Solucionar problemas de alta disponibilidade do Firepower Threat Defense

Contents

Introduction

Este documento descreve a operação, a verificação e os procedimentos de Troubleshooting para High Availability (HA) no Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Plataformas FTD e ASA
- Capturas de pacotes em dispositivos FTD

É altamente recomendável que o Guia de configuração do Firepower, Configurar alta disponibilidade de FTD em dispositivos Firepower, seja lido para compreender melhor os conceitos descritos neste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD da Cisco
- Cisco Firepower Management Center (FMC)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As informações e os exemplos são baseados no FTD, mas a maioria dos conceitos também é totalmente aplicável ao Adaptive Security Appliance (ASA).

Um DTF suporta dois modos principais de gestão:

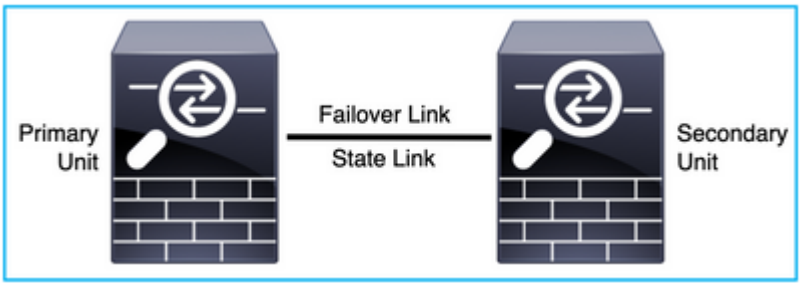
- Off-box via FMC - também conhecido como gerenciamento remoto
- On-box via Firepower Device Manager (FDM) - também conhecido como gerenciamento local

---

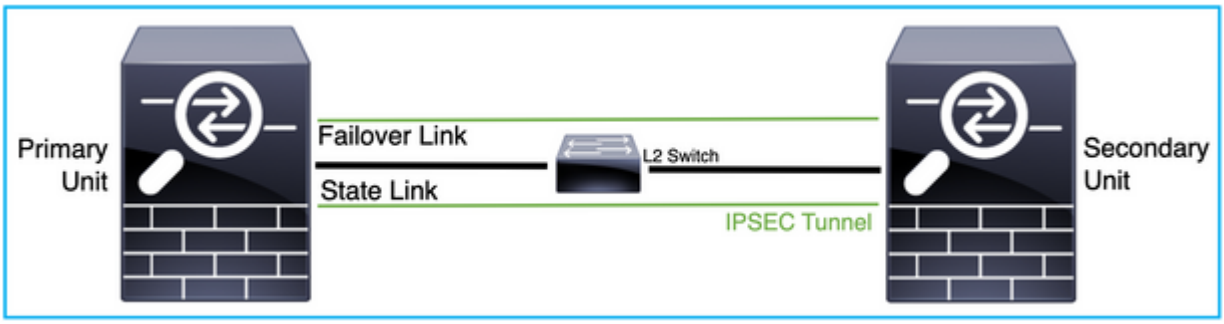
> **Observação**: o FTD gerenciado via FDM pode ser adicionado em Alta Disponibilidade a partir do código de versão do Firepower v6.3.0.

Opções de design

Do ponto de vista do design do FTD, ele pode ser conectado diretamente, como mostrado na imagem a seguir:



Ou pode ser conectado através do switch de Camada 2 (L2), como mostrado nesta imagem:



Terminologia HA

Ativo	O ASA ativo recebe todos os fluxos de tráfego e filtra todo o tráfego de rede. As alterações de configuração são feitas no ASA ativo.
Link HA	As duas unidades em um par de failover se comunicam constantemente por um link de failover para determinar o status operacional de cada unidade e sincronizar as alterações de configuração. As informações compartilhadas no link são: • O estado da unidade (ativo ou em espera) • Mensagens Hello (keep-alive) • Status do Link de Rede • Troca de endereço MAC • Replicação e sincronização de configuração
Preliminar	Esta é a unidade que normalmente é configurada primeiro quando você cria um HA. O significado disso é que se ambos os dispositivos de um ASA HA viessem a se reunir no mesmo instante, o principal assumiria a função ativa.
Secundário	Esta é a unidade que geralmente é configurada em segundo quando você cria um HA. O significado disso é que, se ambos os dispositivos de um ASA HA fossem ativados juntos no mesmo instante, o secundário assumiria a função de standby.
Standby	O ASA em standby não processa nenhum tráfego ativo, ele sincroniza as conexões e a configuração do dispositivo ativo e assume a função ativa em caso de failover.
Link de Estado	A unidade ativa usa o link de estado para passar informações de estado de conexão para o dispositivo de standby. Portanto, a unidade de standby pode manter certos tipos de conexões e isso não o afeta. Essas informações ajudam a unidade em standby a manter as conexões existentes quando ocorre um failover. Observação: quando você usa o mesmo link para failover e failover stateful, você conserva as interfaces da melhor maneira. No entanto, você deve considerar uma interface dedicada para o link de estado e o link de failover, se tiver uma configuração grande e uma rede de alto tráfego. Recomendamos que a largura de banda do link de failover stateful corresponda à maior largura de

	banda das interfaces de dados no dispositivo.

