Solución de problemas de optimización de TCP y DRE de AppQoE en SD-WAN de Cisco Catalyst

Contenido

Introducción

Este documento describe cómo resolver problemas de optimización de TCP de AppQoE y DRE en Cisco Catalyst SD-WAN.

Antecedentes

Utilice esta guía cuando un flujo TCP habilitado para AppQoE no esté optimizado, se omita, se restablezca después de la desviación, informe de un nodo de servicio no correcto o muestre una reducción de la eliminación de la redundancia de datos (DRE) menor de la esperada.

Comience con el triaje de 10 minutos. Separa los problemas de ruta y política de los problemas de estado de los nodos de servicio, estado de flujo, capacidad, transporte TCP y eficacia de DRE. Continúe con una sección de síntomas sólo después de saber dónde el flujo deja de comportarse como se esperaba.

Objetivo, alcance y seguridad

En esta guía se tratan los dispositivos Cisco IOS® XE Catalyst SD-WAN que utilizan la optimización de TCP o DRE con nodos de servicio AppQoE integrados o externos.

Elemento de validación	Estado
CLI operativa y de comportamiento público	Alineada con la documentación actual de Cisco Catalyst SD-WAN AppQoE 26.x
Semántica de contador interna	Se vuelve a comprobar con el origen actual de Cisco IOS XE en 2026-07-15
Versión exacta, plataforma y topología utilizadas para la publicación	Captura de laboratorio: Cisco IOS XE Catalyst SD-WAN 17.18.2 en C8000v, AppQoE de nodo de servicio externo. Controlador AppNav c8000v-appqoe-3, nodo de servicio c8000v-appqoe-4, nodo de servicio-appqoe de SN externo (SN IP 15.15.15.2). SNG SNG-APPQOE, política de datos _vpn-10_appqoe-policy (TCP + DRE) en VPN 10. Capturado 2026-07-15.

La disponibilidad y el resultado de los comandos varían según la versión de software, la plataforma y la función. Confirme la sintaxis con la ayuda de comandos en el dispositivo de destino. Los comandos QFP de bajo nivel de esta guía son de solo lectura, pero son específicos

de la plataforma y la versión; utilícelos sólo cuando el comando esté presente.

A continuación se muestran los puntos de control de versiones clave; no sustituyen la documentación de escalabilidad y soporte específica de la plataforma.

Capacidad	Punto de control de versión mínimo
DRE y gestión automatizada de MTU de controlador de servicio/nodo de servicio	Cisco IOS XE Catalyst SD-WAN 17.5.1a
Solución de problemas de AppQoE mejorada y estado de subservicio	17.6.1 bis
Resolución de problemas de detalle de flujo ampliado	17.9.1 bis
Proxy SSL con TLS 1.3	17.13.1a/Manager 20.13.1
DRE a través de grupos de configuración	17.14.1a/Manager 20.14.1

DRE requiere nodos de servicio compatibles en ambos extremos y gestión de flujo simétrico. No se ejecuta en un dispositivo con un rol Service-Controller-Only y AppQoE no se puede combinar con la duplicación de paquetes en la misma conexión. El tráfico cifrado requiere la gestión de SSL/TLS admitida si se desea optimizar su carga.

Antes de cambiar la directiva, borrar las estadísticas, reiniciar un servicio o activar la depuración, capture:

- Versión de software, plataforma y función AppQoE en ambos extremos
- Direcciones IP de origen y destino, puertos, protocolo, VPN y tiempo de prueba UTC
- Secuencia de políticas y asignación de nodo de servicio esperadas
- Si el síntoma afecta a un flujo, un par de sitios o todo el tráfico de AppQoE
- Dos instantáneas de contador en el mismo intervalo de prueba

---

Nota: No borre la caché DRE durante la resolución de problemas inicial. Si se borra, se reinicia DRE y se destruye la caché de calor, lo que cambia la condición que se mide.

