在 Firepower 设备上配置 FTD 高可用性

目录

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)（主用/备用故障切换）。

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 配置中的两台设备必须满足此处提到的条件。

任务1.检验条件

任务要求：

验证两台FTD设备均符合注释要求并可配置为HA设备。

解决方案：

步骤1: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#
```

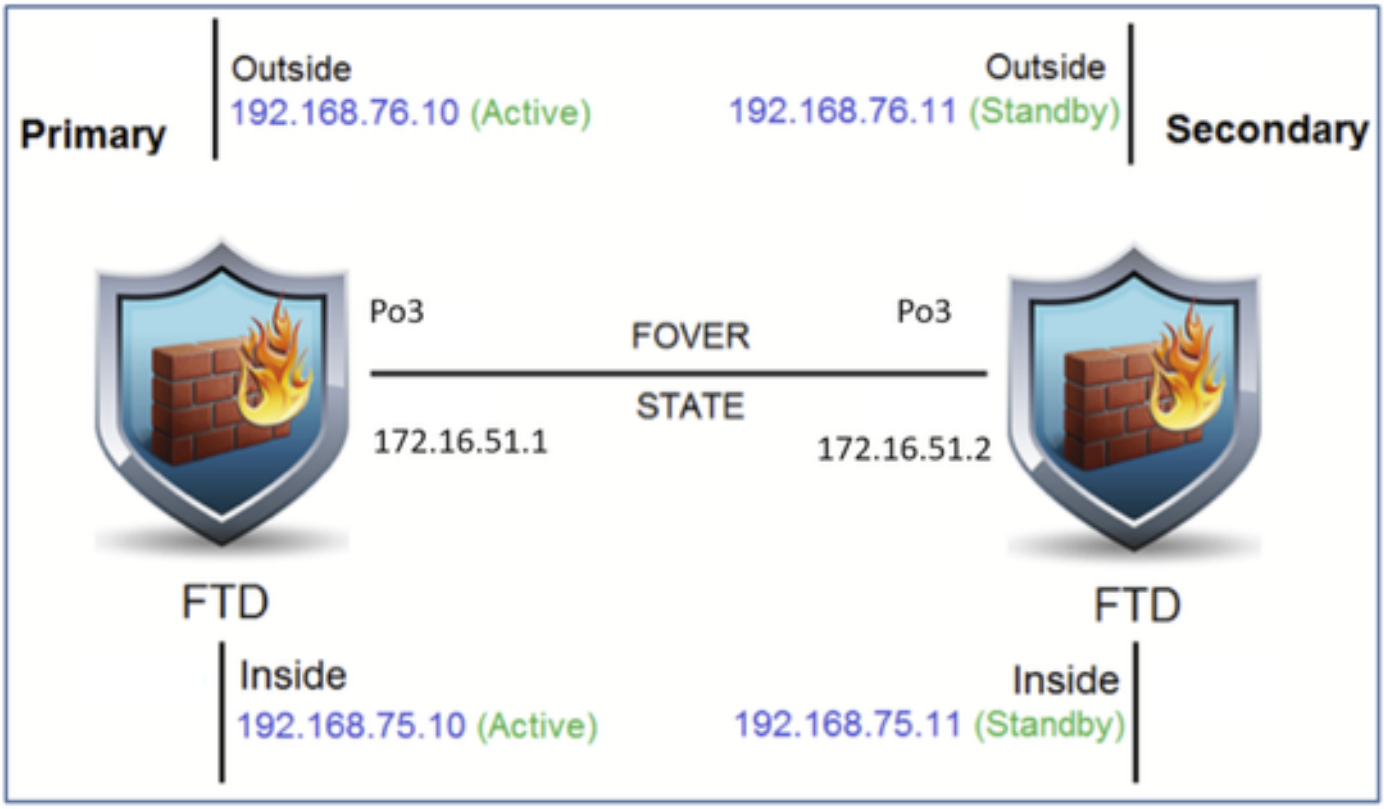
第二步：登录FPR9300-1机箱管理器并导航到逻辑设备。

检验软件的版本、编号和接口类型。

任务2.配置FTD HA

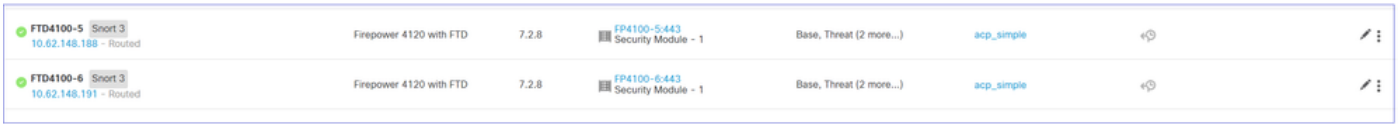
任务要求：

根据此图配置主用/备用故障切换 (HA) 。在本例中，使用41xx对。

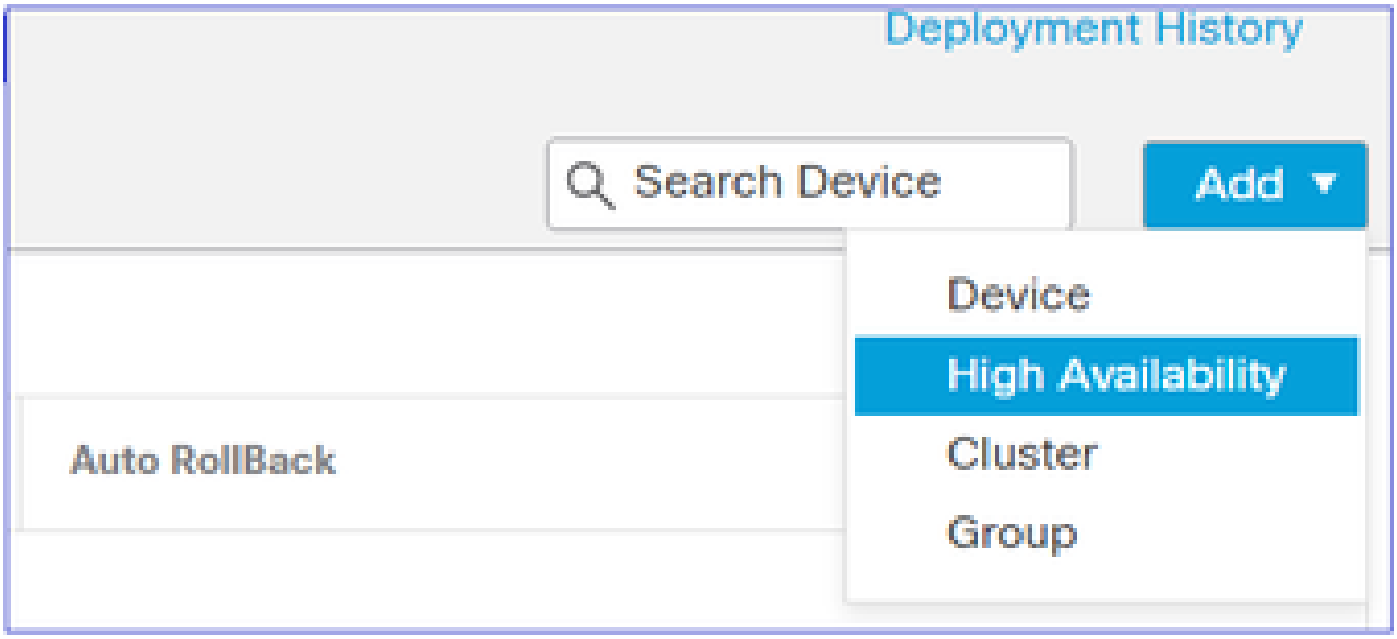


解决方案

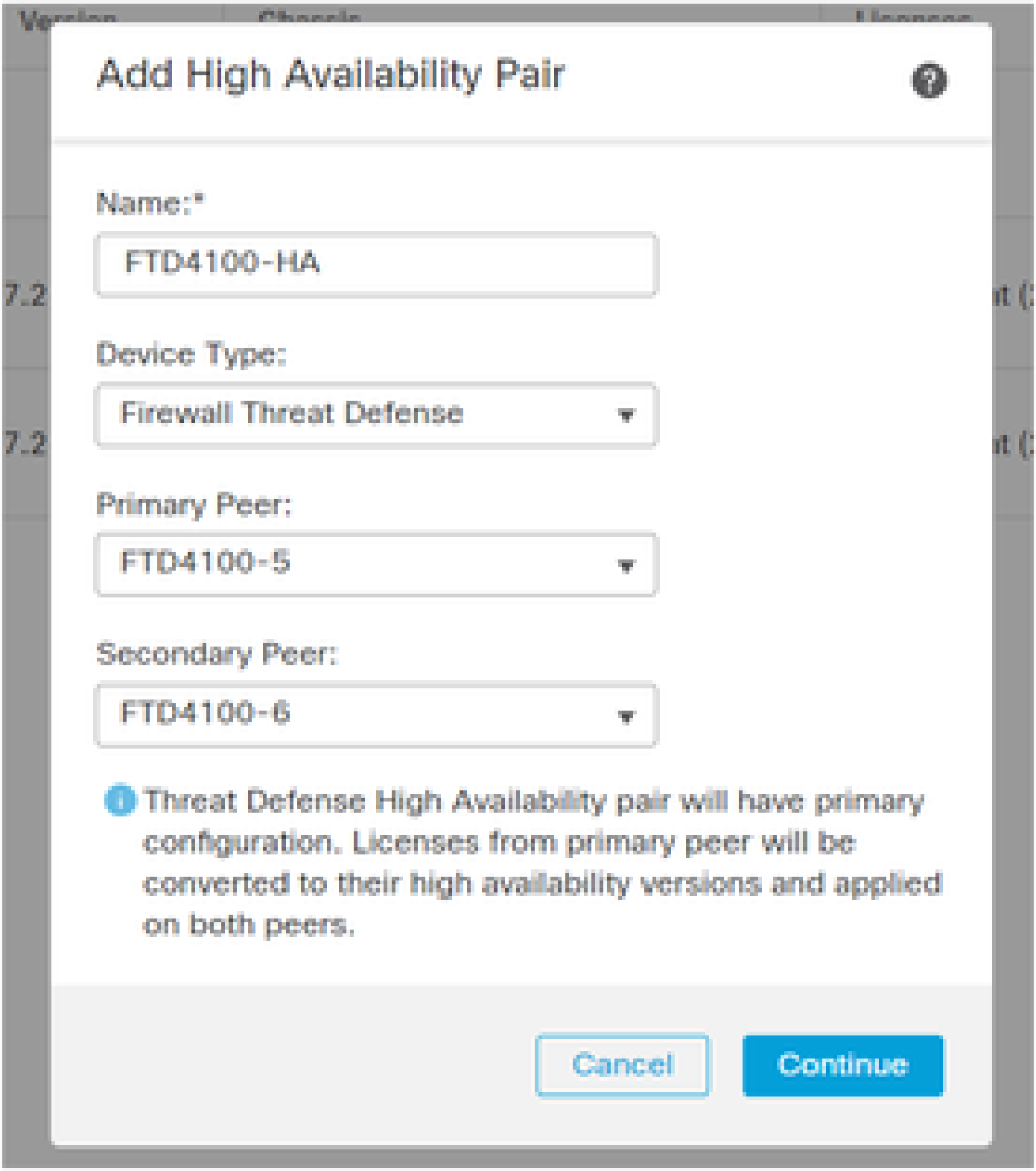
两台 FTD 设备都已在 FMC 上注册，如下图所示。



