Konfigurieren von ASA Active/Active Failover in Firepower der Serie 4100

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Aktiv/Aktiv-Failover in der Cisco FirePOWER 4145 NGFW-Appliance konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Aktiv/Standby-Failover in der Cisco Adaptive Security Appliance (ASA).

Verwendete Komponenten

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

- Cisco FirePOWER 4145 NGFW-Appliance (ASA) 9.18(3)56
- FirePOWER Extensible Operating System (FXOS) 2.12(0.498)
- Windows 10

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 kennen.

Hintergrundinformationen

Active/Active-Failover ist nur für Sicherheits-Appliances verfügbar, die im Multi-Context-Modus ausgeführt werden. In diesem Modus ist die ASA logisch in mehrere virtuelle Geräte unterteilt, die als Kontexte bezeichnet werden. Jeder Kontext agiert als unabhängiges Gerät mit eigenen Sicherheitsrichtlinien, Schnittstellen und Administratoren.

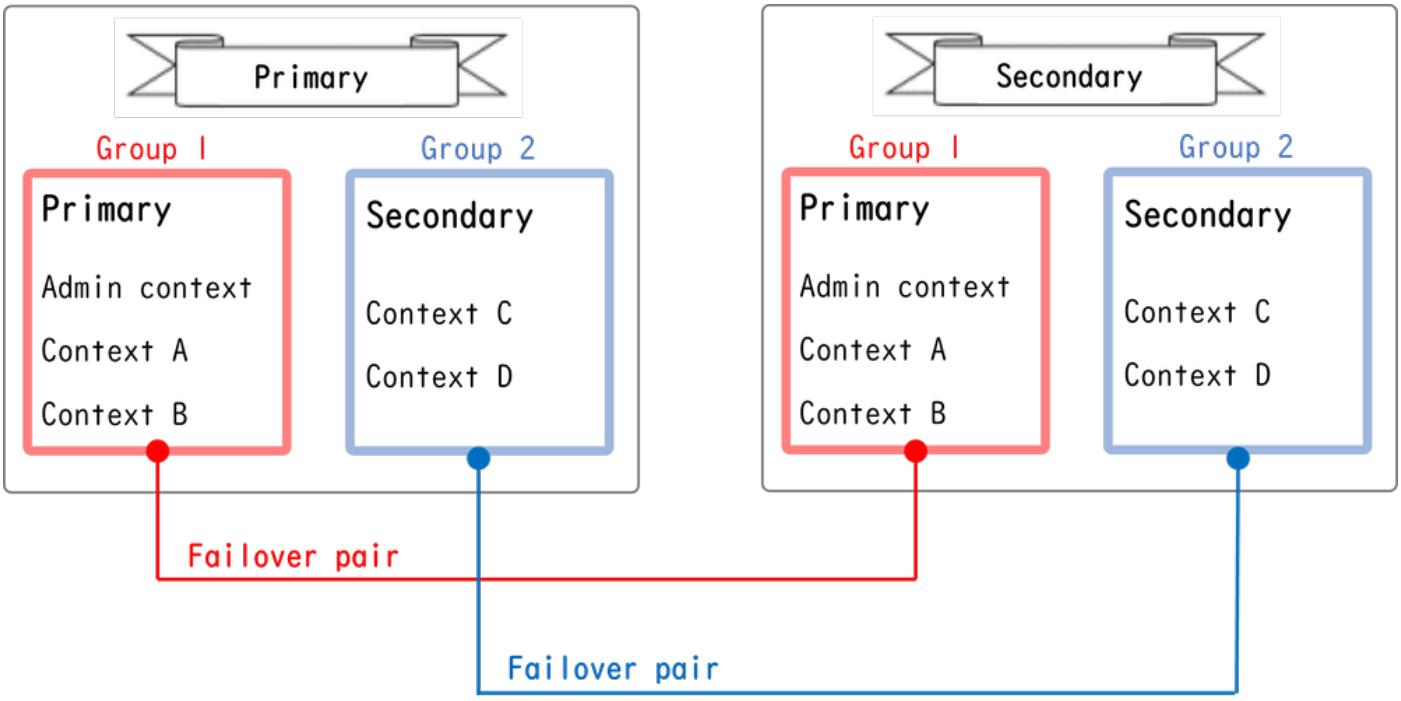
Das Aktiv/Aktiv-Failover ist eine Funktion der Adaptive Security Appliance (ASA), mit der zwei Firepower-Geräte den Datenverkehr gleichzeitig weiterleiten können. Diese Konfiguration wird in der Regel für ein Load Balancing-Szenario verwendet, in dem Sie den Datenverkehr zur Maximierung des Durchsatzes auf zwei Geräte aufteilen möchten. Darüber hinaus wird sie für Redundanzzwecke genutzt. Fällt eine ASA aus, kann die andere übernehmen, ohne dass es zu Serviceunterbrechungen kommt.

Mechanismus für ASA Aktiv/Aktiv-Failover

Jeder Kontext in Active/Active Failover wird manuell entweder Gruppe 1 oder Gruppe 2 zugewiesen. Der Admin-Kontext wird standardmäßig Gruppe 1 zugewiesen. Dieselbe Gruppe (Gruppe1 oder Gruppe2) in den beiden Chassis (Einheiten) bildet ein Failover-Paar, das die Redundanzfunktion übernimmt. Das Verhalten jedes Failover-Paars entspricht im Wesentlichen dem eines Aktiv/Standby-Failovers. Weitere Informationen zu Aktiv/Standby-Failover finden Sie unter Aktiv/Standby-Failover konfigurieren. Beim Aktiv/Aktiv-Failover hat jede Gruppe neben der Rolle (primär oder sekundär) jedes Chassis auch eine Rolle (primär oder sekundär). Diese Rollen

werden vom Benutzer manuell voreingestellt und dienen dazu, den HA-Status (High Availability) (Aktiv oder Standby) für jede Failover-Gruppe zu bestimmen.

Der Admin-Kontext ist ein spezieller Kontext, der die grundlegende Chassis-Management-Verbindung (z. B. SSH) verarbeitet. Dies ist ein Abbild des Aktiv/Aktiv-Failovers.



Failover-Paar in Aktiv/Aktiv-Failover

Datenverkehrsfluss

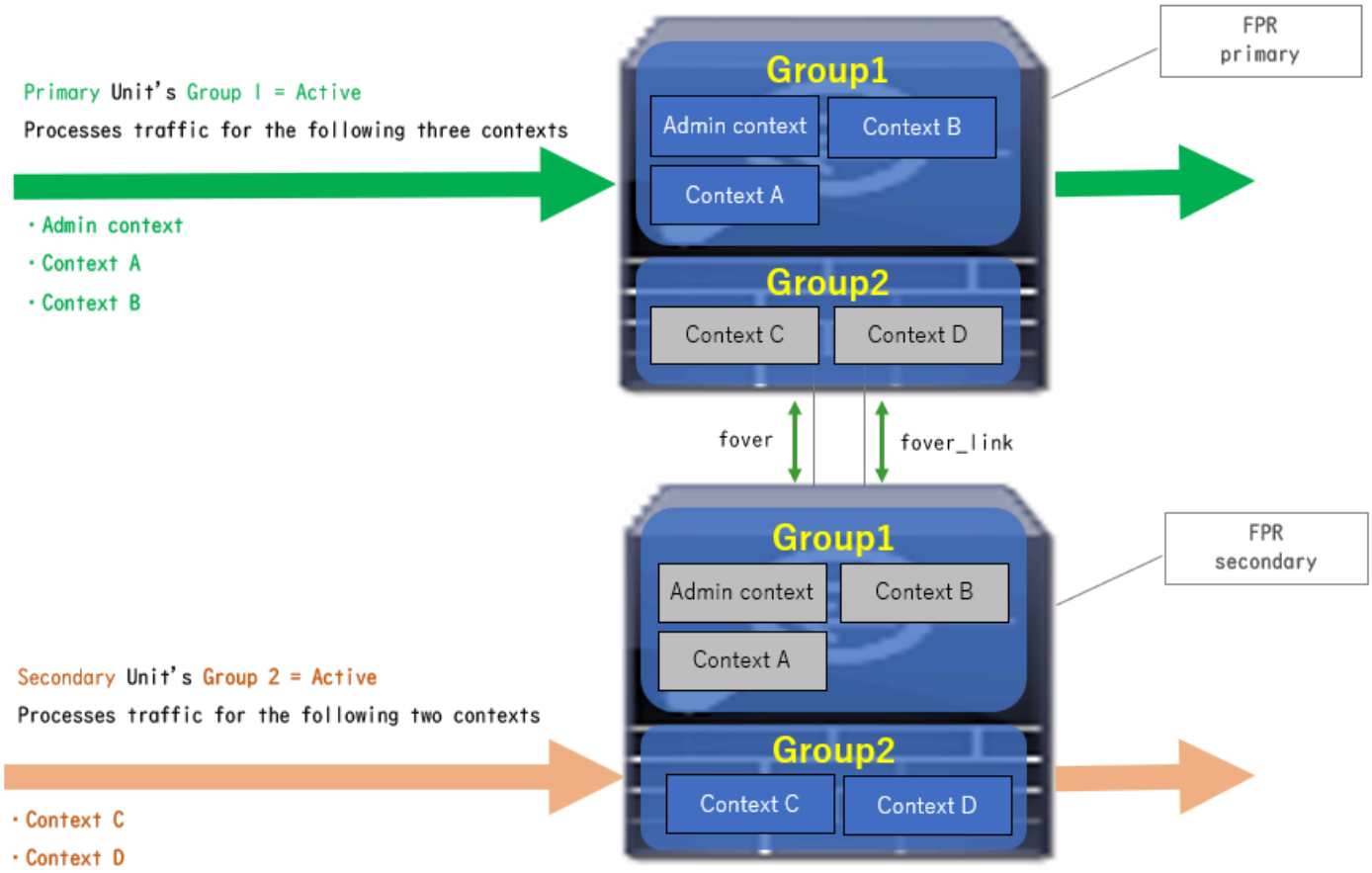
Bei einem Aktiv/Aktiv-Failover kann der Datenverkehr nach den verschiedenen Mustern verarbeitet werden, wie im nächsten Bild gezeigt.

