Cisco FirePOWER 7000 および 8000 シリーズのデバイスでのクラスタリングの設定

内容

概要

デバイスのクラスタリングにより、2 つのデバイスまたはスタック間の構成およびネットワーク機能の冗長性を提供します。この記事では、Cisco Firepower 7000および8000シリーズデバイスでクラスタリングを設定する方法について説明します。

前提条件

クラスタを確立する前に、クラスタリングのさまざまな機能に精通している必要があります。詳細については、『FireSIGHT System User Guide』の「Clustering Device」セクションを参照することをお勧めします。

要件

両方のデバイスは、次の同じコンポーネントを備えている必要があります。

1. 同じハードウェアモデル
   注：スタックと1つのデバイスをクラスタ内で設定することはできません。同じタイプのスタックまたは2つの類似した単一デバイスに存在する必要があります。
2. 同じスロットに同じネットワークモジュール(Netmod)
   注：クラスタの前提条件をチェックする際には、netmodsのスタック構成は考慮されません。これらは空のスロットと同じとみなされます。
3. 同じライセンスで、まったく同じでなければなりません。1つのデバイスに追加ライセンスがある場合、クラスタを形成できません。
4. 同じソフトウェアバージョン
5. 同じVDBバージョン

6. 同じNATポリシー（設定されている場合）

使用するコンポーネント

- バージョン5.4.0.4の2台のCisco Firepower 7010
- FireSIGHT Management Center 5.4.1.3

注：このドキュメントの情報は、特定のラボ環境のデバイスから作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

