

排除Firepower威脅防禦高可用性問題

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設計選項](#)

[HA術語](#)

[HA狀態](#)

[HA狀態流程圖](#)

[UI驗證](#)

[Firepower管理中心託管FTD HA](#)

[FDM託管的FTD HA](#)

[ASDM託管ASA HA](#)

[適用於執行FTD/ASA HA的4100/9300的Firepower機箱管理員](#)

[驗證CLI](#)

[疑難排解](#)

[案例](#)

[APP-SYNC失敗](#)

[備用節點無法加入HA，因為「CD應用同步錯誤是應用配置應用失敗」](#)

[備用節點無法加入HA並顯示「由於APP SYNC超時，HA狀態進展失敗」](#)

[備用節點無法加入HA，並顯示「CD應用同步錯誤無法在備用節點上應用SSP配置」](#)

[運行狀況檢查失敗](#)

[Snort關閉或磁碟故障](#)

[檢測引擎 \(SNORT例項\) 已關閉](#)

[裝置顯示磁碟使用率高](#)

[服務卡故障](#)

[MIO心跳故障](#)

[相關資訊](#)

簡介

本檔案介紹Firepower威脅防禦(FTD)上的高可用性(HA)的操作、驗證和疑難排解程式。

必要條件

需求

思科建議瞭解以下主題：

- FTD和ASA平台
- FTD裝置上的封包擷取

強烈建議閱讀Firepower配置指南[在Firepower裝置上配置FTD高可用性](#)，以更好地瞭解本文檔中介紹的概念。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco FTD
- Cisco Firepower Management Center(FMC)

