在 Firepower 设备上配置 FTD 高可用性

目录

简介

本文档介绍如何在 FPR9300 上配置和验证 Firepower Threat Defense (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：

- 2xCisco Firepower 9300 安全设备 - FXOS SW 2.0(1.23)
- FTD版本10.10.1.1（内部版本1023）
- Firepower 管理中心 (FMC) - SW 10.10.1.1 (build 1023)

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#

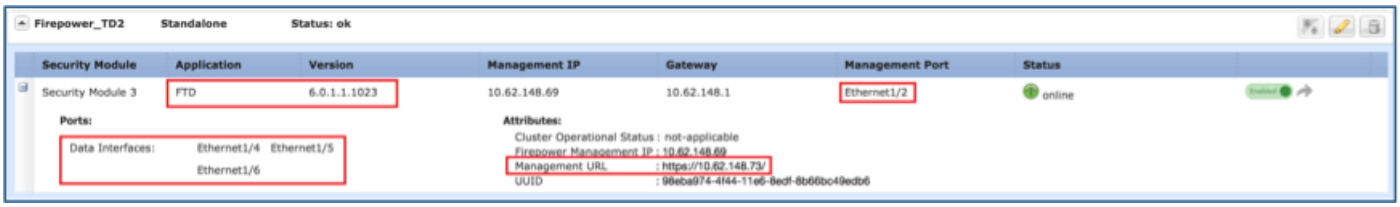
show server inventory

```
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#
```

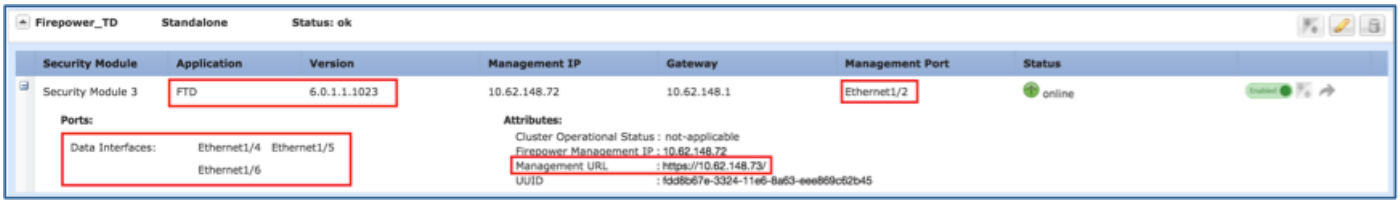
第二步：登录FPR9300-1机箱管理器并导航到逻辑设备。

如图所示，验证软件版本、接口编号和接口类型。

FPR9300-1



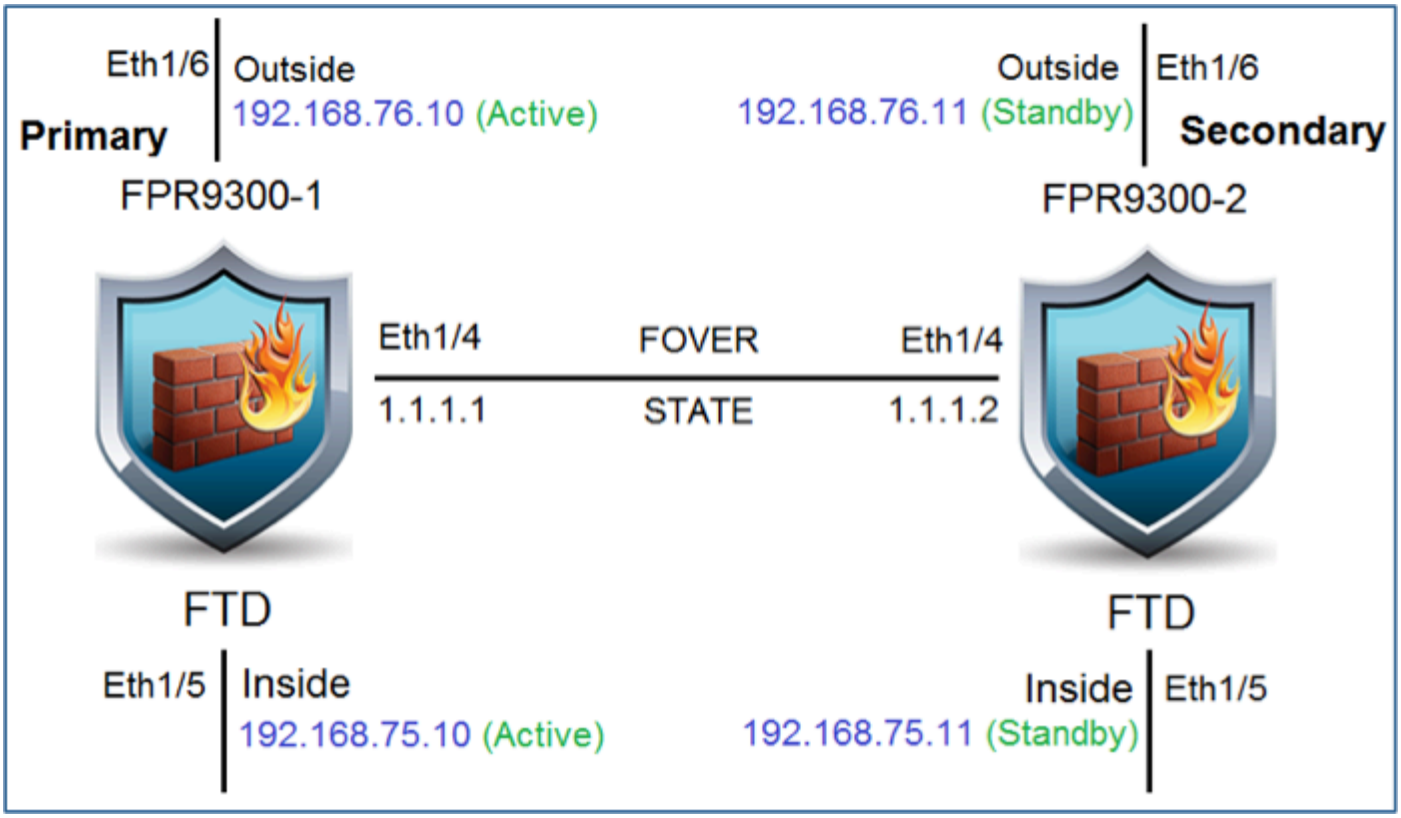
FPR9300-2



任务2.在FPR9300上配置FTD HA

任务要求：

根据此图配置主用/备用故障切换 (HA) 。



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）。

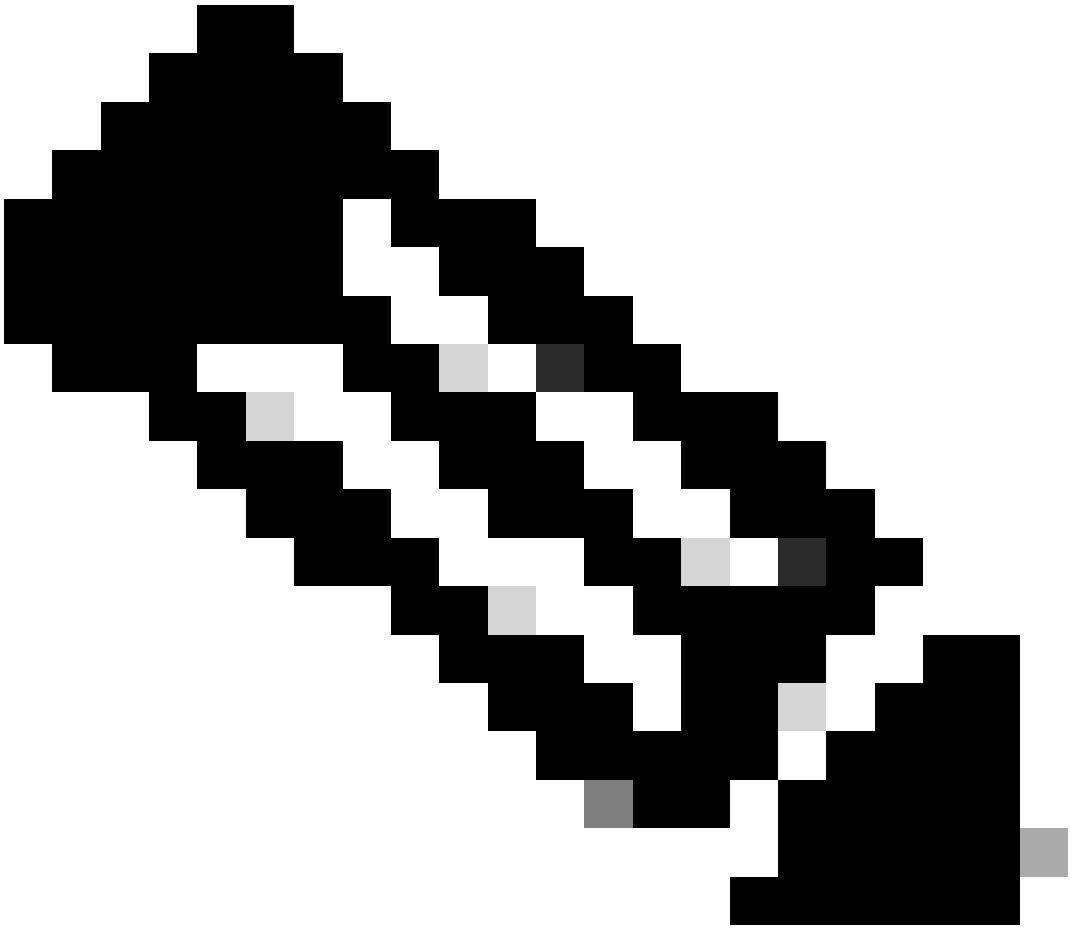
警告：确保选择正确的设备作为主要设备。所选主设备上的所有配置都将复制到所选辅助FTD设备。由于复制，可以替换辅助设备上的当前配置。