Estados HA

Ativo	O dispositivo lida atualmente com o tráfego em tempo real na rede e todas as alterações de configuração que precisam ser feitas devem ser executadas nesse dispositivo.
Sincronização de Aplicativo	O dispositivo neste estado sincroniza a configuração a partir do dispositivo ativo.
Sincronização em Massa	O dispositivo neste estado sincroniza a configuração a partir do dispositivo ativo.
Desabilitado	O failover na unidade foi desabilitado (comando: no failover).
Negociação	O dispositivo verifica a disponibilidade do dispositivo ativo e assume a função ativa se o dispositivo ativo não estiver pronto para espera.
Pronto para espera	O dispositivo atualmente não lida com o tráfego, mas assume a função ativa se o dispositivo ativo mostrar qualquer problema de verificação de integridade.
Configuração de Sincronização	A configuração é replicada do dispositivo ativo para o dispositivo em standby.
Modo de espera frio	O dispositivo assume o controle como ativo no failover, mas não replica os eventos de conexão.

Diagrama de fluxo do estado HA

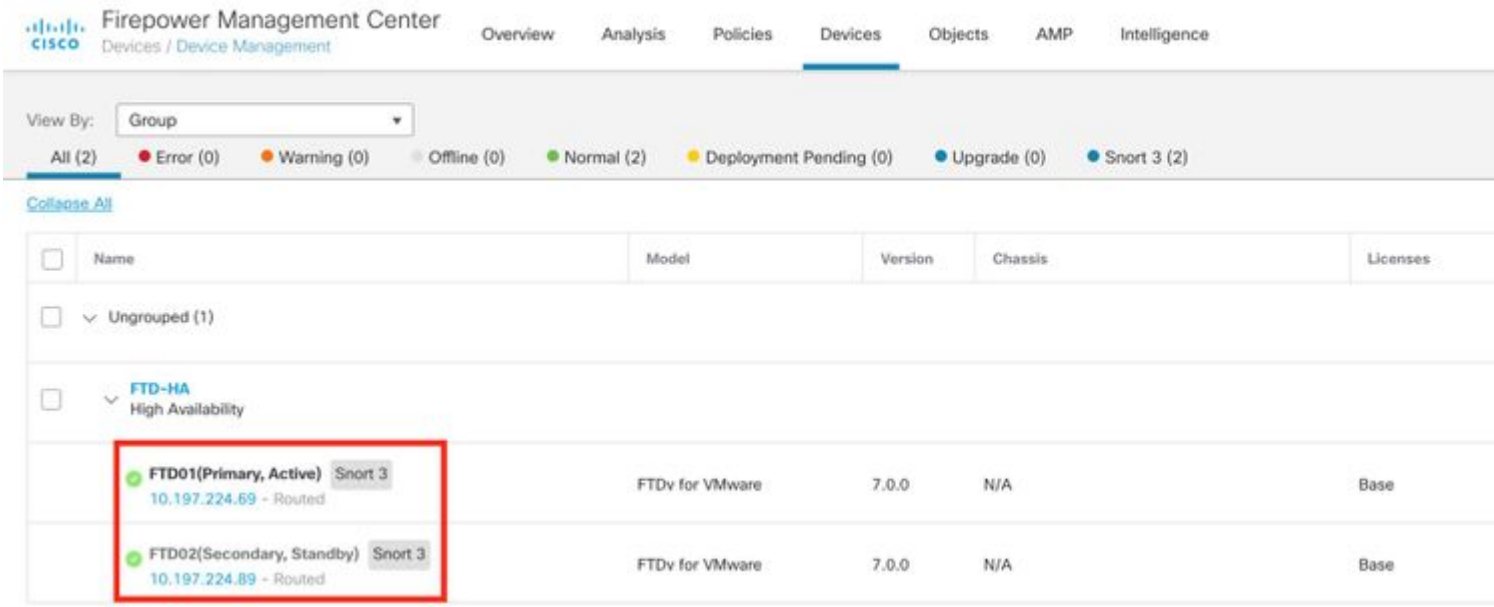
Primário (sem nenhum par conectado):

Secundário (com um par conectado ativo):

