Configuración de la conmutación por fallo activa/activa de ASA en Firepower serie 4100

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Mecanismo de conmutación por fallas activa/activa de ASA
- Flujo de tráfico
  - Condición de flujo de tráfico 1
  - Condición de flujo de tráfico 2
  - Condición de flujo de tráfico 3
  - Condición de flujo de tráfico 4
- Reglas de selección para Activo/En espera
- Diagrama de la red
- Configuración
  - Paso 1. Preconfigurar interfaces
  - Paso 2. Configuración en la unidad principal
  - Paso 3. Configuración en la unidad secundaria
  - Paso 4. Confirmar estado de conmutación por error después de que la sincronización finalizó correctamente
- Verificación
  - Paso 1. Iniciar conexión FTP de Win10-01 a Win10-02
  - Paso 2. Confirmar conexión FTP antes de conmutación por error
  - Paso 3. LinkDOWN E1/1 de la unidad primaria
  - Paso 4. Confirmar estado de failover
  - Paso 5. Confirmar la conexión FTP después de la conmutación por error
  - Paso 6. Confirmar el comportamiento del tiempo de preferencia
- Dirección MAC virtual
  - Configuración manual de la dirección MAC virtual
  - Configuración automática de la dirección MAC virtual
  - Configuración predeterminada de la dirección MAC virtual
- Actualizar
- Información Relacionada

Introducción

Este documento describe cómo configurar Active/Active Failover en Cisco Firepower 4145 NGFW

Appliance.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

- Conmutación por fallo activo/en espera en Cisco Adaptive Security Appliance (ASA).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo NGFW Cisco Firepower 4145 (ASA) 9.18(3)56
- Sistema operativo extensible (FXOS) Firepower 2.12(0.498)
- Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La conmutación por fallo activa/activa solo está disponible para los dispositivos de seguridad que se ejecutan en el modo de contexto múltiple. En este modo, el ASA se divide lógicamente en varios dispositivos virtuales, conocidos como contextos. Cada contexto funciona como un dispositivo independiente, con su propia política de seguridad, interfaces y administradores.

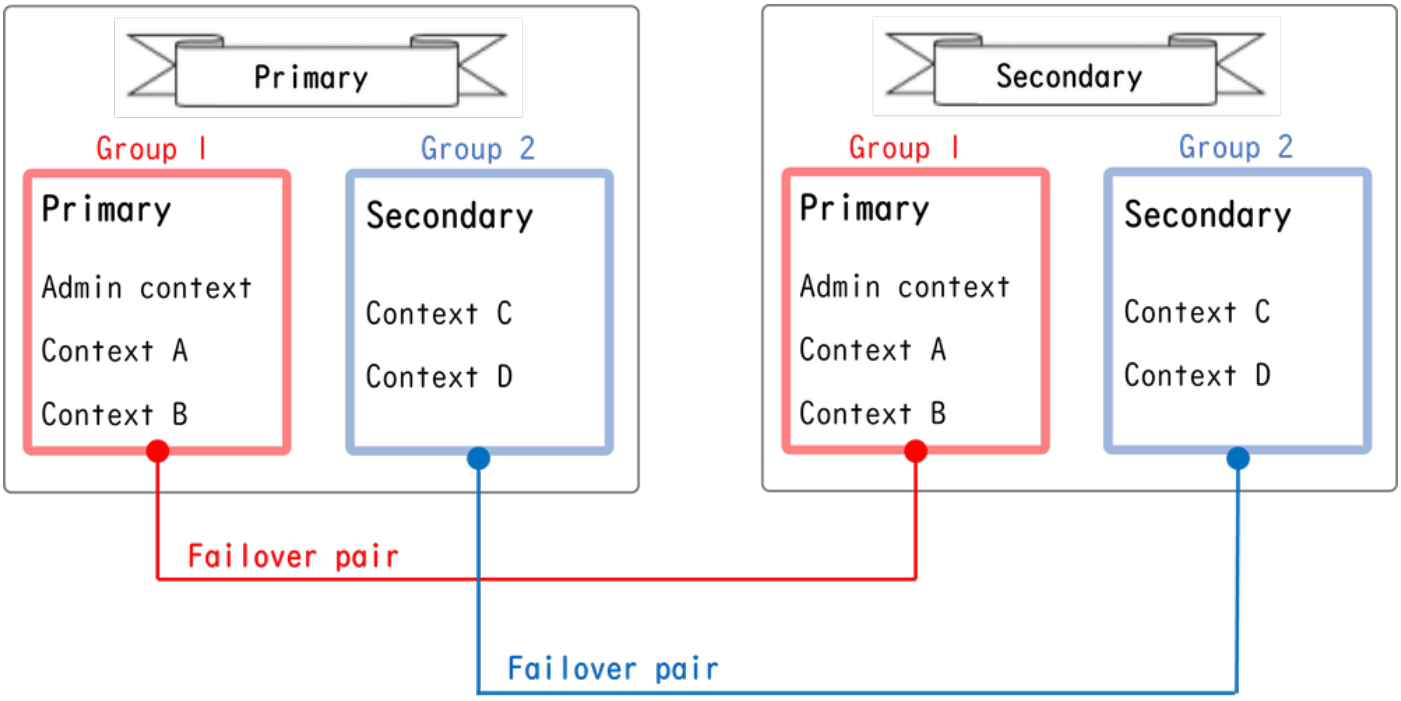
La conmutación por fallo activa/activa es una función del dispositivo de seguridad adaptable (ASA) que permite que dos dispositivos Firepower pasen el tráfico simultáneamente. Esta configuración se utiliza normalmente para un escenario de equilibrio de carga en el que se desea dividir el tráfico entre dos dispositivos para maximizar el rendimiento. También se utiliza para fines de redundancia, por lo que si un ASA falla, el otro puede asumir el control sin causar una interrupción en el servicio.

Mecanismo de conmutación por fallas activa/activa de ASA

Cada contexto en Active/Active failover se asigna manualmente al grupo 1 o al grupo 2. El contexto Admin se asigna al grupo 1 de forma predeterminada. El mismo grupo (grupo1 o grupo2) en los dos chasis (unidades) forman un par de failover que está realizando la función de redundancia. El comportamiento de cada par de failover es básicamente el mismo que el comportamiento en un failover activo/en espera. Para obtener más detalles sobre la conmutación

por fallas activa/en espera, consulte Configuración de la conmutación por fallas activa/en espera. En la conmutación por error activa/activa, además del rol (principal o secundario) de cada chasis, cada grupo también tiene un rol (principal o secundario). El usuario predefine manualmente estas funciones, que se utilizan para decidir el estado de alta disponibilidad (HA) (activo o en espera) de cada grupo de conmutación por fallo.

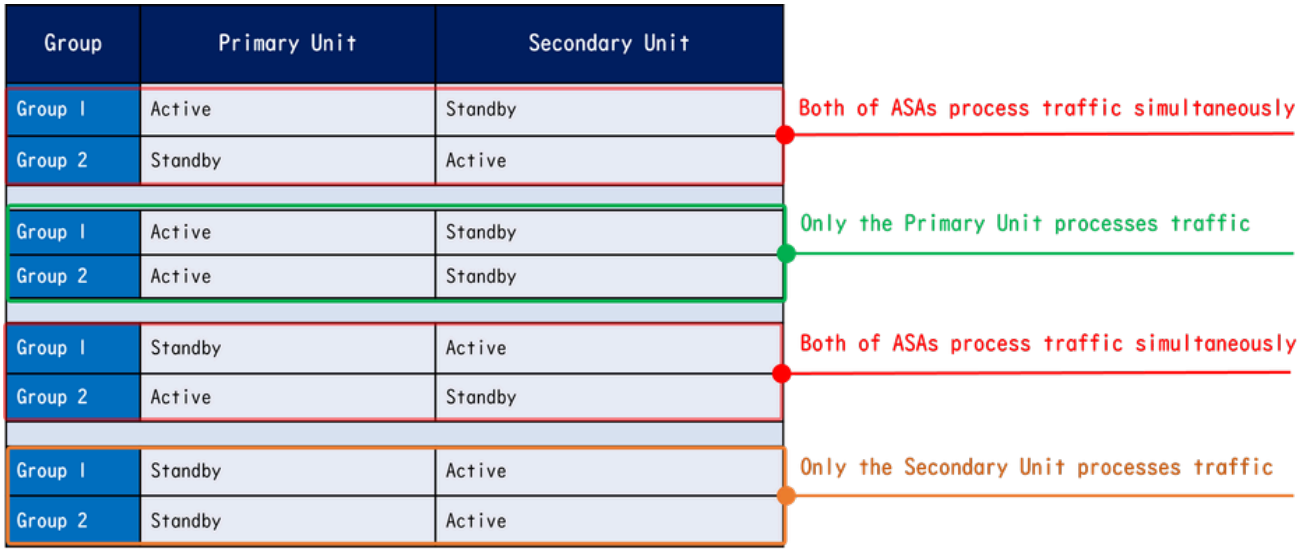
El contexto de administración es un contexto especial que gestiona la conexión de administración básica del chasis (como SSH). Imagen de conmutación por fallo activa/activa.



