

Konfiguration des Clustering auf Cisco FirePOWER-Geräten der Serien 7000 und 8000

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Hinzufügen eines Clusters](#)

[Brechen eines Clusters](#)

[Teilen des Staates](#)

[Fehlerbehebung](#)

[Gerät ist nicht richtig konfiguriert](#)

[Alle HA-Mitglieder müssen über aktuelle Richtlinien verfügen.](#)

[Verwandte Dokumente](#)

Einführung

Das Clustering von Geräten ermöglicht die Redundanz der Konfigurations- und Netzwerkfunktionen zwischen zwei Geräten oder Stacks. In diesem Artikel wird beschrieben, wie Sie Clustering auf Geräten der Cisco Firepower 7000- und 8000-Serie konfigurieren.

Voraussetzungen

Bevor Sie versuchen, einen Cluster einzurichten, müssen Sie mit verschiedenen Clustering-Funktionen vertraut sein. Cisco empfiehlt, den Abschnitt [Clustering-Geräte](#) im FireSIGHT System-Benutzerhandbuch für weitere Informationen zu lesen.

Anforderungen

Beide Geräte müssen über die folgenden identischen Komponenten verfügen:

1. Dieselben Hardwaremodelle
Hinweis: Ein Stack und ein einzelnes Gerät können nicht in einem Cluster konfiguriert werden. Sie müssen sich im Stack desselben Typs oder zwei ähnlichen Einzelgeräten befinden.
2. Dieselben Netzwerkmodule (Netmod) in exakt denselben Steckplätzen
Hinweis: Stacking-Netzwerkmodule werden nicht berücksichtigt, wenn die Voraussetzungen für Cluster überprüft werden. Sie gelten als gleiche wie ein leerer Steckplatz.
3. Die gleichen Lizenzen müssen identisch sein. Wenn ein Gerät über eine zusätzliche Lizenz verfügt, kann der Cluster nicht gebildet werden.
4. Dieselben Softwareversionen

5. Gleiche VDB-Versionen
6. Dieselbe NAT-Richtlinie (falls konfiguriert)

Verwendete Komponenten

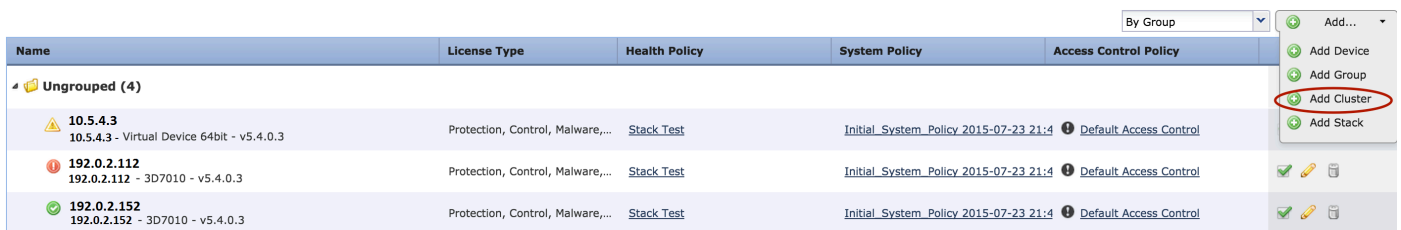
- Zwei Cisco Firepower 7010 in Version 5.4.0.4
- FireSIGHT Management Center 5.4.1.3