Verificação de IU

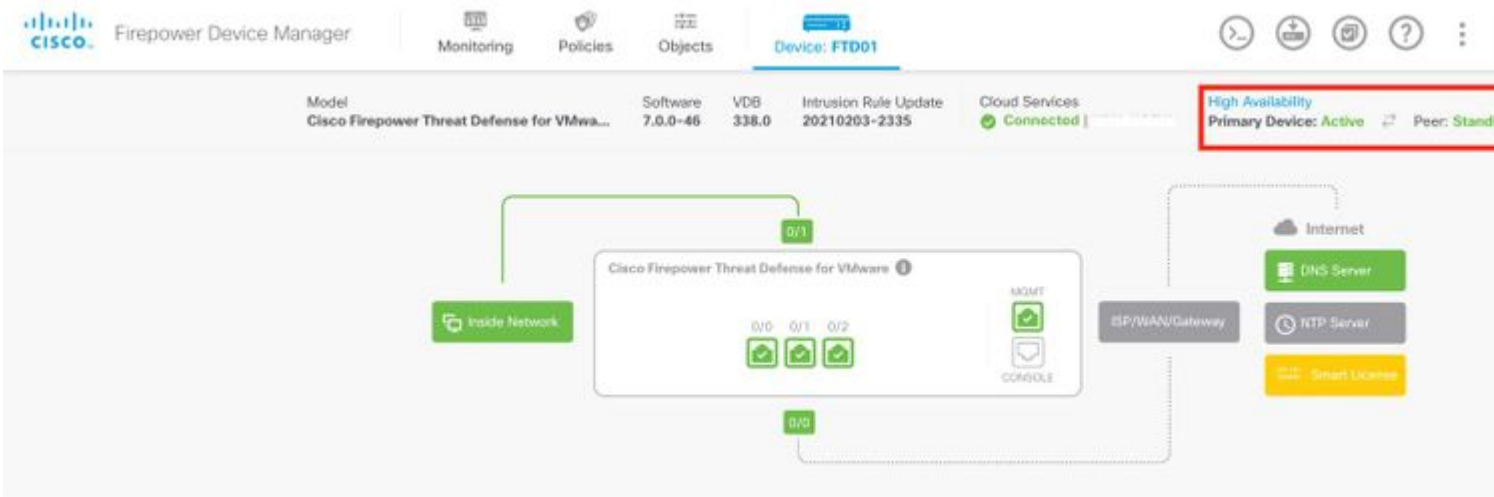
Firepower Management Center HA FTD gerenciado

O estado HA do FTD pode ser verificado na interface do usuário do FMC quando você navega para **Device > Device Management**, como mostrado nesta imagem:



FDM Gerenciado FTD HA

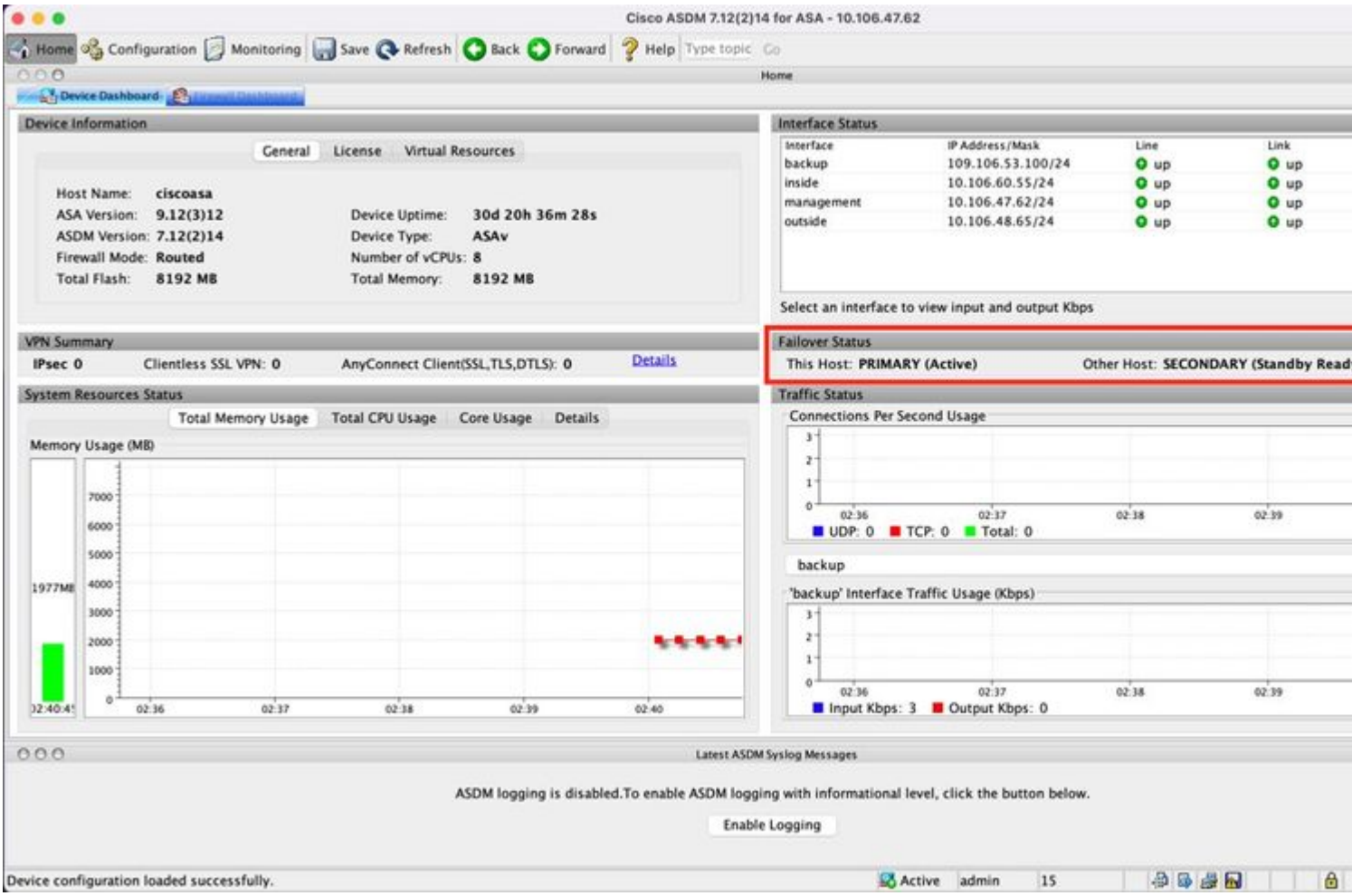
Página Visão Geral do FDM Principal:



