

Sostituzione di un firewall ASA in una coppia di failover attivo/standby

Sommario

[Introduzione](#)

[Premesse](#)

[Differenza tra le unità primarie e secondarie nella configurazione di failover](#)

[Differenza tra le unità attive e in standby nella configurazione di failover](#)

[Sostituire l'errore del firewall secondario](#)

[Sostituire l'errore del firewall primario](#)

Introduzione

In questo documento viene descritto come sostituire un firewall ASA (Adaptive Security Appliance) con una coppia di failover attivo/standby.

Premesse

I firewall ASA supportano due configurazioni di failover, il failover attivo/attivo e il failover attivo/standby.

Sono disponibili 2 firewall:

- firewall-a è principale/attivo
- firewall-b è secondario/in standby

Differenza tra le unità primarie e secondarie nella configurazione di failover

Questo comando indica che il firewall esegue sempre il push della configurazione attiva nel firewall secondario.

```
# failover lan unit primary
```

Questo comando indica che il firewall riceve sempre la configurazione attiva dal firewall primario.

```
# failover lan unit secondary
```

Differenza tra le unità attive e in standby nella configurazione di failover

Questo comando indica che il firewall è il firewall attivo in esecuzione nella coppia di failover.

```
# failover active
```

Questo comando indica che il firewall è in standby e esegue un firewall nella coppia di failover.

```
# failover standby
```

Sostituire l'errore del firewall secondario

1. Verificare che il firewall primario sia attivo e in linea. Ad esempio:

```
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. Arrestare e rimuovere fisicamente il firewall secondario.

3. Aggiungere fisicamente il nuovo firewall secondario e accenderlo.

4. Una volta che il nuovo firewall secondario è attivo con la configurazione predefinita di fabbrica, abilitare il collegamento di failover, ovvero `no shutdown` il collegamento fisico di failover.

Esempio:

```
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. Configurare i comandi di failover. Ad esempio:

```
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#
```

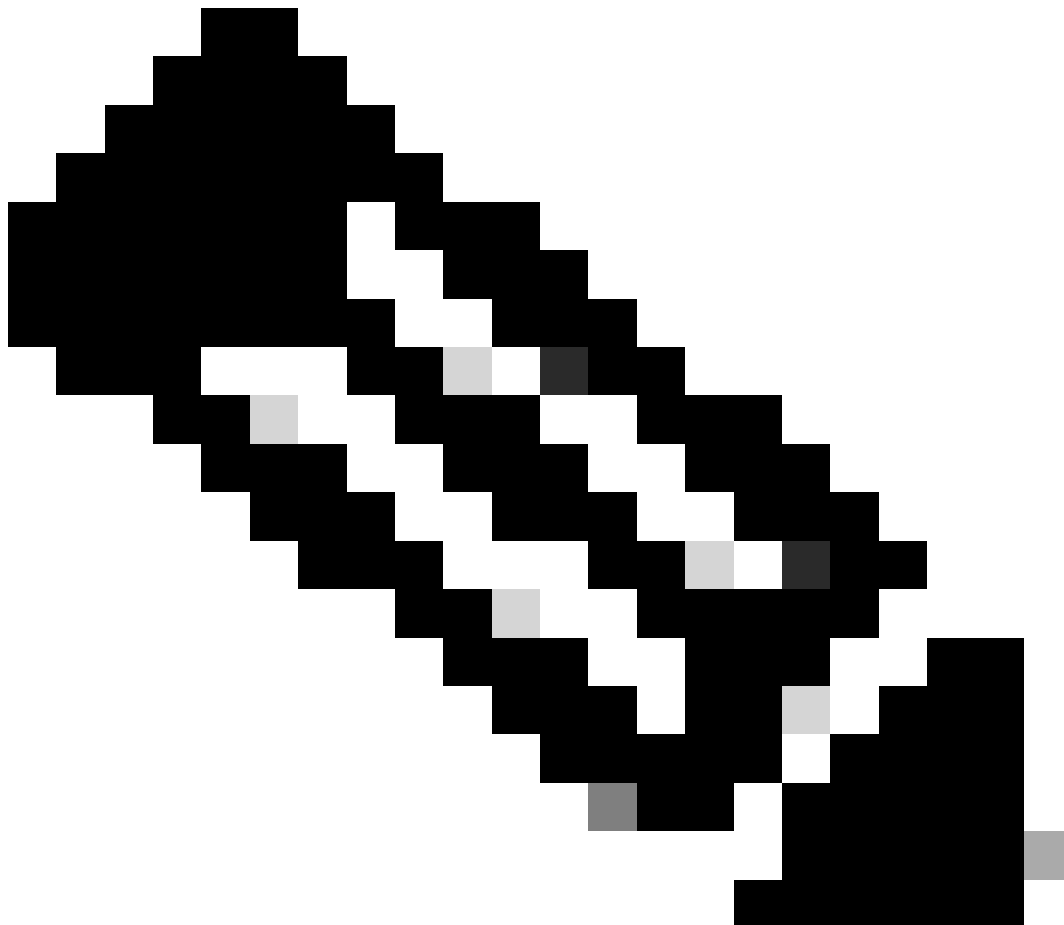
```
firewall-b/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/sec/stby#
```