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。

背景資訊

資訊和示例基於FTD，但大多數概念也完全適用於自適應安全裝置(ASA)。

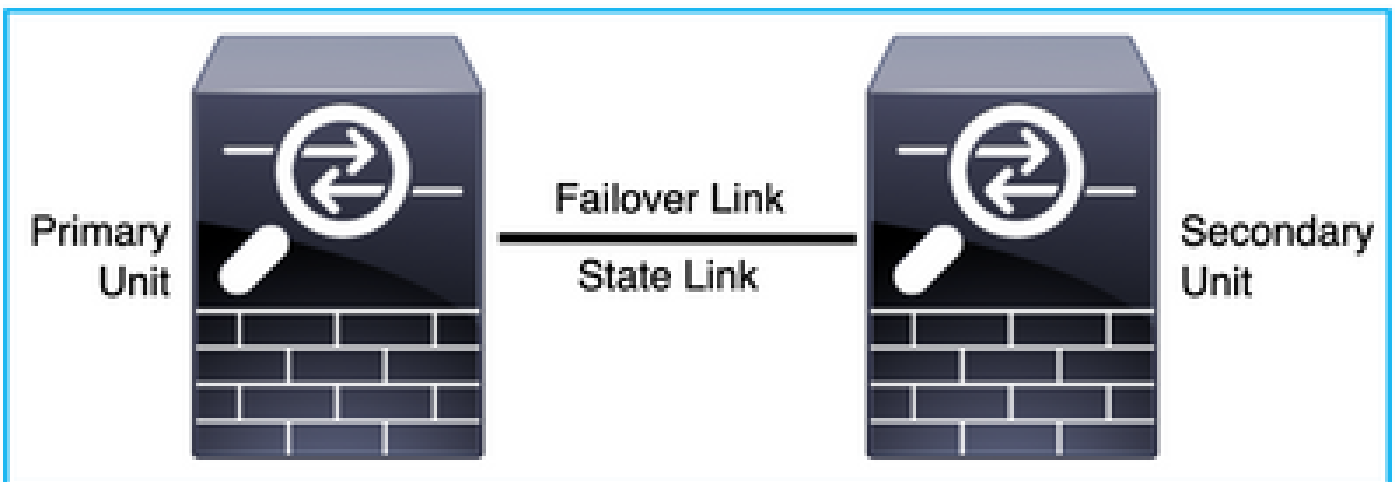
FTD支援兩種主要管理模式：

- 通過FMC實現開箱即用 — 也稱為遠端管理
- 通過Firepower裝置管理器(FDM)進行開箱操作 — 也稱為本地管理

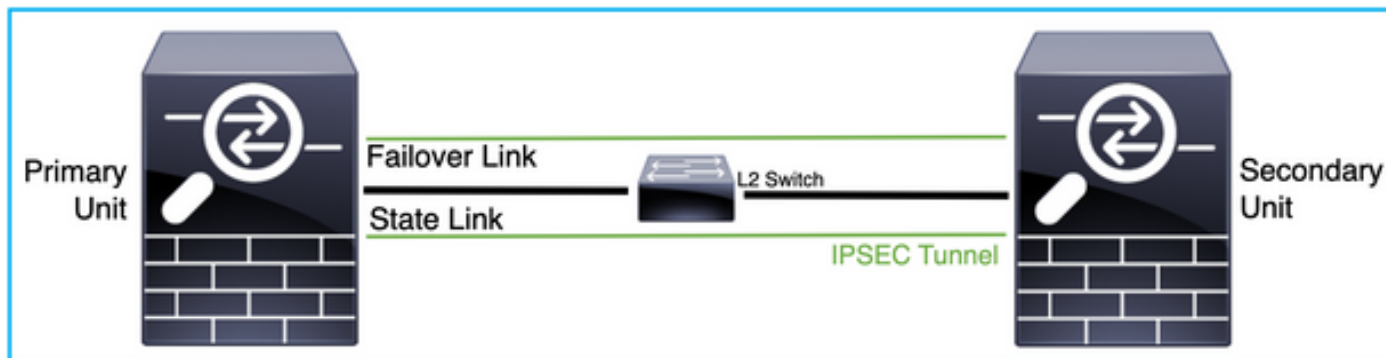
 注意：通過FDM管理的FTD可以從Firepower版本代碼6.3.0版開始新增到高可用性中。

設計選項

從FTD的設計角度來看，它可以直接連線，如下圖所示：



也可以透過第2層(L2)交換器連線，如下圖所示：



HA術語

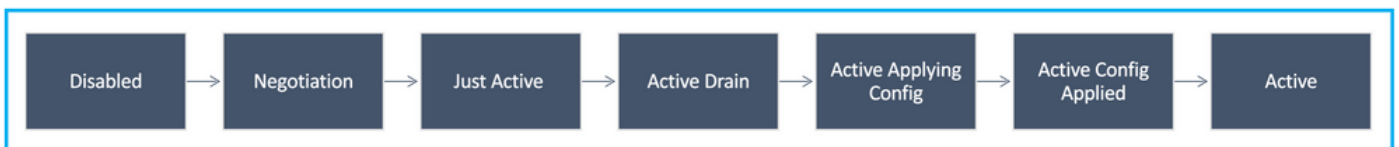
| | |
|--------------|---|
| Active (作用中) | 活動ASA接收所有流量流並過濾所有網路流量。配置更改在活動ASA上進行。 |
| HA連結 | <p>故障轉移對中的兩個裝置通過故障轉移鏈路持續通訊，以確定每個裝置的運行狀態並同步配置更改。通過鏈路共用的資訊是：</p> <ul style="list-style-type: none"> • 裝置狀態 (主用或備用) • Hello消息 (保持連線) • 網路鏈路狀態 • MAC地址交換 • 配置複製和同步 |
| 主要 | 這是通常在您建立HA時首先配置的裝置。其意義在於，如果ASA HA的兩台裝置在同一時刻同時啟動，則主裝置將承擔主用角色。 |
| 次要 | 這是通常在建立HA時再次配置的裝置。其意義在於，如果ASA HA的兩台裝置在同一時刻同時啟動，則輔助裝置將承擔備用角色。 |
| Standby (待命) | 備用ASA不處理任何即時流量，它同步來自活動裝置的連線和配置，並在發生故障切換時承擔主用角色。 |
| 狀態連結 | <p>主用單元使用狀態鏈路將連線狀態資訊傳遞給備用裝置。因此，備用裝置可以維護某些型別的連線，而不會影響您。此資訊可幫助備用裝置在故障轉移時保持存在的連線。NB：當使用同一鏈路進行故障切換和有狀態故障切換時，可以最有效地節省介面。但是，如果您有大型配置和高流量網路，則必須考慮為狀態鏈路和故障轉移鏈路提供專用介面。我們建議有狀態故障切換鏈路的頻寬必須與裝置上資料介面的最大頻寬相匹配。</p> |