Group	Primary Unit	Secondary Unit	
Group 1	Active	Standby	Both of ASAs process traffic simultaneously
Group 2	Standby	Active	
Group 1	Active	Standby	Only the Primary Unit processes traffic
Group 2	Active	Standby	
Group 1	Standby	Active	Both of ASAs process traffic simultaneously
Group 2	Active	Standby	
Group 1	Standby	Active	Only the Secondary Unit processes traffic
Group 2	Standby	Active	

Datenverkehrsfluss

Verkehrsflussbedingung 1

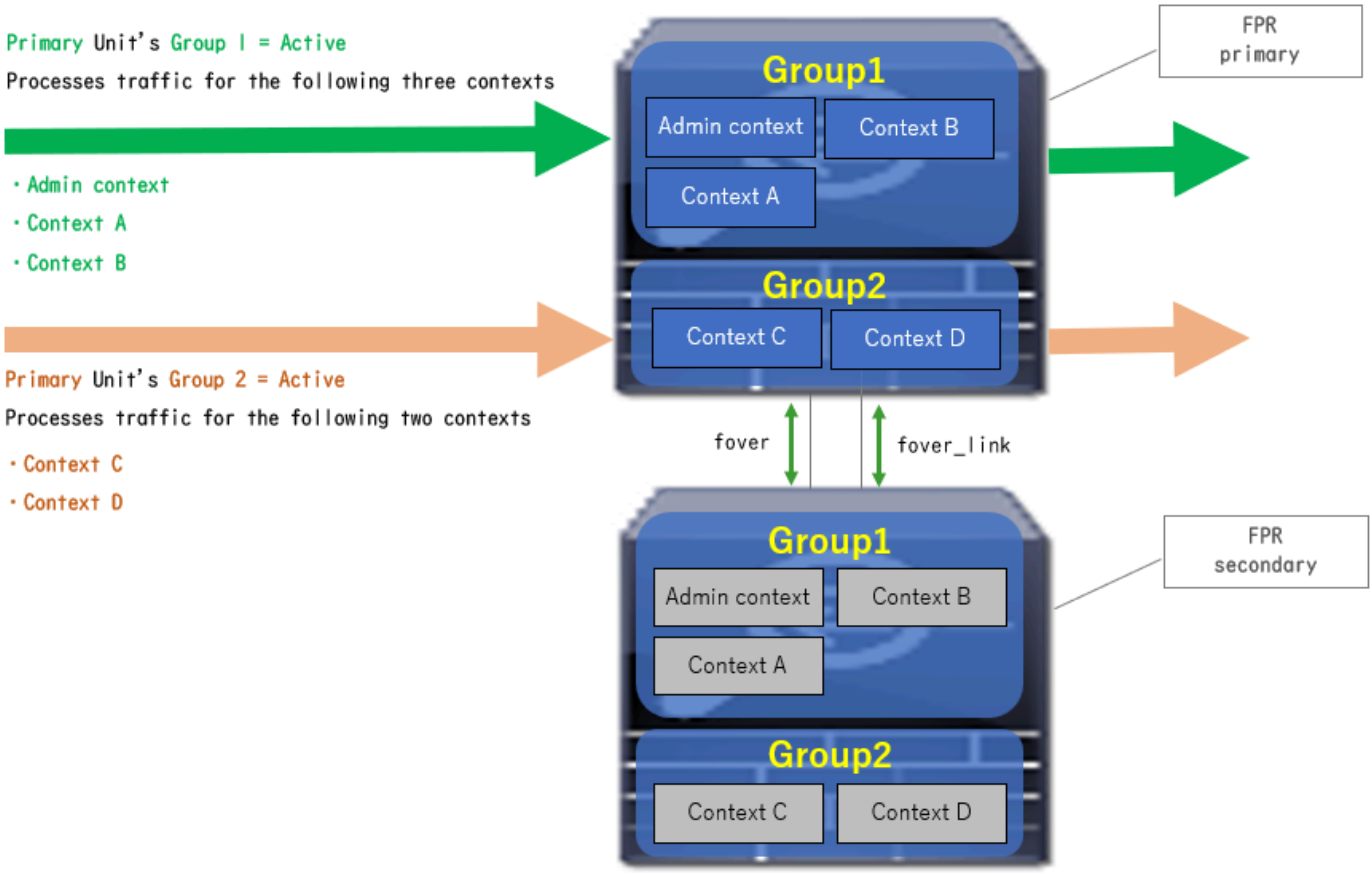
- Primäre Einheit: Gruppe 1 = aktiv, Gruppe 2 = Standby
- Sekundäreinheit: Gruppe 1 = Standby, Gruppe 2 = Aktiv



Verkehrsflussbedingung 1

Verkehrsfluss - Bedingung 2

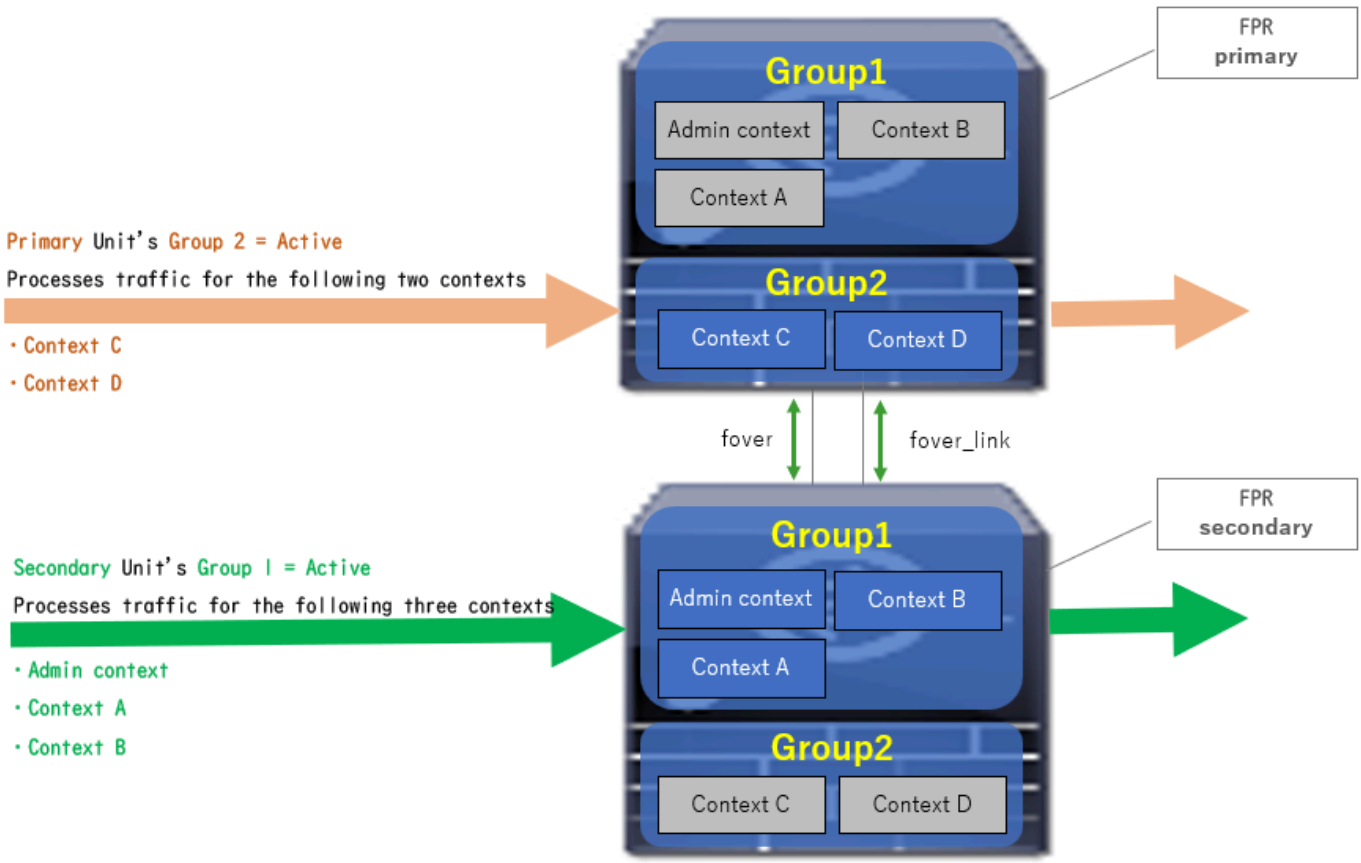
- Primäre Einheit: Gruppe 1 = aktiv, Gruppe 2 = aktiv
- Sekundäreinheit: Gruppe 1 = Standby, Gruppe 2 = Standby



