# 在 Firepower 设备上配置 FTD 高可用性

## 目录


简介

先决条件

- 要求
- 使用的组件

任务1.检验条件

任务2.配置FTD HA

- 条件

任务 3. 验证 FTD HA 和许可证

任务 4. 调换故障切换角色

任务 5. 中断 HA 对

任务6.删除高可用性对

任务 7. 暂停 HA

常见问题解答 (FAQ)

相关信息


## 简介

本文档介绍如何在Firepower设备上配置和验证Firepower威胁防御(FTD)高可用性(HA)。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 2个Cisco Firepower 9300
- 2个Cisco Firepower 4100(7.2.8)
- Firepower管理中心(FMC)(7.2.8)

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。

注意：在带有FTD的FPR9300设备上，只能配置机箱间HA。HA配置中的两个单元必须满足此处提到的条件。

# 任务1.检验条件

任务要求：

检验两台FTD设备是否满足注释要求，以及是否可配置为HA设备。

解决方案：

第 1 步： 连接到 FPR9300 管理 IP 并验证模块硬件。

验证FPR9300-1硬件：

<#root>

```
KSEC-FPR9K-1-A#

show server inventory

Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19216KK6          Equipped                  262144         36
1/2     FPR9K-SM-36  V01          FLM19206H71          Equipped                  262144         36
1/3     FPR9K-SM-36  V01          FLM19206H7T          Equipped                  262144         36
KSEC-FPR9K-1-A#
```

验证FPR9300-2硬件：

<#root>

```
KSEC-FPR9K-2-A#

show server inventory

Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
```

```
1/1       FPR9K-SM-36  V01          FLM19206H9T          Equipped                  262144          36
1/2       FPR9K-SM-36  V01          FLM19216KAX          Equipped                  262144          36
1/3       FPR9K-SM-36  V01          FLM19267A63          Equipped                  262144          36
KSEC-FPR9K-2-A#
```

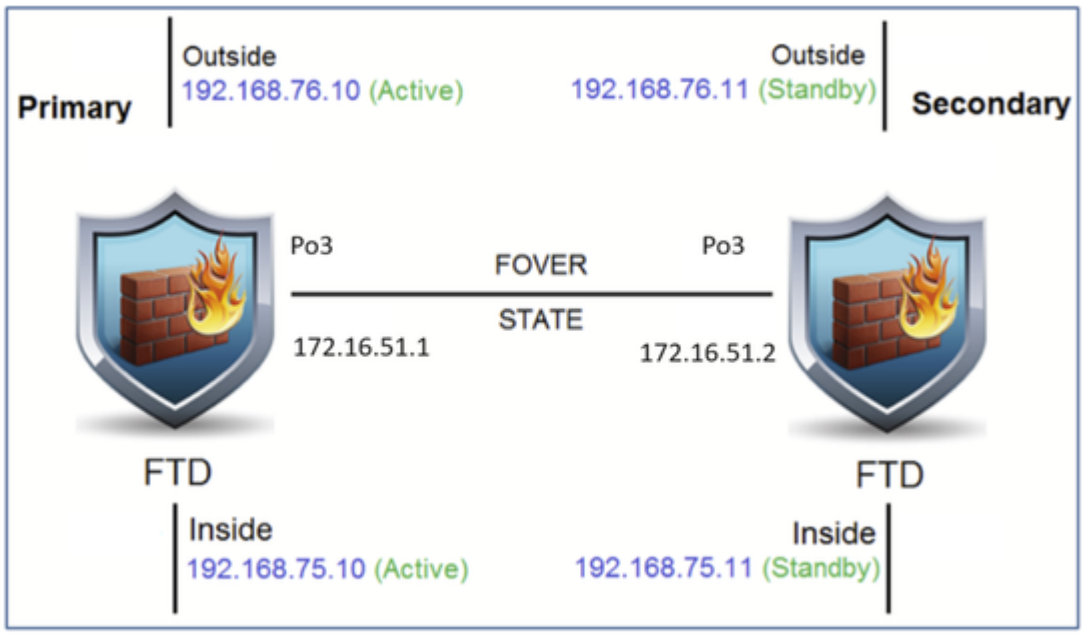
步骤2.登录到FPR9300-1 Chassis Manager并导航到Logical Devices。

步骤3.检验软件的版本、编号和接口类型。

# 任务2.配置FTD HA

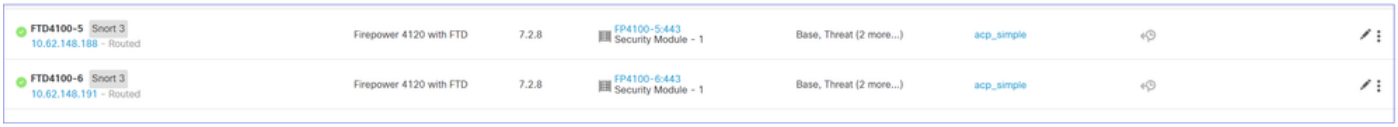
任务要求：

步骤1.根据图配置主用/备用故障切换(HA)。在本例中，使用41xx对。

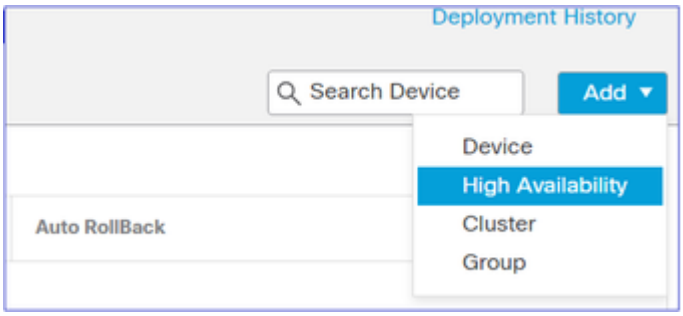



解决方案

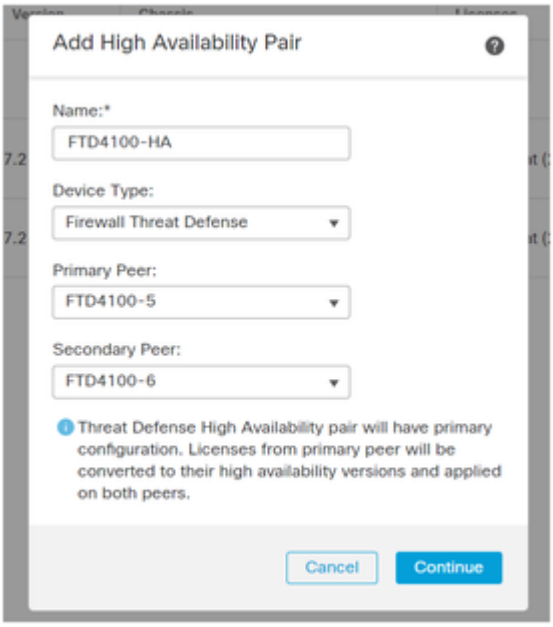
两台FTD设备均在FMC上注册。




步骤1.要配置FTD故障切换，请导航到设备>设备管理，然后选择添加高可用性。




步骤2.输入Primary Peer和Secondary Peer，然后选择Continue。




警告：确保选择正确的设备作为主设备。所选主设备上的所有配置都将复制到所选辅助FTD设备。通过复制，可以替换辅助设备上的当前配置。

## 条件

要在两个FTD设备之间创建HA，必须满足以下条件：

- 相同型号
- 相同版本适用于FXOS和FTD — 主要（第一个号码）、次要（第二个号码）和维护（第三个号码）必须相等。
- 相同数量的接口数
- 相同类型的接口
- 两台设备在FMC中属于同一个组/域
- 具有相同的网络时间协议(NTP)配置

- 必须完全部署在FMC上，且无未提交的更改
- 必须处于同一防火墙模式：路由或透明

---



注意：必须在FTD设备和FMC GUI上检查此项，因为已经有FTD具有相同模式的情况，但FMC不会反映这种情况。

---

- 没有在任何接口上配置DHCP/以太网点对点协议(PPPoE)。
- 两个机箱的不同主机名[完全限定域名(FQDN)]。要检查机箱主机名，请导航至FTD CLI并运行以下命令：

```
<#root>

firepower#

show chassis-management-url


https://

KSEC-FPR9K-1.cisco.com

:443//
```

---

 注意：在6.3 FTD之后的版本中，使用命令show chassis detail。

---

```
<#root>

Firepower-module1#

show chassis detail



Chassis URL : https://FP4100-5:443//


Chassis IP : 10.62.148.187
Chassis IPv6 : ::
Chassis Serial Number : JAD19500BAB
Security Module : 1
```