Comience aquí: Triage de 10 minutos

1. Verificar el estado de AppQoE y los errores recientes

Ejecutar en los dispositivos periféricos o controladores de servicio participantes:

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

Ejemplo de laboratorio:

c8000v-appqoe-4 (nodo de servicio, 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)
```

Aquí el estado general es AMARILLO solamente porque el SSL AO no está en uso (el proxy SSL está en modo despejado); Los subservicios TCP, de cadena de servicio y de administrador de recursos son de color VERDE. No hay caídas de Ps o fallas de conexión nueva.

Busque los servicios habilitados, el estado actual del nodo de servicio, los errores de flujo recientes y cualquier motivo que explique directamente el comportamiento de omisión o omisión.

2. Verificar la asignación de nodos de servicio y políticas en ambas direcciones

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

Ejemplo de laboratorio:

c8000v-appqoe-3 (controlador de AppNav), 2026-07-15.

```
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
```

La acción accept lleva tanto tcp-optimization como dre-optimization apuntando a SNG-APPQOE, y el SN está activo con tcp/dre GREEN. ssl/http/utd muestra RED/NOT AVAILABLE porque esos AOs no están configurados — se espera para una prueba TCP+DRE solamente.

Confirme que la secuencia deseada coincide con ambas direcciones del flujo de prueba, incluye las acciones TCP/DRE esperadas y apunta al grupo de nodos de servicio deseado. DRE requiere la gestión de flujos simétricos y extremos.

3. Inspeccionar un flujo conocido y rastrearlo de extremo a extremo

```
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
```

Rastreo de un solo flujo

Primero, ejecute show sdwan appqoe flow vpn-id **<vpn-id>** server-ip **<server-ip>** server-port **<port>** en los routers de borde y DC. Este comando devuelve el ID de flujo. Una vez que tenga el ID de flujo, ejecute show sdwan appqoe flow-id **<flow-id>** en ambos routers.

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

Ejemplo de laboratorio:

c8000v-appqoe-4 (nodo de servicio), 2026-07-15. No había flujos activos en el momento de la captura, por lo que se muestra la tabla histórica (cerrada).

```
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)
```

Service = T significa que estos flujos fueron optimizados para TCP; RR% está en blanco porque el ratio de reducción de DRE se informa por flujo optimizado de DRE (ver las secciones DRE). Utilice flow flow-id <id> en un flujo activo para leer su estado de optimización/omisión registrado directamente. El flujo de seguimiento anterior muestra Service = TD (TCP + DRE) y una secuencia de eventos de proxy completa (intercambio de opciones SYN, aceptación/conexión, éxito de creación de flujo DRE y datos habilitados), lo que confirma la optimización completa de extremo a extremo.

Clasifique el flujo como optimizado, omitido/de paso o fallido. Prefiera el estado registrado del motivo de flujo o paso a través sobre una inferencia de un contador agregado.

4. Verificar los recursos del nodo de servicio y DRE

Ejecute los comandos que se aplican a la función de dispositivo:

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

Ejemplo de laboratorio:

c8000v-appqoe-4 (nodo de servicio), 2026-07-15. Salida DRE larga recortada en los campos de estado/capacidad.

```
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
```

Health GREEN, sin alarmas, latencia de disco de 2 ms y una buena tasa de reducción general del 48%. La tabla de pares confirma que ambos pares DRE son alcanzables y compatibles con la versión (vea aoim-statistics).

Verifique el estado, las conexiones máximas y activas, la compatibilidad de pares, el estado de la memoria caché, la latencia o las alarmas del disco y los bytes delta originales versus optimizados.

5. Captura de tráfico entre el controlador de servicios (SC) y el nodo de servicios (SN)

Realice una captura de monitor en la interfaz de túnel entre el SC y el SN. Proporciona datos claros y no encapsulados.

Método 1: CLI (captura de paquetes integrada — EPC)

Puede utilizar la función Cisco IOS XE Embedded Packet Capture (EPC) directamente en la CLI del dispositivo. Esta es la configuración paso a paso utilizando Tunnel2000000001 como ejemplo:

```
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, puede realizar esta captura directamente desde la GUI de Cisco SD-WAN Manager (anteriormente vManage), que generará automáticamente un archivo .pcap para que lo descargue:

1. Vaya a **Monitor > Devices**.
2. Elija su dispositivo (**c8000v-appqoe-4**).
3. Haga clic en **Troubleshooting** en el panel izquierdo.