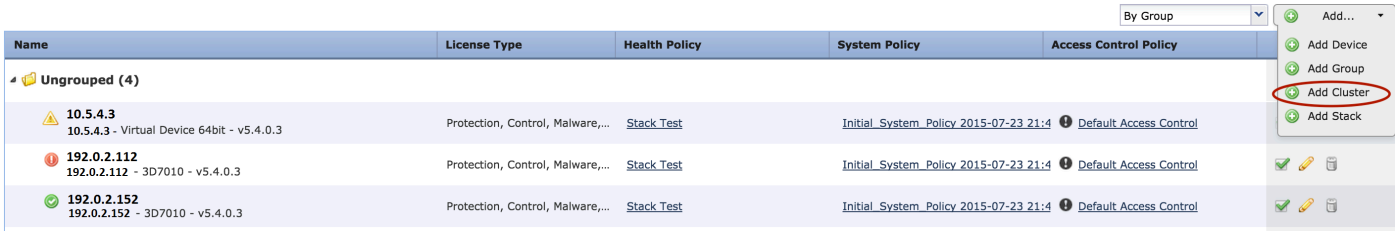
コンフィギュレーション

クラスタの追加

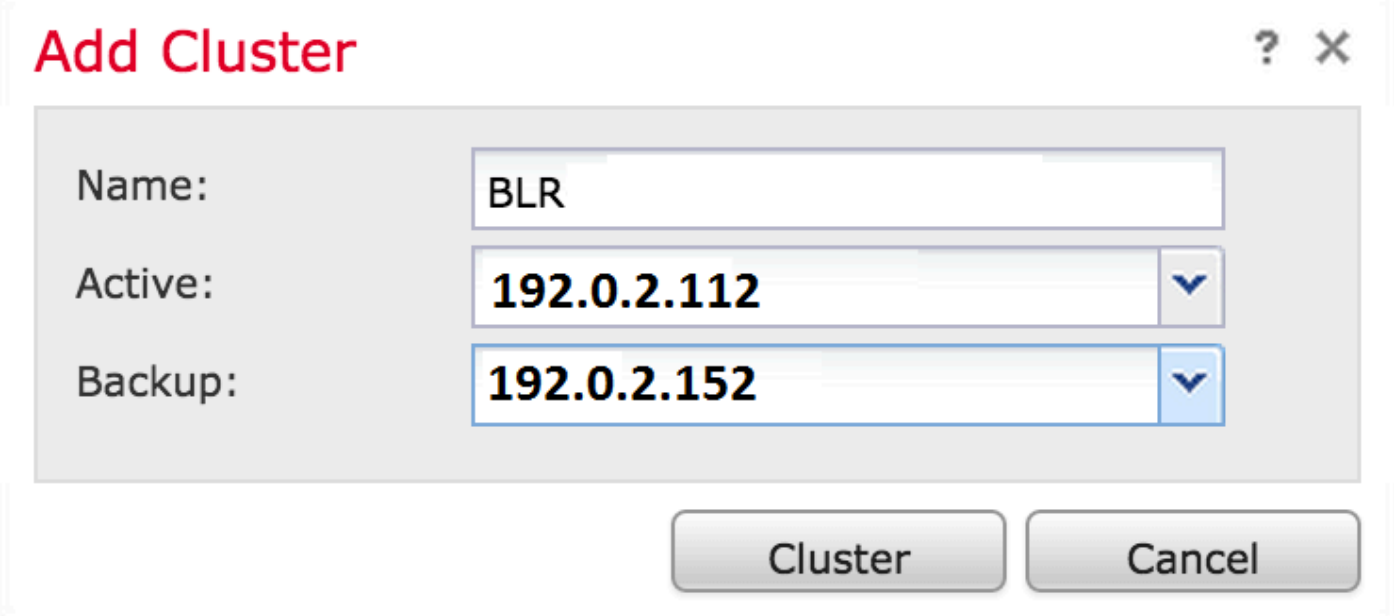
1. [Device] > [**Device Management]に移動します。**

2.クラスタ化するデバイスを選択します。