Hinweis: Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfiguration

Hinzufügen eines Clusters

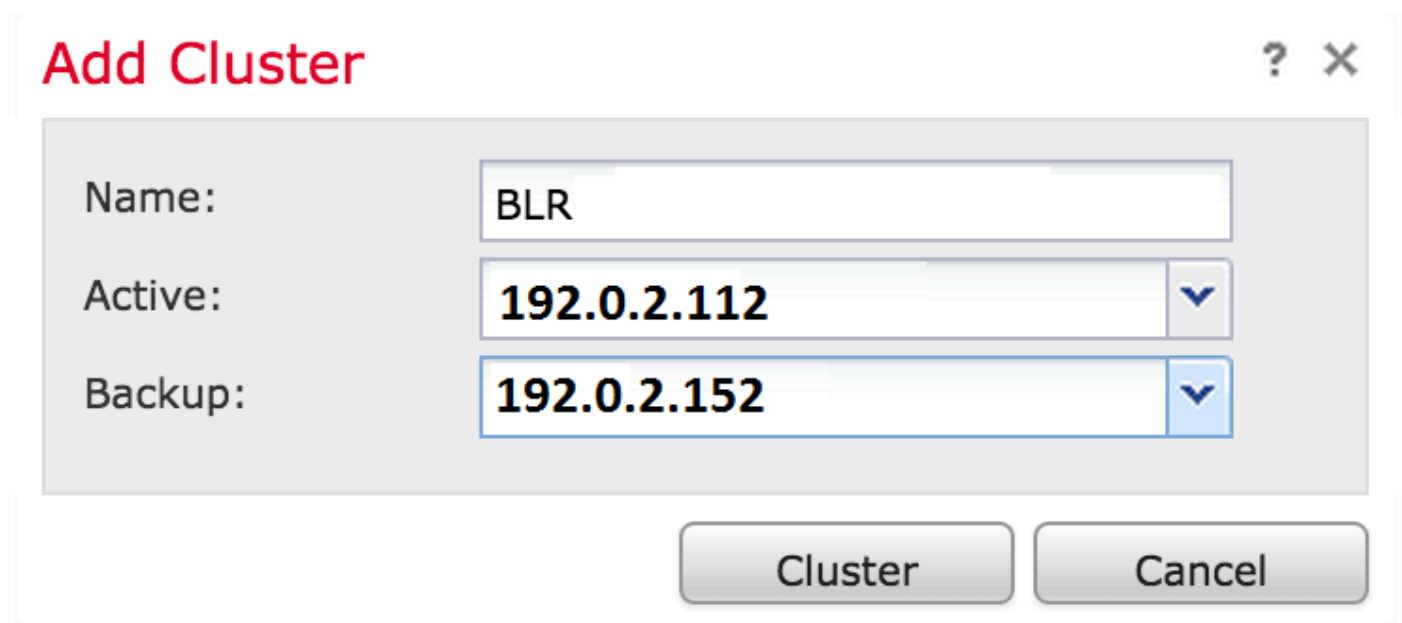
1. Navigieren Sie zu **Gerät > Gerätemanagement**.
2. Wählen Sie die Geräte aus, die Sie einem Cluster hinzufügen möchten. Wählen Sie oben rechts auf der Seite die Dropdown-Liste **Hinzufügen aus**.
3. Wählen Sie **Cluster hinzufügen aus**.



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

4. Das Popup-Fenster **Cluster hinzufügen** wird angezeigt. Sie sehen den folgenden Bildschirm. Geben Sie die IP-Adressen der aktiven Geräte und der Backup-Geräte an.



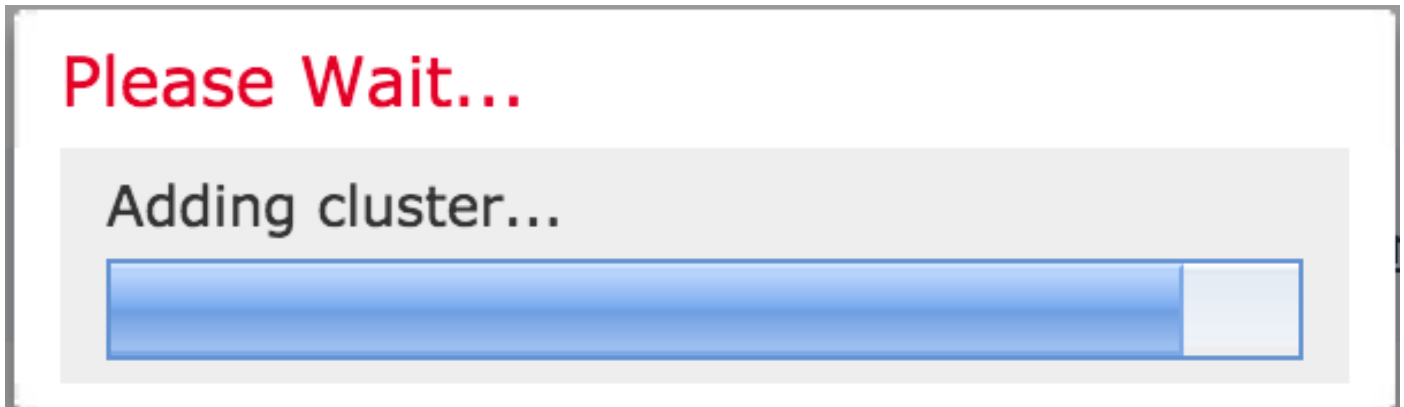
Add Cluster [?] [X]

Name:

Active: [v]

Backup: [v]

5. Klicken Sie auf die Schaltfläche **Cluster**. Wenn alle Voraussetzungen erfüllt sind, wird das Statusfenster **Cluster-Hinzufügen** für bis zu 10 Minuten angezeigt.



6. Sobald der Cluster erfolgreich erstellt wurde, finden Sie die aktualisierten Geräte auf der Seite "Gerätemanagement".

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. Sie können den aktiven Peer in einem Cluster wechseln, indem Sie auf den rotierenden Pfeil neben dem Bleistiftsymbol klicken.

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	

Brechen eines Clusters

Sie können einen Cluster unterbrechen, indem Sie neben dem Recyclingbin-Symbol auf die Option Break Cluster (Cluster abbrechen) klicken.