HA狀態

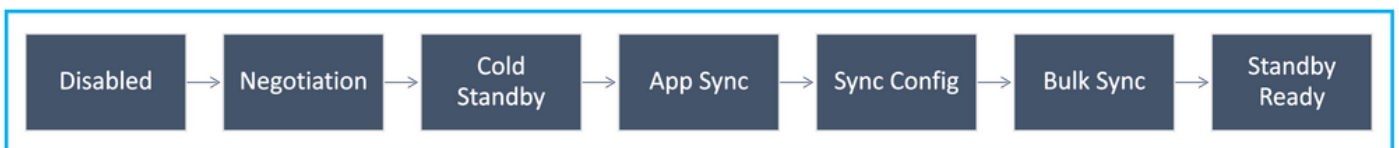
| | |
|----------------|--|
| Active (作用中) | 裝置當前處理網路上的即時流量，需要完成的所有配置更改都在此裝置上執行。 |
| 應用程式同步 | 處於此狀態的裝置將從活動裝置同步配置。 |
| 批次同步 | 處於此狀態的裝置將從活動裝置同步配置。 |
| 已禁用 | 已禁用裝置上的故障轉移 (命令 : no failover) 。 |
| 交涉 | 裝置將檢查活動裝置的可用性，如果發現活動裝置未準備好待機，則擔當活動角色。 |
| 備用就緒 | 裝置當前不處理流量，但是如果活動裝置顯示任何運行狀況檢查問題，則裝置將承擔活動角色。 |
| 同步配置 | 配置從主用裝置複製到備用裝置。 |
| 冷待機 | 裝置在故障切換時作為主用裝置接管，但不會複製連線事件。 |

HA狀態流程圖

主要 (無任何連線的對等體) :



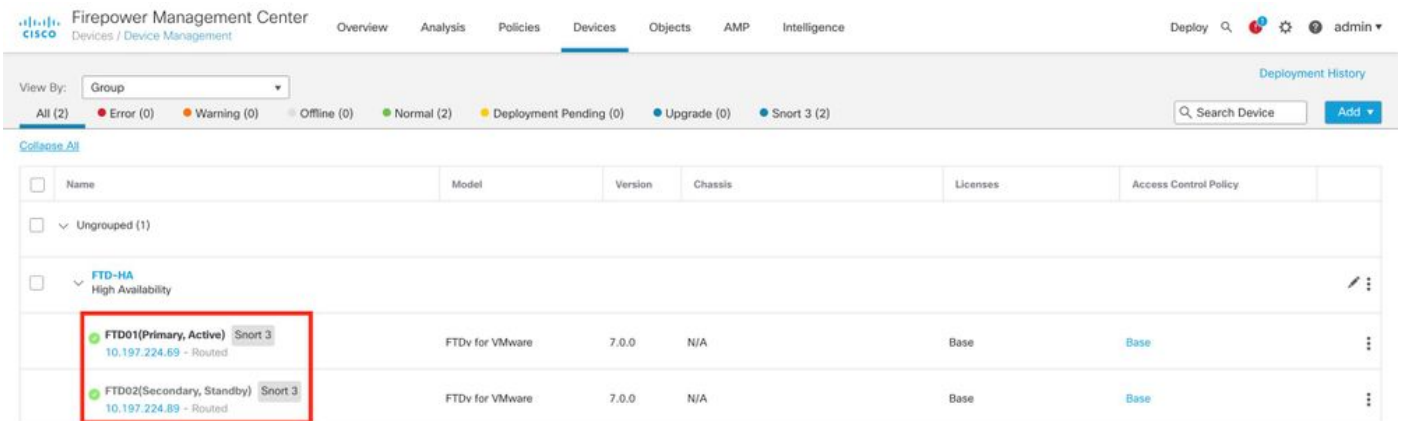
輔助 (具有活動連線對等體) :