如果两个机箱的名称相同，请使用以下命令更改一个机箱的名称：

<#root>

```
KSEC-FPR9K-1-A#

scope system

KSEC-FPR9K-1-A /system #

set name FPR9K-1new

Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #

commit-buffer

FPR9K-1-A /system #

exit


FPR9K-1new-A

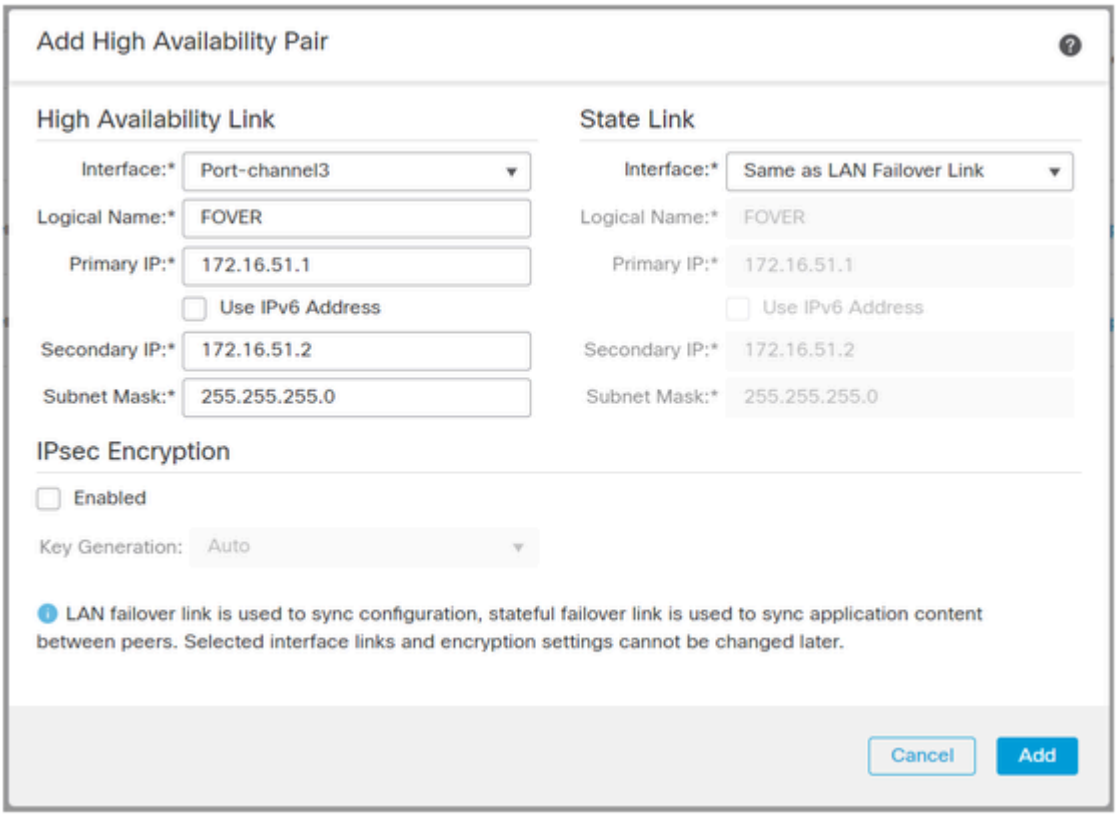
#
```