Verkehrsfluss - Bedingung 2

Verkehrsfluss - Bedingung 3

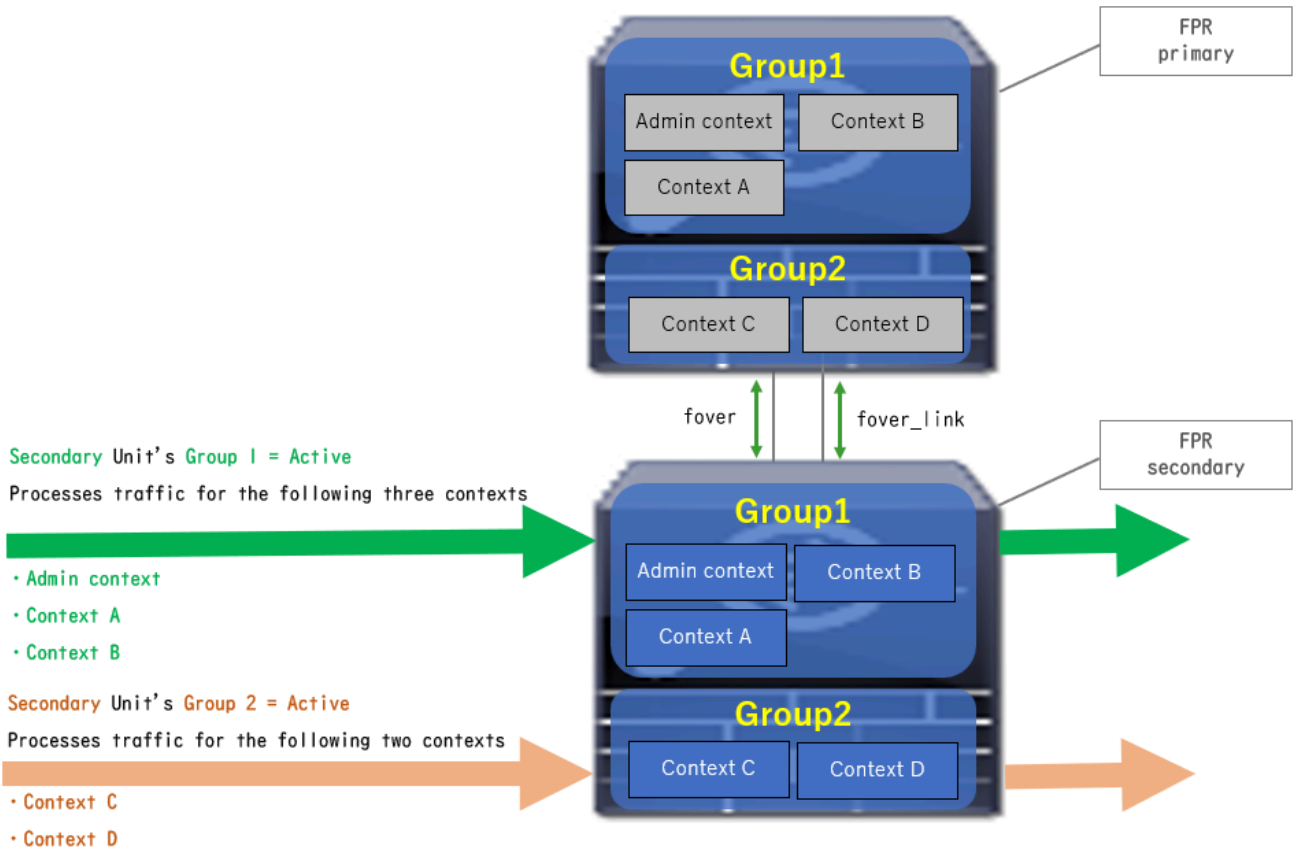
- Primäreinheit: Gruppe 1 = Standby, Gruppe 2 = Aktiv
- Sekundäreinheit: Gruppe 1 = aktiv, Gruppe 2 = Standby



Verkehrsfluss - Bedingung 3

Verkehrsfluss - Bedingung 4

- Primäre Einheit: Gruppe 1 = Standby, Gruppe 2 = Standby
- Sekundäreinheit: Gruppe 1 = aktiv, Gruppe 2 = aktiv



Verkehrsfluss - Bedingung 4

Auswahlregeln für Aktiv/Standby

Bei Aktiv/Aktiv-Failover wird der Status (aktiv/Standby) jeder Gruppe durch die folgenden Regeln bestimmt:

- Angenommen, zwei Geräte werden fast gleichzeitig hochgefahren, dann wird eine der Einheiten (Primär oder Sekundär) zuerst aktiv.
- Nach Ablauf der Freischaltungszeit wird die Gruppe aktiviert, die dieselbe Rolle im Chassis und in der Gruppe hat.
- Wenn ein Failover-Ereignis eintritt (z. B. Schnittstelle DOWN), ändert sich der Status der Gruppe auf die gleiche Weise wie bei Active/Standby-Failover.
- Nach manuellem Failover funktioniert die Freischaltungszeit nicht mehr.

Dies ist ein Beispiel für die Statusänderung.

- Beide Geräte werden fast gleichzeitig hochgefahren. Status A →
- Vorbelegungszeit verstrichen. Status B →
- Primärer Geräteausfall (Failover wird ausgelöst). Status C →
- Die Vorbelegungszeit ist seit der Wiederherstellung des primären Geräts nach einem Fehler verstrichen. Status D →
- Manuelles Auslösen des Failovers. Status E

Weitere Informationen zu Failover-Auslösern und zur Integritätsüberwachung finden Sie unter Failover Events (Failover-Ereignisse).