UI驗證

Firepower管理中心託管FTD HA

導覽至Device > Device Management時，可以從FMC UI檢查FTD HA狀態，如下圖所示：



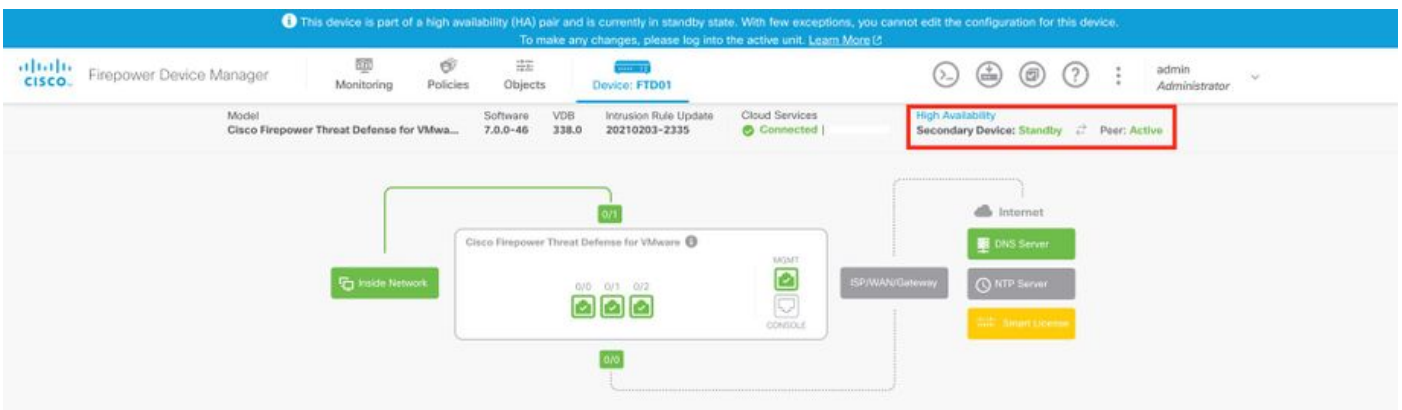
| Name | Model | Version | Chassis | Licenses | Access Control Policy |
|---|-----------------|---------|---------|----------|-----------------------|
| Ungrouped (1) | | | | | |
| FTD-HA High Availability | | | | | |
| FTD01(Primary, Active) Snort 3 10.197.224.69 - Routed | FTDv for VMware | 7.0.0 | N/A | Base | Base |
| FTD02(Secondary, Standby) Snort 3 10.197.224.89 - Routed | FTDv for VMware | 7.0.0 | N/A | Base | Base |

FDM託管的FTD HA

「主FDM概覽」頁：



輔助FDM概覽頁：



ASDM託管ASA HA

主ASA的首頁：

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.62

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

Device Information

General License Virtual Resources

Host Name: **ciscoasa**
 ASA Version: **9.12(3)12**
 ASDM Version: **7.12(2)14**
 Firewall Mode: **Routed**
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 36m 28s**
 Device Type: **ASAv**
 Number of vCPUs: **8**
 Total Memory: **8192 MB**

Interface Status

| Interface | IP Address/Mask | Line | Link | Kbps |
|------------|-------------------|------|------|------|
| backup | 109.106.53.100/24 | up | up | 3 |
| inside | 10.106.60.55/24 | up | up | 1 |
| management | 10.106.47.62/24 | up | up | 5 |
| outside | 10.106.48.65/24 | up | up | 1 |

Select an interface to view input and output Kbps

Failover Status

This Host: **PRIMARY (Active)** Other Host: **SECONDARY (Standby Ready)** [Details](#)

VPN Summary

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0 [Details](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

1977MB
02:40:41

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

backup

'backup' Interface Traffic Usage (Kbps)

Input Kbps: 3 Output Kbps: 0

Latest ASDM Syslog Messages

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

[Enable Logging](#)

Device configuration loaded successfully.

Active admin 15 25/11/21 2:40:45 AM UTC

輔助ASA的首頁：

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.64

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

Device Information

General License Virtual Resources

Host Name: **ciscoasa**
 ASA Version: **9.12(3)12**
 ASDM Version: **7.12(2)14**
 Firewall Mode: **Routed**
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 39m 10s**
 Device Type: **ASAv**
 Number of vCPUs: **8**
 Total Memory: **8192 MB**

Interface Status

| Interface | IP Address/Mask | Line | Link | Kbps |
|------------|-----------------|------|------|------|
| backup | no ip address | up | up | 2 |
| inside | no ip address | up | up | 1 |
| management | 10.106.47.64/24 | up | up | 89 |
| outside | no ip address | up | up | 1 |

Select an interface to view input and output Kbps

Failover Status

This Host: **SECONDARY (Standby Ready)** Other Host: **PRIMARY (Active)** [Details](#)

VPN Summary

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0 [Details](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

1979MB
02:43:21

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 2 Total: 2

backup

'backup' Interface Traffic Usage (Kbps)

Input Kbps: 2 Output Kbps: 0

Latest ASDM Syslog Messages

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

[Enable Logging](#)

Device configuration loaded successfully.

