

Solucionar Problemas de Falha no Emparelhamento de Alta Disponibilidade no FDM

Contents

Problema

O emparelhamento de Alta Disponibilidade (HA) entre dois dispositivos Cisco Firepower 1120 que executam o FTD 7.4.2.4 falha durante a sincronização de aplicativos com o nó secundário, entrando consistentemente em um estado de Falha devido a uma incompatibilidade do modo de registro de licença. A mensagem de erro específica encontrada é:

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

O comando `show app-sync-history` revela falhas repetidas com mensagens como:

```
App Sync Status: FAILURE
```

```
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

Esse problema ocorreu depois que os dois firewalls foram redefinidos, as configurações foram restauradas do backup, o software foi atualizado para a versão 7.4.2.4 do FTD, as versões VDB e Snort foram atualizadas e as licenças foram reaplicadas com tokens novos. O firewall secundário permanece em um estado de Falha, impedindo a conclusão do HA e afetando a redundância do firewall.

Ambiente

- Dispositivos NGFW Cisco Firepower 1120 configurados para alta disponibilidade

- Firepower Threat Defense (FTD) versão 7.4.2.4-9
- Mecanismo de inspeção Snort: 3.1.53.2003 - N.º 175
- VDB: 425.0
- Banco de dados de localização geográfica: 2026-03-07-053
- Dispositivos convertidos do Smart Licensing para o modo PLR (Reserva de Licença Permanente)
- Dispositivo primário tentando conectividade de nuvem após conversão de PLR
- Os dois dispositivos foram restaurados do backup

Resolução

A resolução envolve a identificação e correção da incompatibilidade do modo de registro de licença entre os dispositivos primário e secundário, a execução do cancelamento de registro na nuvem e a conclusão de uma implantação completa.

Passo 1: Identificar a Incompatibilidade do Modo de Registro de Licença

Verifique o modo de registro de licença em ambos os dispositivos verificando o histórico de sincronização de aplicativos para obter os motivos de falha específicos:

```
show app-sync-history
```

A saída mostra falhas que indicam:

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

Passo 2: Realizar Cancelamento de Registro na Nuvem

Como o dispositivo primário ainda estava tentando a conectividade de nuvem após a conversão do Smart Licensing para o modo PLR, o cancelamento do registro de nuvem é necessário.

Configure um proxy temporário na interface do usuário do FDM (se nenhum proxy estiver configurado):

Navegue até System Settings > See More > HTTP Proxy tab e configure um proxy fictício temporariamente [isso pode ser removido posteriormente].

Use SSH no dispositivo FTD e execute o script do conector:

```
ssh admin@<device-ip>
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

Passo 3: Resolver conflito de porta 8989

Se o script do conector falhar com este erro:

```
Error: listen tcp :8989: bind: address already in use
```

Identifique e encerre o processo usando a porta 8989 (normalmente a Cisco Success Network):

```
netstat -tulpn | grep 8989
kill <pid>
```

Passo 4: Cancelamento de registro de nuvem completo

Execute novamente o script do conector após resolver o conflito de portas:

```
/ngfw/var/sf/bin/connector.sh
```

A execução bem-sucedida deve mostrar uma saída semelhante a:

```
Starting connector
```

```
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.x
```

```
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x
```

Vá para a GUI do FDM, Configurações do Sistema > Serviços em Nuvem > Serviços em Nuvem e clique na opção de cancelamento de registro. Verifique se o dispositivo não está registrado nos serviços de nuvem.

Passo 5: Executar implantação completa e retomar HA

Após o cancelamento do registro na nuvem, se o emparelhamento de HA ainda falhar com o mesmo erro de incompatibilidade de licença, execute uma implantação completa na unidade ativa por meio da interface do FDM.

Navegue para Implantar > Implantar agora e conclua o processo de implantação.

Quando a implantação estiver concluída, tente a formação de HA novamente. Os dispositivos devem formar com êxito um par de HA ativo-em espera com interfaces conectadas e em um estado pronto.

Passo 6: Verificar status de HA

Confirmar formação de HA bem-sucedida:

```
show failover
```

A saída deve mostrar ambas as unidades nos estados HA adequados com sincronização bem-sucedida.

Causa

A causa principal foi uma incompatibilidade do modo de registro de licença entre os dispositivos Firepower 1120 primário e secundário. Os dispositivos foram convertidos do modo Smart Licensing para o modo PLR (Permanent License Reservation); no entanto, o dispositivo primário continuou tentando a conectividade de nuvem, levando a uma incompatibilidade no estado de conformidade de exportação/agente de licença durante a validação de HA. Isso resultou em repetidas falhas de validação do FDM/FIM durante a sincronização do aplicativo. Além disso, o cancelamento de registro na nuvem foi inicialmente bloqueado por um conflito de porta 8989 relacionado à Cisco Success Network, que exigiu resolução antes que o cancelamento de registro pudesse continuar.

Conteúdo relacionado

- [Aplicar licenças permanentes em redes Air-Gapped](#)
- [Recriar uma defesa contra ameaças de firewall seguro](#)
- [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.