Solucionar problemas de otimização de TCP AppQoE e DRE no Cisco Catalyst SD-WAN

Contents

Introdução

Este documento descreve como solucionar problemas de otimização de TCP AppQoE e DRE no Cisco Catalyst SD-WAN.

Informações de Apoio

Use este guia quando um fluxo TCP habilitado para AppQoE não for otimizado, for ignorado, redefinir após desvio, relatar um nó de serviço não íntegro ou mostrar menos redução de DRE (Eliminação de Redundância de Dados) do que o esperado.

Comece com a triagem de 10 minutos. Ele separa os problemas de política e caminho dos problemas de integridade de nó de serviço, estado de fluxo, capacidade, transporte TCP e eficiência de DRE. Continue até a seção de sintomas somente depois de saber onde o fluxo pára de se comportar como esperado.

Finalidade, escopo e segurança

Este guia aborda os dispositivos Cisco IOS® XE Catalyst SD-WAN que usam otimização de TCP ou DRE com nós de serviço AppQoE integrados ou externos.

Item de Validação	Status
Comportamento público e CLI operacional	Alinhado com a documentação atual do Cisco Catalyst SD-WAN AppQoE 26.x
Contador semântico interno	Verificada novamente a origem atual do Cisco IOS XE em 15 de julho de 2026
Versão, plataforma e topologia exatas usadas para publicação	Captura de laboratório: Cisco IOS XE Catalyst SD-WAN 17.18.2 no C8000v, nó de serviço externo AppQoE. AppNav controller c8000v-appqoe-3, service node c8000v-appqoe-4, SN appqoe-service-node externo (SN IP 15.15.15.2). SNG SNG-APPQOE, política de dados _vpn-10_appqoe-policy (TCP + DRE) na VPN 10. Capturado em 15.7.2026.

A disponibilidade e a saída do comando variam de acordo com a versão do software, a plataforma e a função. Confirme a sintaxe com a ajuda do comando no dispositivo de destino. Os comandos QFP de baixo nível neste guia são somente leitura, mas são específicos para plataforma e versão; use-os somente quando o comando estiver presente.

Os principais pontos de verificação da versão são mostrados abaixo; eles não substituem o

suporte específico da plataforma e a documentação de escala.

Capacidade	Ponto de Verificação de Versão Mínimo
Tratamento de MTU de controlador de serviço/nó de serviço automatizado e DRE	Catalyst SD-WAN 17.5.1a do Cisco IOS XE
Solução de problemas de AppQoE e integridade de subserviço aprimoradas	17.6.1a
Solução de problemas detalhada de fluxo expandido	17.9.1a
Proxy SSL com TLS 1.3	17.13.1a/Gerenciador 20.13.1
DRE por meio de grupos de configuração	17.14.1a/Gerenciador 20.14.1

A DRE requer nós de serviço suportados em ambas as extremidades e tratamento de fluxo simétrico. Ele não é executado em um dispositivo na função somente de controlador de serviço e AppQoE não pode ser combinado com a Duplicação de Pacotes na mesma conexão. O tráfego criptografado exigirá o tratamento SSL/TLS com suporte se o seu payload for otimizado.

Antes de alterar a política, limpar as estatísticas, reiniciar um serviço ou ativar a depuração, capture:

- Versão de software, plataforma e função AppQoE em ambas as extremidades
- Endereços IP origem e destino, portas, protocolo, VPN e tempo de teste UTC
- Sequência de política esperada e atribuição de nó de serviço
- Se o sintoma afeta um fluxo, um par de sites ou todo o tráfego de AppQoE
- Dois instantâneos de contador sobre o mesmo intervalo de teste

---

Note: Não limpe o cache DRE durante a solução de problemas inicial. Limpá-lo reinicia o DRE e destrói o cache quente, o que altera a condição que está sendo medida.

Comece aqui: Triagem de 10 minutos

1. Verificar o Estado do AppQoE e Erros Recentes

Executar nos dispositivos de borda ou controladores de serviço participantes:

```
show sdwan appqoe status
show sdwan appqoe error recent
```

Exemplo de laboratório:

c8000v-appqoe-4 (nó de serviço, C8000v, IOS XE 17.18.2).

```
c8000v-appqoe-4#show sdwan appqoe status
APPQOE Status : YELLOW
Service Status:
  SSLPROXY : YELLOW
  TCPPROXY : GREEN
  SERVICE CHAIN : GREEN
  RESOURCE MANAGER : GREEN

c8000v-appqoe-4#show sdwan appqoe error recent
Appqoe Statistics Recent
------------------------
Label                        Current value        Value(30 sec bfr)      Value(60 sec bfr)
RM TCP used sessions                 0                    0                    0
RM TCP session allocated             21516                21516                21516
TCP number of connections            21215                21215                21215
TCP failed connections               298                  298                  298
vPath drop due to pps                0                    0                    0
vPath new connection failed          0                    0                    0
BBR Active connections               1                    1                    1
Syn Drop Max PPS Reached             0                    0                    0
... (output truncated)
```

Aqui o status geral é AMARELO apenas porque o AO SSL não está em uso (o proxy SSL está no modo claro); Os subserviços TCP, cadeia de serviços e gerenciador de recursos são VERDES. Nenhum descarte de Ps ou falhas de nova conexão.