1. Beide Geräte werden fast gleichzeitig hochgefahren.

Operation	Primary Unit		Secondary Unit	
	Group 1: primary	Group 2: secondary	Group 1: primary	Group 2: secondary
Both devices started simultaneously	Active	Active	Standby	Standby
	or			
	Standby	Standby	Active	Active

Status A

2. Die Vorbelegungszeit (30 s in diesem Dokument) wurde überschritten.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

Status B

3. Fehler (z. B. "Interface Down") in Gruppe 1 der primären Einheit.

Failover event	Standby	Standby	Active	Active

Status C

4. Die Vorbelegungszeit (in diesem Dokument 30 s) ist seit der Wiederherstellung des Fehlers in Gruppe 1 des primären Geräts vergangen.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

Status D

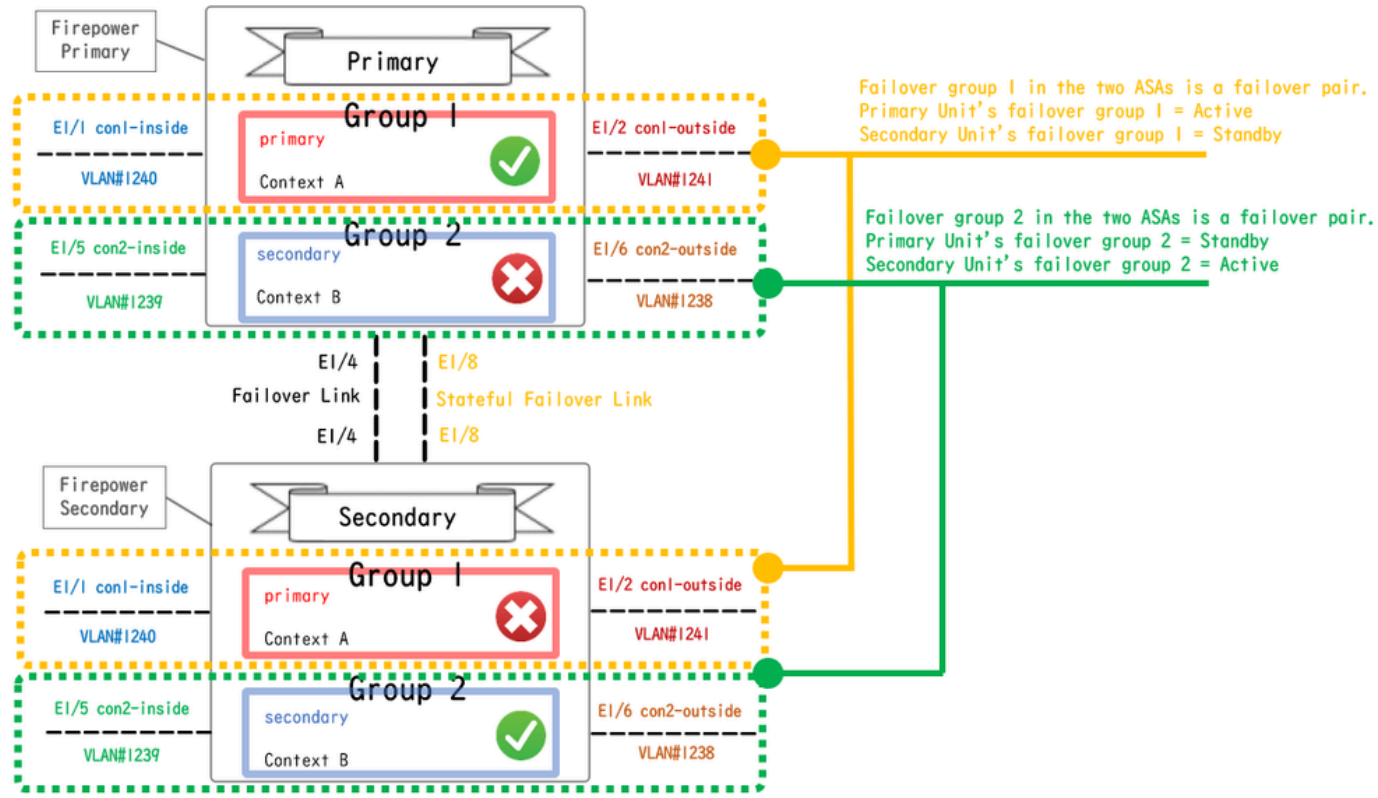
5. Gruppe 2 der primären Einheit manuell auf "Aktiv" setzen.

Manual failover	Active	Active	Standby	Standby

Status E

Netzwerkdiagramm

In diesem Dokument wird die Konfiguration und Überprüfung für Aktiv/Aktiv-Failover anhand dieses Diagramms vorgestellt.



Logisches Konfigurationsdiagramm

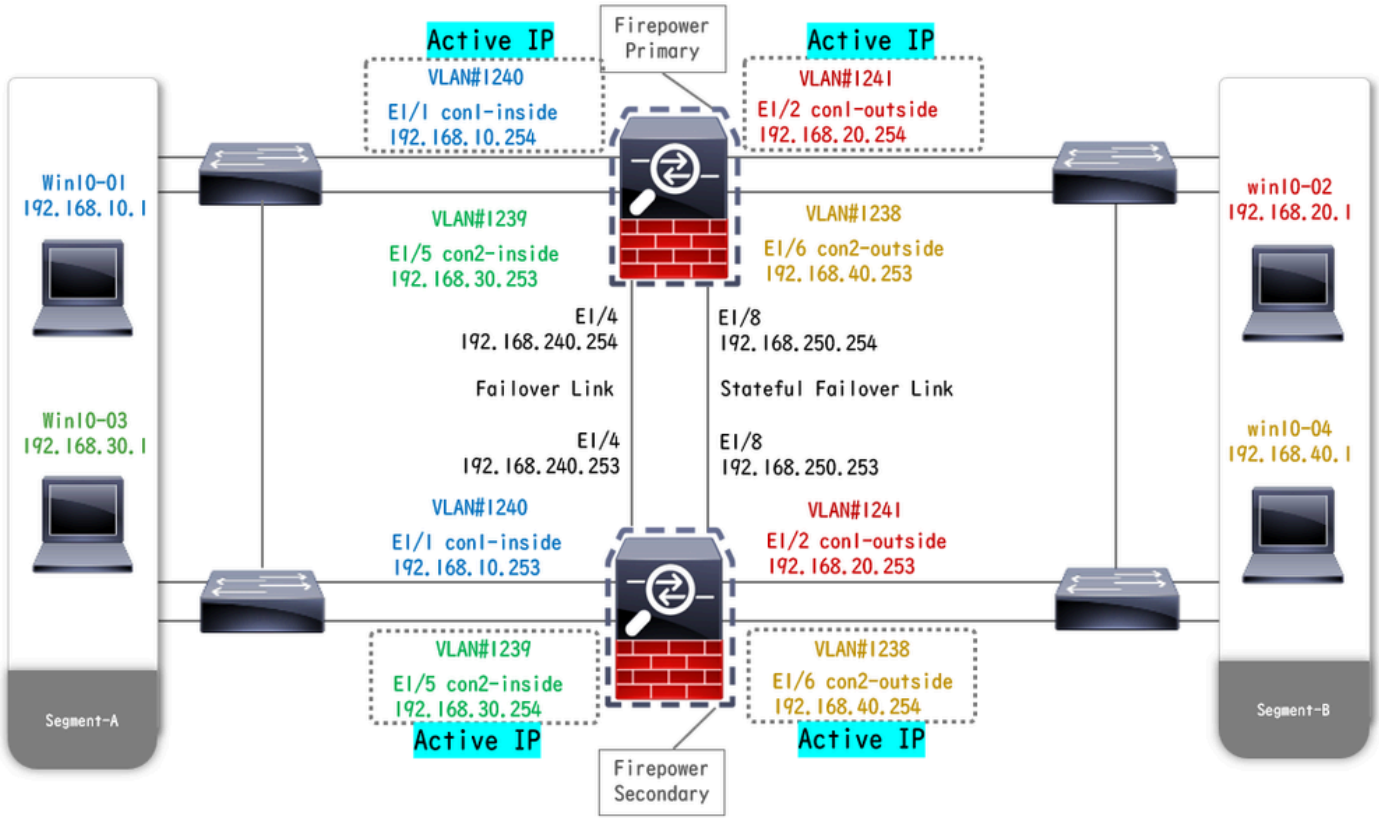
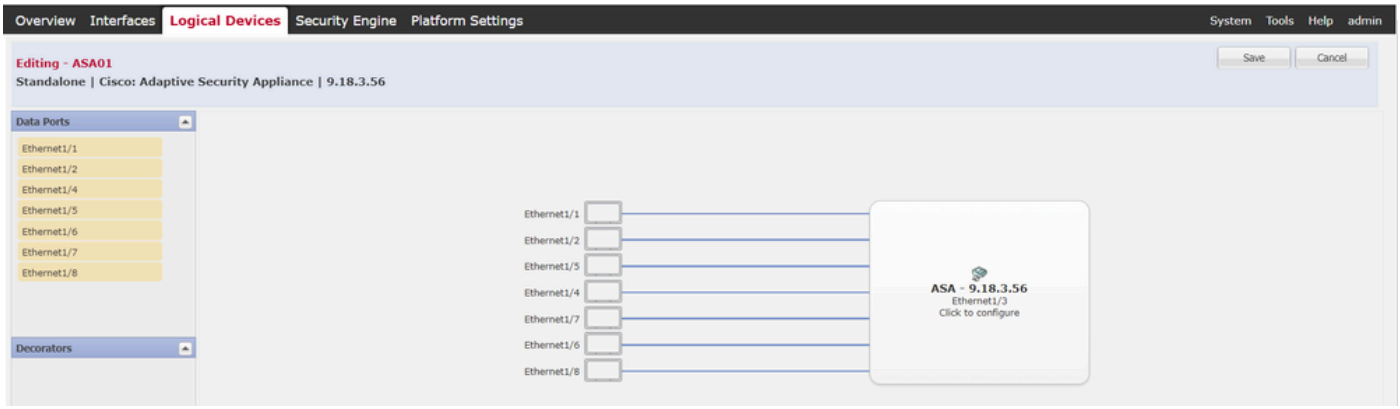