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（如图所示）。



第二步：输入Primary Peer和Secondary Peer，然后选择Continue（如图所示）。



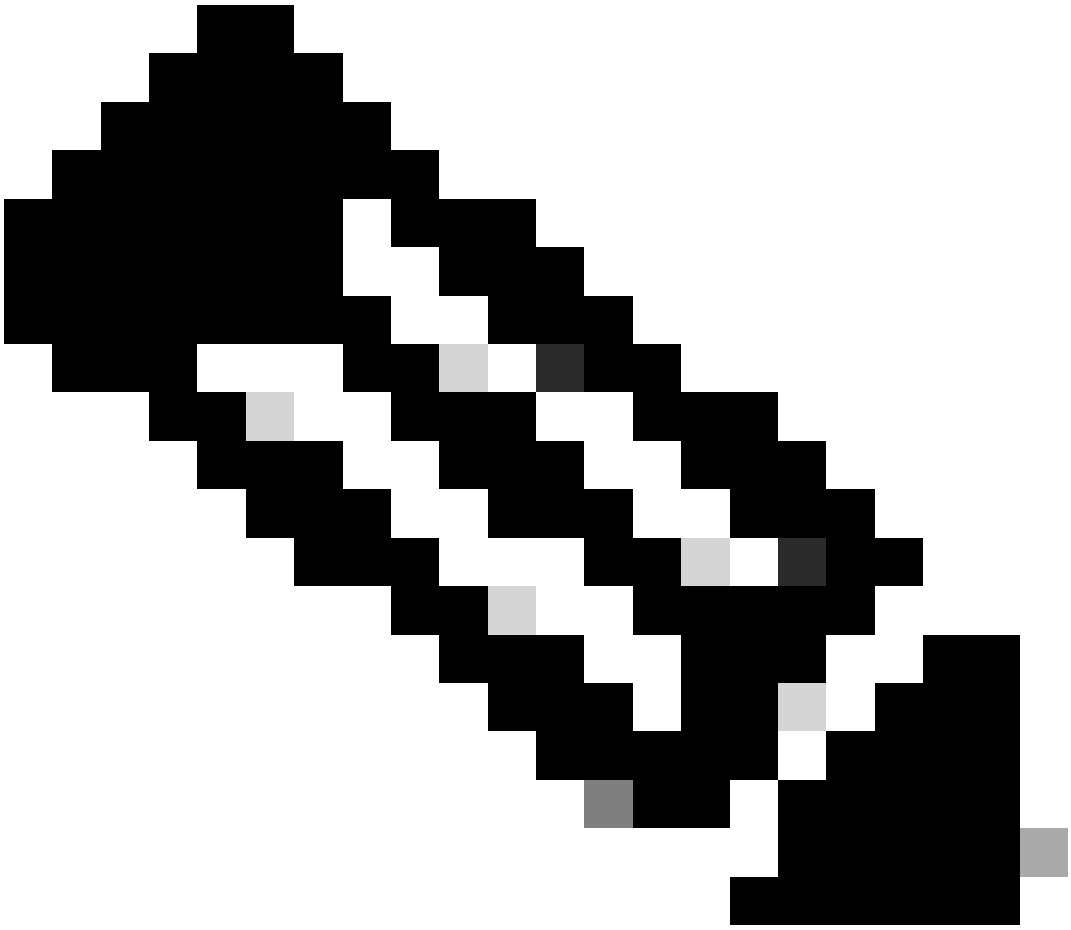
⚠ 警告：确保选择正确的设备作为主要设备。所选主设备上的所有配置都将复制到所选辅助FTD设备。由于复制，可以替换辅助设备上的当前配置。

条件

若要在两台 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（第一个数字）、次要（第二个数字）和维护（第三个数字）必须相等。
- 相同数量的接口数
- 相同类型的接口
- 两台设备作为FMC中相同组/域的一部分。
- 具有相同的网络时间协议(NTP)配置。
- 在FMC上完全部署，无需进行未提交的更改。
- 处于相同的防火墙模式：路由或透明。



注意：在FTD设备和FMC GUI上都必须检查此情况，因为已出现FTD具有相同的模式，但FMC未反映此模式的情况。

- 在任何接口中未配置DHCP/以太网点对点协议(PPPoE)。
- 两个机箱的主机名[完全限定域名(FQDN)]不同。要检查机箱主机名，请导航到FTD CLI，然后运行此命令：

