Konfigurieren von FTD-Hochverfügbarkeit auf Firepower-Appliances

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Aufgabe 1: Überprüfen der Bedingungen](#)
[Aufgabe 2: Konfigurieren von FTD HA auf FPR9300](#)
[Bedingungen](#)
[Aufgabe 3: Überprüfen von FTD HA und Lizenz](#)
[Aufgabe 4: Failover-Rollen wechseln](#)
[Aufgabe 5: Aufbrechen des HA-Paars](#)
[Aufgabe 6. HA-Paar deaktivieren](#)
[Aufgabe 7: HA aussetzen](#)
[Häufig gestellte Fragen](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Firepower Threat Defense (FTD) High Availability (HA) (Aktiv/Standby-Failover) auf FPR9300 konfigurieren und überprüfen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 2 Cisco FirePOWER 9300 Security Appliances - FXOS SW 2.0(1.23)
- FTD-Version 10.10.1.1 (Build 1023)
- FirePOWER Management Center (FMC) - SW 10.10.1.1 (Build 1023)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

> **Anmerkung:** Auf einer FPR9300-Appliance mit FTD können Sie nur Interchassis-HA konfigurieren. Die beiden Einheiten einer HA-Konfiguration müssen die hier genannten Bedingungen erfüllen.

Aufgabe 1: Überprüfen der Bedingungen

Aufgabenanforderung:

Überprüfen Sie, ob beide FTD-Einheiten die Anforderungen für die Notizen erfüllen und als HA-Einheiten konfiguriert werden können.

Lösung:

Schritt 1: Stellen Sie eine Verbindung zur Management-IP des FPR9300 her, und überprüfen Sie die Modulhardware.

Überprüfen Sie die FPR9300-1-Hardware.

```
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#
```

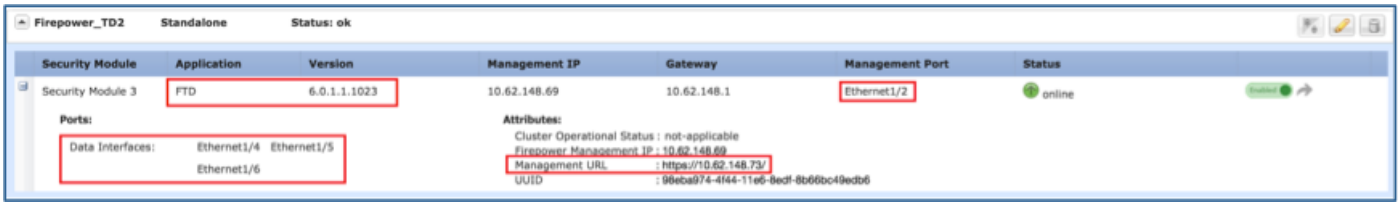
Überprüfen Sie die FPR9300-2-Hardware.

```
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#
```

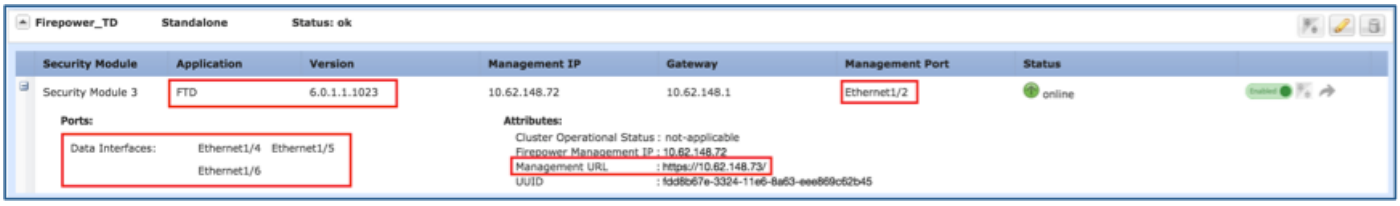
Schritt 2: Melden Sie sich beim FPR9300-1 Chassis Manager an, und navigieren Sie zu Logical Devices (Logische Geräte).

Überprüfen Sie die Softwareversion, die Anzahl und den Schnittstellentyp, wie in den Images gezeigt.

