Sustitución de un firewall ASA en un par de failover activo/en espera

Contenido

Introducción

Este documento describe cómo reemplazar un firewall de Adaptive Security Appliance (ASA) por un par de failover activo/en espera.

Antecedentes

Los firewalls ASA admiten dos configuraciones de conmutación por fallo, conmutación por fallo activa/activa y conmutación por fallo activa/en espera.

Hay 2 firewalls:

- firewall-a es principal/activo
- firewall-b es secundario/en espera

Diferencia entre las Unidades Primarias y Secundarias en la Configuración de Failover

Este comando significa que este firewall siempre envía la configuración activa al firewall secundario.

```
# failover lan unit primary
```

Este comando significa que este firewall siempre recibe la configuración activa del firewall principal.

```
# failover lan unit secondary
```

Diferencia entre las Unidades Activas y en Espera en la Configuración de Failover

Este comando significa que este firewall es el firewall activo en ejecución en el par de failover.

```
# failover active
```

Este comando significa que este firewall es el que está en espera ejecutando un firewall en el par de failover.

```
# failover standby
```

Reemplace la falla del firewall secundario

1. Valide que el firewall principal esté activo y en línea. Por ejemplo:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Primary - Active
        Active time: 2204 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Secondary - Failed
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Apague y elimine físicamente el firewall secundario.

3. Agregue físicamente el nuevo firewall secundario y enciéndalo.

4. Una vez que el nuevo firewall secundario esté activo con la configuración de fábrica predeterminada, habilite el link de failover,`no shutdown`el link físico de failover.

Ejemplo:

```
firewall-a/pri/act#conf t
firewall-a/pri/act#(config)#interface Port-channel1
firewall-a/pri/act#(config-if)#no shutdown
firewall-a/pri/act#(config)#exit
firewall-a/pri/act#
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#interface Port-channel1
firewall-b/sec/stby#(config-if)#no shutdown
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
```

5. Configure los comandos de failover. Por ejemplo:

```
firewall-a/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/pri/act#

firewall-b/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/sec/stby#
```

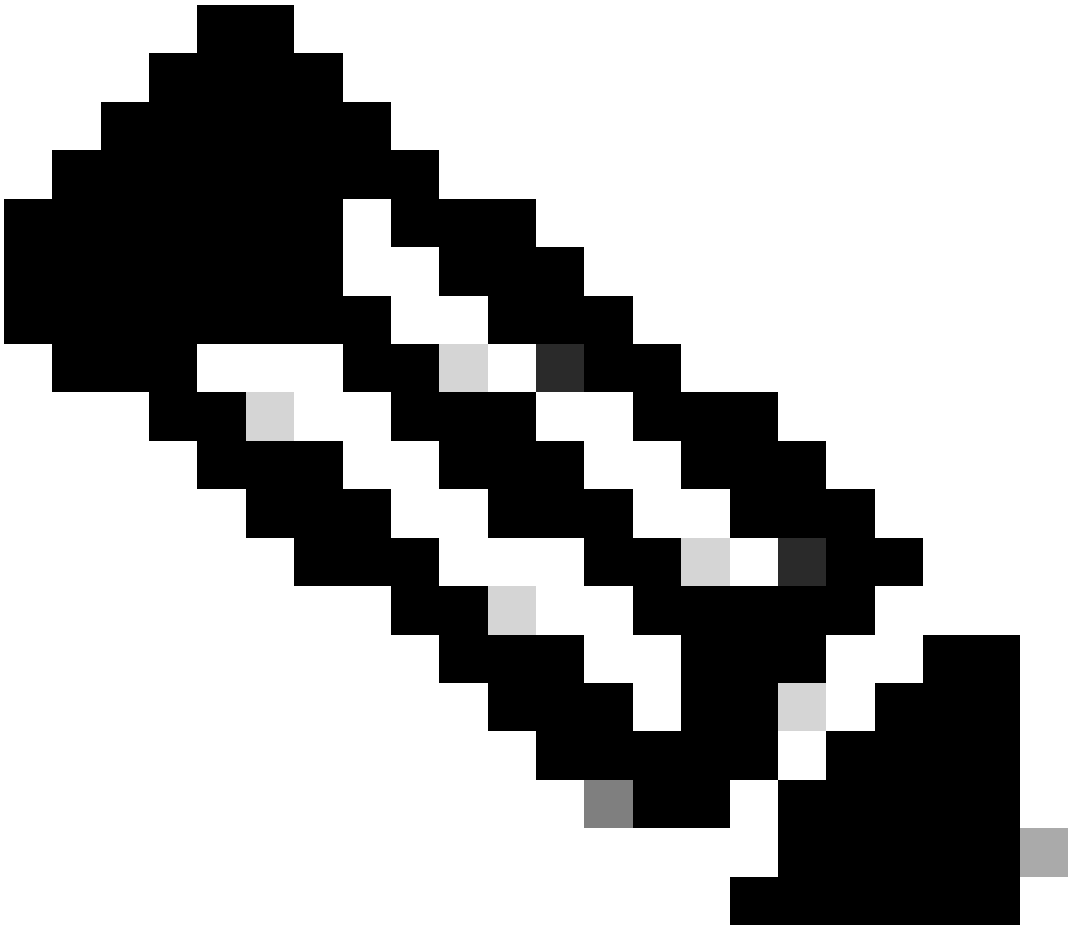
6. Active la conmutación por fallo en el nuevo firewall secundario. Por ejemplo:

```
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#failover
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
firewall-b/sec/stby# sh run | inc fail
```