ページの右上で、[追加]ドロップダウン**リスト**を選択します。

3. 「クラスタの追**加」を選択します。**

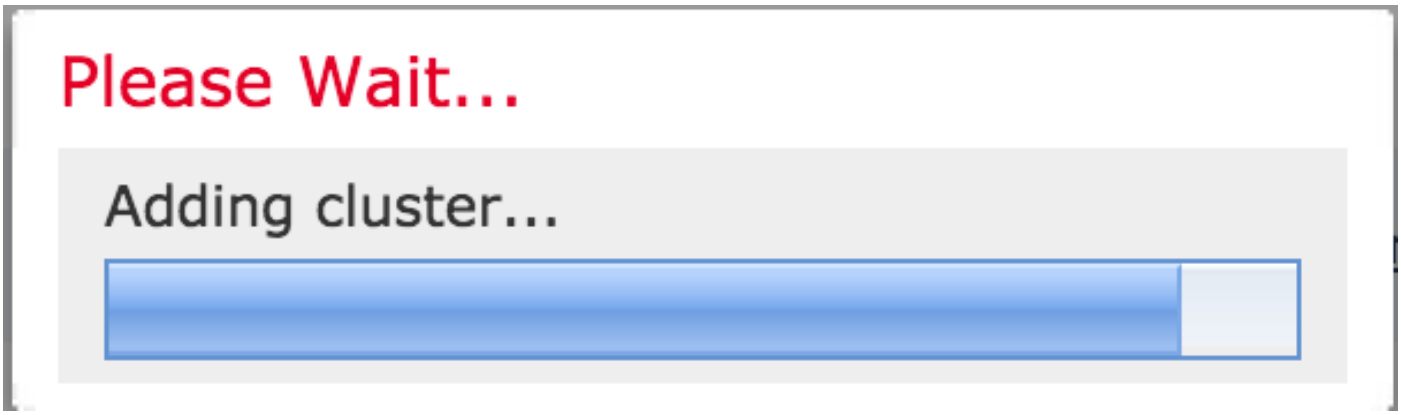


4. [クラスタの追**加]ポップアップウ**ィンドウが表示されます。次の画面が表示されます。アクティブデバイスとバックアップデバイスのIPアドレスを指定します。