Procure os serviços habilitados, o estado atual do nó de serviço, os erros de fluxo recentes e qualquer razão que explique diretamente o comportamento de ignorar ou descartar.

2. Verificar a Atribuição de Nós de Serviço e Política em Ambas as Direções

```
show sdwan policy from-vsmart
show service-insertion type appqoe service-node-group
```

Exemplo de laboratório:

c8000v-appqoe-3 (AppNav controller), 15 de julho de 2026.

```
c8000v-appqoe-3#show sdwan policy from-vsmart
from-vsmart data-policy _vpn-10_appqoe-policy
 direction all
 vpn-list vpn-10
  sequence 1
   match
    source-ip 31.31.31.0/24 41.41.41.0/24
   action accept
    tcp-optimization
    dre-optimization
    service-node-group SNG-APPQOE
  default-action accept
from-vsmart lists vpn-list vpn-10
 vpn 10

c8000v-appqoe-3#show service-insertion type appqoe service-node-group
Service Node Group name         : SNG-APPQOE
    Service Context             : appqoe/1
    Member Service Node count   : 1

Service Node (SN)                   : 15.15.15.2
Auto discovered                     : No
SN belongs to SNG                   : SNG-APPQOE
Current status of SN                : Alive
System IP                           : 10.20.0.1
Site ID                             : 30
Time current status was reached     : Fri Jun 12 07:45:14 2026

Cluster protocol VPATH version               : 2 (Bitmap recvd: 3)
Cluster protocol incarnation number          : 3

Health Markers:
              AO       Load State
             tcp           GREEN 0%
             ssl  RED/NOT AVAILABLE
             dre           GREEN 0%
            http  RED/NOT AVAILABLE
        utd chnl  RED/NOT AVAILABLE
```

A ação accept transporta otimização tcp e otimização dre apontando para SNG-APPQOE, e o SN está ativo com tcp/dre GREEN. ssl/http/utd show RED/NOT AVAILABLE porque esses AOs não estão configurados — esperado para um teste somente TCP+DRE.

Confirme se a sequência pretendida corresponde às duas direções do fluxo de teste, inclui as ações TCP/DRE esperadas e aponta para o grupo de nós de serviço pretendido. A DRE exige o tratamento de extremidades e de fluxo simétrico.

3. Inspecione um fluxo conhecido e rastreie-o de ponta a ponta

```
show sdwan appqoe flow vpn-id <vpn-id> server-port <port>
show sdwan appqoe flow flow-id <flow-id>
show sdwan appqoe flow closed all
```

Rastreando um único fluxo

Primeiro, execute show sdwan appqoe flow vpn-id **<vpn-id>** server-ip **<server-ip>** server-port **<port>** nos roteadores de borda e de CC. Esse comando retorna o ID do fluxo. Depois de ter o ID do fluxo, execute show sdwan appqoe flow-id **<flow-id>** em ambos os roteadores.

```
show sdwan appqoe flow vpn-id <vpn-id> server-ip <server-ip> server-port <port>
show sdwan appqoe flow flow-id <flow-id>
```

Exemplo de laboratório:

c8000v-appqoe-4 (nó de serviço), 15-7-2026. Nenhum fluxo estava ativo no momento da captura, portanto a tabela histórica (fechada) é mostrada.

```
c8000v-appqoe-4#show sdwan appqoe flow all

Active Flows: 0

T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
Flow ID      VPN  Source IP:Port          Destination IP:Port          Service
No Matching Flows

c8000v-appqoe-4#show sdwan appqoe flow closed all
Current Historical Optimized Flows: 100

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
RR: DRE Reduction Ratio

Flow ID      VPN  Source IP:Port         Destination IP:Port        Service  RR%
91989394759551 10   41.41.41.2:50748       185.125.190.99:80          T        -
91990285862945 10   41.41.41.2:36804       185.125.190.100:80         T        -
91996708679695 10   41.41.41.2:54614       91.189.91.97:80            T        -
92002614507991 10   41.41.41.2:57534       91.189.91.97:80            T        -
92101839402141 10   41.41.41.2:36856       185.125.188.54:443         T        -
... (95 more rows truncated)

++++ Tracing single flow end to end, run below command on both edge and DC routers +++++++
================================================================================

c8000v-appqoe-4#show sdwan appqoe flow vpn-id 10 server-ip 41.41.41.2 server-port 21
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP

Flow ID      VPN  Source IP:Port               Destination IP:Port          Service
```

```
93741048628578 10   31.31.31.2:37632              41.41.41.2:21                  TD

c8000v-appqoe-4#show sdwan appqoe flow flow-id 93741048628578
Flow ID: 93741048628578

VPN: 10  APP: 0 [Client 31.31.31.2:37632 - Server 41.41.41.2:21]

HTTP Connect: 0
TCP stats
---------
Client Bytes Received   : 213
Client Bytes Sent       : 363
Server Bytes Received   : 176
Server Bytes Sent       : 36

Client Bytes sent to SSL: 165
Server Bytes sent to SSL: 176

... (195 more rows truncated)

TCP Flow Events
   1. time:303.932637   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:303.932696   ::   Event:TCPPROXY_EVT_AD_RX_SYN_WITH_OPTIONS
   3. time:303.932741   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   4. time:303.932759   ::   Event:TCPPROXY_EVT_AD_TX_CORE_SYNACK
   5. time:303.933496   ::   Event:TCPPROXY_EVT_AD_RX_CORE_ACK_WITH_OPTIONS
   6. time:303.933594   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   7. time:303.933650   ::   Event:TCPPROXY_EVT_AD_TX_CORE_SYN_NO_OPTIONS
   8. time:303.933657   ::   Event:TCPPROXY_EVT_CONNECT_START
   9. time:303.933993   ::   Event:TCPPROXY_EVT_AD_RX_CORE_SYNACK
  10. time:303.934022   ::   Event:TCPPROXY_EVT_AD_TX_CORE_ACK_NO_OPTIONS
  11. time:303.934024   ::   Event:TCPPROXY_EVT_CONNECT_DONE
  12. time:303.934049   ::   Event:TCPPROXY_EVT_FLOW_CREATE_DRE_SENT
  13. time:303.934198   ::   Event:TCPPROXY_EVT_FLOW_CREATE_DRE_RSP_SUCCESS
  14. time:303.934222   ::   Event:TCPPROXY_EVT_FLOW_CREATE_SSL_DONE
  15. time:303.934232   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS

... (95 more rows truncated)
```

Serviço = T significa que esses fluxos foram otimizados para TCP; RR% está em branco porque a taxa de redução de DRE é informada por fluxo otimizado de DRE (consulte as seções de DRE). Use flow-id <id> em um fluxo ao vivo para ler seu status gravado otimizado/desvio diretamente. O fluxo rastreado acima mostra Serviço = TD (TCP + DRE) e uma sequência completa de eventos de proxy — troca de opções SYN, aceitação/conexão, sucesso de criação de fluxo DRE e dados ativados — confirmando a otimização completa de ponta a ponta.

Classifique o fluxo como otimizado, ignorado/passagem ou com falha. Prefira o status registrado do fluxo ou a razão da passagem a uma inferência de um contador agregado.

4. Verificar recursos de nó de serviço e DRE

Execute os comandos que se aplicam à função do dispositivo:

```
show sdwan appqoe rm-resources
show sdwan appqoe dreopt status detail
show sdwan appqoe dreopt statistics detail
show sdwan appqoe dreopt statistics peer
```

Exemplo de laboratório:

c8000v-appqoe-4 (nó de serviço), 2026-07-15. Saída DRE longa aparada para os campos de integridade/capacidade.

```
c8000v-appqoe-4#show sdwan appqoe rm-resources
=========================================================
              RM Resources
=========================================================
RM Global Resources :
 System Memory Status        : GREEN
 Num sessions Status         : GREEN
 Overall HTX health Status   : GREEN
Registered Service Resources :
TCP Resources:  Max Sessions : 40000   Used Sessions : 0
SSL Resources:  Max Sessions : 40000   Used Sessions : 0
DRE Resources:  Max Sessions : 750     Used Sessions : 0

c8000v-appqoe-4#show sdwan appqoe dreopt status detail
DRE ID              : 52:54:dd:77:4a:a7-019cdaae7bca-9a025f66
DRE uptime          : 126:13:46:58
Health status       : GREEN
DRE cache status    : Active
Disk cache usage    : 29%
Disk latency        : 2 ms
Active alarms:      None
Configuration:
  Profile type            : S
  Maximum connections     : 750
  Disk size               : 60 GB
  Compression type        : DRE-LZ

c8000v-appqoe-4#show sdwan appqoe dreopt statistics detail
Total connections                  : 48
Max concurrent connections         : 2
Current active connections         : 0
Total original bytes               : 63254 MB
Total optimized bytes              : 32691 MB
Overall reduction ratio            : 48%
Disk size used                     : 29%
Cache details:
  Cache status  : Active   Cache Size : 59132 MB   Cache used : 29%
... (per-connection reset/EBP/encode/decode detail truncated)

c8000v-appqoe-4#show sdwan appqoe dreopt statistics peer
  Peer No.  System IP          Hostname    Active connections    Cummulative connections
-----------------------------------------------------------------------------------------
         0  10.30.0.1        c8000v-app                     0                         22
         1  10.20.0.1        appqoe-ser                     0                         26
```

ECOLOGICAMENTE CORRETO, sem alarmes, latência de disco de 2 ms e uma taxa geral de redução saudável de 48%. A tabela de peer confirma que ambos os peers DRE são alcançáveis e compatíveis com a versão (consulte aoim-statistics).