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	

Wenn Sie auf das Papierkorb-Symbol klicken, werden Sie aufgefordert, die Schnittstellenkonfiguration vom Sicherungsgerät zu entfernen. Wählen Sie **Ja** oder **Nein** aus.

Confirm Break



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

Remove the interface configurations on **192.0.2.152**

Yes

No

Sie können auch einen Cluster löschen und die Registrierung der Geräte im Management Center aufheben, indem Sie auf den **Papierkorb** klicken.

Wenn Ihr Gerät den Zugriff auf das Management Center verloren hat, können Sie das Clustering mithilfe des folgenden Befehls in der CLI unterbrechen:

```
> configure clustering disable
```

Teilen des Staates

Die gemeinsame Nutzung im Cluster-Zustand ermöglicht den geclusterten Geräten oder Cluster-Stacks die Synchronisierung der Zustände, sodass der andere Peer bei Ausfall eines der Geräte oder des Stacks den Datenverkehrsfluss ohne Unterbrechung übernehmen kann.

Hinweis: Sie müssen die Hochverfügbarkeits-Verbindungsschnittstellen auf beiden Geräten oder auf den primären Stack-Geräten im Cluster konfigurieren und aktivieren, bevor Sie die geclusterte Zustandsfreigabe konfigurieren.

Vorsicht: Die Aktivierung der Zustandsfreigabe verlangsamt die Systemleistung.

Um die Zustandsfreigabe auf einem HA-Link zu aktivieren, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Geräte > Gerätemanagement**. Wählen Sie den Cluster aus, und bearbeiten Sie ihn.
2. Wählen Sie die Registerkarte **Schnittstellen** aus.
3. Wählen Sie den Link aus, den Sie als HA-Link erstellen möchten.
4. Klicken Sie auf **Bearbeiten** (Bleistiftsymbol). Das Fenster **Schnittstelle bearbeiten** wird angezeigt.

Edit Interface



None Passive Inline Switched Routed **HA Link**

Enabled:

Mode: Autonegotiation

MDI/MDIX: Auto-MDIX

MTU: 9922

Save Cancel

5. Wenn Sie den Link aktiviert und andere Optionen konfiguriert haben, klicken Sie auf **Speichern**.
6. Navigieren Sie jetzt zur Registerkarte **Cluster**. Im rechten Bereich der Seite wird der Abschnitt **Zustandsfreigabe** angezeigt.

State Sharing



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

7. Klicken Sie auf das **Bleistiftsymbol**, um die Zustandsfreigabeoptionen zu bearbeiten.
8. Stellen Sie sicher, dass die Option **Aktiviert** aktiviert ist.
9. Optional können Sie die Flusslebensdauer, das Synchronisierungsintervall und die maximale HTTP-URL-Länge ändern.

Die Statusfreigabe ist jetzt aktiviert. Sie können Verkehrsstatistiken überprüfen, indem Sie auf das Lupensymbol neben Statistik klicken. Sie sehen die Verkehrsstatistik für beide Geräte, wie unten gezeigt.

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	View	View

Refresh

Close

Wenn die Statusfreigabe aktiviert ist und eine Schnittstelle auf dem aktiven Mitglied ausfällt, werden alle TCP-Verbindungen auf das Standby-Gerät übertragen, das jetzt aktiv geworden ist.

Fehlerbehebung

Gerät ist nicht richtig konfiguriert

Wenn eine der [Voraussetzungen](#) nicht erfüllt ist, wird die folgende Fehlermeldung angezeigt:

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

Navigieren Sie im Management Center zu **Devices > Device Management** (Geräte >

Gerätemanagement), und überprüfen Sie, ob beide Geräte über dieselben Softwareversionen, Hardwaremodelle, Lizenzen und Richtlinien verfügen.

Alternativ können Sie auf einem Gerät den folgenden Befehl ausführen, um die angewendete Zugriffskontrollrichtlinie und die Hardware- und Softwareversion zu überprüfen:

```
> 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
.
```

Führen Sie zum Überprüfen der NAT-Richtlinie auf dem Gerät den folgenden Befehl aus:

```
> show nat config
```

Hinweis: Die Lizenzen können nur im Management Center geprüft werden, da die Lizenzen nur im Management Center gespeichert sind.

Alle HA-Mitglieder müssen über aktuelle Richtlinien verfügen.

Ein weiterer Fehler, auf den Sie möglicherweise stoßen, ist der folgende:

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

Dieser Fehler tritt auf, wenn die Zugriffskontrollrichtlinien nicht auf dem neuesten Stand sind. Wenden Sie die Richtlinien erneut an, und versuchen Sie es erneut.

Verwandte Dokumente

- [Clustering-Gerät - Benutzerhandbuch zum FireSIGHT-System](#)