Standby admin 15 25/11/21 2:43:25 AM UTC

適用於執行FTD/ASA HA的4100/9300的Firepower機箱管理員

「主FCM邏輯裝置」頁：

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

| Application | Version | Resource Profile | Management IP | Gateway | Management Port | Status |
|----------------|-----------|------------------|---------------|---|-----------------|--------|
| ASA | 9.12.4.18 | | 10.197.216.7 | 10.197.216.1 | Ethernet1/7 | Online |
| Interface Name | | Type | | Attributes | | |
| Ethernet1/1 | | data | | Cluster Operational Status : not-applicable | | |
| Ethernet1/2 | | data | | HA-LINK-INTF : Ethernet3/7 | | |
| Ethernet1/3 | | data | | HA-LAN-INTF : Ethernet3/7 | | |
| Ethernet1/4 | | data | | HA-ROLE : active | | |
| Ethernet1/5 | | data | | | | |
| Ethernet1/6 | | data | | | | |
| Ethernet1/8 | | data | | | | |
| Ethernet3/7 | | data | | | | |
| Ethernet3/8 | | data | | | | |

「輔助FCM邏輯裝置」頁：

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

| Application | Version | Resource Profile | Management IP | Gateway | Management Port | Status |
|----------------|-----------|------------------|---------------|---|-----------------|--------|
| ASA | 9.12.4.18 | | 10.197.216.8 | 10.197.216.1 | Ethernet1/7 | Online |
| Interface Name | | Type | | Attributes | | |
| Ethernet1/1 | | data | | Cluster Operational Status : not-applicable | | |
| Ethernet1/2 | | data | | HA-LINK-INTF : Ethernet3/7 | | |
| Ethernet1/3 | | data | | HA-LAN-INTF : Ethernet3/7 | | |
| Ethernet1/4 | | data | | HA-ROLE : standby | | |
| Ethernet1/5 | | data | | | | |
| Ethernet1/6 | | data | | | | |
| Ethernet1/8 | | data | | | | |
| Ethernet3/7 | | data | | | | |
| Ethernet3/8 | | data | | | | |