Verifique a integridade, as conexões máximas e ativas, a compatibilidade de pares, o estado do cache, a latência ou os alarmes do disco e os deltas de bytes originais versus otimizados.

5. Capturar Tráfego entre o Controlador de Serviço (SC) e o Nó de Serviço (SN)

Faça uma captura de monitor na interface de túnel entre o SC e o SN. Ele fornece dados claros e não encapsulados.

Método 1: CLI (Embedded Packet Capture - EPC)

Você pode usar o recurso Cisco IOS XE Embedded Packet Capture (EPC) diretamente na CLI do dispositivo. Aqui está a configuração passo a passo usando Tunnel2000000001 como exemplo:

```
monitor capture APPQOE_CAP interface Tunnel2000000001 both
monitor capture APPQOE_CAP match <ipv4 or any or access-list>
monitor capture APPQOE_CAP start
show monitor capture APPQOE_CAP
monitor capture APPQOE_CAP stop
monitor capture APPQOE_CAP export bootflash:appqoe_clear_data.pcap
```

Método 2: GUI (Cisco SD-WAN Manager)

Como alternativa, você pode executar essa captura diretamente na GUI do Cisco SD-WAN Manager (anteriormente vManage), que enviará automaticamente um arquivo .pcap para download:

1. Navegue até **Monitor > Devices**.
2. Escolha o dispositivo (**c8000v-appqoe-4**).
3. Clique em **Solução de problemas** no painel esquerdo.
4. Na seção **Tráfego**, escolha **Captura de pacotes**.
5. No menu suspenso de seleção de interface, escolha a interface de túnel AppQoE (por exemplo, **Tunnel2000000001**).
6. (Opcional) Aplique qualquer filtro de Porta ou IP de Origem/Destino.
7. Clique em **Start** para iniciar a captura e em **Stop** quando terminar. O sistema preparará um arquivo **.pcap** para download.

6. Escolha a próxima seção

Primeiro Resultado Anormal	Continuar para
A política não corresponde nas duas direções	Sem otimização ou desvio
Nenhum nó de serviço íntegro ou qualificado foi atribuído	Integridade e atribuição do nó de serviço
O fluxo é ignorado ou tem um motivo de passagem	Falha de desvio e desvio de desvio
Redefinições de fluxo existentes ou descarte de pacotes	Quedas após o desvio
Somente novas conexões falham durante um burst	vigilante SYN e taxa de conexão
Aumento das falhas de CFT/FID	CFT e capacidade
Paralisações de TCP e evidências de PMTU/MSS presentes	MTU e MSS
O fluxo é otimizado, mas a redução é fraca	Eficácia da DRE

Como a otimização de TCP e a DRE processam um fluxo

Com a otimização de TCP dual-end e DRE, a conexão original é representada por três conexões TCP:

```
Client <-- LAN leg --> Edge A proxy/SN <== overlay leg + DRE ==> Edge B proxy/SN <-- LAN leg --> Server
```

O DRE compacta dados repetidos no trecho de sobreposição. O dispositivo da extremidade oposta reconstrói o fluxo original antes de encaminhá-lo ao destino. Uma topologia de nó de serviço externo adiciona redirecionamento de controlador de serviço para nó de serviço, mas os mesmos pontos de verificação permanecem: política, simetria de caminho, elegibilidade de nó de serviço, desvio de fluxo, compatibilidade de peer e estado DRE.

Termo	Significado neste guia
Otimizada	O serviço AppQoE selecionado está ativo para o fluxo.
Ignorar ou passar	O tráfego continua sem o serviço AppQoE escolhido; inspecione o motivo da passagem.
Soltar	O pacote não continua; isso afeta o usuário e requer uma correlação de queda/erro.
Estado de fluxo de fechamento com falha	Após um fluxo ter sido inspecionado/desviado, algumas falhas de desvio posteriores não podem voltar com segurança para o desvio comum.
SC	Controlador de serviço
SN/ISN/ESN	Nó de serviço/Nó de serviço integrado/Nó de serviço externo
CFT	Tabela de Fluxo de Conexão usada para rastrear fluxos e seu estado de recurso

Sem otimização ou desvio

Confirmar

1. Confirme a correspondência da política e as ações em ambas as direções.
2. Confirme o roteamento simétrico através do par esperado de dispositivos AppQoE.
3. Confirme se o grupo de nós de serviço e as IDs de site estão corretos.
4. Confirme se a DRE está implantada e em bom estado nas duas extremidades.
5. Inspecione o status do fluxo de destino ou a razão da passagem.