Diagramm der physischen Konfiguration

Konfiguration

Schritt 1: Schnittstellen vorkonfigurieren

Melden Sie sich für beide Firepower an der FCM-GUI an. Navigieren Sie zu Logische Geräte > Bearbeiten. Fügen Sie der ASA eine Datenschnittstelle hinzu, wie im Bild dargestellt.



Schnittstellen vorkonfigurieren

Schritt 2: Konfiguration auf der primären Einheit

Stellen Sie über SSH oder eine Konsole eine Verbindung zur primären FXOS-CLI her. Führen Sie einen **connect module 1 console** und einen connect asa Befehl aus, um die ASA CLI zu starten.

a. Konfigurieren Sie Failover auf der primären Einheit (führen Sie den Befehl im Systemkontext der primären Einheit aus).

<#root>

failover lan unit primary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby 1

failover group 1

□□□<--- group 1 is assigned to primary by default preempt 30 failover group 2 secondary preempt 30 fai

b. Konfigurieren Sie die Failover-Gruppe für den Kontext (führen Sie den Befehl im Systemkontext der primären Einheit aus).

<#root>

admin-context admin

context admin

<--- admin context is assigned to group 1 by default allocate-interface E1/3 config-url disk0:/admin.c

join-failover-group 1

<--- add con1 context to group 1 ! context con2 allocate-interface E1/5 allocate-interface E1/6 config

join-failover-group 2

<--- add con2 context to group 2

c. Führen Sie den Befehl changeto context con1 aus, um den Kontext con1 aus dem Systemkontext zu verbinden. Konfigurieren Sie die IP-Adresse für die Schnittstelle des Kontexts con1 (führen Sie den Befehl im Kontext con1 der primären Einheit aus).

interface E1/1 nameif con1-inside ip address 192.168.10.254 255.255.255.0 standby 192.168.10.253 security-level 100 no shutdown interface E1/2 nameif

d. Führen Sie changeto context con2 aus, um den con2-Kontext aus dem Systemkontext zu verbinden. Konfigurieren Sie die IP-Adresse für die Schnittstelle des con2-Kontexts (führen Sie den Befehl im con2-Kontext der primären Einheit aus).

interface E1/5 nameif con2-inside ip address 192.168.30.254 255.255.255.0 standby 192.168.30.253 security-level 100 no shutdown interface E1/6 nameif

Schritt 3: Konfiguration der Sekundäreinheit

a. Stellen Sie über SSH oder die Konsole eine Verbindung mit der sekundären FXOS-CLI her. Konfigurieren Sie Failover auf der sekundären Einheit (führen Sie den Befehl im Systemkontext der sekundären Einheit aus).

failover lan unit secondary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby

b. Befehl ausführen failover (im Systemkontext der sekundären Einheit ausführen).

failover

Schritt 4: Failover-Status nach erfolgreicher Synchronisierung bestätigen

a. Im Systemkontext der sekundären Einheit ausführenshow failover.

<#root>

asa#

show failover

 Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) Version: Ours 9.18(

Secondary

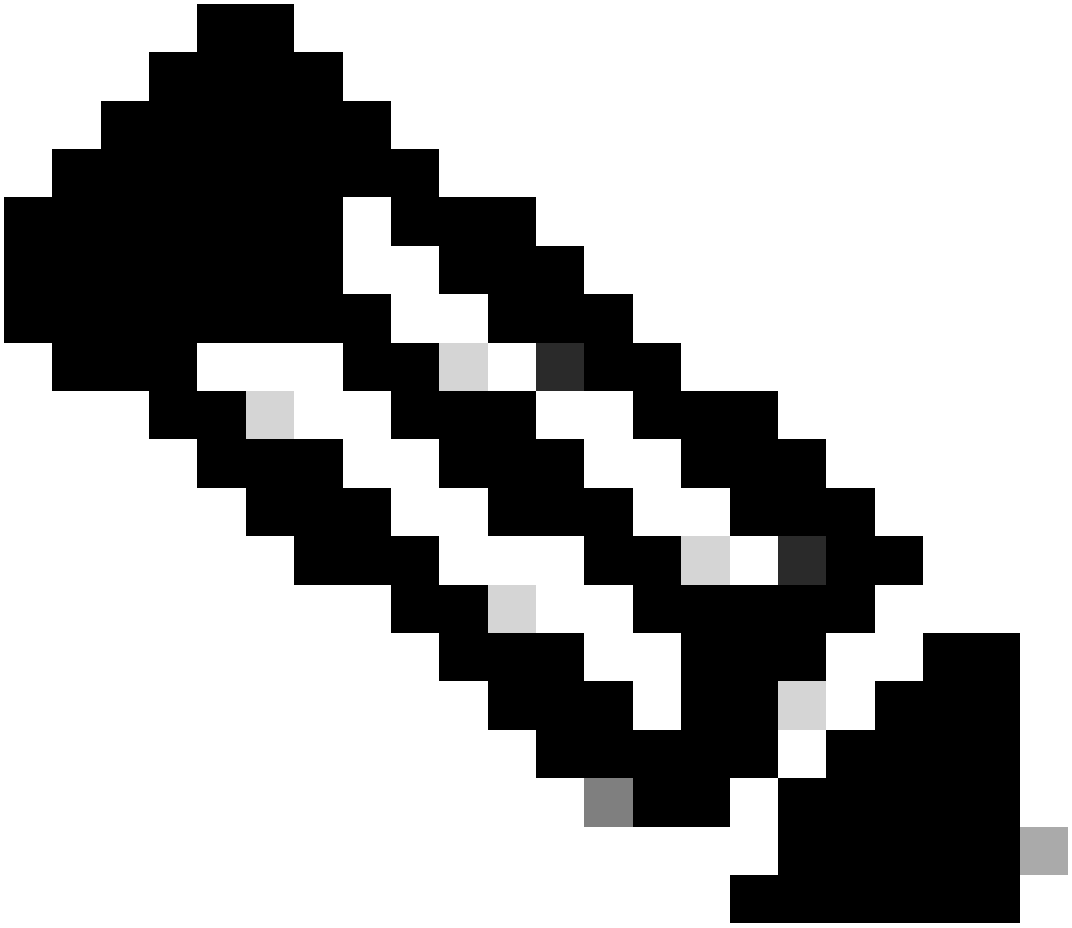
<--- group 1 and group 2 are Standby status in Secondary Unit Group 1 State:

Standby Ready

```
 Active time: 0 (sec) Group 2 State:
Standby Ready
 Active time: 945 (sec) con1 Interface con1-inside (192.168.10.253): Unknown (Waiting) con1 Interface c
Primary
<--- group 1 and group 2 are Active status in Primary Unit Group 1 State:
Active
 Active time: 1637 (sec) Group 2 State:
Active
 Active time: 93 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface c
```

b. (Optional) Führen Sie den **no failover active group 2** Befehl aus, um Gruppe 2 der primären Einheit manuell in den Standby-Status zu versetzen (im Systemkontext der primären Einheit auszuführen). Dadurch kann die Datenverkehrslast durch die Firewall ausgeglichen werden.

