أستكشاف أخطاء FMC وترقية FTD وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند خطوات أستكشاف الأخطاء وإصلاحها الخاصة برسائل خطأ الترقية على مركز إدارة Firepower (FMC) والدفاع عن تهديد FirePOWER (FTD).

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من التالي موضوع

- معرفة أساسية بقشرة لينوكس.
- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)

المكونات المستخدمة

- FMCv ل VMWare على الإصدار 7.2.8.
- FTDv ل VMWare على الإصدار 7.2.8.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تم بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الخلفية

تقوم Cisco بإنشاء الأدلة المقابلة لمتابعة ترقية أجهزة FirePOWER. حتى بعد التحقق من هذا الدليل، يمكن للمستخدم مواجهة أي من هذه السيناريوهات:

رسائل خطأ ترقية مركز إدارة Firepower و Firepower Threat Defense

فشل الاتصال

يمكن عرض هذه الرسالة في السيناريوهات التالية.

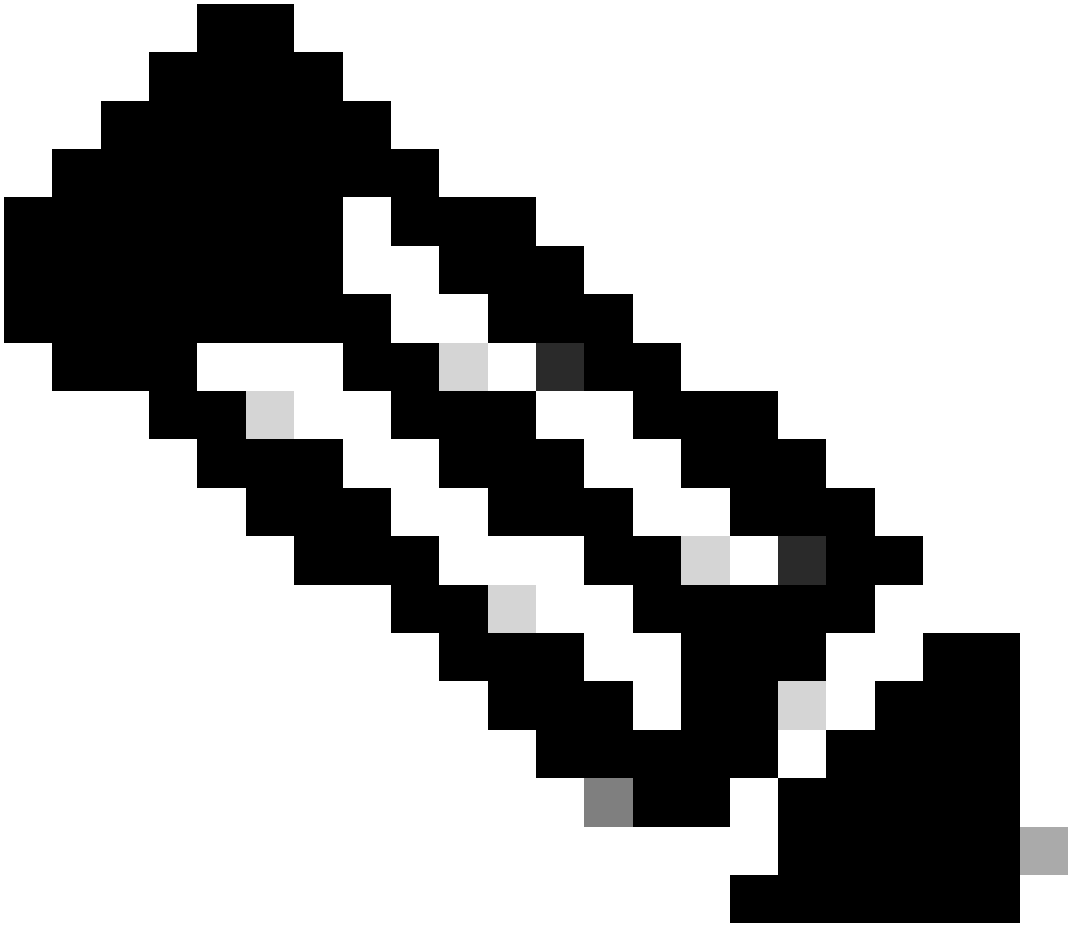
تم أختراق اتصال FMC-HA

وهذا يحدث عندما يفشل الاتصال بين FMC-HA، يمكن للعميل تشغيل هذه الأوامر للتحقق من الاتصال بين الأجهزة.

يجب تطبيق الأوامر التالية على مستوى جذر FMC.

إختبار الاتصال <peer-ip-address>. يمكن إستخدام هذا الأمر للتحقق من إمكانية الوصول بين كل الجهازين.

netstat - an | جرب 8305. يعرض هذا الأمر الأجهزة المتصلة بالمنفذ 8305.



ملاحظة: المنفذ 8305 وه المنفذ الافتراضي الذي تم تكوينه على أجهزة FirePOWER لإنشاء قناة الاتصال باستخدام FMC.

للحصول على مزيد من المعلومات من حالة صحة FMC-HA، يمكن للمستخدم تشغيل البرنامج النصي troubleshooting_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:
```

تم أختراق الاتصال بين FMC و FTD

للتحقق من الاتصال من FTD إلى FMC، يمكن للعميل تشغيل هذه الأوامر من مستوى clish:

نظام إختبار الاتصال <fmc-ip> لإنشاء تدفق ICMP من واجهة إدارة FTD.

