

ASAファイアウォールのアクティブ/スタンバイフェールオーバーペアへの置き換え

内容

[はじめに](#)

[背景説明](#)

[フェールオーバー構成でのプライマリユニットとセカンダリユニットの違い](#)

[フェールオーバー構成でのアクティブユニットとスタンバイユニットの違い](#)

[セカンダリファイアウォールの障害を交換してください](#)

[プライマリファイアウォールの障害の交換](#)

はじめに

このドキュメントでは、適応型セキュリティアプライアンス(ASA)ファイアウォールをアクティブ/スタンバイフェールオーバーペアに置き換える方法について説明します。

背景説明

ASAファイアウォールでは、アクティブ/アクティブフェールオーバーとアクティブ/スタンバイフェールオーバーという2つのフェールオーバー構成がサポートされています。

ファイアウォールは2つあります。

- firewall-aはプライマリ/アクティブ
- firewall-bはセカンダリ/スタンバイです。

フェールオーバー構成でのプライマリユニットとセカンダリユニットの違い

このコマンドは、このファイアウォールがアクティブな設定を常にセカンダリファイアウォールにプッシュすることを意味します。

```
# failover lan unit primary
```

このコマンドは、このファイアウォールが常にプライマリファイアウォールからアクティブな設定を受信することを意味します。

```
# failover lan unit secondary
```

フェールオーバー構成でのアクティブユニットとスタンバイユニットの違い

このコマンドは、このファイアウォールがフェールオーバーペアでアクティブに実行されているファイアウォールであることを意味します。

```
# failover active
```

このコマンドは、このファイアウォールがフェールオーバーペアのファイアウォールを実行するスタンバイであることを意味します。

```
# failover standby
```

セカンダリファイアウォールの障害を交換してください

1. プライマリファイアウォールがアクティブでオンラインであることを確認します。例：

```
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. セカンダリファイアウォールをシャットダウンし、物理的に取り外します。
3. 新しいセカンダリファイアウォールを物理的に追加し、電源をオンにします。
4. 工場出荷時のデフォルト設定で新しいセカンダリファイアウォールがアクティブになったら、フェールオーバーリンク、no shutdown、フェールオーバー物理リンクを有効にします。

以下に例を挙げます。

```
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. フェールオーバーコマンドを設定します。例：

```
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#
```

