Échec de la mise à jour automatique du téléchargement sur Firepower Management Center

Contenu

Introduction

Ce document explique les raisons pour lesquelles une tâche planifiée de mise à jour de Cisco Firepower Management Center peut échouer. Vous pouvez mettre à jour un Cisco Firepower Management Center manuellement ou automatiquement. Afin d'effectuer une mise à jour logicielle automatique, vous pouvez créer une tâche de planification sur votre Management Center pour l'exécuter ultérieurement.

Raisons possibles de l'échec

Un Firepower Management Center peut ne pas télécharger un fichier de mise à jour à partir de l'infrastructure de mise à jour du téléchargement Cisco lorsque l'une des actions suivantes se produit sur votre réseau :

- La stratégie de sécurité de votre entreprise bloque le trafic DNS (Domain Name System).
- La configuration en dehors de votre Management Center a un impact sur le téléchargement. Par exemple, une règle de pare-feu peut autoriser une seule adresse IP pour support.sourcefire.com.

  Attention : Cisco utilise le DNS round robin pour l'équilibrage de charge, la tolérance aux pannes et la disponibilité. Par conséquent, les adresses IP des serveurs DNS peuvent changer.

Incidence

Si Vous Utilisez Cette Méthode...	Action
Configuration par défaut du système pour le téléchargement automatique	Aucune actio requise
Téléchargez le fichier de mise à jour manuellement et téléchargez-le dans Firepower	Aucune actio

Management Center Règles de pare-feu pour filtrer l'accès à l'infrastructure de mise à jour de téléchargement gérée par Cisco	requise Suivez la solu

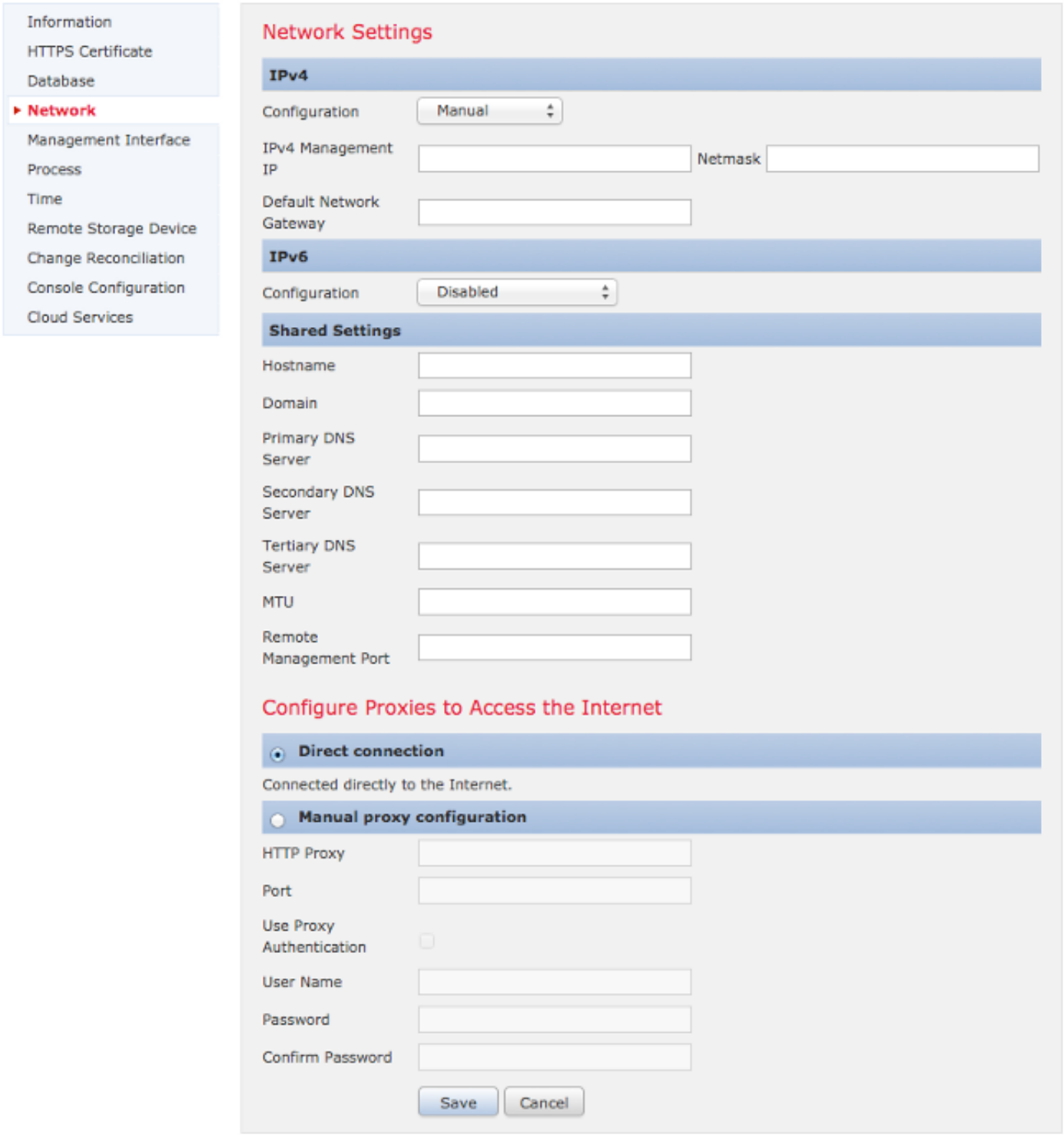
- Les échecs sont partiellement atténués par les trois nouvelles tentatives et la prochaine exécution planifiée. Les défaillances répétées sont probablement une indication d'un facteur externe tel que des pare-feu ou une panne de l'infrastructure.
- Étant donné que le DNS round robin se trouve sur le nom de domaine, vous devez prendre des mesures pour vous assurer qu'il n'y a pas d'échecs de téléchargement intermittents.