驗證CLI

```
<#root>
```

```
>
```

```
show running-config failover
```

```
failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

這裡需要考慮的要點是：

容錯移轉

failover lan unit secondary —>裝置是主裝置還是輔助裝置

failover lan interface failover-link GigabitEthernet0/2 —>裝置上的故障切換鏈路物理介面
故障切換複製http

failover link failover-link GigabitEthernet0/2

failover interface ip failover-link 10.10.69.49 255.255.255.0備用10.10.69.89 —>主裝置和備用裝置

故障切换链路ip地址。

<#root>

>

show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
 This host: Secondary - Standby Ready
 Active time: 0 (sec)
 slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
 Interface outside (0.0.0.0): Normal (Not-Monitored)
 Interface inside (192.168.45.2): Normal (Not-Monitored)
 Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
 slot 1: snort rev (1.0) status (up)
 slot 2: diskstatus rev (1.0) status (up)
 Other host: Primary - Active
 Active time: 707216 (sec)
 Interface outside (0.0.0.0): Normal (Not-Monitored)
 Interface inside (192.168.45.1): Normal (Not-Monitored)
 Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
 slot 1: snort rev (1.0) status (up)
 slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)

| Stateful Obj | xmit | xerr | rcv | rerr |
|---------------|-------|------|--------|------|
| General | 95752 | 0 | 115789 | 0 |
| sys cmd | 95752 | 0 | 95752 | 0 |
| up time | 0 | 0 | 0 | 0 |
| RPC services | 0 | 0 | 0 | 0 |
| TCP conn | 0 | 0 | 0 | 0 |
| UDP conn | 0 | 0 | 0 | 0 |
| ARP tbl | 0 | 0 | 20036 | 0 |
| Xlate_Timeout | 0 | 0 | 0 | 0 |
| IPv6 ND tbl | 0 | 0 | 0 | 0 |
| VPN IKEv1 SA | 0 | 0 | 0 | 0 |
| VPN IKEv1 P2 | 0 | 0 | 0 | 0 |
| VPN IKEv2 SA | 0 | 0 | 0 | 0 |
| VPN IKEv2 P2 | 0 | 0 | 0 | 0 |
| VPN CTCP upd | 0 | 0 | 0 | 0 |
| VPN SDI upd | 0 | 0 | 0 | 0 |
| VPN DHCP upd | 0 | 0 | 0 | 0 |
| SIP Session | 0 | 0 | 0 | 0 |
| SIP Tx | 0 | 0 | 0 | 0 |
| SIP Pinhole | 0 | 0 | 0 | 0 |
| Route Session | 0 | 0 | 0 | 0 |

| | | | | |
|----------------|---|---|---|---|
| Router ID | 0 | 0 | 0 | 0 |
| User-Identity | 0 | 0 | 1 | 0 |
| CTS SGTNAME | 0 | 0 | 0 | 0 |
| CTS PAC | 0 | 0 | 0 | 0 |
| TrustSec-SXP | 0 | 0 | 0 | 0 |
| IPv6 Route | 0 | 0 | 0 | 0 |
| STS Table | 0 | 0 | 0 | 0 |
| Rule DB B-Sync | 0 | 0 | 0 | 0 |
| Rule DB P-Sync | 0 | 0 | 0 | 0 |
| Rule DB Delete | 0 | 0 | 0 | 0 |

Logical Update Queue Information

| | | | |
|---------|-----|-----|--------|
| | Cur | Max | Total |
| Recv Q: | 0 | 5 | 504656 |
| Xmit Q: | 0 | 1 | 95752 |

故障切换開啟：故障切换已启用或已禁用。

此主機：輔助 — 備用就緒。此裝置的角色和介面的狀態。

其他主機：主 — 活動。另一台裝置處於Active狀態並與當前裝置通訊。

<#root>

>

show failover history

```
=====
```

| From State | To State | Reason |
|--|------------------------|----------------------|
| 01:18:14 UTC Nov 25 2021 Not Detected | Negotiation | No Error |
| 01:18:27 UTC Nov 25 2021 Negotiation | Just Active | No Active unit found |
| 01:18:27 UTC Nov 25 2021 Just Active | Active Drain | No Active unit found |
| 01:18:27 UTC Nov 25 2021 Active Drain | Active Applying Config | No Active unit found |
| 01:18:27 UTC Nov 25 2021 Active Applying Config | Active Config Applied | No Active unit found |
| 01:18:27 UTC Nov 25 2021 Active Config Applied | Active | No Active unit found |

```
=====
```

使用此選項可以檢查裝置的歷史狀態以及這些狀態更改的原因：

<#root>

>

```
show failover state
```

```
State                Last Failure Reason  Date/Time
This host - Secondary Standby Ready        None
Other host - Primary  Active              None

====Configuration State====
  Sync Done - STANDBY
====Communication State====
  Mac set
```

檢查裝置的當前狀態以及上次故障切換的原因：

| 欄位 | 說明 |
|------|--|
| 配置狀態 | <p>顯示配置同步的狀態。</p> <p>備用裝置可能的配置狀態：</p> <ul style="list-style-type: none">• Config Syncing - STANDBY — 執行同步配置時設定。• Interface Config Syncing - STANDBY• Sync Done - STANDBY — 當備用裝置已完成從活動裝置的配置同步時設定。 <p>活動裝置可能的配置狀態：</p> <ul style="list-style-type: none">• Config Synching — 當活動裝置與備用裝置執行配置同步時，在活動裝置上設定。• 介面組態同步• Sync Done — 當主用裝置成功完成與備用裝置的配置同步時設定。• Ready for Config Sync — 當備用裝置發出準備好接收配置同步訊號時，在活動裝置上設定。 |
| 通訊狀態 | <p>顯示MAC地址同步的狀態。</p> <ul style="list-style-type: none">• Mac set — 已將MAC地址從對等裝置同步到此裝置。• 更新的Mac — 在更新一個MAC地址並需要同步到另一個裝置時使用。也用於裝置更新從對等裝置同步的本地MAC地址的轉換時。 |

| 欄位 | 說明 |
|----------|--|
| 日期/時間 | 顯示故障的日期和時間戳。 |
| 上次失敗原因 | <p>顯示上次報告失敗的原因。即使清除故障條件，也不會清除此資訊。僅當發生故障切換時，此資訊才會更改。</p> <p>可能的失敗原因：</p> <ul style="list-style-type: none"> • Interface Failure — 符合故障切換條件並導致故障切換的介面數。 • 通訊故障 — 故障切換鏈路發生故障或對等裝置已關閉。 • 底板故障 |
| 狀態 | 顯示裝置的主要/輔助和主用/備用狀態。 |
| 此主機/其他主機 | 此主機指示在其上執行命令的裝置的資訊。另一台主機指示故障轉移對中另一台裝置的資訊。 |