show manager يسرد هذا الأمر معلومات المديرين حيث يتم تسجيل الجهاز.

SFTUNNEL-status يتحقق هذا الأمر من صحة قناة الاتصال التي تم إنشاؤها بين الأجهزة. تتلقى هذه القناة اسم 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
```

مساحة القرص غير كافية لترقية الجهاز

يتم إنشاء رسالة الخطأ هذه عندما لا يكون لدى الجهاز الحد الأدنى من مساحة القرص المطلوبة لمتابعة عملية الترقية. قد يحدث هذا بسبب الجهاز الذي يخزن حزم الترقية القديمة، أو حزم التغطية القديمة، أو السجلات القديمة من عمليات الترقية، أو ملفات أستكشاف الأخطاء وإصلاحها القديمة، أو ملفات النسخ الاحتياطي القديمة، أو بسبب زيادة حجم قاعدة بيانات الموقع الجغرافي (معرف تصحيح الأخطاء من Cisco CSCwe44571).

على مستوى الجذر، يمكن إستخدام الأوامر التالية ل FMC و FTD لتعريف الملفات التي تستهلك مساحة القرص

- df -h
- DF -TH
- df -k
- 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
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

أوامر أستكشاف أخطاء FTD وإصلاحها

إظهار إدارة الأقراص. عرض المعلومات من تخزين المواد والملفات على قرص FTD.

نظام تصريف مخازن دعم الأنظمة. السماح للمستخدم بإزالة تخزين الملفات على قرص FTD بأمان.

<#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:
```

تلف قاعدة البيانات

عادة ما يتم عرض هذه الرسالة بعد تشغيل فحص الاستعداد لحزمة التحديث. ويلاحظ ذلك بشكل شائع في وحدة إدارة الاتصالات الفيدرالية (FMC).

عندما يعرض اذه الخطأ في FMC، ال تنس إنشاء ملفات أستكشاف الأخطاء وإصلاحها من FMC.

وهذا يسمح لمهندس TAC بالبدء في تحقيق السجلات، وتحديد المشكلة، وتقديم خطة عمل بشكل أسرع.

<#root>

```
FMC Database error


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

المراجع

دليل تقنية الدفاع ضد تهديد FirePOWER من Cisco لمركز ادارة FirePOWER.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).