Firepower Management Center(FMC)での自動ダウンロード更新障害

内容

[概要](#)
[障害の考えられる原因](#)
[影響](#)
[確認](#)
[DNS設定の確認](#)
[接続の確認](#)
[トラブルシュート](#)
[関連資料](#)

概要

このドキュメントでは、Cisco Firepower Management Center(FMC)を更新するためのスケジュールされたタスクが失敗する理由について説明します。Cisco Firepower Management Centerは、手動または自動で更新できます。自動ソフトウェア更新を実行するには、Management Center で、今後実行するスケジュール タスクを作成します。

障害の考えられる原因

Firepower Management Center(FMC)は、ネットワークで次のいずれかのアクションが発生すると、Cisco Download Update Infrastructureからの更新ファイルのダウンロードに失敗する可能性があります。

- 会社のセキュリティポリシーは、ドメインネームシステム(DNS)トラフィックをブロックします。
- Management Center以外の設定は、ダウンロードに影響します。たとえば、ファイアウォール規則では、support.sourcefire.comに対して1つのIPアドレスのみを許可する場合があります。

  注意：シスコは、ロードバランシング、耐障害性、アップタイムにラウンドロビンDNSを使用します。したがって、DNSサーバのIPアドレスが変更される可能性があります。

影響

この方法を使用すると…	アクションアイ
自動ダウンロードのシステムデフォルト設定	対応不要
アップデートファイルを手動でダウンロードし、Firepower Management Centerにアップロードします	対応不要
Cisco Managed Download Update Infrastructureへのアクセスをフィルタリングするファイアウォールルール	ソリューションに

- 障害は、3回の再試行と次のスケジュールされた実行によって一部軽減されます。繰り返し失

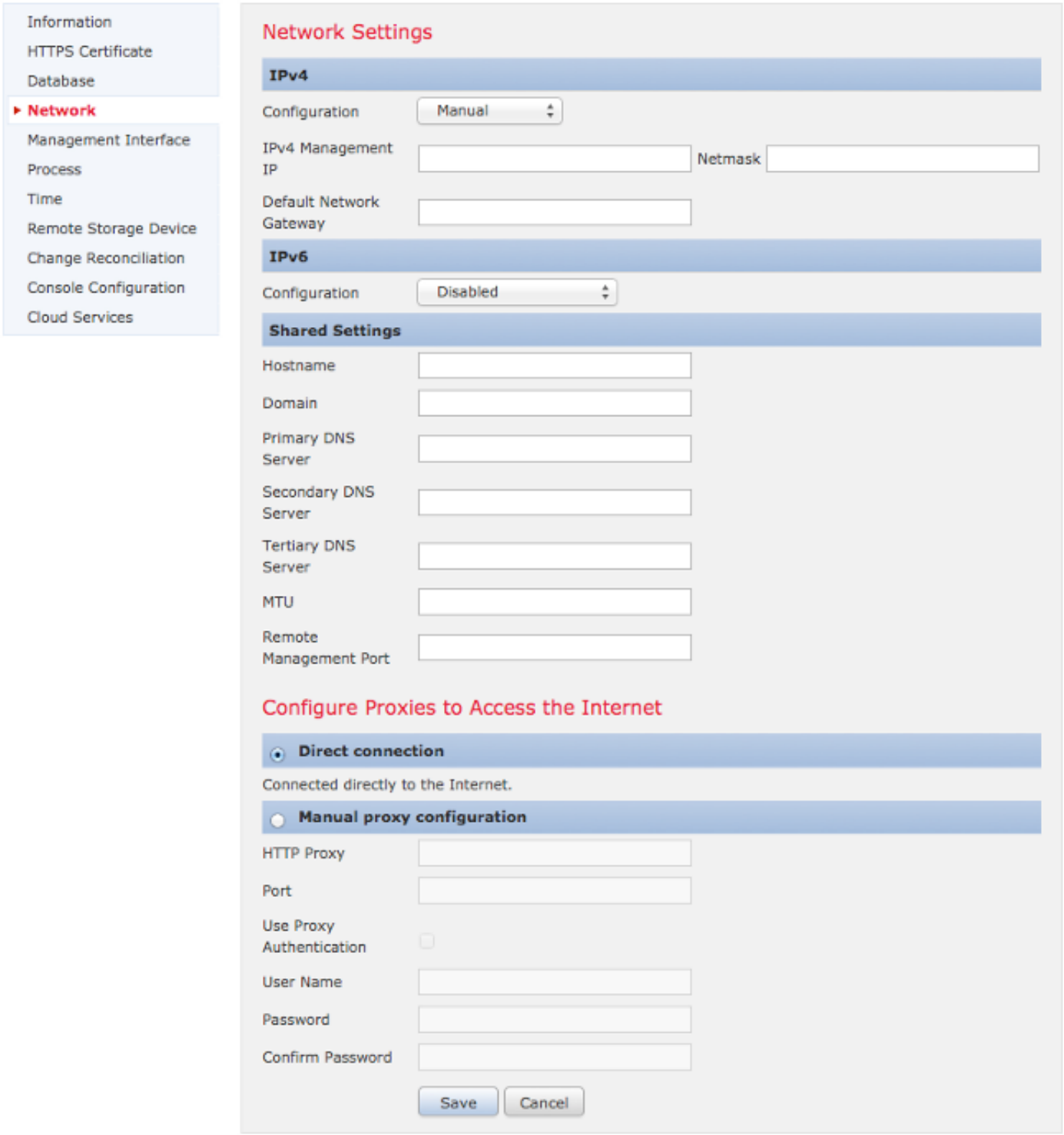
敗することは、ファイアウォールやインフラストラクチャの停止などの外部要因を示している可能性があります。
- ラウンドロビンDNSがドメイン名にあるため、断続的なダウンロード障害が発生しないようにするための手順を実行する必要があります。

