

# 排除Firepower威胁防御高可用性问题的目录

## 目录

---

### [简介](#)

### [先决条件](#)

[要求](#)

[使用的组件](#)

### [背景信息](#)

[设计选项](#)

[HA术语](#)

[HA状态](#)

[HA状态流程图](#)

### [UI验证](#)

[Firepower管理中心托管FTD高可用性](#)

[FDM托管FTD高可用性](#)

[ASDM托管ASA HA](#)

[适用于4100/9300的Firepower机箱管理器 - 运行FTD/ASA HA](#)

### [验证CLI](#)

### [故障排除](#)

### [场景](#)

#### [APP-SYNC失败](#)

[备用节点无法加入HA - 显示“CD App Sync error is App Config Apply Failed”](#)

[备用节点无法加入HA并显示“由于APP SYNC超时，HA状态进展失败”](#)

[备用节点无法加入HA - 出现“CD App Sync error is Failed to apply SSP config on standby” \(CD应用同步错误无法在备用节点上应用SSP配置\)](#)

#### [运行状况检查失败](#)

#### [Snort关闭或磁盘故障](#)

[检测引擎 \(SNORT实例\) 已关闭](#)

[设备显示高磁盘利用率](#)

#### [服务卡故障](#)

#### [MIO心跳故障](#)

### [相关信息](#)

---

## 简介

本文档介绍Firepower威胁防御(FTD)高可用性(HA)的操作、验证和故障排除过程。

## 先决条件

### 要求

建议掌握下列主题的相关知识：

- FTD和ASA平台
- FTD设备上的数据包捕获

强烈建议阅读Firepower配置指南[在Firepower设备上配置FTD高可用性](#)，以更好地了解本文档中介绍的概念。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD
- 思科Firepower管理中心(FMC)