Par De Failover En Failover Activo/Activo

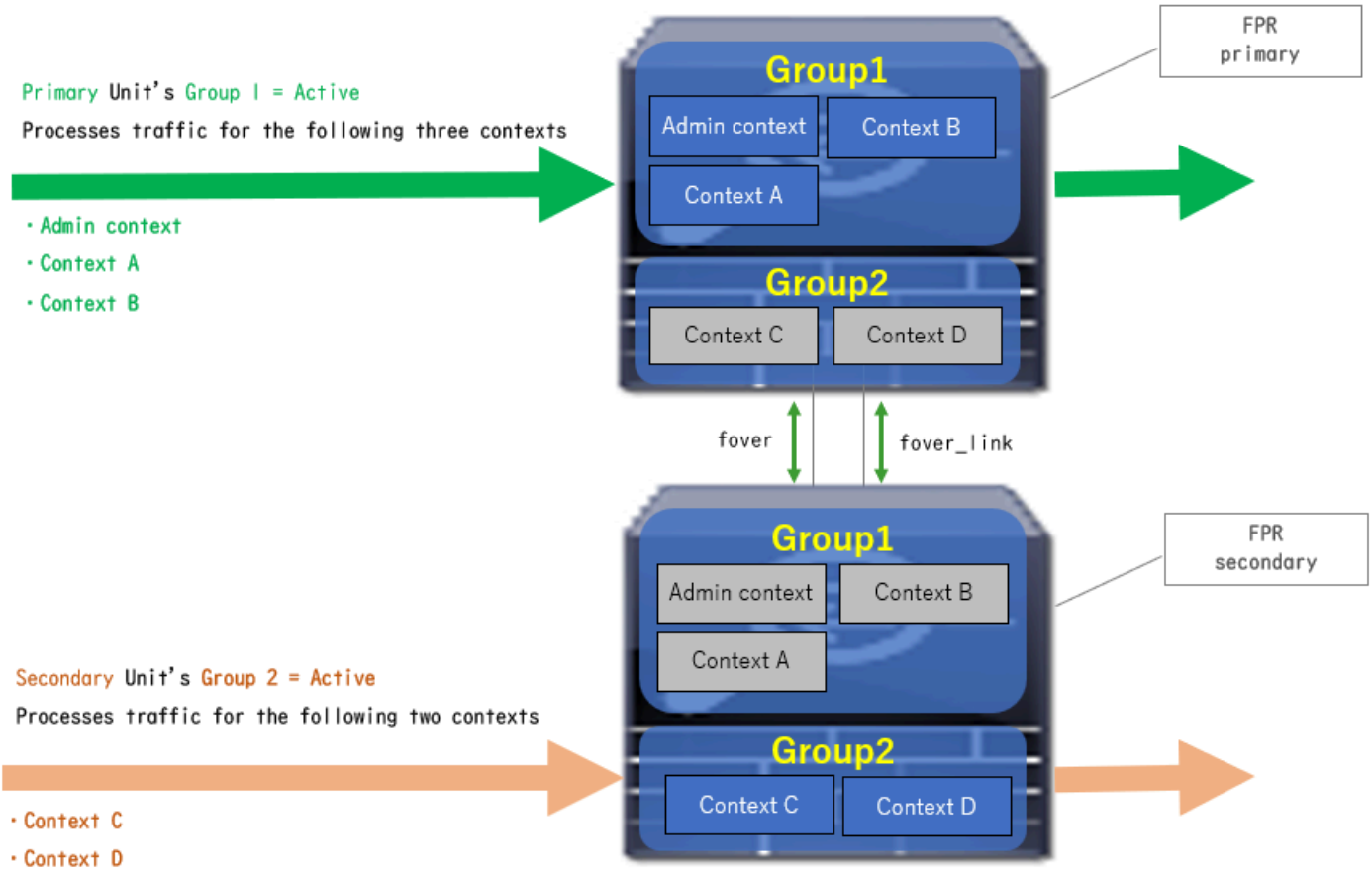
Flujo de tráfico

En la conmutación por fallas activa/activa, el tráfico se puede manejar en los diversos patrones que se muestran en la siguiente imagen.



Condición de flujo de tráfico 1

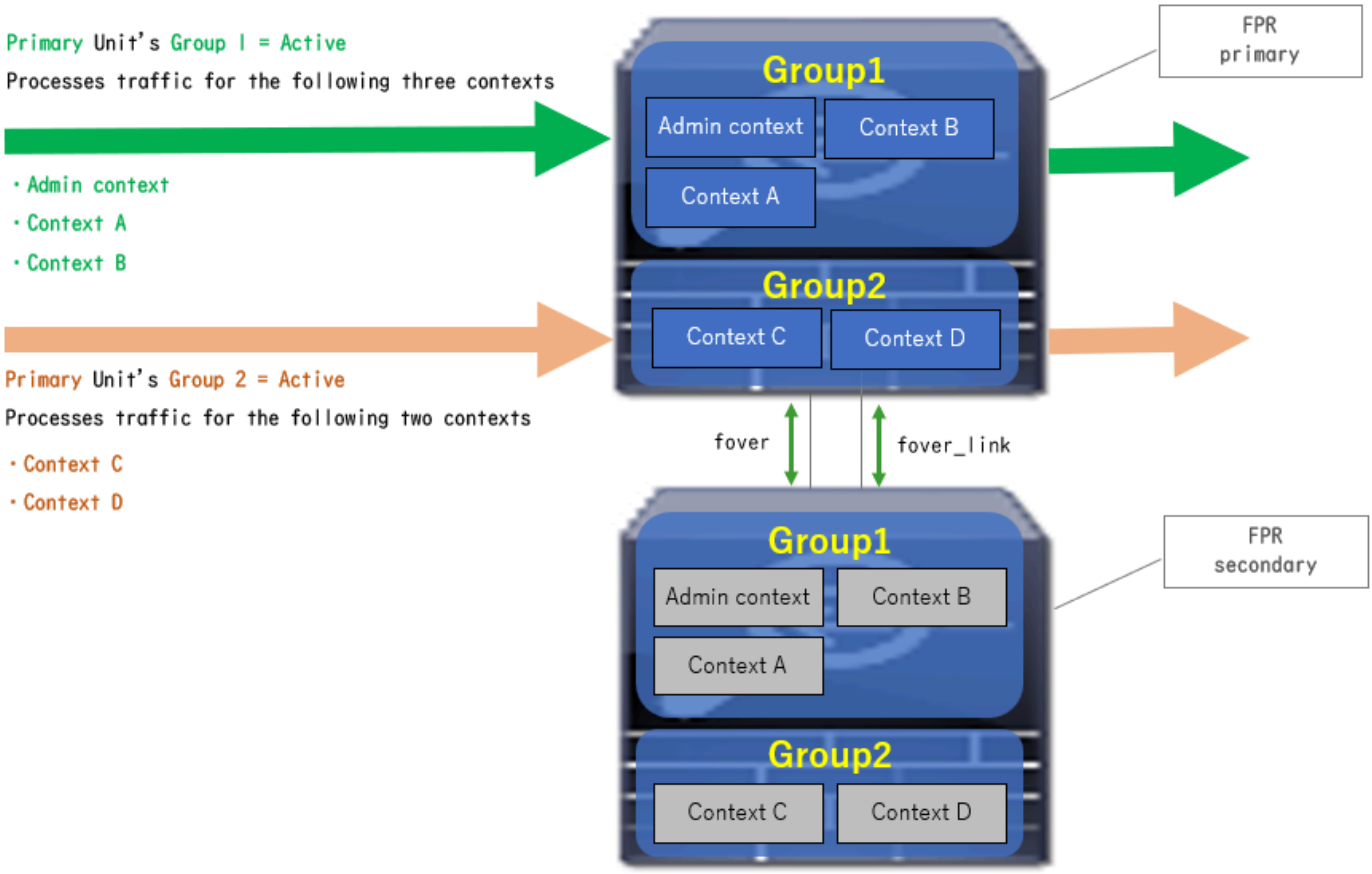
- Unidad principal: Grupo 1 = Activo, Grupo 2 = En espera
- Unidad secundaria: grupo 1 = en espera, grupo 2 = activa