Vérification

Vérification des paramètres DNS

Vérifiez que votre Firepower Management Center est configuré pour utiliser votre serveur DNS.

Attention : Cisco vous recommande vivement de conserver les paramètres par défaut.



Vous pouvez configurer les paramètres DNS dans **System > Local > Configuration**, sous la section **Network**. Dans la section **Shared Settings**, vous pouvez spécifier jusqu'à trois serveurs DNS.

> **Note**: Si vous avez sélectionné **DHCP** dans la liste déroulante **Configuration**, vous ne pouvez pas spécifier manuellement les **paramètres partagés**.

Vérifier la connexion

Vous pouvez utiliser diverses commandes, telles que telnet, nslookup, ou dig afin de déterminer l'état du serveur DNS, et les paramètres DNS sur votre Firepower Management Center. Exemple :

```
telnet support.sourcefire.com 443

nslookup support.sourcefire.com

dig support.sourcefire.com
```

> **Note**: La commande ping vers support.sourcefire.com ne fonctionne pas. Il ne doit donc pas être utilisé comme test de connectivité.

Afin de tester la connexion au site d'assistance à partir d'une appliance (pour télécharger des mises à jour, etc.), vous pouvez vous connecter à votre appliance via SSH ou un accès direct à la console, et utiliser cette commande :

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

Cette commande affiche la négociation de certificat et vous fournit l'équivalent d'une session Telnet vers un serveur Web du port 80. Voici un exemple du résultat de la commande :

```
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)
---
```

Il ne doit pas y avoir d'invite à ce stade. Cependant, comme la session attend une entrée, vous pouvez entrer la commande suivante :

```
GET /
```

Vous devriez recevoir du code HTML brut qui est la page de connexion du site de support.

Dépannage

Option 1 : Remplacez l'adresse IP statique par le nom de domaine support.sourcefire.com sur les pare-feu. Si vous devez utiliser une adresse IP statique, assurez-vous qu'elle est correcte. Voici les informations détaillées du serveur de téléchargement utilisé par un système Firepower :

- **Domaine :** support.sourcefire.com

- **Port** : 443/tcp (bidirectionnel)
- **Adresse IP:** 50.19.123.95, 50.16.210.129

Les adresses IP supplémentaires qui sont également utilisées par le support.sourcefire.com (dans la méthode round robin) sont :

```
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
```

Option 2 : Vous pouvez télécharger les mises à jour manuellement à l'aide d'un navigateur Web, puis les installer manuellement pendant votre fenêtre de maintenance.

Option 3 : Ajoutez un enregistrement A pour support.sourcefire.com sur votre serveur DNS.

Documents associés

- Types de mises à jour pouvant être installées sur un système Firepower
- Adresses de serveur requises pour les opérations Advanced Malware Protection (AMP)
- Ports de communication requis pour le fonctionnement du système Firepower
- Support et documentation techniques - Cisco Systems