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。

## 背景信息

信息和示例基于FTD，但大多数概念也完全适用于自适应安全设备(ASA)。

FTD支持两种主要管理模式：

- 通过FMC进行机外 — 也称为远程管理
- 通过Firepower设备管理器(FDM)进行机上部署 — 也称为本地管理

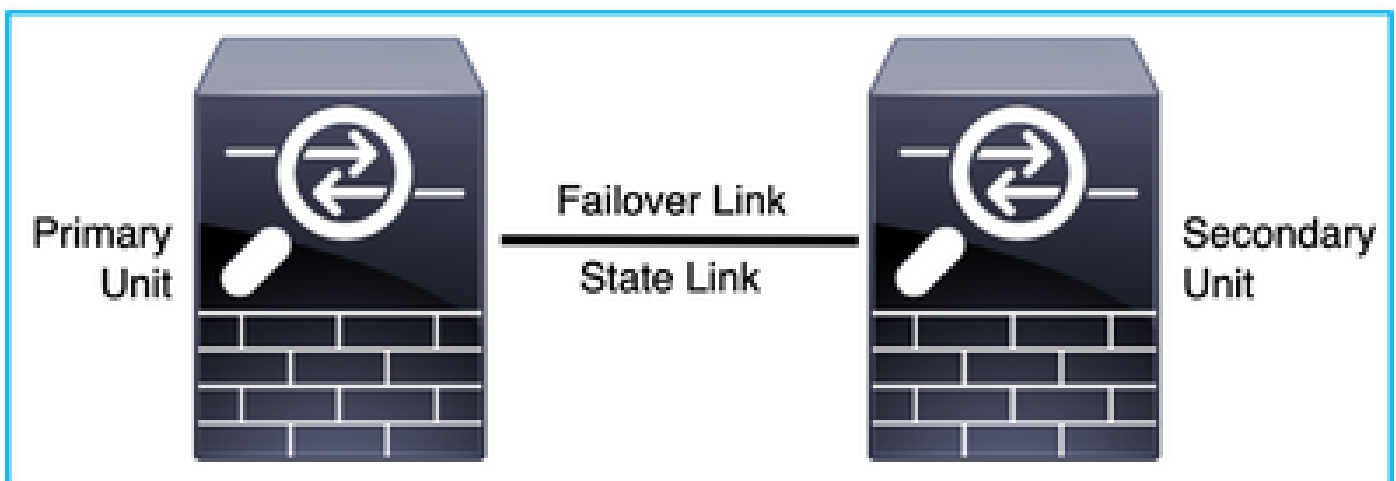
---

 注意：通过FDM管理的FTD可以从Firepower版本代码v6.3.0开始添加到高可用性中。

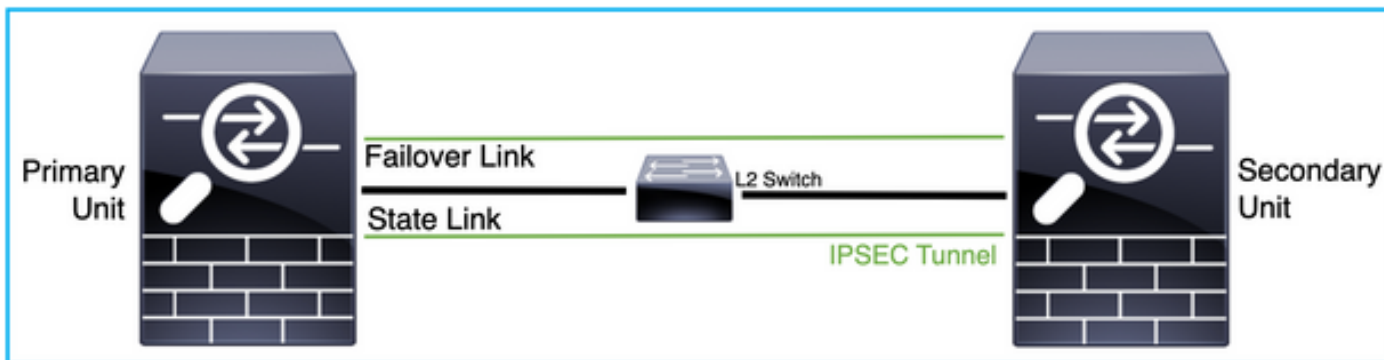
---

## 设计选项

从FTD的设计角度来看，它可以直接连接，如下图所示：



或者，它可以通过第2层(L2)交换机连接，如下图所示：



## HA术语

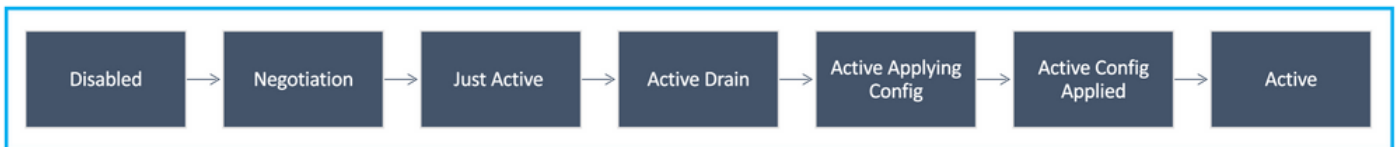
主用	活动ASA接收所有流量并过滤所有网络流量。配置更改在活动ASA上进行。
高可用性链路	故障切换对中的两台设备通过故障切换链路持续通信，以确定每台设备的运行状态并同步配置更改。通过链路共享的信息是： <ul style="list-style-type: none"> <li>• 设备状态（主用或备用）</li> <li>• Hello消息（保持连接）</li> <li>• 网络链路状态</li> <li>• MAC地址交换</li> <li>• 配置复制和同步</li> </ul>
主	这是通常在您创建HA时首先配置的设备。其意义在于，如果ASA HA的两台设备在同一时刻同时出现，则主设备将承担活动角色。
辅助	这是通常在创建HA时第二个配置的设备。此功能的意义在于，如果ASA HA的两个设备在同一时刻一起运行，则辅助设备将承担备用角色。
备用	备用ASA不处理任何实时流量，它同步来自主用设备的连接和配置，并在发生故障切换时承担主用角色。
状态链路	主用设备使用状态链路将连接状态信息传递给备用设备。因此，备用设备可以维护某些类型的连接，而不会影响到您。此信息可帮助备用设备在发生故障切换时保持存在的连接。NB：当您同一链路用于故障切换和有状态故障切换时，您会以最佳方式节省接口。但是，如果您有大型配置和高流量网络，则必须考虑为状态链路和故障切换链路提供专用接口。我们建议有状态故障切换链路的带宽必须匹配设备上数据接口的最大带宽。