```
<#root>
```

```
firepower#
show chassis-management-url

https://
KSEC-FPR9K-1.cisco.com
:443//
```

注意：在6.3以后的FTD中，请使用命令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其中一个机箱的名称：

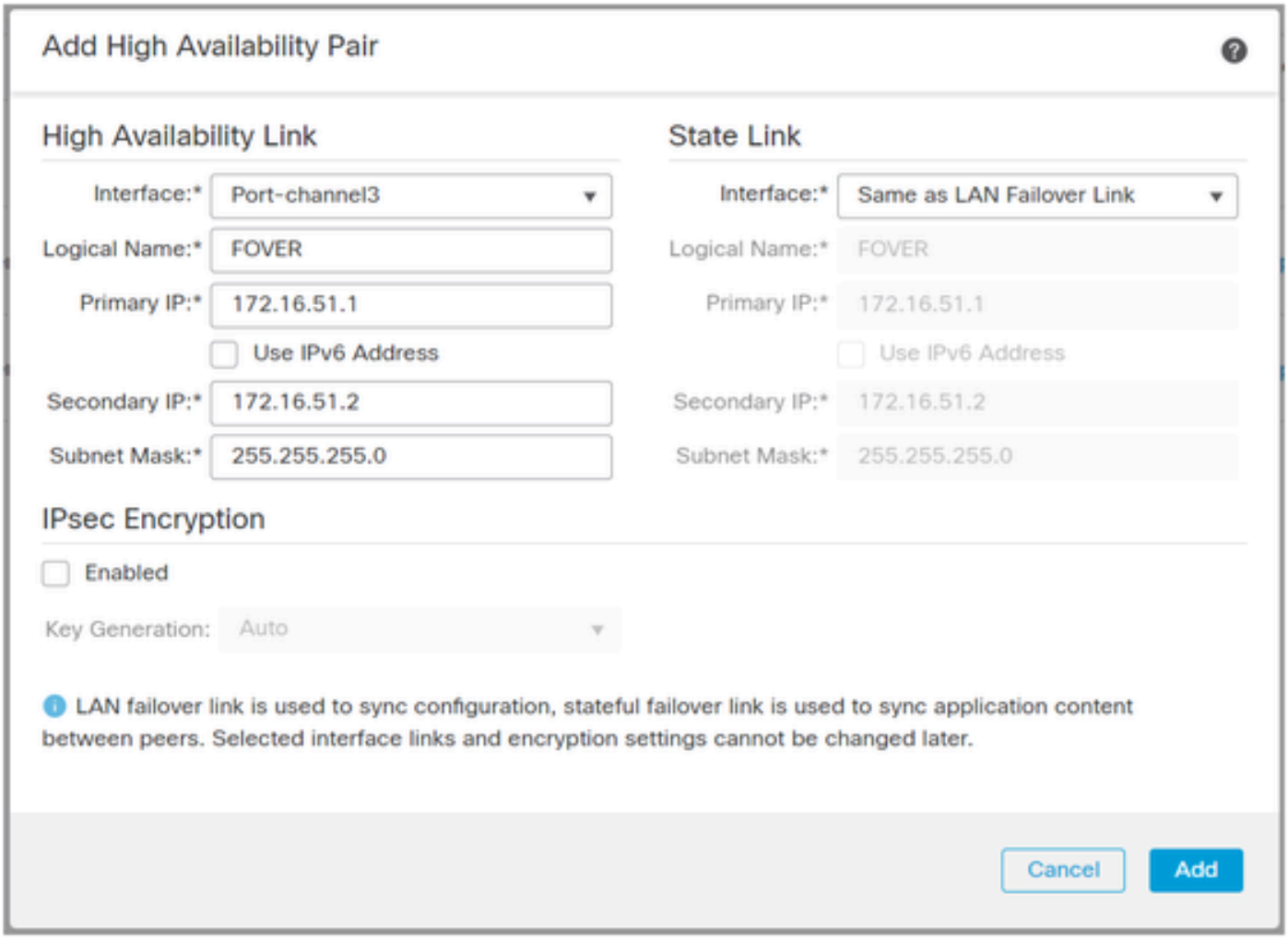
```
<#root>
KSEC-FPR9K-1-A#
scope system
KSEC-FPR9K-1-A /system #
set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #
commit-buffer
FPR9K-1-A /system #
exit
FPR9K-1new-A
#
```

更改机箱名称后，从 FMC 上注销 FTD 并重新注册。然后继续创建 HA 对。