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#
show chassis detail

Chassis URL              : https://KSEC-FPR4100-1:443//
Chassis IP               : 192.0.2.1
Chassis Serial Number    : JMX12345678
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：

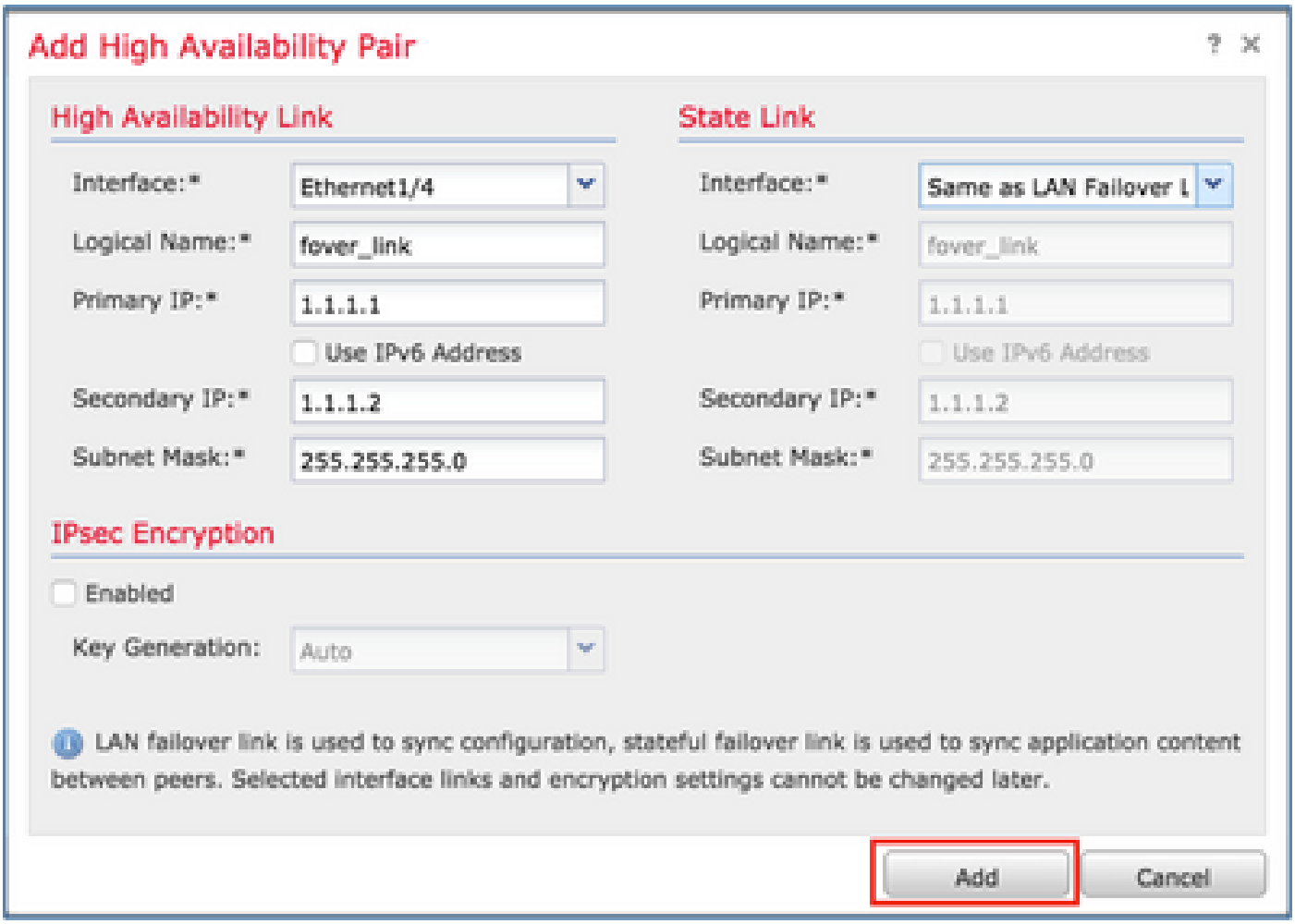
```
<#root>
KSEC-FPR9K-1-A#
scope system

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。

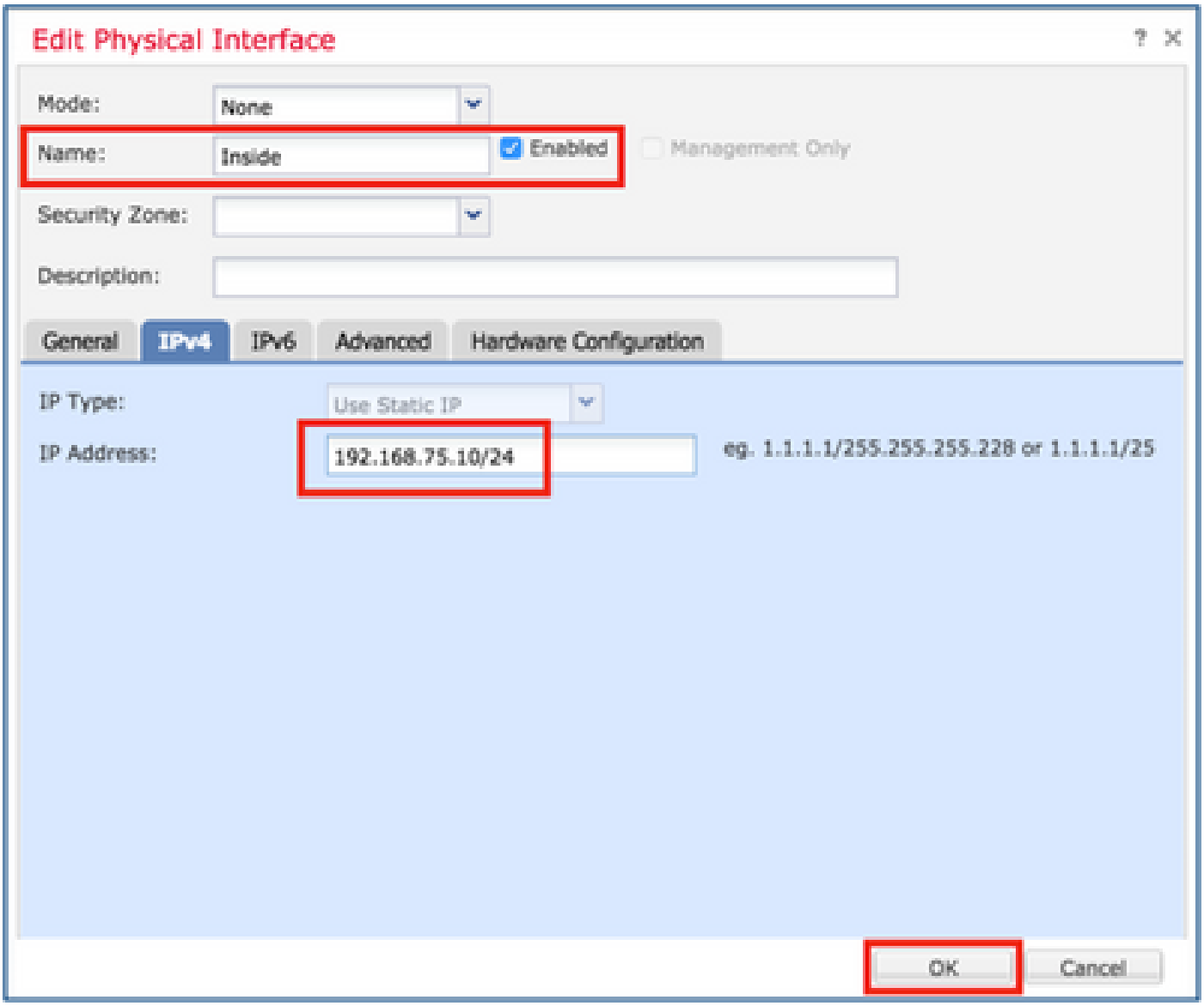


第四步：配置数据接口（主IP地址和备用IP地址）

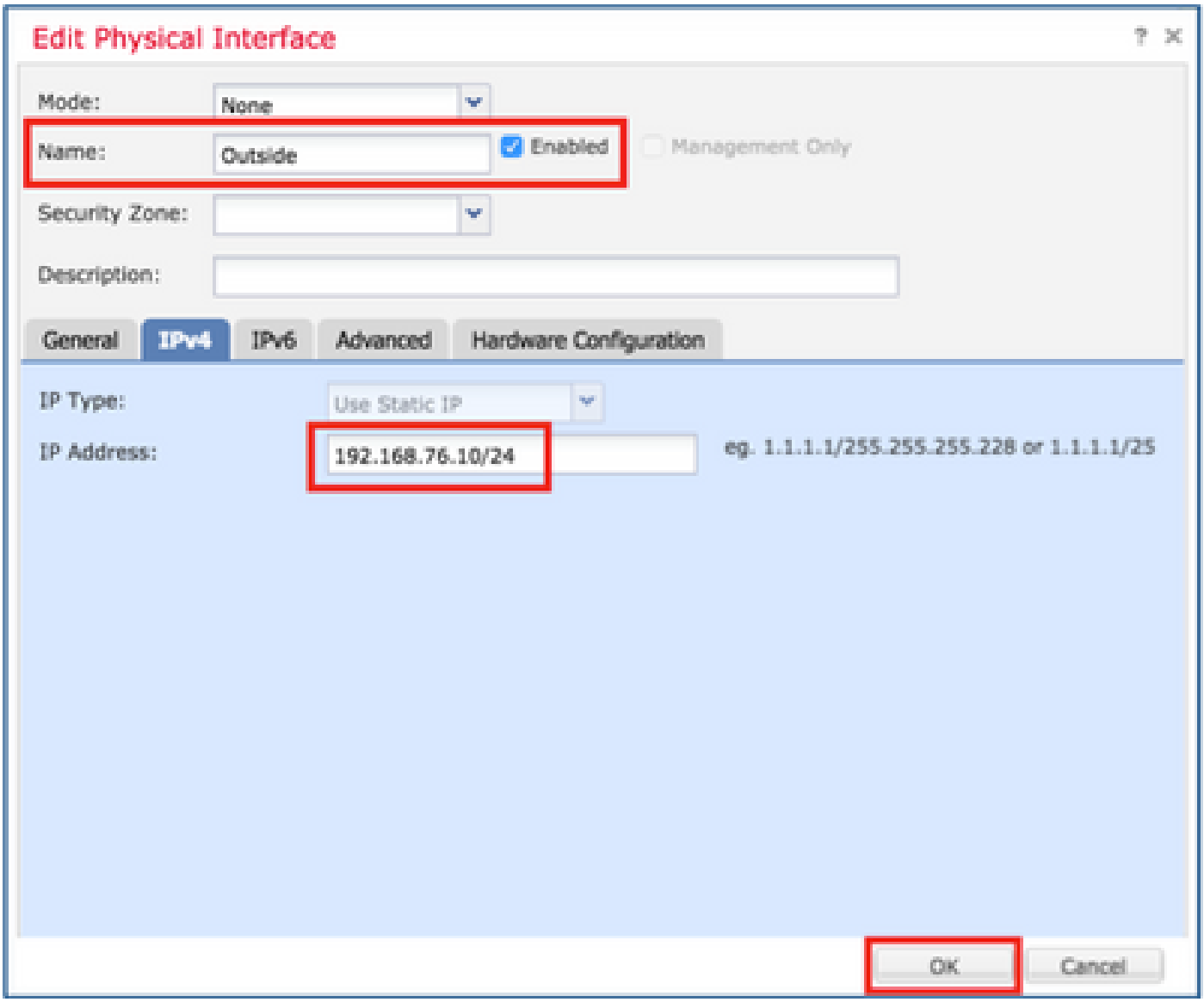
从FMC GUI中，选择HA Edit（如图所示）。

第五步：如图所示配置接口设置。

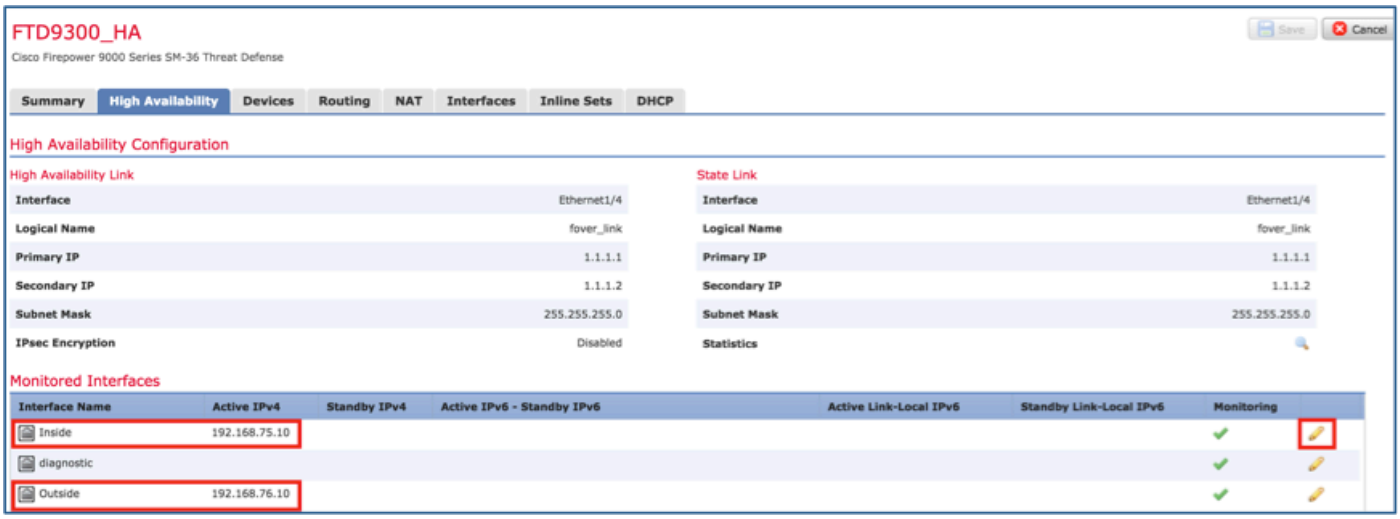
以太网 1/5 接口。


Edit Physical Interface
Mode:
None
Name:
Inside
Enabled
Management Only
Security Zone:
Description:
General
IPv4
IPv6
Advanced
Hardware Configuration
IP Type:
Use Static IP
IP Address:
192.168.75.10/24
eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25
OK
Cancel

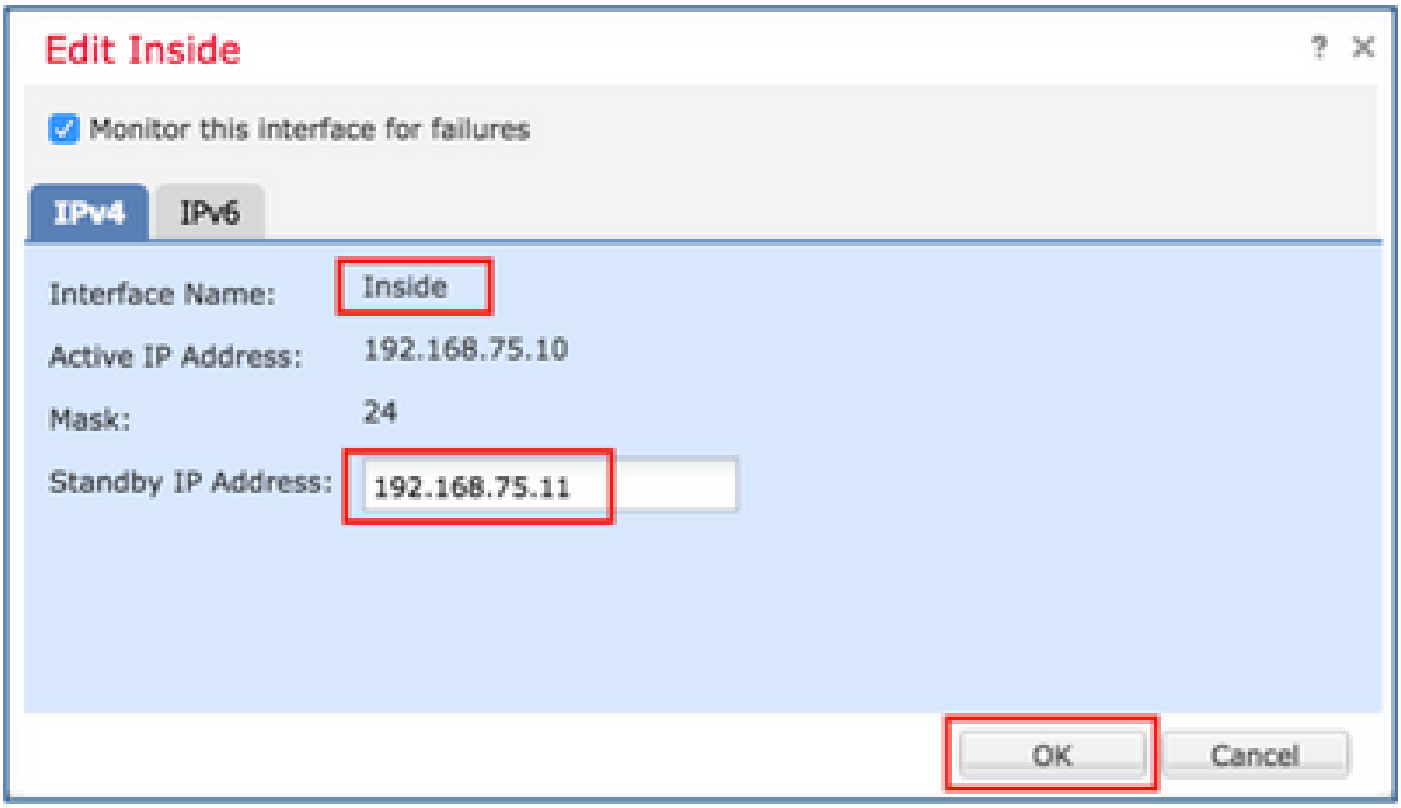
以太网 1/6 接口。



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。

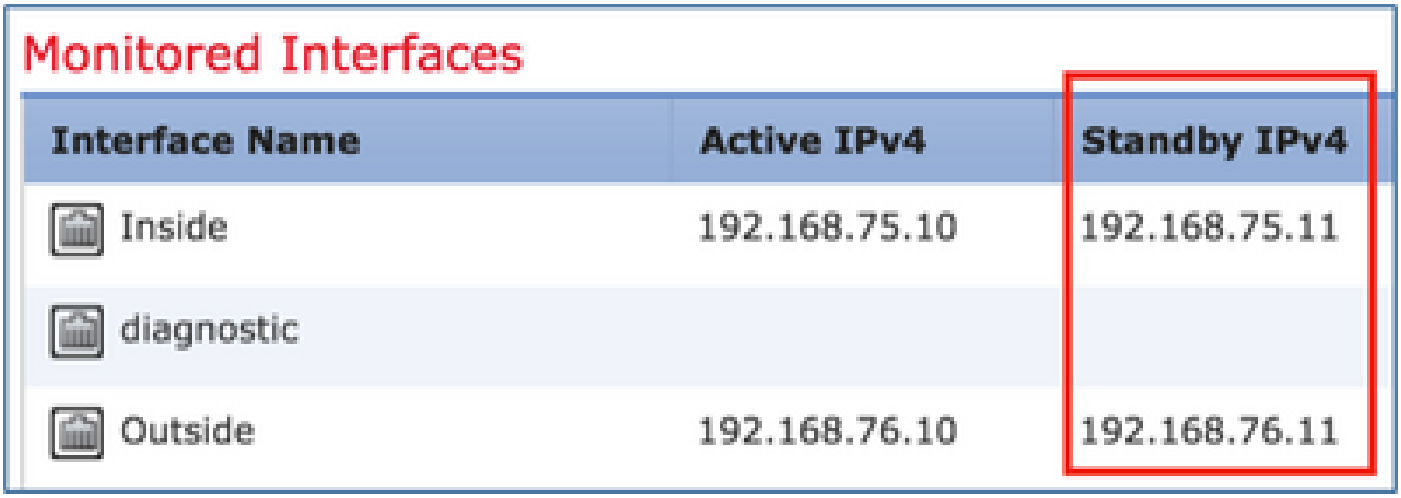


步骤 7.用于内部接口，如图所示。

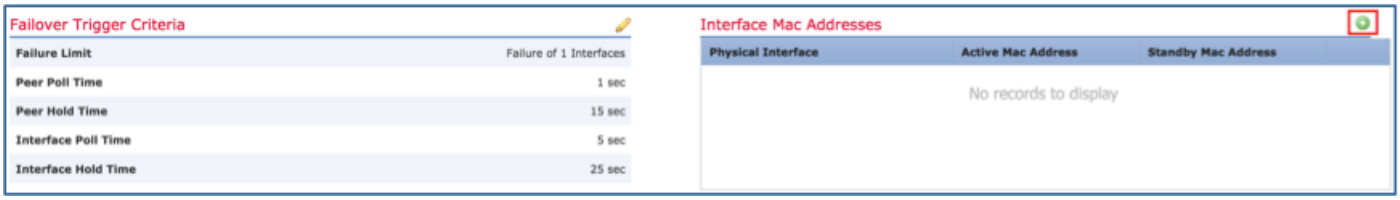