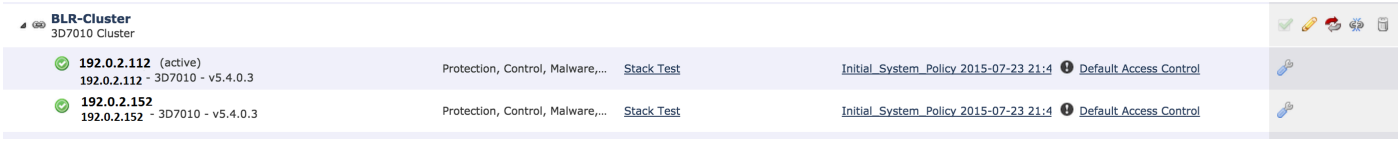


5. 「クラスタ」ボタンを**クリック**します。すべての前提条件が満たされている場合は、最大10分

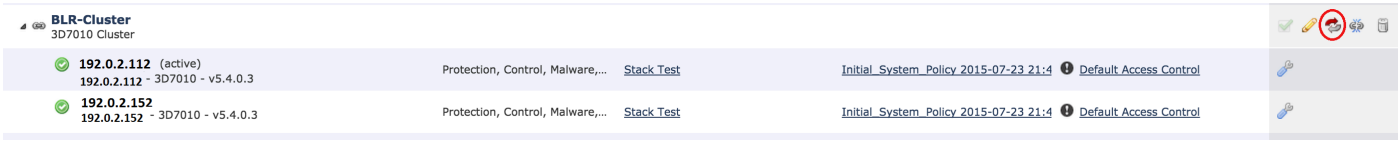
間の[クラスターの追加]ステータスウィンドウが表示されます。



6.クラスタが正常に作成されると、[デバイスの管理]ページで更新されたデバイスが検索されます。

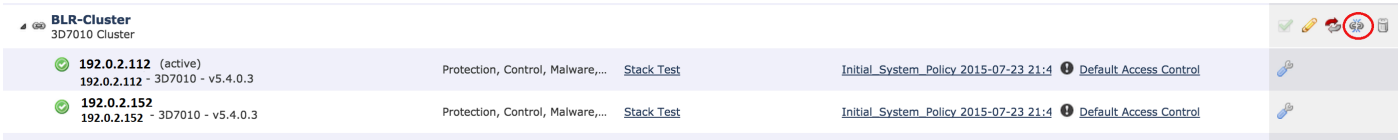


7.鉛筆アイコンの横にある回転矢印をクリックすると、クラスタ内のアクティブピアを切り替えることができます。

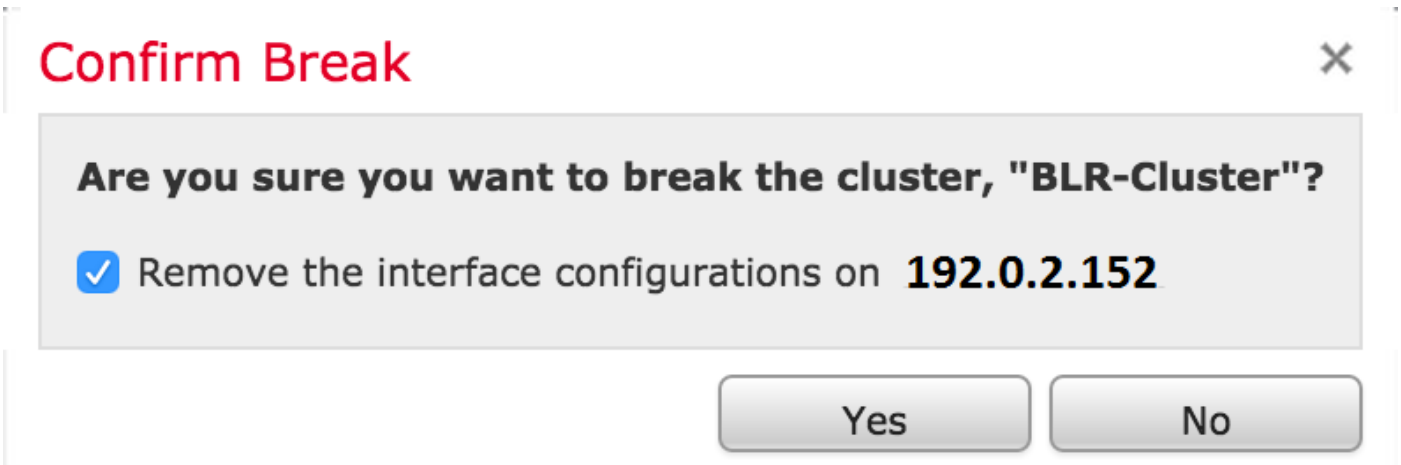


クラスタの分割

[ごみ箱]アイコンの横にある[クラスタの解除]オプションをクリックすると、クラスタを解除できます。



ごみ箱アイコンをクリックすると、バックアップデバイスからインターフェイス設定を削除するように求められます。[はい]または[いいえ]を選択します。



また、ごみ箱をクリックして、クラスタを削除し、管理センターからデバイスを登録解除することもできます。

デバイスからManagement Centerへのアクセスが失われた場合は、CLIで次のコマンドを使用してクラスタリングを解除できます。

```
> configure clustering disable
```

状態の共有

クラスタ化された状態共有では、クラスタ化されたデバイスまたはスタックの状態を同期できるため、デバイスまたはスタックの1つに障害が発生した場合、他のピアがトラフィックフローを中断することなく引き継ぐことができます。

> **注**：クラスタ状態共有を設定する前に、クラスタ内の両方のデバイスまたはプライマリスタックデバイスでハイアベイラビリティ(HA)リンクインターフェイスを設定して有効にする必要があります。