更改机箱名称后，从FMC取消注册FTD，然后重新注册。然后继续创建 HA 对。

第 3 步： 配置 HA 和状态链路设置。

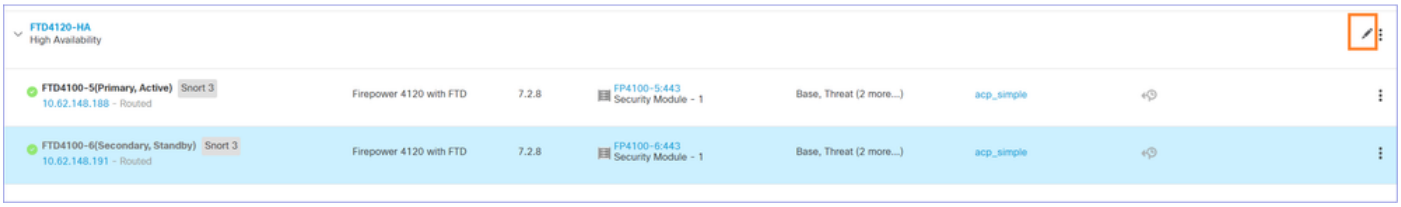
在这种情况下，状态链路的设置与高可用性链路的设置相同。

步骤4.选择Add并等待几分钟，以便部署HA对。

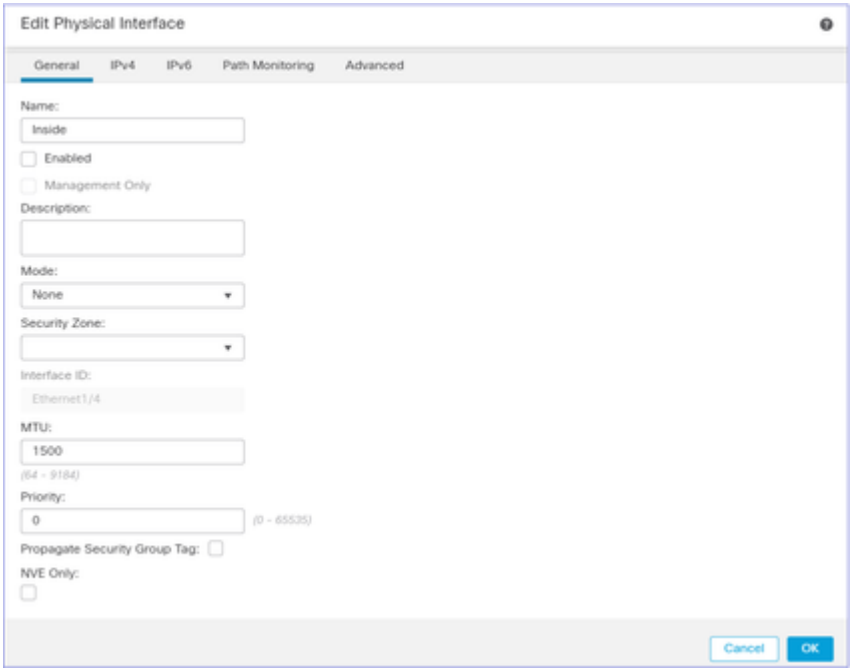


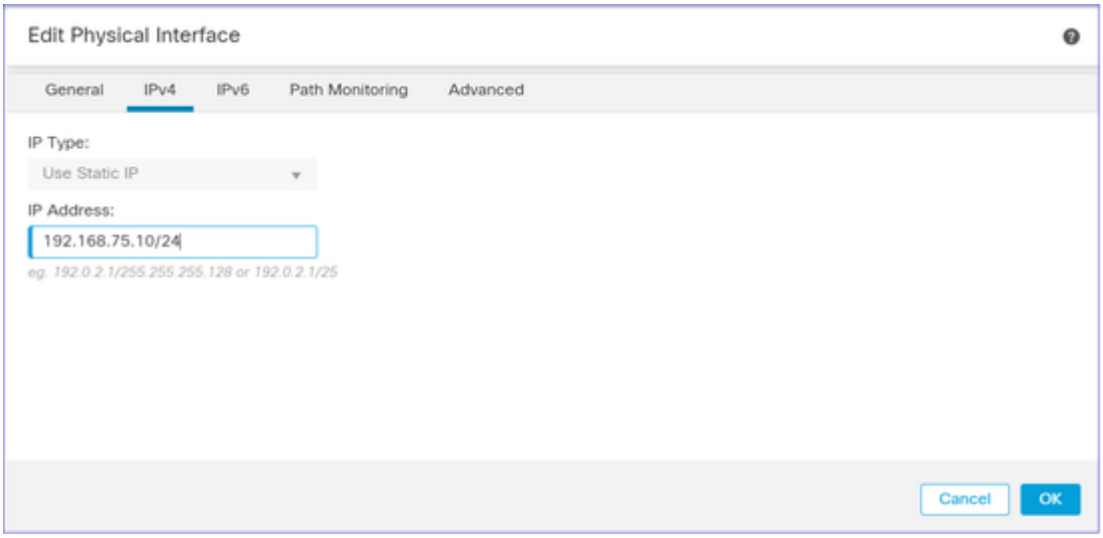

步骤5.配置数据接口（主要和备用IP地址）。

步骤6.从FMC GUI中选择HA Edit。

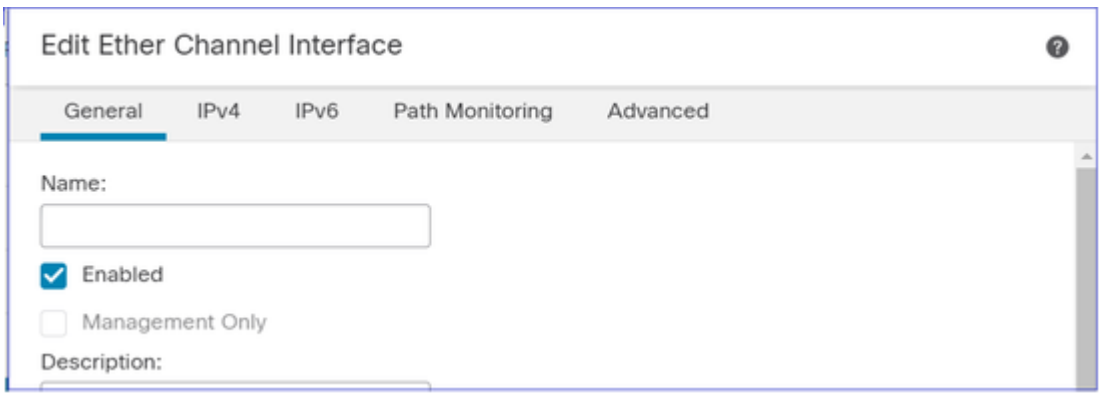



步骤7.配置接口设置：

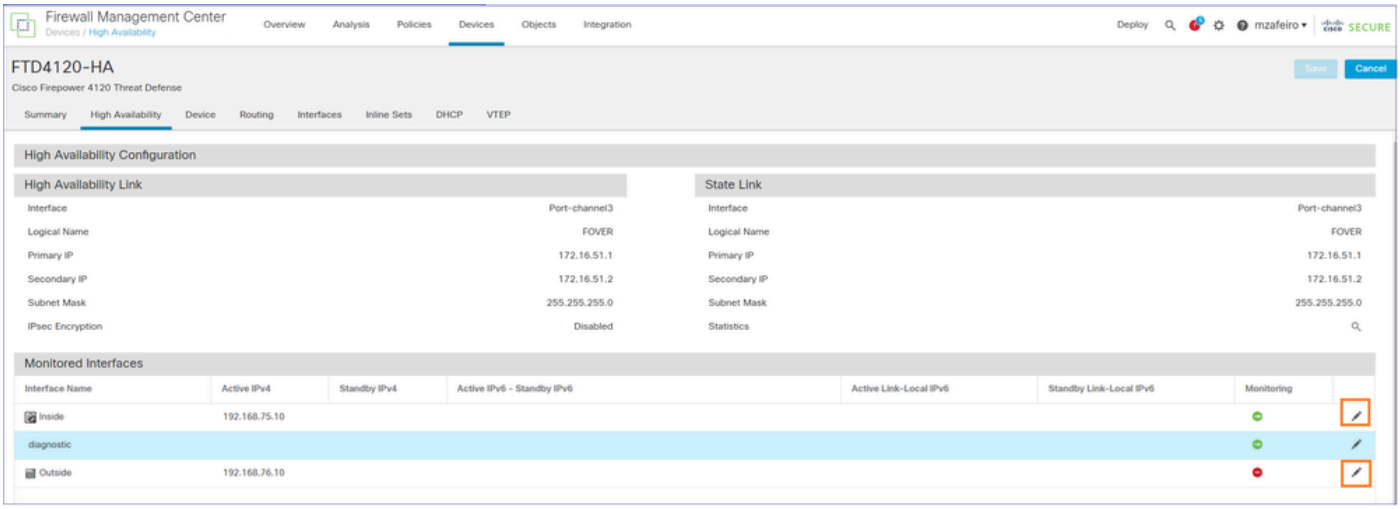


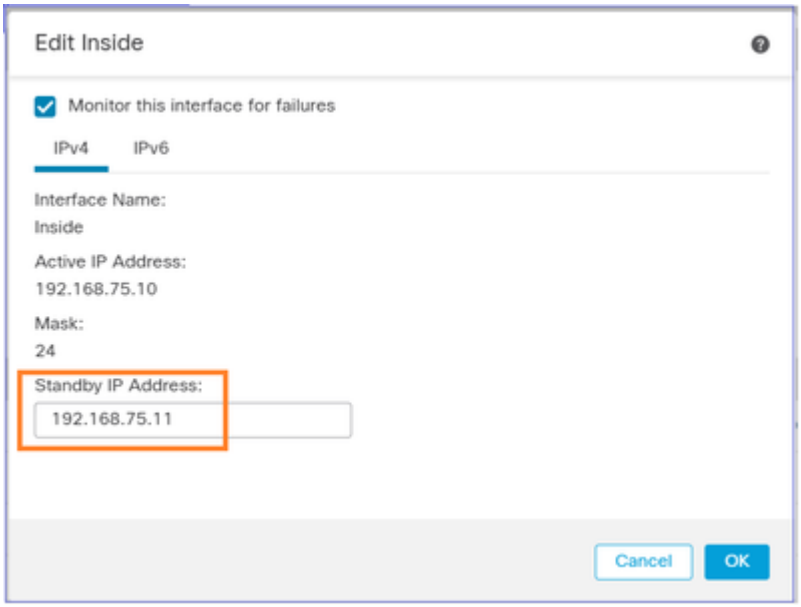




对于子接口，必须启用父接口：




步骤8.导航到高可用性并选择接口名称，然后单击编辑以添加备用IP地址。



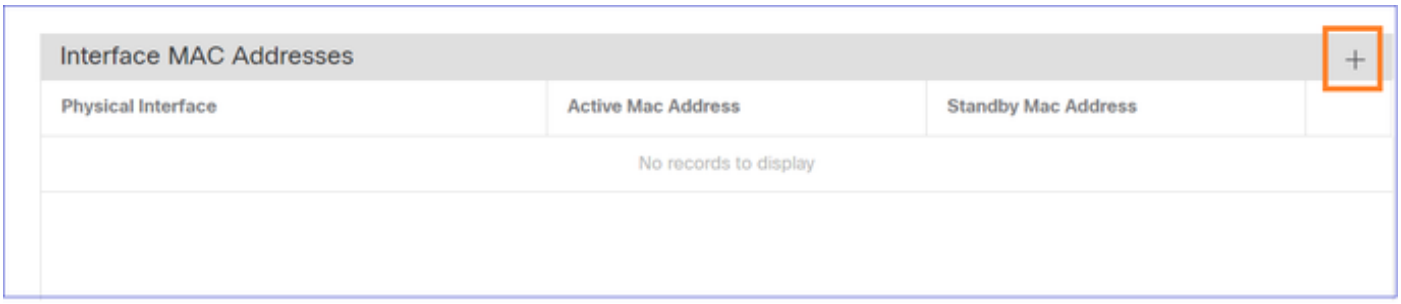




步骤9.完成与外部接口相同的步骤。

步骤10.检验结果。




步骤11.保持高可用性选项卡，并配置虚拟MAC地址。




步骤12.内部接口映像。




步骤13.完成与外部接口相同的步骤。

步骤14.检验结果。




步骤15.配置更改后，选择Save和Deploy。

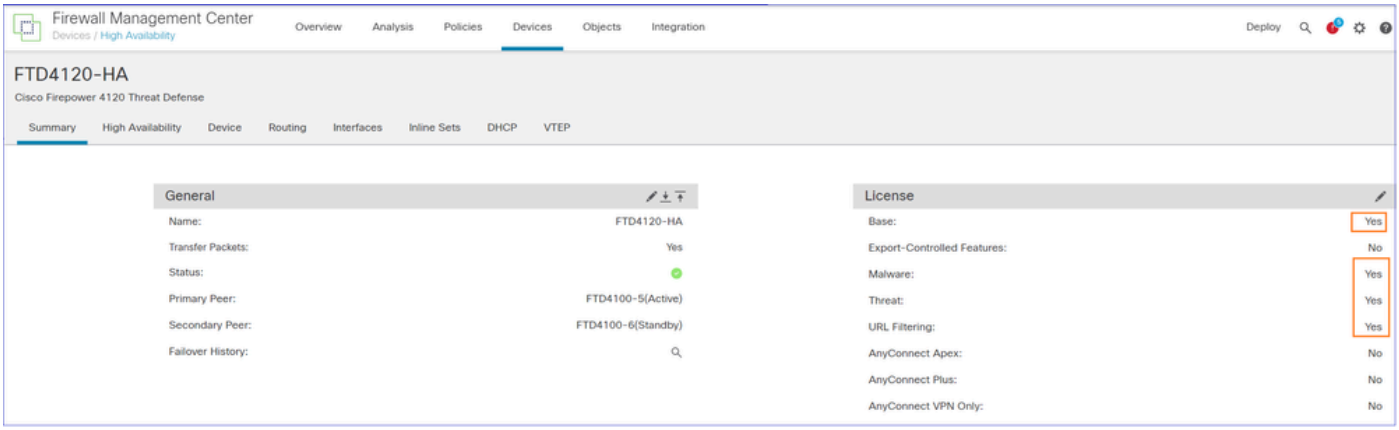
# 任务 3. 验证 FTD HA 和许可证

任务要求：

验证FTD HA设置并从FMC GUI和FTD CLI启用许可证。

解决方案：

步骤1.导航到Summary并选中HA设置并启用许可证。




步骤2.从FTD CLISH CLI运行show high-availability config或show failover命令：

<#root>

>

**show high-availability config**

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel3 (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 2 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG
Last Failover at: 08:46:30 UTC Jul 18 2024
```

**This host: Primary - Active**