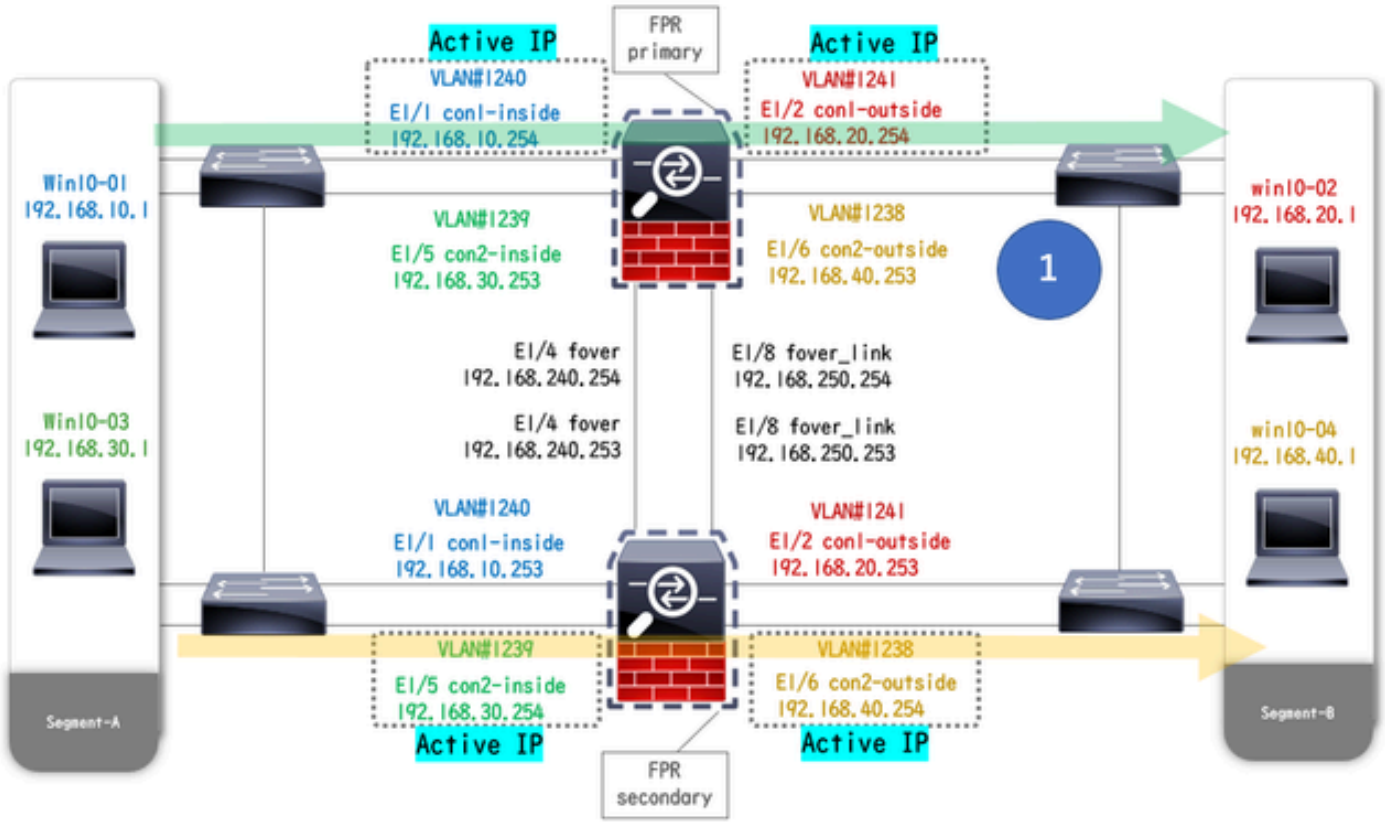
```
<#root>

no failover active group 2
```



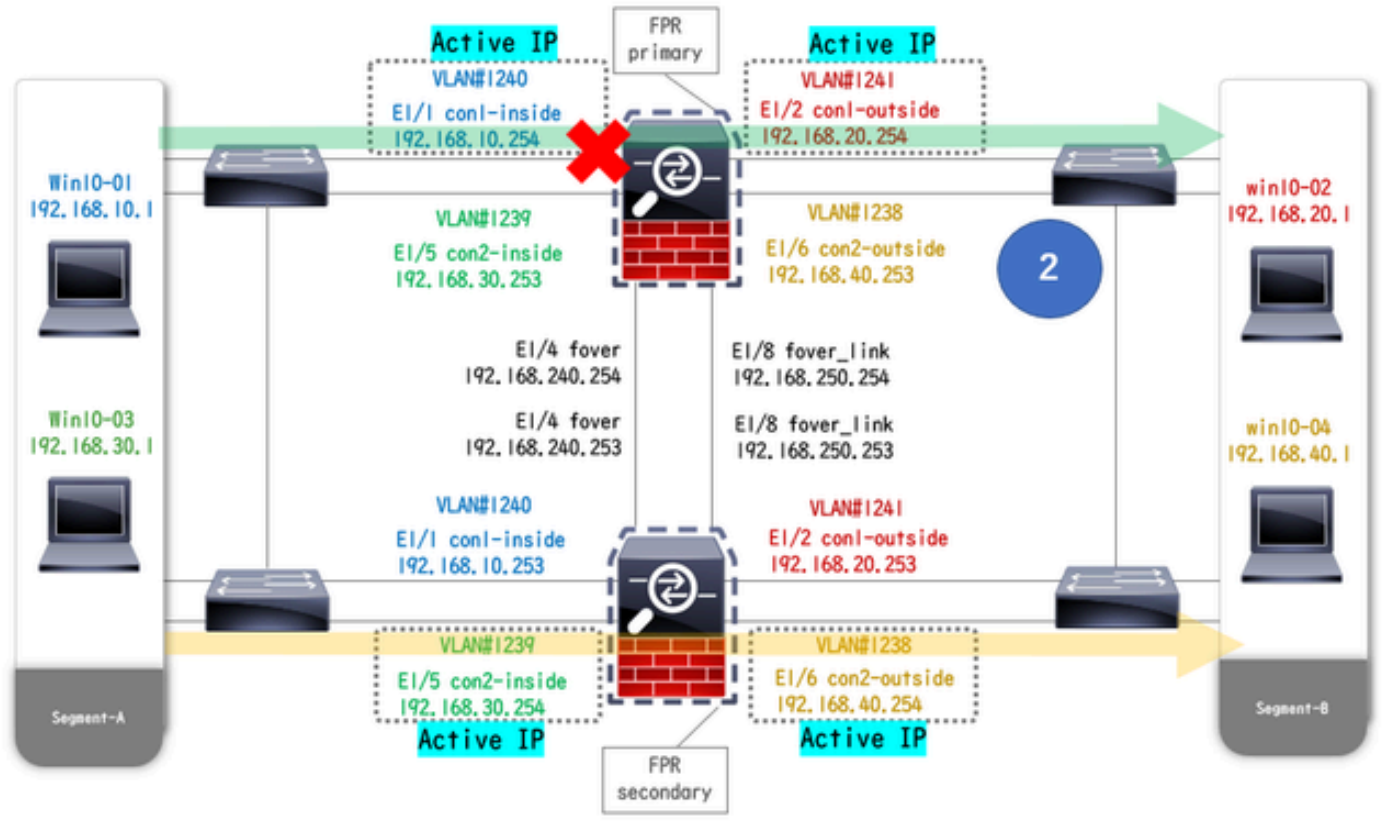
Hinweis: Wenn Sie diesen Befehl ausführen, stimmt der Failover-Status mit der Verkehrsflussbedingung 1 überein.

