Fehlerbehebung bei AppQoE-TCP-Optimierung und DRE im Cisco Catalyst SD-WAN

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für AppQoE TCP-Optimierung und DRE im Cisco Catalyst SD-WAN beschrieben.

Hintergrundinformationen

Verwenden Sie diesen Leitfaden, wenn ein AppQoE-fähiger TCP-Fluss nicht optimiert ist, umgangen wird, nach der Umleitung zurückgesetzt wird, einen fehlerhaften Serviceknoten meldet oder weniger DRE-Reduzierung (Data Redundancy Elimination) als erwartet anzeigt.

Beginnen Sie mit der 10-minütigen Triage. Sie trennt Richtlinien- und Pfadprobleme von Problemen mit Serviceknoten, Flow-Status, Kapazität, TCP-Transport und DRE-Effektivität. Fahren Sie erst dann mit dem Symptomabschnitt fort, wenn Sie wissen, wo der Fluss nicht mehr wie erwartet verläuft.

Zweck, Umfang und Sicherheit

In diesem Leitfaden werden Cisco IOS® XE Catalyst SD-WAN-Geräte mit TCP-Optimierung oder DRE mit integrierten oder externen AppQoE-Serviceknoten behandelt.

Validierungselement	Status
Public Behavior und betriebliche CLI	abgestimmt auf die aktuelle Cisco Catalyst SD-WAN AppQoE 26.x-Dokumentation
Interne Zählersemantik	Vergleich mit aktueller Cisco IOS XE-Quelle am 15.07.2026 erneut durchgeführt
Genaue für die Veröffentlichung verwendete Version, Plattform und Topologie	Laboraufnahme: Cisco IOS XE Catalyst SD-WAN 17.18.2 auf C8000v, externer Serviceknoten, Anwendungs-QoE. AppNav-Controller c8000v-appqoe-3, Serviceknoten c8000v-appqoe-4, externer SN-Appqoe-Service-Knoten (SN IP 15.15.15.2). SNG SNG-APPQOE, data policy _vpn-10_appqoe-policy (TCP + DRE) on VPN 10. Gefunden am 2026-07-15.

Die Befehlsverfügbarkeit und -ausgabe variiert je nach Softwareversion, Plattform und Rolle. Bestätigen Sie die Syntax mithilfe der Befehlshilfe auf dem Zielgerät. Die einfachen QFP-Befehle in diesem Leitfaden sind schreibgeschützt, aber plattform- und veröffentlichungsspezifisch. verwenden sie nur, wenn der Befehl vorhanden ist.

Die wichtigsten Freigabeprüfpunkte sind unten dargestellt. Sie ersetzen nicht den

plattformspezifischen Support und die skalierte Dokumentation.

Funktionen	Minimaler Freigabeprüfpunkt
DRE und automatisierte Service-Controller-/Service-Node-MTU-Verarbeitung	Cisco IOS XE Catalyst SD-WAN 17.5.1a
Verbesserte AppQoE-Fehlerbehebung und Zustand untergeordneter Services	17.6.1a
Erweiterte Fehlerbehebung mit Flow-Detail	17.9.1a
SSL-Proxy mit TLS 1.3	17.13.1a/Manager 20.13.1
DRE durch Konfigurationsgruppen	17.14.1a/Manager 20.14.1

Für die DRE-Komprimierung sind auf beiden Seiten unterstützte Serviceknoten sowie eine symmetrische Datenflussbehandlung erforderlich. Er wird nicht auf einem Gerät in der reinen Service-Controller-Rolle ausgeführt, und AppQoE kann nicht mit Paketduplizierung auf derselben Verbindung kombiniert werden. Für verschlüsselten Datenverkehr ist die unterstützte SSL/TLS-Verarbeitung erforderlich, um seine Nutzlast zu optimieren.