> **注意**：状態共有を有効にすると、システムのパフォーマンスが低下します。

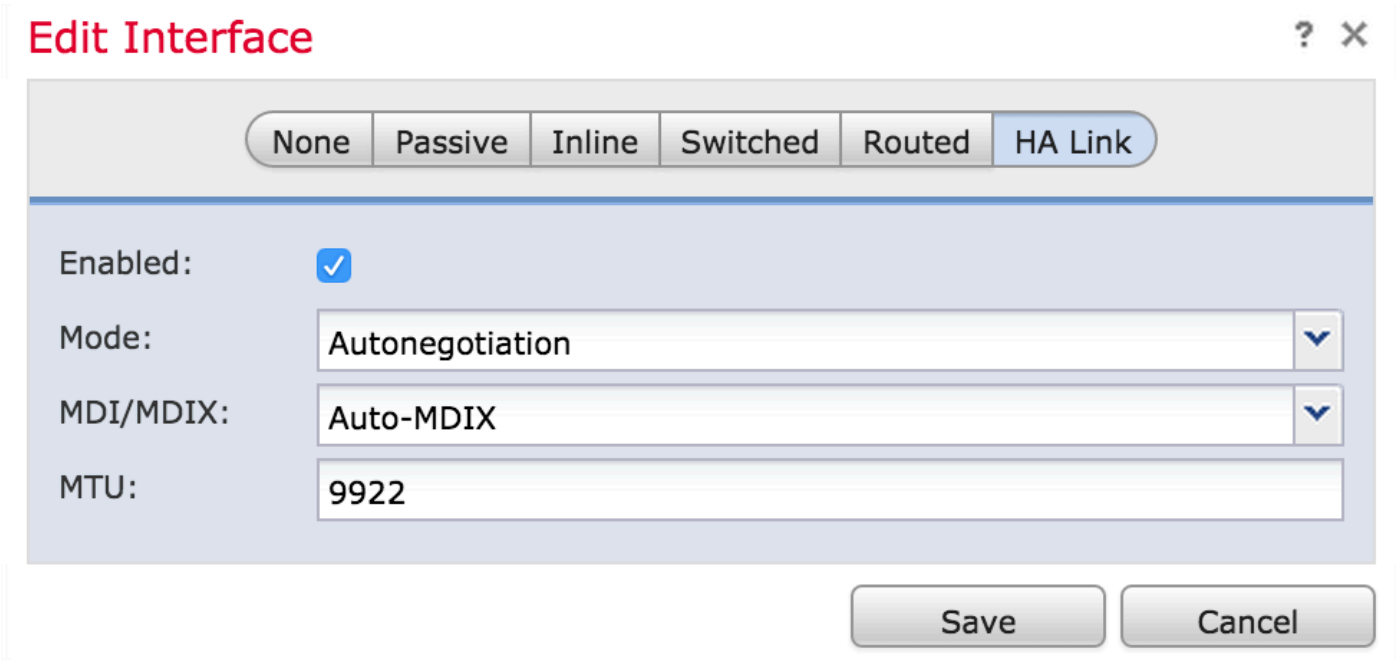
HAリンクで状態共有を有効にするには、次の手順を実行します。

1. [Devices] > [Device Management]に移動します。クラスタを選択して編集します。

2. 「インタフェース」タブを選択します。

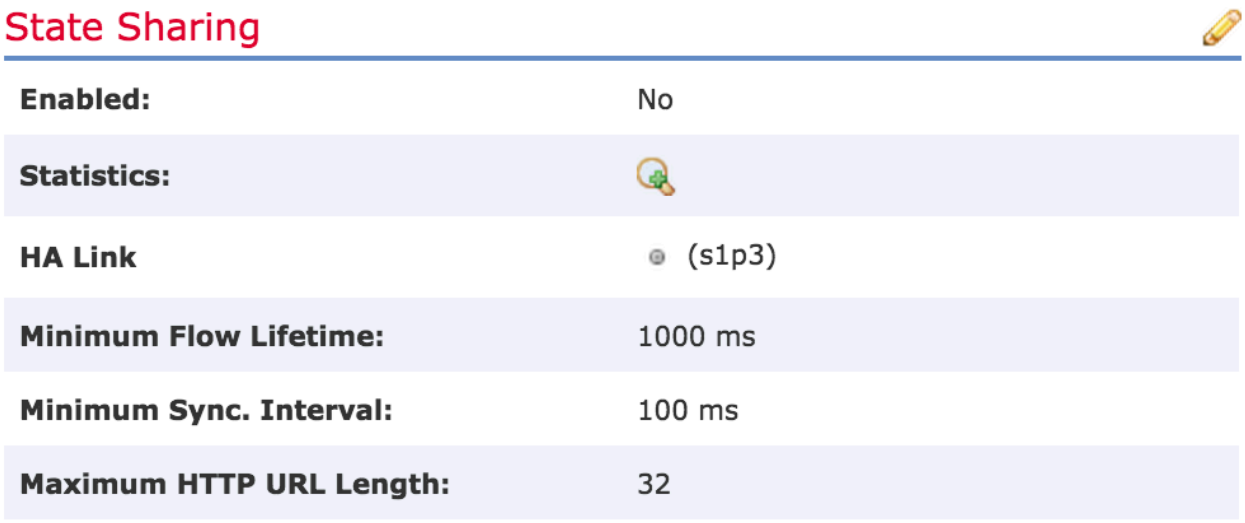
3. HAリンクとして作成するリンクを選択します。

4. 「edit」(鉛筆アイコン)をクリックします。 [インターフェイスの編集]ウィンドウが表示されます。



5.リンクを有効にして他のオプションを構成したら、[保存]をクリックします。