```
                Active time: 1999 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.10): Link Down (Shutdown)
                  Interface Outside (192.168.76.10): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
```

```
                slot 2: diskstatus rev (1.0) status (up)


Other host: Secondary - Standby Ready


                Active time: 1466 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.11): Link Down (Shutdown)
                  Interface Outside (192.168.76.11): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
<output omitted>
```

步骤3.在辅助设备上完成相同步骤。

第 4 步： 从 LINA CLI 上运行 show failover state 命令：

<#root>

```
firepower#

show failover state


               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             18:32:56 EEST Jul 21 2016

====Configuration State===
    Sync Done
====Communication State===
    Mac set

firepower#
```

步骤5.从主设备(LINA CLI)验证配置设置：

<#root>

```
>

show running-config failover
```

```
failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2

>
```

**show running-config interface**

```
!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
shutdown
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
>
```

# 任务 4. 调换故障切换角色

任务要求：

从 FMC 上将故障切换角色从主/主用、辅助/备用切换到主/备用、和辅助/主用.

解决方案：

步骤1.选择图标。




步骤2.确认操作。

您可以使用show failover history命令输出：

| 在新的Active | 在新备 |
| --- | --- |
| > show failover history<br>==========<br>从状态到状态原因<br>==========<br><br>世界协调时2024年7月18日09:27:11<br>备用就绪仅激活其他设备希望我激活<br>（通过config命令设置）<br><br>世界协调时2024年7月18日09:27:11<br>仅活动活动排出其他单元希望我处于活动状态<br>（通过config命令设置）<br><br>世界协调时2024年7月18日09:27:11<br>Active Drain Active Applying Config其他设备要激活<br>（通过config命令设置）<br><br>世界协调时2024年7月18日09:27:11<br>Active Applying Config Active Config Applied Other unit deses me Active<br>（通过config命令设置）<br><br>世界协调时2024年7月18日09:27:11<br>Active Config Applied Active Other Unit deses me Active<br>（通过config命令设置） | > show<br>======<br>从状态<br>======<br><br>世界协<br>通过co |

步骤3.检验后，使主设备再次激活。

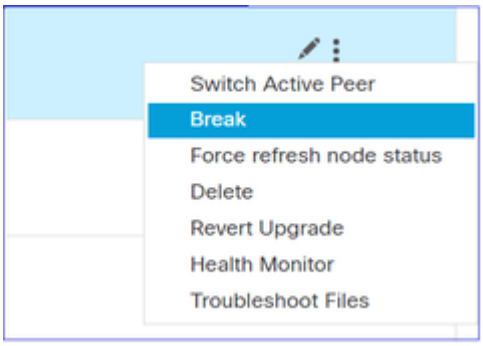
# 任务 5. 中断 HA 对

任务要求：

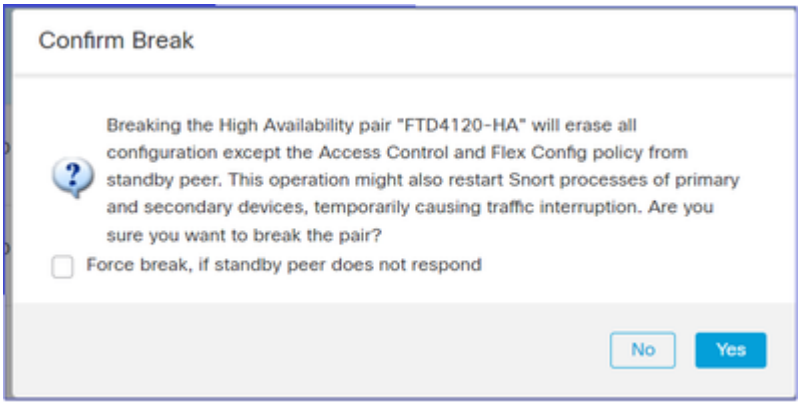
从 FMC 上中断故障切换对。

解决方案：

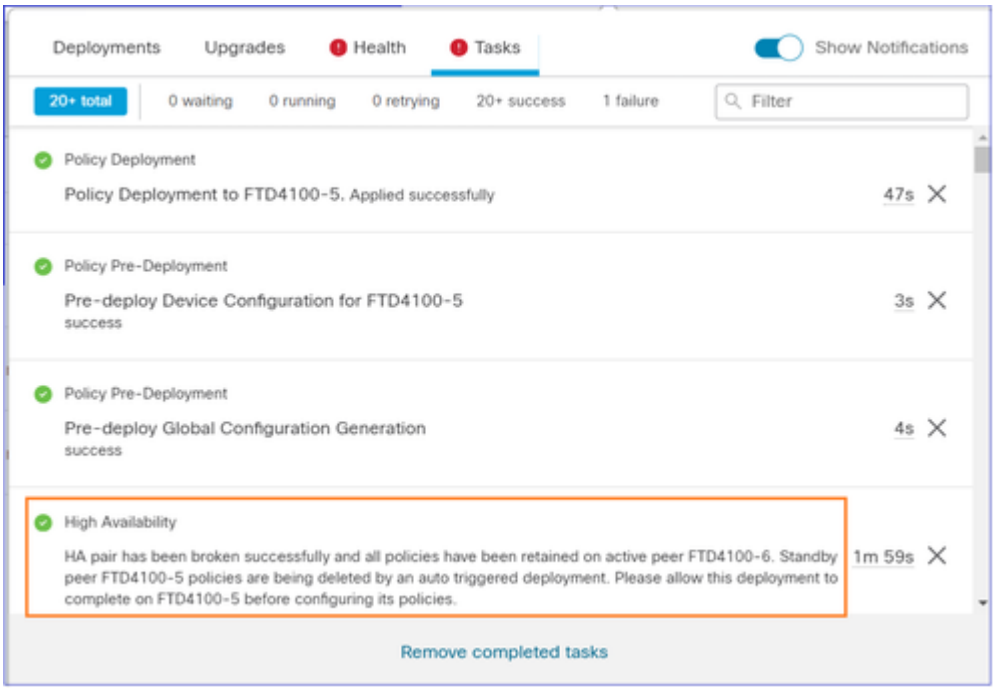
步骤1.选择图标。




步骤2.查看通知。




步骤3.记录消息。




步骤4.从FMC GUI或CLI检验结果。

步骤5.在HA中断前后在主设备上显示running-config:

| 高可用性中断前的主/备用设备 | 高可用性中断后的主设备 |
| --- | --- |
| > show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM1949C5RR<br>:Hardware:FPR4K-SM-24,73850 MB RAM，CPU Xeon E5系列2200 MHz，2 CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname firepower<br>enable password ***** encrypted<br>strong-encryption-disable<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto<br><br>!<br>interface Port-channel2<br>no nameif | >信息：此设备当前处于备用状态。通过禁用故障切换，此设备将保持备用状态。<br><br>> show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM1949C5RR<br>:Hardware:FPR4K-SM-24,73850 MB RAM，CPU Xeon E5系列2200 MHz，2 CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname firepower<br>enable password ***** encrypted<br>strong-encryption-disable<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto |

cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
无安全级别
no ip address
!
interface Port-channel2.202
vlan 202
nameif外部
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
说明LAN/STATE故障切换接口
!
interface Ethernet1/1
仅管理
nameif diagnostic
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
no ip address
!
interface Ethernet1/4
nameif内部
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id 9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit

!
interface Port-channel2
shutdown
no nameif
无安全级别
no ip address
!
interface Port-channel3
shutdown
no nameif
无安全级别
no ip address
!
interface Ethernet1/1
仅管理
shutdown
no nameif
无安全级别
no ip address
!
interface Ethernet1/4
shutdown
no nameif
无安全级别
no ip address
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id 9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998

ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434433:访问策略:acp_simple — 默认
access-list CSM_FW_ACL_ remark rule-id 268434433:L4规则：默认操作规则
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
无传呼机
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
1500以外的MTU
mtu diagnostic 1500
mtu内部1500
故障转移
failover lan unit primary
failover lan interface FOVER Port-channel3
故障切换复制http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
access-list CSM_FW_ACL_ remark rule-id 268439552:访问策略:acp_simple — 必填
access-list CSM_FW_ACL_ remark rule-id 268439552:L7规则：rule1
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
urgent-flag allow
!
无传呼机
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
不执行故障切换
<省略部分输出>

| | |
|---|---|
| failover mac address Port-channel2.202<br>aaaa.bbbb.3333 aaaaa.bbbb.4444<br>failover link FOVER Port-channel3<br>failover interface ip FOVER 172.16.51.1<br>255.255.255.0 standby 172.16.51.2<br><br><省略部分输出> | |

| 高可用性中断前的辅助/主用设备 | 高可用性中断后的辅助设备 |
|---|---|
| >show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM2108V9YG<br>:Hardware:FPR4K-SM-24,73850 MB<br>RAM，CPU Xeon E5系列2200 MHz，2<br>CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname firepower<br>enable password ***** encrypted<br>strong-encryption-disable<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto<br><br>!<br>interface Port-channel2<br>no nameif<br>无安全级别<br>no ip address<br>!<br>interface Port-channel2.202<br>vlan 202<br>nameif外部<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 192.168.76.10 255.255.255.0<br>standby 192.168.76.11<br>! | > show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM2108V9YG<br>:Hardware:FPR4K-SM-24,73850 MB<br>RAM，CPU Xeon E5系列2200 MHz，2<br>CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname firepower<br>enable password ***** encrypted<br>strong-encryption-disable<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto<br><br>!<br>interface Port-channel2<br>no nameif<br>无安全级别<br>no ip address<br>!<br>interface Port-channel2.202<br>vlan 202<br>nameif外部<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 192.168.76.10 255.255.255.0<br>standby 192.168.76.11 |