Erfassen Sie vor dem Ändern von Richtlinien, dem Löschen von Statistiken, dem Neustarten eines Diensts oder dem Aktivieren des Debuggens Folgendes:

- Softwareversion, Plattform und AppQoE-Rolle auf beiden Seiten
- Quell- und Ziel-IP-Adressen, Ports, Protokoll, VPN und UTC-Testzeit
- Erwartete Richtliniensequenz und Dienstknotenzuweisung
- Legt fest, ob das Symptom einen Datenfluss, ein Standortpaar oder den gesamten AppQoE-Datenverkehr beeinflusst.
- Zwei Zählermomentaufnahmen über dasselbe Testintervall

Anmerkung: Löschen Sie den DRE-Cache nicht während der ersten Fehlerbehebung. Durch das Löschen wird DRE neu gestartet, und der warme Cache wird zerstört, wodurch sich der gemessene Zustand ändert.

Hier starten: 10-Minuten-Triage

1. Überprüfen des AppQoE-Status und der letzten Fehler

Ausführen auf den teilnehmenden Edge-Geräten oder Service-Controllern:

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

Laborbeispiel:

c8000v-appqoe-4 (Serviceknoten, 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)
```

Der Gesamtstatus ist GELB, da SSL AO nicht verwendet wird (SSL-Proxy befindet sich im Clear-Modus). Die TCP-, Service-Chain- und Ressourcen-Manager-Subservices sind GRÜN. Keine Verwerfungen von PPs oder Fehler bei neuen Verbindungen.

Suchen Sie nach den aktivierten Services, dem aktuellen Serviceknoten-Status, den neuesten Datenflussfehlern und allen Gründen, die das Umgehungs- oder Löschverhalten direkt erklären.

2. Überprüfen Sie die Richtlinien- und Serviceknoten-Zuweisung in beide Richtungen.

```
show sdwan policy from-vsmart
```

```
show service-insertion type appqoe service-node-group
```

Laborbeispiel:

c8000v-appqoe-3 (AppNav-Controller), 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
```

Die Aktion "accept" führt sowohl TCP-Optimierung als auch Dre-Optimierung und verweist auf SNG-APPQOE, und die SN ist mit tcp/dre GREEN aktiv. ssl/http/utd zeigt RED/NOT AVAILABLE, da diese AOs nicht konfiguriert sind - für einen reinen TCP+DRE-Test wird erwartet.

Vergewissern Sie sich, dass die beabsichtigte Sequenz mit beiden Richtungen des Testflusses übereinstimmt, die erwarteten TCP/DRE-Aktionen enthält und auf die beabsichtigte Serviceknotengruppe verweist. Für die DRE-Komprimierung sind beide Enden und ein

symmetrisches Flow-Handling erforderlich.

3. Überprüfen Sie einen bekannten Fluss, und verfolgen Sie ihn Ende-zu-Ende

```
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
```

Verfolgen eines einzelnen Datenflusses

Führen Sie zunächst show sdwan appqoe flow vpn-id **<vpn-id>** server-ip **<server-ip>** server-port **<port>** auf den Edge- und DC-Routern aus. Dieser Befehl gibt die Fluss-ID zurück. Sobald Sie die Flow-ID haben, führen Sie show sdwan appqoe flow-id **<flow-id>** auf beiden Routern aus.

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

Laborbeispiel:

c8000v-appqoe-4 (Serviceknoten), 2026-07-15. Zum Zeitpunkt der Erfassung waren keine Flows aktiv, daher wird die historische (geschlossene) Tabelle angezeigt.

```
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 bedeutet, dass diese Datenflüsse TCP-optimiert wurden; RR% ist leer, da das DRE-Reduktionsverhältnis pro DRE-optimiertem Fluss gemeldet wird (siehe DRE-Abschnitte). Verwenden Sie flow-id <id> für einen Live-Fluss, um den aufgezeichneten Optimierungs-/Bypass-Status direkt zu lesen. Der nachverfolgte Fluss oben zeigt Service = TD (TCP + DRE) und eine vollständige Proxy-Ereignissequenz — SYN-Optionen, Austausch, Annahme/Verbindung, erfolgreiche Erstellung des DRE-Flusses und aktivierte Daten — mit Bestätigung der vollständigen End-to-End-Optimierung.

Klassifizieren Sie den Datenfluss als optimiert, umgangen/weitergeleitet oder als ausgefallen.

Bevorzugen Sie den aufgezeichneten Status des Flusses oder Durchgangs-Grundes einer Inferenz von einem Sammelzähler.

4. Überprüfen der Serviceknoten-Ressourcen und DRE

Führen Sie die folgenden Befehle für die Geräterolle aus:

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

Laborbeispiel:

c8000v-appqoe-4 (Serviceknoten), 2026-07-15. Lange DRE-Ausgabe auf die Integritäts-/Kapazitätsfelder zugeschnitten.

