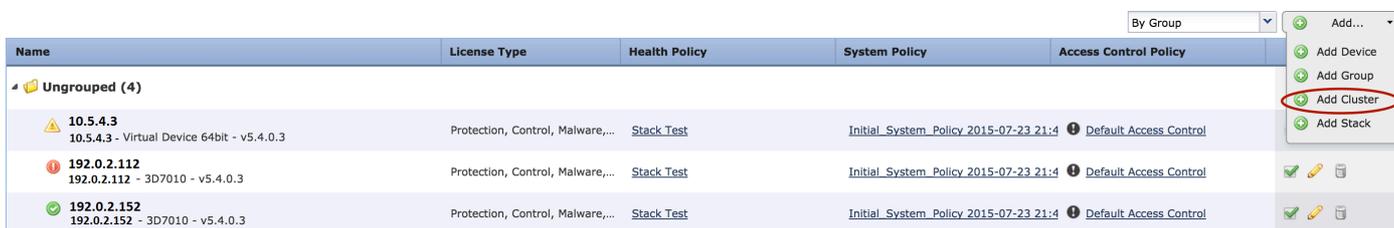
- 两个Cisco Firepower 7010，版本5.4.0.4
- FireSIGHT管理中心5.4.1.3

注意：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

### 添加集群

1. 导航至“设备”>“设备管理”。
2. 选择要集群的设备。在页面右上角，选择“添加”下拉列表。
3. 选择“添加集群”。

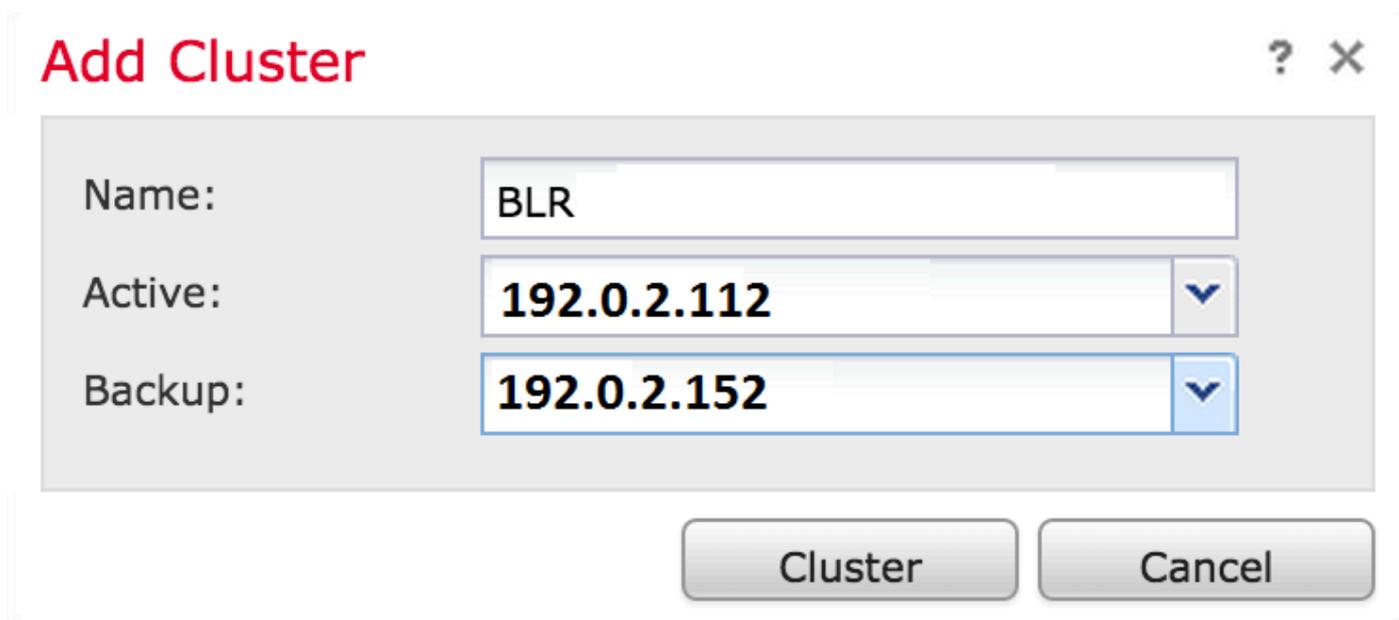


Name	License Type	Health Policy	System Policy	Access Control Policy
Ungrouped (4)				
10.5.4.3 10.5.4.3 - Virtual Device 64bit - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial_System_Policy_2015-07-23_21:4	Default Access Control
192.0.2.112 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control,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

