Substituir um firewall ASA em um par de failover ativo/em espera

Contents

Introdução

Este documento descreve como substituir um firewall Adaptive Security Appliance (ASA) por um par de failover ativo/standby.

Informações de Apoio

Os firewalls ASA oferecem suporte a duas configurações de failover, failover ativo/ativo e failover ativo/standby.

Há 2 firewalls:

- firewall-a é principal/ativo
- o firewall-b é secundário/em espera

Diferença entre as Unidades Primárias e Secundárias na Configuração de Failover

Esse comando significa que esse firewall sempre envia a configuração ativa para o firewall secundário.

```
# failover lan unit primary
```

Esse comando significa que esse firewall sempre recebe a configuração ativa do firewall principal.

```
# failover lan unit secondary
```

Diferença entre as Unidades Ativas e em Espera na Configuração de Failover

Esse comando significa que esse firewall é o firewall ativo em execução no par de failover.

```
# failover active
```

Esse comando significa que esse firewall é o standby que executa um firewall no par de failover.

```
# failover standby
```

Substitua a falha do firewall secundário

1. Verifique se o firewall principal está ativo e on-line. Por exemplo:

```
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. Desligue e remova fisicamente o firewall secundário.

3. Adicione fisicamente o novo firewall secundário e ligue-o.

4. Quando o novo firewall secundário estiver ativo com a configuração de fábrica padrão, habilite o link de failover,no shutdowno link físico de failover.

Exemplo:

```
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 os comandos de failover. Por exemplo:

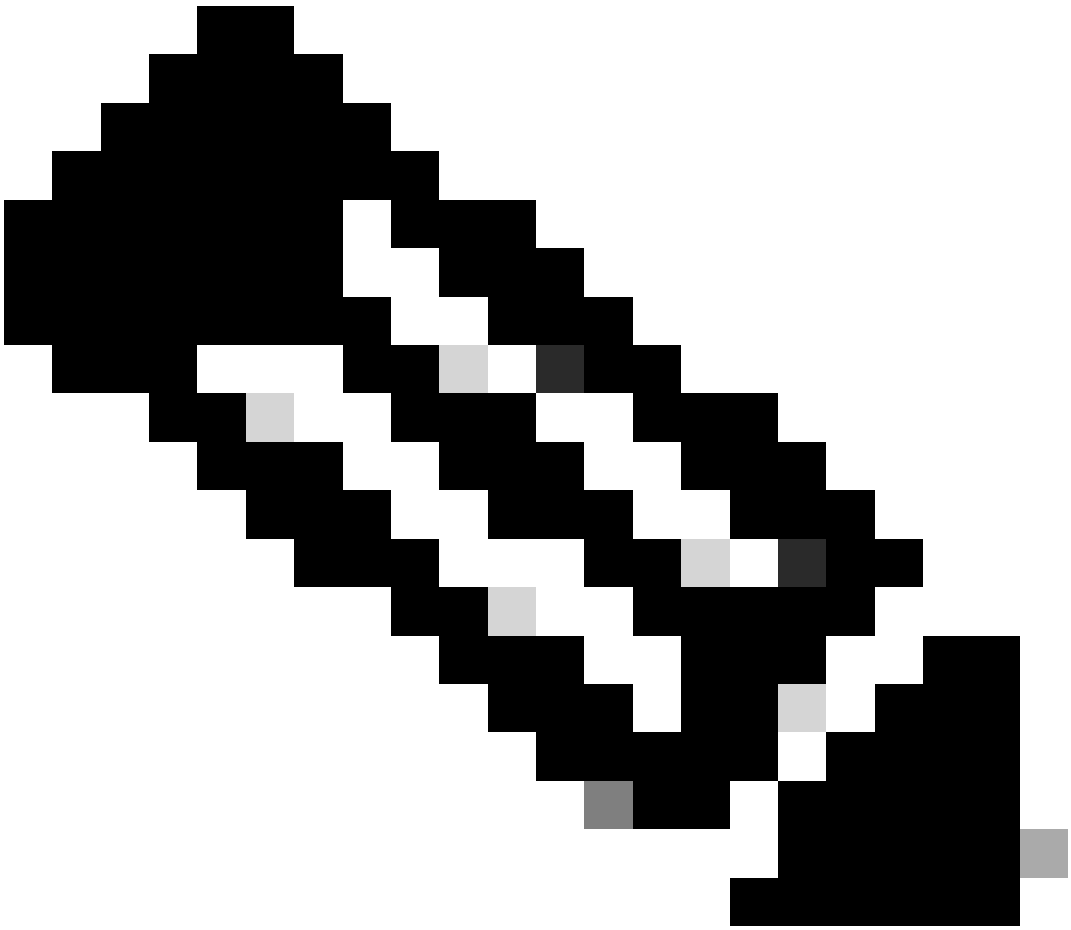
```
firewall-a/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/pri/act#

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. Ative o failover no novo firewall secundário. Por exemplo:

```
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. Aguarde até que a configuração ativa seja sincronizada com a nova unidade e valide o estado de failover correto. Por exemplo:

```
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#
```



Observação: observe que o firewall principal (firewall-a) envia a configuração para o firewall secundário (firewall-b).