```
interface Port-channel3
说明LAN/STATE故障切换接口
!
interface Ethernet1/1
仅管理
nameif diagnostic
安全级别0
no ip address
!
interface Ethernet1/4
nameif内部
安全级别0
ip address 192.168.75.10 255.255.255.0
standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id
9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id
9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id
9998
access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268439552:访问策略:acp_simple — 必填
access-list CSM_FW_ACL_ remark rule-id
268439552:L7规则：rule1
access-list CSM_FW_ACL_ advanced permit ip
any any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
```

```
!
interface Port-channel3
no nameif
无安全级别
no ip address
!
interface Ethernet1/1
仅管理
nameif diagnostic
安全级别0
no ip address
!
interface Ethernet1/4
nameif内部
安全级别0
ip address 192.168.75.10 255.255.255.0
standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id
9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id
9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id
9998
access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268439552:访问策略:acp_simple — 必填
access-list CSM_FW_ACL_ remark rule-id
268439552:L7规则：rule1
access-list CSM_FW_ACL_ advanced permit ip
any any rule-id 268439552
!
tcp-map UM_STATIC_TCP_MAP
```

| | |
|---|---|
| urgent-flag allow<br>!<br>无传呼机<br>no logging message 106015<br>no logging message 313001<br>no logging message 313008<br>no logging message 106023<br>no logging message 710003<br>no logging message 106100<br>no logging message 302015<br>no logging message 302014<br>no logging message 302013<br>no logging message 302018<br>no logging message 302017<br>no logging message 302016<br>no logging message 302021<br>no logging message 302020<br>1500以外的MTU<br>mtu diagnostic 1500<br>mtu内部1500<br>故障转移<br>failover lan unit secondary<br>failover lan interface FOVER Port-channel3<br>故障切换复制http<br>failover link FOVER Port-channel3<br>failover interface ip FOVER 172.16.51.1<br>255.255.255.0 standby 172.16.51.2<br><br><省略部分输出> | tcp-options range 6 7 allow<br>tcp-options range 9 18 allow<br>tcp-options range 20 255 allow<br>urgent-flag allow<br>!<br>无传呼机<br>no logging message 106015<br>no logging message 313001<br>no logging message 313008<br>no logging message 106023<br>no logging message 710003<br>no logging message 106100<br>no logging message 302015<br>no logging message 302014<br>no logging message 302013<br>no logging message 302018<br>no logging message 302017<br>no logging message 302016<br>no logging message 302021<br>no logging message 302020<br>1500以外的MTU<br>mtu diagnostic 1500<br>mtu内部1500<br>不执行故障切换<br>no monitor-interface外部<br>no monitor-interface service-module<br><br><省略部分输出> |

关于 HA 中断的主要注意事项：

| 主/备用设备 | 辅助/主用设备 |
|---|---|
| • 所有故障切换配置已删除<br>• 删除所有IP配置 | • 所有故障切换配置已删除<br>• 备用IP将保留，但在下次部署时删除 |

步骤6.完成此任务后，重新创建HA对。

# 任务6.删除高可用性对

此任务基于使用7.2.8软件的41xx上的HA设置。在本例中，设备最初处于以下状态：

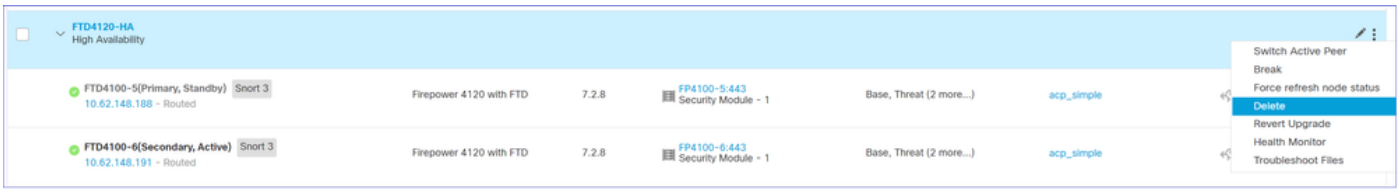
- 主/备用
- 辅助/主用

任务要求：

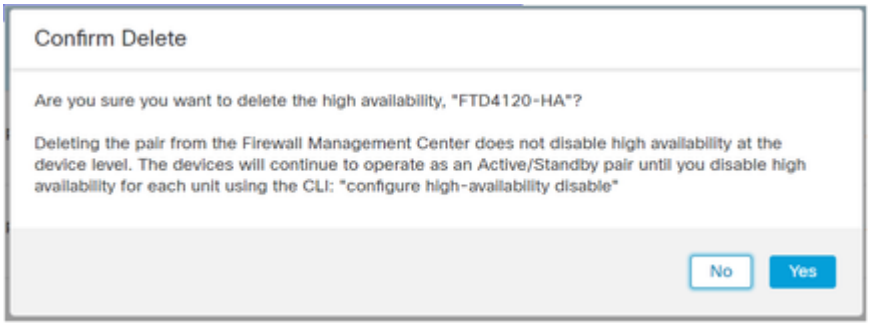
从FMC中删除故障切换对。

解决方案：

步骤1.选择图标。




步骤2.检查通知并确认。




第 3 步： 删除 HA 后，两台设备均从 FMC 取消注册（删除）。

步骤4.显示LINA CLI的running-config结果：

| 主设备（备用） | 辅助设备（主用） |
| --- | --- |
| > show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM1949C5RR<br>:Hardware:FPR4K-SM-24,73853 MB | > show running-config<br>: 已储存<br><br>:<br>:序列号(S):FLM2108V9YG<br>:Hardware:FPR4K-SM-24,73853 MB |

| | |
|---|---|
| RAM，CPU Xeon E5系列2200 MHz，2<br>CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname Firepower-module1<br>enable password ***** encrypted<br>strong-encryption-disable<br>no asp inspect-dp ack-passthrough<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto<br><br>!<br>interface Port-channel2<br>no nameif<br>无安全级别<br>no ip address<br>!<br>interface Port-channel2.202<br>vlan 202<br>nameif NET202<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2<br>!<br>interface Port-channel2.203<br>vlan 203<br>nameif NET203<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2<br>!<br>interface Port-channel3<br>说明LAN/STATE故障切换接口<br>!<br>interface Ethernet1/1<br>仅管理<br>nameif diagnostic | RAM，CPU Xeon E5系列2200 MHz，2<br>CPU（48核）<br>:<br>NGFW版本7.2.8<br>!<br>hostname Firepower-module1<br>enable password ***** encrypted<br>strong-encryption-disable<br>no asp inspect-dp ack-passthrough<br>service-module 0 keepalive-timeout 4<br>service-module 0 keepalive-counter 6<br>名称<br>no mac-address auto<br><br>!<br>interface Port-channel2<br>no nameif<br>无安全级别<br>no ip address<br>!<br>interface Port-channel2.202<br>vlan 202<br>nameif NET202<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2<br>!<br>interface Port-channel2.203<br>vlan 203<br>nameif NET203<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2<br>!<br>interface Port-channel3<br>说明LAN/STATE故障切换接口<br>!<br>interface Ethernet1/1<br>仅管理<br>nameif diagnostic |

| | |
|---|---|
| cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>no ip address<br>!<br>interface Ethernet1/4<br>nameif NET204<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2<br>!<br>ftp mode passive<br>ngips conn-match vlan-id<br>no object-group-search access-control<br>access-group CSM_FW_ACL_ global<br>access-list CSM_FW_ACL_ remark rule-id 9998:预过滤器策略：默认隧道和优先级策略<br>access-list CSM_FW_ACL_ remark rule-id 9998:规则：默认隧道操作规则<br>access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998<br>access-list CSM_FW_ACL_ remark rule-id 268434433:访问策略:acp_simple — 默认<br>access-list CSM_FW_ACL_ remark rule-id 268434433:L4规则：默认操作规则<br>access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433<br>!<br>tcp-map UM_STATIC_TCP_MAP<br>tcp-options range 6 7 allow<br>tcp-options range 9 18 allow<br>tcp-options range 20 255 allow | cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>no ip address<br>!<br>interface Ethernet1/4<br>nameif NET204<br>cts manual<br>propagate sgt preserve-untag<br>策略静态sgt已禁用，受信任<br>安全级别0<br>ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2<br>!<br>ftp mode passive<br>ngips conn-match vlan-id<br>no object-group-search access-control<br>access-group CSM_FW_ACL_ global<br>access-list CSM_FW_ACL_ remark rule-id 9998:预过滤器策略：默认隧道和优先级策略<br>access-list CSM_FW_ACL_ remark rule-id 9998:规则：默认隧道操作规则<br>access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998<br>access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998<br>access-list CSM_FW_ACL_ remark rule-id 268434433:访问策略:acp_simple — 默认<br>access-list CSM_FW_ACL_ remark rule-id 268434433:L4规则：默认操作规则<br>access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433<br>!<br>tcp-map UM_STATIC_TCP_MAP<br>tcp-options range 6 7 allow<br>tcp-options range 9 18 allow<br>tcp-options range 20 255 allow |

| | |
|---|---|
| tcp-options md5 clear<br>urgent-flag allow<br>!<br>无传呼机<br>no logging message 106015<br>no logging message 313001<br>no logging message 313008<br>no logging message 106023<br>no logging message 710003<br>no logging message 106100<br>no logging message 302015<br>no logging message 302014<br>no logging message 302013<br>no logging message 302018<br>no logging message 302017<br>no logging message 302016<br>no logging message 302021<br>no logging message 302020<br>mtu NET202 1500<br>mtu NET203 1500<br>mtu diagnostic 1500<br>mtu NET204 1500<br>故障转移<br>failover lan unit primary<br>failover lan interface FOVER Port-channel3<br>故障切换复制http<br>failover link FOVER Port-channel3<br>failover interface ip FOVER 172.16.51.1<br>255.255.255.0 standby 172.16.51.2<br>monitor-interface NET202<br>monitor-interface NET203<br>icmp unreachable rate-limit 1 burst-size 1<br><br><省略部分输出><br><br>> show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0配置<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0配置<br>未设置172.16.51.1 255.255.255.0的PORT-<br>channel3<br>Ethernet1/4 NET204 172.16.204.1 | tcp-options md5 clear<br>urgent-flag allow<br>!<br>无传呼机<br>no logging message 106015<br>no logging message 313001<br>no logging message 313008<br>no logging message 106023<br>no logging message 710003<br>no logging message 106100<br>no logging message 302015<br>no logging message 302014<br>no logging message 302013<br>no logging message 302018<br>no logging message 302017<br>no logging message 302016<br>no logging message 302021<br>no logging message 302020<br>mtu NET202 1500<br>mtu NET203 1500<br>mtu diagnostic 1500<br>mtu NET204 1500<br>故障转移<br>failover lan unit secondary<br>failover lan interface FOVER Port-channel3<br>故障切换复制http<br>failover link FOVER Port-channel3<br>failover interface ip FOVER 172.16.51.1<br>255.255.255.0 standby 172.16.51.2<br>monitor-interface NET202<br>monitor-interface NET203<br>icmp unreachable rate-limit 1 burst-size 1<br><br><省略部分输出><br><br>>show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0配置<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0配置<br>未设置172.16.51.1 255.255.255.0的PORT-<br>channel3<br>Ethernet1/4 NET204 172.16.204.1 |

255.255.255.0配置
当前IP地址：
接口名称IP地址子网掩码方法
Port-channel2.202 NET202 172.16.202.2
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.2
255.255.255.0配置
未设置172.16.51.1 255.255.255.0的PORT-channel3
Ethernet1/4 NET204 172.16.204.2
255.255.255.0配置

> show failover
故障切换开启
故障切换设备主设备
故障切换LAN接口：FOVER Port-channel3(up)
重新连接超时0:00:00
设备轮询频率1秒，保持时间15秒
接口轮询频率5秒，保持时间25秒
接口策略1
受监控接口4（共1291个）
未设置MAC地址移动通知间隔
故障切换复制http
版本：我们的版本9.18(4)210，我们的版本9.18(4)210
序列号(S):我们的FLM1949C5RR，配对FLM2108V9YG
上次故障切换时间：13:56:37 UTC 2024年7月16日
此主机：主 — 备用就绪
活动时间:0秒)
插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）
接口NET202(172.16.202.2):正常（受监控）
接口NET203(172.16.203.2):正常（受监控）
接口诊断(0.0.0.0):正常（等待）
接口NET204(172.16.204.2):正常（受监控）
插槽 1：snort rev(1.0)状态(up)
插槽 2：diskstatus rev(1.0)状态(up)
其他主机：辅助 — 活动
活动时间:70293（秒）
接口NET202(172.16.202.1):正常（受监控）
接口NET203(172.16.203.1):正常（受监控）
接口诊断(0.0.0.0):正常（等待）
接口NET204(172.16.204.1):正常（受监控）
插槽 1：snort rev(1.0)状态(up)

255.255.255.0配置
当前IP地址：
接口名称IP地址子网掩码方法
Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置
未设置172.16.51.2 255.255.255.0的PORT-channel3
Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置

> show failover
故障切换开启
辅助故障切换设备
故障切换LAN接口：FOVER Port-channel3(up)
重新连接超时0:00:00
设备轮询频率1秒，保持时间15秒
接口轮询频率5秒，保持时间25秒
接口策略1
受监控接口4（共1291个）
未设置MAC地址移动通知间隔
故障切换复制http
版本：我们的版本9.18(4)210，我们的版本9.18(4)210
序列号(S):我们的型号FLM2108V9YG，配件FLM1949C5RR
上次故障切换时间：13:42:35 UTC 2024年7月16日
此主机：辅助 — 活动
活动时间:70312（秒）
插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）
接口NET202(172.16.202.1):正常（受监控）
接口NET203(172.16.203.1):正常（受监控）
接口诊断(0.0.0.0):正常（等待）
接口NET204(172.16.204.1):正常（受监控）
插槽 1：snort rev(1.0)状态(up)
插槽 2：diskstatus rev(1.0)状态(up)
其他主机：主 — 备用就绪
活动时间:0秒)
插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）
接口NET202(172.16.202.2):正常（受监控）
接口NET203(172.16.203.2):正常（受监控）
接口诊断(0.0.0.0):正常（等待）

| | |
|---|---|
| 插槽 2：diskstatus rev(1.0)状态(up)<br><br><省略部分输出> | 接口NET204(172.16.204.2):正常（受监控）<br>插槽 1：snort rev(1.0)状态(up)<br>插槽 2：diskstatus rev(1.0)状态(up)<br><br><省略部分输出> |

第 5 步： 两台 FTD 设备都已从 FMC 注销：

<#root>

**> show managers**

No managers configured.

在 FMC 中禁用 HA 选项的主要注意事项：

| 主要单元 | 辅助单元 |
|---|---|
| 设备会从 FMC 中删除。<br><br>未从 FTD 设备删除任何配置. | 设备会从 FMC 中删除。<br><br>未从 FTD 设备删除任何配置. |

情形 1：

运行configure high-availability disable命令以从活动FTD设备中删除故障切换配置：

<#root>

>

**configure high-availability disable**

 ?
Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear
<cr>

<#root>

>

**configure high-availability disable**

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.
```