Interpretar

- Nenhuma correspondência de política geralmente significa que a classificação, a direção, a VPN ou o anexo estão errados.
- Uma correspondência unilateral pode ativar o tratamento TCP/DRE em uma borda, mas não pode fornecer um caminho DRE válido de duas extremidades.
- Um fluxo pode ignorar corretamente quando o tráfego já está otimizado, é um tipo de fluxo sem suporte, é assimétrico ou corresponde a uma condição de desvio automático.

Corrigir e verificar

Corrija problemas de política, direção, grupo de nós, ID do site ou roteamento. Em seguida, crie uma nova conexão TCP e verifique o fluxo em ambas as extremidades. Não use uma conexão existente para validar uma alteração de política.

Falha e desvio de desvio

Use estatísticas QFP internas somente depois que os comandos de erro e fluxo AppQoE suportados reduzirem o problema:

```
show platform hardware qfp active feature appqoe stats global
show platform hardware qfp active feature appqoe stats all
show platform hardware qfp active feature appqoe internal all
```

Comparar dois instantâneos; esses contadores são cumulativos.

Exemplo de laboratório:

c8000v-appqoe-3 (controlador AppNav), 15-07-2026. Desvio saudável: o índice de SN é Verde e nenhum contador de causa de queda está subindo além dos transientes não saudáveis de SN esperados registrados anteriormente.

```
c8000v-appqoe-3#show platform hardware qfp active feature appqoe stats all
 APPQOE Feature Statistics:
 Global:
     ip-non-tcp-pkts: 1354682
     cft_handle_pkt: 0
     sdvt_divert_req_fail: 1374
     appqoe_svc_on_appqoe_vpn_drop: 0
     appqoe_sng_not_configured: 0
   SDVT Global stats:
     within SDVT syn policer limit: 71660
 SNG: 0 SN Index [0 (Green)], IP: 15.15.15.2, oce_id: 221252816
     APPNAV STATS: toSN 85540403 / 75619122643 fromSN 105667460 / 109985814214
                   NoFoDrop 0 / 0
   SDVT Count stats:
     Active Connections: 4
     decaps: 58388600   encaps: 47119306
   SDVT Packet stats:
     Divert packets / bytes   47119306 / 34139250226
     Reinject packets / bytes 58388600 / 52530512355
     Pkts dropped packets / bytes 10 / 690
   SDVT Drop Cause stats:
     Packets Dropped as SN Unhealthy: 10
```

```
c8000v-appqoe-3#show platform hardware qfp active feature appqoe internal all
 APPQOE Feature Internal:
     syn_policer_rate: 2700
     Cluster Type: External
     Service chnl health : Green
     TCP sub-chnl health : Green
     SSL sub-chnl health : Red
     DREOPT sub-chnl health : Green
 Service-Node-Group: 0
     Active SN Bitmask:  0x0000000000000001
     SN Table:
         Idx | Id  | Ver | Status | DP Status | msecs ago |  IP
           0 |   1 |   2 |  Green |     Green |     27707 |  15.15.15.2
```

cft_handle_pkt: 0 e appqoe_svc_on_appqoe_vpn_drop: 0 exclua falha de CFT/FID e um descarte de VPN recursivo. Os pacotes foram descartados como SN não íntegros: 10 é uma pequena contagem histórica — correlacione-se com as transições de saúde do SN antes de tratá-lo como impacto ativo.

Quedas após Desvio

Confirmar

```
show sdwan appqoe error recent
show sdwan appqoe flow closed all
show sdwan appqoe status
show service-insertion type appqoe service-node-group
```

Se presente na versão e na plataforma, compare stats global ou stats all antes e depois de uma reprodução controlada.

Exemplo de laboratório:

Linha de base íntegra, c8000v-appqoe-3 (controlador), 2026-07-15. Não há descartes de fechamento com falha; o SN está Ativo/Verde e o erro recente mostra queda do vPath devido a PPs: 0 e nova conexão do vPath falhou: 0. O instantâneo de causa descartada do caminho de dados é a evidência decisiva:

```
c8000v-appqoe-3#show platform hardware qfp active feature appqoe stats all | include Drop|Unhealthy|NoF
   SDVT Drop Cause stats:
     Packets Dropped as SN Unhealthy: 10
   NoFoDrop 0 / 0
```

Correlacione o tempo exato de reprodução com esses deltas antes de rotular um reset como fail-close.

Interpretar

Um fluxo inspecionado/desviado anteriormente pode cair quando o nó de serviço se tornar inutilizável ou um redirecionamento posterior do AppNav falhar. Isso protege o estado de proxy estabelecido; a conexão original cliente-servidor nem sempre pode ser reconstruída de forma transparente depois que um caminho de proxy desaparece. Os fluxos da cadeia de serviços também podem cair quando o bypass comum violar o processamento da cadeia.