Überprüfung

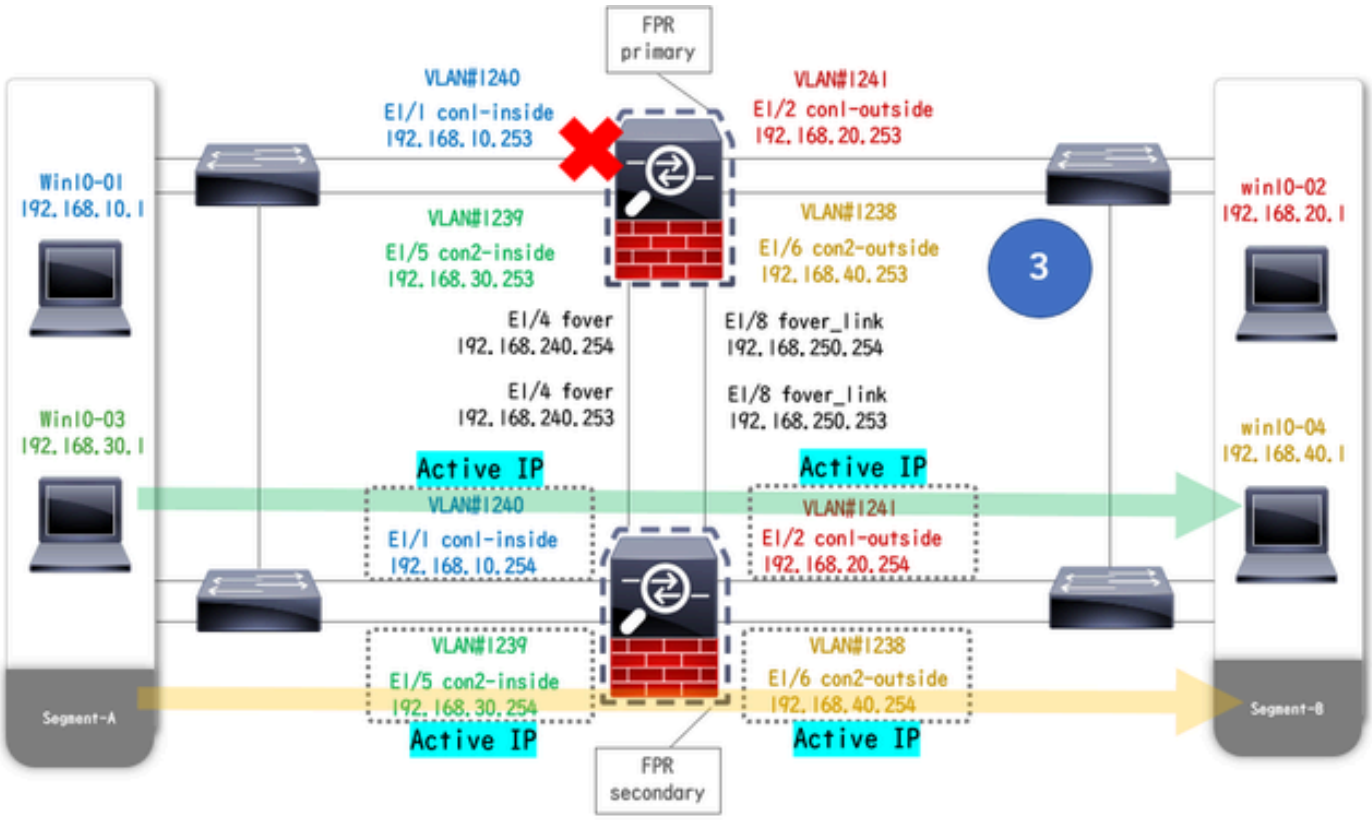
Wenn E1/1 AUSFÄLLT, wird das Failover der Gruppe 1 ausgelöst, und die Datenschnittstellen auf der Standby-Seite (Sekundäreinheit) übernehmen die IP- und MAC-Adresse der ursprünglichen aktiven Schnittstelle, sodass der Datenverkehr (FTP-Verbindung in diesem Dokument) kontinuierlich von den ASAs weitergeleitet wird.



Vor Link



DownWährend Link Down



Failover ausgelöst

Schritt 1: FTP-Verbindung von Win10-01 zu Win10-02 initiieren

Schritt 2: FTP-Verbindung vor Failover bestätigen

Führen Sie changeto context con1 aus, um den Kontext con1 aus dem Systemkontext zu verbinden. Stellen Sie sicher, dass in beiden ASA-Einheiten eine FTP-Verbindung besteht.

<#root>

asa/act/pri/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Primary Unit TCP
```

con1-outside

192.168.20.1:21

con1-inside 192.168.10.1:49703

, idle 0:00:11, bytes 528, flags UIO asa/stby/sec/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Secondary Unit TCP
```

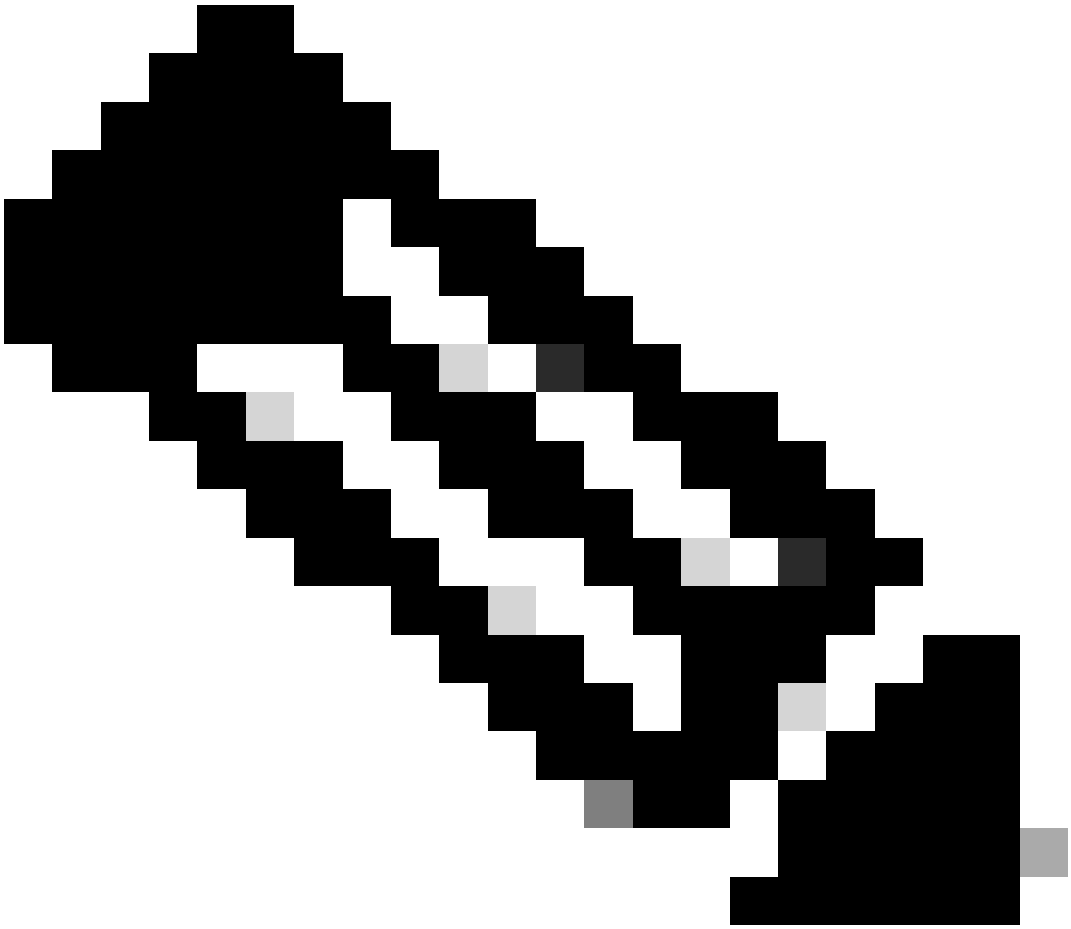
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:14, bytes 528, flags UIO

Schritt 3: LinkDOWN E1/1 der primären Einheit

Schritt 4: Failover-Status bestätigen

Stellen Sie im Systemkontext sicher, dass in Gruppe 1 ein Failover stattfindet.



Hinweis: Der Failover-Status stimmt mit dem Verkehrsflusszustand überein 4.

<#root>

asa/act/sec#

show failover

Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) ..... Group 1 last

Secondary

Group 1 State:

Active

<--- group 1 of Secondary Unit is Switching to Active Active time: 5 (sec) Group 2 State:

Active

Active time: 10663 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Waiting) con1 Interface

Primary

Group 1 State:

Failed

<--- group 1 of Primary Unit is Switching to Failed status Active time: 434 (sec) Group 2 State:

Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.253): Failed (Waiting) con1 Interface co

Schritt 5: FTP-Verbindung nach Failover bestätigen

Führen Sie changeto context con1 den Befehl aus, um den Kontext con1 aus dem Systemkontext heraus zu verbinden, und stellen Sie sicher, dass die FTP-Verbindung nicht unterbrochen wird.

<#root>

asa/act/sec#

changeto context con1

asa/act/sec/con1# show conn 11 in use, 11 most used
! --- Confirm the target FTP connection exists in group 1 of the Secondary Unit TCP

con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:09, bytes 529, flags UIO

Schritt 6: Verhalten der Vorbelegungszeit bestätigen

LinkUP E1/1 der Primäreinheit, 30 Sekunden Wartezeit (Preempt-Zeit); der Failover-Status kehrt in den ursprünglichen Zustand zurück (Übereinstimmung mit Datenverkehrsfluss in Muster 1).