步骤 8对Outside接口执行相同操作。

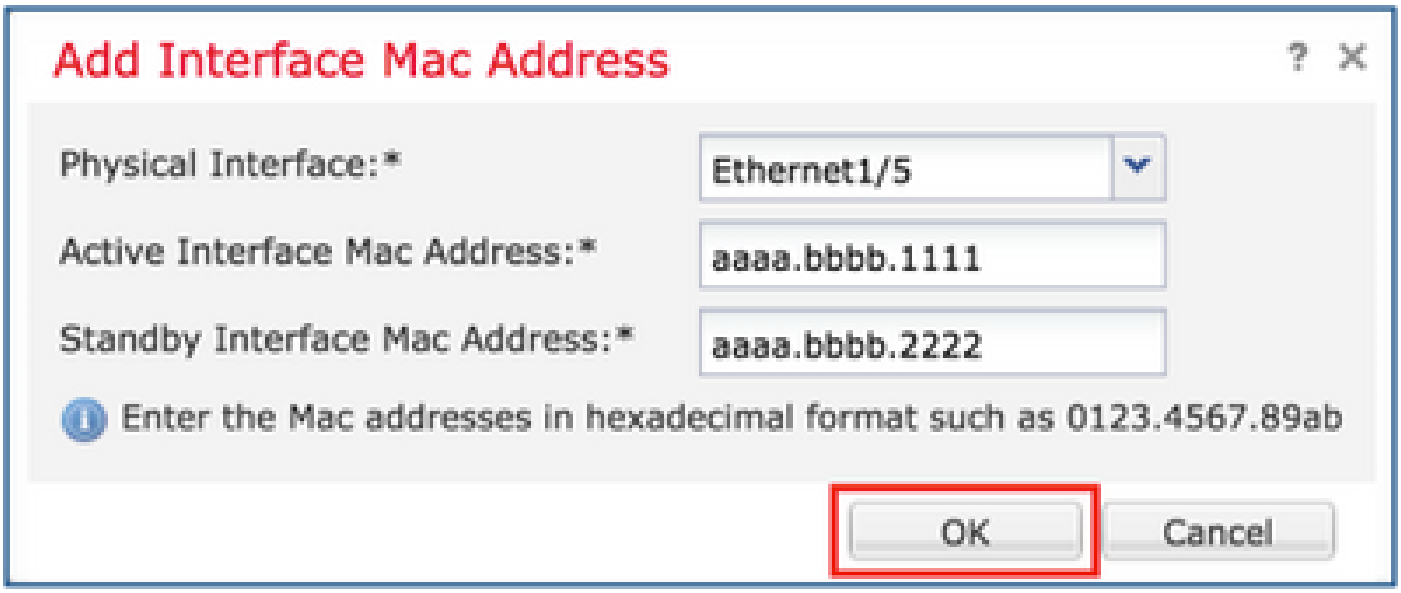
步骤 9验证结果如图所示。



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运行以下命令：

<#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
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours FLM19267A63, Mate FLM19206H7T
Last Failover at: 18:32:38 EEST Jul 21 2016
    This host: Primary - Active
        Active time: 3505 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 172 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
    Link : fover_link Ethernet1/4 (up)
    Stateful Obj     xmit       xerr       rcv        rerr
    General        417        0          416        0
    sys cmd      416        0          416        0
    up time      0          0          0          0
    RPC services      0          0          0          0
    TCP conn     0          0          0          0
    UDP conn     0          0          0          0
    ARP tbl      0          0          0          0
    Xlate_Timeout      0          0          0          0
    IPv6 ND tbl      0          0          0          0
    VPN IKEv1 SA     0          0          0          0
    VPN IKEv1 P2     0          0          0          0
    VPN IKEv2 SA     0          0          0          0
    VPN IKEv2 P2     0          0          0          0
    VPN CTCP upd     0          0          0          0
    VPN SDI upd     0          0          0          0
    VPN DHCP upd     0          0          0          0
```

```
    SIP Session     0          0          0          0
    SIP Tx     0          0          0          0
    SIP Pinhole     0          0          0          0
    Route Session     0          0          0          0
    Router ID     0          0          0          0
    User-Identity     1          0          0          0
    CTS SGTNAME     0          0          0          0
    CTS PAC     0          0          0          0
    TrustSec-SXP     0          0          0          0
    IPv6 Route     0          0          0          0
    STS Table     0          0          0          0

    Logical Update Queue Information
               Cur     Max     Total
    Recv Q:      0     10      416
    Xmit Q:      0     11      2118

>
```