Condición de flujo de tráfico 1

Condición de flujo de tráfico 2

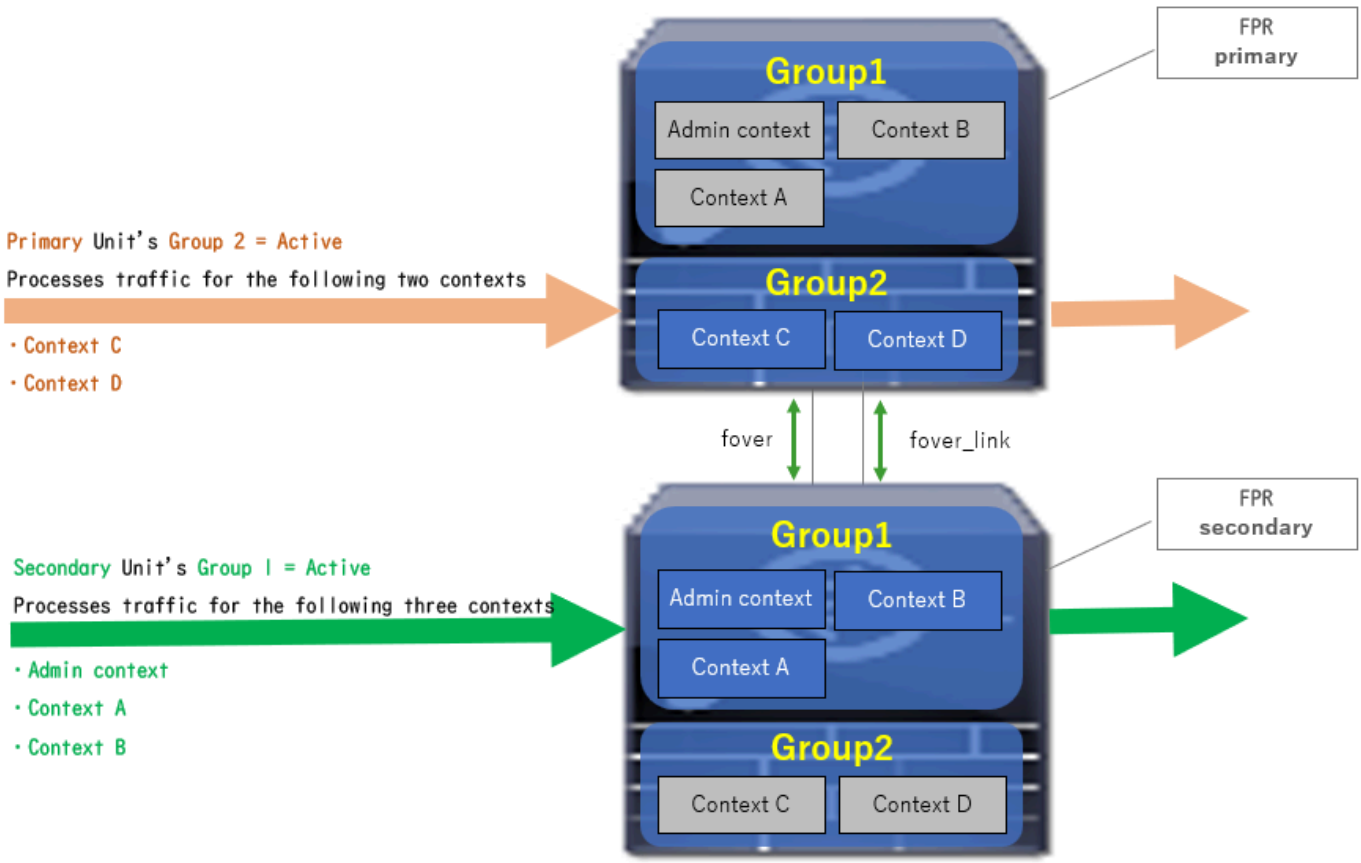
- Unidad principal: Grupo 1 = Activo, Grupo 2 = Activo
- Unidad secundaria: grupo 1 = en espera, grupo 2 = en espera



Condición de flujo de tráfico 2

Condición de flujo de tráfico 3

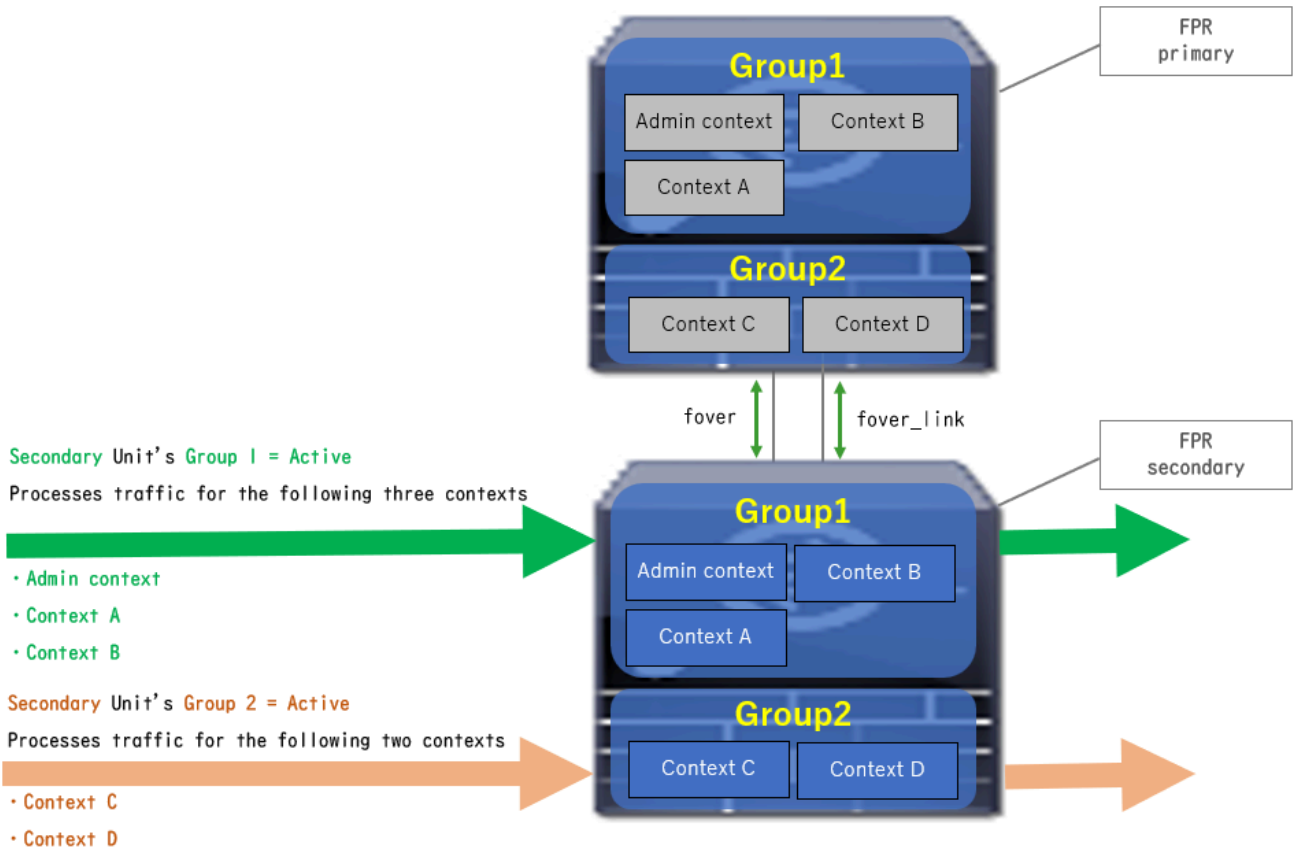
- Unidad principal: Grupo 1 = En espera, Grupo 2 = Activo
- Unidad Secundaria: Grupo 1 = Activo, Grupo 2 = En espera