<#root>

asa/stby/pri#

Group 1 preempt mate

□□□□<--- Failover is triggered automatically, after the preempt time has passed asa/act/pri# show fail

Primary

Group 1 State:

Active

<--- group 1 of Primary Unit is switching to Active status Active time: 34 (sec) Group 2 State:

Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface

Secondary

Group 1 State:

Standby Ready

□□<---- group 1 of Secondary Unit is switching to Standby status Active time: 125 (sec) Group 2 State:

Active

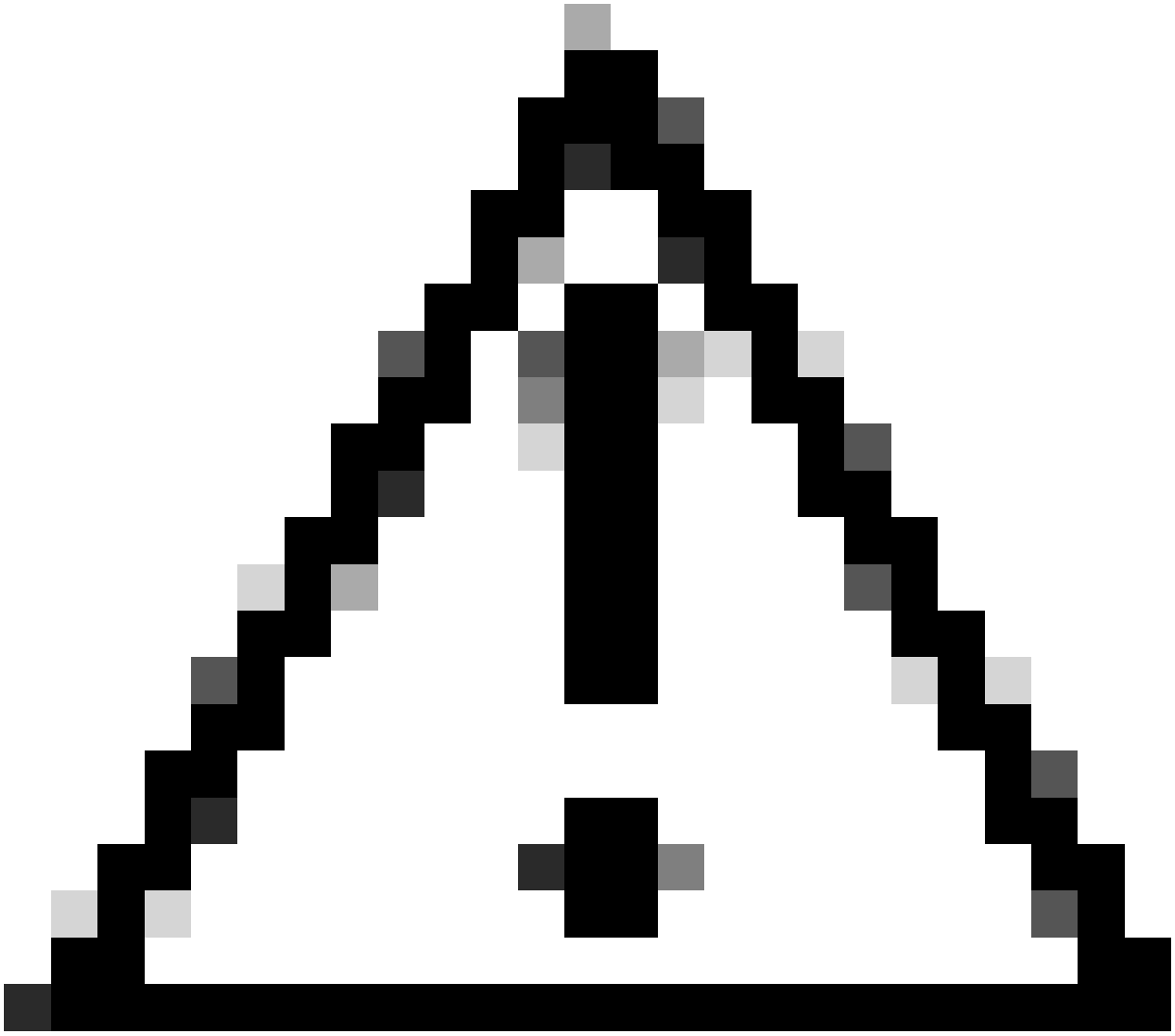
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

Virtuelle MAC-Adresse

Im Aktiv/Aktiv-Failover wird immer die virtuelle MAC-Adresse (manuell festgelegter Wert, automatisch generierter Wert oder Standardwert) verwendet. Die aktive virtuelle MAC-Adresse ist mit der aktiven Schnittstelle verknüpft.

Manuelles Festlegen der virtuellen MAC-Adresse

Um die virtuelle MAC-Adresse für physische Schnittstellen manuell festzulegen, kann der mac address Befehl oder der mac-address Befehl (im I/F-Einstellungsmodus) verwendet werden. Dies ist ein Beispiel für das manuelle Festlegen einer virtuellen MAC-Adresse für die physische Schnittstelle E1/1.



Vorsicht: Vermeiden Sie die Verwendung dieser beiden Befehlstypen auf demselben Gerät.

<#root>

asa/act/pri(config)# failover group 1 asa/act/pri(config-fover-group)#

mac address E1/1 1234.1234.0001 1234.1234.0002

asa/act/pri(config-fover-group)# changeto context con1 asa/act/pri/con1(config)# show interface E1/1 |

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500 <--- Checking virtual MAC on the Secondary Unit(con1) side

ODER

<#root>

asa/act/pri(config)# changeto context con1 asa/act/pri/con1(config)# int E1/1 asa/act/pri/con1(config-if)#

mac-addr

1234.1234.0001 standby 1234.1234.0002

asa/act/pri/con1(config)# show interface E1/1 | in MAC MAC address

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500<--- Checking virtual MAC on the Secondary Unit(con1) side

Automatische Einstellung der virtuellen MAC-Adresse

Die automatische Generierung virtueller MAC-Adressen wird ebenfalls unterstützt. Dies kann mithilfe des mac-address auto <prefix prefix> Befehls erreicht werden. Das Format der virtuellen MAC-Adresse ist A2 xx.yyzz.zzzz, die automatisch generiert wird.
A2: fester Wert
xx.yy : wird durch das in der Befehlsoption angegebene <Präfix-Präfix> generiert (Das Präfix wird in Hexadezimalform konvertiert und dann in umgekehrter Reihenfolge eingefügt).
zz.zzzz : generiert durch einen internen Zähler

Dies ist ein Beispiel für die Generierung einer virtuellen MAC-Adresse über einen **mac-address auto** Befehl für die Schnittstelle.

<#root>

asa/act/pri(config)#

mac-address auto

INFO: Converted to mac-address auto prefix 31

```
asa/act/pri(config)#
```

show run all context con1

```
 <--- Checking the virtual MAC addresses generated on con1 context
allocate-interface Ethernet1/1
mac-address auto Ethernet1/1 a21f.0000.0008 a21f.0000.0009
allocate-interface Ethernet1/2
mac-address auto Ethernet1/2 a21f.0000.000a a21f.0000.000b
config-url disk0:/con1.cfg
join-failover-group 1

asa/act/pri(config)#
```

show run all context con2

```
<--- Checking the virtual MAC addresses generated on con2 context
context con2
allocate-interface Ethernet1/5
mac-address auto Ethernet1/5 a21f.0000.000c a21f.0000.000d
allocate-interface Ethernet1/6
mac-address auto Ethernet1/6 a21f.0000.000e a21f.0000.000f
config-url disk0:/con2.cfg
join-failover-group 2
```

Standardeinstellung für virtuelle MAC-Adresse

Wenn weder die automatische noch die manuelle Generierung einer virtuellen MAC-Adresse festgelegt ist, wird die standardmäßige virtuelle MAC-Adresse verwendet.

Weitere Informationen zur standardmäßigen virtuellen MAC-Adresse finden Sie im Command Default of MAC address im Cisco Secure Firewall ASA Series Command Reference Guide.

Upgrade

Ein Upgrade eines Aktiv/Aktiv-Failover-Paars ohne Ausfallzeiten kann über CLI oder ASDM durchgeführt werden. Weitere Informationen finden Sie unter Upgrade an Active/Active Failover Pair.

Zugehörige Informationen

- Aktualisieren eines Aktiv/Aktiv-Failover-Paars mithilfe der CLI
- MAC-Adresse
- Technischer Support und Downloads von Cisco

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.