---

8. Salve a configuração no principal/ativo e valide a memória de gravação no novo secundário/standby. Por exemplo:

```
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. Verifique se o par de failover está ativo/ativo em ambos os firewalls. Por exemplo:

```
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)
```

Substitua a falha principal do firewall

1. Valide se o firewall secundário está ativo e online. Por exemplo:

```
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. Desligue e remova fisicamente o firewall principal.
3. Adicione fisicamente o novo firewall principal e ligue-o.

4. Agora, o novo firewall principal fica ativo com a configuração padrão de fábrica.
5. Ative o link de failover, sem desligamento do link físico de failover. Por exemplo:

```
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. Salvar configuração. Grave memória no firewall secundário/ativo e verifique se o failover lan unit secondary está na configuração de inicialização.

Exemplo:

```
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 failover.
    1. No firewall secundário/ativo, você deve primeiro definir o comando failover lan unit primary para garantir que a configuração ativa seja enviada do firewall secundário/ativo para a nova configuração padrão do firewall principal/standby. Por exemplo:

```
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 a configuração de failover em ambos os dispositivos. Por exemplo:

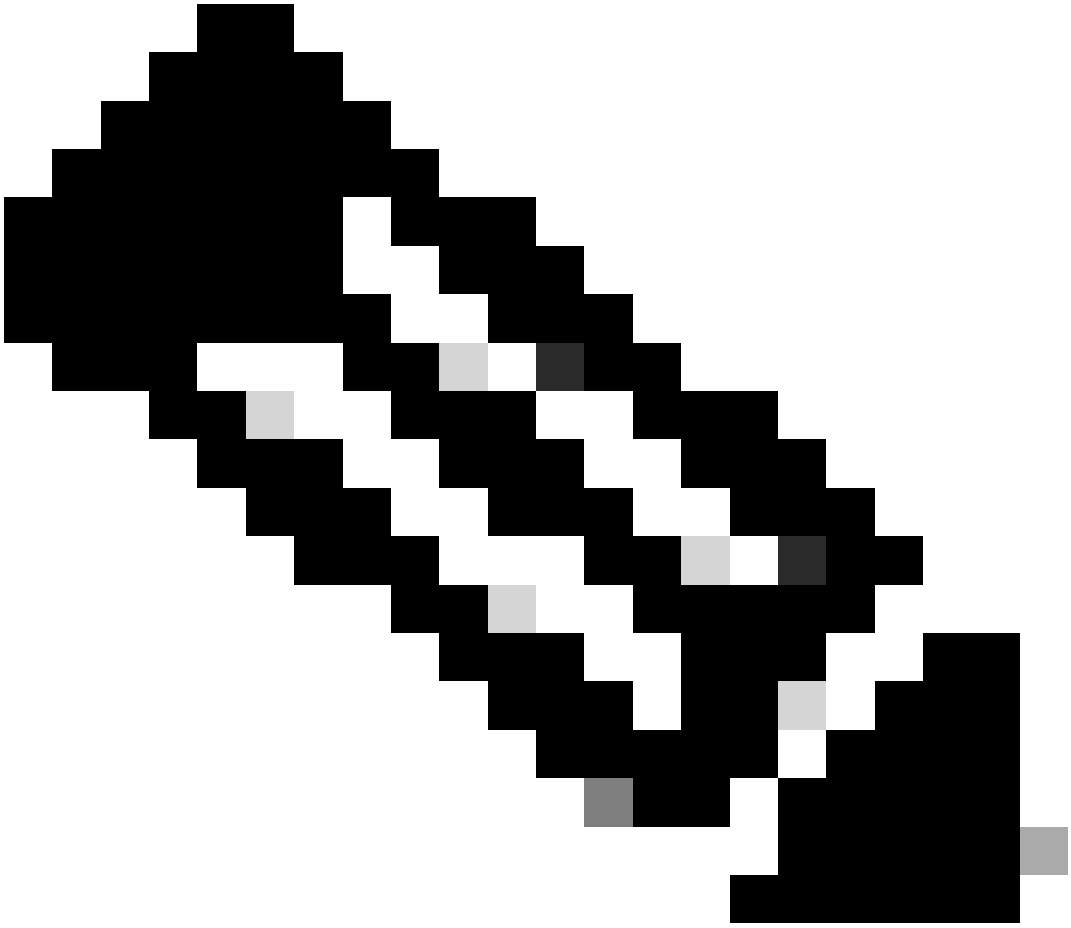
```
firewall-b/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/pri/act#