第三步：配置HA并声明链路设置。

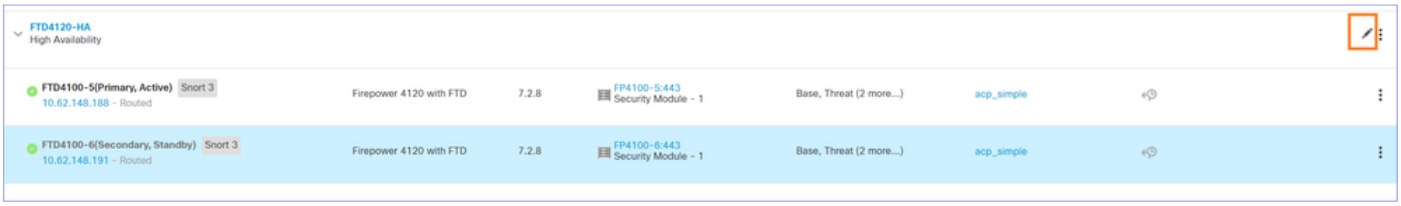
在本例中，状态链路与高可用性链路采用相同的设置。

选择Add并等待几分钟，以便部署HA对，如图所示。

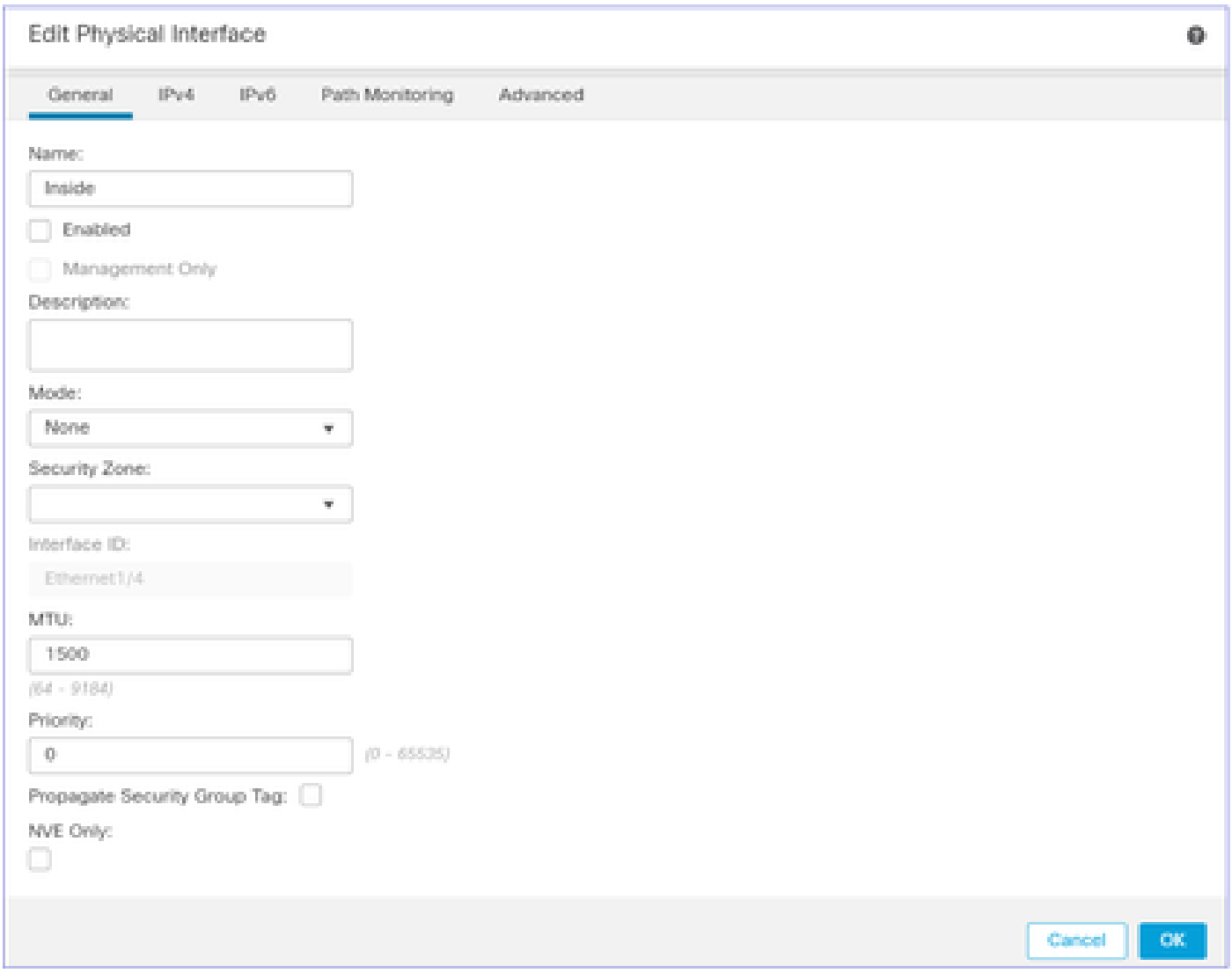


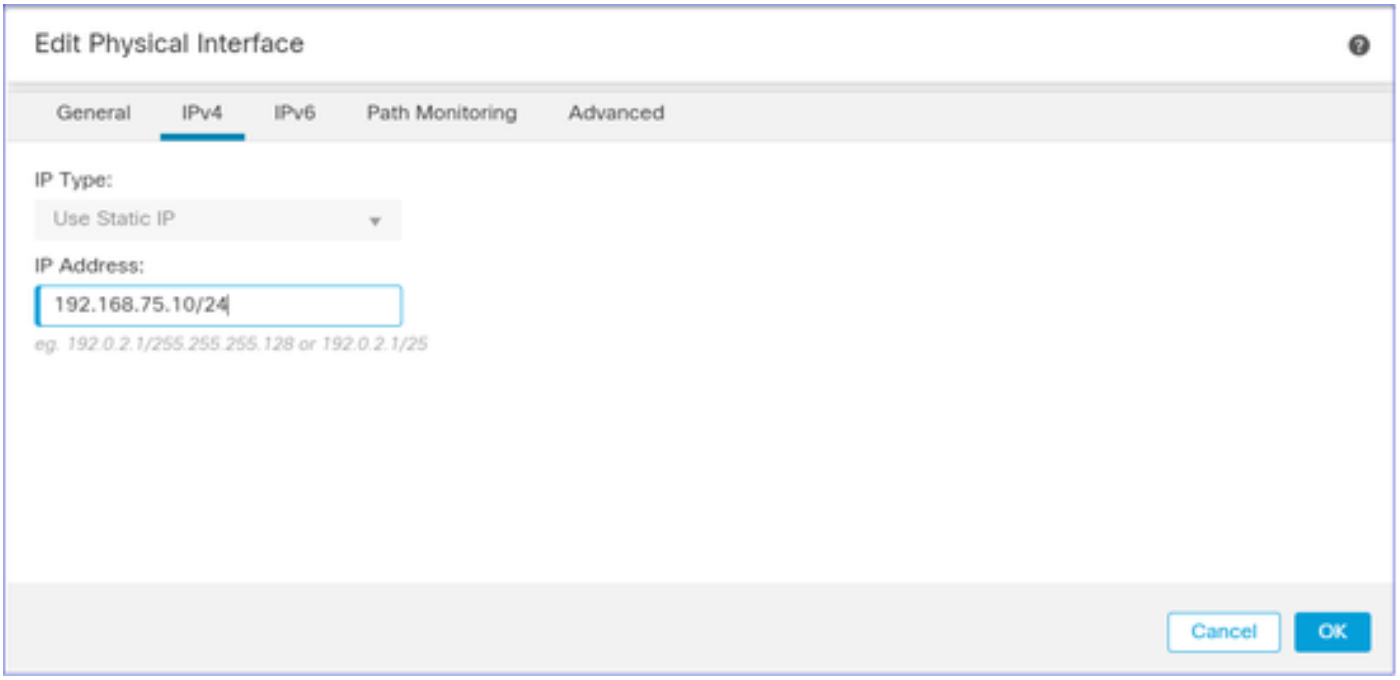
第四步：配置数据接口（主IP地址和备用IP地址）

从FMC GUI中，选择HA Edit（如图所示）。



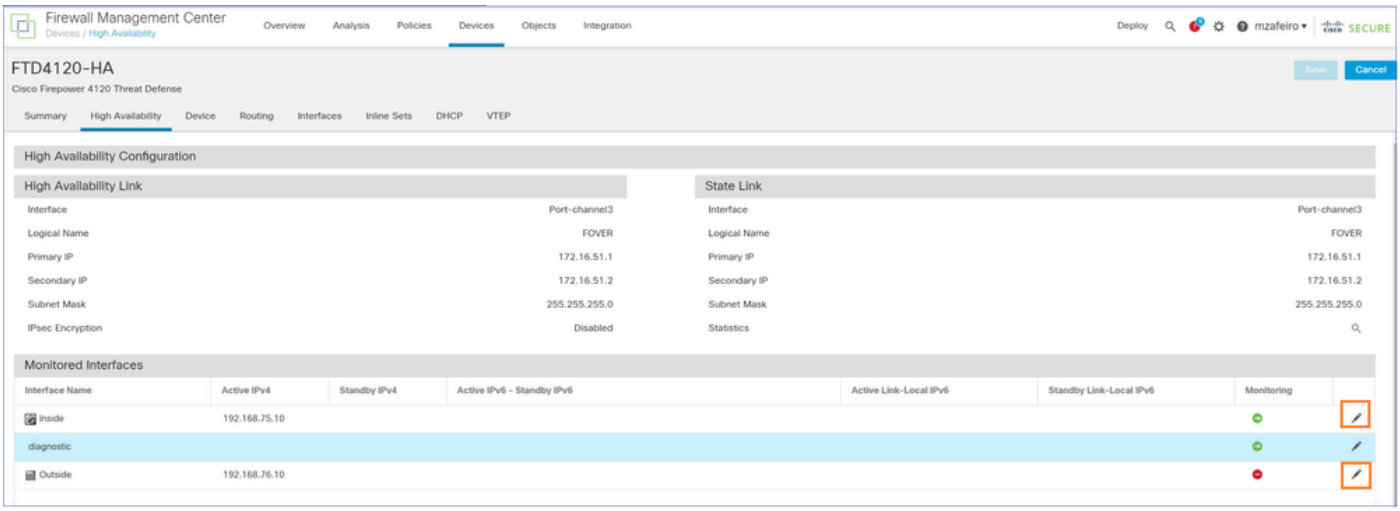
第五步：配置接口设置：



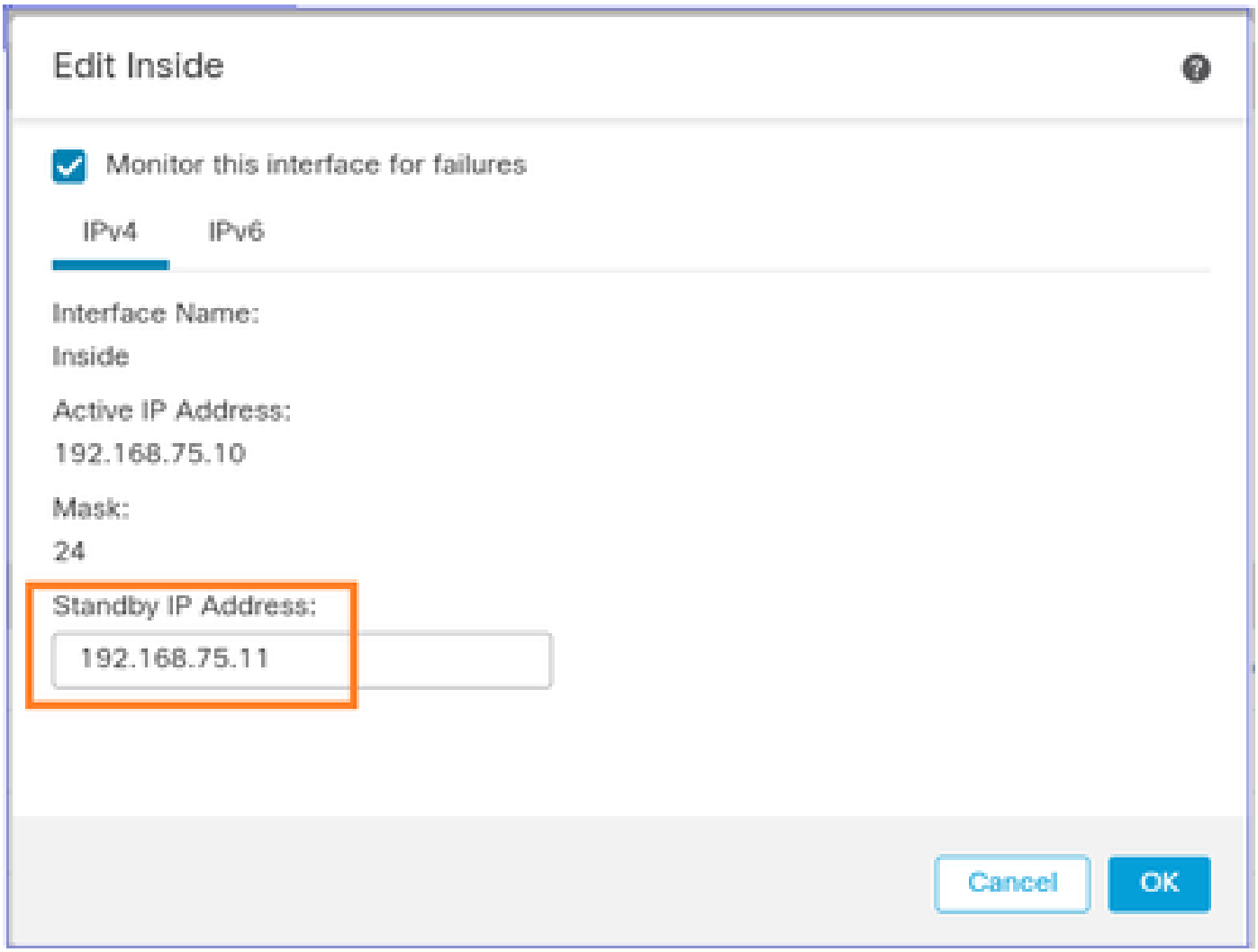


对于子接口，您需要首先启用父接口：

第六步：导航到High Availability，并选择Interface Name Edit以添加备用IP地址，如图所示。



