

# FDMでの高可用性ペアリング障害のトラブルシューティング

## 内容

---

## 問題

FTD 7.4.2.4を実行している2台のCisco Firepower 1120アプライアンス間のハイアベイラビリティ (HA)ペアリングが、アプリケーションの同期中に失敗し、ライセンス登録モードの不一致が原因でセカンダリノードが継続的に障害状態になります。発生したエラーメッセージは次のとおりです。

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

show app-sync-historyコマンドは、次のようなメッセージの繰り返し失敗を明らかにします。

```
App Sync Status: FAILURE
```

```
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

この問題は、両方のファイアウォールがリセットされ、設定がバックアップから復元され、ソフトウェアがFTDバージョン7.4.2.4にアップデートされ、VDBとSnortのバージョンがアップデートされ、ライセンスが新しいトークンで再適用された後に発生しました。セカンダリファイアウォールは障害状態のままであるため、HAが完了せず、ファイアウォールの冗長性に影響を与えます。

## 環境

- ハイアベイラビリティ向けに構成されたCisco Firepower 1120 NGFWアプライアンス
- Firepower Threat Defense(FTD)バージョン7.4.2.4-9

- Snortインスペクションエンジン : 3.1.53.203 - 175
- VDB: 425.0
- 位置情報データベース : 2026-03-07-053
- デバイスがスマートライセンスからPLR ( パーマネントライセンス予約 ) モードに変換される
- PLR変換後にクラウド接続を試行するプライマリデバイス
- 両方のデバイスがバックアップから復元された

## 解決方法

この問題の解決には、プライマリデバイスとセカンダリデバイス間のライセンス登録モードの不一致の特定と修正、クラウドの登録解除の実行、および完全な導入の完了が含まれます。

### ステップ1 : ライセンス登録モードの不一致を特定する

両方のデバイスでapp-sync-historyを確認して、特定の障害の原因についてライセンス登録モードを確認します。

```
show app-sync-history
```

出力は、次の障害を示しています。

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

### ステップ2 : クラウドの登録解除の実行

スマートライセンスからPLRモードに変換した後も、プライマリデバイスがクラウド接続を試行しているため、クラウドの登録解除が必要です。

FDM UIで一時プロキシを構成します ( プロキシが構成されていない場合 ) :

System Settings > See More > HTTP Proxy tabの順に移動し、一時的にダミープロキシを設定します[これは後で削除できます]。

FTDデバイスにSSHで接続し、コネクタスクリプトを実行します。

```
ssh admin@<device-ip>
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

### ステップ3 : ポート8989の競合の解決

コネクタスクリプトが次のエラーで失敗した場合 :

```
Error: listen tcp :8989: bind: address already in use
```

ポート8989 ( 通常はCisco Success Network ) を使用してプロセスを特定し、終了します。

```
netstat -tulpn | grep 8989
kill <pid>
```

### ステップ4 : クラウドの登録解除を完了する

ポートの競合を解決した後、コネクタスクリプトを再実行します。

```
/ngfw/var/sf/bin/connector.sh
```

実行が成功すると、次のような出力が表示されます。

Starting connector

INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https\_proxy=http://1xx.xx.x

INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http\_proxy=http://1xx.xx.x

FDM GUIの「システム設定」>「クラウド・サービス」>「クラウド・サービス」に移動し、「登録解除」オプションをクリックします。デバイスがクラウドサービスから登録解除されていることを確認します。

## ステップ5：完全導入の実行とHAの再開

クラウドの登録解除後も、HAペアリングが同じライセンス不一致エラーで失敗する場合は、FDMインターフェイスを使用してアクティブユニットで完全導入を実行します。

Deploy > Deploy Nowの順に移動し、導入プロセスを完了します。

導入が完了したら、HAの形成を再試行します。これらのデバイスは、接続されたインターフェイスを備え、準備完了状態のアクティブ/スタンバイHAペアを正常に形成する必要があります。

## ステップ6:HAステータスの確認

正常なHA形成を確認します。

```
show failover
```

出力には、同期が正常に行われ、両方のユニットが適切なHA状態で表示される必要があります。

## 原因

根本的な原因は、プライマリとセカンダリのFirepower 1120デバイス間のライセンス登録モードの不一致でした。デバイスはスマートライセンスからPLR（パーマネントライセンス予約）モードに変換されましたが、プライマリデバイスはクラウド接続の試行を続け、HA検証中にライセンスエージェント/エクスポートコンプライアンス状態の不一致が発生しました。これにより、アプ

リケーションの同期中にFDM/FIM検証エラーが繰り返し発生しました。さらに、クラウドの登録解除は当初、Cisco Success Networkに関連するポート8989の競合によってブロックされ、登録解除を続行するには解決が必要でした。

## 関連コンテンツ

- [エアギャップネットワークでの無期限ライセンスの適用](#)
- [セキュアなファイアウォール脅威対策の再イメージ化](#)
- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。