疑難排解FMC和FTD升級錯誤訊息

目錄

簡介

本檔案說明Firepower管理中心(FMC)和Firepower威脅防禦(FTD)上升級錯誤訊息的疑難排解步驟。

必要條件

需求

思科建議您瞭解以下主題

- Linux shell基礎知識。
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

採用元件

- 7.2.8版上適用於VMWare的FMCv。
- 7.2.8版上適用於VMWare的FTDv。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

思科生成相應的指南以繼續進行Firepower裝置升級。即使在檢視本指南之後，使用者仍可面對以下

任一情況：

Firepower管理中心和Firepower威脅防禦升級錯誤消息

通訊失敗

此訊息可在下一個案例中顯示。

FMC-HA通訊受到威脅

當FMC-HA之間的通訊失敗時，會發生這種情況。客戶可以運行這些命令來檢查裝置之間的連線。

接下來的命令需要在FMC根級別應用。

ping <peer-ip-address>。此命令可用於檢查兩台裝置之間的可接通性。

netstat -an | grep 8305。此命令顯示連線到埠8305的裝置。

註：埠8305是Firepower裝置上配置的預設埠，用於建立與FMC的通訊通道。

要從FMC-HA運行狀況狀態獲取詳細資訊，使用者可以運行指令碼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之間的通訊受到損害

若要驗證從FTD到FMC的通訊，客戶可以從通話層級執行下列指令：

ping system <fmc-IP>，從FTD管理介面產生ICMP流量。

show managers 此命令列出裝置註冊所在的管理器的資訊。

sftunnel-status 此命令驗證在裝置之間建立的通訊通道。此通道接收sftunnel的名稱。

<#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..1
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..1
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
```

磁碟空間不足，無法升級裝置

當裝置沒有繼續升級程式所需的最小磁碟空間時，會產生此錯誤訊息。這可能是由於儲存舊升級軟體套件、舊覆蓋軟體套件、來自升級過程的舊日誌、舊故障排除檔案、舊備份檔案或者地理位置資料庫大小增加(思科漏洞ID CSCwe44571)所致。

在根級別，可以使用FMC和FTD的下一個命令來辨識消耗磁碟資源的檔案

- 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磁碟使用率疑難排解指令

show disk-manager。顯示FTD磁碟上資源與檔案儲存體的資訊。

系統支援思洛儲存器引出。允許使用者安全消除FTD磁碟上的檔案儲存。

<#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:
```

資料庫損毀

此訊息通常會在執行更新封裝的準備程度檢查後顯示。在FMC中最為常見。

當此錯誤顯示在FMC中時，切勿忘記從FMC生成故障排除檔案。

這使TAC工程師可以開始調查日誌，確定問題出在哪裡，並更快地提供行動計畫。

<#root>

```
FMC Database error

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

參考資料

[適用於Firepower管理中心的Cisco Firepower威脅防禦升級指南。]()

關於此翻譯