4. En la sección **Tráfico**, elija **Captura de paquetes**.
5. En el menú desplegable de selección de interfaz, elija la interfaz de túnel AppQoE (por ejemplo, **Tunnel200000001**).
6. (Opcional) Aplique cualquier filtro de puerto o IP de origen o destino.
7. Haga clic en **Start** para comenzar la captura y en **Stop** cuando haya terminado. El sistema preparará un archivo **.pcap** para su descarga.

6. Seleccione la siguiente sección

Primer resultado anormal	Continuar a
La política no coincide en ambas direcciones	Sin optimización ni desvío
No se ha asignado ningún nodo de servicio que cumpla los requisitos o que esté en buen estado	Estado y asignación del nodo de servicio
El flujo se omite o tiene un motivo de paso a través	Desvío fallido y desvío
El flujo existente se restablece o los paquetes se descartan	Caídas después de la desviación
Sólo las nuevas conexiones fallan durante una ráfaga	Regulador SYN y velocidad de conexión
Aumento de los fallos CFT/FID	CFT y capacidad
Se detienen TCP y hay evidencia de PMTU/MSS	MTU y MSS
Flujo optimizado pero reducción débil	eficacia de DRE

Cómo la optimización de TCP y DRE procesan un flujo

Con la optimización TCP de extremo dual y DRE, la conexión original se representa mediante tres conexiones TCP:

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

DRE comprime los datos repetidos en el tramo superpuesto. El dispositivo de extremo lejano reconstruye el flujo original antes de reenviarlo al destino. Una topología de nodo de servicio externo agrega una redirección de controlador de servicio a nodo de servicio, pero siguen existiendo los mismos puntos de control: política, simetría de ruta, elegibilidad de nodo de servicio, desviación de flujo, compatibilidad de pares y estado DRE.

Término	Significado de esta guía
Su infraestructura	El servicio AppQoE seleccionado está activo para el flujo.
Omisión o paso a través	El tráfico continúa sin el servicio AppQoE seleccionado; inspeccione el motivo de paso a través.
Abandonar	El paquete no continúa; esto afecta al usuario y requiere una correlación de caída/error.
Estado de flujo de cierre en caso de fallo	Después de que un flujo haya sido inspeccionado/desviado, algunos fallos de desviación posteriores no pueden volver de forma segura a la derivación normal.
SC	Controlador de servicio
SN/ISN/ESN	Nodo de servicio/Nodo de servicio integrado/Nodo de servicio externo
CFT	Tabla de flujo de conexión utilizada para realizar un seguimiento de los flujos y su estado de función

Sin optimización ni desvío

Confirmar

1. Confirme la coincidencia de políticas y las acciones en ambas direcciones.
2. Confirme el enrutamiento simétrico a través del par esperado de dispositivos AppQoE.
3. Confirme que el grupo de nodos de servicio y los ID de sitio son correctos.
4. Confirme que DRE esté implementado y en buen estado en ambos extremos.
5. Inspeccione el estado del motivo de paso o flujo de destino.

Interpretar

- Ninguna coincidencia de política normalmente significa que la clasificación, dirección, VPN o conexión es incorrecta.
- Una coincidencia unilateral puede habilitar el manejo de TCP/DRE en un borde pero no puede proporcionar una trayectoria DRE válida de dos extremos.
- Un flujo puede omitirse correctamente cuando el tráfico ya está optimizado, es un tipo de flujo no admitido, es asimétrico o coincide con una condición de omisión automática.

Corregir y verificar

Corrija los problemas de política, dirección, grupo de nodos, ID de sitio o enrutamiento. A continuación, cree una nueva conexión TCP y verifique el flujo en ambos extremos. No utilice una conexión existente para validar un cambio de directiva.