6. 「クラスタ」タブに移動します。ページの右側のセクションにState Sharingというセクションが表示されます。

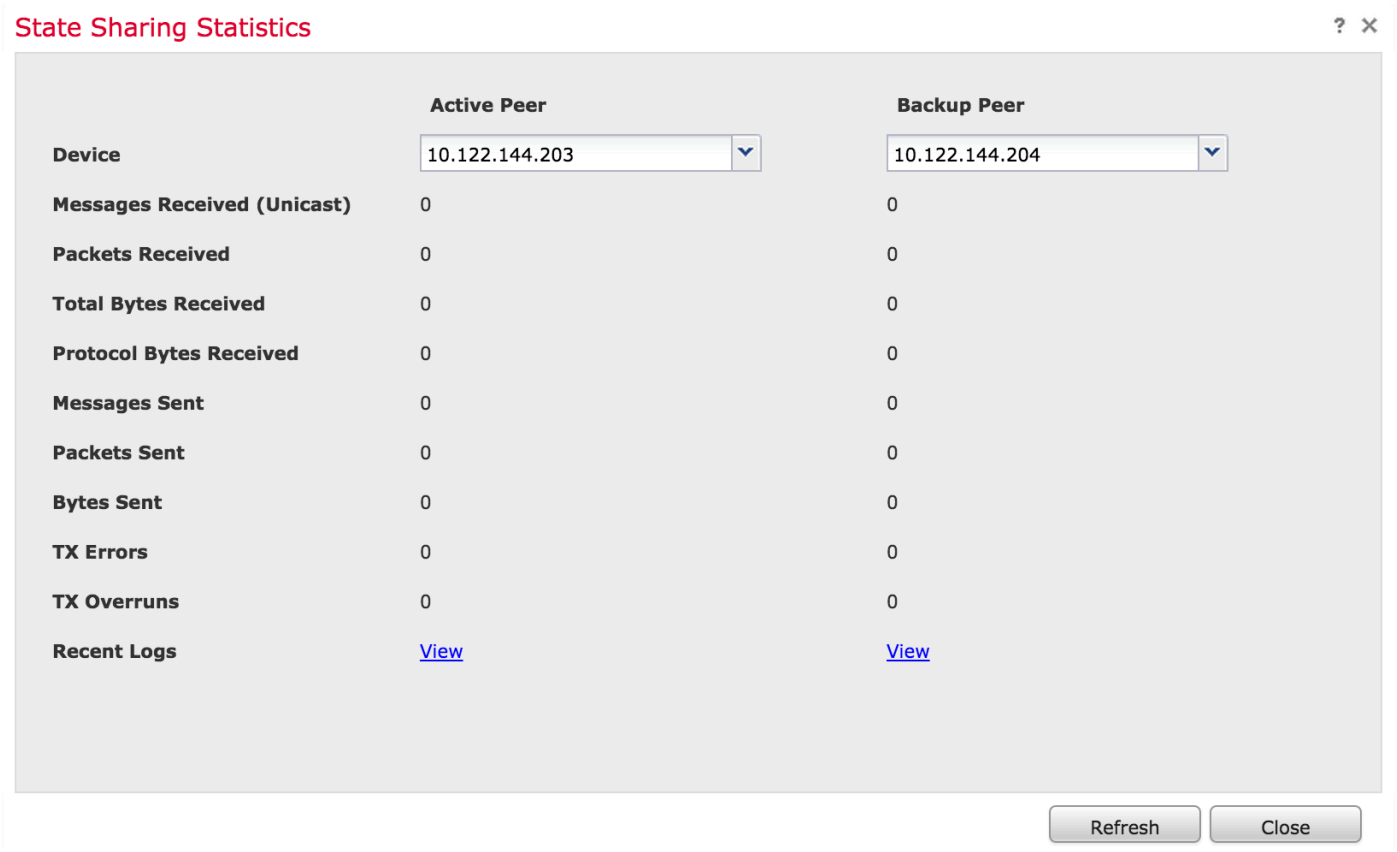


7.鉛筆アイコンをクリックして、状態共有オプションを編集します。

8. [有効]オプションがオンになっていることを確認してください。

9.オプションで、[Flow Lifetime]、[Sync Interval]、および[Max HTTP URL Length]を変更できます。

状態共有が有効になりました。トラフィックの統計情報を確認するには、[Statistics]の横にある虫眼鏡のアイコンをクリックします。次に示すように、両方のデバイスのトラフィック統計情報が表示されます。