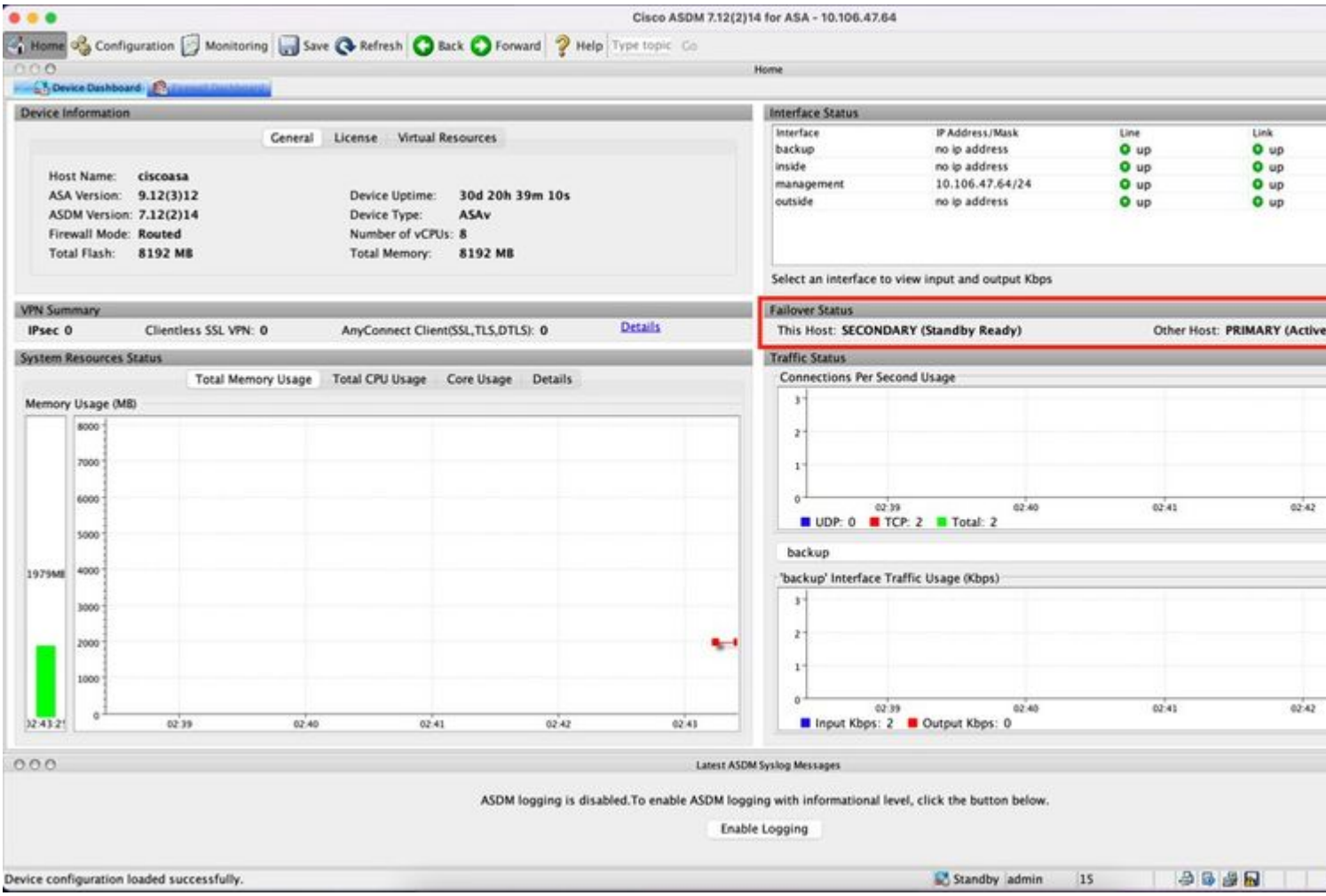
Página Visão Geral Secundária do FDM:

ASA HA gerenciado ASDM

Página inicial do ASDM para o ASA principal:

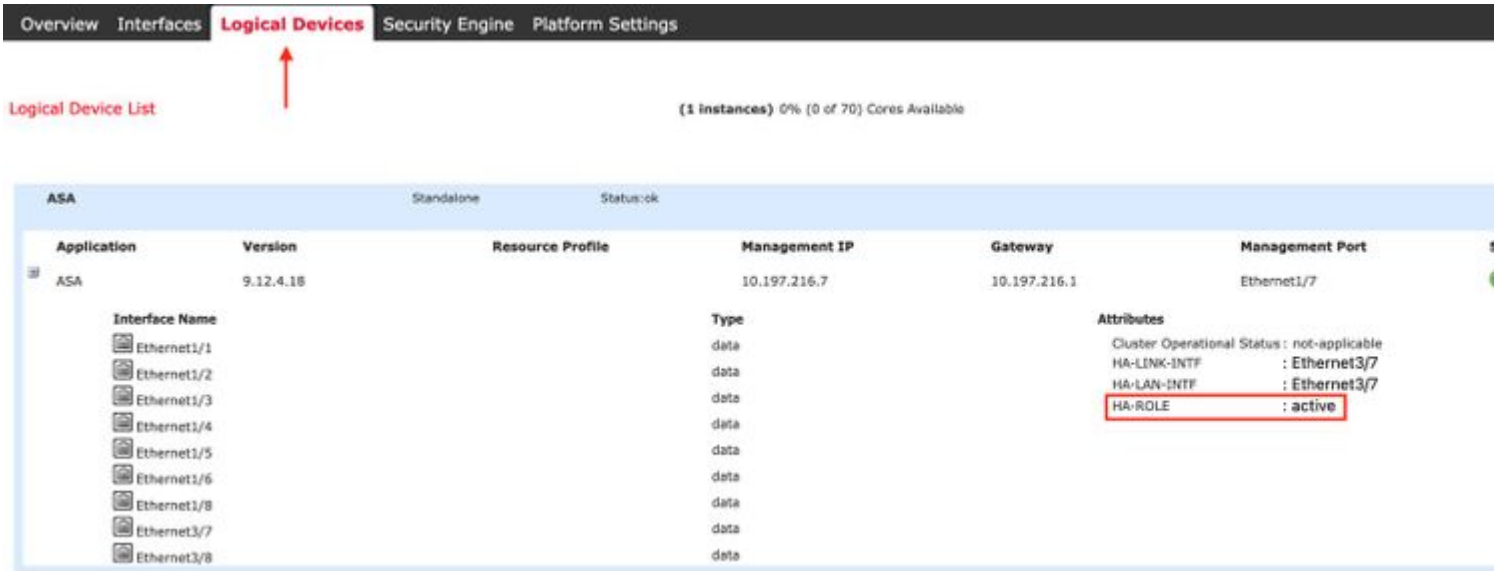


Página inicial do ASDM para o ASA secundário:

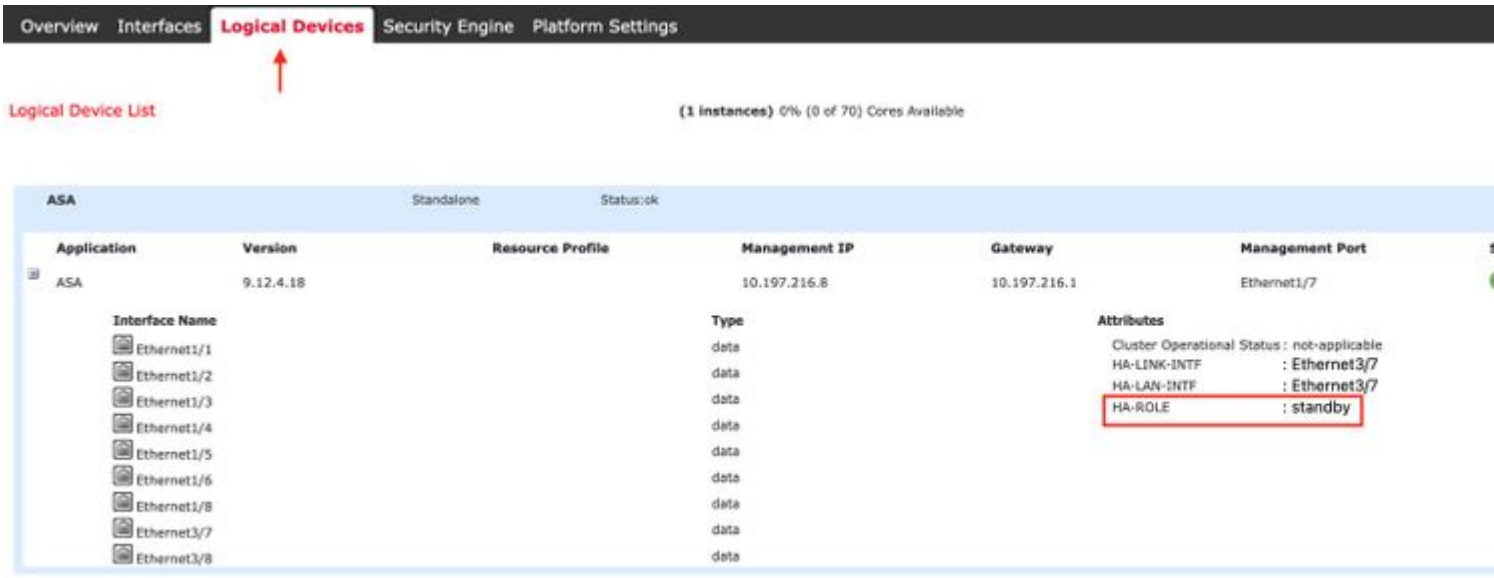


Firepower Chassis Manager para 4100/9300 executando FTD/ASA HA

Página Dispositivo lógico FCM primário:



Página do dispositivo lógico secundário do FCM:



Verificar CLI

<#root>

>

show running-config failover

```
failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

Os pontos importantes a serem considerados neste documento são:

failover
failover lan unit secondary â€”> se a unidade é primária ou secundária
failover lan interface failover-link GigabitEthernet0/2 â€”> failover link interface física no dispositivo
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 â€”> primary and the standby device failover link ip addresses.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (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 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.2): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)
    Other host: Primary - Active
        Active time: 707216 (sec)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.1): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
    Link : failover-link GigabitEthernet0/2 (up)
    Stateful Obj        xmit       xerr          rcv          rerr
    General             95752       0           115789          0
    sys cmd             95752       0            95752          0
    up time               0         0              0            0
    RPC services          0         0              0            0
    TCP conn              0         0              0            0
    UDP conn              0         0              0            0
    ARP tbl               0         0            20036          0
    Xlate_Timeout         0         0              0            0
    IPv6 ND tbl           0         0              0            0
    VPN IKEv1 SA          0         0              0            0
    VPN IKEv1 P2          0         0              0            0
    VPN IKEv2 SA          0         0              0            0
    VPN IKEv2 P2          0         0              0            0
    VPN CTCP upd          0         0              0            0
    VPN SDI upd           0         0              0            0
    VPN DHCP upd          0         0              0            0
    SIP Session           0         0              0            0
    SIP Tx                0         0              0            0
    SIP Pinhole           0         0              0            0
    Route Session         0         0              0            0
    Router ID             0         0              0            0
    User-Identity         0         0              1            0
    CTS SGTNAME           0         0              0            0
    CTS PAC               0         0              0            0
    TrustSec-SXP          0         0              0            0
    IPv6 Route            0         0              0            0
    STS Table             0         0              0            0
    Rule DB B-Sync        0         0              0            0
    Rule DB P-Sync        0         0              0            0
    Rule DB Delete        0         0              0            0

    Logical Update Queue Information
       Cur   Max    Total
Recv Q: 0     5     504656
```

```
Xmit Q: 0     1     95752
```

Failover ativado: o failover está ativado ou desativado.

Este host: Secundário - Pronto para Espera. A função deste dispositivo e os estados das interfaces.

Outros hosts: Principal - Ativo. O outro dispositivo está em um estado Ativo e se comunica com o dispositivo atual.

<#root>

>

show failover history

```
==========================================================================
From State                  To State                    Reason
==========================================================================
01:18:14 UTC Nov 25 2021
Not Detected               Negotiation                 No Error

01:18:27 UTC Nov 25 2021
Negotiation                Just Active                 No Active unit found

01:18:27 UTC Nov 25 2021
Just Active                Active Drain                No Active unit found

01:18:27 UTC Nov 25 2021
Active Drain               Active Applying Config      No Active unit found

01:18:27 UTC Nov 25 2021
Active Applying Config     Active Config Applied       No Active unit found

01:18:27 UTC Nov 25 2021
Active Config Applied         Active                   No Active unit found
==========================================================================
```

Use isto para verificar os estados históricos dos dispositivos e as razões para essas alterações de estado:

<#root>

>

show failover state

```
              State              Last Failure Reason      Date/Time
This host -   Secondary
              Standby Ready          None
Other host -  Primary
              Active                 None

====Configuration State===
    Sync Done - STANDBY
```

```
====Communication State===
    Mac set
```

Verifique os estados atuais dos dispositivos e o motivo do último failover:

Campo	Descrição
Estado da configuração	Exibe o estado da sincronização de configuração. Possíveis estados de configuração para a unidade de standby: • Config Syncing - STANDBY â€" Defina enquanto a configuração sincronizada é executada. • Sincronização da configuração de interface - STANDBY • Sync Done - STANDBY â€" (Sincronização concluída - EM ESPERA) Define quando a unidade em espera concluiu uma sincronização de configuração da unidade ativa. Possíveis estados de configuração para a unidade ativa: • Config Syncing â€" Defina na unidade ativa quando ela executar uma sincronização de configuração para a unidade de standby. • Sincronização de configuração de interface • Sync Done (Sincronização concluída) â€" Defina quando a unidade ativa tiver concluído uma sincronização de configuração bem-sucedida com a unidade de standby. • Ready for Config Sync â€" Ativa a unidade ativa quando a unidade de standby sinalizar que está pronta para receber uma sincronização de configuração.
Estado da Comunicação	Exibe o status da sincronização do endereço MAC. • Mac set â€" Os endereços MAC foram sincronizados da unidade peer para esta unidade. • Mac atualizado â€" usado quando um endereço MAC é atualizado e precisa ser sincronizado com a outra unidade. Também usado no momento da transição, em que a unidade atualiza os endereços MAC locais sincronizados a partir da unidade peer.
Data/Hora	Exibe uma data e um timestamp para a falha.
Motivo da Última Falha	Exibe o motivo da última falha relatada. Essas informações não são apagadas, mesmo que a condição de falha seja apagada. Essas informações são alteradas somente quando ocorre um failover.

