Solucionar problemas de mensagens de erro de atualização do FMC e do FTD

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Background

Mensagens de erro de atualização do Firepower Management Center e do Firepower Threat Defense

- comunicação Inband
  - A comunicação FMC-HA está comprometida
  - A comunicação entre o CVP e o DTF está comprometida
- Espaço em disco insuficiente para atualizar o dispositivo
  - Comandos de solução de problemas de utilização de disco FTD
- Corrupção do banco de dados

Referências

Introdução

Este documento descreve as etapas de solução de problemas para mensagens de erro de atualização no Firepower Management Center (FMC) e no Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento dos próximos tópicos

- Conhecimento básico do shell do Linux.
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

- FMCv para VMWare na versão 7.2.8.
- FTDv para VMWare na versão 7.2.8.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Background

A Cisco gera os guias correspondentes para prosseguir com a atualização dos dispositivos Firepower. Mesmo depois de consultar este guia, o usuário pode enfrentar qualquer um destes cenários:

Mensagens de erro de atualização do Firepower Management Center e do Firepower Threat Defense

comunicação Inband

Essa mensagem pode ser exibida nos próximos cenários.

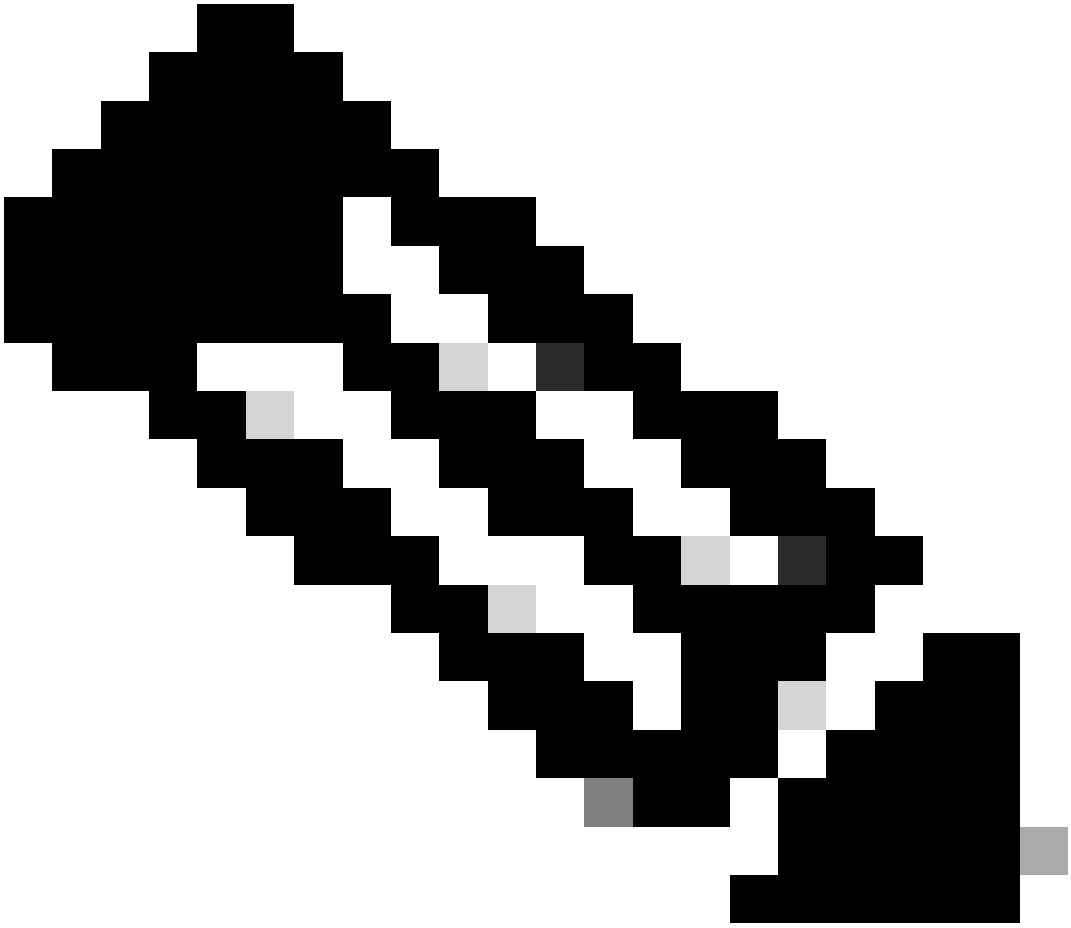
A comunicação FMC-HA está comprometida

Isso acontece quando a comunicação entre o FMC-HA falha. O cliente pode executar esses comandos para verificar a conectividade entre os dispositivos.

Os próximos comandos devem ser aplicados no nível raiz do FMC.

ping <peer-ip-address>. Esse comando pode ser usado para verificar a acessibilidade entre ambos os dispositivos.

netstat -an | grep 8305 Esse comando exibe os dispositivos conectados à porta 8305.



Observação: a porta 8305 é a porta padrão configurada nos dispositivos Firepower para estabelecer o canal de comunicação com o FMC.

Para obter mais informações sobre o status de saúde do FMC-HA, o usuário pode executar o 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:
```

A comunicação entre o CVP e o DTF está comprometida

Para validar a comunicação do FTD com o FMC, o cliente pode executar estes comandos a partir do nível do clish:

ping system <fmc-IP> Para gerar um fluxo ICMP a partir da interface de gerenciamento do FTD.

show managers Este comando lista as informações dos gerentes onde o dispositivo está registrado.

sftunnel-status Esse comando valida o canal de comunicação estabelecido entre os dispositivos.

Esse canal recebe o nome 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..
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
```

Espaço em disco insuficiente para atualizar o dispositivo

Essa mensagem de erro é gerada quando o dispositivo não tem o espaço em disco mínimo necessário para continuar com o processo de atualização. Isso pode ser causado pelo dispositivo que armazena pacotes de atualização antigos, pacotes de cobertura antigos, registros antigos dos processos de atualização, arquivos de solução de problemas antigos, arquivos de backup antigos ou porque o tamanho do banco de dados de localização geográfica aumenta (ID de bug Cisco CSCwe4571).

No nível raiz, os próximos comandos podem ser usados para FMC e FTD para identificar os arquivos que estão consumindo os recursos do disco

- 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
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Comandos de solução de problemas de utilização de disco FTD

show disk-manager. Exiba as informações do armazenamento de recursos e arquivos no disco FTD.

suporte do sistema silo-dreno. Permitir que o usuário elimine com segurança o armazenamento de arquivos no disco FTD.

<#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:
```

Corrupção do banco de dados

Esta mensagem é geralmente exibida após a execução da verificação de preparação do pacote de atualização. É mais comumente visto no FMC.

Quando esse erro for exibido no FMC, não se esqueça de gerar os arquivos de solução de problemas do FMC.

Isso permite que o engenheiro do TAC comece com a investigação de registros, determine qual é o problema e forneça um plano de ação mais rápido.

<#root>

FMC Database error

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

Referências

[Guia de atualização do Cisco Firepower Threat Defense para Firepower Management Center.]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.