Condición de flujo de tráfico 3

Condición de flujo de tráfico 4

- Unidad principal: Grupo 1 = En espera, Grupo 2 = En espera
- Unidad Secundaria: Grupo 1 = Activo, Grupo 2 = Activo



Condición de flujo de tráfico 4

Reglas de selección para Activo/En espera

En Active/Active failover , el estado (activo/en espera) de cada grupo está determinado por estas reglas:

- Suponga que dos dispositivos se están iniciando casi al mismo tiempo y que una de las unidades (principal o secundaria) se activa en primer lugar.
- Cuando pasa el tiempo de preferencia, el grupo que tiene la misma función en el chasis y el grupo se activa.
- Cuando hay un evento de failover (como la interfaz ABAJO), el estado del grupo cambia de la misma manera que con el failover Activo/En espera.
- El tiempo de prioridad no funciona después de realizar manualmente la conmutación por error.

Este es un ejemplo del cambio de estado.

- Ambos dispositivos arrancan casi al mismo tiempo. Estado A →
- Tiempo de preferencia transcurrido. Estado B →
- Error del dispositivo principal (se activa la conmutación por fallo). Estado C →
- Tiempo de preferencia transcurrido desde que el dispositivo principal se recuperó del error. Estado D →
- Activación manual de la conmutación por fallo. Estado E

Para obtener detalles sobre los disparadores de failover y la supervisión de estado, consulte

[Eventos de Failover.]

1. Ambos dispositivos se están iniciando casi al mismo tiempo.

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

Estado A

2. Tiempo de preferencia (30 s en este documento) transcurrido.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

Estado B

3. Se ha producido un fallo (por ejemplo, una interfaz inactiva) en el grupo 1 de la unidad primaria.

Failover event	Standby	Standby	Active	Active

Estado C

4. Tiempo de preferencia (30 s en este documento) transcurrido desde que el grupo 1 del dispositivo principal se recuperó del error.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

Estado D

5. Configuración manual del grupo 2 de la unidad primaria en Activo.

Manual failover	Active	Active	Standby	Standby

Estado E

Diagrama de la red

Este documento presenta la configuración y verificación para Active/Active failover base en este diagrama.