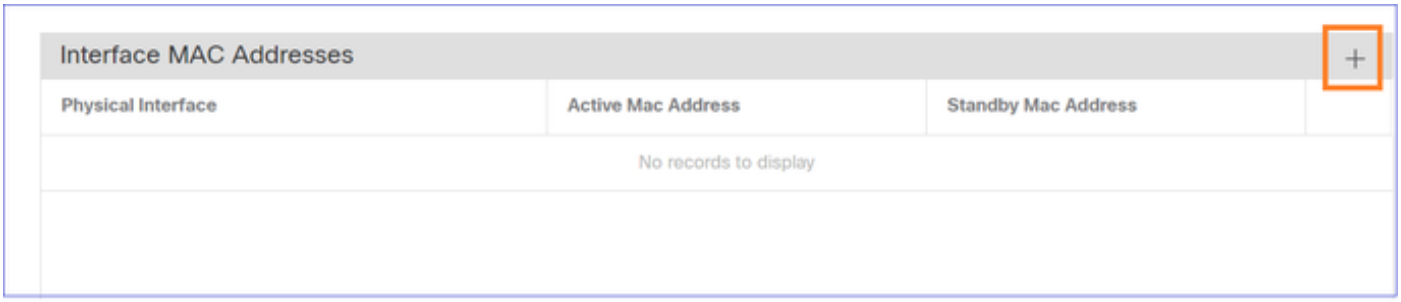
步骤 7.用于内部接口，如图所示。



步骤 8对Outside接口执行相同操作。

步骤 9验证结果如图所示。

步骤 10停留在High Availability选项卡上，配置虚拟MAC地址，如图所示。



步骤 11内部接口则如图所示。

步骤 12对Outside接口执行相同操作。

步骤 13验证结果如图所示。

步骤 14配置更改后，请选择Save和Deploy。

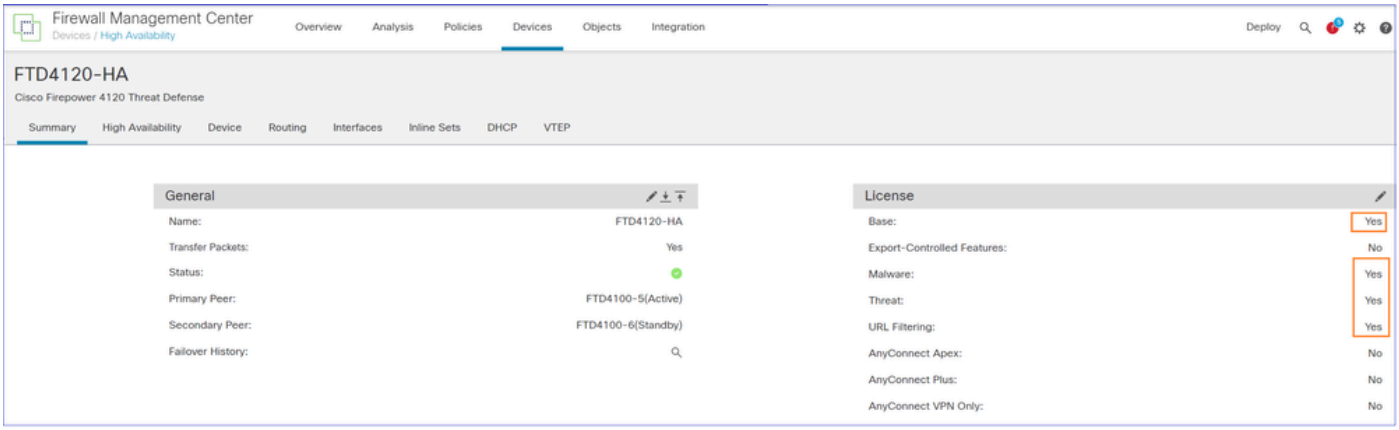
任务3.验证FTD HA和许可证

任务要求：

从 FMC GUI 和 FTD CLI 上验证 FTD HA 设置和启用的许可证。

解决方案：

步骤1:导航到摘要，然后检查HA设置和已启用的许可证，如图所示。



第二步：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>
```