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. Habilite o failover no novo firewall primário. Por exemplo:

```
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. Aguarde até que a configuração ativa seja sincronizada com a nova unidade e valide o estado de failover correto. Por exemplo:

```
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#
```



Observação: observe que o firewall principal (firewall-b) envia a configuração para o firewall secundário (firewall-a). Não grave memória no firewall primário/ativo (firewall-b).

10. Recarregue o firewall agora principal/ativo (firewall-b) para que ele seja reinicializado como o firewall secundário/em espera.

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

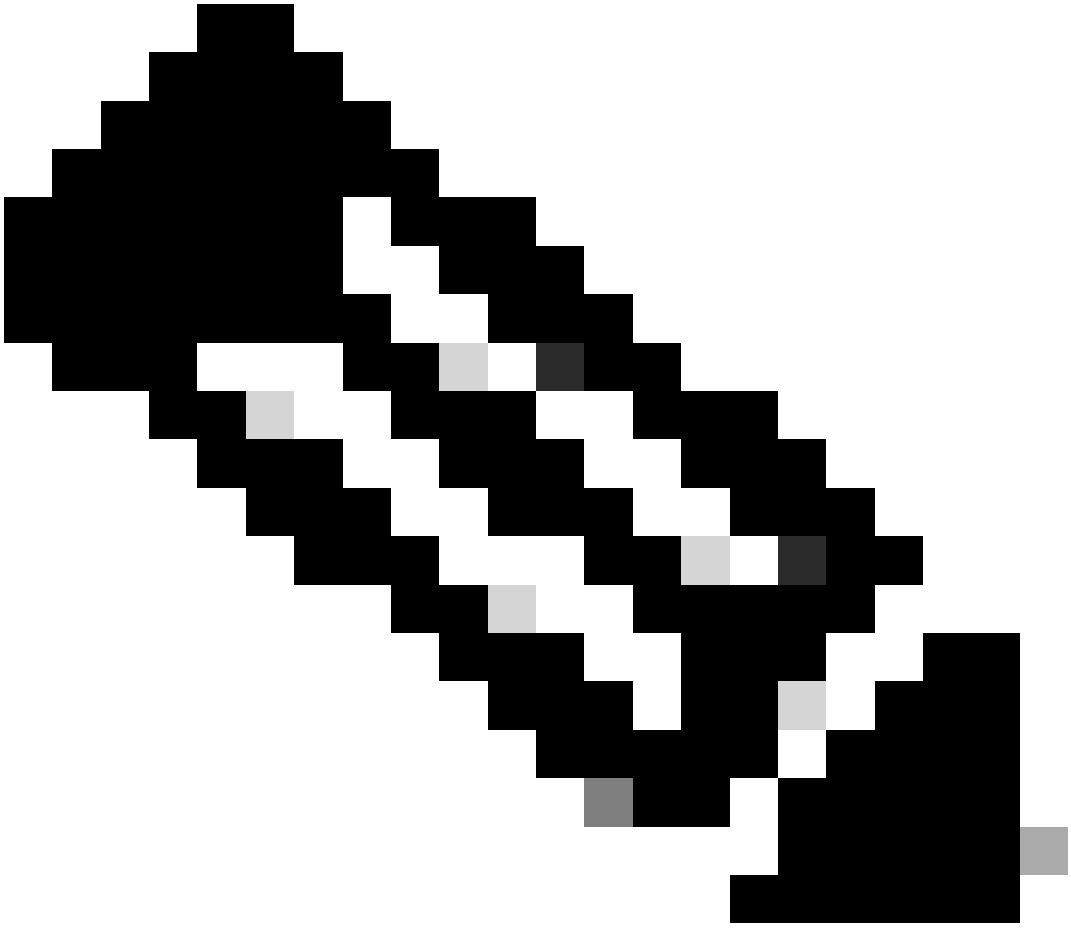
11. Logo após executar o comando "firewall-b reload" (aguarde 15 segundos), mude para o novo firewall primário (firewall-a) e digite o comando failover lan unit primary , seguido de write memory.

```
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. Aguarde até que o firewall-b seja totalmente inicializado e junte-se ao par de failover como secundário/standby. Por exemplo:

```
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#
```



Observação: observe que o firewall principal (firewall-a) envia a configuração para o firewall secundário (firewall-b).

13. Salve a configuração, grave a memória no principal/ativo e valide a memória de gravação no novo secundário/standby. Por exemplo:

```
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. Verifique se o par de failover está ativo/ativo em ambos os firewalls. Por exemplo:

```
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)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.