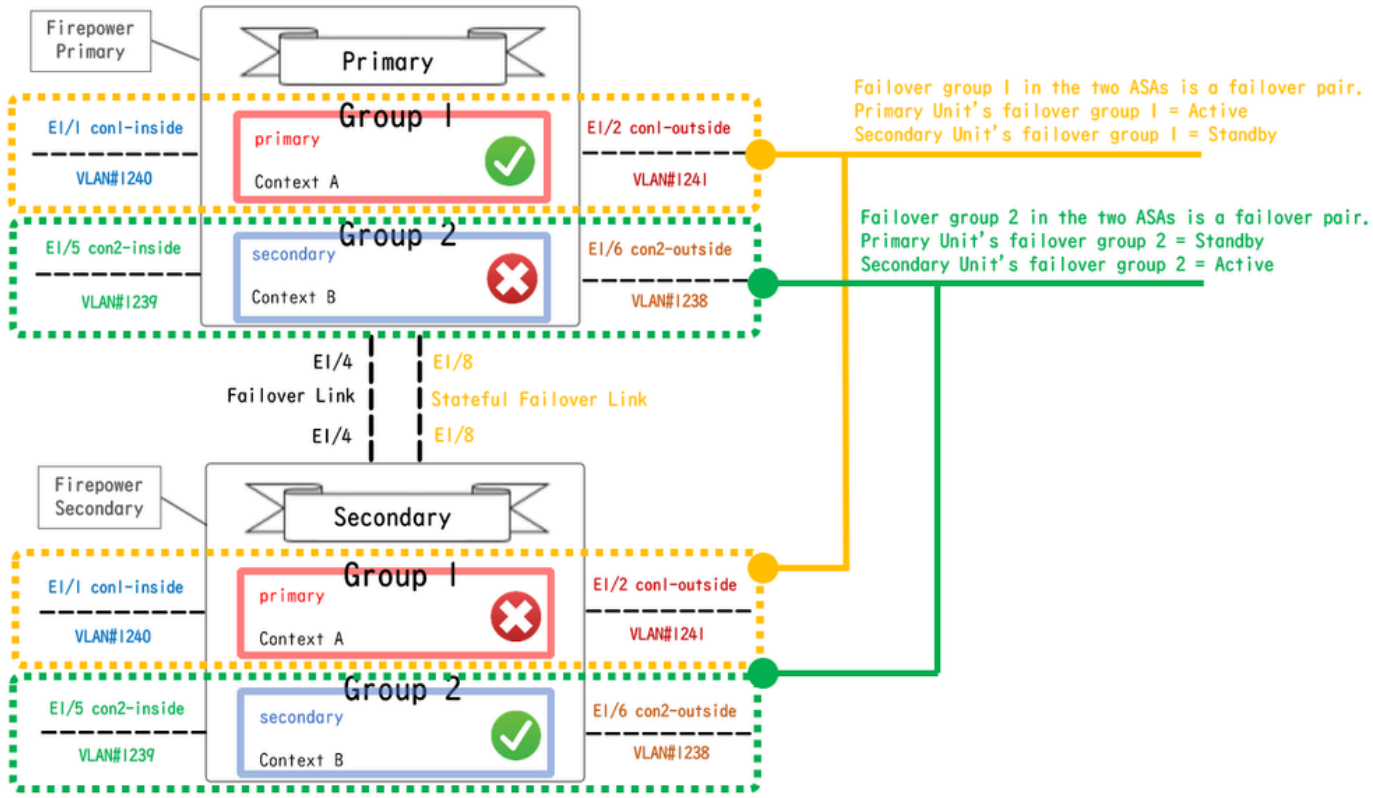


Diagrama de configuración lógica

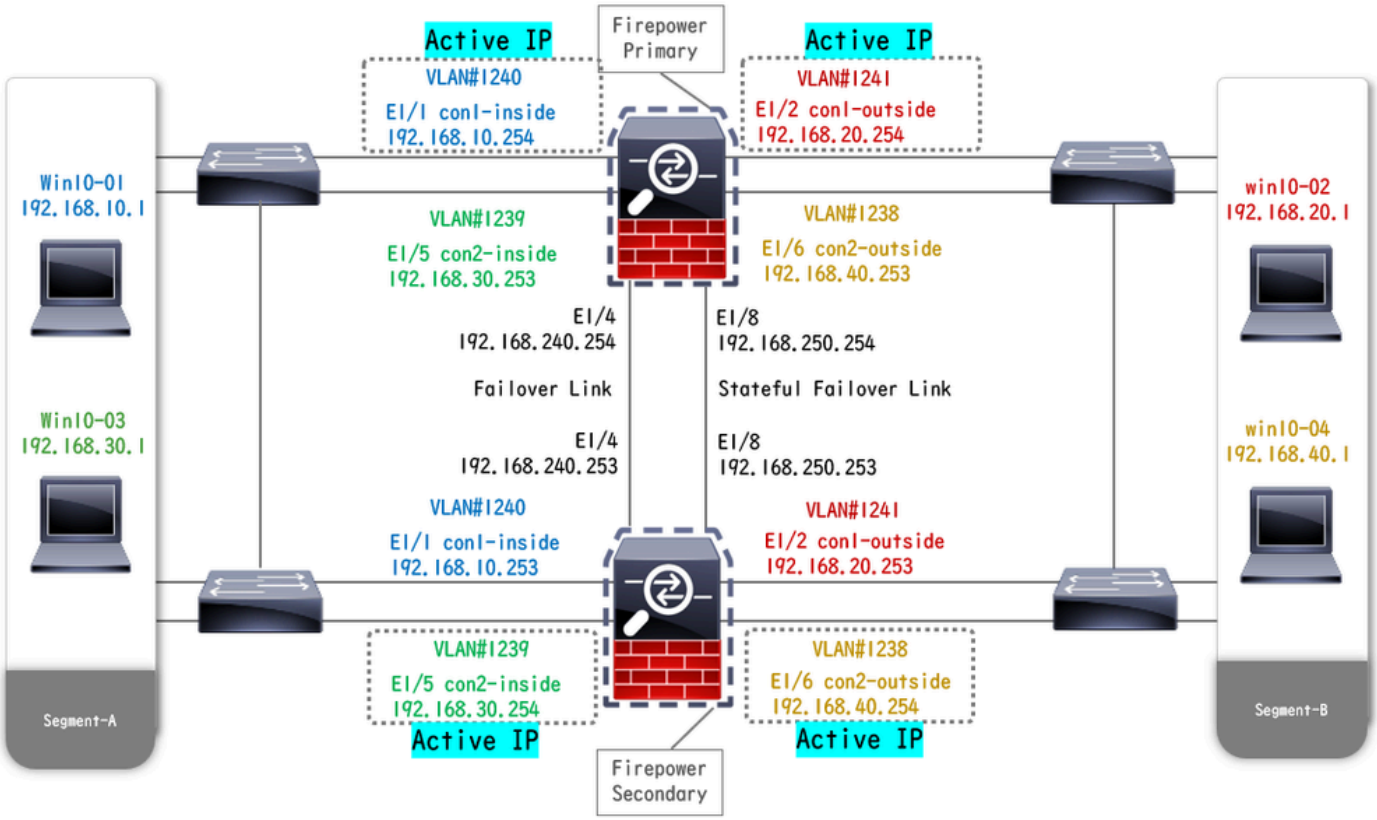
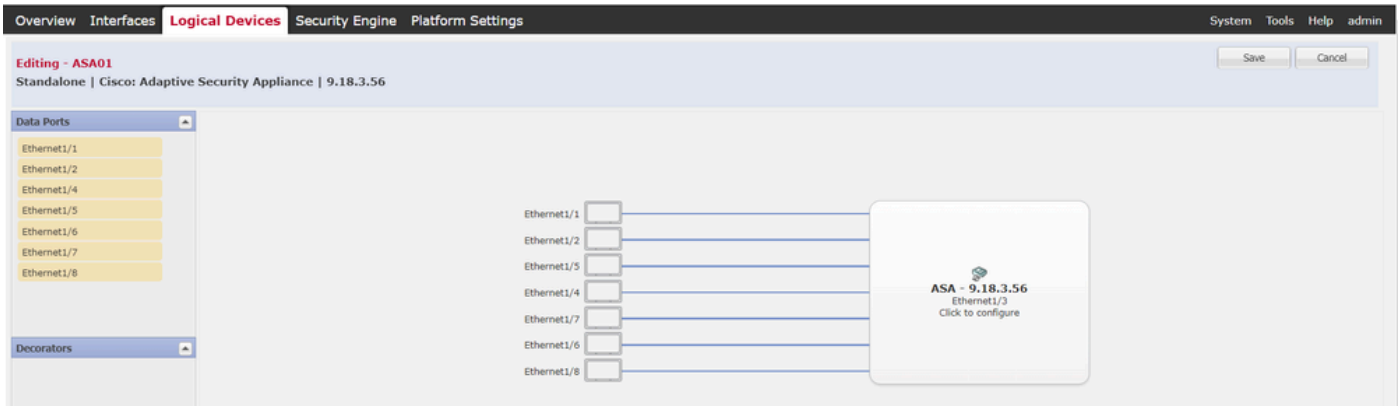


Diagrama de configuración física

Configuración

Paso 1. Preconfigurar interfaces

Para ambos Firepower, inicie sesión en la GUI de FCM. Vaya a Logical Devices > Edit. Agregue la interfaz de datos al ASA, como se muestra en la imagen.



Preconfigurar interfaces

Paso 2. Configuración en la unidad principal

Conéctese a la CLI de FXOS principal mediante SSH o la consola. Ejecute **connect module 1 console** y connect asaejecute el comando para entrar en la CLI de ASA.

a. Configure el failover en la unidad primaria (ejecute el comando en el contexto del sistema de la unidad primaria).

<#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. Configure el grupo de failover para el contexto (ejecute el comando en el contexto del sistema de la unidad primaria).

<#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. Ejecute changeto context con1 para conectar el contexto con1 desde el contexto del sistema . Configure la IP para la interfaz del contexto con1 (ejecute el comando en el contexto con1 de la unidad primaria).

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. Ejecute changeto context con2 para conectar el contexto con2 desde el contexto del sistema . Configure la IP para la interfaz del contexto con2 (ejecute el comando en el contexto con2 de la unidad primaria).

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

Paso 3. Configuración en la unidad secundaria

a. Conéctese a la CLI secundaria de FXOS a través de SSH o de la consola. Configure el failover en la unidad secundaria (ejecute el comando en el contexto del sistema de la unidad secundaria).

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. Ejecutar failover comando (ejecutar en el contexto del sistema de la unidad secundaria).

failover

Paso 4. Confirmar estado de conmutación por error después de que la sincronización finalizó correctamente

a. Ejecutar show failover en el contexto del sistema de la unidad secundaria.

<#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:

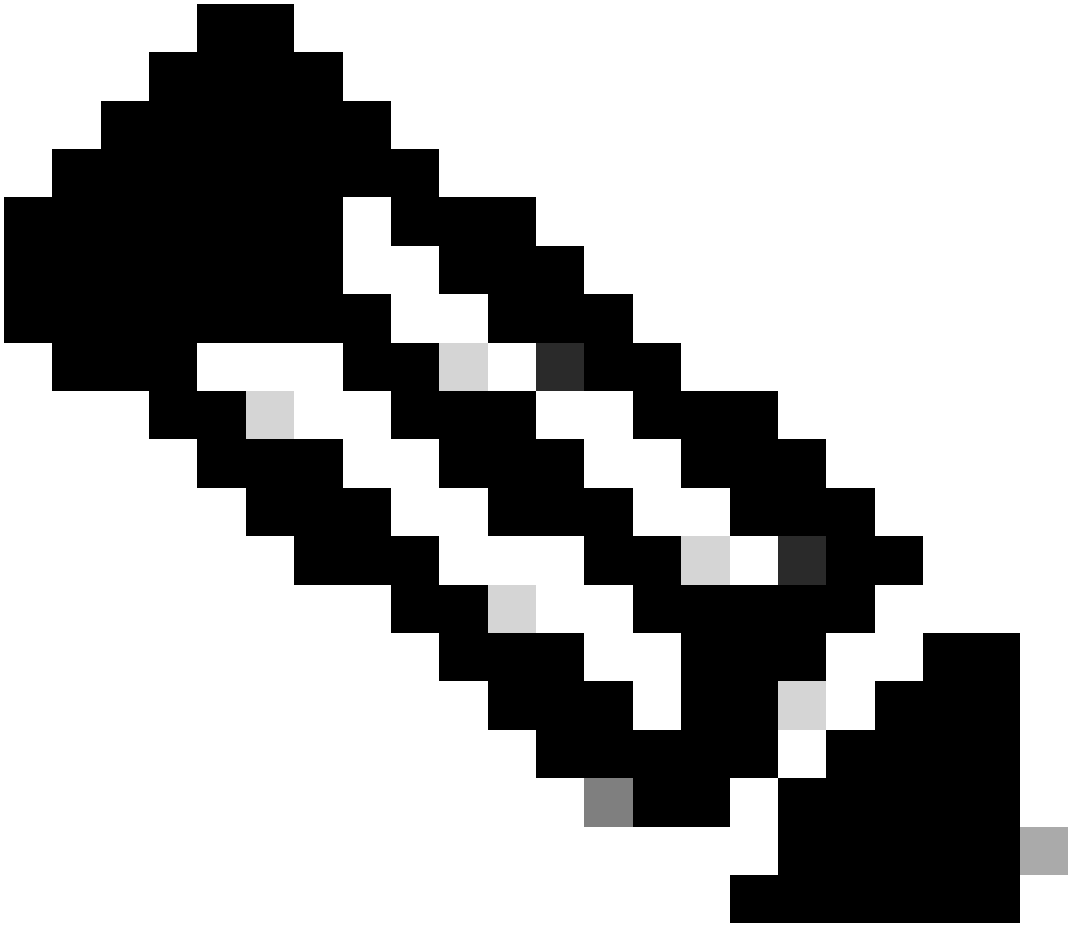
Standby Ready

```
 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. (Opcional) Ejecute el **no failover active group 2** comando para conmutar manualmente el grupo 2 de la unidad primaria al estado en espera (ejecute en el contexto del sistema de la unidad primaria). Esto puede equilibrar la carga de tráfico a través del firewall.

<#root>

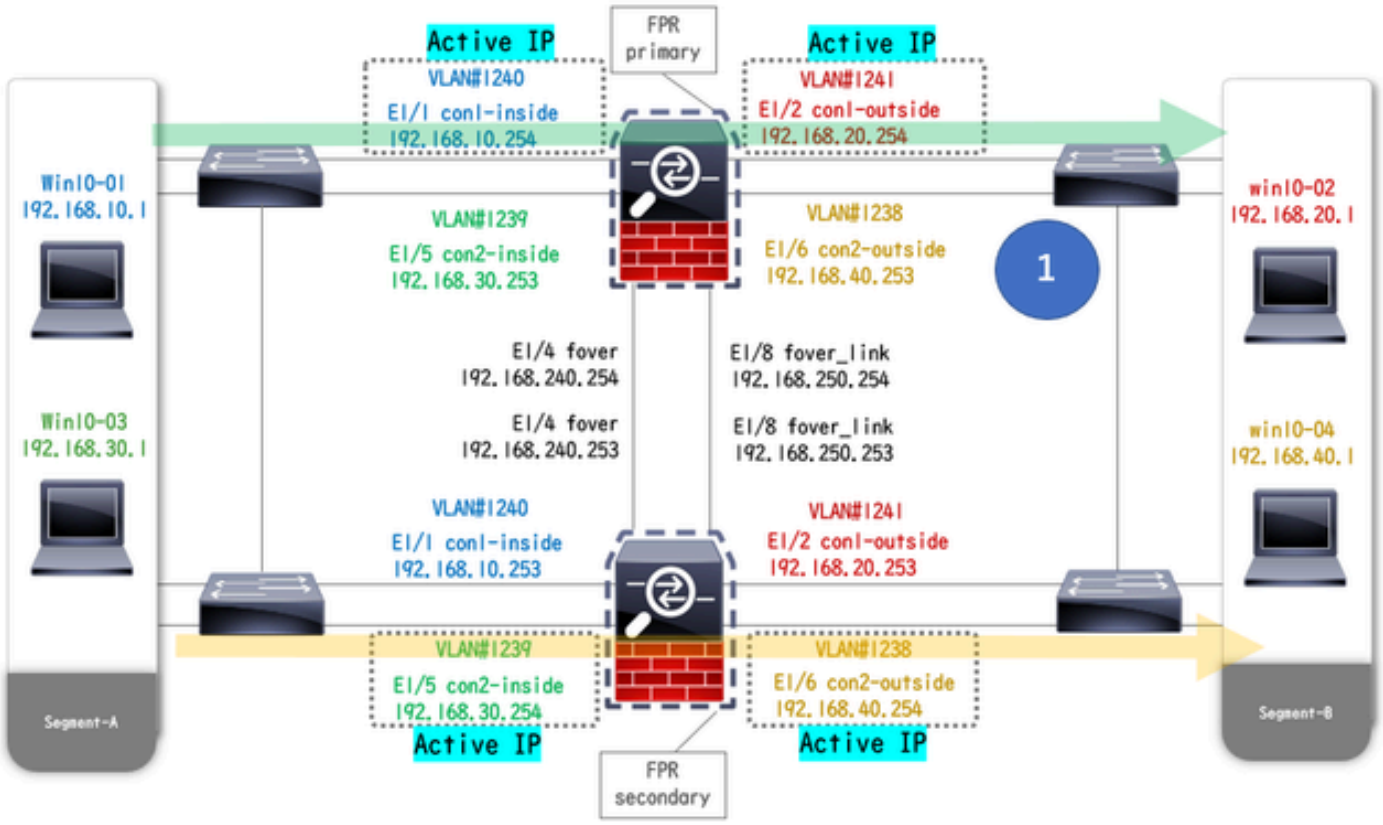
```
no failover active group 2
```



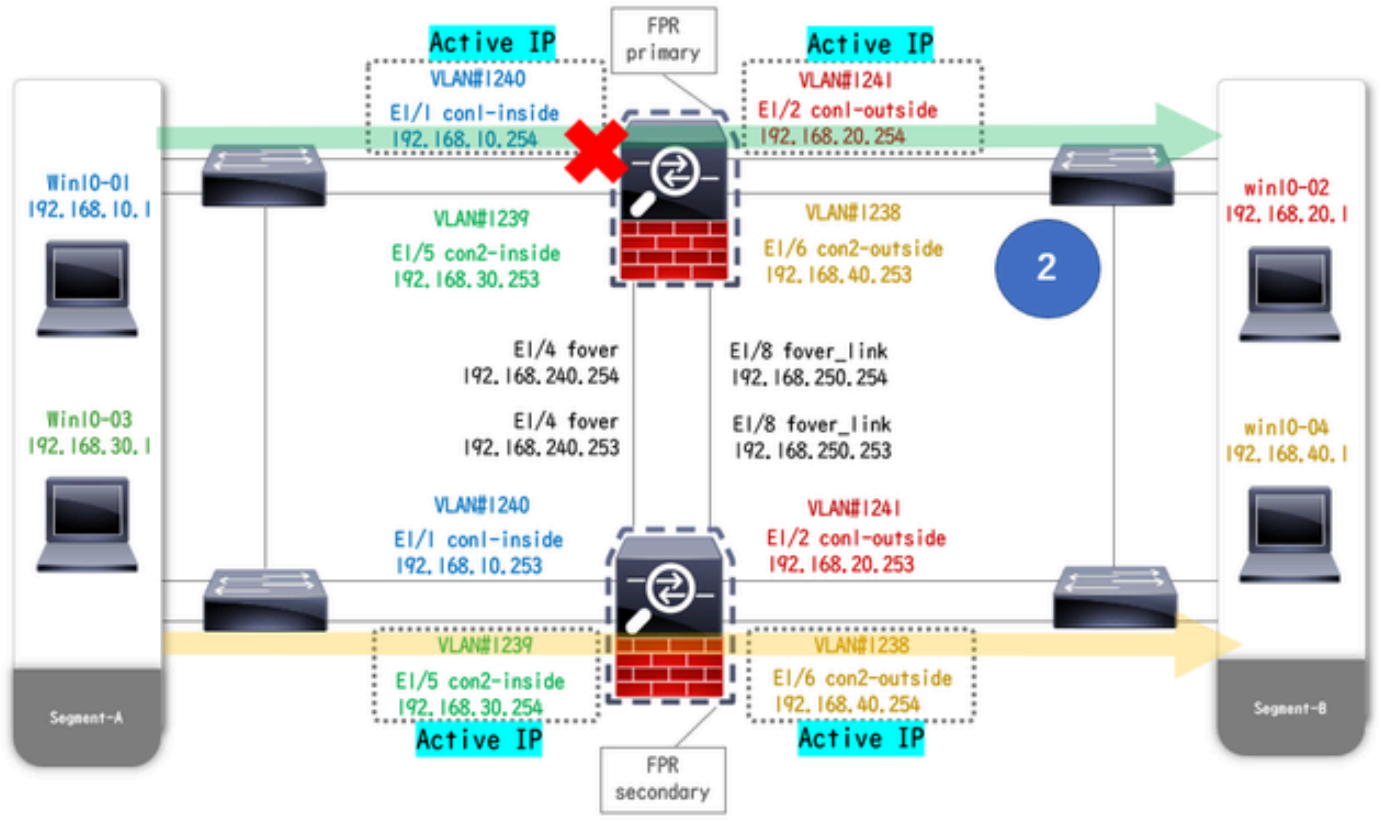
Nota: Si ejecuta este comando, el estado de failover coincide con la condición de flujo de tráfico 1.

Verificación

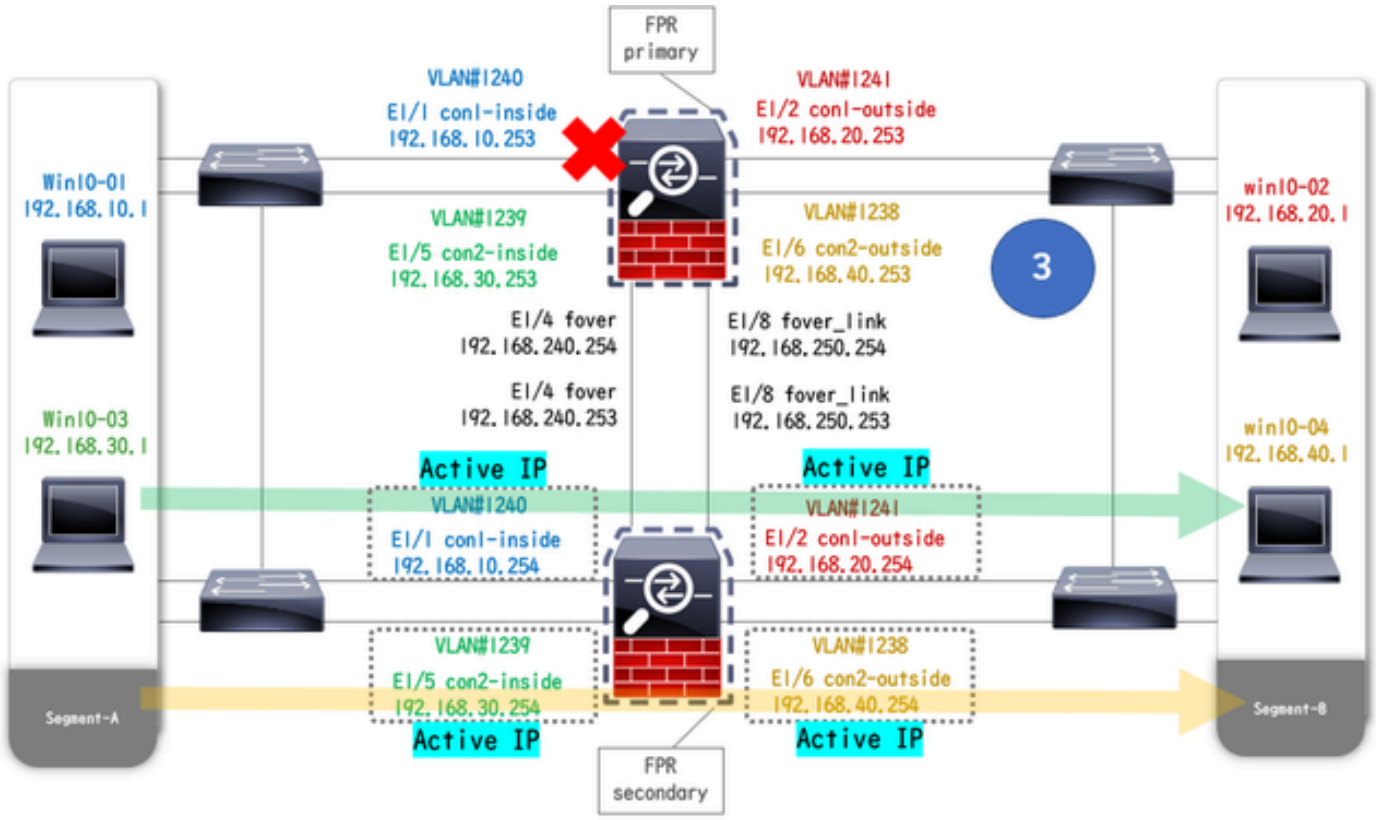
Cuando E1/1 se DESACTIVA, se dispara la conmutación por fallas del grupo 1 y las interfaces de datos en el lado en espera (Unidad Secundaria) toman el control de la dirección IP y MAC de la Interfaz Activa original, asegurando que el tráfico (conexión FTP en este documento) sea pasado continuamente por los ASA.



Antes del enlace



hacia abajoDurante el enlace hacia abajo



Conmutación por fallas activada

Paso 1. Iniciar conexión FTP de Win10-01 a Win10-02

Paso 2. Confirmar conexión FTP antes de conmutación por error

Ejecute changeto context con1 para conectar el contexto con1 desde el contexto del sistema. Confirme que se haya establecido una conexión FTP en ambas unidades ASA.

<#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
```