## HA状态

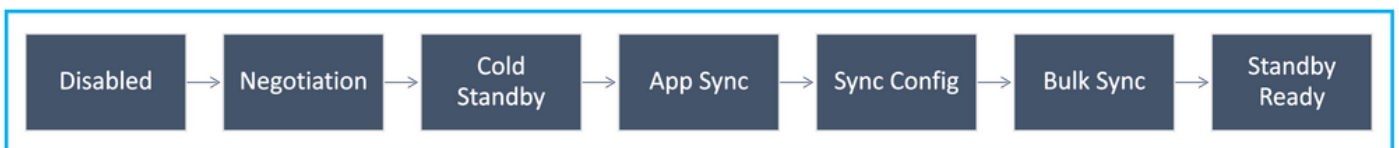
主用	设备当前处理网络上的实时流量，需要完成的所有配置更改都在此设备上执行。
应用同步	处于此状态的设备会同步来自活动设备的配置。
批量同步	处于此状态的设备会同步来自活动设备的配置。
禁用	已禁用设备上的故障切换（命令：no failover）。
协商	设备会检查活动设备的可用性，如果发现活动设备未准备好备用，则设备会承担活动角色。
备用就绪	设备当前不处理流量，但是如果活动设备显示任何运行状况检查问题，则设备将承担活动角色。
同步配置	配置会从主用设备复制到备用设备。
冷备份	设备在故障切换时作为主用设备接管，但不会复制连接事件。