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>

```
firepower#

show running-config failover

failover
failover lan unit primary
failover lan interface fover_link Ethernet1/4
failover replication http
```

```
failover mac address Ethernet1/5

aaaa.bbbb.1111 aaaa.bbbb.2222

failover mac address Ethernet1/6

aaaa.bbbb.3333 aaaa.bbbb.4444

failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2
firepower#

firepower#

show running-config interface

!
interface Ethernet1/2
 management-only
 nameif diagnostic
 security-level 0
 no ip address
!
interface Ethernet1/4
 description LAN/STATE Failover Interface
!
interface Ethernet1/5
 nameif Inside
 security-level 0
 ip address 192.168.75.10 255.255.255.0

standby 192.168.75.11

!
interface Ethernet1/6
 nameif Outside
 security-level 0
 ip address 192.168.76.10 255.255.255.0

standby 192.168.76.11

firepower#
```

任务4.切换故障切换角色

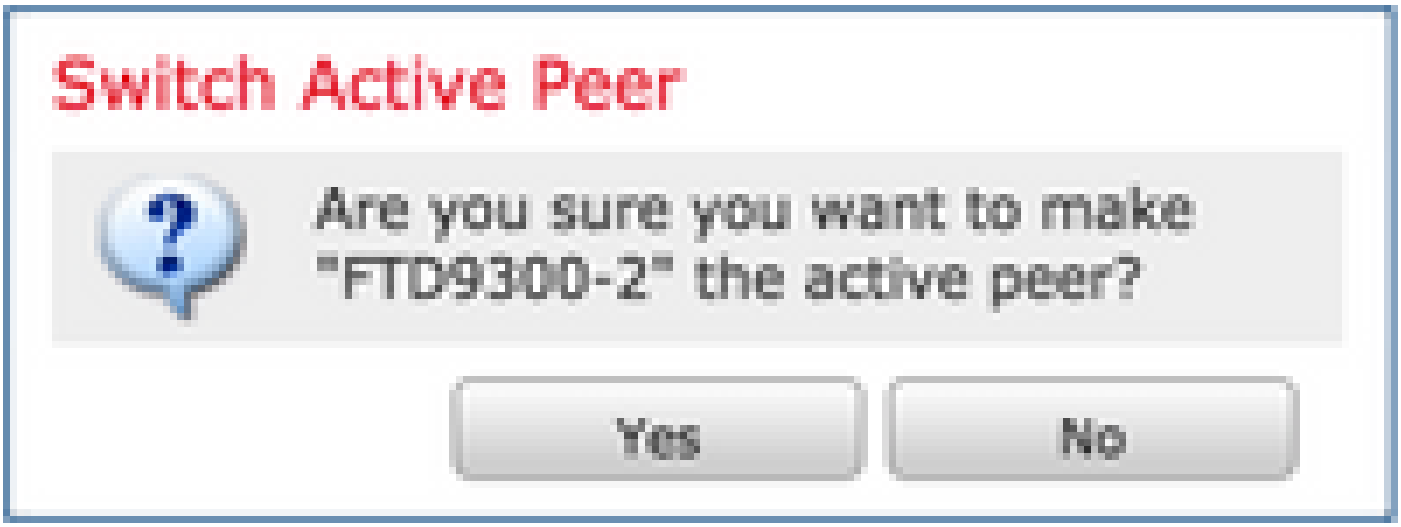
任务要求：

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：确认弹出窗口中的操作（如图所示）。



第三步：验证结果如图所示。

从 LINA CLI，可以看到系统在主/主用设备上执行了命令 no failover active：

```
<#root>

Jul 22 2016 10:39:26: %ASA-5-111008: User 'enable_15' executed the '

no failover active

' command.
Jul 22 2016 10:39:26: %ASA-5-111010: User 'enable_15', running 'N/A' from IP 0.0.0.0, executed 'no fail
```

您还可以在 show failover history 命令的输出中进行验证：

```
<#root>

firepower#

show failover history

==========================================================================
From State                  To State                    Reason
10:39:26 EEST Jul 22 2016
Active                      Standby Ready               Set by the config command
```

第四步：验证后，再次激活主设备。

任务5.中断HA对

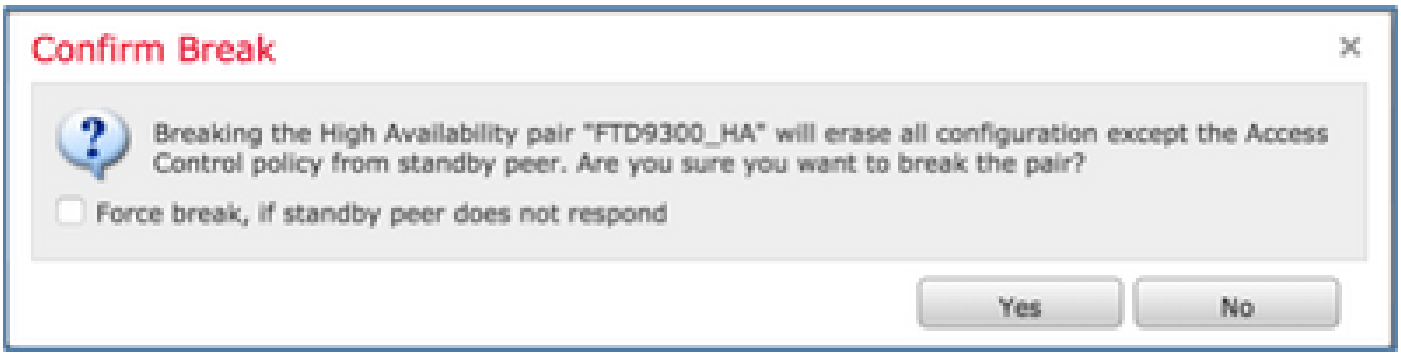
任务要求：

从 FMC 上中断故障切换对。

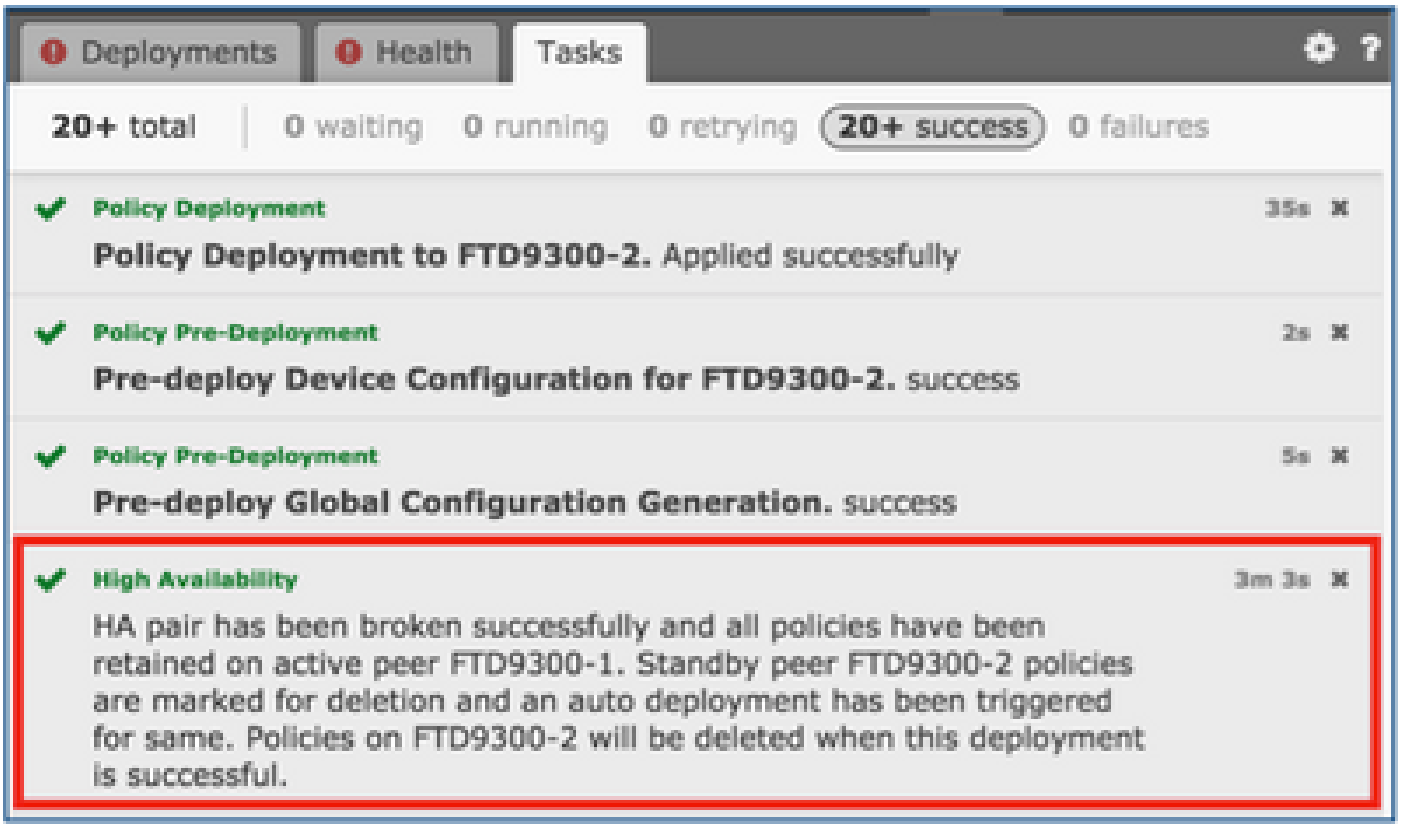
解决方案：

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：验证FMC GUI的结果（如图所示）。

在 HA 中断前后在主设备上运行 show running-config：

在 HA 中断之前	在 HA 中断之后
firepower# sh run : 已储存 : ：序列号：FLM19267A63 ：硬件：FPR9K-SM-36，135839 MB RAM，CPU Xeon E5系列2294 MHz，2个CPU（72核） : NGFW版本10.10.1.1 !	firepower# sh run : 已储存 : ：序列号：FLM19267A63 ：硬件：FPR9K-SM-36，135839 MB RA列2294 MHz，2个CPU（72核） : NGFW版本10.10.1.1 !

hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted 名称 ! interface Ethernet1/2 仅管理 nameif diagnostic security-level 0 no ip address ! interface Ethernet1/4 description LAN/STATE Failover Interface ! interface Ethernet1/5 nameif内部 security-level 0 ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11 ! interface Ethernet1/6 nameif外部 security-level 0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! ftp mode passive ngips conn-match vlan-id	hostname firepower enable password 8Ry2YjIyt7RRXU24 enc 名称 ! interface Ethernet1/2 仅管理 nameif diagnostic security-level 0 no ip address ! interface Ethernet1/4 no nameif no security-level no ip address ! interface Ethernet1/5 nameif内部 security-level 0 ip address 192.168.75.10 255.255.255.0 192.168.75.11 ! interface Ethernet1/6 nameif外部 security-level 0 ip address 192.168.76.10 255.255.255.0 192.168.76.11 !