FPR9300-1



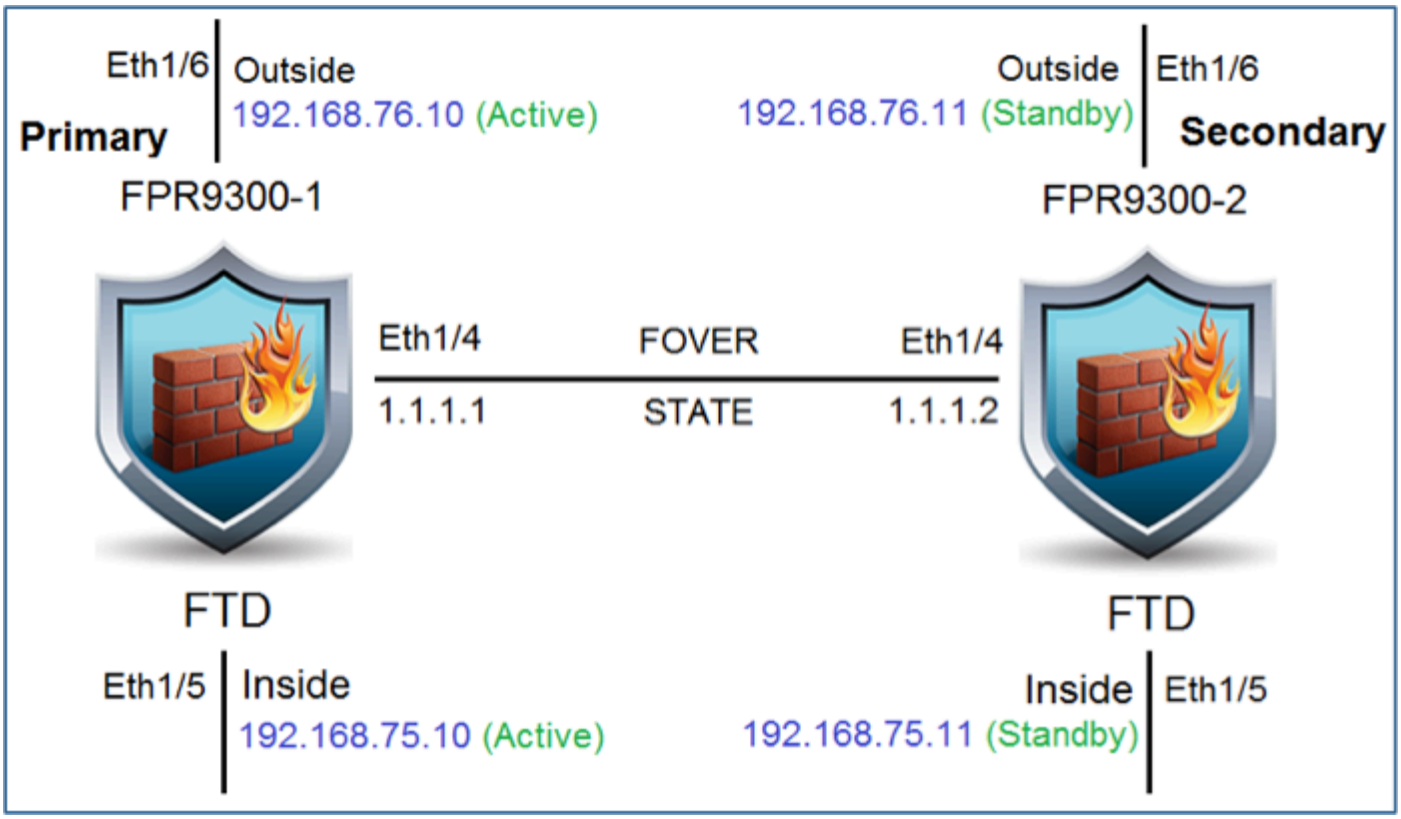
FPR9300-2



Aufgabe 2: Konfigurieren von FTD HA auf FPR9300

Aufgabenanforderung:

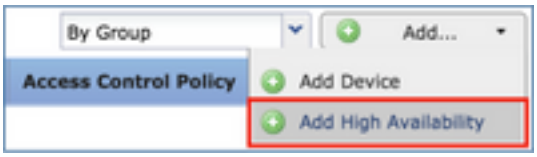
Konfigurieren Sie Aktiv/Standby-Failover (HA) gemäß diesem Diagramm.



Lösung:

Beide FTD-Geräte sind bereits auf dem FMC registriert (siehe Abbildung).

Schritt 1: Um FTD-Failover zu konfigurieren, navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung)** und wählen Sie **Add High Availability (Hochverfügbarkeit hinzufügen),** wie im Bild dargestellt.



Schritt 2: Geben Sie den **primären Peer** und den **sekundären Peer ein**, und wählen Sie **Weiter** aus, wie im Bild dargestellt.

> **Warnung:** Stellen Sie sicher, dass Sie die richtige Einheit als **primäre** Einheit auswählen. Alle Konfigurationen auf der ausgewählten primären Einheit werden auf die ausgewählte sekundäre FTD-Einheit repliziert. Durch die Replikation kann die aktuelle Konfiguration auf der sekundären Einheit **ersetzt** werden.

Bedingungen

Um eine hohe Verfügbarkeit zwischen zwei FTD-Geräten zu erreichen, müssen folgende Bedingungen erfüllt sein:

- Gleiches Modell
- Gleiche Version (gilt für FXOS und FTD - (Major (erste Zahl), Minor (zweite Zahl) und Wartung (dritte Zahl) müssen gleich sein))
- Gleiche Anzahl an Schnittstellen
- Derselbe Schnittstellentyp
- Beide Geräte gehören zur gleichen Gruppe/Domäne im FMC.
- Identische NTP-Konfiguration (Network Time Protocol)
- Vollständige Bereitstellung auf dem FMC ohne unbestätigte Änderungen
- Wechseln Sie in denselben Firewall-Modus: geroutet oder transparent.
- Beachten Sie, dass dies sowohl auf FTD-Geräten als auch auf der FMC-GUI überprüft werden muss, da es Fälle gegeben hat, in denen die FTDs den gleichen Modus hatten, aber

FMC spiegelt dies nicht wider.

- Keine DHCP/Point-to-Point Protocol over Ethernet (PPPoE)-Konfiguration an einer der Schnittstellen
- Anderer Hostname (FQDN, Fully Qualified Domain Name) für beide Chassis. Um den Chassis-Hostnamen zu überprüfen, navigieren Sie zu FTD CLI, und führen Sie den folgenden Befehl aus:

```
firepower# show chassis-management-url

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

Anmerkung: Verwenden Sie nach 6.3 FTD den Befehl **'show chassis detail'.**