Error y omisión de desvío

Utilice las estadísticas internas de QFP sólo después de que los comandos de flujo y error de AppQoE admitidos hayan reducido el 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
```

Compare dos instantáneas; estos contadores son acumulativos.

Ejemplo de laboratorio:

c8000v-appqoe-3 (controlador AppNav), 2026-07-15. Diversión saludable: el índice de SN es verde y ningún contador de causa de caída está subiendo más allá de los transitorios no saludables esperados de SN 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 y appqoe_svc_on_appqoe_vpn_drop: 0 descarta la falla CFT/FID y una caída recursiva de VPN. Los paquetes descartados como SN no saludable: 10 es un pequeño recuento histórico: se correlaciona con las transiciones sanitarias del SN antes de tratarlo como impacto activo.

Caídas después del desvío

Confirmar

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

Si está presente en la versión y la plataforma, compare stats global o stats all antes y después de una reproducción controlada.

Ejemplo de laboratorio:

Línea de base saludable, c8000v-appqoe-3 (controlador), 2026-07-15. No se acumulan caídas de

cierre por fallo; el SN está activo/verde y el error reciente muestra la caída de vPath debido a los PP: 0 y la nueva conexión de vPath ha fallado: 0. La instantánea de la causa de descarte de la ruta de datos es la prueba 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 el tiempo de reproducción exacto con estos deltas antes de etiquetar un reinicio como cerrado a fallos.

Interpretar

Un flujo inspeccionado/desviado anteriormente puede perderse cuando el nodo de servicio se vuelve inutilizable o falla una redirección posterior de AppNav. Esto protege el estado de proxy establecido; la conexión original de cliente a servidor no siempre se puede reconstruir de forma transparente después de que desaparece una ruta de proxy. Los flujos de la cadena de servicio también pueden disminuir cuando el desvío ordinario infringe el procesamiento de la cadena.

No etiquete cada reinicio como cerrado a fallos. Correlacione el tiempo de prueba exacto con el error de flujo, la transición de estado del nodo de servicio y el contador delta.

Corregir y verificar

Restaure un nodo de servicio estable que cumpla los requisitos y corrija la ruta o el fallo de la cadena de servicio. Valide con una nueva conexión TCP y, a continuación, confirme que el contador de caídas correspondiente deja de aumentar.

Estado y asignación de nodo de servicio

El estado es específico de cada función y servicio. La actividad, la capacidad de recursos y el estado de un optimizador de aplicaciones (AO) concreto están relacionados pero no son intercambiables.

Estado	Comportamiento de ruta de datos esperado
Verde	Apto para flujos nuevos y existentes

Estado	Comportamiento de ruta de datos esperado
Amarillo	El tráfico no SYN inspeccionado existente puede continuar; Los nuevos SYN no se desvían a ese nodo. Un nodo FULL es una posible condición amarilla
Rojo o abajo	Los flujos nuevos/no comprometidos normalmente se omiten cuando se permiten; los flujos ya inspeccionados/de fallo-cierre pueden caer; los flujos de la cadena de servicio pueden disminuir

Ejecute:

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

Compruebe la pertenencia al nodo, la ID del sitio, la actividad, el estado del AO, la carga/capacidad, las alarmas DRE y la disponibilidad de los pares. Antes de Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, se pueden limitar los detalles de estado de los subservicios; interprete la salida anterior en consecuencia.

Ejemplo de laboratorio:

Nodo saludable, 2026-07-15. En el controlador el SN está vivo con marcadores de salud por AO; en el nodo, el administrador de recursos informa Verde con margen de ampliación:

```
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
```

La carga es del 0% y las sesiones usadas están muy por debajo de los límites 40000/750, por lo que este nodo no está lleno ni es amarillo por motivos de capacidad. El estado general en amarillo que se observa en show sdwan appqoe sólo se remonta al estado de SSL AO no

utilizado.

Cuando un nodo está lleno o amarillo porque está cerca de su capacidad de sesión configurada, distribuya nuevas conexiones, aumente el perfil de recursos de AppQoE admitido donde la plataforma lo permite o agregue capacidad. No asuma que la adición de DRAM de router cambia la escala de flujo de hardware soportada.

CFT y capacidad

appqoe_cft_handle_pkt es un contador de errores. Aumenta cuando AppQoE no puede obtener un ID de flujo válido de la gestión de CFT. Un valor creciente es evidencia de una falla de manejo de CFT/FID; un valor bajo en relación con el tráfico total no es prueba de saturación.

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

Interpretar el estado CFT por separado de la capacidad del nodo de servicio:

Ejemplo de laboratorio:

c8000v-appqoe-3 (controller), 2026-07-15. Tabla de elementos de memoria larga recortada.

