將ASA防火牆更換為活動/備用故障切換對

目錄

簡介

本文檔介紹如何使用主用/備用故障切換對替換自適應安全裝置(ASA)防火牆。

背景資訊

ASA防火牆支援兩種故障切換配置：活動/活動故障切換和活動/備用故障切換。

共有兩個防火牆：

- firewall-a為主用/主用
- firewall-b為輔助/備用

故障切換配置中的主要裝置和輔助裝置之間的差異

此命令意味著此防火牆始終將活動配置推送到輔助防火牆。

failover lan unit primary

此命令意味著此防火牆始終從主防火牆接收活動配置。

failover lan unit secondary

故障切換配置中的主用裝置和備用裝置之間的差異

此命令表示此防火牆是故障轉移對中的活動運行防火牆。

failover active

此命令表示此防火牆是備用防火牆，在故障轉移對中運行防火牆。

failover standby

更換輔助防火牆故障

1. 驗證主防火牆是否處於活動狀態且處於聯機狀態。舉例來說：

```
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. 關閉並實際移除次要防火牆。

3. 以物理方式增加新的輔助防火牆並打開其電源。

4. 當新的輔助防火牆以預設出廠配置處於活動狀態後，啟用故障切換鏈路，即no shutdown故障切換物理鏈路。

範例：

```
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. 配置故障切換命令。舉例來說：

```
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#
```
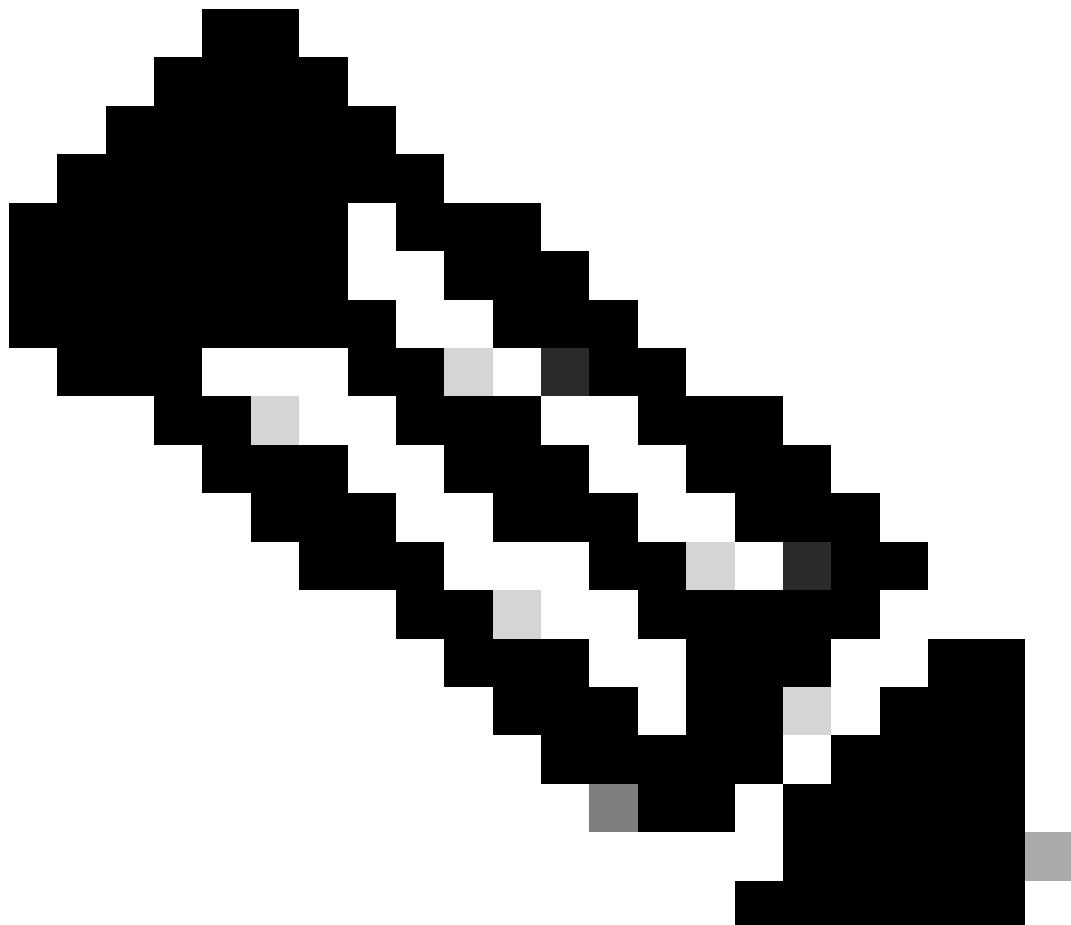
6. 在新的輔助防火牆上啟用故障切換。舉例來說：

```
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. 等待活動配置同步到新裝置並驗證正確的故障切換狀態。舉例來說：