Não rotule cada redefinição como fail-close. Correlacione o tempo de teste exato com o erro de fluxo, a transição de integridade do nó de serviço e o delta do contador.

Corrigir e verificar

Restaure um nó de serviço qualificado estável e corrija a falha do caminho ou da cadeia de serviços. Valide com uma nova conexão TCP e confirme se o contador de queda relevante para de aumentar.

Integridade e atribuição do nó de serviço

A integridade é específica de função e serviço. A vida, a capacidade de recursos e a integridade de um Otimizador de Aplicativos (AO) específico estão relacionadas, mas não são intercambiáveis.

Estado	Comportamento do caminho de dados a ser esperado
Verde	Elegível para fluxos novos e existentes
Amarelo	O tráfego não SYN inspecionado existente pode continuar; novos SYNs não são desviados para esse nó. Um nó FULL é uma condição Yellow possível
Vermelho ou para baixo	Os fluxos novos/não autorizados são normalmente desviados quando autorizados; os fluxos já inspecionados/com falha no fechamento podem cair; os fluxos da cadeia de serviços podem descartar

Executar:

```
show service-insertion type appqoe service-node-group
show sdwan appqoe status
show sdwan appqoe rm-resources
show sdwan appqoe dreopt status detail
```

Verifique a associação do nó, a ID do site, o tempo de vida, a integridade do AO, a carga/capacidade, os alarmes DRE e a acessibilidade do peer. Antes do Cisco IOS XE Catalyst SD-WAN versão 17.6.1a, os detalhes de integridade do subserviço podem ser limitados; interprete a saída mais antiga de acordo.

Exemplo de laboratório:

Nó saudável, 2026-07-15. No controlador o SN está Vivo com marcadores de saúde per-AO; no nó, o gerenciador de recursos informa Verde com espaço:

```
c8000v-appqoe-3#show service-insertion type appqoe service-node-group | begin Health
Health Markers:
               AO       Load State
              tcp           GREEN 0%
              ssl  RED/NOT AVAILABLE
              dre           GREEN 0%

c8000v-appqoe-4#show sdwan appqoe rm-resources | include Status|Max Sessions|Used Sessions
 System Memory Status        : GREEN
 Num sessions Status         : GREEN
 Overall HTX health Status   : GREEN
TCP Resources:  Max Sessions : 40000   Used Sessions : 0
DRE Resources:  Max Sessions : 750     Used Sessions : 0
```

A carga é de 0% e as sessões usadas estão bem abaixo dos limites de 40000/750, portanto esse nó não está cheio nem amarelo por motivos de capacidade. O status geral amarelo visto em show sdwan appqoe status rastreia apenas o AO SSL não utilizado.

Quando um nó estiver cheio ou amarelo porque está próximo da capacidade de sessão configurada, distribua novas conexões, aumente o perfil de recurso AppQoE suportado onde a plataforma permitir ou adicione capacidade. Não suponha que a adição de DRAM do roteador altere a escala de fluxo de hardware suportada.

CFT e capacidade

appqoe_cft_handle_pkt é um contador de erros. Incrementa quando AppQoE não pode obter um ID de fluxo válido do tratamento CFT. Um valor crescente é a prova de uma falha de manipulação de CFT/FID; um valor baixo em relação ao tráfego total não é prova de saturação.

```
show platform hardware qfp active infrastructure cft status
show platform hardware qfp active feature appqoe stats global
show sdwan appqoe rm-resources
```

Interpretar o estado CFT separadamente da capacidade do nó de serviço:

Exemplo de laboratório:

c8000v-appqoe-3 (controlador), 2026-07-15. Tabela de elementos de memória longa aparada.

```
c8000v-appqoe-3#show platform hardware qfp active infrastructure cft status
===================================== CFT 1/1 =======================================
    CFT id: 0   CFT name: GLOBAL_CFT
    General Parameters:
        Max flows: 1000000
        Number of buckets in CFT hash table: 7227108
    Statistics:
        Total number of flows added               : 1424672
        Total number of flows removed             : 1424664
        Total number of currently allocated flows  : 8
    ... (per-feature memory element table truncated)
```

Número total de fluxos alocados atualmente: 8 contra um máximo de 1.000.000 significa sem pressão na mesa e cft_handle_pkt: 0 nas estatísticas de AppQoE confirma que não há falha na aquisição de FID. Um cft_handle_pkt crescente — não apenas a ocupação de tabela — é o que aponta para um problema de CFT/FID.

- O estado CFT identifica o caudal de borda ou a pressão/erros de identificação do caudal.
- rm-resources identifica a capacidade de sessão do nó de serviço AppQoE.
- Tabelas cheias ou pressão de memória são causas possíveis de falha na aquisição do FID, mas não são as únicas causas.