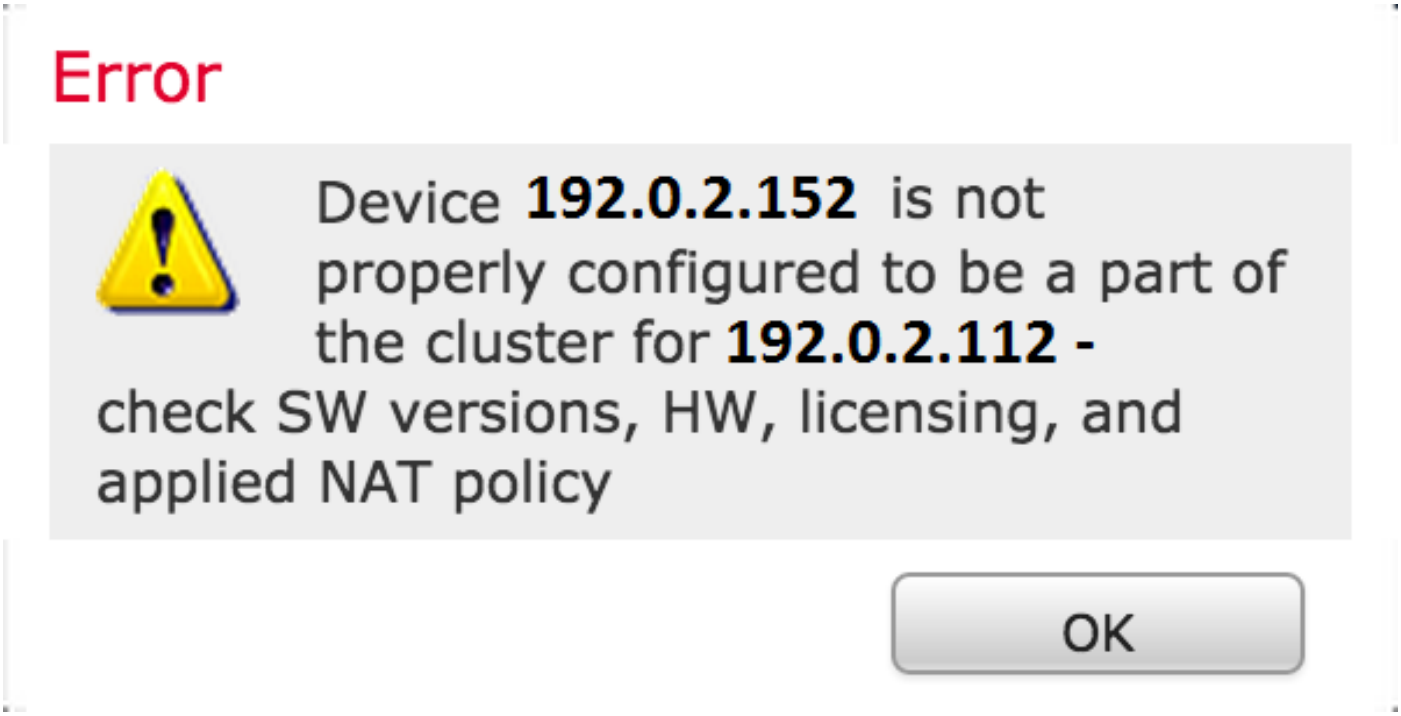


状態共有が有効で、アクティブメンバのインターフェイスがダウンすると、すべてのTCP接続がスタンバイデバイスに転送され、スタンバイ側デバイスはアクティブになります。

トラブルシューティング

デバイスが正しく設定されていない

前提条件のいずれかが満たされない場合は、次のエラーメッセージが表示されます。



Management Centerで、[Devices] > [Device Management] に移動し、両方のデバイスのソフトウェアバージョン、ハードウェアモデル、ライセンス、およびポリシーが同じかどうかを確認します。

