Risolvere i problemi relativi ai messaggi di errore di FMC e FTD

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi ai messaggi di errore di aggiornamento su Firepower Management Center (FMC) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei prossimi argomenti

- Conoscenze base della shell di Linux.
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componenti usati

- FMCv per VMWare versione 7.2.8.
- FTDv per VMWare sulla versione 7.2.8.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Introduzione

Cisco genera le guide corrispondenti per procedere con l'aggiornamento delle periferiche Firepower. Anche dopo aver controllato questa guida, l'utente può affrontare uno qualsiasi dei seguenti scenari:

Messaggi di errore di aggiornamento di Firepower Management Center e Firepower Threat Defense

Errore di comunicazione

Questo messaggio può essere visualizzato nei prossimi scenari.

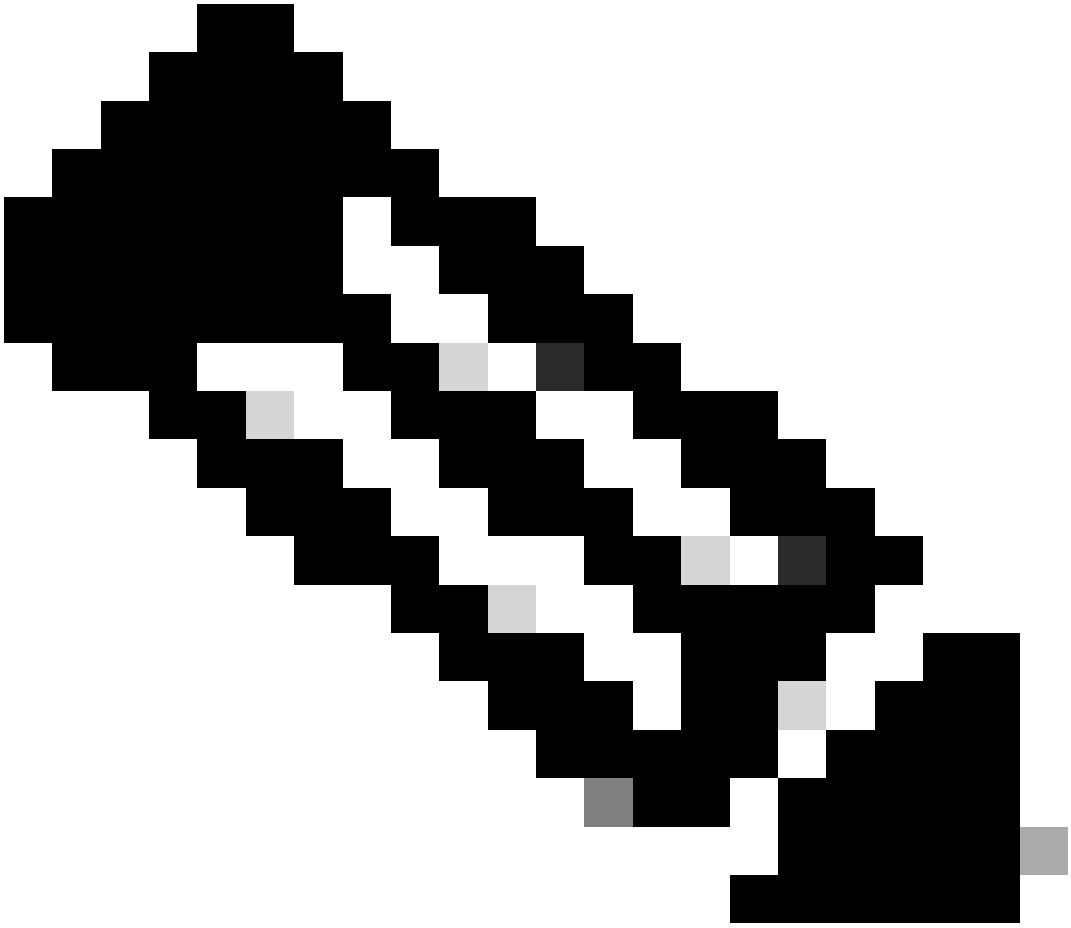
La comunicazione FMC-HA è compromessa

Questo accade quando la comunicazione tra FMC-HA non riesce Il cliente può eseguire questi comandi per controllare la connettività tra i dispositivi.

I comandi successivi devono essere applicati a livello di radice del CCP.

ping <indirizzo-ip-peer>. Questo comando può essere usato per verificare la raggiungibilità tra entrambi i dispositivi.

netstat -an | grep 8305 Questo comando visualizza i dispositivi collegati alla porta 8305.



Nota: la porta 8305 è la porta predefinita configurata sui dispositivi Firepower per stabilire il canale di comunicazione con il FMC.

Per ottenere ulteriori informazioni dallo stato di integrità FMC-HA, è possibile eseguire lo 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 comunicazione tra il CCP e l'FTD è compromessa

Per convalidare la comunicazione tra FTD e FMC, il cliente può eseguire questi comandi a livello di codice:

ping system <fmc-IP> Per generare un flusso ICMP dall'interfaccia di gestione FTD.

show manager Questo comando elenca le informazioni sui manager in cui è registrato il dispositivo.

sftunnel-status Questo comando convalida il canale di comunicazione stabilito tra i dispositivi.

Questo canale riceve il nome di 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
```

Spazio su disco insufficiente per aggiornare il dispositivo

Questo messaggio di errore viene generato quando il dispositivo non dispone dello spazio minimo su disco necessario per continuare il processo di aggiornamento. Il problema può essere causato dal dispositivo che archivia i vecchi pacchetti di aggiornamento, i vecchi pacchetti di code coverage, i vecchi log dei processi di aggiornamento, i vecchi file di risoluzione dei problemi e di backup o dall'aumento delle dimensioni del database di georilevazione (ID bug Cisco CSCwe44571).

A livello principale, i comandi successivi possono essere utilizzati per FMC e FTD per identificare i file che utilizzano le risorse del 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
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Comandi per la risoluzione dei problemi relativi all'utilizzo del disco FTD

show disk-manager. Visualizzare le informazioni dall'archivio risorse e file sul disco FTD.

supporto di sistema per silo-drain. Consentire all'utente di eliminare in modo sicuro lo storage dei file sul 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:
```

Danneggiamento database

Questo messaggio viene in genere visualizzato dopo l'esecuzione del controllo di preparazione del pacchetto di aggiornamento. È più comunemente visto nel FMC.

Quando l'errore viene visualizzato nel FMC, non dimenticare di generare i file di risoluzione dei problemi dal FMC.

Questo consente al tecnico TAC di iniziare l'indagine sui log, determinare qual è il problema e fornire un piano d'azione più rapidamente.

<#root>

FMC Database error

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

Riferimenti

Guida all'aggiornamento di Cisco Firepower Threat Defense per Firepower Management Center.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).