

FMCおよびFTDアップグレードのエラーメッセージのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[Firepower Management Center\(FMC\)およびFirepower Threat Defenseのアップグレードエラーメッセージ](#)

[通信障害](#)

[FMC-HA通信が侵害されている](#)

[FMCとFTD間の通信が侵害されている](#)

[ディスク領域が不足しているため、デバイスをアップグレードできません](#)

[FTDディスク使用率のトラブルシューティングコマンド](#)

[データベースの破損](#)

[参考資料](#)

はじめに

このドキュメントでは、Firepower Management Center(FMC)およびFirepower Threat Defense(FTD)でのアップグレードエラーメッセージのトラブルシューティング手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます

- Linuxシェルに関する基礎知識。
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

使用するコンポーネント

- VMWareのFMCvバージョン7.2.8
- VMWare用のFTDvバージョン7.2.8

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

シスコは、Firepowerデバイスのアップグレードに進むために対応するガイドを生成します。このガイドを確認した後でも、次のような状況が発生する可能性があります。

Firepower Management Center(FMC)およびFirepower Threat Defenseのアップグレードエラーメッセージ

通信障害

このメッセージは、次のシナリオで表示できます。

FMC-HA通信が侵害されている

これは、FMC-HA間の通信が失敗した場合に発生します。お客様は、次のコマンドを実行してデバイス間の接続を確認できます。

次のコマンドは、FMCルートレベルで適用する必要があります。

`ping <peer-ip-address>`を発行します。このコマンドは、両方のデバイス間の到達可能性を確認するために使用できます。

`netstat -an | grep 8305`を実行します。このコマンドは、ポート8305に接続されているデバイスを表示します。

注：ポート8305は、FMCとの通信チャネルを確立するためにFirepowerデバイスに設定されたデフォルトポートです。

FMC-HAヘルスステータスからより詳細な情報を取得するには、スクリプト `troubleshoot_HADC.pl` を実行します。

```
<#root>
```

```
> expert
```

```
admin@firepower:~$
```

```
sudo su
```

```
root@firepower:/Volume/home/admin#
```

```
ping xx.xx.18.102
```

```
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.  
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.533 ms  
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.563 ms  
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.431 ms  
^C  
--- xx.xx.18.102 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 59ms  
rtt min/avg/max/mdev = 0.431/0.509/0.563/0.056 ms
```

```
root@firepower:/Volume/home/admin#
```

```
netstat -an | grep 8305
```

```
tcp 0 0 xx.xx.18.101:8305 0.0.0.0:* LISTEN  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.253:48759 ESTABLISHED  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:53875 ESTABLISHED  
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:49205 ESTABLISHED  
tcp 0 0 xx.xx.18.101:60871 xx.xx.18.253:8305 ESTABLISHE
```

```
root@firepower:/Volume/home/admin#
```

```
troubleshoot_HADC.pl
```

```
***** Troubleshooting Utility *****
```

- 1 Show HA Info Of FMC
- 2 Execute Sybase DBPing
- 3 Show Arbiter Status
- 4 Check Peer Connectivity
- 5 Print Messages of AQ Task
- 6 Show FMC HA Operations History (ASC order)
- 7 Dump To File: FMC HA Operations History (ASC order)
- 8 Last Successful Periodic Sync Time (When it completed)
- 9 Print HA Status Messages
- 10 Compare active and standby device list
- 11 Check manager status of standby missing devices
- 12 Check critical PM processes details
- 13 Get Remote Stale Sync AQ Info
- 14 Help
- 0 Exit

```
*****
```

```
Enter choice:
```