Se o erro aumentar durante o intervalo de teste, capture o erro/estado CFT, a escala da plataforma, as conexões ativas e os recursos do nó. Reduza a pressão da conexão, reequilibre os nós de serviço, altere o perfil de recursos suportado ou mude para uma plataforma com a escala necessária. Envolva o Cisco TAC antes de tratar um erro CFT genérico como uma conclusão de capacidade de hardware.

Vigilante SYN e Taxa de Conexão

Use o status completo e os contadores documentados. "SDVT_DROP_ERROR" é uma classe de erro; por si só, não é prova de que o vigilante SYN foi acionado.

```
show sdwan appqoe libuinet-statistics
show sdwan appqoe error recent
show sdwan appqoe rm-resources
```

Correlacione falhas de nova conexão com Syn Drop Max PPs alcançados, queda de vPath devido a PPs e o mesmo intervalo de teste. Fluxos de longa duração que permanecem saudáveis, enquanto apenas novos SYNs falham fortalece a hipótese do vigilante.

Exemplo de laboratório:

c8000v-appqoe-4 (nó de serviço), 2026-07-15. libuinet-statistics é longo; o bloco de estatísticas Vpath relevante para o vigilante é mostrado.

```
c8000v-appqoe-4#show sdwan appqoe libuinet-statistics | begin Vpath Statistics
Vpath Statistics:
 Packets In                 : 112733521
 Syn Packets                : 21516
 Syn Drop Max PPS Reached   : 0
 Flow Info Allocs           : 21516
 Flow Info Allocs Failed    : 0
 Vpath drops due to min threshhold: 0
 Failed to create new connection: 0
```

Máx. de PPs de queda de SYN atingidos: 0 (e queda de vPath devido a PPs: 0 (erro recente) determina o vigilante SYN aqui. A taxa configurada no controlador é syn_policer_rate: 2700 (de todos internos); compare-o com a sua taxa SYN oferecida antes de agir.

Reduza a taxa de intermitência, se possível, distribua novas conexões por toda a capacidade íntegra e confirme se os contadores de vigilante documentados param de aumentar. Não sintonize ou contorne limites protetores de um guia genérico; use a orientação de escala da plataforma e do TAC quando as taxas sustentadas se aproximarem dos limites suportados.

MTU e MSS

O ajuste de MSS não é, por si só, um caminho de queda de SYN de AppQoE direto. O caminho de dados calcula um MSS a partir do MTU de adjacência do nó de serviço e da sobrecarga de encapsulamento. Quando possível, ele ajusta o MSS do cliente e armazena um MSS do servidor; quando as informações de MTU não estiverem disponíveis, elas poderão continuar sem esse ajuste.

Portanto, não use sdvt_drop_appnav_divert sozinho como prova de uma falha de cálculo do MSS.

Confirmar

- Registrar a versão do software; o tratamento automatizado de MTU de SC para SN foi introduzido na versão 17.5.1a.
- Verifique uma MTU uniforme suportada através do caminho do controlador de serviço/nó de serviço e da subjacência SD-WAN.
- Use o teste MTU de caminho de bits DF e capturas SYN/SYN-ACK sincronizadas nas bordas relevantes.
- Compare os valores MSS oferecidos e ajustados e verifique se há fragmentação ou buraco negro.

Comando de plataforma útil quando suportado:

```
show platform hardware qfp active feature sdwan datapath session summary
```

Exemplo de laboratório:

c8000v-appqoe-3 (controlador), 15-7-2026.

```
c8000v-appqoe-3#show platform hardware qfp active feature sdwan datapath session summary
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU     Flags
------          ------          -------- -------    ------   -------  ----------- -----    -----
192.168.172.19  192.168.172.6   12346    12346      IPSEC    65528    20005       1442     0x0
192.168.172.19  192.168.172.5   12346    12366      IPSEC    65528    20009       1442     0x0
192.168.172.19  192.168.172.20  12346    12346      IPSEC    65528    20006       1442     0x0
```

As sessões de sobreposição de IPsec relatam um PMTU 1442 uniforme. Um PMTU consistente nos túneis SC/SN (e sem buraco negro nos testes de bit DF) significa que o MSS está sendo derivado de um MTU de adjacência estável — descarte isso antes de tocar o MTU do túnel.

Corrija a política MTU ou MSS do caminho somente depois de confirmar o salto com falha. Não aumente uma MTU de túnel a menos que o caminho completo da subjacência possa transportá-la.

A DRE está ativa, mas a redução é fraca

A baixa redução não significa automaticamente que a DRE foi interrompida. Dados exclusivos de primeira passagem, um cache frio, cargas úteis já compactadas, tráfego criptografado sem o tratamento SSL/TLS necessário, fluxos assimétricos, incompatibilidade de pares ou autodesvio

podem produzir pouca ou nenhuma redução.