## HA状态流程图

主（无任何连接的对等体）：



辅助（具有活动连接的对等体）：



## UI验证

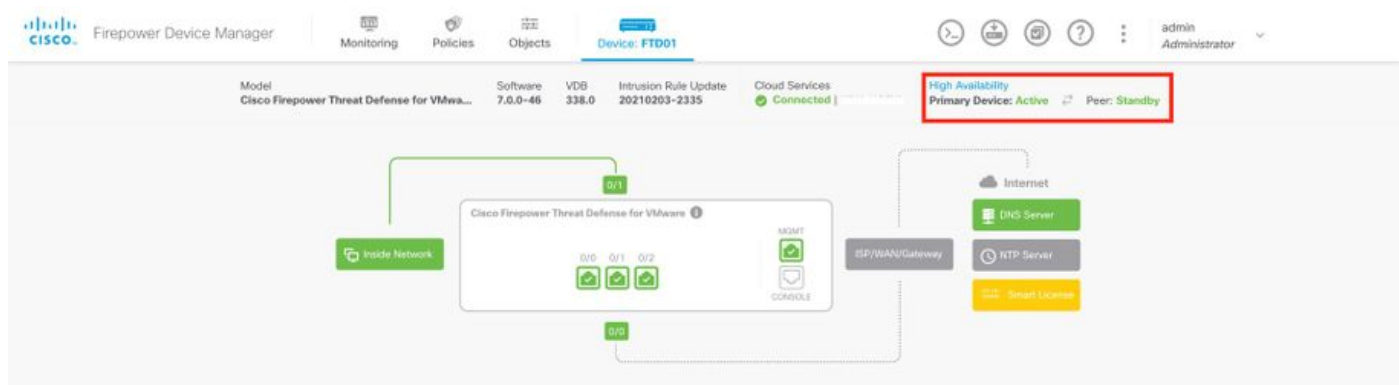
## Firepower管理中心托管FTD高可用性

导航到Device > Device Management时，可以从FMC UI检查FTD HA状态，如下图所示：

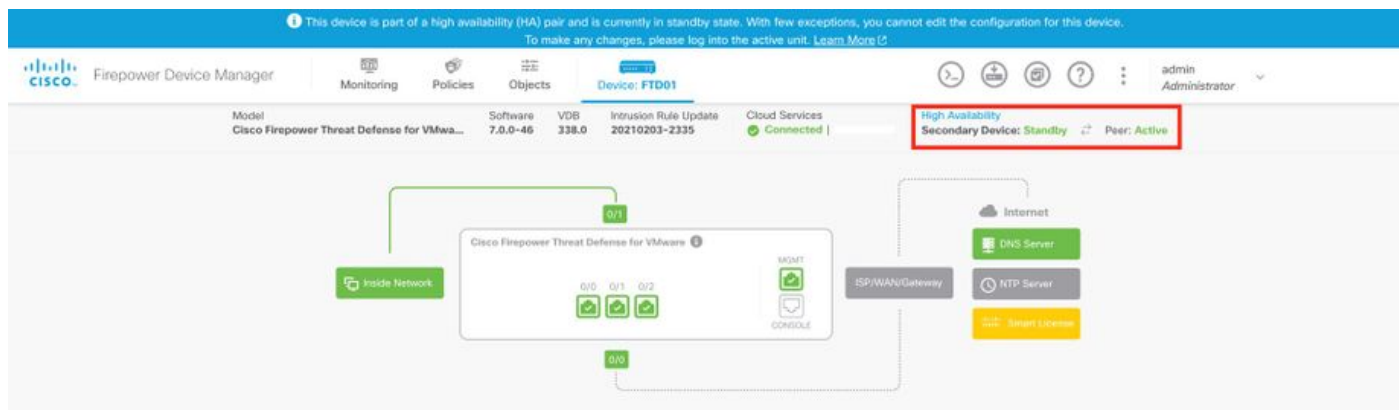
Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (1)					
FTD-HA High Availability					
FTD01(Primary, Active) Snort 3 10.197.224.69 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base
FTD02(Secondary, Standby) Snort 3 10.197.224.89 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base

## FDM托管FTD高可用性

主FDM概述页：



辅助FDM概览页：



## ASDM托管ASA HA

ASDM主页到主ASA:

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)**

**VPN Summary**

IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0

**System Resources Status**

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

1977MB  
32.40.41

**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

ASDM主页到辅助ASA:

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)**

**VPN Summary**

IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0

**System Resources Status**

Total Memory Usage Total CPU Usage Core Usage Details

Memory Usage (MB)

1979MB  
32.43.21

**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.

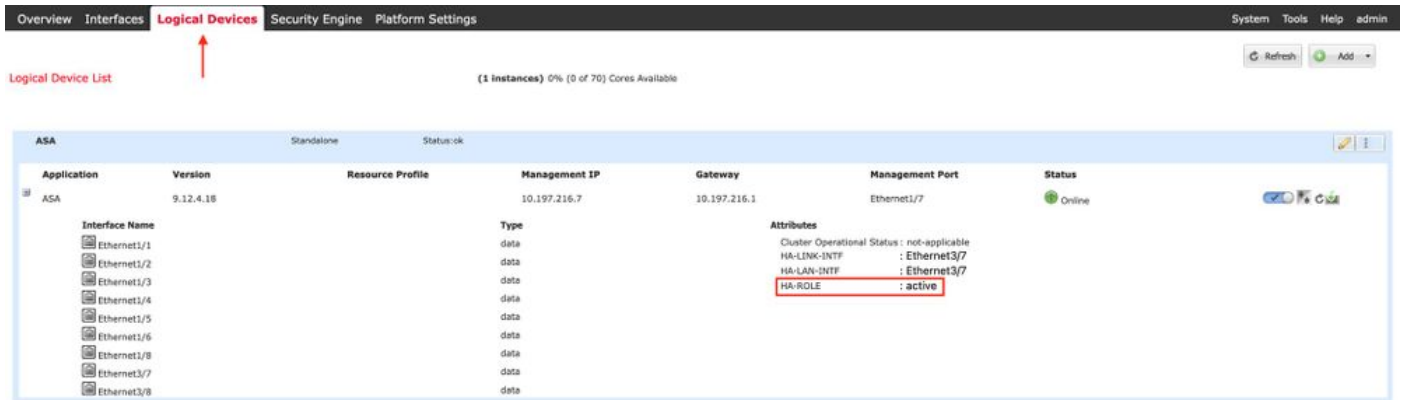
Enable Logging

Device configuration loaded successfully.