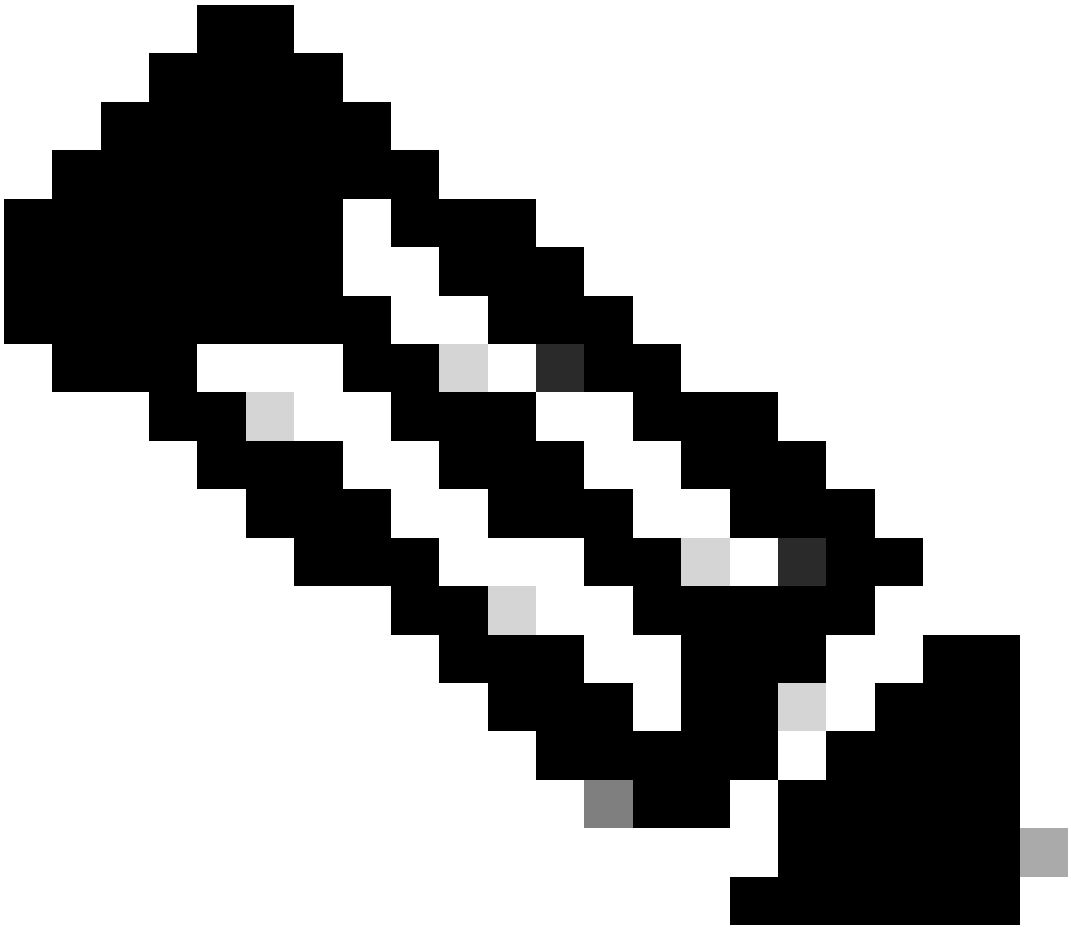
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