failover
firewall-b/sec/stby#

7. Espere a que la configuración activa se sincronice con la nueva unidad y valide el estado de conmutación por error correcto. Por ejemplo:

firewall-a/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-a/pri/act#
firewall-b/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-b/sec/stby#



Nota: Observe que el firewall principal (firewall-a) envía la configuración al firewall

---

secundario (firewall-b).

8. Guarde la configuración en el primario/activo y valide la memoria de escritura en el nuevo secundario/en espera. Por ejemplo:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342
64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act#
firewall-b/sec/stby#
May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
firewall-b/sec/stby#
```

9. Valide que el par de conmutación por fallo esté activo/activo en ambos firewalls. Por ejemplo:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Primary - Active
        Active time: 71564 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)

firewall-b/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
    Other host: Primary - Active
        Active time: 71635 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1: Normal (Not-Monitored)
          Interface outide (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
```

Reemplace la falla del firewall principal

1. Valide que el firewall secundario esté activo y en línea. Por ejemplo:

```
firewall-b/sec/act# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 19:54:29 GMT May 23 2023
    This host: Secondary - Active
        Active time: 2204 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.1): Normal (Not-Monitored)
          Interface outside (10.1.1.1): Normal (Not-Monitored)
          Interface management (10.2.2.1): Normal (Not-Monitored)
    Other host: Primary - Failed
        Active time: 0 (sec)
        slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
          Interface inside (10.0.0.2): Normal (Not-Monitored)
          Interface outside (10.1.1.2): Normal (Not-Monitored)
          Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Apague y elimine físicamente el firewall principal.
3. Agregue físicamente el nuevo firewall principal y enciéndalo.
4. Ahora, el nuevo firewall principal se activa con la configuración de fábrica predeterminada.
5. Habilite el link de failover, no shutdown el link físico de failover. Por ejemplo:

```
firewall-a/pri/stby#conf t
firewall-a/pri/stby#(config)#interface Port-channel1
firewall-a/pri/stby#(config-if)#no shutdown
firewall-a/pri/stby#(config)#exit
firewall-a/pri/stby#

firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#interface Port-channel1
firewall-b/sec/act#(config-if)#no shutdown
firewall-b/sec/act#(config)#exit
firewall-b/sec/act#
```

6. Guardar configuración. Escriba la memoria en el firewall secundario/activo y asegúrese de que el secundario de la unidad lan de failover esté en la configuración de inicio.

Ejemplo:

```
firewall-b/sec/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-b/sec/act# show start | inc unit
failover lan unit secondary
firewall-b/sec/act#
```

7. Configurar comandos de conmutación por error.
    1. En el firewall secundario/activo, primero debe establecer el comando failover lan unit primary para asegurarse de que la configuración activa se transfiere desde el firewall secundario/activo al nuevo firewall primario/en espera de la configuración predeterminada. Por ejemplo:

```
firewall-b/sec/act# sh run | inc unit
failover lan unit secondary
firewall-b/sec/act#

firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#failover lan unit primary
firewall-b/sec/act#(config)#exit
firewall-b/sec/act# sh run | inc unit
```

```
failover lan unit primary
firewall-b/pri/act#
```

b. Valide la configuración de failover en ambos dispositivos. Por ejemplo:

```
firewall-b/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/pri/act#

firewall-a/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/sec/stby#
```

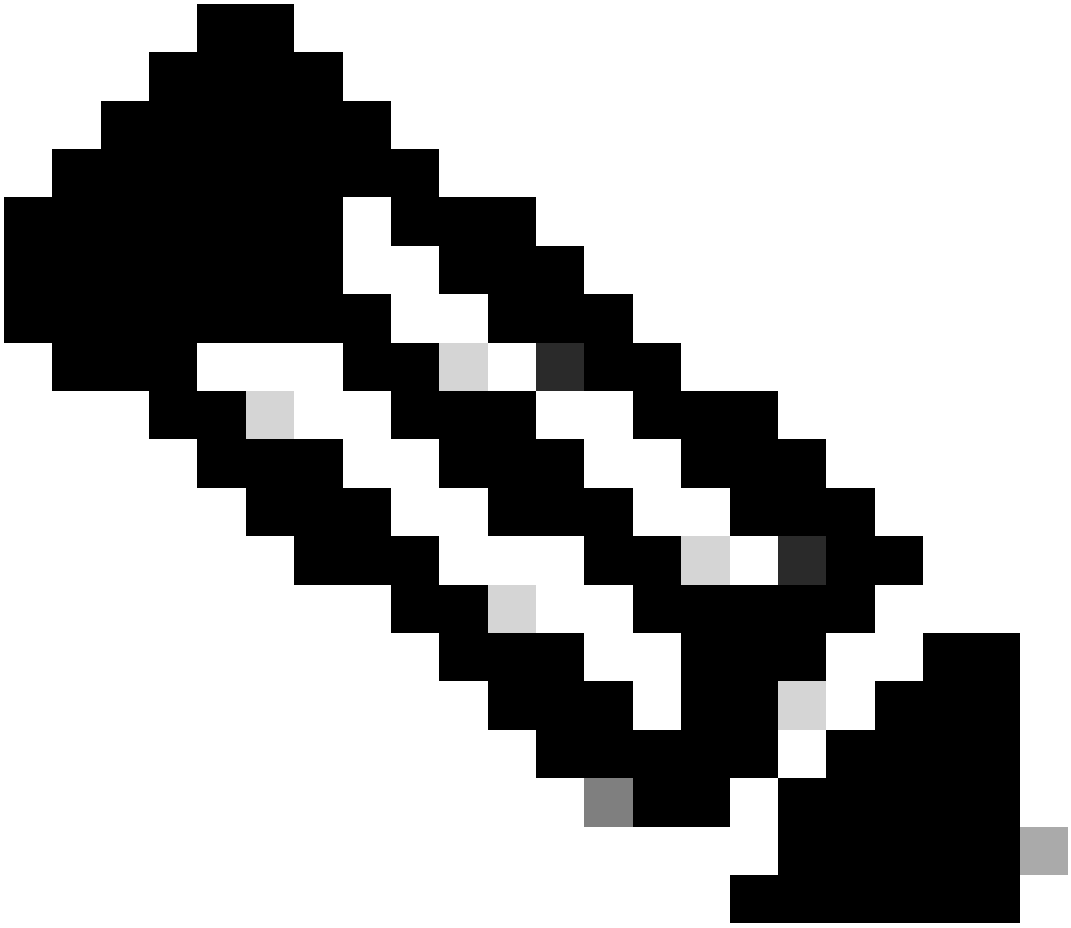
8. Active la conmutación por fallo en el nuevo firewall principal. Por ejemplo:

```
firewall-a/sec/stby#conf t
firewall-a/sec/stby#(config)#failover
firewall-a/sec/stby#(config)#exit
firewall-a/sec/stby#

firewall-a/sec/stby# sh run | inc fail
failover
firewall-a/sec/stby#
```

9. Espere a que la configuración activa se sincronice con la nueva unidad y valide el estado de conmutación por error correcto. Por ejemplo:

```
firewall-b/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-b/pri/act#
firewall-a/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-a/sec/stby#
```



Nota: Observe que el firewall principal (firewall-b) envía la configuración al firewall secundario (firewall-a). No escriba memoria en el firewall principal/activo (firewall-b).

10. Vuelva a cargar el firewall principal/activo (firewall-b) para que se inicie como firewall secundario/en espera.

