

安全防火牆FTD高可用性同步介面檢查失敗

目錄

問題

高可用性(HA)對中的FTD始終以Failed狀態顯示。HA對等體之間的配置同步未完成，儘管裝置之間成功建立了IP連線。部署是運行思科安全防火牆威脅防禦軟體的新實施，尚未投入生產。

問題出現在主裝置被移動到其最終位置，並且其管理IP地址被更改而沒有首先中斷HA對之後。HA進程在受監控的資料介面上檢測到失敗的介面檢查，這觸發了HA狀態評估邏輯將主裝置置於「失敗」角色中。

環境

- 安全防火牆FTD HA，由FMC管理
- 遷移活動的新部署，尚未投入生產

解析

解決方案涉及從HA介面監控配置中刪除選定的資料介面，以防止錯誤故障檢測。

已執行的故障排除步驟

1:故障排除資料確認受監控資料介面上的HA介面檢查失敗，而HA對等體連線（心跳和ping）仍然正常工作。

```
device# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FailOver Ethernet1/8 (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 5 of 776 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.20(2)121, Mate 9.20(2)121
Serial Number: Ours SERIAL#, Mate SERIAL#
Last Failover at: 17:14:25 UTC Mar 16 2026
```

This host: Primary - Failed

```
Active time: 0 (sec)
slot 0: FPR-1120 hw/sw rev (2.0/9.20(2)121) status (Up Sys)
```

```
Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)
Interface To-DC1-WAN (0.0.0.0): No Link (Waiting)
```

```
Interface management (203.0.113.131/fe80::a610:b6ff:fe3d:e101): Normal (Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Active
Active time: 184688 (sec)
```

```
Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)
```

```
Interface To-DC1-WAN (10.230.2.2): Normal (Waiting)
Interface management (203.0.113.130/fe80::6ae5:9eff:fee6:d681): Normal (Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

2:已確認正在根據介面監控結果而非管理平面連線問題進行HA狀態轉換。

<#root>

```
device# show failover history
17:16:51 UTC Mar 16 2026
Standby Ready
```

```
Failed                Interface check
```

This host:2

```
single_vf: To-DC1-ACC
single_vf: To-DC1-WAN
```

Other host:1
single_vf: To-DC1-ACC

配置更改

- 1:已更新HA配置，可從介面運行狀況監控中排除受影響的資料介面，從而防止錯誤故障檢測。
- 2:配置更改後，主FTD成功轉換為備用就緒狀態，從而確認正確的HA同步和狀態穩定性。
- 3:已成功完成HA故障轉移測試，並獲得了預期結果，從而在更改後驗證HA配置的穩定性。

預期行為說明

根據設計，在故障排除期間觀察到以下行為：

- FTD對等點上的主機名重複：在FTD HA中，顯示相同主機名的兩個裝置都是預期行為，因為活動裝置主機名是在系統範圍內顯示的(在增強請求CSCwe31354下跟蹤)
- IP地址所有權：只有活動FTD才會顯示資料介面上的活動IP地址，這是設計為防止大腦分裂而預期的行為。如果未配置任何介面備用IP地址，則備用就緒FTD在其介面上顯示為未配置IP地址。

原因

由於受監控資料介面上的高可用性介面運行狀況檢查失敗，主FTD被標籤為「失敗」，導致具有更多操作介面的對等裝置保持活動狀態。此行為設計在FTD高可用性中，並記錄在Cisco安全防火牆HA准則中。HA進程在受監控的資料介面上檢測到失敗的介面檢查，這觸發了HA狀態評估邏輯將主裝置置於「失敗」角色中。

相關內容

- [思科安全防火牆裝置管理器配置指南 — 高可用性 \(故障轉移\)](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。