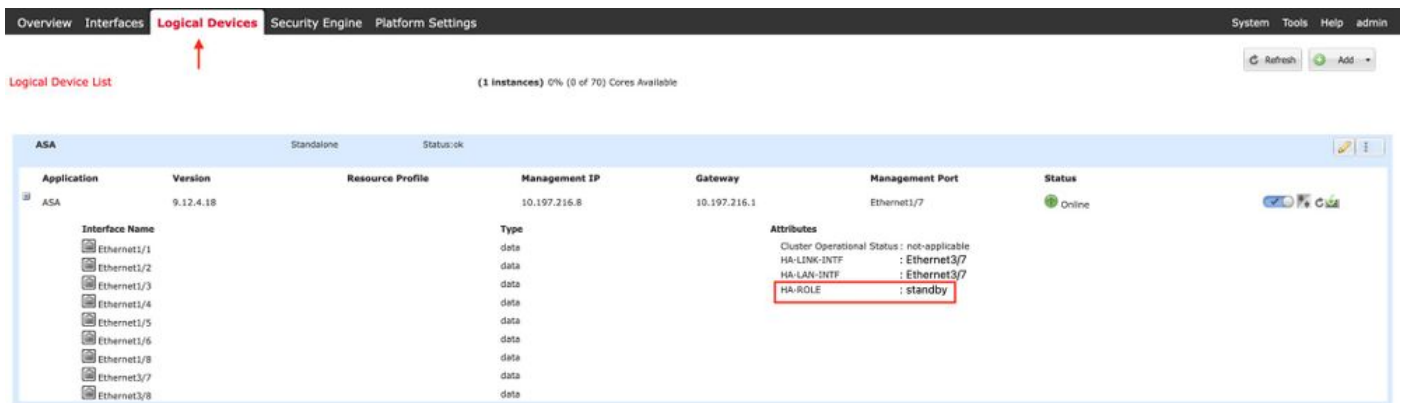
Standby admin 15 25/11/21 2:43:25 AM UTC

适用于4100/9300的Firepower机箱管理器，运行FTD/ASA HA

主FCM逻辑设备页面：



辅助FCM逻辑设备页面：



## 验证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
```

这里需要考虑的要点包括：

### 故障转移

failover lan unit secondary —>设备是主设备还是辅助设备

failover lan interface failover-link GigabitEthernet0/2 —>设备上的故障切换链路物理接口

故障切换复制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 —>主设备和备用

设备故障切换链路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

故障切换开启：故障切换已启用或已禁用。

此主机：辅助 — 备用就绪。此设备的角色和接口的状态。

其他主机：主 — 活动。另一台设备处于Active状态并与当前设备通信。

<#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
=====

```

使用此命令检查设备的历史状态以及这些状态更改的原因：

<#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
```

检查设备的当前状态和上次故障切换的原因：

字段	描述
配置状态	<p>显示配置同步的状态。</p> <p>备用设备的可能配置状态：</p> <ul style="list-style-type: none"><li>• Config Syncing - STANDBY — 执行同步配置时设置。</li><li>• 接口配置同步 — 备用</li><li>• Sync Done - STANDBY — 在备用设备从主用设备完成配置同步时设置。</li></ul> <p>主用设备可能的配置状态：</p> <ul style="list-style-type: none"><li>• Config Syncing — 当主用设备与备用设备执行配置同步时，在主用设备上设置。</li><li>• 接口配置同步</li><li>• Sync Done — 当主用设备成功完成与备用设备的配置同步时设置。</li><li>• Ready for Config Sync — 当备用设备发出准备好接收配置同步信号时，在主用设备上设置。</li></ul>
通信状态	<p>显示MAC地址同步的状态。</p> <ul style="list-style-type: none"><li>• Mac set - MAC地址已从对等设备同步到此设备。</li><li>• 更新的Mac — 当MAC地址更新并需要同步到其他设备时使用。在设备更新从对等设备同步的本地MAC地址时也使用。</li></ul>

字段	描述
日期/时间	显示故障的日期和时间戳。
上次失败原因	<p>显示上次报告失败的原因。即使清除故障条件，也不会清除此信息。仅当发生故障切换时，此信息才会更改。</p> <p>可能的故障原因：</p> <ul style="list-style-type: none"> <li>• Interface Failure — 出现故障的接口数符合故障切换条件并导致故障切换。</li> <li>• Comm Failure — 故障切换链路发生故障或对等体关闭。</li> <li>• 底板故障</li> </ul>
状态	显示设备的主要/辅助和主用/备用状态。
此主机/其他主机	此主机指示在其上执行命令的设备的信息。另一台主机指示故障切换对中另一台设备的信息。

```
<#root>
```

```
>
```

```
show failover descriptor
```

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

## 故障排除

调试