```
<#root>
```

```
>
```

```
show failover descriptor
```

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

疑難排解

調試

```
<#root>
```

```
>
```

```
debug fover ?
```

```
cable          Failover LAN status
cmd-exec       Failover EXEC command execution
fail           Failover internal exception
fmsg           Failover message
```

```
ifc      Network interface status trace
open     Failover device open
rx       Failover Message receive
rxdump   Failover recv message dump (serial console only)
rxip     IP network failover packet recv
snort    Failover NGFW mode snort processing
switch   Failover Switching status
sync     Failover config/command replication
tx       Failover Message xmit
txdump   Failover xmit message dump (serial console only)
txip     IP network failover packet xmit
verify   Failover message verify
```

捕獲：

故障切换介面捕獲：

您可以參考此捕獲來確定故障切换hello資料包是否以傳送速率在故障切换鏈路上傳送。

```
<#root>
```

```
>
show capture

capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
>
show capture capfail
```

```
15 packets captured
```

```
1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

故障切换鏈路上的ARP捕獲：

您可以執行此擷取，檢視對等路由器是否在ARP表中具有Mac專案。

```
<#root>
>
show capture

capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
>
show capture caparp

22 packets captured

1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

案例

如果對等裝置未能加入HA組或在您從活動裝置部署更改時失敗，請登入到故障裝置，導航到「高可用性」頁，然後按一下「故障切換歷史記錄」連結。

APP-SYNC失敗

如果show failover history輸出指示App Sync失敗，則在HA驗證階段出現問題，在該階段系統檢查裝置能否作為高可用性組正常運行。

當From State為App Sync時，將顯示消息「All validation passed」（所有驗證通過），並且節點將移至Standby Ready狀態。

任何驗證失敗都會將對等體轉換為Disabled(Failed)狀態。解決這些問題，使對等體再次作為高可用性組運行。

請注意，如果您修復了應用同步錯誤並對活動單元進行了更改，則必須部署這些錯誤並恢復HA以便對等節點加入。

這些消息指示故障，並說明了如何解決問題。這些錯誤可能會在節點加入和每個後續部署上發生。

在節點加入時，系統會針對活動裝置上上次部署的配置執行檢查。

備用節點無法加入HA，因為「CD應用同步錯誤是應用配置應用失敗」

在待命FTD命令列/ngfw/var/log/action_queue.log上，必須存在組態失敗的原因。

修正：識別配置錯誤後，進行所需的更改後，可以恢復HA。

請參閱Cisco [錯誤ID CSCvu15611](#)。

<#root>

```
=====
From State          To State          Reason
=====
15:10:16 CDT Sep 28 2021
Not Detected        Disabled          No Error
15:10:18 CDT Sep 28 2021
Disabled           Negotiation      Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation        Cold Standby     Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby       App Sync         Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync           Disabled
CD App Sync error is App Config Apply Failed
=====
```

備用節點無法加入HA並顯示「由於APP SYNC超時，HA狀態進展失敗」

在待命FTD命令列/ngfw/var/log/ngfwmanager.log上，必須存在應用同步逾時的原因。

在這個階段，策略部署也會失敗，因為活動裝置認為應用同步仍在進行中。

策略部署引發錯誤 — 「由於newNode join/AppSync進程正在進行中，不允許進行配置更改，因此拒絕部署請求。請在一段時間後重試部署」

補救：有時，當您在備用節點上恢復高可用性時，它可以解決此問題。

請參閱思科錯誤ID [CSCvt48941](#)

請參閱思科錯誤ID [CSCvx11636](#)

<#root>

