

# Resolución de problemas de mensajes de error de actualización FMC y FTD

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Mensajes de error de actualización de Firepower Management Center y Firepower Threat Defence](#)

[falla de comunicación Entrante](#)

[La comunicación FMC-HA está en peligro](#)

[La comunicación entre el CSP y el FTD está comprometida](#)

[El espacio en disco es insuficiente para actualizar el dispositivo](#)

[comandos de resolución de problemas de utilización del disco FTD](#)

[Base de datos dañada](#)

[Referencias](#)

---

## Introducción

Este documento describe los pasos para solucionar problemas de los mensajes de error de actualización en Firepower Management Center (FMC) y Firepower Threat Defence (FTD).

## Prerequisites

### Requirements

Cisco recomienda que conozca los siguientes temas

- Conocimiento básico de Linux shell.
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

### Componentes Utilizados

- FMCv para VMWare en la versión 7.2.8.
- FTDv para VMWare en la versión 7.2.8.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

## Background

Cisco genera las guías correspondientes para continuar con la actualización de los dispositivos Firepower. Incluso después de consultar esta guía, el usuario puede enfrentarse a cualquiera de estos escenarios:

## Mensajes de error de actualización de Firepower Management Center y Firepower Threat Defence

### falla de comunicación Entrante

Este mensaje se puede mostrar en los siguientes escenarios.

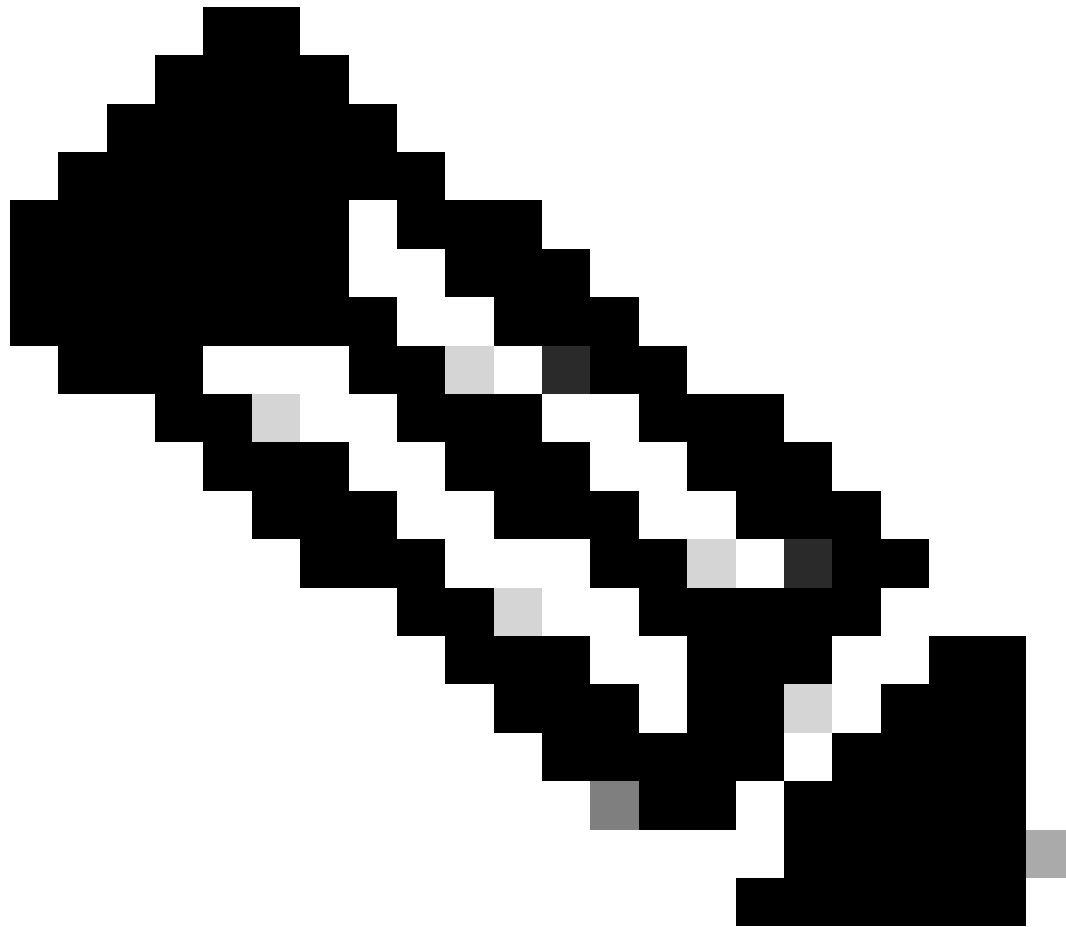
La comunicación FMC-HA está en peligro

Esto sucede cuando falla la comunicación entre el FMC-HA. El cliente puede ejecutar estos comandos para verificar la conectividad entre los dispositivos.

Los siguientes comandos deben aplicarse en el nivel raíz de FMC.

`ping <peer-ip-address>`. Este comando se puede utilizar para verificar el alcance entre ambos dispositivos.

`netstat -an | grep 8305`. Este comando muestra los dispositivos conectados al puerto 8305.



Nota: El puerto 8305 es el puerto predeterminado configurado en los dispositivos Firepower para establecer el canal de comunicación con el FMC.

---

Para obtener más información del estado de salud de FMC-HA, el usuario puede ejecutar el 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:
```

La comunicación entre el CSP y el FTD está comprometida

Para validar la comunicación del FTD al FMC, el cliente puede ejecutar estos comandos desde el nivel de cliente:

ping system <fmc-IP> Para generar un flujo ICMP desde la interfaz de administración de FTD.

show managers Este comando enumera la información de los administradores donde está registrado el dispositivo.

sftunnel-status Este comando valida el canal de comunicación establecido entre los dispositivos.

Este canal recibe el nombre de 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..18.102'  
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18.102'

\*\*\*\*\*

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

\*\*\*\*\*

\*\*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



/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:

## Base de datos dañada

Este mensaje suele aparecer después de ejecutar la comprobación de disponibilidad del paquete de actualización. Se observa con mayor frecuencia en el CSP.

Cuando aparezca este error en el FMC, no olvide generar los archivos de solución de problemas desde el FMC.

Esto permite al ingeniero del TAC comenzar con la investigación de los registros, determinar cuál es el problema y proporcionar un plan de acción más rápido.

<#root>

**FMC Database error**



Fatal error: Database integrity check failed. Error running script 000\_start/110\_DB\_integrity\_check.sh.

## Referencias

[Guía de actualización de Cisco Firepower Threat Defence para Firepower Management Center.](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).