access-list CSM_FW_ACL_ remark rule-id 268447744：访问策略：FTD9300 -强制/1 access-list CSM_FW_ACL_ remark rule-id 268447744： L4 RULE： Allow_ICMP access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600：访问策略：FTD9300 -默认/1 access-list CSM_FW_ACL_ remark rule-id 268441600： L4规则：默认操作规则 access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600 ！ tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow urgent-flag allow ！ 无传呼机 logging enable logging timestamp logging standby logging buffer-size 100000 日志记录缓冲调试 logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 mtu diagnostic 1500 mtu内部1500 1500以外的MTU	ftp mode passive ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -强制/1 access-list CSM_FW_ACL_ remark rule-id RULE： Allow_ICMP access-list CSM_FW_ACL_ advanced per rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -默认/1 access-list CSM_FW_ACL_ remark rule-id 则：默认操作规则 access-list CSM_FW_ACL_ advanced per 268441600 ！ tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow urgent-flag allow ！ 无传呼机 logging enable logging timestamp logging standby logging buffer-size 100000 日志记录缓冲调试 logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 mtu diagnostic 1500

故障转移	mtu内部1500
failover lan unit primary	1500以外的MTU
failover lan interface fover_link Ethernet1/4	不执行故障切换
failover replication http	no monitor-interface service-module
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	icmp unreachable rate-limit 1 burst-size 1
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaaa.bbbb.4444	no asdm history enable
failover link fover_link Ethernet1/4	arp timeout 14400
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	no arp permit-nonconnected
icmp unreachable rate-limit 1 burst-size 1	access-group CSM_FW_ACL_ global
no asdm history enable	timeout xlate 3:00:00
arp timeout 14400	timeout pat-xlate 0:00:30
no arp permit-nonconnected	timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02
access-group CSM_FW_ACL_ global	timeout sunrpc 0:10:00 h323 0:05:00 h22 0:05:00 mgcp-pat 0:05:00
timeout xlate 3:00:00	timeout sip 0:30:00 sip_media 0:02:00 sip disconnect 0:02:00
timeout pat-xlate 0:00:30	timeout sip-provisional-media 0:02:00 uau
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout tcp-proxy-reassembly 0:00:30
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout floating-conn 0:00:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	aaa proxy-limit disable
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	no snmp-server location
timeout tcp-proxy-reassembly 0:00:30	no snmp-server contact
timeout floating-conn 0:00:00	no snmp-server enable traps snmp authen linkdown coldstart warmstart
aaa proxy-limit disable	crypto ipsec security-association pmtu-ag
no snmp-server location	crypto ca trustpool policy
	telnet超时5

no snmp-server contact

no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet超时5

ssh stricthostkeycheck

ssh超时5

ssh key-exchange group dh-group1-sha1

控制台超时0

动态访问策略记录DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset_dns_map

参数

消息长度最大客户端自动

message-length maximum 512

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

参数

eool操作允许

nop操作允许

router-alert action allow

policy-map global_policy

ssh stricthostkeycheck

ssh超时5

ssh key-exchange group dh-group1-sha1

控制台超时0

动态访问策略记录DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset_dns_r

参数

消息长度最大客户端自动

message-length maximum 512

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

参数

eool操作允许

nop操作允许

router-alert action allow

policy-map global_policy

class inspection_default

inspect dns preset_dns_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect rsh

class inspection_default	inspect rtsp
inspect dns preset_dns_map	inspect sqlnet
inspect ftp	inspect skinny
inspect h323 h225	inspect sunrpc
inspect h323 ras	inspect xdmcp
inspect rsh	inspect sip
inspect rtsp	inspect netbios
inspect sqlnet	inspect tftp
inspect skinny	inspect icmp
inspect sunrpc	inspect icmp error
inspect xdmcp	inspect dcerpc
inspect sip	inspect ip-options UM_STATIC_IP_OPTIC
inspect netbios	class class-default
inspect tftp	set connection advanced-options UM_ST
inspect icmp	!
inspect icmp error	service-policy global_policy global
inspect dcerpc	prompt hostname context
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	呼叫总部
class class-default	profile CiscoTAC-1
set connection advanced-options UM_STATIC_TCP_MAP	无活动
!	目的地址http https://tools.cisco.com/its/service/oddce/s
service-policy global_policy global	目的地址电邮callhome@cisco.com
prompt hostname context	destination transport-method http
呼叫总部	订阅警报组诊断
profile CiscoTAC-1	subscribe-to-alert-group环境
无活动	每月定期订阅警报组资产

目的地址http https://tools.cisco.com/its/service/oddce/services/DDCEService 目的地址电邮callhome@cisco.com destination transport-method http 订阅警报组诊断 subscribe-to-alert-group环境 每月定期订阅警报组资产 每月定期进行subscribe-to-alert-group配置 订用警报组遥测每天定期 Cryptochecksum：933c594fc0264082edc0f24bad358031 ：结束 firepower#	每月定期进行subscribe-to-alert-group配置 订用警报组遥测每天定期 Cryptochecksum：fb6f5c369dee730b912 ：结束 firepower#

在HA断开前后在辅助单元上show running-config，如此处的表中所示。

在 HA 中断之前	在 HA 中断之后
firepower# sh run : 已储存 ： ：序列号：FLM19206H7T ：硬件：FPR9K-SM-36，135841 MB RAM，CPU Xeon E5系列2294 MHz，2个CPU（72核） ： NGFW版本10.10.1.1 ！ hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted 名称	firepower# sh run : 已储存 ： ：序列号：FLM19206H7T ：硬件：FPR9K-SM-36，135841 MB RA列2294 MHz，2个CPU（72核） ： NGFW版本10.10.1.1 ！ hostname firepower enable password 8Ry2YjIyt7RRXU24 enc 名称

!	!
interface Ethernet1/2	interface Ethernet1/2
仅管理	仅管理
nameif diagnostic	nameif diagnostic
security-level 0	security-level 0
no ip address	no ip address
!	!
interface Ethernet1/4	interface Ethernet1/4
description LAN/STATE Failover Interface	shutdown
!	no nameif
interface Ethernet1/5	no security-level
nameif内部	no ip address
security-level 0	!
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	interface Ethernet1/5
!	shutdown
interface Ethernet1/6	no nameif
nameif外部	no security-level
security-level 0	no ip address
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	!
!	interface Ethernet1/6
ftp mode passive	shutdown
ngips conn-match vlan-id	no nameif
access-list CSM_FW_ACL_ remark rule-id 268447744：访问策略：FTD9300 -强制/1	no security-level
access-list CSM_FW_ACL_ remark rule-id 268447744： L4 RULE： Allow_ICMP	no ip address
	!
	ftp mode passive

access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600：访问策略：FTD9300 -默认/1 access-list CSM_FW_ACL_ remark rule-id 268441600： L4规则：默认操作规则 access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600 ！ tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow urgent-flag allow ！ 无传呼机 logging enable logging timestamp logging standby logging buffer-size 100000 日志记录缓冲调试 logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 mtu diagnostic 1500 mtu内部1500 1500以外的MTU 故障转移 failover lan unit secondary failover lan interface fover_link Ethernet1/4	ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -强制/1 access-list CSM_FW_ACL_ remark rule-id RULE： Allow_ICMP access-list CSM_FW_ACL_ advanced per rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -默认/1 access-list CSM_FW_ACL_ remark rule-id 则：默认操作规则 access-list CSM_FW_ACL_ advanced per 268441600 ！ tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 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

failover replication http	no logging message 302018
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	no logging message 302017
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaaa.bbbb.4444	no logging message 302016
failover link fover_link Ethernet1/4	no logging message 302021
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	no logging message 302020
icmp unreachable rate-limit 1 burst-size 1	mtu diagnostic 1500
no asdm history enable	不执行故障切换
arp timeout 14400	no monitor-interface service-module
no arp permit-nonconnected	icmp unreachable rate-limit 1 burst-size 1
access-group CSM_FW_ACL_ global	no asdm history enable
timeout xlate 3:00:00	arp timeout 14400
timeout pat-xlate 0:00:30	no arp permit-nonconnected
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	access-group CSM_FW_ACL_ global
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout xlate 3:00:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	timeout pat-xlate 0:00:30
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02
timeout tcp-proxy-reassembly 0:00:30	timeout sunrpc 0:10:00 h323 0:05:00 h22 0:05:00 mgcp-pat 0:05:00
timeout floating-conn 0:00:00	timeout sip 0:30:00 sip_media 0:02:00 sip disconnect 0:02:00
用户身份默认域本地	timeout sip-provisional-media 0:02:00 uau
aaa proxy-limit disable	timeout tcp-proxy-reassembly 0:00:30
no snmp-server location	timeout floating-conn 0:00:00
no snmp-server contact	aaa proxy-limit disable
no snmp-server enable traps snmp authentication linkup	no snmp-server location
	no snmp-server contact
	no snmp-server enable traps snmp auther

linkdown coldstart warmstart	linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite	crypto ipsec security-association pmtu-ag
crypto ca trustpool policy	crypto ca trustpool policy
telnet超时5	telnet超时5
ssh stricthostkeycheck	ssh stricthostkeycheck
ssh超时5	ssh超时5
ssh key-exchange group dh-group1-sha1	ssh key-exchange group dh-group1-sha1
控制台超时0	控制台超时0
动态访问策略记录DfltAccessPolicy	动态访问策略记录DfltAccessPolicy
!	!
class-map inspection_default	class-map inspection_default
match default-inspection-traffic	match default-inspection-traffic
!	!
!	!
policy-map type inspect dns preset_dns_map	policy-map type inspect dns preset_dns_m
参数	参数
消息长度最大客户端自动	消息长度最大客户端自动
message-length maximum 512	message-length maximum 512
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
参数	参数
eool操作允许	eool操作允许
nop操作允许	nop操作允许
router-alert action allow	router-alert action allow
policy-map global_policy	policy-map global_policy
class inspection_default	class inspection_default
inspect dns preset_dns_map	inspect dns preset_dns_map