Confirmar estado de DRE e colegas

```
show sdwan appqoe dreopt status detail
show sdwan appqoe dreopt statistics detail
show sdwan appqoe dreopt statistics peer
show sdwan appqoe dreopt auto-bypass
show sdwan appqoe ad-statistics
show sdwan appqoe aoim-statistics
show sslproxy status
```

Exemplo de laboratório:

c8000v-appqoe-4 (nó de serviço), 2026-07-15. O status/estatísticas/peer da DRE aparecem na triagem Passo 4. exemplo acima; os comandos restantes:

```
c8000v-appqoe-4#show sdwan appqoe dreopt auto-bypass
c8000v-appqoe-4#
                              (empty — no flows in DRE auto-bypass)

c8000v-appqoe-4#show sdwan appqoe ad-statistics
 [Edge] AD Negotiation Start                : 21513
 [Edge] AD Negotiation Done                 : 21215
 [Edge] Rcvd SYN-ACK w/o AD options         : 21167
 [Core] AD Negotiation Start                : 55
 [Core] AD Negotiation Done                 : 55

c8000v-appqoe-4#show sdwan appqoe aoim-statistics
 Total Number Of Peer Syncs      : 2
 Total Passthrough Connections Due to Peer Version Mismatch   : 0
 LOCAL AO Statistics:  SSL 1.3 (Y),  DRE 0.23 (Y)
 PEER 10.20.0.1:  SSL 1.3 InCompatible=N,  DRE 0.23 InCompatible=N
 PEER 10.30.0.1:  SSL 1.3 InCompatible=N,  DRE 0.23 InCompatible=N

c8000v-appqoe-4#show sslproxy status
CA TP Label                    : PROXY-SIGNING-CA
Dual-Side Optimization         : TRUE
Min TLS Ver                    : TLS Version 1
Clear Mode                     : TRUE
```

Nada está em desvio automático, a negociação do AD está sendo concluída e aoim-statistics mostra 0 passagem de incompatibilidade de versão com os dois pares DRE marcados como incompatíveis = N. sslproxy status mostra Modo de Limpeza: VERDADEIRO, para que as cargas HTTPS atravessem sem descriptografia — redução de DRE fraca esperada em tráfego já criptografado, a menos que o proxy SSL esteja habilitado. A redução de 48% medida (etapa de triagem 4.) é o benefício real da DRE nos fluxos de texto claro.

Verifique:

1. A política de DRE corresponde às duas direções em ambas as extremidades.
2. O fluxo é simétrico e usa os peers esperados.
3. A integridade da DRE e o estado do cache estão ativos sem nenhum alarme relevante.
4. As versões de peer e os recursos de AO são compatíveis.
5. A latência do disco e a utilização de recursos estão dentro da faixa suportada.
6. O fluxo não está em desvio automático.
7. O tráfego criptografado tem a descriptografia SSL/TLS necessária e a configuração de otimização dual-end.

Meça corretamente

Use um conjunto de dados representativo e o mesmo intervalo de tempo em ambas as extremidades. Capture os contadores de bytes originais e otimizados antes e depois do teste. Preferem deltas de intervalo em relação a uma taxa de redução de duração. Se estiver testando o benefício do cache, documente se a execução é de cache frio ou quente e repita o mesmo conteúdo.

Coleta e encaminhamento de evidências

Use primeiro os comandos operacionais suportados. Se a causa não estiver clara, colete:

- Janela de reprodução UTC e tupla/VPN afetada
- Um com falha e um fluxo em boas condições do mesmo par de locais
- Status de AppQoE, erros recentes, política, grupo de nós de serviço e saída de fluxo de ambas as extremidades
- Status de DRE, estatísticas de peer, estado do recurso e deltas de byte de intervalo
- Status CFT e estatísticas QFP AppQoE quando esses comandos existirem
- Admin-tech capturado antes de limpar contadores ou reiniciar serviços

show sdwan appqoe flow all debug é uma saída show expandida, não uma licença para habilitar a depuração de plataforma ampla. Pode ser caro e pode expor tuplas de fluxo; use-o somente para uma coleção curta e com escopo quando os comandos de fluxo direcionados forem insuficientes.

Não publique um comando generic platform-debug sem uma versão/plataforma validada, uma duração de captura, um destino de saída e um procedimento de parada testado. Use as orientações do TAC da Cisco para depuração ativa ou coleta de rastreamento de pacotes em um dispositivo de produção ocupado.

Documentação relacionada da Cisco

- Verificação e solução de problemas do AppQoE
- Otimização de TCP
- Otimização de tráfego com DRE
- Nós de Serviço Externos para Serviços AppQoE
- DRE AppQoE Catalyst SD-WAN: Topologia, configuração, verificação
- 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.