または、デバイスで次のコマンドを実行して、適用されたアクセスコントロールポリシーとハードウェアおよびソフトウェアのバージョンを確認できます。

```
> 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
.
```

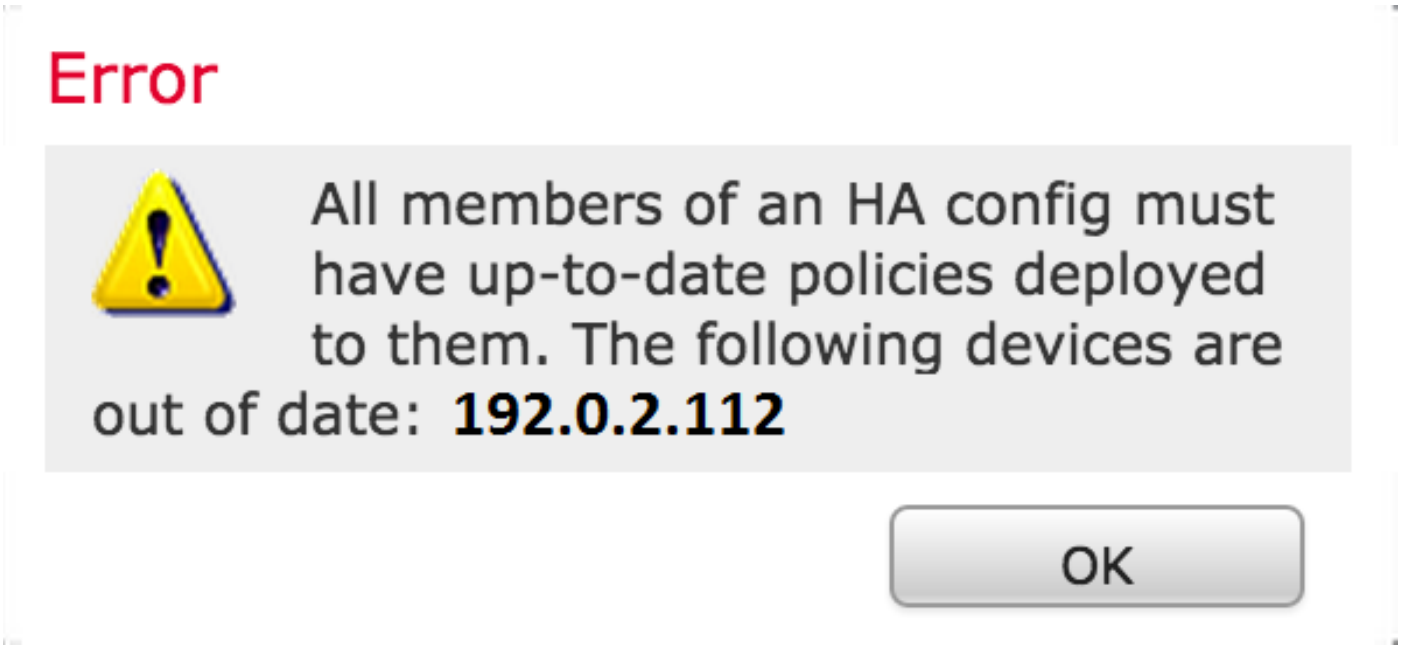
NATポリシーを確認するには、デバイスで次のコマンドを実行します。

```
> show nat config
```

注：ライセンスはManagement Centerにのみ保存されるため、ライセンスはManagement Centerでのみ確認できます。

すべてのHAメンバーに最新のポリシーが必要

次のエラーも発生する可能性があります



このエラーは、アクセスコントロールポリシーが最新でない場合に発生します。ポリシーを再適用し、クラスタ設定を再試行します。

関連資料

- クラスタリングデバイス – FireSIGHTシステムユーザガイド