Troubleshoot FMC and FTD Upgrade Error Messages

Contents

Introduction

This document describes troubleshooting steps for upgrade error messages on Firepower Management Center (FMC) and Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of the next topics

- Basic knowledge of Linux shell.
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Components Used

- FMCv for VMWare on version 7.2.8.
- FTDv for VMWare on version 7.2.8.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

Cisco generates the corresponding guides to proceed with the Firepower devices upgrade. Even after checking this guide, the user can face any of these scenarios:

Firepower Management Center and Firepower Threat Defense Upgrade Error Messages

Communication failure

This message can be displayed in the next scenarios.

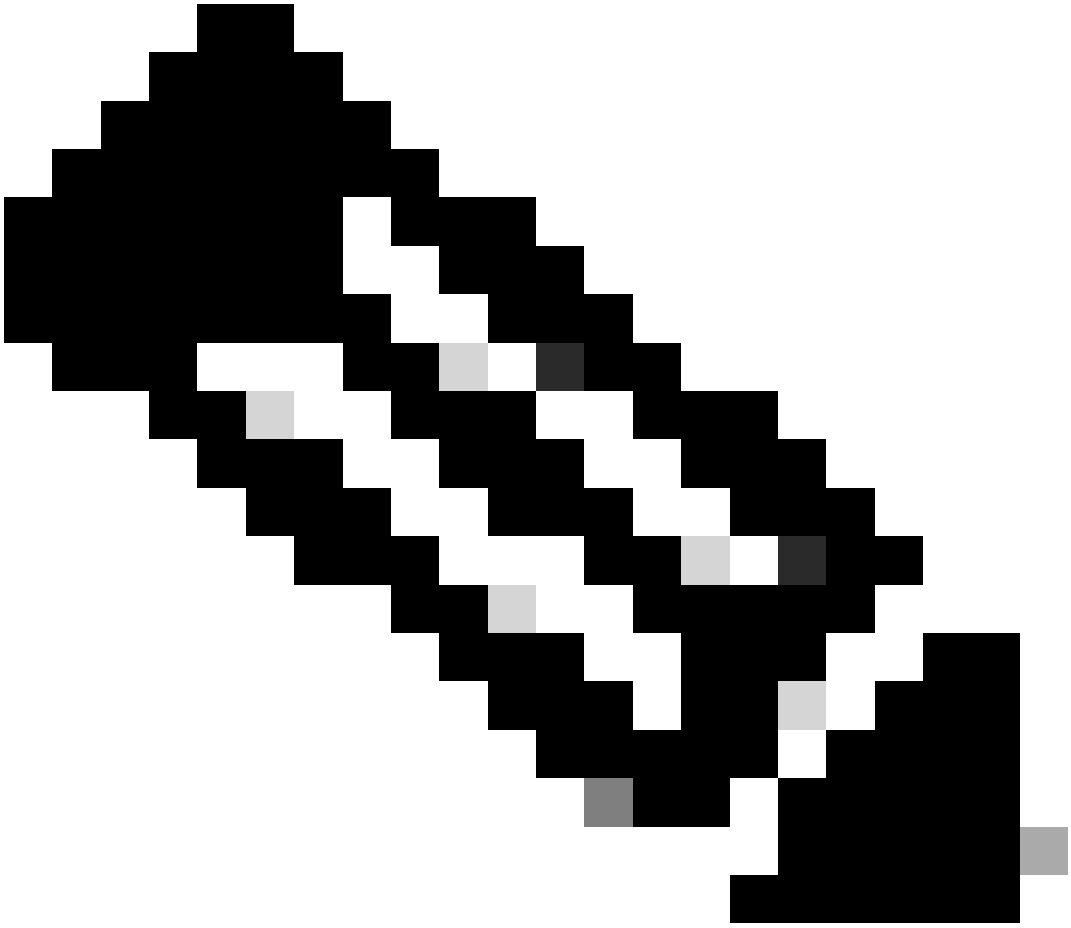
The FMC-HA communication is compromised

This happens when the communication between the FMC-HA fails The customer can run these commands to check the connectivity between the devices.

The next commands need to be applied at the FMC root level.

ping <peer-ip-address>. This command can be used to check the reachability between both devices.

netstat -an | grep 8305. This command displays the devices connected to port 8305.



Note: The port 8305 is the default port configured on the Firepower devices to establish the communication channel with the FMC.

To obtain more information from the FMC-HA health status the user can run the script **troubleshoot_HADC.pl**

<#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:
```

The communication between the FMC and the FTD is compromised

To validate the communication from the FTD to the FMC, the customer can run these commands from clish level:

ping system <fmc-IP> To generate an ICMP flow from the FTD management interface.

show managers This command lists the information of the managers where the device is registered.

sftunnel-status This command validates the communication channel established between the devices. This channel receives the name of sftunnel.

<#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..
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18

**********

**RUN STATUS****xx.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..
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18

**********
**RPC STATUS****xx.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 STATUS****xx.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
```

Disk space is insufficient to upgrade the device

This error message is generated when the device does not have the minimum disk space required to proceed with the upgrade process. This can be caused by the device storing old upgrade packages, old coverage

packages, old logs from the upgrade processes, old troubleshooting files, old backup files, or because the Geolocation Database size increases (Cisco bug ID CSCwe44571).

At root level, the next commands can be used for FMC and FTD to identify the files that are consuming the disk resources

- df -h
- df -Th
- df -kh
- du -sh *

<#root>

FTD upgrade failure message

```
****************** FAILURE SCRIPT: 1 **********************************
[241006 15:10:00:063] SCRIPT NAME: 000_start/410_check_disk_space.sh
RECOVERY MESSAGE: Not enough disk space available in /ngfw(Filesystem:/dev/sda8) to perform the upgrade
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

FTD disk utilization troubleshooting commands commands

show disk-manager. Display the information from the resources and files storage on the FTD disk.

system support silo-drain. Allow the user to eliminate safely the file storage on the FTD disk.

<#root>

>

show disk-manager

```
Partition:Silo                                  Used       Minimum      Maximum
/ngfw/var:Temporary Files                       621 KB     108.588 MB   434.354 MB
/ngfw/var:Action Queue Results                  0 KB       108.588 MB   434.354 MB
/ngfw/var:User Identity Event                   0 KB       108.588 MB   434.354 MB
/ngfw/var:UI Caches                             0 KB       325.766 MB   651.532 MB
/ngfw/var:Backups                               0 KB       868.710 MB   2.121 GB
/ngfw/var:Updates                               0 KB       1.273 GB     3.181 GB
/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:
```

Database corruption

This message is usually displayed after running the readiness check of the update package. It is most commonly seen in the FMC.

When this error is displayed in the FMC, do not forget to generate the Troubleshooting files from the FMC.

This allows the TAC engineer to begin with the logs investigation, determine which is the issue, and provide an action plan faster.

<#root>

FMC Database error

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

References

Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center.