第三步：在辅助设备上执行相同的操作。

第四步：从LINA CLI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#
```

第五步：从主设备(LINA CLI)验证配置：

```
<#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.切换故障切换角色

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，如图所示。

第二步：确认操作。

可以使用show failover history命令输出：

在新的Active	在新待
> show failover history ========== 从状态到状态的原因 ========== 世界协调时2024年7月18日9时27分11秒 Standby Ready Just Active其他设备希望我处于活动状态 （通过config命令设置） 世界协调时2024年7月18日9时27分11秒 仅主用主用耗尽其他单元需要我主用 （通过config命令设置） 世界协调时2024年7月18日9时27分11秒 Active Drain Active Applying Config Other unit deses me Active （通过config命令设置） 世界协调时2024年7月18日9时27分11秒 Active Applying Config Active Config Applied Other unit deses me Active （通过config命令设置） 世界协调时2024年7月18日9时27分11秒 Active Config Applied Active Other unit wants me Active （通过config命令设置）	> show ====== 从状态 ====== 世界协 通过co

第四步：验证后，再次激活主设备。

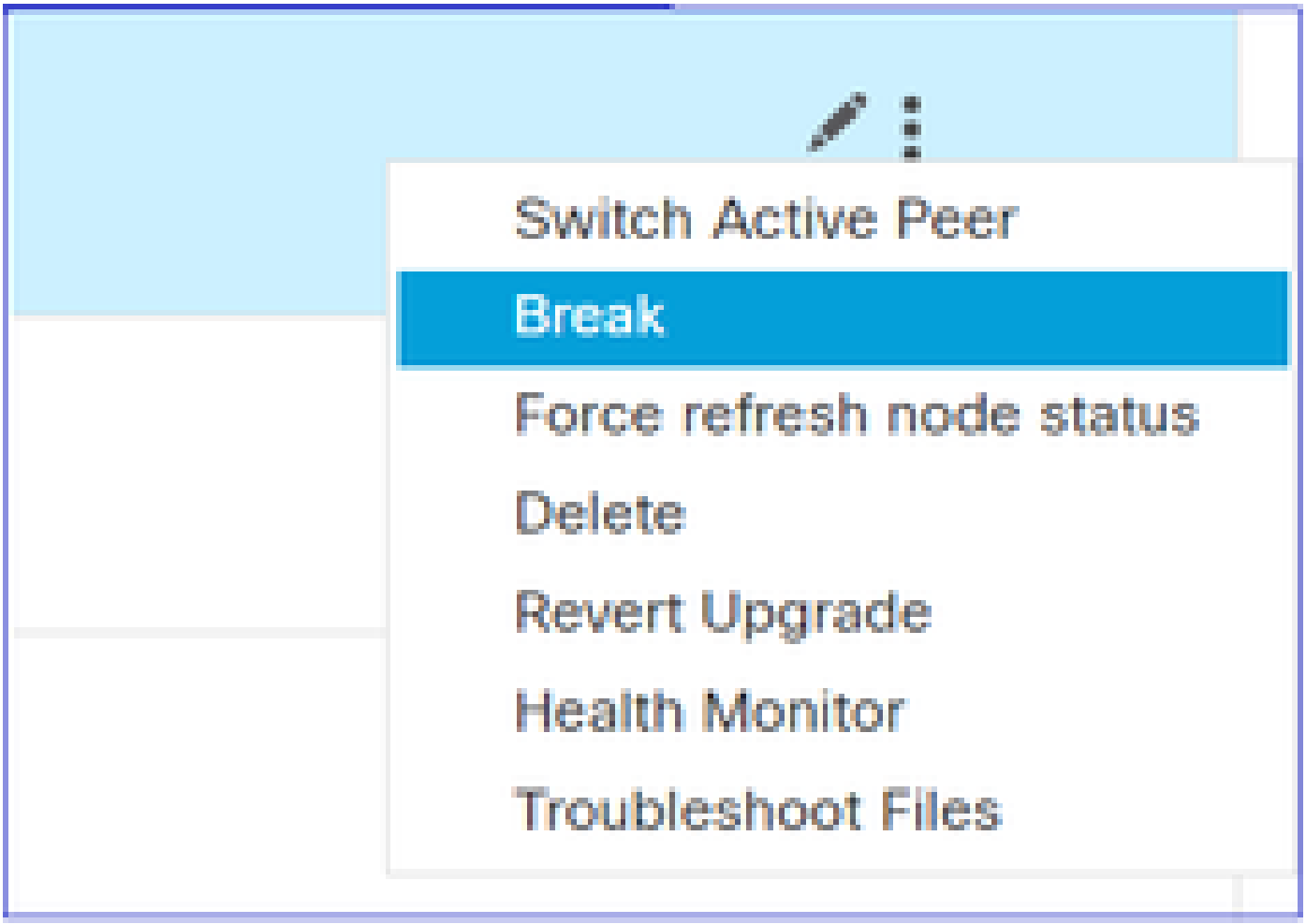
任务5.中断HA对

任务要求：

从 FMC 上中断故障切换对。

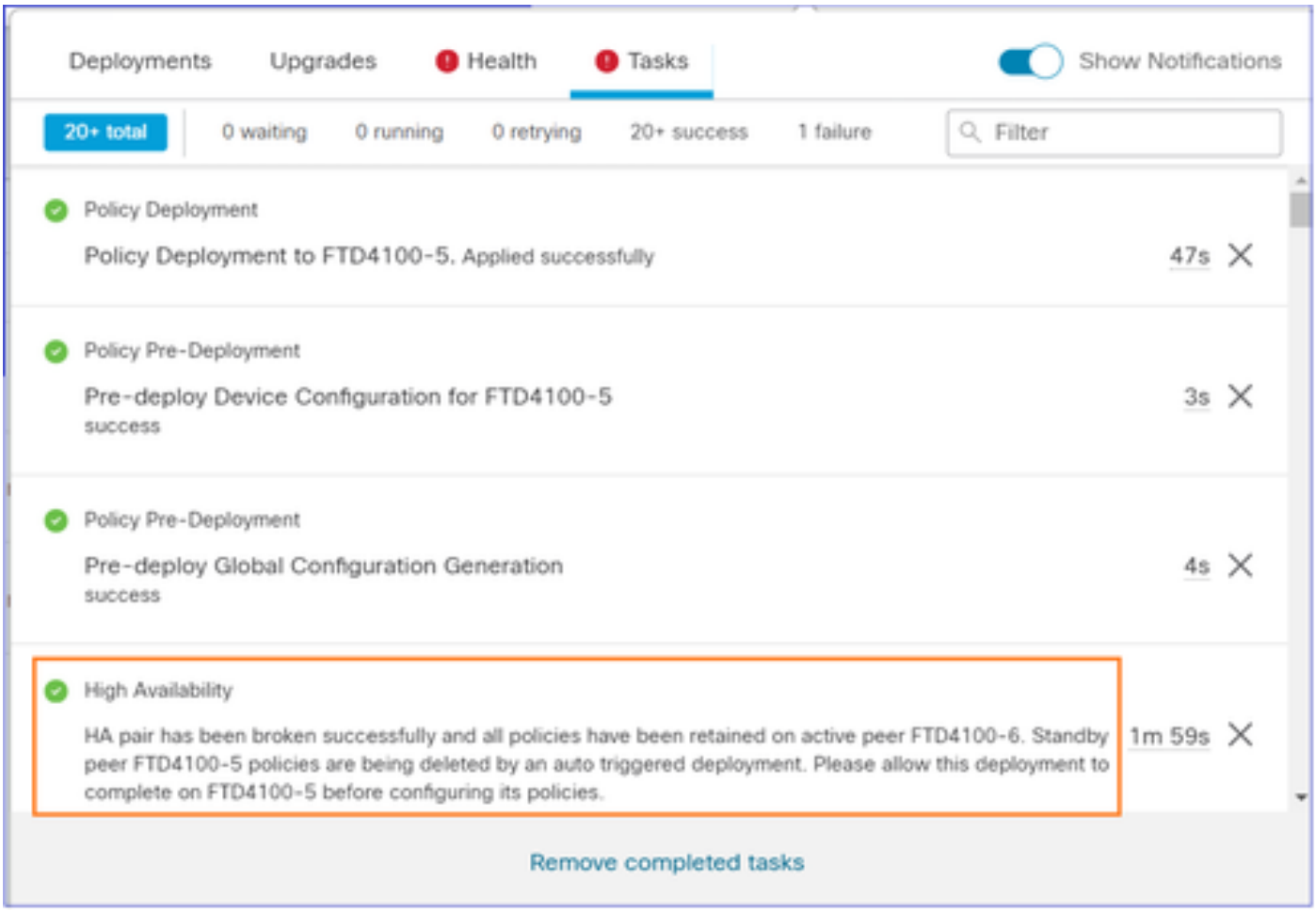
解决方案：

步骤1:选择图标，如图所示。



第二步：检查通知，如图所示。

第三步：请注意下图中所示的消息。



第四步：从FMC GUI或CLI验证结果

在 HA 中断前后在主设备上运行 show running-config：

HA中断前的主/备用设备	HA中断后的主设备
> show running-config : 已储存 ： ：序列号：FLM1949C5RR ：硬件：FPR4K-SM-24，73850 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！ hostname firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4	> INFO：此设备当前处于备用状态。通过禁用故障转移，此设备将保持备用状态。 > show running-config : 已储存 ： ：序列号：FLM1949C5RR ：硬件：FPR4K-SM-24，73850 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！

service-module 0 keepalive-counter 6
名称
no mac-address auto

!
interface Port-channel2
no nameif
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif外部
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
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
仅管理
nameif diagnostic
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
security-level 0
no ip address
!
interface Ethernet1/4
nameif内部
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id

hostname firepower
enable password ***** encrypted
strong-cryption-disable
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
名称
no mac-address auto

!
interface Port-channel2
shutdown
no nameif
no security-level
no ip address
!
interface Port-channel3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1/1
仅管理
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1/4
shutdown
no nameif
no security-level
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： PREFILTER POLICY： Default Tunnel and Priority Policy
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

object-group-search access-control
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998： PREFILTER POLICY： Default Tunnel and Priority Policy
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： ACCESS POLICY： 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
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 -强制
access-list CSM_FW_ACL_ remark rule-id 268439552： L7规则：规则1
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>

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 failover replication http failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222 failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaaa.bbbb.4444 failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <省略部分输出>	