```
firepower# show chassis detail
Chassis URL              : https://KSEC-FPR4100-1:443//
Chassis IP               : 192.0.2.1
Chassis Serial Number    : JMX12345678
Security Module          : 1
```

Wenn beide Chassis denselben Namen haben, ändern Sie den Namen in einem Chassis mithilfe der folgenden Befehle:

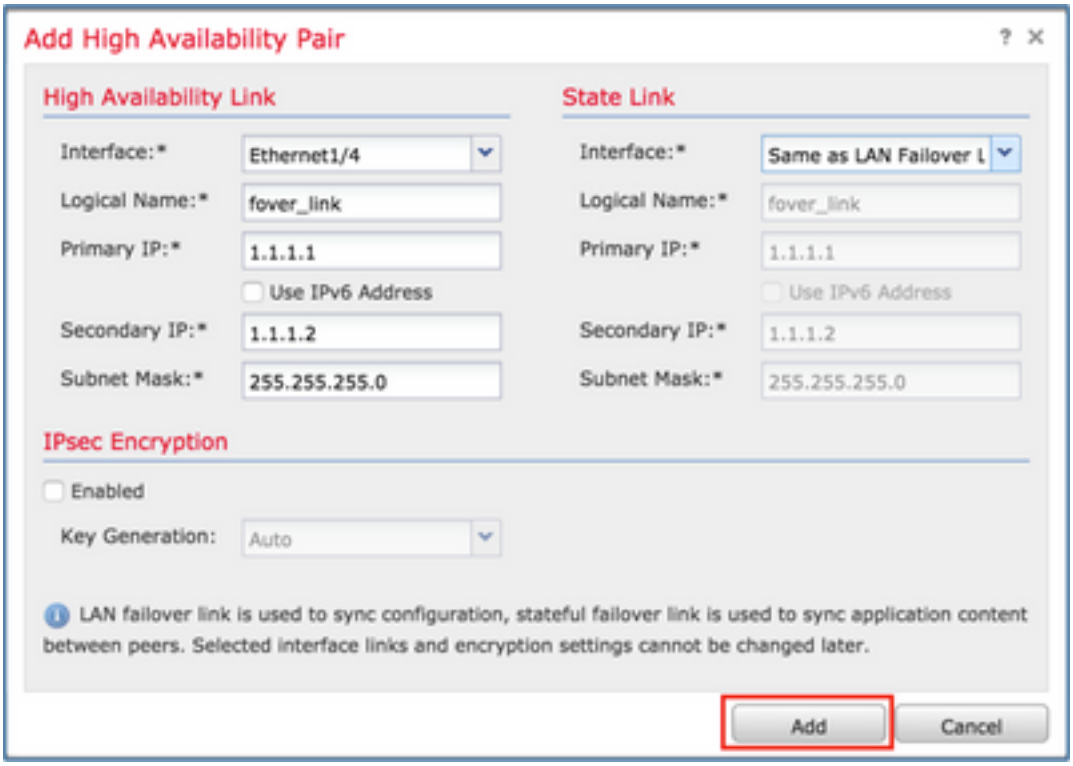
```
KSEC-FPR9K-1-A# scope system
KSEC-FPR9K-1-A /system # set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* # commit-buffer
FPR9K-1-A /system # exit
FPR9K-1new-A#
```

Nachdem Sie den Chassis-Namen geändert haben, heben Sie die FTD-Registrierung beim FMC auf, und registrieren Sie sie erneut. Fahren Sie dann mit der HA Pair-Erstellung fort.

Schritt 3: Konfigurieren Sie HA, und geben Sie die Einstellungen für die Links an.

In Ihrem Fall hat der Status-Link die gleichen Einstellungen wie der Hochverfügbarkeits-Link.

Wählen Sie **Add (Hinzufügen**) aus, und warten Sie einige Minuten, bis das HA-Paar wie im Image dargestellt bereitgestellt wird.

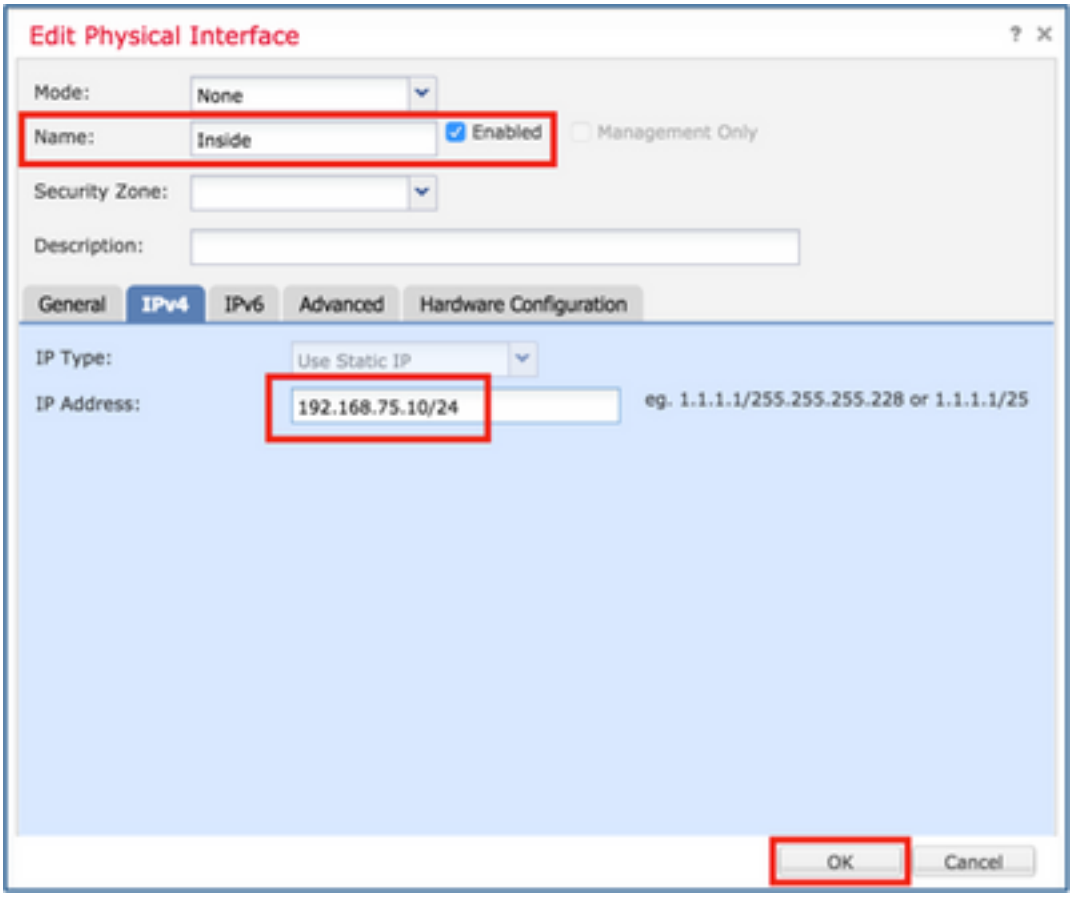


Schritt 4: Konfigurieren der Datenschnittstellen (primäre und Standby-IP-Adressen)

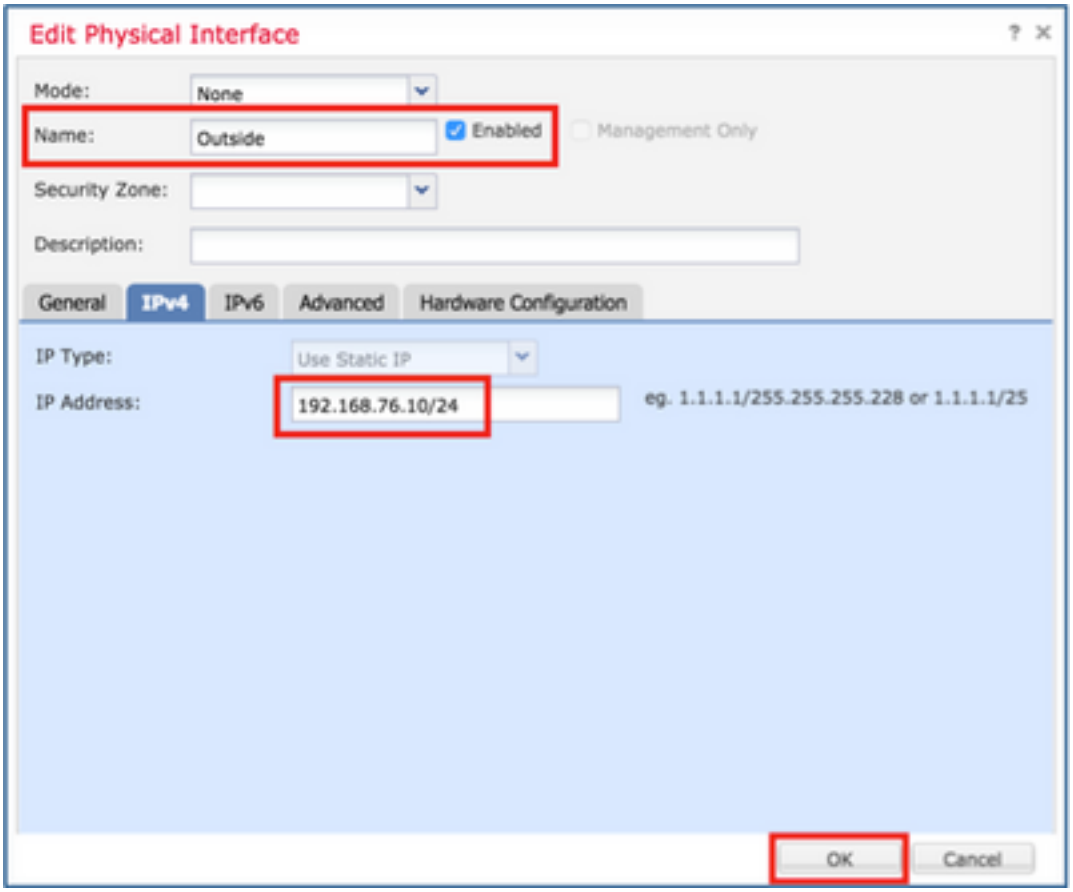
Wählen Sie in der FMC-GUI die Option HA **Edit** wie im Bild dargestellt aus.

Schritt 5: Konfigurieren Sie die Schnittstelleneinstellungen wie in den Bildern dargestellt.

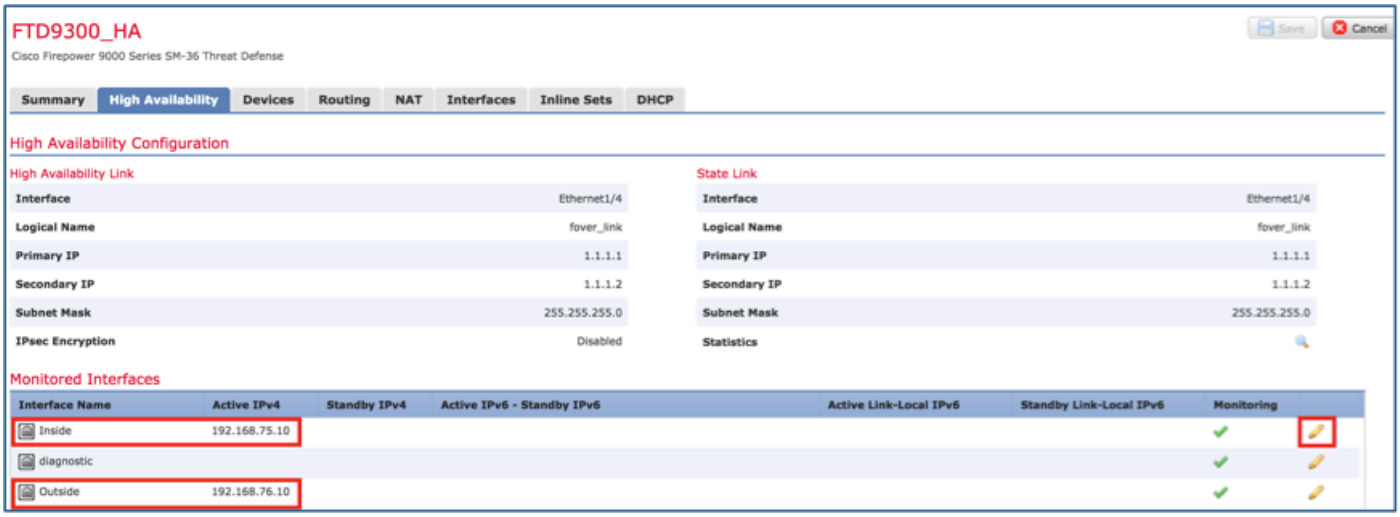
Ethernet 1/5-Schnittstelle.