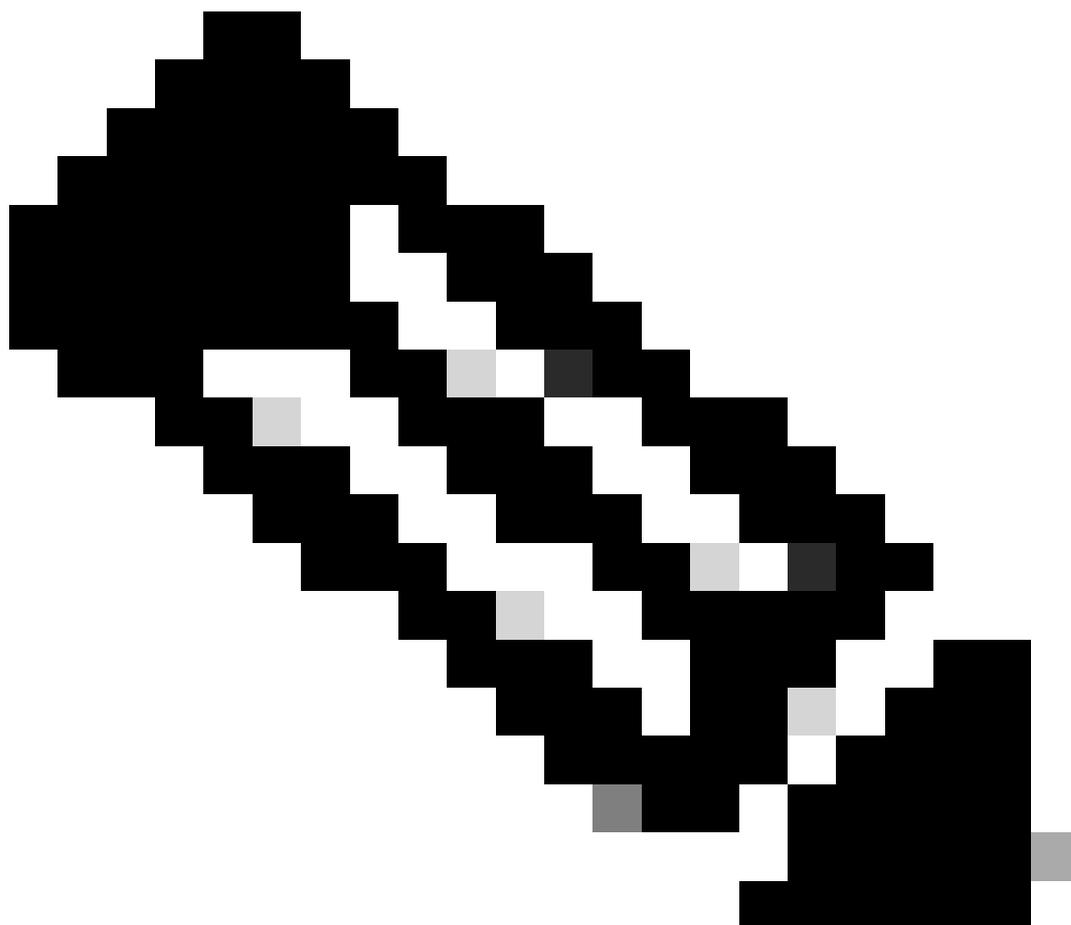
6. 新しいセカンダリファイアウォールでフェールオーバーを有効にします。例：

```
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. アクティブ構成が新しいユニットと同期し、正しいフェールオーバー状態を確認するのを待ちます。例：

```
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：プライマリファイアウォール(firewall-a)が設定をセカンダリファイアウォール

(firewall-b)に送信することに注意してください。

8. プライマリ/アクティブの構成を保存し、新しいセカンダリ/スタンバイの書き込みメモリを検証します。例：

```
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. 両方のファイアウォールでフェールオーバーペアがアップ/アップの状態であることを確認します。例：

```
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)
```

プライマリファイアウォールの障害の交換

1. セカンダリファイアウォールがアクティブでオンラインであることを確認します。例：

```
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. プライマリファイアウォールをシャットダウンして物理的に取り外します。
3. 新しいプライマリファイアウォールを物理的に追加し、電源をオンにします。
4. これで、新しいプライマリファイアウォールが工場出荷時のデフォルト設定でアクティブになります。
5. フェールオーバーリンクをイネーブルにし、フェールオーバー物理リンクをno shutdownにします。例：

```
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. 設定を保存します。セカンダリ/アクティブファイアウォールにメモリを書き込み、failover lan unit secondary がスタートアップコンフィギュレーションにあることを確認します。

以下に例を挙げます。

```
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. failoverコマンドを設定します。

1. セカンダリ/アクティブファイアウォールでは、まずfailover lan unit primaryコマンドを設定して、アクティブな設定がセカンダリ/アクティブファイアウォールから新しいデフォルト設定のプライマリ/スタンバイファイアウォールに確実にプッシュされるようにする必要があります。例：

```
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. 両方のデバイスのフェールオーバー設定を検証します。例：

```
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. 新しいプライマリファイアウォールでフェールオーバーを有効にします。例：