```
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#
```

注意：請注意，主防火牆(firewall-a)將配置傳送到輔助防火牆(firewall-b)。

---

8. 儲存主要/作用中的組態，並驗證新的輔助/待命的寫入記憶體。舉例來說：

```
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. 驗證兩個防火牆上的故障轉移對是否都處於up/up活動狀態。舉例來說：

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)
```

替換主防火牆故障

1. 驗證輔助防火牆是否處於活動狀態且處於聯機狀態。舉例來說：

```
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. 關閉並實際移除主防火牆。
3. 以物理方式增加新的主防火牆並打開其電源。
4. 現在，新的主防火牆會使用預設出廠配置啟用。
5. 啟用故障切換鏈路，no shutdown故障切換物理鏈路。舉例來說：

```
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. 儲存配置。在輔助/活動防火牆上寫入記憶體，並確保啟動配置中有failover lan unit secondary。

範例：

```
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. 配置故障切換命令。
    1. 在輔助/主用防火牆上，必須首先設定failover lan unit primary命令，以確保主用配置從輔助/主用防火牆推進到新的預設配置主/備用防火牆。舉例來說：

```
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. 驗證兩台裝置上的故障切換配置。舉例來說：

```
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#
```
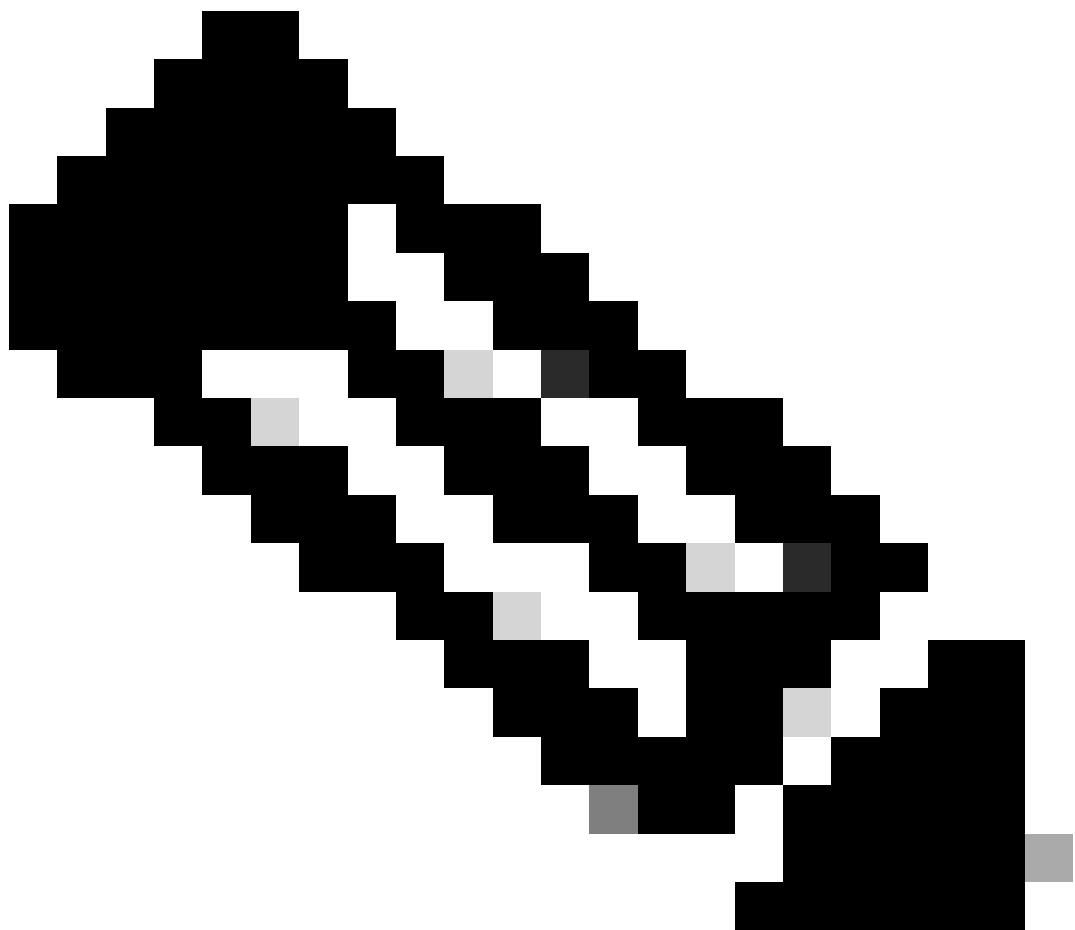
8. 在新主防火牆上啟用故障切換。舉例來說：