inspect ftp	inspect ftp
inspect h323 h225	inspect h323 h225
inspect h323 ras	inspect h323 ras
inspect rsh	inspect rsh
inspect rtsp	inspect rtsp
inspect sqlnet	inspect sqlnet
inspect skinny	inspect skinny
inspect sunrpc	inspect sunrpc
inspect xdmcp	inspect xdmcp
inspect sip	inspect sip
inspect netbios	inspect netbios
inspect tftp	inspect tftp
inspect icmp	inspect icmp
inspect icmp error	inspect icmp error
inspect dcerpc	inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect ip-options UM_STATIC_IP_OPTIC
class class-default	class class-default
set connection advanced-options UM_STATIC_TCP_MAP	set connection advanced-options UM_ST
!	!
service-policy global_policy global	service-policy global_policy global
prompt hostname context	prompt hostname context
呼叫总部	呼叫总部
profile CiscoTAC-1	profile CiscoTAC-1
无活动	无活动
目的地址http https://tools.cisco.com/its/service/oddce/services/DDCEService	目的地址http https://tools.cisco.com/its/service/oddce/s
目的地址电邮callhome@cisco.com	目的地址电邮callhome@cisco.com

destination transport-method http 订阅警报组诊断 subscribe-to-alert-group环境 每月定期订阅警报组资产 每月定期进行subscribe-to-alert-group配置 订用警报组遥测每天定期 Cryptochecksum：e648f92dd7ef47ee611f2aaa5c6cbd84 ：结束 firepower#	destination transport-method http 订阅警报组诊断 subscribe-to-alert-group环境 每月定期订阅警报组资产 每月定期进行subscribe-to-alert-group配置 订用警报组遥测每天定期 Cryptochecksum：08ed87194e9f5cd914 ：结束 firepower#

关于 HA 中断的主要注意事项：

主要单元	辅助单元
所有故障切换配置已删除. 备用IP地址保留。	删除所有配置。

第五步：完成此任务后，重新创建HA对。

任务6.禁用HA对

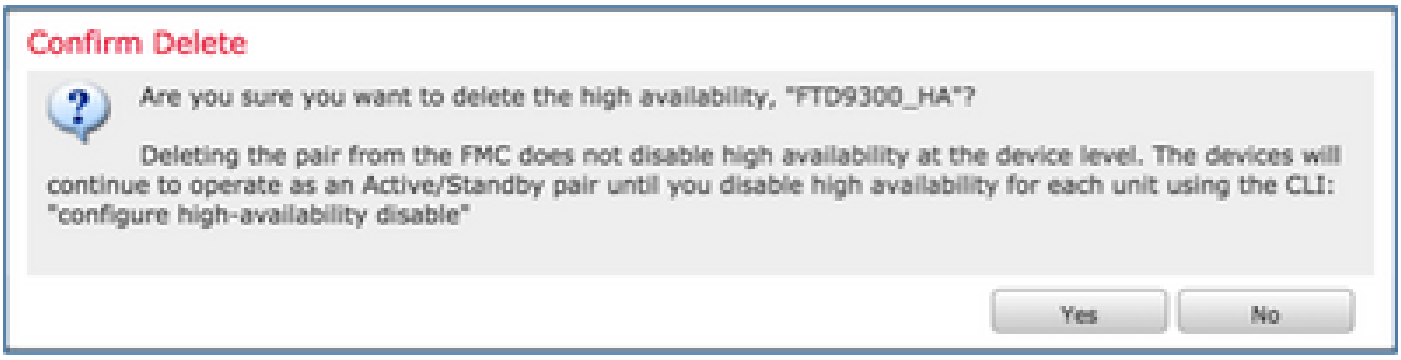
任务要求：

从 FMC 上禁用故障切换对。

解决方案：

步骤1:选择图标，如图所示。

第二步：如图所示，检查通知并确认。



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：

主要单元	辅助单元
firepower# sh run : 已储存 ： ：序列号：FLM19267A63 ：硬件：FPR9K-SM-36，135839 MB RAM，CPU Xeon E5系列2294 MHz，2个CPU（72核） ： NGFW版本10.10.1.1 ！ hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted 名称 ！ interface Ethernet1/2 仅管理 nameif diagnostic security-level 0 no ip address	firepower# sh run : 已储存 ： ：序列号：FLM19206H7T ：硬件：FPR9K-SM-36，135841 MB RA 列2294 MHz，2个CPU（72核） ： NGFW版本10.10.1.1 ！ hostname firepower enable password 8Ry2YjIyt7RRXU24 enc 名称 ！ interface Ethernet1/2 仅管理 nameif diagnostic security-level 0 no ip address

!	!
interface Ethernet1/4	interface Ethernet1/4
description LAN/STATE Failover Interface	description LAN/STATE Failover Interface
!	!
interface Ethernet1/5	interface Ethernet1/5
nameif内部	nameif内部
security-level 0	security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	ip address 192.168.75.10 255.255.255.0 s 192.168.75.11
!	!
interface Ethernet1/6	interface Ethernet1/6
nameif外部	nameif外部
security-level 0	security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	ip address 192.168.76.10 255.255.255.0 s 192.168.76.11
!	!
ftp mode passive	ftp mode passive
ngips conn-match vlan-id	ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744：访问策略：FTD9300 -强制/1	access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -强制/1
access-list CSM_FW_ACL_ remark rule-id 268447744： L4 RULE： Allow_ICMP	access-list CSM_FW_ACL_ remark rule-id RULE： Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both	access-list CSM_FW_ACL_ advanced per rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 268441600：访问策略：FTD9300 -默认/1	access-list CSM_FW_ACL_ remark rule-id 略：FTD9300 -默认/1
access-list CSM_FW_ACL_ remark rule-id 268441600： L4规则：默认操作规则	access-list CSM_FW_ACL_ remark rule-id 则：默认操作规则
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600	access-list CSM_FW_ACL_ advanced per 268441600

!	!
tcp-map UM_STATIC_TCP_MAP	tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 7 allow	tcp-options range 6 7 allow
tcp-options range 9 255 allow	tcp-options range 9 255 allow
urgent-flag allow	urgent-flag allow
!	!
无传呼机	无传呼机
logging enable	logging enable
logging timestamp	logging timestamp
logging standby	logging standby
logging buffer-size 100000	logging buffer-size 100000
日志记录缓冲调试	日志记录缓冲调试
logging flash-minimum-free 1024	logging flash-minimum-free 1024
logging flash-maximum-allocation 3076	logging flash-maximum-allocation 3076
mtu diagnostic 1500	mtu diagnostic 1500
mtu内部1500	mtu内部1500
1500以外的MTU	1500以外的MTU
故障转移	故障转移
failover lan unit primary	failover lan unit secondary
failover lan interface fover_link Ethernet1/4	failover lan interface fover_link Ethernet1/
failover replication http	failover replication http
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	failover mac address Ethernet1/5 aaaa.bb aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaaa.bbbb.4444	failover mac address Ethernet1/6 aaaa.bb aaaaa.bbbb.4444
failover link fover_link Ethernet1/4	failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	failover interface ip fover_link 10.10.1.1 25 10.10.1.2

icmp unreachable rate-limit 1 burst-size 1	icmp unreachable rate-limit 1 -size 1
no asdm history enable	no asdm history enable
arp timeout 14400	arp timeout 14400
no arp permit-nonconnected	no arp permit-nonconnected
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
timeout xlate 3:00:00	timeout xlate 3:00:00
timeout pat-xlate 0:00:30	timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout sunrpc 0:10:00 h323 0:05:00 h22 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	timeout sip 0:30:00 sip_media 0:02:00 sip disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout sip-provisional-media 0:02:00 uau
timeout tcp-proxy-reassembly 0:00:30	timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00	timeout floating-conn 0:00:00
aaa proxy-limit disable	用户身份默认域本地
no snmp-server location	aaa proxy-limit disable
no snmp-server contact	no snmp-server location
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	no snmp-server contact
crypto ipsec security-association pmtu-aging infinite	no snmp-server enable traps snmp authe linkdown coldstart warmstart
crypto ca trustpool policy	crypto ipsec security-association pmtu-ag
telnet超时5	crypto ca trustpool policy
ssh stricthostkeycheck	telnet超时5
ssh超时5	ssh stricthostkeycheck
ssh key-exchange group dh-group1-sha1	ssh超时5
控制台超时0	ssh key-exchange group dh-group1-sha1

动态访问策略记录DfltAccessPolicy ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map 参数 消息长度最大客户端自动 message-length maximum 512 policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP 参数 eool操作允许 nop操作允许 router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc	控制台超时0 动态访问策略记录DfltAccessPolicy ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_r 参数 消息长度最大客户端自动 message-length maximum 512 policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP 参数 eool操作允许 nop操作允许 router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny

inspect xdmcp	inspect sunrpc
inspect sip	inspect xdmcp
inspect netbios	inspect sip
inspect tftp	inspect netbios
inspect icmp	inspect tftp
inspect icmp error	inspect icmp
inspect dcerpc	inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect dcerpc
class class-default	inspect ip-options UM_STATIC_IP_OPTIC
set connection advanced-options UM_STATIC_TCP_MAP	class class-default
！	set connection advanced-options UM_STA
service-policy global_policy global	！
prompt hostname context	service-policy global_policy global
呼叫总部	prompt hostname context
profile CiscoTAC-1	呼叫总部
无活动	profile CiscoTAC-1
目的地址http https://tools.cisco.com/its/service/oddce/services/DDCEService	无活动
目的地址电邮callhome@cisco.com	目的地址http https://tools.cisco.com/its/service/oddce/s
destination transport-method http	目的地址电邮callhome@cisco.com
订阅警报组诊断	destination transport-method http
subscribe-to-alert-group环境	订阅警报组诊断
每月定期订阅警报组资产	subscribe-to-alert-group环境
每月定期进行subscribe-to-alert-group配置	每月定期订阅警报组资产
订用警报组遥测每天定期	每月定期进行subscribe-to-alert-group配置
Cryptochecksum：933c594fc0264082edc0f24bad358031	订用警报组遥测每天定期
：结束	Cryptochecksum：e648f92dd7ef47ee611

firepower#	：结束 firepower#

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.