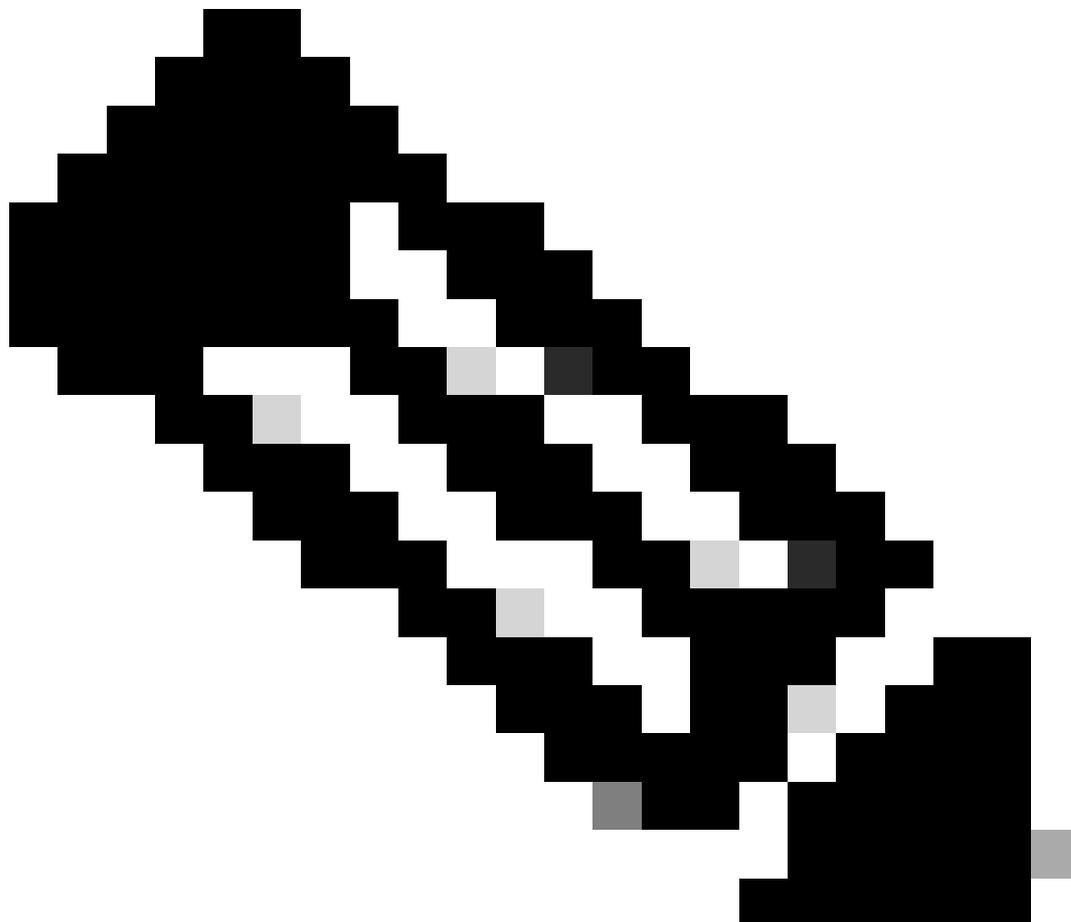
```
firewall-a/sec/stby#conf t
firewall-a/sec/stby#(config)#failover
firewall-a/sec/stby#(config)#exit
firewall-a/sec/stby#
```

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

9. アクティブ構成が新しいユニットと同期し、正しいフェールオーバー状態を確認するまで待ちます。例：

```
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：プライマリファイアウォール(firewall-b)が設定をセカンダリファイアウォール(firewall-a)に送信することに注意してください。現在プライマリ/アクティブファイアウォール(firewall-b)にメモリを書き込まないでください。

10. 現在プライマリ/アクティブファイアウォール(firewall-b)をリロードして、セカンダリ/スタンバイファイアウォールとしてブートアップします。

firewall-b/pri/act#reload

11. 「firewall-b reload」コマンドを実行した直後 (15秒間待った後)、新しいプライマリファイアウォール(firewall-a)に切り替え、failover lan unit primaryコマンドを入力し、続いて

write memoryを入力します。

```
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. firewall-bが完全に起動するまで待ち、フェールオーバーペアをセカンダリ/スタンバイとして結合します。例：

```
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：プライマリファイアウォール(firewall-a)が設定をセカンダリファイアウォール(firewall-b)に送信することに注意してください。

-
13. 構成を保存し、プライマリ/アクティブのメモリに書き込み、新しいセカンダリ/スタンバイのメモリに書き込みを行います。例：

```
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. 両方のファイアウォールでフェールオーバーペアがアップ/アップアクティブであることを確認します。例：

```
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)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。