- Add...
- Add Device
- Add Group
- Add Cluster**
- Add Stack

4. 出现“添加集群”弹出窗口。您将看到以下屏幕。提供活动和备份设备的IP地址。



### Add Cluster

Name:

Active:

Backup:

5. 单击“集群”按钮。如果满足所有必备条件，您将看到“添加集群状态”窗口，最长10分钟。

# Please Wait...

## Adding cluster...



6.成功创建集群后，您将在“设备管理”页中找到更新的设备。

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.除铅笔图标外，单击旋转箭头可切换集群中的活动对等体。

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	

## 中断集群

您可以通过点击除回收站图标外的Break集群选项来中断集群。

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	

点击回收站图标后，系统将要求您从备份设备中删除接口配置。选择是或否。

## Confirm Break



Are you sure you want to break the cluster, "BLR-Cluster"?

Remove the interface configurations on **192.0.2.152**

Yes

No

您还可以通过单击回收站从管理中心删除集群和取消注册设备。

如果设备无法访问管理中心，您可以在CLI上使用以下命令中断集群：

> configure clustering disable

## 共享状态

集群状态共享允许集群设备或集群堆栈同步状态，这样，如果其中一个设备或堆栈发生故障，另一个对等设备就可以在流量传输不中断的情况下接管。

**注意：**在配置集群状态共享之前，必须在两台设备或集群中的主堆叠设备上配置并启用高可用性(HA)链路接口。

**警告：**启用状态共享会降低系统性能。

要在HA链路上启用状态共享，请执行以下步骤：

1. 导航至“设备”>“设备管理”。选择集群并编辑。
2. 选择“接口”选项卡。
3. 选择要作为HA链接的链路。
4. 单击编辑(铅笔图标)。系统将显示“编辑接口”窗口。

### Edit Interface



None Passive Inline Switched Routed HA Link

Enabled:

Mode: Autonegotiation

MDI/MDIX: Auto-MDIX

MTU: 9922

Save Cancel

5. 启用链接并配置其他选项后，单击**Save**。

6. 现在导航至“集群”选项卡。您将在页面右侧看到一个名为“状态共享”的部分。

## State Sharing



**Enabled:** No

**Statistics:**



**HA Link**  (s1p3)

**Minimum Flow Lifetime:** 1000 ms

**Minimum Sync. Interval:** 100 ms

**Maximum HTTP URL Length:** 32

7.单击铅笔图标可编辑状态共享选项。

8.确保选中“启用”选项。

9.或者，您可以更改“流生存期”、“同步间隔”和“最大HTTP URL长度”。

状态共享现已启用。您可以通过点击Statistics旁边的放大镜图标来检查流量统计信息。您将看到两个设备的流量统计信息，如下所示。

### State Sharing Statistics



	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	<a href="#">View</a>	<a href="#">View</a>

Refresh Close

启用状态共享后，活动成员上的接口关闭，所有TCP连接都会传输到现在已变为活动状态的备用设备。

## 故障排除

## 设备配置不正确

如果其中一个必备条件未执行，则显示以下错误消息：

### 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

在管理中心上，导航至**Devices > Device Management**，并验证两台设备是否具有相同的软件版本、硬件型号、许可证和策略。

或者，在设备上，可以运行以下命令来验证应用的访问控制策略以及硬件和软件版本：

```
> 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
.
```

要验证NAT策略，请在设备上运行以下命令：

```
> show nat config
```

**注意：**许可证只能在管理中心上检查，因为许可证只存储在管理中心上。

## 所有HA成员必须具有最新策略

您可能会遇到的另一个错误是：

## 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

当访问控制策略不是最新时，会发生此错误。重新应用策略并重新尝试集群配置。

## 相关文档

- [集群设备 — FireSIGHT系统用户指南](#)