第五步：运行此命令可从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.
```

注意：必须在两台设备上运行命令

结果：

主要单元	辅助单元
> **show failover**	> **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 2 of 1041 maximum** **MAC Address Move Notification Interval not set** >	**Failover Off (pseudo-Standby)** **Failover unit Secondary** **Failover LAN Interface: FOVER Ethernet1/3.205 (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 1041 maximum** **MAC Address Move Notification Interval not set** **failover replication http** >

主	辅助
firepower# show run ! hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted 名称 arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 ! interface GigabitEthernet1/1 nameif outside cts manual（cts手册） propagate sgt preserve-untag 策略静态sgt已禁用，受信任 security-level 0	firepower# show run ! hostname firepower enable password 8Ry2YjIyt7RRXU24 enc 名称 arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 ! interface GigabitEthernet1/1 shutdown no nameif no security-level no ip address !

```
ip address 10.1.1.1 255.255.255.0 <—已删除standby IP
!
interface GigabitEthernet1/2
 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 192.168.1.1 255.255.255.0 <—已删除standby IP
!
interface GigabitEthernet1/3
 说明LAN故障切换接口
!
interface GigabitEthernet1/4
 description STATE Failover Interface
!
interface GigabitEthernet1/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/6
 shutdown
 no nameif
 no security-level
```

```
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 说明LAN故障切换接口
!
interface GigabitEthernet1/4
 description STATE Failover Interface
!
interface GigabitEthernet1/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/6
 shutdown
 no nameif
no security-level
 no ip address
!
interface GigabitEthernet1/7
 shutdown
```

```
 no ip address
 !
interface GigabitEthernet1/7
 shutdown
 no nameif
 no security-level
 no ip address
 !
interface GigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
 !
接口管理1/1
 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
 !
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998： PREFILTER POLICY： Default Tunnel and Priority Policy
```

```
 no nameif
 no security-level
 no ip address
 !
interface GigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
 !
接口管理1/1
 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
 !
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id
POLICY： Default Tunnel and Priority Pol
access-list CSM_FW_ACL_ remark rule-id
隧道操作规则
access-list CSM_FW_ACL_ advanced per
rule-id 9998
access-list CSM_FW_ACL_ advanced per
```

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 41 any any rule-id 9998

access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998

access-list CSM_FW_ACL_ advanced permit udp any any eq 3544 rule-id 9998

access-list CSM_FW_ACL_ remark rule-id 268435456：访问策略：FTD_HA -默认/1

access-list CSM_FW_ACL_ remark rule-id 268435456： L4规则：默认操作规则

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435456

!

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

logging enable

logging timestamp

日志记录缓冲调试

logging flash-minimum-free 1024

logging flash-maximum-allocation 3076

id 9998

access-list CSM_FW_ACL_ advanced per
id 9998

access-list CSM_FW_ACL_ advanced per
3544 rule-id 9998

access-list CSM_FW_ACL_ remark rule-id
略：FTD_HA -默认/1

access-list CSM_FW_ACL_ remark rule-id
则：默认操作规则

access-list CSM_FW_ACL_ advanced per
268435456

!

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

logging enable

logging timestamp

日志记录缓冲调试

logging flash-minimum-free 1024

logging flash-maximum-allocation 3076

no logging message 106015

no logging message 313001

no logging message 313008

no logging message 106023

no logging message 106015	no logging message 710005
no logging message 313001	no logging message 710003
no logging message 313008	no logging message 106100
no logging message 106023	no logging message 302015
no logging message 710005	no logging message 302014
no logging message 710003	no logging message 302013
no logging message 106100	no logging message 302018
no logging message 302015	no logging message 302017
no logging message 302014	no logging message 302016
no logging message 302013	no logging message 302021
no logging message 302018	no logging message 302020
no logging message 302017	1500外部的MTU
no logging message 302016	mtu inside 1500
no logging message 302021	mtu diagnostic 1500
no logging message 302020	不执行故障切换
1500外部的MTU	failover lan unit secondary
mtu inside 1500	failover lan interface FOVER GigabitEther
mtu diagnostic 1500	failover replication http
不执行故障切换	failover link STATE GigabitEthernet1/4
icmp unreachable rate-limit 1 burst-size 1	failover interface ip FOVER 10.10.1.1 255 10.10.1.2
no asdm history enable	failover interface ip STATE 10.10.2.1 255 10.10.2.2
access-group CSM_FW_ACL_ global	icmp unreachable rate-limit 1 burst-size 1
00 community *****版本2c	no asdm history enable
no snmp-server location	access-group CSM_FW_ACL_ global
no snmp-server contact	timeout xlate 3:00:00
snmp-server community *****	

service sw-reset-button

crypto ipsec security-association pmtu-aging infinite

crypto ca trustpool policy

telnet超时5

控制台超时0

动态访问策略记录DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset_dns_map

参数

消息长度最大客户端自动

message-length maximum 512

no tcp-inspection

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

参数

eool操作允许

nop操作允许

router-alert action allow

policy-map global_policy

class inspection_default

inspect dns preset_dns_map

inspect ftp

inspect h323 h225

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 0:02:00 icmp 0:00:02

timeout sunrpc 0:10:00 h323 0:05:00 h22 0:05:00 mgcp-pat 0:05:00

timeout sip 0:30:00 sip_media 0:02:00 sip disconnect 0:02:00

timeout sip-provisional-media 0:02:00 uau

timeout tcp-proxy-reassembly 0:00:30

timeout floating-conn 0:00:00

timeout conn-holddown 0:00:15

用户身份默认域本地

aaa proxy-limit disable

snmp-server host outside 192.168.1.100 c version 2c

no snmp-server location

no snmp-server contact

snmp-server community *****

service sw-reset-button

crypto ipsec security-association pmtu-ag

crypto ca trustpool policy

telnet超时5

控制台超时0

动态访问策略记录DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

inspect h323 ras

inspect rsh

inspect rtsp

inspect esmtp

inspect sqlnet

inspect skinny

inspect sunrpc

inspect xdmcp

inspect sip

inspect netbios

inspect tftp

inspect icmp

inspect icmp error

inspect dcerpc

inspect ip-options UM_STATIC_IP_OPTIONS_MAP

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

!

service-policy global_policy global

prompt hostname context

呼叫总部

profile CiscoTAC-1

无活动

目的地址http https://tools.cisco.com/its/service/oddce/services/DDCEService

目的地址电邮callhome@cisco.com

destination transport-method http

!

policy-map type inspect dns preset_dns_r

参数

消息长度最大客户端自动

message-length maximum 512

no tcp-inspection

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP

参数

eool操作允许

nop操作允许

router-alert action allow

policy-map global_policy

class inspection_default

inspect dns preset_dns_map

inspect ftp

inspect h323 h225

inspect h323 ras

inspect rsh

inspect rtsp

inspect esmtp

inspect sqlnet

inspect skinny

inspect sunrpc

inspect xdmcp

inspect sip

inspect netbios

订阅警报组诊断 subscribe-to-alert-group环境 每月定期订阅警报组资产 每月定期进行subscribe-to-alert-group配置 订用警报组遥测每天定期 Cryptochecksum：768a03e90b9d3539773b9d7af66b3452	inspect tftp inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTI class class-default set connection advanced-options UM_ST ! service-policy global_policy global prompt hostname context 呼叫总部 profile CiscoTAC-1 无活动 目的地址http https://tools.cisco.com/its/service/oddce/s 目的地址电邮callhome@cisco.com destination transport-method http 订阅警报组诊断 subscribe-to-alert-group环境 每月定期订阅警报组资产 每月定期进行subscribe-to-alert-group配 订用警报组遥测每天定期 Cryptochecksum：ac9b8f401e18491fee6

从 FTD CLI 上禁用 HA 的主要注意事项：

主要单元	辅助单元

故障切换配置和备用IP aretimeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:00:30 timeout floating-conn 0:00:00 timeout conn-holddown 0:00:15 aaa proxy-limit disable snmp-server host outside 192.168.1.1 removed。	• 接口配置已删除. • 设备进入伪备用模式.

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

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

Y <-- Be careful. This will disable 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）。