```
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 flujos asignados actualmente: 8 contra un máximo de 1.000.000 significa que no hay presión de tabla y cft_handle_pkt: 0 en el estado de AppQoE confirma que no se ha producido ningún fallo en la adquisición de FID. Un cft_handle_pkt creciente, no solo la ocupación de la tabla, es lo que apunta a un problema de CFT/FID.

- El estado CFT identifica la tabla de flujo de borde o la presión/errores de ID de flujo.

- rm-resources identifica la capacidad de sesión de nodo de servicio de AppQoE.
- Las tablas completas o la presión de memoria son posibles causas de falla de adquisición de FID, pero no las únicas causas.

Si el error aumenta durante el intervalo de prueba, capture el error/estado CFT, la escala de plataforma, las conexiones activas y los recursos de nodo. Reduzca la presión de conexión, vuelva a equilibrar los nodos de servicio, cambie el perfil de recursos admitidos o cambie a una plataforma con la escala necesaria. Póngase en contacto con Cisco TAC antes de tratar un error CFT genérico como una conclusión de capacidad de hardware.

Regulador SYN y velocidad de conexión

Utilice el estado completo y los contadores documentados. "SDVT_DROP_ERROR" es una clase de error; por sí solo no es prueba de que el regulador SYN disparara.

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

Relacionar de forma conjunta los fallos de conexión nueva con los puntos de acceso máximos de descarte sincrónico alcanzados, el descarte de vPath debido a los puntos de acceso y el mismo intervalo de prueba. Los flujos de larga duración que permanecen saludables mientras solo fallan los SYNs nuevos fortalecen la hipótesis del regulador.

Ejemplo de laboratorio:

c8000v-appqoe-4 (nodo de servicio), 2026-07-15. libuinet-statistics es long; se muestra el bloque de estadísticas de Vpath relevante para el regulador.

```
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
```

Se alcanzó el número máximo de puntos de desconexión sincrónica: 0 (y vPath descartado debido a los PP: 0 (error reciente) controla el regulador SYN aquí. La velocidad configurada en el

controlador es syn_policer_rate: 2700 (de la lista interna); compárelo con la tasa SYN ofrecida antes de actuar.

Reduzca la velocidad de ráfaga si es posible, distribuya las nuevas conexiones a través de una capacidad saludable y confirme que los contadores de regulación documentados dejan de aumentar. No ajustar o eludir los límites de protección de una guía genérica; utilice la guía de escala de la plataforma y del TAC cuando las tasas sostenidas se aproximen a los límites admitidos.

MTU y MSS

El ajuste de MSS no es, por sí solo, una ruta de caída SYN de AppQoE directa. La ruta de datos calcula un MSS a partir de la MTU de adyacencia de nodo de servicio y la sobrecarga de encapsulación. Cuando puede, ajusta el MSS del cliente y almacena un MSS del lado del servidor; cuando la información de MTU no está disponible, puede continuar sin ese ajuste.

Por lo tanto, no utilice sdvt_drop_appnav_divert solo como prueba de un error de cálculo de MSS.

Confirmar

- Registre la versión de software; La gestión automatizada de MTU de SC a SN se introdujo en 17.5.1a.
- Verifique una MTU compatible uniforme a través de la ruta del controlador de servicio/nodo de servicio y la capa subyacente de SD-WAN.
- Utilice pruebas DF-bit path-MTU y capturas SYN/SYN-ACK sincronizadas en los bordes relevantes.
- Compare los valores de MSS ofrecidos y ajustados y verifique si hay fragmentación o agujeros negros.