HA中断前的辅助/主用设备	HA中断后的辅助设备
> show running-config : 已储存 ： ：序列号：FLM2108V9YG ：硬件：FPR4K-SM-24，73850 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！ hostname firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名称 no mac-address auto ！ interface Port-channel2 no nameif no security-level no ip address ！ interface Port-channel2.202	> show running-config : 已储存 ： ：序列号：FLM2108V9YG ：硬件：FPR4K-SM-24，73850 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！ hostname firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名称 no mac-address auto ！ interface Port-channel2 no nameif no security-level no ip address ！

vlan 202
nameif外部
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
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
仅管理
nameif diagnostic
security-level 0
no ip address
！
interface Ethernet1/4
nameif内部
security-level 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： PREFILTER POLICY： Default Tunnel and Priority Policy
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

interface Port-channel2.202
vlan 202
nameif外部
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
security-level 0
ip address 192.168.76.10 255.255.255.0
standby 192.168.76.11
！
interface Port-channel3
no nameif
no security-level
no ip address
！
interface Ethernet1/1
仅管理
nameif diagnostic
security-level 0
no ip address
！
interface Ethernet1/4
nameif内部
security-level 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： PREFILTER POLICY： Default Tunnel and Priority Policy
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

268439552：访问策略：acp_simple -强制 access-list CSM_FW_ACL_ remark rule-id 268439552： L7规则：规则1 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 1500以外的MTU mtu diagnostic 1500 mtu内部1500 故障转移 failover lan unit secondary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <省略部分输出>	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 -强制 access-list CSM_FW_ACL_ remark rule-id 268439552： L7规则：规则1 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 1500以外的MTU mtu diagnostic 1500 mtu内部1500 不执行故障切换 no monitor-interface外部 no monitor-interface service-module <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 • 已删除所有IP配置	• 所有故障切换配置已删除 • 备用IP将保留，但在下次部署时被删除

第五步：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软件在41xx上进行的HA设置。在本例中，设备最初处于以下状态：

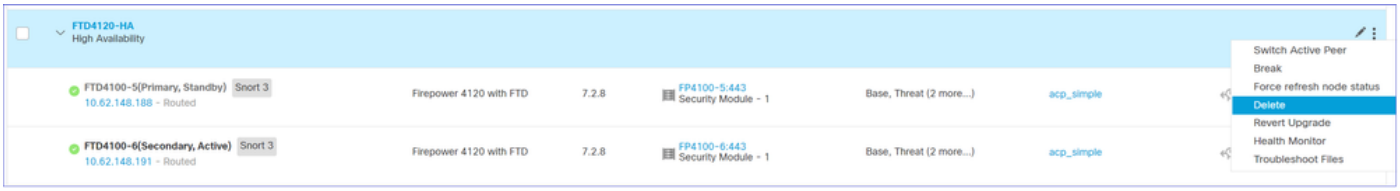
- 主要/标准
- 辅助/主用

任务要求：

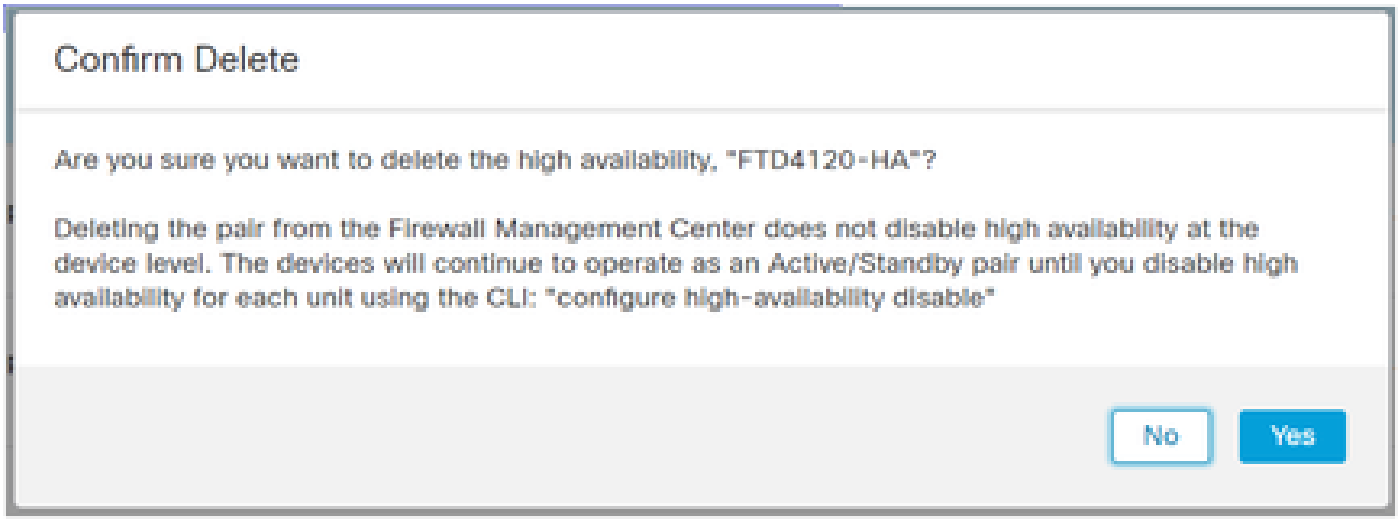
从FMC中删除故障切换对。

解决方案：

步骤1:选择图标，如图所示：



第二步：检查通知并确认问题，如图所示：



第三步：删除HA后，两个设备都会从FMC中注销（移除）。

从 LINA CLI 运行 show running-config ，结果如下表所示：

主设备（备用）	辅助设备（主用）

> show running-config : 已储存 ： ：序列号：FLM1949C5RR ：硬件：FPR4K-SM-24，73853 MB RAM，CPU Xeon E5系列2200 MHz，2个 CPU（48核） ： NGFW版本7.2.8 ！ hostname Firepower-module1 enable password ***** encrypted strong-cryption-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 no security-level no ip address ！ interface Port-channel2.202 vlan 202 nameif NET202 cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 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（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0 ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2 ！	> show running-config : 已储存 ： ：序列号：FLM2108V9YG ：硬件：FPR4K-SM-24，73853 MB RAM，CPU Xeon E5系列2200 MHz，2个 CPU（48核） ： NGFW版本7.2.8 ！ hostname Firepower-module1 enable password ***** encrypted strong-cryption-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 no security-level no ip address ！ interface Port-channel2.202 vlan 202 nameif NET202 cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 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（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0 ip address 172.16.203.1 255.255.255.0 standby 172.16.203.2 ！

interface Port-channel3 description LAN/STATE Failover Interface ! interface Ethernet1/1 仅管理 nameif diagnostic cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0 no ip address ! interface Ethernet1/4 nameif NET204 cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 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： PREFILTER POLICY： Default Tunnel and Priority Policy 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： ACCESS POLICY： acp_simple - 默认 access-list CSM_FW_ACL_ remark rule-id	interface Port-channel3 description LAN/STATE Failover Interface ! interface Ethernet1/1 仅管理 nameif diagnostic cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0 no ip address ! interface Ethernet1/4 nameif NET204 cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 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： PREFILTER POLICY： Default Tunnel and Priority Policy 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： ACCESS POLICY： 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 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 故障转移 failover lan unit primary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <省略部分输出> > show ip 系统IP地址：	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 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 故障转移 failover lan unit secondary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <省略部分输出> > show ip 系统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 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset 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 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.2 255.255.255.0配置	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 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset 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 172.16.202.1 255.255.255.0配置 Port-channel2.203 NET203 172.16.203.1 255.255.255.0配置 Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0配置
> show failover 故障切换开启 故障转移设备主设备 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 failover replication http 版本：Ours 9.18(4)210、Mate 9.18(4)210 序列号：我们的FLM1949C5RR，配对FLM2108V9YG 上次故障转移时间：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)	> show failover 故障切换开启 辅助故障转移设备 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 failover replication http 版本：Ours 9.18(4)210、Mate 9.18(4)210 序列号：我们的FLM2108V9YG，配对FLM1949C5RR 上次故障转移时间：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：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) 插槽2：diskstatus rev (1.0)状态(up) <省略部分输出>	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） 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) <省略部分输出>

第四步：两台FTD设备均未从FMC注册：

<#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。 未从 FTD 设备删除任何配置.	设备会从 FMC 中删除。 未从 FTD 设备删除任何配置.