```
firewall-b/pri/act#reload
```

11. Inmediatamente después de ejecutar el comando "firewall-b reload" (espere 15 segundos), cambie al nuevo firewall primario (firewall-a) e ingrese el comando failover lan unit primary, seguido por write memory.

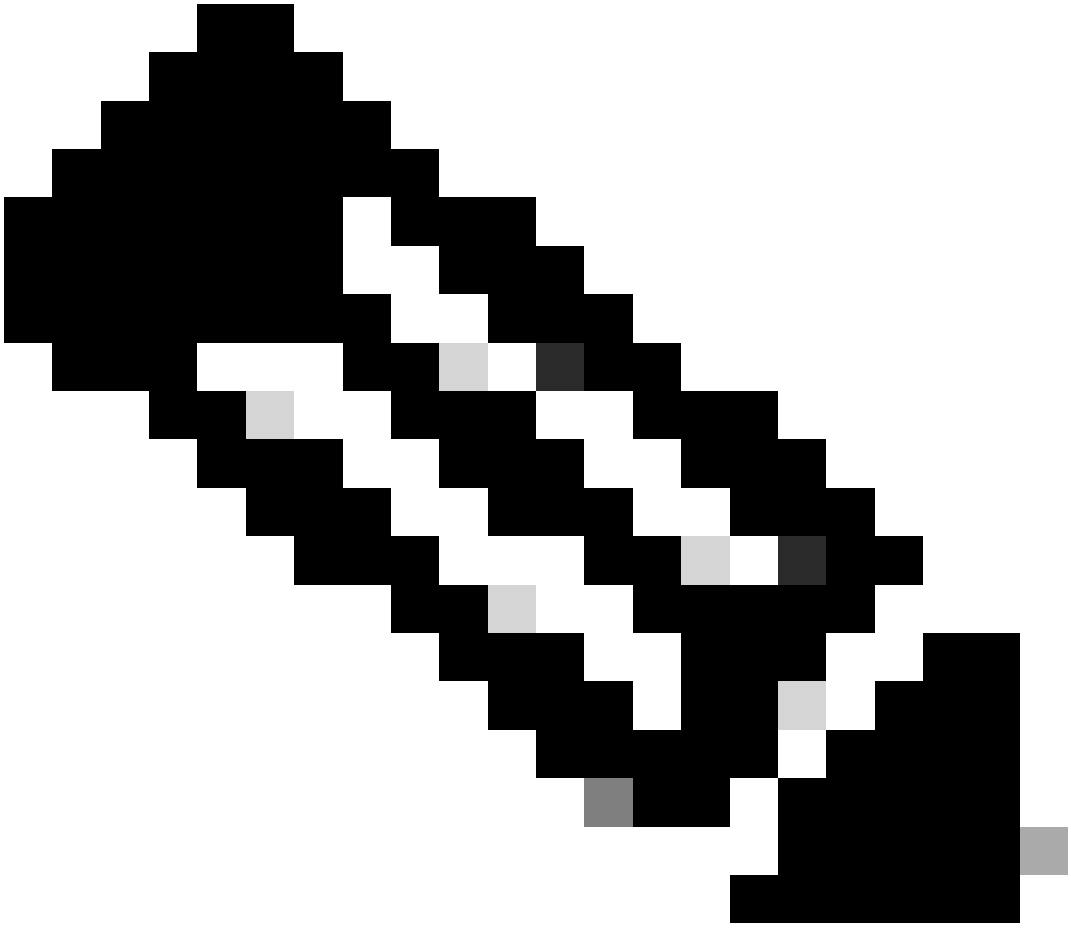
```
firewall-a/sec/act#conf t
firewall-a/sec/act#(config)#failover lan unit primary
```

```
firewall-a/sec/act#(config)#exit
firewall-a/sec/act# sh run | inc unit
failover lan unit primary
firewall-a/pri/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act# show start | inc unit
failover lan unit primary
firewall-a/pri/act#
```

12. Espere a que el firewall-b se inicie por completo y se una al par de failover como secundario/en espera. Por ejemplo:

```
firewall-a/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-a/pri/act#
firewall-b/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-b/sec/stby#
```



Nota: Tenga en cuenta que el firewall principal (firewall-a) envía la configuración al firewall secundario (firewall-b).

13. Guarde la configuración, escriba la memoria en el primario/activo y valide la memoria de escritura en el nuevo secundario/en espera. Por ejemplo:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act#

firewall-b/sec/stby#
May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
```

May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
firewall-b/sec/stby#

14. Valide que el par de conmutación por fallas esté activo/activo en ambos firewalls. Por ejemplo:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
   This host: Primary - Active
      Active time: 71564 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
        Interface inside (10.0.0.1): Normal (Not-Monitored)
        Interface outside (10.1.1.1): Normal (Not-Monitored)
        Interface management (10.2.2.1): Normal (Not-Monitored)
   Other host: Secondary - Standby Ready
      Active time: 0 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
        Interface inside (10.0.0.2): Normal (Not-Monitored)
        Interface outside (10.1.1.2): Normal (Not-Monitored)
        Interface management (10.2.2.2): Normal (Not-Monitored)

firewall-b/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
   This host: Secondary - Standby Ready
      Active time: 0 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
        Interface inside (10.0.0.2): Normal (Not-Monitored)
        Interface outside (10.1.1.2): Normal (Not-Monitored)
        Interface management (10.2.2.2): Normal (Not-Monitored)
   Other host: Primary - Active
      Active time: 71635 (sec)
      slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
```

Interface inside (10.0.0.1: Normal (Not-Monitored)
Interface outide (10.1.1.1): Normal (Not-Monitored)
Interface management (10.2.2.1): Normal (Not-Monitored)

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).