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

Paso 3. LinkDOWN E1/1 de la unidad primaria

Paso 4. Confirmar estado de failover

En el contexto del sistema, confirme que la conmutación por fallas ocurre en el grupo 1.



Nota: El estado del failover match traffic flow condition 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

Paso 5. Confirmar la conexión FTP después de la conmutación por error

Ejecute changeto context con1 para conectar el contexto con1 desde el contexto del sistema, confirme que la conexión FTP no se interrumpa.

<#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

Paso 6. Confirmar el comportamiento del tiempo de preferencia

LinkUP E1/1 de la unidad principal y espere 30 segundos (tiempo de preferencia), el estado de failover vuelve al estado original (coincidencia del flujo de tráfico en el patrón 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

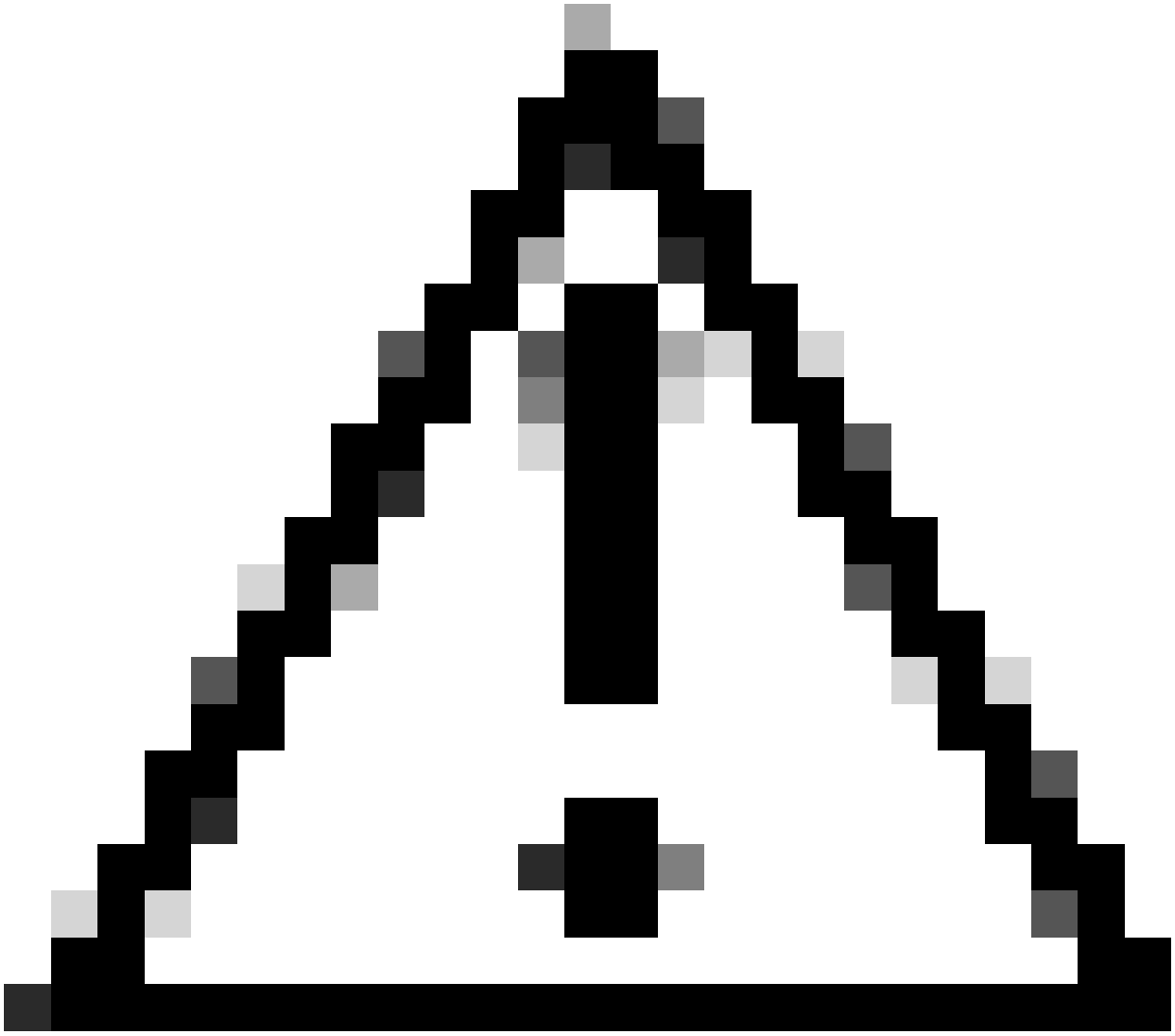
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

Dirección MAC virtual

En la conmutación por fallo activa/activa, siempre se utiliza la dirección MAC virtual (valor definido manualmente, valor generado automáticamente o valor predeterminado). La dirección MAC virtual activa está asociada a la interfaz activa.

Configuración manual de la dirección MAC virtual

Para configurar manualmente la dirección MAC virtual para las interfaces físicas, se puede utilizar el mac address comando o el mac-address comando (en el modo de configuración I/F). Este es un ejemplo de configuración manual de una dirección MAC virtual para la interfaz física E1/1.



Precaución: evite utilizar estos dos tipos de comandos dentro del mismo dispositivo.

<#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

O

<#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

Configuración automática de la dirección MAC virtual

También se admite la generación automática de direcciones MAC virtuales. Se puede lograr mediante el mac-address auto <prefix prefix> comando. El formato de la dirección MAC virtual es A2 xx.yyzz.zzzz, que se genera automáticamente.
A2: valor fijo
xx.yy: generado por el <prefix prefix> especificado en la opción de comando (el prefijo se convierte a hexadecimal y luego se inserta en orden inverso).
zz.zzzz: generado por un contador interno

Este es un ejemplo sobre la generación de direcciones MAC virtuales por **mac-address auto** comando para la interfaz.

<#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
```

Configuración predeterminada de la dirección MAC virtual

En caso de que no se establezca la generación automática o manual de una dirección MAC virtual, se utilizará la dirección MAC virtual predeterminada.

Para obtener más información sobre la dirección MAC virtual predeterminada, consulte la Command Default of mac address en la Guía de referencia de comandos de la serie ASA de Cisco Secure Firewall.

Actualizar

Puede lograr una actualización sin tiempo de inactividad de un par de conmutación por error Activo/Activo mediante CLI o ASDM. Para obtener más información, consulte Actualización de un Par de Failover Activo/Activo.

Información Relacionada

- Actualización de un Par de Failover Activo/Activo Usando la CLI
- Dirección MAC
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).