结果：

| 主设备（非备用） | 辅助设备（非主用） |
| --- | --- |
| > INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state.<br><br>> **show failover**<br>**Failover Off (pseudo-Standby)**<br>Failover unit Primary<br>Failover LAN Interface: FOVER Port-channel3 (up)<br>Reconnect timeout 0:00:00<br>Unit Poll frequency 1 seconds, holdtime 15 seconds<br>Interface Poll frequency 5 seconds, holdtime 25 seconds<br>Interface Policy 1<br>Monitored Interfaces 0 of 1291 maximum<br>MAC Address Move Notification Interval not set<br>failover replication http<br><br>> **show ip**<br>System IP Addresses:<br>Interface Name IP address Subnet mask Method<br>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset<br>Current IP Addresses:<br>Interface Name IP address Subnet mask Method<br>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset | > **show failover**<br>Failover Off<br>Failover unit Secondary<br>Failover LAN Interface: not Configured<br>Reconnect timeout 0:00:00<br>Unit Poll frequency 1 seconds, holdtime 15 seconds<br>Interface Poll frequency 5 seconds, holdtime 25 seconds<br>Interface Policy 1<br>Monitored Interfaces 4 of 1291 maximum<br>MAC Address Move Notification Interval not set<br><br>> **show ip**<br>System IP Addresses:<br>Interface Name IP address Subnet mask Method<br>Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG<br>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG<br>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG<br>Current IP Addresses:<br>Interface Name IP address Subnet mask Method<br>Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG<br>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG<br>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG |
| 主（非备用） | 辅助（非活动） |

```
> show running-config
: 已储存

:
:序列号(S):FLM1949C5RR
:Hardware:FPR4K-SM-24,73853 MB
RAM，CPU Xeon E5系列2200 MHz，2
CPU（48核）
:
NGFW版本7.2.8
!
hostname Firepower-module1
enable password ***** encrypted
strong-encryption-disable
no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
名称
no mac-address auto

!
interface Port-channel2
shutdown
no nameif
无安全级别
no ip address < — 删除IP
!
interface Port-channel3
说明LAN/STATE故障切换接口
!
interface Ethernet1/1
仅管理
shutdown
no nameif
无安全级别
no ip address
!
interface Ethernet1/4
shutdown
no nameif
无安全级别
no ip address
!
ftp mode passive
ngips conn-match vlan-id
no object-group-search access-control
```

```
> show running-config
: 已储存

:
:序列号(S):FLM2108V9YG
:Hardware:FPR4K-SM-24,73853 MB
RAM，CPU Xeon E5系列2200 MHz，2
CPU（48核）
:
NGFW版本7.2.8
!
hostname Firepower-module1
enable password ***** encrypted
strong-encryption-disable
no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
名称
no mac-address auto

!
interface Port-channel2
no nameif
无安全级别
no ip address
!
interface Port-channel2.202
vlan 202
nameif NET202
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
ip address 172.16.202.1 255.255.255.0 standby
172.16.202.2
!
interface Port-channel2.203
vlan 203
nameif NET203
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
ip address 172.16.203.1 255.255.255.0 standby
172.16.203.2
!
```

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id
9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id
9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id
9998
access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268434433:访问策略:acp_simple — 默认
access-list CSM_FW_ACL_ remark rule-id
268434433:L4规则：默认操作规则
access-list CSM_FW_ACL_ advanced permit ip
any any rule-id 268434433
!
tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow
tcp-options range 9 18 allow
tcp-options range 20 255 allow
tcp-options md5 clear
urgent-flag allow
!
无传呼机
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

```
interface Port-channel3
no nameif
无安全级别
no ip address
!
interface Ethernet1/1
仅管理
nameif diagnostic
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
no ip address
!
interface Ethernet1/4
nameif NET204
cts manual
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
安全级别0
ip address 172.16.204.1 255.255.255.0 standby
172.16.204.2
!
ftp mode passive
ngips conn-match vlan-id
no object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id
9998:预过滤器策略：默认隧道和优先级策略
access-list CSM_FW_ACL_ remark rule-id
9998:规则：默认隧道操作规则
access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id
9998
access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id
268434433:访问策略:acp_simple — 默认
access-list CSM_FW_ACL_ remark rule-id
```

| | |
|---|---|
| 不执行故障切换<br>failover lan unit primary<br>failover lan interface FOVER Port-channel3<br>故障切换复制http<br>failover link FOVER Port-channel3<br>failover interface ip FOVER 172.16.51.1<br>255.255.255.0 standby 172.16.51.2<br>no monitor-interface service-module<br><br><省略部分输出> | 268434433:L4规则：默认操作规则<br>access-list CSM_FW_ACL_ advanced permit ip<br>any any rule-id 268434433<br>!<br>tcp-map UM_STATIC_TCP_MAP<br>tcp-options range 6 7 allow<br>tcp-options range 9 18 allow<br>tcp-options range 20 255 allow<br>tcp-options md5 clear<br>urgent-flag allow<br>!<br>无传呼机<br>no logging message 106015<br>no logging message 313001<br>no logging message 313008<br>no logging message 106023<br>no logging message 710003<br>no logging message 106100<br>no logging message 302015<br>no logging message 302014<br>no logging message 302013<br>no logging message 302018<br>no logging message 302017<br>no logging message 302016<br>no logging message 302021<br>no logging message 302020<br>mtu NET202 1500<br>mtu NET203 1500<br>mtu diagnostic 1500<br>mtu NET204 1500<br>不执行故障切换<br>monitor-interface NET202<br>monitor-interface NET203<br>no monitor-interface service-module |

从活动FTD CLI禁用HA需要注意的要点：

| 主用设备 | 备用单元 |
|---|---|
| • 故障切换配置已删除<br>• 未删除备用IP | • 接口配置已删除.<br>• 故障切换配置未删除，但故障切换已禁用（伪备用） |

此时，您可以在非备用设备上禁用HA。

场景2(不推荐

⚠ 警告：此场景会导致主用/主用情况，因此不建议使用。仅显示用于感知。

运行configure high-availability disable命令以从备用FTD设备中删除故障切换配置：

```
<#root>

>

configure high-availability disable


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES


Successfully disabled high-availability.
```

结果：

| 主（非备用） | 辅助（活动） |
| --- | --- |
| > show failover<br>故障切换关闭<br>辅助故障切换设备<br>故障切换LAN接口：未配置<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1<br>受监控接口4（共1291个）<br>未设置MAC地址移动通知间隔<br><br>> show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法 | > show failover<br>故障切换开< — 故障切换未禁用<br>辅助故障切换设备<br>故障切换LAN接口：FOVER Port-channel3(up)<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1<br>受监控接口4（共1291个）<br>未设置MAC地址移动通知间隔<br>故障切换复制http<br>版本：我们的版本9.18(4)210，我们的版本9.18(4)210<br>序列号(S):我们的型号FLM2108V9YG，配件FLM1949C5RR |

| | |
|---|---|
| Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手动< — 设备使用与ex-Active相同的IP!<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手册<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册 | 上次故障切换时间：12:44:06 UTC 2024年7月17日<br>此主机：辅助 — 活动<br>活动时间:632（秒）<br>插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）<br>接口诊断(0.0.0.0):正常（等待）<br>接口NET204(172.16.204.1):正常（受监控）<br>接口NET203(172.16.203.1):正常（受监控）<br>接口NET202(172.16.202.1):正常（受监控）<br>插槽 1：snort rev(1.0)状态(up)<br>插槽 2：diskstatus rev(1.0)状态(up)<br>其他主机：主要 — 已禁用<br>活动时间:932（秒）<br>插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）<br>接口诊断(0.0.0.0):未知（正在等待）<br>接口NET204(172.16.204.2):未知（受监控）<br>接口NET203(172.16.203.2):未知（受监控）<br>接口NET202(172.16.202.2):未知（受监控）<br>插槽 1：snort rev(1.0)状态(up)<br>插槽 2：diskstatus rev(1.0)状态(up)<br><br>> show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手动< — 设备使用与ex-Standby相同的IP!<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>未设置172.16.51.1 255.255.255.0的PORT-channel3<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手册<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>未设置172.16.51.2 255.255.255.0的PORT-channel3<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册 |

从活动FTD CLI禁用HA需要注意的要点：

| 主用设备 | 备用单元 |
| --- | --- |
| • 故障切换配置未删除且保持启用状态<br>• 设备使用与外部备用设备相同的IP | • 故障切换配置已删除<br>• 设备使用与主用设备相同的IP |

情形 3：

运行configure high-availability disable clear-interfaces命令以从活动FTD设备中删除故障切换配置：

```
<#root>

>

configure high-availability disable clear-interfaces


High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes


Successfully disabled high-availability.

>
```