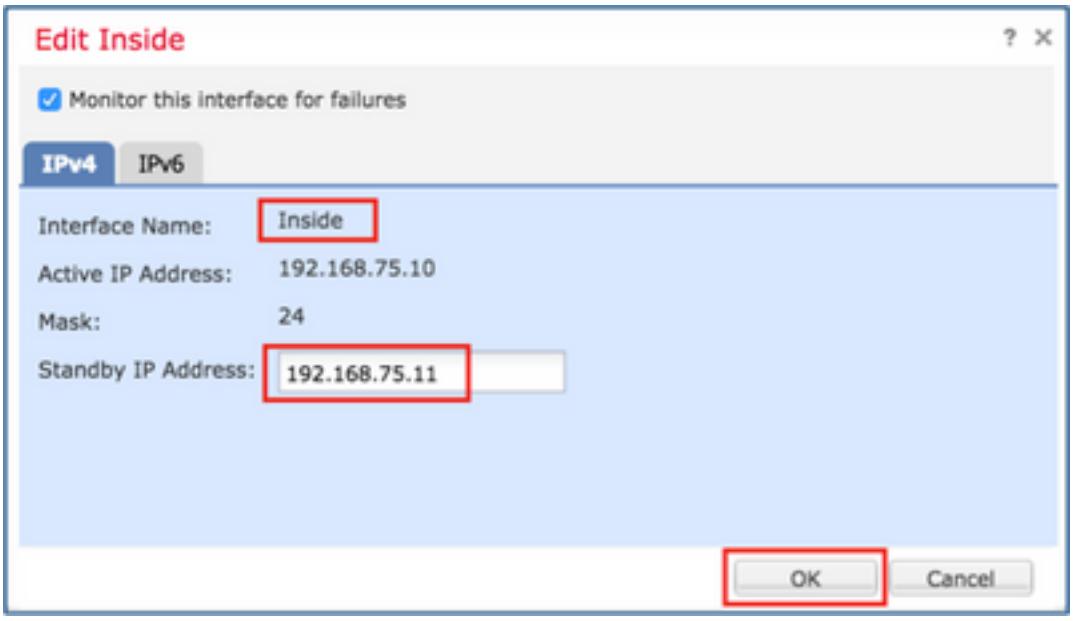
Ethernet 1/6-Schnittstelle.



Schritt 6: Navigieren Sie zu **Hochverfügbarkeit,** und wählen Sie Schnittstellenname **Bearbeiten** aus, um die Standby-IP-Adressen wie im Bild dargestellt hinzuzufügen.

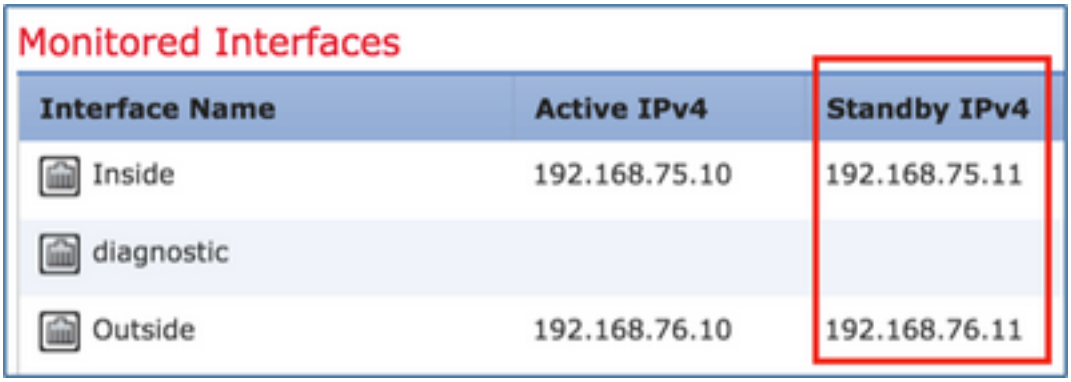


Schritt 7. Für die interne Schnittstelle wie im Bild dargestellt.

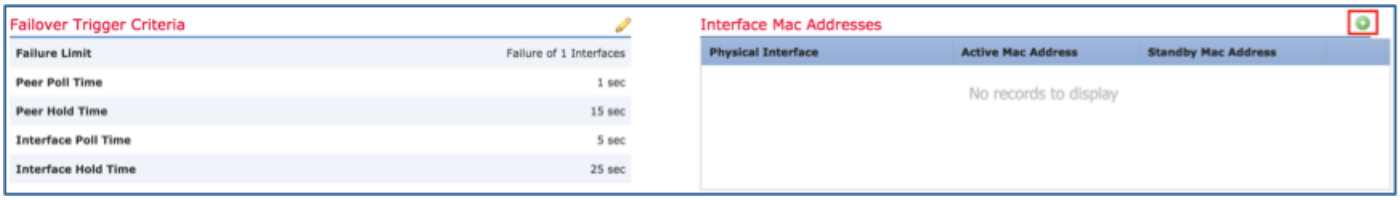


Schritt 8: Führen Sie den gleichen Vorgang für die externe Schnittstelle aus.

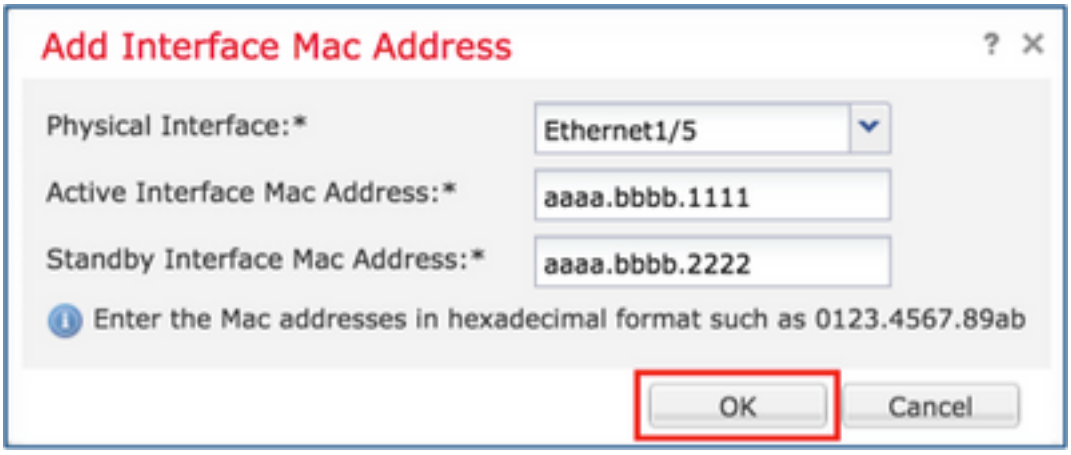
Schritt 9: Überprüfen Sie das Ergebnis wie im Bild dargestellt.



Schritt 10: Bleiben Sie auf der Registerkarte für hohe Verfügbarkeit, und konfigurieren Sie virtuelle MAC-Adressen wie im Bild dargestellt.



Schritt 11. Für die interne Schnittstelle ist wie im Bild dargestellt.



Schritt 12: Führen Sie den gleichen Vorgang für die externe Schnittstelle aus.

Schritt 13: Überprüfen Sie das Ergebnis wie im Bild dargestellt.

Schritt 14: Wählen Sie nach der Konfiguration der Änderungen **Speichern** und Bereitstellen.

Aufgabe 3: Überprüfen von FTD HA und Lizenz

Aufgabenanforderung:

Überprüfen Sie die FTD HA-Einstellungen und aktivierten Lizenzen über die FMC-GUI und die FTD CLI.

Lösung:

Schritt 1: Navigieren Sie zu **Übersicht**, und überprüfen Sie die HA-Einstellungen und aktivierten Lizenzen, wie im Bild dargestellt.

Schritt 2: Führen Sie in der FTD CLISH CLI die folgenden Befehle aus:

```
> 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
General417        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

>
```

Schritt 3: Führen Sie die gleichen Schritte auf dem sekundären Gerät durch.

Schritt 4: Führen Sie den Befehl **show failover state** in der LINA-CLI aus:

```
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#
```

Schritt 5: Überprüfen der Konfiguration der primären Einheit (LINA CLI):

```
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#
```

Aufgabe 4: Failover-Rollen wechseln

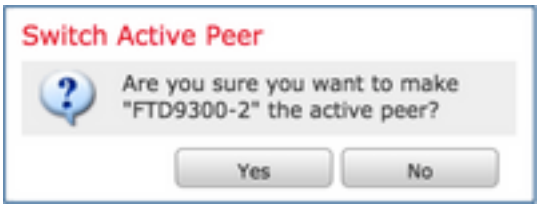
Aufgabenanforderung:

Switching der Failover-Rollen vom FMC von Primary/Active, Secondary/Standby zu Primary/Standby, Secondary/Active

Lösung:

Schritt 1: Wählen Sie das Symbol, wie im Bild dargestellt.

Schritt 2: Bestätigen Sie die Aktion im Popup-Fenster, wie im Bild dargestellt.



Schritt 3: Überprüfen Sie das Ergebnis wie im Bild dargestellt.

In der LINA-CLI können Sie sehen, dass der Befehl **no failover active** auf der primären/aktiven Einheit ausgeführt wurde:

```
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 failover active'
```

Sie können dies auch in der Befehlsausgabe **show failover history** überprüfen:

```
firepower# show failover history
==========================================================================
```

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

Schritt 4: Aktivieren Sie die primäre Einheit nach der Überprüfung wieder.

Aufgabe 5: Aufbrechen des HA-Paars

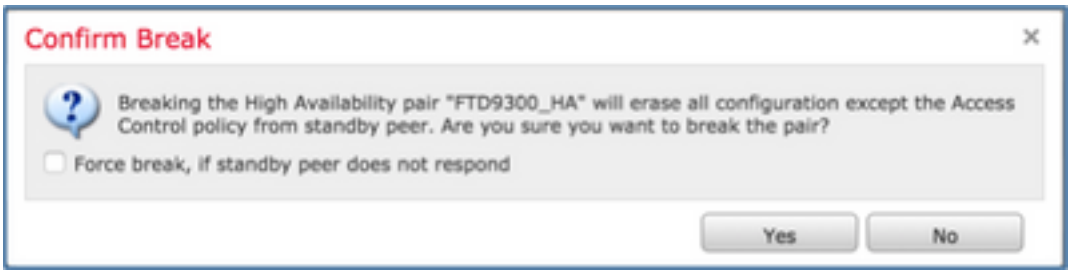
Aufgabenanforderung:

Brechen Sie das Failover-Paar vom FMC ab.

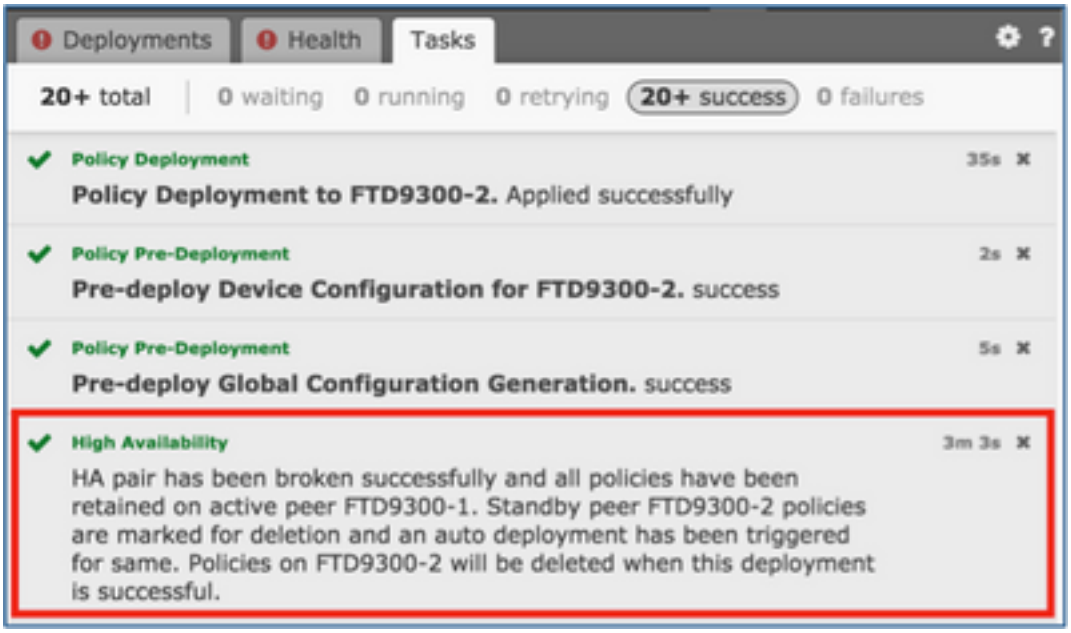
Lösung:

Schritt 1: Wählen Sie das Symbol, wie im Bild dargestellt.

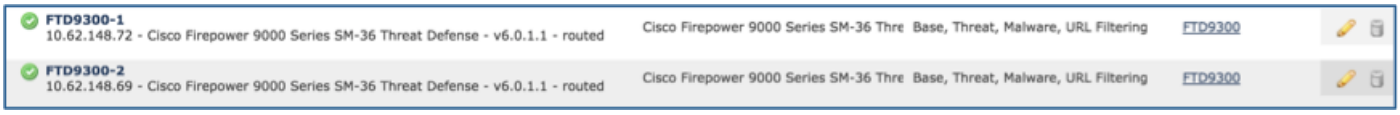
Schritt 2: Überprüfen Sie die Benachrichtigung wie im Bild dargestellt.



Schritt 3. Beachten Sie die Nachricht wie im Bild dargestellt.



Schritt 4: Überprüfen Sie das Ergebnis der FMC-GUI wie im Bild dargestellt.



show running-config auf der primären Einheit vor und nach der HA-Unterbrechung:

Vor HA-Pause

```
firepower# sh run
: Saved
:
: Serial Number: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB RAM, CPU
Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 10.10.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744:
ACCESS POLICY: FTD9300 - Mandatory/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:
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268441600:
L4 RULE: DEFAULT ACTION RULE
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
!
no pager
logging enable
logging timestamp
logging standby
```

Nach HA-Pause

```
firepower# sh run
: Saved
:
: Serial Number: FLM19267A63
: Hardware:   FPR9K-SM-36, 135839 MB RAM, C
Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
:
NGFW Version 10.10.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet1/2
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
no nameif
no security-level
no ip address
!
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
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icm
any rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip a
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
!
no pager
logging enable
```

logging buffer-size 100000
logging buffered debugging
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
mtu diagnostic 1500
mtu Inside 1500
mtu Outside 1500
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
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout 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
aaa proxy-limit disable
no snmp-server location
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 timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
router-alert action allow
policy-map global_policy
class inspection_default
inspect dns preset_dns_map

logging timestamp
logging standby
logging buffer-size 100000
logging buffered debugging
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
mtu diagnostic 1500
mtu Inside 1500
mtu Outside 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:0
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0
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
absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infin
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
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

inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
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
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:933c594fc0264082edc0f24bad358031
: end
firepower#

inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_M
class class-default
set connection advanced-options
UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/
EService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic month
subscribe-to-alert-group configuration periodic mo
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:fb6f5c369dee730b9125650517
9
: end
firepower#

show running-config auf der sekundären Einheit vor und nach der HA-Unterbrechung, wie in der Tabelle hier gezeigt.

Vor HA-Pause	Nach HA-Pause
firepower# sh run : Saved : : Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores) : NGFW Version 10.10.1.1 ! hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet1/2 management-only nameif diagnostic security-level 0 no ip address ! **interface Ethernet1/4** **description LAN/STATE Failover Interface** **!**	firepower# sh run : Saved : : Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, C Xeon E5 series 2294 MHz, 2 CPUs (72 cores) : NGFW Version 10.10.1.1 ! hostname firepower enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet1/2 management-only nameif diagnostic security-level 0 no ip address ! **interface Ethernet1/4** **shutdown** **no nameif**

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
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/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: ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE
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
!
no pager
logging enable
logging timestamp
logging standby
logging buffer-size 100000
logging buffered debugging
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
mtu diagnostic 1500
mtu Inside 1500
mtu Outside 1500
failover
failover lan unit secondary
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
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout 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

no security-level
no ip address
!
interface Ethernet1/5
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1/6
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icm
any rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip a
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
!
no pager
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 diagnostic 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:0
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0
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 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
user-identity default-domain LOCAL
aaa proxy-limit disable
no snmp-server location
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 timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
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
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
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
```

```
timeout sip-provisional-media 0:02:00 uauth 0:05
absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infin
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
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
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_M
class class-default
set connection advanced-options
UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/
EService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
```

destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84
: end
firepower#

subscribe-to-alert-group inventory periodic month
subscribe-to-alert-group configuration periodic mo
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:08ed87194e9f5cd9149fab3c0e93
: end
firepower#

Wichtigste Punkte für die HA-Pause:

Haupteinheit	Sekundäreinheit
Alle Failover-Konfigurationen werden entfernt. Standby-IP-Adressen verbleiben	Alle Konfigurationen werden entfernt.

Schritt 5. Nachdem Sie diese Aufgabe abgeschlossen haben, erstellen Sie das HA-Paar neu.

