

Firepower Management Center の自動ダウンロード アップデート失敗

目次

[はじめに](#)

[失敗のための考えられる原因](#)

[影響](#)

[確認](#)

[DNS 設定を確認して下さい](#)

[接続の確認](#)

[トラブルシューティング](#)

[関連資料](#)

概要

この資料は原因を Cisco Firepower Management Center をアップデートする定期タスク失敗するかもしれません説明します。 Cisco Firepower Management Center を手動または自動でアップデートできます。 自動ソフトウェア アップデートを行うために、未来の時に動作する管理センターのスケジュール タスクを作成できます。

失敗のための考えられる原因

Firepower Management Center はかもしれませんこれらの操作の 1 つがネットワークに発生するとき Cisco ダウンロード アップデート インフラストラクチャからアップデート ファイルをダウンロードしないことを:

- 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。
- 管理センター影響ダウンロードの外の設定。 たとえば、ファイアウォール ルールは `support.sourcefire.com` のための 1 IP アドレスだけ割り当てるかもしれません。

注意 : Cisco はロード バランシング、フォールトトレランスおよび稼働時間のためにラウンドロビン DNS を利用します。 従って、DNSサーバ mgihit の IP アドレスは変更されます

。

影響

使用すればこの方式を...

自動ダウンロードのためのシステムデフォルト設定

アップデート ファイルを手動でダウンロードし、Firepower Management Center にアップロードして下さい

Cisco によって管理されるダウンロード アップデート インフラストラクチャ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

やるべきこと

必要な操作無し

必要な操作無し

ソリューションに従って

- 失敗は 3 つの再試行および次にスケジュールされた実行部分的に軽減されます。 繰り返され

た失敗は本当らしいですインフラストラクチャのファイアウォールまたは停止のような外部ファクタの示す値。

- ラウンドロビン DNS がドメイン名にあると同時に、断続的なダウンロード失敗がないことを確認するためにステップを踏む必要があります。

確認

DNS 設定を確認して下さい

DNSサーバを使用するために Firepower Management Center が設定されるようにして下さい。

注意： Cisco はデフォルト設定を保存することを強く推奨します。

- Information
- HTTPS Certificate
- Database
- ▶ **Network**
- Management Interface
- Process
- Time
- Remote Storage Device
- Change Reconciliation
- Console Configuration
- Cloud Services

Network Settings

IPv4

Configuration

IPv4 Management IP Netmask

Default Network Gateway

IPv6

Configuration

Shared Settings

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

MTU

Remote Management Port

Configure Proxies to Access the Internet

Direct connection

Connected directly to the Internet.

Manual proxy configuration

HTTP Proxy

Port

Use Proxy Authentication

User Name

Password

Confirm Password

ネットワーク セクションの下でシステム > ローカル > 設定の DNS 設定を、行うことができます。 共用設定セクションの下で、3 つまでの DNSサーバを規定できます。

注: 設定ドロップダウン リストで『DHCP』を選択した場合、手動で共用設定を規定できません。

接続の確認

DNSサーバの状態、および Firepower Management Center の DNS 設定を確認するために telnet、nslookup、またはのようなささまざまなコマンドを、使用できます。次に、例を示します。

```
telnet support.sourcefire.com 443
```

```
nslookup support.sourcefire.com
```

```
dig support.sourcefire.com
```

注: support.sourcefire.com への Ping ははたきません。それ故にそれは接続テストとして使用するべきではありません。

アプライアンスからのサポート サイトへのテスト接続 (更新をダウンロードするため、等)、SSH がダイレクトコンソール アクセスによってアプライアンスにログイン することができこ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ネゴシエーションを示したり、また Telnetセッションの等量をポート 80 Webサーバに与えたものです。コマンド 出力の例はここにあります:

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

この時点で敏速がないはずですが。ただし、セッションが入力を待っているため、それからコマンドを入力できます:

```
GET /
```

サポート サイト ログイン ページである未加工 HTML を受け取る必要があります。

トラブルシューティング

オプション 1: ファイアウォールのドメイン名 support.sourcefire.com と静的IP アドレスを取り替えて下さい。静的IP アドレスを使用しなければならない場合これが正しいことを確かめて下さい。Firepower システムによって使用されるダウンロード サーバの詳細な情報はここにあります:

- **ドメイン:** support.sourcefire.com
- **Port:** 443/tcp (双方向)
- **IP Address:** 50.19.123.9550.16.210.129

また support.sourcefire.com によって使用する追加 IP アドレスは (ラウンドロビン方式で) 次のとおりです:

```
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

方法 2： Webブラウザとアップデートを手動でダウンロードでき次に Maintenance ウィンドウの間にそれを手動でインストールします。

オプション 3： DNSサーバの `support.sourcefire.com` のための A レコードを追加して下さい。

関連資料

- [Firepower システムでインストールされるかもしれない更新の型](#)
- [Advanced Malware Protection \(アンペア\) オペレーションのための必須サーバ アドレス](#)
- [Firepower システムオペレーションのための必須 COM ポート](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)