Comando útil de la plataforma donde se soporta:

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

Ejemplo de laboratorio:

c8000v-appqoe-3 (controlador), 2026-07-15.

```
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
```

Las sesiones superpuestas de IPsec informan de una PMTU 1442 uniforme. Una PMTU uniforme a través de los túneles SC/SN (y sin agujeros negros en las pruebas de bit DF) significa que MSS se deriva de una MTU de adyacencia estable; descarte esto antes de tocar la MTU del túnel.

Corrija la política MTU o MSS de trayectoria sólo después de confirmar el salto fallido. No aumente una MTU de túnel a menos que la trayectoria subyacente completa pueda transportarla.

DRE está activo pero la reducción es débil

Una reducción baja no significa automáticamente que DRE se haya roto. Los datos únicos de primer paso, una memoria caché en frío, las cargas útiles ya comprimidas, el tráfico cifrado sin la gestión SSL/TLS necesaria, los flujos asimétricos, la incompatibilidad entre pares o la omisión automática pueden producir una reducción mínima o nula.

Confirmar estado DRE y pares

```
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
```

Ejemplo de laboratorio:

c8000v-appqoe-4 (nodo de servicio), 2026-07-15. El estado de DRE/estadísticas/peer aparecen en el paso de clasificación 4. muestra anterior; los 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
```

No hay nada en la omisión automática, la negociación de AD se está completando y aoim-statistics muestra 0 passthrough de la discordancia de la versión con ambos peers DRE marcados como incompatibles = N. El estado de sslproxy muestra el modo de borrado: TRUE, de modo que las cargas de HTTPS atraviesan sin descifrado (se espera una reducción débil de DRE en el tráfico ya cifrado) a menos que el proxy SSL esté habilitado. La reducción medida del 48% (paso 4.1 de clasificación) es un beneficio real de DRE en los flujos de texto sin formato.

Controle lo siguiente:

1. La política DRE coincide con ambas direcciones en ambos extremos.
2. El flujo es simétrico y utiliza los pares esperados.
3. El estado DRE y el estado de la caché están activos sin alarma relevante.
4. Las versiones de pares y las capacidades de AO son compatibles.
5. La latencia de disco y la utilización de recursos se encuentran dentro del intervalo admitido.
6. El flujo no está en la derivación automática.
7. El tráfico cifrado tiene el descifrado SSL/TLS necesario y la configuración de optimización de dos extremos.

Medir correctamente

Utilice un conjunto de datos representativo y el mismo intervalo de tiempo en ambos extremos. Capture contadores de bytes originales y optimizados antes y después de la prueba. Prefiere deltas de intervalo sobre un ratio de reducción de duración. Si se prueba el beneficio de caché, documente si la ejecución es caché en frío o caché en caliente y repita el mismo contenido.

Recopilación y derivación de pruebas

Utilice primero los comandos operativos compatibles. Si la causa no está clara, recopile:

- Ventana de reproducción UTC y tupla/VPN afectada
- Una falla y un flujo de funcionalidad comprobada del mismo par de sitios
- Estado de AppQoE, errores recientes, política, grupo de nodos de servicio y salida de flujo desde ambos extremos
- estado DRE, estadísticas de peer, estado de recurso y deltas de bytes de intervalo
- Estadísticas de estado CFT y QFP AppQoE cuando existen esos comandos
- Tecnología de administración capturada antes de borrar contadores o reiniciar servicios

show sdwan appqoe flow all debug es una salida show expandida, no una licencia para habilitar la depuración de plataforma amplia. Puede ser costoso y puede exponer tuplas de flujo; utilícelo sólo para una colección corta con ámbito cuando los comandos de flujo de destino sean insuficientes.

No publique un comando generic platform-debug sin una versión/plataforma validada, una duración de captura, un destino de salida y un procedimiento de detención probado. Utilice la guía del TAC de Cisco para la depuración activa o la recopilación de seguimiento de paquetes en un dispositivo de producción ocupado.

Documentación de Cisco relacionada

- Verificación y solución de problemas de AppQoE
- Optimización de TCP
- Optimización del tráfico con DRE
- Nodos de servicios externos para servicios AppQoE
- Catalyst SD-WAN AppQoE DRE: Topología, configuración, verificación
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).