Aufgabe 6. HA-Paar deaktivieren

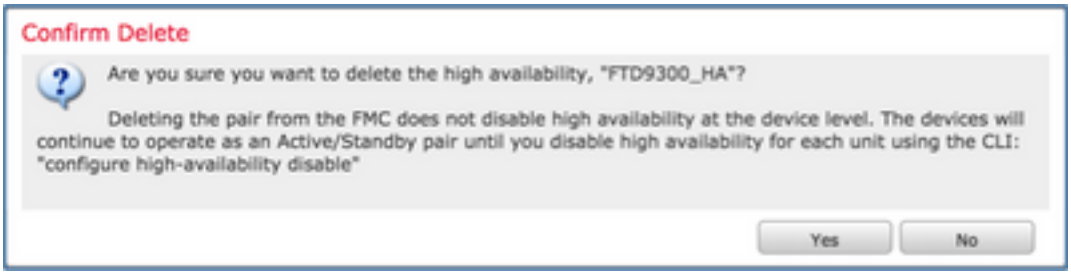
Aufgabenanforderung:

Deaktivieren Sie das Failover-Paar vom FMC aus.

Lösung:

Schritt 1: Wählen Sie das Symbol, wie im Bild dargestellt.

Schritt 2: Überprüfen Sie die Benachrichtigung, und bestätigen Sie, wie im Bild dargestellt.



Schritt 3: Nach dem Löschen der HA werden beide Geräte vom FMC abgemeldet (entfernt).

show running-config result aus der LINA-CLI wird in der folgenden Tabelle dargestellt:

Haupteinheit	Sekundäreinheit
firepower# sh run : Saved : : Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores) :	firepower# sh run : Saved : : Serial Number: FLM19206H7T : Hardware: FPR9K-SM-36, 135841 MB RAM, C Xeon E5 series 2294 MHz, 2 CPUs (72 cores) :

```
NGFW Version 10.10.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 268447744:
ACCESS POLICY: FTD9300 - Mandatory/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:
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268441600:
L4 RULE: DEFAULT ACTION RULE
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
!
no pager
logging enable
logging timestamp
logging standby
logging buffer-size 100000
logging buffered debugging
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
mtu diagnostic 1500
mtu Inside 1500
mtu Outside 1500
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
```

```
NGFW Version 10.10.1.1
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 standb
192.168.75.11
!
interface Ethernet1/6
nameif Outside
security-level 0
ip address 192.168.76.10 255.255.255.0 standb
192.168.76.11
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: Allow_ICMP
access-list CSM_FW_ACL_ advanced permit icm
any rule-id 268447744 event-log both
access-list CSM_FW_ACL_ remark rule-id 26844
ACCESS POLICY: FTD9300 - Default/1
access-list CSM_FW_ACL_ remark rule-id 26844
L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip a
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
!
no pager
logging enable
logging timestamp
logging standby
logging buffer-size 100000
logging buffered debugging
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
mtu diagnostic 1500
mtu Inside 1500
mtu Outside 1500
failover
failover lan unit secondary
failover lan interface fover_link Ethernet1/4
failover replication http
failover mac address Ethernet1/5 aaaa.bbbb.1
aaaa.bbbb.2222
failover mac address Ethernet1/6 aaaa.bbbb.3
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
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout 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
aaa proxy-limit disable
no snmp-server location
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 timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
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
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc
inspect ip-options UM_STATIC_IP_OPTIONS_MAP

failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1
255.255.255.0 standby 10.10.1.2
icmp unreachable rate-limit 1 -size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group CSM_FW_ACL_ global
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:0
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0
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
absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infin
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
parameters
eool action allow
nop action allow
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
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect dcerpc

class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:933c594fc0264082edc0f24bad358031
: end
firepower#

inspect ip-options UM_STATIC_IP_OPTIONS_M
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic month
subscribe-to-alert-group configuration periodic mo
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c64
: end
firepower#

Schritt 4: Beide FTD-Geräte wurden vom FMC abgemeldet:

```
> show managers
No managers configured.
```

Wichtigste Punkte für die Option "HA deaktivieren" in FMC:

Haupteinheit	Sekundäreinheit
Das Gerät wird aus dem FMC entfernt.	Das Gerät wird aus dem FMC entfernt.
Keine Konfiguration wird aus dem FTD-Gerät entfernt	Keine Konfiguration wird aus dem FTD-Gerät entfe

Schritt 5: Führen Sie diesen Befehl aus, um die Failover-Konfiguration von den FTD-Geräten zu entfernen:

```
> 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.
```

Anmerkung: Sie müssen den Befehl auf beiden Geräten ausführen

Ergebnis:

Haupteinheit	Sekundäreinheit
>**show failover**	>**show failover**
Failover Off	**Failover Off (pseudo-Standby)**
Failover unit Secondary	Failover unit Secondary
Failover LAN Interface: not Configured	Failover LAN Interface: FOVER Ethernet1/3.205
Reconnect timeout 0:00:00	Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds	Unit Poll frequency 1 seconds, holdtime 15 secon
Interface Poll frequency 5 seconds, holdtime 25 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
>
```

Primary

```
firepower# show run
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
interface GigabitEthernet1/1
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
ip address 10.1.1.1 255.255.255.0   <-- standby IP
was removed
!
interface GigabitEthernet1/2
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
ip address 192.168.1.1 255.255.255.0   <-- standby
IP was removed
!
interface GigabitEthernet1/3
 description LAN Failover Interface
!
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 nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
```

```
Interface Policy 1
Monitored Interfaces 0 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

Sekundär

```
firepower# show run
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 description LAN Failover Interface
!
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 nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 no ip address
!
ftp mode passive
```

```
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 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
access-list CSM_FW_ACL_ remark rule-id 9998:
RULE: DEFAULT TUNNEL ACTION RULE
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:
ACCESS POLICY: FTD_HA - Default/1
access-list CSM_FW_ACL_ remark rule-id 268435456:
L4 RULE: DEFAULT ACTION RULE
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
!
no pager
logging enable
logging timestamp
logging buffered debugging
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 710005
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 outside 1500
mtu inside 1500
mtu diagnostic 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
access-group CSM_FW_ACL_ global
timeout 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
```

```
ngips conn-match vlan-id
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:
RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipin
any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41
any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre
any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp
any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 26843
ACCESS POLICY: FTD_HA - Default/1
access-list CSM_FW_ACL_ remark rule-id 26843
L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip a
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
!
no pager
logging enable
logging timestamp
logging buffered debugging
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 710005
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 outside 1500
mtu inside 1500
mtu diagnostic 1500
no failover
failover lan unit secondary
failover lan interface FOVER GigabitEthernet1
failover replication http
failover link STATE GigabitEthernet1/4
failover interface ip FOVER 10.10.1.1 255.255.2
standby 10.10.1.2
failover interface ip STATE 10.10.2.1 255.255.2
standby 10.10.2.2
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
access-group CSM_FW_ACL_ global
timeout xlate 3:00:00
```