场景 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. **> show failover** **Failover Off (pseudo-Standby)** **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 0 of 1291 maximum** **MAC Address Move Notification Interval not set** **failover replication http** **> show ip** **System IP Addresses:** **Interface Name IP address Subnet mask Method** **Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset** **Current IP Addresses:** **Interface Name IP address Subnet mask Method** **Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset**	**> show failover** **Failover Off** **Failover unit Secondary** **Failover LAN Interface: not Configured** **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 4 of 1291 maximum** **MAC Address Move Notification Interval not set** **> show ip** **System IP Addresses:** **Interface Name IP address Subnet mask Method** **Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG** **Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG** **Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG** **Current IP Addresses:** **Interface Name IP address Subnet mask Method** **Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG** **Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG** **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：FLM1949C5RR ：硬件：FPR4K-SM-24，73853 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！ hostname Firepower-module1 enable password ***** encrypted strong-cryption-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 no security-level no ip address <-已删除IP ！ interface Port-channel3 description LAN/STATE Failover Interface ！ interface Ethernet1/1 仅管理 shutdown no nameif no security-level no ip address ！ interface Ethernet1/4 shutdown no nameif no security-level no ip address ！ ftp mode passive	> show running-config : 已储存 ： ：序列号：FLM2108V9YG ：硬件：FPR4K-SM-24，73853 MB RAM，CPU Xeon E5系列2200 MHz，2个CPU（48核） ： NGFW版本7.2.8 ！ hostname Firepower-module1 enable password ***** encrypted strong-cryption-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 no security-level no ip address ！ interface Port-channel2.202 vlan 202 nameif NET202 cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 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（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0 ip address 172.16.203.1 255.255.255.0 standby

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： PREFILTER POLICY： Default Tunnel and Priority Policy
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： ACCESS POLICY： 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
172.16.203.2
！
interface Port-channel3
no nameif
no security-level
no ip address
！
interface Ethernet1/1
仅管理
nameif diagnostic
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
security-level 0
no ip address
！
interface Ethernet1/4
nameif NET204
cts manual（cts手册）
propagate sgt preserve-untag
策略静态sgt已禁用，受信任
security-level 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： PREFILTER POLICY： Default Tunnel and Priority Policy
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

no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 不执行故障切换 failover lan unit primary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 no monitor-interface service-module <省略部分输出>	access-list CSM_FW_ACL_ remark rule-id 268434433： ACCESS POLICY： 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 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 不执行故障切换 monitor-interface NET202 monitor-interface NET203 no monitor-interface service-module

从活动FTD CLI禁用HA的注意事项：

主用设备	备用设备
• 故障切换配置已删除	• 接口配置已删除.

• 未删除备用IP	• 故障切换配置未删除，但故障切换已禁用（伪备用）

此时，您也可以在非备用设备上禁用HA。

场景2(不推荐)

⚠ 警告：此方案会导致主用/主用情况，因此不推荐使用。它仅用于感知。

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 故障切换关闭 辅助故障转移设备 故障切换LAN接口：未配置 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 > show ip 系统IP地址： 接口名称IP地址子网掩码方法 Port-channel2.202 NET202 172.16.202.1	> show failover 故障切换开启<-故障切换未禁用 辅助故障转移设备 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 failover replication http 版本：Ours 9.18(4)210、Mate 9.18(4)210 序列号：我们的FLM2108V9YG，配对FLM1949C5RR 上次故障转移时间：12:44:06 UTC 2024年7月17日

255.255.255.0 manual <-设备使用与ex-Active相同的IP！ Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Ethernet1/4 NET204 172.16.204.1 255.255.255.0手册 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手册 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Ethernet1/4 NET204 172.16.204.1 255.255.255.0手册	此主机：辅助-活动 活动时间：632 （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） 接口诊断(0.0.0.0)：正常（等待） 接口NET204 (172.16.204.1)：正常（受监控） 接口NET203 (172.16.203.1)：正常（受监控） 接口NET202 (172.16.202.1)：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-已禁用 活动时间：932 （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） 接口诊断(0.0.0.0)：未知（等待） 接口NET204 (172.16.204.2)：未知（受监控） 接口NET203 (172.16.203.2)：未知（受监控） 接口NET202 (172.16.202.2)：未知（受监控） 插槽1：snort rev (1.0)状态(up) 插槽2：diskstatus rev (1.0)状态(up) > show ip 系统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 manual <-设备使用与ex-standby相同的IP！ Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0手册 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手册 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0手册

从活动FTD CLI禁用HA的注意事项：

主用设备	备用设备
• 故障切换配置未删除且保持启用状态 • 设备使用的IP与ex-Standby设备相同	• 故障切换配置已删除 • 设备使用与主用设备相同的IP

场景 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 故障切换关闭（伪备用） 故障转移设备主设备 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0的最大值为1291 未设置MAC地址移动通知间隔 failover replication http > show ip	> show failover 故障切换关闭 辅助故障转移设备 故障切换LAN接口：未配置 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0的最大值为1291 未设置MAC地址移动通知间隔 > show ip 系统IP地址：

系统IP地址： 接口名称IP地址子网掩码方法 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset 当前IP地址： 接口名称IP地址子网掩码方法 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset **>**	接口名称IP地址子网掩码方法 当前IP地址： 接口名称IP地址子网掩码方法 **>**

禁用HA以及来自活动FTD CLI的“clear-interfaces”的注意要点：

主用设备	备用设备
• 故障切换配置已删除 • 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） • 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	**>** show failover

故障切换关闭 辅助故障转移设备 故障切换LAN接口：未配置 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0的最大值为1291 未设置MAC地址移动通知间隔 > show ip 系统IP地址： 接口名称IP地址子网掩码方法 当前IP地址： 接口名称IP地址子网掩码方法 >	故障切换开启 辅助故障转移设备 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 failover replication http 版本：Ours 9.18(4)210、Mate 9.18(4)210 序列号：我们的FLM2108V9YG，配对 FLM1949C5RR 上次故障转移时间：07:06:56 UTC 2024年7月 18日 此主机：辅助-活动 活动时间：1194（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） 接口诊断(0.0.0.0)：正常（等待） 接口NET204 (172.16.204.1)：正常（受监控） 接口NET202 (172.16.202.1)：正常（受监控） 接口NET203 (172.16.203.1)：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-已禁用 活动时间：846（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） 接口诊断(0.0.0.0)：未知（等待） 接口NET204 (172.16.204.2)：未知（受监控） 接口NET202 (172.16.202.2)：未知（受监控） 接口NET203 (172.16.203.2)：未知（受监控） 插槽1：snort rev (1.0)状态(up) 插槽2：diskstatus rev (1.0)状态(up) > show ip 系统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手册 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1

	255.255.255.0手册 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手册 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手册 Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0手册

禁用HA以及来自活动FTD CLI的“clear-interfaces”的注意要点：

主用设备	备用设备
• 未删除故障切换配置 • 未删除IP	• 故障切换配置已删除 • IP将被删除

第六步：完成任务后，将设备注册到FMC并启用HA对。

任务7.挂起HA

任务要求：

从 FTD CLISH CLI 上暂停 HA

解决方案：

步骤1: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 a

YES

Successfully suspended high-availability.
```

第二步：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
```

第三步：辅助设备上的结果：

<#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
```

第四步：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

第五步：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)

复制配置时，是立即（逐行）保存还是复制结束时保存？
在复制结束时保存。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        <--
```

如果设备处于伪备用状态（禁用故障切换），然后在另一个设备启用故障切换、处于活动状态时重新加载该设备，会发生什么情况？
您最终会处于主用/主用情形（虽然从技术上讲，它是主用/故障切换关闭）。具体而言，设备启动后会禁用故障切换，但设备会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
- Unit-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。

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，则故障切换配置会发生什么情况？
禁用故障切换时，它不是永久更改（不保存在启动配置中，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，第二种方式必须小心：

例 1.从CLISH重新启动

从 CLISH 重启不需要确认。 因此，配置更改不会保存到启动配置中：

<#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禁用了故障转移。在这种情况下，设备为Standby，并如预期进入伪备用状态，以避免出现主用/主用情况：

```
<#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 重启（reload 命令）需要确认。因此，如果您选择Y（是），配置更改将保存到启动配置中：

```
<#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，不要将更改保存到启动配置中。

相关信息

- 可以在此处找到所有版本的思科 Firepower 管理中心 (FMC) 配置指南

[思科安全防火墙威胁防御文档导航]

- 可以在此处找到所有版本的 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威胁防御(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]

- 有关Firepower技术的所有配置和故障排除技术说明

[思科安全防火墙管理中心]

- [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）。