FMCとFTD間の通信が侵害されている

FTDからFMCへの通信を検証するために、お客様は次のコマンドをクリッシュレベルで実行できます。

ping system <fmc-IP>:FTD管理インターフェイスからICMPフローを生成します。

show managers : このコマンドは、デバイスが登録されているマネージャの情報をリストします。

sftunnel-status : このコマンドは、デバイス間で確立されている通信チャネルを検証します。この

チャンネルはsftunnelという名前を受け取ります。

```
<#root>
```

```
>
```

```
ping system xx.xx.18.102
```

```
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.  
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.595 ms  
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.683 ms  
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.642 ms  
64 bytes from xx.xx.18.102: icmp_seq=4 ttl=64 time=24.4 ms  
64 bytes from xx.xx.18.102: icmp_seq=5 ttl=64 time=11.4 ms  
^C  
--- xx.xx.18.102 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 128ms  
rtt min/avg/max/mdev = 0.595/7.545/24.373/9.395 ms
```

```
> show managers
```

```
Type : Manager  
Host : xx.xx..18.101  
Display name : xx.xx..18.101  
Version : 7.2.8 (Build 25)  
Identifier : fc3e3572-xxxx-xxxx-xxxx-39e0098c166c  
Registration : Completed  
Management type : Configuration and analytics
```

```
Type : Manager  
Host : xx.xx..18.102  
Display name : xx.xx..18.102  
Version : 7.2.8 (Build 25)  
Identifier : bb333216-xxxx-xxxx-xxxx-c68c0c388b44  
Registration : Completed  
Management type : Configuration and analytics
```

```
> sftunnel-status
```

```
SFTUNNEL Start Time: Mon Oct 14 21:29:16 2024
```

```
Both IPv4 and IPv6 connectivity is supported  
Broadcast count = 5  
Reserved SSL connections: 0  
Management Interfaces: 2  
eth0 (control events) xx.xx..18.254,  
tap_nlp (control events) 169.254.1.2,fd00:0:0:1::2
```

```
*****
```

```
**RUN STATUS**xx.xx..18.102*****
```

```
Key File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-key.pem  
Cert File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-cert.pem  
CA Cert = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/cacert.pem  
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)  
ChannelA Connected: Yes, Interface eth0
```

Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.102' Start Time: Tue Oct 15 00:38:43 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.102' via Primary ip/host 'xx.xx..18.102'

PEER INFO:

sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.102,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18.102'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18.102'

RUN STATUSxx.xx..18.101*****

Key File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-key.pem
Cert File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-cert.pem
CA Cert = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/cacert.pem
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.101' Start Time: Mon Oct 14 21:29:15 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.101' via Primary ip/host 'xx.xx..18.101'

PEER INFO:

sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.101,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18.101'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18.101'

RPC STATUSxx.xx..18.102*****

'uuid' => 'bb333216-xxxx-xxxx-xxxx-c68c0c388b44',
'uuid_gw' => '',
'last_changed' => 'Wed Oct 9 07:00:11 2024',
'active' => 1,
'name' => 'xx.xx..18.102',
'ip' => 'xx.xx..18.102',
'ipv6' => 'IPv6 is not configured for management'

RPC STATUSxx.xx..18.101*****

'uuid_gw' => '',
'uuid' => 'fc3e3572-xxxx-xxxx-xxxx-39e0098c166c',
'last_changed' => 'Mon Jun 10 18:59:54 2024',
'active' => 1,
'ip' => 'xx.xx..18.101',
'ipv6' => 'IPv6 is not configured for management',
'name' => 'xx.xx..18.101'

Check routes:

No peers to check

/ngfw/var:Other Detection Engine	0 KB	651.532 MB	1.273 GB
/ngfw/var:Performance Statistics	1.325 GB	217.177 MB	1.485 GB
/ngfw/var:Other Events	0 KB	434.354 MB	868.710 MB
/ngfw/var:IP Reputation & URL Filtering	0 KB	542.943 MB	1.060 GB
/ngfw/var:arch_debug_file	0 KB	2.121 GB	12.725 GB
/ngfw/var:Archives & Cores & File Logs	0 KB	868.710 MB	8.483 GB
/ngfw/var:RNA Events	0 KB	868.710 MB	1.485 GB
/ngfw/var:Unified Low Priority Events	2.185 GB	1.060 GB	5.302 GB
/ngfw/var:File Capture	0 KB	2.121 GB	4.242 GB
/ngfw/var:Unified High Priority Events	0 KB	3.181 GB	7.423 GB
/ngfw/var:IPS Events	292 KB	2.545 GB	6.363 GB

>

system support silo-drain

Available Silos

- 1 - Temporary Files
- 2 - Action Queue Results
- 3 - User Identity Events
- 4 - UI Caches
- 5 - Backups
- 6 - Updates
- 7 - Other Detection Engine
- 8 - Performance Statistics
- 9 - Other Events
- 10 - IP Reputation & URL Filtering
- 11 - arch_debug_file
- 12 - Archives & Cores & File Logs
- 13 - RNA Events
- 14 - Unified Low Priority Events
- 15 - File Capture
- 16 - Unified High Priority Events
- 17 - IPS Events
- 0 - Cancel and return

Select a Silo to drain:

データベースの破損

このメッセージは通常、アップデートパッケージの準備状況チェックを実行した後に表示されま
す。これはFMCで最も一般的に見られます。

このエラーがFMCに表示されたら、FMCからトラブルシューティングファイルを生成することを
忘れないでください。

これにより、TACエンジニアはログの調査を開始し、問題を特定して、迅速にアクションプラン
を提供できます。

<#root>

FMC Database error

Fatal error: Database integrity check failed. Error running script 000_start/110_DB_integrity_check.sh.

参考資料

[Firepower Management Center向けCisco Firepower Threat Defenseアップグレードガイド](#)

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。