Campo	Descrição
	Possíveis motivos de falha: • Falha de interface â€" O número de interfaces que falharam atendeu aos critérios de failover e causou o failover. • Falha de Comm â€" O link de failover falhou ou o peer está inoperante. • Falha do backplane
Estado	Exibe o status Principal/Secundário e Ativo/Em Espera da unidade.
Este host/Outros hosts	Esse host indica informações para o dispositivo no qual o comando foi executado. Outro host indica informações para o outro dispositivo no par de failover.

<#root>

>

show failover descriptor

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

Troubleshoot

Debugs

<#root>

>

debug fover ?

```
cable         Failover LAN status
cmd-exec      Failover EXEC command execution
fail          Failover internal exception
fmsg          Failover message
ifc           Network interface status trace
open          Failover device open
rx            Failover Message receive
rxdmp         Failover recv message dump (serial console only)
rxip          IP network failover packet recv
snort         Failover NGFW mode snort processing
switch        Failover Switching status
```

```
sync          Failover config/command replication
tx            Failover Message xmit
txdmp         Failover xmit message dump (serial console only)
txip          IP network failover packet xmit
verify        Failover message verify
```

Capturas:

Capturas de interface de failover:

Você pode consultar essa captura para determinar se os pacotes de saudação de failover são enviados no link de failover na taxa em que são enviados.

<#root>

>

show capture

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
>
```

show capture capfail

```
15 packets captured

1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

Captura ARP no link de failover:

Você pode fazer essa captura para ver se os peers têm entradas Mac na tabela ARP.

<#root>

>

```
show capture


capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
>

show capture caparp



22 packets captured

1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

Cenários

Se a unidade peer falhar em ingressar no grupo HA ou falhar enquanto você implanta as alterações da unidade ativa, faça login na unidade que falhou, navegue até a página Alta Disponibilidade e clique no link Histórico de Failover.

Falha de APP-SYNC

Se a saída show failover history indicar uma falha do App Sync, houve um problema no momento da fase de validação de HA, em que o sistema verifica se as unidades podem funcionar corretamente como um grupo de alta disponibilidade.

A mensagem "Todas as validações foram aprovadas" quando o Estado De é Sincronização de Aplicativos é exibido, e o nó passa para o estado Pronto para espera.

Qualquer falha de validação faz a transição do peer para o estado Disabled (Failed). Resolva os problemas para fazer com que os peers funcionem como um grupo de alta disponibilidade novamente.

Observe que se você corrigir um erro de sincronização de aplicativo e fizer alterações na unidade ativa, você deve implantá-las e retomar o HA para o nó par ingressar.

As mensagens indicam falhas, com uma explicação de como você pode resolver os problemas. Esses erros podem ocorrer na junção do nó e em cada implantação subsequente.

No momento em que um nó ingressa, o sistema executa uma verificação em relação à última configuração implantada na unidade ativa.

O nó de standby falha ao ingressar no HA com "erro de sincronização de aplicativo de CD é falha de aplicação de configuração de aplicativo"

Na linha de comando do FTD de standby, **/ngfw/var/log/action_queue.log** deve ter o motivo da falha de configuração.
Correção: Ao identificar o erro de configuração, após fazer as alterações necessárias, o HA pode ser retomado.
Consulte o bug da Cisco IDCSCvu15611.

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
15:10:16 CDT Sep 28 2021
Not Detected                Disabled                    No Error
15:10:18 CDT Sep 28 2021
Disabled                    Negotiation                 Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation                 Cold Standby                Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby                App Sync                    Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync                    Disabled
```

CD App Sync error is App Config Apply Failed

```
================================================================================
```

O nó em espera falha ao ingressar no HA com "falha na progressão do estado do HA devido ao tempo limite de SINCRONIZAÇÃO DO APLICATIVO"

Na linha de comando FTD em standby, **/ngfw/var/log/ngfwmanager.log** deve ter o motivo para o timeout de sincronização de aplicativos.
Neste estágio, as implantações de política também falham porque a unidade ativa acha que a sincronização de aplicativos ainda está em andamento.
A implantação da política lança o erro - "como o processo newNode join/AppSync está em andamento, as Alterações de Configuração não são permitidas e, portanto, rejeita a solicitação de implantação. Tente a implantação novamente mais tarde"
Correção: às vezes, quando você retoma a alta disponibilidade no nó Standby, ele pode resolver o problema.
Consulte o bug da Cisco ID CSCvt48941
Consulte o bug da Cisco ID CSCvx11636