6. Abilitare il failover sul nuovo firewall secondario. Ad esempio:

```
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. Attendere che la configurazione attiva venga sincronizzata con la nuova unità e convalidare lo stato di failover corretto. Ad esempio:

```
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: si noti che il firewall principale (firewall-a) invia la configurazione al firewall secondario (firewall-b).

8. Salvare la configurazione sul database primario/attivo e convalidare la memoria di scrittura sul nuovo database secondario/standby. Ad esempio:

```
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. Verificare che la coppia di failover sia attiva/attiva su entrambi i firewall. Ad esempio:

```
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 outside (10.1.1.1): Normal (Not-Monitored)
Interface management (10.2.2.1): Normal (Not-Monitored)

Sostituire l'errore del firewall primario

1. Verificare che il firewall secondario sia attivo e in linea. Ad esempio:

```
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. Arrestare e rimuovere fisicamente il firewall principale.

3. Aggiungere fisicamente il nuovo firewall principale e accenderlo.

4. A questo punto, il nuovo firewall principale diventa attivo con la configurazione predefinita di fabbrica.
5. Abilitare il collegamento di failover, senza arrestare il collegamento fisico di failover. Ad esempio:

```
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. Salvare la configurazione. Scrivere la memoria sul firewall secondario/attivo e verificare che l'unità secondaria della LAN di failover si trovi nella configurazione di avvio.

Esempio:

```
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. Configurare i comandi di failover.

1. Sul firewall secondario/attivo, impostare prima il comando failover lan unit primary per garantire che la configurazione attiva venga trasferita dal firewall secondario/attivo al nuovo firewall predefinito per la configurazione primaria/standby. Ad esempio:

```
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. Convalidare la configurazione di failover su entrambi i dispositivi. Ad esempio:

```
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. Abilitare il failover sul nuovo firewall primario. Ad esempio:

```
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. Attendere che la configurazione attiva venga sincronizzata con la nuova unità e convalidare lo stato di failover corretto. Ad esempio:

```
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: si noti che il firewall principale (firewall-b) invia la configurazione al firewall secondario (firewall-a). Non scrivere memoria sul firewall attivo/primario (firewall-b).

-
10. Ricaricare il firewall attivo/primario (firewall-b) in modo che venga avviato come firewall secondario/standby.

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

11. Subito dopo aver eseguito il comando "firewall-b reload" (attendere 15 secondi), passare al nuovo firewall principale (firewall-a) e immettere il comando failover lan unit primary, quindi scrivere memoria.

```
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. Attendere che il firewall-b si avvii completamente e si unisca alla coppia di failover come database secondario/standby. Ad esempio:

```
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: il firewall principale (firewall-a) invia la configurazione al firewall secondario (firewall-b).

13. Salvare la configurazione, scrivere la memoria sul database primario/attivo e convalidare la memoria di scrittura sul nuovo database secondario/standby. Ad esempio:

```
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. Verificare che la coppia di failover sia attiva/attiva su entrambi i firewall. Ad esempio:

```
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 outside (10.1.1.1): Normal (Not-Monitored)
```

Interface management (10.2.2.1): Normal (Not-Monitored)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).