```
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. 等待活動配置同步到新裝置並驗證正確的故障切換狀態。舉例來說：

```
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#
```

注意：請注意，主防火牆(firewall-b)將配置傳送到輔助防火牆(firewall-a)。請勿在現在的主用/主用防火牆(firewall-b)上寫入記憶體。

---

10. 重新載入目前的主要/作用中防火牆(firewall-b)，使其以次要/待命防火牆的身份進行備份。

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

11. 執行「firewall-b reload」命令（等待15秒）後，立即切換到新的主防火牆(firewall-a)，並輸入failover lan unit primary命令，然後輸入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
```
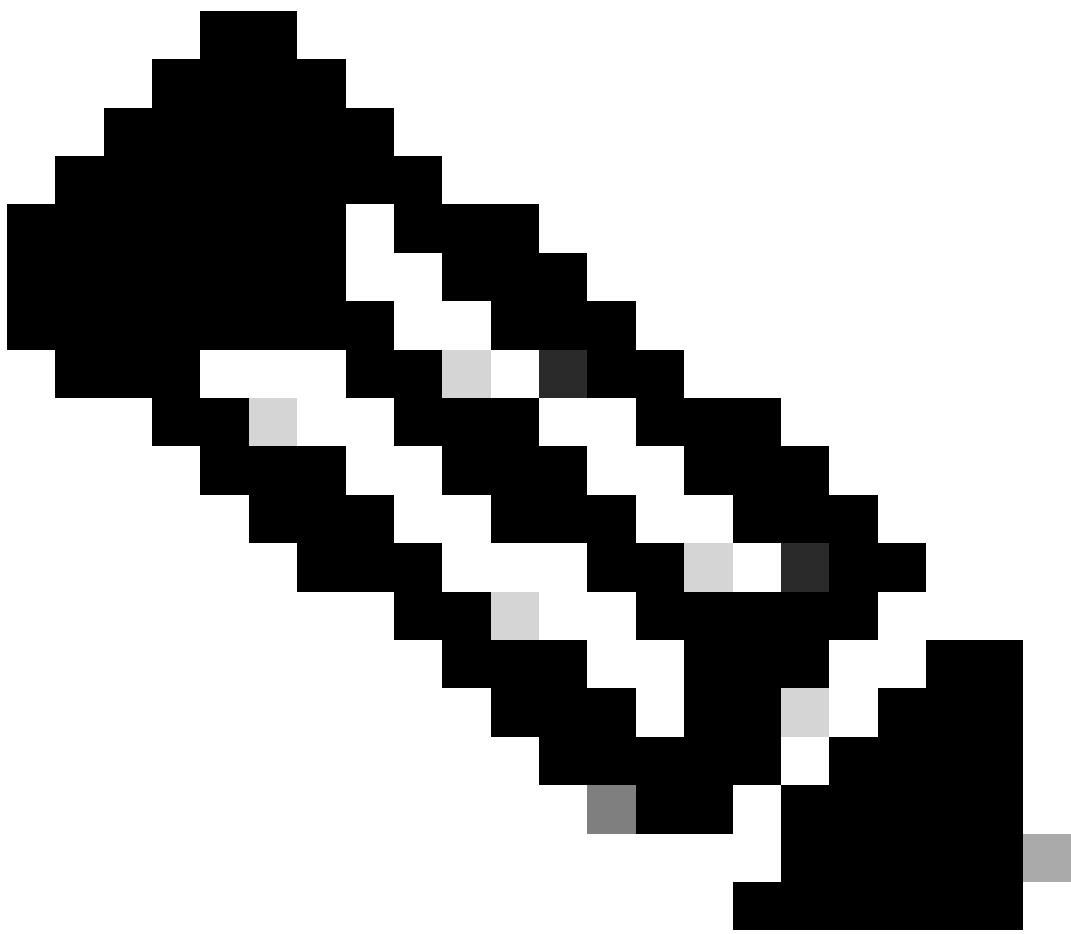
```
failover lan unit primary
firewall-a/pri/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342

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. 等待firewall-b完全啟動，並將故障轉移對作為輔助/備用裝置加入。舉例來說：

```
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#
```

注意：請注意，主防火牆(firewall-a)將配置傳送到輔助防火牆(firewall-b)。

13. 儲存配置，在主用/主用上寫入記憶體，並驗證新輔助/備用上的寫入記憶體。舉例來說：

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. 驗證兩個防火牆上的故障轉移對是否都處於up/up活動狀態。舉例來說：

```
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)
```