<#root>

```
==========================================================================
From State                  To State                    Reason
==========================================================================
19:07:01 EST MAY 31 2021
Not Detected               Disabled                    No Error
19:07:04 EST MAY 31 2021
Disabled                   Negotiation                 Set by the config command
19:07:06 EST MAY 31 2021
Negotiation                Cold Standby                Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby               App Sync                    Detected an Active mate
21:11:18 EST Jun 30 2021
App Sync                   Disabled
```

HA state progression failed due to APP SYNC timeout

```
==========================================================================
```

O nó em espera falha ao ingressar no HA com "O erro de sincronização de aplicativo de CD falhou ao aplicar a configuração do SSP em espera"

Na linha de comando do FTD de standby, **/ngfw/var/log/ngfwmanager.log** deve ter o motivo exato para a falha.

Correção: às vezes, quando você retoma a alta disponibilidade no nó Standby, ele pode resolver o problema.

Consulte a ID do bug da Cisco CSCvy04965

<#root>

```
==========================================================================
From State                  To State                    Reason
==========================================================================
04:15:15 UTC Apr 17 2021
Not Detected               Disabled                    No Error
04:15:24 UTC Apr 17 2021
Disabled                   Negotiation                 Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation                Cold Standby                Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby               App Sync                    Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync                   Disabled
```

CD App Sync error is Failed to apply SSP config on standby

```
==========================================================================
```

Falha na Verificação de Integridade

"HELLO not heard from mate" significa que o correspondente está offline ou que o link de failover não comunica as mensagens de manutenção de atividade HELLO.

Tente fazer login no outro dispositivo, se o SSH não funcionar, obtenha acesso ao console e verifique se o dispositivo está operacional ou offline.

Se estiver operacional, identifique a causa da falha com o comando **show failover state.**

Se não estiver operacional, tente uma reinicialização normal e verifique se você vê algum registro de inicialização no console; caso contrário, o dispositivo pode ser considerado defeituoso por hardware.

<#root>

```
==========================================================================
From State                To State                  Reason
==========================================================================
04:53:36 UTC Feb 6 2021
Failed                    Standby Ready
```

Interface check

```
02:12:46 UTC Jul 11 2021
Standby Ready             Just Active               HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied     Active                    HELLO not heard from mate
==========================================================================
```

Snort Down ou Falha de Disco

Se o FTD fornecer este erro, "Falha do mecanismo de inspeção de detecção devido a falha de disco", há 2 possibilidades.

O mecanismo de detecção (instância do SNORT) está inoperante

Isso pode ser validado com o comando no lado do Linux, **pmtool status | grep -i de**

Correção: se alguma das instâncias estiver inativa, verifique **/ngfw/var/log/messages** e identifique a causa.

O Dispositivo Mostra Alta Utilização De Disco

Isso pode ser validado com o comando no lado do Linux, **df -Th**.

Correção: identifique o diretório que consome a maior parte do disco e entre em contato com o TAC para excluir os arquivos indesejados.

<#root>

```
==========================================================================
From State                To State                  Reason
==========================================================================
Active Config Applied     Active                    No Active unit found
16:07:18 UTC Dec 5 2020
Active                    Standby Ready             Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready             Failed
```

Detect Inspection engine failure due to disk failure

```
16:07:29 UTC Dec 5 2020
Failed                    Standby Ready             My Inspection engine is as good as peer due to dis
================================================================================
```

Falha da placa de serviço

Esses problemas são geralmente relatados devido a uma falha do módulo Firepower em dispositivos ASA 5500-X. Verifique a sanidade do módulo através de **show module sfr details**.

Correção: Colete o Syslog ASA no momento da falha, e eles podem conter detalhes como falha de controle ou plano de dados.

Isso pode ser devido a vários motivos no módulo SFR. É recomendável abrir o TAC para encontrar a causa raiz desse problema no IPS.

<#root>

```
================================================================================
From State                To State                  Reason
================================================================================
21:48:19 CDT Aug 1 2021
Active                    Standby Ready             Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready             Just Active
```

Service card in other unit has failed

```
21:48:19 CDT Aug 1 2021
Active Config Applied     Active                    Service card in other unit has failed
================================================================================
```

Falha de pulsação de MIO

O Firepower Threat Defense/ASA relata falha devido a "falha de pulsação de MIO-blade" em FPR1K, 2K, 4K, 9K.

Consulte a ID do bug da Cisco CSCvy14484
Consulte a ID do bug da Cisco CSCvh26447

<#root>

```
================================================================================
From State                To State                  Reason
================================================================================
20:14:45 EDT Apr 14 2021
Active Config Applied     Active                    No Active unit found
20:15:18 EDT Apr 14 2021
Active                    Failed
```

MIO-blade heartbeat failure

```
20:15:19 EDT Apr 14 2021
Failed                      Negotiation               MIO-blade heartbeat recovered
================================================================================
```

Informações Relacionadas

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185
- **Suporte Técnico e Documentação - Cisco Systems**

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.