结果：

| 主（非备用） | 辅助（非活动） |
| --- | --- |
| > show failover<br>故障切换关闭（伪备用）<br>故障切换设备主设备<br>故障切换LAN接口：FOVER Port-channel3(up)<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1 | > show failover<br>故障切换关闭<br>辅助故障切换设备<br>故障切换LAN接口：未配置<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1 |

| | |
|---|---|
| 受监控接口0（最多1291个）<br>未设置MAC地址移动通知间隔<br>故障切换复制http<br><br>**>** show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>未设置172.16.51.1 255.255.255.0的PORT-channel3<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>未设置172.16.51.1 255.255.255.0的PORT-channel3<br>**>** | 受监控接口0（最多1291个）<br>未设置MAC地址移动通知间隔<br><br>**>** show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>**>** |

Disable HA以及clear-interfaces from Active FTD CLI的注意事项：

| 主用设备 | 备用单元 |
|---|---|
| • 故障切换配置已删除<br>• IP将被删除 | • 故障切换配置未删除，但故障切换已禁用（伪备用）<br>• IP将被删除 |

场景 4

运行configure high-availability disable clear-interfaces命令以从备用FTD设备中删除故障切换配置：

**<#root>**

>

**configure high-availability disable clear-interfaces**

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':
```

**YES**

```
Successfully disabled high-availability.
```

>

结果：

| 主（非备用） | 辅助（活动） |
| --- | --- |
| > show failover<br>故障切换关闭<br>辅助故障切换设备<br>故障切换LAN接口：未配置<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1<br>受监控接口0（最多1291个）<br>未设置MAC地址移动通知间隔<br><br>> show ip<br>系统IP地址：<br>接口名称IP地址子网掩码方法<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>> | > show failover<br>故障切换开启<br>辅助故障切换设备<br>故障切换LAN接口：FOVER Port-channel3(up)<br>重新连接超时0:00:00<br>设备轮询频率1秒，保持时间15秒<br>接口轮询频率5秒，保持时间25秒<br>接口策略1<br>受监控接口4（共1291个）<br>未设置MAC地址移动通知间隔<br>故障切换复制http<br>版本：我们的版本9.18(4)210，我们的版本9.18(4)210<br>序列号(S):我们的型号FLM2108V9YG，配件FLM1949C5RR<br>上次故障切换时间：世界协调时2024年7月18日07:06:56<br>此主机：辅助 — 活动<br>活动时间:1194（秒）<br>插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）<br>接口诊断(0.0.0.0):正常（等待）<br>接口NET204(172.16.204.1):正常（受监控）<br>接口NET202(172.16.202.1):正常（受监控）<br>接口NET203(172.16.203.1):正常（受监控）<br>插槽 1：snort rev(1.0)状态(up)<br>插槽 2：diskstatus rev(1.0)状态(up)<br>其他主机：主要 — 已禁用<br>活动时间:846（秒）<br>插槽 0：UCSB-B200-M3-U硬件/软件版本(0.0/9.18(4)210)状态（启动系统）<br>接口诊断(0.0.0.0):未知（正在等待）<br>接口NET204(172.16.204.2):未知（受监控）<br>接口NET202(172.16.202.2):未知（受监控）<br>接口NET203(172.16.203.2):未知（受监控）<br>插槽 1：snort rev(1.0)状态(up)<br>插槽 2：diskstatus rev(1.0)状态(up)<br><br>> show ip<br>系统IP地址： |

| | |
|---|---|
| | 接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手册<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>未设置172.16.51.1 255.255.255.0的PORT-<br>channel3<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册<br>当前IP地址：<br>接口名称IP地址子网掩码方法<br>Port-channel2.202 NET202 172.16.202.1<br>255.255.255.0手册<br>Port-channel2.203 NET203 172.16.203.1<br>255.255.255.0手册<br>未设置172.16.51.2 255.255.255.0的PORT-<br>channel3<br>Ethernet1/4 NET204 172.16.204.1<br>255.255.255.0手册 |

从活动FTD CLI禁用HA和clear-interfaces的要点：

| 主用设备 | 备用单元 |
|---|---|
| • 故障切换配置未删除<br>• 未删除IP | • 故障切换配置已删除<br>• IP将被删除 |

步骤6.完成此任务后，将设备注册到FMC并启用HA对。

# 任务 7. 暂停 HA

任务要求：

从 FTD CLISH CLI 上暂停 HA.

解决方案：

第 1 步： 在主 FTD 上运行命令并确认（键入 YES）。

<#root>

**> configure high-availability suspend**

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

**YES**

Successfully suspended high-availability.

第 2 步： 验证主设备上的更改：

<#root>

>

**show high-availability config**

**Failover Off**

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http

步骤3.辅助单元上的结果：

<#root>

>

**show high-availability config**
**Failover Off (pseudo-Standby)**

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http

步骤4.恢复主设备上的HA:

<#root>

>

**configure high-availability resume**

```
Successfully resumed high-availablity.

> .

    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>
```

<#root>

>

**show high-availability config**

**Failover On**

```
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

步骤5.恢复HA后辅助设备上的结果：

<#root>

> ..

**Detected an Active mate**

```
Beginning configuration replication from mate.
```

```
WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.

>
```

<#root>

```
>
```

**show high-availability config**

**Failover On**

```
Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

# 常见问题解答 (FAQ)

问:复制配置后，是立即（逐行）保存还是复制结束时保存？
答：在复制结束时。根据 debug fover sync 命令输出的末尾内容，其中显示了配置/命令复制：

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
```

```
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:

write memory        <--
```

问：如果设备处于伪备用状态（禁用故障转移），然后您重新加载设备，而另一设备已启用故障转移且处于主用状态，会发生什么情况？
答：您最终会处于主用/主用场景（尽管从技术上讲，这是主用/故障切换关闭）。 具体来说，一旦设备启动，故障切换将被禁用，但设备使用与主用设备相同的IP。因此，实际上您的设备状态如下：

- 设备 1:主用
- 设备 2:故障切换关闭，设备使用与设备1相同的数据IP，但使用不同的MAC地址。

问:如果您手动禁用故障切换（配置高可用性挂起），然后重新加载设备，故障切换配置会发生什么情况？
答：禁用故障转移时，它不是永久更改（不会保存在startup-config中，除非您决定明确执行此操作）。 您可以通过两种不同的方式重新启动/重新加载设备，但第二种方式必须谨慎：

案例 1. 从 CLISH 重启

从 CLISH 重启不需要确认。因此，配置更改不会保存到startup-config:

```
<#root>

>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.
```

running-config已禁用故障转移。在这种情况下，设备处于备用状态，并按预期置于伪备用状态，以避免出现主用/主用场景：

<#root>

```
firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

startup-config仍然启用故障切换：

<#root>

```
firepower#

show startup | include failover


failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

从 CLISH 重启设备（reboot 命令）：

<#root>

```
>

reboot

This command will reboot the system.  Continue?
Please enter 'YES' or 'NO':

YES


Broadcast message from root@
```

```
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

设备启动后，由于故障切换处于启用状态，设备会进入故障切换协商阶段并尝试检测远程对等体：

<#root>

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

**Detected an Active mate**

案例2.从LINA CLI重新启动：
从LINA重新启动(reload命令)，并请求确认。因此，如果您选择Y（是），并且配置更改会保存到启动配置中：

<#root>

```
firepower#
```

**reload**

```
System config has been modified. Save? [Y]es/[N]o:
```

**Y  <-- Be careful. This disables the failover in the startup-config**

```
Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs
Proceed with reload? [confirm]
firepower#
```

**show startup | include failover**

**no failover**

```
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
```

```
failover ipsec pre-shared-key *****
```

设备启动后将禁用故障切换：

```
<#root>

firepower#

show failover | include Fail

Failover Off

Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

注意：要避免这种情况，请确保在出现提示时，不要将更改保存到startup-config中。

# 相关信息

- 请参阅所有版本的Cisco Firepower管理中心配置指南：

查找 Cisco Secure Firewall Threat Defense 文档

- 请参阅所有版本的FXOS机箱管理器和CLI配置指南：

导航Cisco Firepower 4100/9300 FXOS文档

- 思科全球技术支持中心(TAC)强烈推荐此可视化指南，以了解有关Cisco Firepower下一代安全技术的深入实践知识：

Cisco Firepower Threat Defense (FTD)：下一代防火墙(NGFW)、下一代入侵防御系统(NGIPS)和高级恶意软件防护(AMP)的配置和故障排除最佳实践

- 请参阅与Firepower技术相关的所有配置和故障排除技术说明：

Cisco Secure Firewall Management Center

- 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）。