

# Falha na Verificação da Interface de Sincronização de Alta Disponibilidade do Secure Firewall FTD

## Contents

---

---

## Problema

O FTD em um par de HA (High Availability, alta disponibilidade) mostrava consistentemente um estado de falha. A sincronização de configuração não foi concluída entre os pares HA, apesar da conectividade IP bem-sucedida entre as unidades. A implantação foi uma nova implementação executando o software Cisco Secure Firewall Threat Defense, que ainda não estava em produção.

O problema surgiu depois que a unidade primária foi movida para seu local final e seu endereço IP de gerenciamento foi alterado sem primeiro quebrar o par HA. O processo HA detectou falhas nas verificações de interface nas interfaces de dados monitoradas, o que disparou a lógica de avaliação do estado HA para colocar a unidade primária em uma função com falha.

## Ambiente

- Firewall seguro FTD HA gerenciado pelo FMC
- Nova implantação de uma atividade de migração, ainda não em produção

## Resolução

A resolução envolvia a remoção de interfaces de dados selecionadas da configuração de monitoramento da interface de alta disponibilidade para evitar a detecção de falhas falsas.

## Etapas de Troubleshooting Executadas

1: Os dados de Troubleshooting confirmaram falhas de verificação de interface HA nas interfaces de dados monitoradas, enquanto a conectividade de peer HA (heartbeat e ping) permaneceu funcional.

```
<#root>
```

```
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: Confirmado que as transições de estado de HA estavam ocorrendo com base nos resultados de monitoramento de interface, não problemas de conectividade do plano de gerenciamento.

<#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
```

## Alterações de configuração

1: A configuração de HA foi atualizada para excluir as interfaces de dados afetadas do monitoramento de integridade da interface, evitando a detecção de falha falsa.

2: Após as alterações de configuração, o FTD primário passou com êxito para o status Standby Ready, confirmando a sincronização de HA apropriada e a estabilidade do estado.

3: O teste de failover de HA foi concluído com êxito, com os resultados esperados, validando a estabilidade da configuração de HA após as alterações.

## Esclarecimentos sobre o comportamento esperado

Esses comportamentos observados durante a solução de problemas são esperados e, por design:

- Nomes de host duplicados em pares FTD: As duas unidades que exibem o mesmo nome de host devem ter um comportamento no FTD HA, pois o nome de host da unidade ativa é apresentado em todo o sistema (rastreado sob a solicitação de aprimoramento CSCwe31354)
- Propriedade de endereço IP: Somente o FTD Ativo exibe endereços IP ativos nas interfaces de dados, que é o comportamento esperado por projeto para evitar situações de split brain. Se nenhum endereço IP em standby da interface estiver configurado, o FTD em standby

pronto será exibido como se não tivesse endereços IP configurados em suas interfaces.

## Causa

O FTD Principal foi marcado como Falha devido a falhas de verificação de integridade da interface de Alta Disponibilidade nas interfaces de dados monitoradas, fazendo com que o par com mais interfaces operacionais permaneça Ativo. Esse comportamento é definido por projeto em Alta disponibilidade de FTD e documentado nas diretrizes de HA do Cisco Secure Firewall. O processo HA detectou falhas nas verificações de interface nas interfaces de dados monitoradas, o que disparou a lógica de avaliação do estado HA para colocar a unidade primária em uma função com falha.

## Conteúdo relacionado

- [Guia de configuração do Gerenciador de dispositivos do Cisco Secure Firewall - Alta disponibilidade \(Failover\)](#)
- [Suporte técnico e downloads da Cisco](#)

## 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.