確認

DNS設定の確認

Firepower Management CenterがDNSサーバを使用するように設定されていることを確認します。

注意：デフォルト設定を維持することを強く推奨します。



DNSの設定は、[ネットワーク]セクションの[システム] > [ローカル] > [構成]で行うことができます。[共有設定]セクションで、最大3台のDNSサーバを指定できます。

> **注**：[構成]ドロップダウンリストで[DHCP]を選択した場合、[共有設定]を手動で指定することはできません。

接続の確認

telnet、nslookup、digなどのさまざまなコマンドを使用して、DNSサーバの状態とFirepower Management CenterのDNS設定を確認できます。以下に、いくつかの例を示します。

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

注：support.sourcefire.comに対してpingを実行すると機能しません。したがって、接続テストとして使用しないでください。

アプライアンスからサポートサイトへの接続をテストするには（アップデートのダウンロードなど）、SSHまたは直接コンソールアクセスを介してアプライアンスにログインし、次のコマンドを使用します。

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

このコマンドは、証明書のネゴシエーションを表示するとともに、ポート80 Webサーバへの Telnetセッションに相当するセッションを提供します。コマンドの出力例を次に示します。

```
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 44A18130176C9171F50F33A367B55F5CFD10AA0FE87F9C5C1D8A7A7E519C695B
Session-ID-ctx:
Master-Key:
D406C5944B9462F1D6CB15D370E884B96B82049300D50E74F9B8332F84786F05C35BF3FD806672630BE26C2218AE5BDE
Key-Arg : None
Start Time: 1398171146
Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

この時点ではプロンプトは表示されません。ただし、セッションが入力を待っている間、次のコマンドを入力できます。

```
GET /
```

サポートサイトのログインページである未加工のHTMLが表示されます。

トラブルシュート

オプション 1：スタティックIPアドレスをファイアウォールのドメイン名 support.sourcefire.comに置き換えてください。スタティックIPアドレスを使用する必要がある場合は、これが正しいことを確認します。Firepowerシステムで使用されるダウンロードサーバの詳細情報を次に示します。

- **ドメイン**：support.sourcefire.com

- **[Port]**：443/tcp(双方向)
- **IP アドレス**：50.19.123.95, 50.16.210.129

support.sourcefire.com（ラウンドロビン方式）でも使用される追加のIPアドレスは次の通りです。

```
54.221.210.248
54.221.211.1
54.221.212.60
54.221.212.170
54.221.212.241
54.221.213.96
54.221.213.209
54.221.214.25
54.221.214.81
```

オプション 2：Webブラウザを使用して更新を手動でダウンロードし、メンテナンスウィンドウで手動でインストールできます。

オプション 3：DNSサーバにsupport.sourcefire.comのAレコードを追加します。

関連資料

- Firepowerシステムにインストールできるアップデートの種類
- 高度なマルウェア防御(AMP)運用に必要なサーバアドレス
- Firepowerシステムの動作に必要な通信ポート
- テクニカル サポートとドキュメント – Cisco Systems