排查 FMC 和 FTD 升级错误消息

目录

简介

先决条件

- 要求
- 使用的组件

背景

Firepower管理中心和Firepower威胁防御升级错误消息

- 通信故障
  - FMC-HA通信受到危害
  - FMC和FTD之间的通信受到危害
- 磁盘空间不足，无法升级设备
  - FTD磁盘利用率故障排除命令
- 数据库损坏

参考

简介

本文档介绍Firepower管理中心(FMC)和Firepower威胁防御(FTD)上升级错误消息的故障排除步骤。

先决条件

要求

思科建议您了解以下主题

- Linux shell基础知识。
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

使用的组件

- 用于VMWare的FMCv在版本7.2.8上。
- 用于VMWare的FTDv在版本7.2.8上。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

思科会生成相应的指南，以继续Firepower设备升级。即使选中了此指南，用户仍可面对下一部分中

指出的任何场景。

Firepower管理中心和Firepower威胁防御升级错误消息

通信故障

此消息可在下一场景中显示。

FMC-HA通信受到危害

当FMC-HA之间的通信失败时会发生这种情况运行这些命令以检查设备之间的连接。

接下来的命令需要在FMC根级别应用。

ping <peer-ip-address>。此命令可用于检查两台设备之间的连通性。

netstat -an | grep 8305。此命令显示连接到端口8305的设备。



注意：端口8305是Firepower设备上配置的默认端口，用于建立与FMC的通信通道。

要从FMC-HA运行状况获取更多信息，用户可以运行脚本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:
```

FMC和FTD之间的通信受到危害

要验证从FTD到FMC的通信，您可以从清洁级别运行以下命令：

ping system <fmc-IP>从FTD管理接口生成ICMP流量。

show managers此命令列出设备注册所在的管理器的信息。

sftunnel-status此命令用于验证设备之间建立的通信信道。此通道接收sftunnel的名称。

<#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
```

磁盘空间不足，无法升级设备

当设备没有继续升级过程所需的最小磁盘空间时，会生成此错误消息。这可能是因为设备存储旧的升级包、旧的覆盖包、升级过程中的旧日志、旧的故障排除文件、旧的备份文件，或者因为地理定位数据库大小增加(Cisco bug ID CSCwe44571)。

在根级别，下一个命令可用于FMC和FTD，以标识消耗磁盘资源的文件

- 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磁盘利用率故障排除命令

show disk-manager。显示FTD磁盘上资源和文件存储的信息。

系统支持孤岛排出。允许用户安全地消除FTD磁盘上的文件存储。

<#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:
```

数据库损坏

此消息通常在运行更新包的准备情况检查后显示。在FMC中最常看到。

当此错误显示在FMC中时，不要忘记从FMC生成故障排除文件。

这样，TAC工程师就可以开始调查日志，确定问题所在，并更快地制定行动计划。

<#root>

FMC Database error

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

参考

- 适用于Firepower管理中心的思科Firepower威胁防御升级指南。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。