```
<#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
```

捕获：

故障切换接口捕获：

您可以参考此捕获来确定故障切换hello数据包是否以发送速率在故障切换链路上发送。

```
<#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
```

故障切换链路上的ARP捕获：

您可以利用此捕获查看对等体在ARP表中是否有Mac条目。

```
<#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
```

```
>
```

## 场景

如果对等设备无法加入HA组或在您从主用设备部署更改时失败，请登录故障设备，导航到High Availability页面，然后点击Failover History链接。

### APP-SYNC失败

如果show failover history输出指示App Sync失败，则在HA验证阶段出现问题，在该阶段系统检查设备能否作为高可用性组正常运行。

当From State为App Sync时，系统显示消息“All validation passed”，并且节点将变为Standby Ready状态。

任何验证失败都会将对等体转换为Disabled(Failed)状态。解决这些问题，使对等体再次作为高可用性组运行。

请注意，如果您修复了应用同步错误并对主用设备进行了更改，则必须部署这些错误并恢复HA，以便对等节点加入。

这些消息指示故障，并说明了如何解决这些问题。这些错误可能会在节点加入和每个后续部署上发生。

在节点加入时，系统会根据主用设备上上次部署的配置执行检查。

备用节点无法加入HA，显示“CD App Sync error is App Config Apply Failed”

在Standby FTD命令行上，/ngfw/var/log/action\_queue.log必须具有配置失败的原因。

补救：识别配置错误后，可继续执行HA所需的更改。

请参阅Cisco bug [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
=====
```

备用节点无法加入HA并显示“由于APP SYNC超时，HA状态进展失败”

在Standby FTD命令行上，/ngfw/var/log/ngfwmanager.log必须具有应用同步超时的原因。

在此阶段，策略部署也会失败，因为主用设备认为应用同步仍在进行中。

策略部署引发错误 — “由于newNode join/AppSync进程正在进行中，不允许配置更改，因此拒绝部署请求。请稍后重试部署”

补救：有时，当您在备用节点上恢复高可用性时，它可以解决此问题。

请参阅思科漏洞ID [CSCvt48941](#)

请参阅思科漏洞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
=====
```

备用节点无法加入HA，出现“CD App Sync error is Failed to apply SSP config on standby”（CD应用同步错误无法在备用节点上应用SSP配置）

在Standby FTD命令行上，/ngfw/var/log/ngfwmanager.log必须具有故障的确切原因。

补救：有时，当您在备用节点上恢复高可用性时，它可以解决此问题。

请参阅思科漏洞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
=====
```

## 运行状况检查失败

“HELLO not hearen from mate”表示该伙伴处于离线状态，或者故障切换链路不通信HELLO keepalive消息。

尝试登录到另一台设备，如果SSH不起作用，请访问控制台，并检查设备是否运行正常或脱机。

如果正常工作，请使用命令show failover state确定故障原因。

如果不运行，请尝试正常重新启动，并检查控制台上是否显示任何启动日志，否则，设备可能会被视为硬件故障。

<#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关闭或磁盘故障

如果FTD出现此错误“Detect Inspection engine failure due to disk failure”，则有两种可能性。

检测引擎 ( SNORT实例 ) 已关闭

这可以通过Linux端的命令pmtool status来验证 | grep -i de

补救：如果任何实例发生故障，请检查/ngfw/var/log/messages并确定原因。

设备显示高磁盘利用率

这可以通过Linux端的命令df -Th进行验证。

修复：确定消耗大部分磁盘的目录，并联系TAC删除不需要的文件。

<#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
=====

```

## 服务卡故障

通常，由于ASA 5500-X设备上的Firepower模块故障，会报告此类问题。请通过show module sfr details检查模块是否正常。

补救：在出现故障时收集ASA系统日志，这些日志可能包含控制或数据平面故障等详细信息。

这可能是由于SFR模块中的各种原因。建议打开TAC以在IPS上查找此问题的根本原因。

<#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威胁防御/ASA在FPR1K、2K、4K和9K上报告由于“MIO-blade心跳故障”导致的故障。

请参阅思科漏洞ID [CSCvy14484](#)

请参阅思科漏洞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

=====

## 相关信息

- <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](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185)
- [技术支持和文档 - Cisco Systems](#)

## 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）。