```
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 192.168.1.100 community
***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  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
  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
call-home
 profile CiscoTAC-1
  no active
  destination address http
```

```
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:0
sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:0
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
absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
user-identity default-domain LOCAL
aaa proxy-limit disable
snmp-server host outside 192.168.1.100 commun
***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
service sw-reset-button
crypto ipsec security-association pmtu-aging infin
crypto ca trustpool policy
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options
UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  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
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ip-options UM_STATIC_IP_OPTIONS_M
 class class-default
  set connection advanced-options
UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
```

https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:768a03e90b9d3539773b9d7af66b3452

call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic mont
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:ac9b8f401e18491fee653f4cfe0c

Wichtigste Punkte, die bei der FTD-CLI zum Deaktivieren von HA zu beachten sind:

Haupteinheit	Sekundäreinheit
Failover-Konfiguration und Standby-IPs werden entfernt	• Schnittstellenkonfigurationen werden entfernt • Das Gerät wechselt in den Pseudo-Standby-Modus.

Schritt 6: Registrieren Sie die Geräte nach Abschluss der Aufgabe beim FMC, und aktivieren Sie das HA-Paar.

Aufgabe 7: HA aussetzen

Aufgabenanforderung:

Hochverfügbarkeit aus der FTD CLISH CLI aussetzen

Lösung:

Schritt 1: Führen Sie auf dem primären FTD den Befehl aus, und bestätigen Sie ihn (geben Sie **YES ein**).

```
> 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 abort: YES
Successfully suspended high-availability.
```

Schritt 2. Überprüfen Sie die Änderungen an der primären Einheit:

```
> 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
```

Schritt 3. Ergebnis auf Sekundäreinheit:

```
> **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
```

Schritt 4: Hochverfügbarkeit auf der primären Einheit fortsetzen:

```
> **configure high-availability resume**
Successfully resumed high-availablity.

> .

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

>

> **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
```

Schritt 5. Das Ergebnis auf der sekundären Einheit, nachdem Sie wieder HA:

```
> ..

**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.

>

> **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
>
```

Häufig gestellte Fragen

Wenn die Konfiguration repliziert wird, wird sie sofort (zeilenweise) oder am Ende der Replikation gespeichert?

Am Ende der Replikation. Der Beweis befindet sich am Ende der **debug fover sync**-Befehlsausgabe, die die config/command-Replikation anzeigt:

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578:
L7 RULE: ACP_Rule_500
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp
object-group group_10 eq 48894 object-group group_10 eq 23470 vlan eq 1392 rule-id 268442578
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078:
ACCESS POLICY: mzafeiro_500 - Default
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078:
L4 RULE: DEFAULT ACTION RULE
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group
group_2 eq 32881 object-group group_433 eq 39084 vlan eq 1693 rule-id 268442076
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id
268442077: ACCESS POLICY: mzafeiro_ACP1500 - Mandatory
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id
268442077: L7 RULE: ACP_Rule_1500
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group
group_6 eq 8988 object-group group_311 eq 32433 vlan eq 619 rule-id 268442077
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id
268440577: ACCESS POLICY: mzafeiro_ACP1500 - Default
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id
268440577: L4 RULE: DEFAULT ACTION RULE
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id
268442078 event-log flow-start
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 <--
```

Was passiert, wenn sich eine Einheit im Pseudo-Standby-Status befindet (Failover deaktiviert) und Sie sie dann neu laden, während die andere Einheit Failover aktiviert hat und aktiv ist?

Sie landen in einem **Aktiv/Aktiv**-Szenario (obwohl technisch ein Aktiv/Failover-Aus ist). Nach dem Einschalten des Geräts ist der Failover deaktiviert, das Gerät verwendet jedoch die gleichen IPs wie das aktive Gerät. Im Endeffekt haben Sie also:

- Einheit 1: Aktiv
- Einheit 2: Failover ist deaktiviert. Die Einheit verwendet dieselben Daten-IPs wie Einheit 1, jedoch unterschiedliche MAC-Adressen.

Was passiert mit der Failover-Konfiguration, wenn Sie den Failover manuell deaktivieren (Hochverfügbarkeits-Suspend konfigurieren) und dann das Gerät neu laden?

Wenn Sie den Failover deaktivieren, handelt es sich nicht um eine permanente Änderung (wird nicht in der Startkonfiguration gespeichert, es sei denn, Sie möchten dies ausdrücklich tun). Beachten Sie, dass Sie das Gerät auf zwei verschiedene Arten neu starten bzw. neu laden können. Bei der zweiten Möglichkeit müssen Sie vorsichtig sein:

Fall 1: Neustart von CLISH

Der Neustart von CLISH fordert keine Bestätigung. Die Konfigurationsänderung wird daher nicht in der Startkonfiguration gespeichert:

```
> 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 abort: YES
Successfully suspended high-availability.
```

Bei der aktuellen Konfiguration ist der Failover deaktiviert. In diesem Fall war das Gerät Standby und wechselte erwartungsgemäß in den Pseudo-Standby-Status, um ein Active/Active-Szenario zu vermeiden:

```
firepower# show failover | include Failover
Failover Off (pseudo-Standby)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Für die Startkonfiguration ist Failover weiterhin aktiviert:

```
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 *****
```

Starten Sie das Gerät über CLISH neu (**reboot**-Befehl):

```
> 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 ...
```

Wenn die Einheit eingeschaltet ist und Failover aktiviert ist, beginnt das Gerät mit der Failover-Aushandlungsphase und versucht, den Remote-Peer zu erkennen:

```
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
```

Fall 2: Neustart von LINA CLI
Reboot from LINA (**reload-**Befehl) fordert Bestätigung. Wenn Sie [Y]es auswählen, wird die Konfigurationsänderung in der Startkonfiguration gespeichert:

```
firepower# reload
System config 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 *****
```

Sobald das Gerät eingeschaltet ist, wird der Failover deaktiviert:

```
firepower# show failover | include Fail
Failover Off
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

> **Anmerkung:** Um dieses Szenario zu vermeiden, stellen Sie sicher, dass Sie die Änderungen an der Startkonfiguration nicht speichern, wenn Sie dazu aufgefordert werden.

Zugehörige Informationen

- Alle Versionen des Konfigurationsleitfadens für das Cisco FirePOWER Management Center finden Sie hier.

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Alle Versionen der Konfigurationsanleitungen für FXOS Chassis Manager und CLI finden Sie hier.

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfId-121950

- Das Cisco Global Technical Assistance Center (TAC) empfiehlt dringend diesen Leitfaden, um detailliertes praktisches Wissen über die Sicherheitstechnologien der nächsten Generation

von Cisco FirePOWER zu erhalten:
http://www.ciscopress.com/title/9781587144806

- Für alle technischen Hinweise zu Konfiguration und Fehlerbehebung in Bezug auf die FirePOWER-Technologien
https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.