```
=====
From State          To State          Reason
=====
19:07:01 EST MAY 31 2021
Not Detected        Disabled          No Error
19:07:04 EST MAY 31 2021
Disabled           Negotiation      Set by the config command
19:07:06 EST MAY 31 2021
Negotiation        Cold Standby     Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby       App Sync         Detected an Active mate
21:11:18 EST Jun 30 2021
App Sync           Disabled
```

HA state progression failed due to APP SYNC timeout

備用節點無法加入HA，並顯示「CD應用同步錯誤無法在備用節點上應用SSP配置」

在待命FTD命令列/ngfw/var/log/ngfwmanager.log上，必須擁有失敗的確切原因。

補救：有時，當您在備用節點上恢復高可用性時，它可以解決此問題。

請參閱思科錯誤ID [CSCvy04965](#)

<#root>

```
=====
From State          To State          Reason
=====
04:15:15 UTC Apr 17 2021
Not Detected        Disabled          No Error
04:15:24 UTC Apr 17 2021
Disabled           Negotiation      Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation        Cold Standby     Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby       App Sync         Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync           Disabled
```

CD App Sync error is Failed to apply SSP config on standby

運行狀況檢查失敗

「HELLO not hearn from mate」表示該夥伴處於離線狀態，或者故障切換鏈路不通訊HELLO

keepalive消息。

嘗試登入到其他裝置，如果SSH不起作用，請訪問控制檯，並檢查裝置是否正常運行或離線。

如果可操作，請使用命令show failover state確定故障原因。

如果無法運行，請嘗試正常重新啟動並檢查控制檯上是否顯示任何啟動日誌，否則，裝置可能會被視為硬體故障。

<#root>

```
=====
From State          To State          Reason
=====
04:53:36 UTC Feb 6 2021
Failed              Standby Ready

Interface check

02:12:46 UTC Jul 11 2021
Standby Ready      Just Active      HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied Active           HELLO not heard from mate
=====
```

Snort關閉或磁碟故障

如果FTD提供此錯誤「Detect Inspection engine failure due to disk failure (檢測由於磁碟故障導致的檢測引擎故障)」，則有兩種可能性。

檢測引擎 (SNORT例項) 已關閉

這可透過Linux端的pmtool status命令驗證 | 格蕾普，

補救：如果任何例項發生故障，請檢查/ngfw/var/log/messages並確定原因。

裝置顯示磁碟使用率高

可以使用Linux端的命令df -Th進行驗證。

修復：確定佔用大部分磁碟的目錄，並聯絡TAC刪除不需要的檔案。

<#root>

```
=====
From State          To State          Reason
=====
Active Config Applied Active           No Active unit found
16:07:18 UTC Dec 5 2020
Active              Standby Ready    Other unit wants me Standby
```


16:07:20 UTC Dec 5 2020

Standby Ready Failed

Detect Inspection engine failure due to disk failure

16:07:29 UTC Dec 5 2020

Failed Standby Ready My Inspection engine is as good as peer due to di

服務卡故障

通常，由於ASA 5500-X裝置上的Firepower模組故障，會報告此類問題。請通過show module sfr details檢查模組是否正常。

補救：在出現故障時收集ASA系統日誌，這些日誌可能包含諸如控制或資料平面故障等詳細資訊。

這可能是由於SFR模組中的各種原因。建議開啟TAC，在IPS上查詢此問題的根本原因。

<#root>

```

=====
From State          To State          Reason
=====
21:48:19 CDT Aug 1 2021
Active              Standby Ready     Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready      Just Active
Service card in other unit has failed

21:48:19 CDT Aug 1 2021
Active Config Applied Active             Service card in other unit has failed
=====

```

MIO心跳故障

Firepower威脅防禦/ASA報告由於FPR1K、2K、4K和9K上的「MIO刀片心跳故障」導致的故障。

請參閱思科錯誤ID [CSCvy14484](#)

請參閱思科錯誤ID [CSCvh26447](#)

<#root>

```

=====
From State          To State          Reason
=====
20:14:45 EDT Apr 14 2021
Active Config Applied Active             No Active unit found
20:15:18 EDT Apr 14 2021
Active              Failed

```

MIO-blade heartbeat failure

20:15:19 EDT Apr 14 2021

Failed

Negotiation

MIO-blade heartbeat recovered

=====

相關資訊

- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html>
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。