```
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
```

Status GRÜN, keine Alarme, Festplattenlatenz 2 ms und eine fehlerfreie Gesamtreduzierung von 48 %. Die Peer-Tabelle bestätigt, dass beide DRE-Peers erreichbar und versionskompatibel sind (siehe AOIM-Statistik).

Überprüfen Sie Zustand, maximale und aktive Verbindungen, Peer-Kompatibilität, Cache-Zustand, Festplattenlatenz oder -warnungen sowie Original- und optimierte Byte-Deltas.

5. Erfassen des Datenverkehrs zwischen Service Controller (SC) und Service Node (SN)

Nehmen Sie eine Monitorerfassung an der Tunnelschnittstelle zwischen SC und SN vor. Sie stellt klare, nicht gekapselte Daten bereit.

Methode 1: CLI (Embedded Packet Capture - EPC)

Sie können die Cisco IOS XE Embedded Packet Capture (EPC)-Funktion direkt auf der Kommandozeile des Geräts verwenden. Hier ist die schrittweise Konfiguration mit Tunnel2000000001 als Beispiel:

```
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
```

Methode 2: Benutzeroberfläche (Cisco SD-WAN Manager)

Alternativ können Sie diese Erfassung direkt über die Benutzeroberfläche des Cisco SD-WAN Manager (ehemals vManage) durchführen, die automatisch eine .pcap-Datei ausgibt, die Sie herunterladen können:

1. Navigieren Sie zu **Überwachen > Geräte**.
2. Wählen Sie Ihr Gerät **(c8000v-appqoe-4**).
3. Klicken Sie im linken Bereich auf **Problembehandlung**.
4. Wählen Sie im Abschnitt **Datenverkehr** die Option **Paketerfassung aus**.
5. Wählen Sie in der Dropdown-Liste für die Schnittstellenauswahl die AppQoE-Tunnelschnittstelle aus (z. B. **Tunnel20000001**).
6. (Optional) Wenden Sie alle Quell-/Ziel-IP- oder Port-Filter an.
7. Klicken Sie auf **Start**, um die Erfassung zu starten, und wenn Sie fertig sind, auf **Stopp**. Das System wird eine .**pcap-**Datei zum Download vorbereiten.

6. Wählen Sie den nächsten Abschnitt

Erstes ungewöhnliches Ergebnis	Fahren Sie mit
Die Richtlinie passt nicht in beide Richtungen	Keine Optimierung oder Umleitung
Es wurde kein gültiger Serviceknoten zugewiesen.	Serviceknoten-Status und -Zuweisung
Fluss wird umgangen oder hat einen Grund für den Passthrough	Umleitungsfehler und Umgehung
Vorhandene Flow-Resets oder Paketverluste	Nach der Umleitung fallen
Nur neue Verbindungen fallen während eines Bursts aus	SYN-Überwachung und Verbindungsrate
Zunahme von CFT/FID-Ausfällen	CFT und Kapazität
TCP-Abstürze und PMTU/MSS-Beweise vorhanden	MTU und MSS
Optimierung des Datenflusses, aber Reduzierung schwach	DRE-Effektivität

So verarbeiten TCP-Optimierung und DRE einen Fluss

Bei einer doppelseitigen TCP-Optimierung und DRE wird die ursprüngliche Verbindung durch drei TCP-Verbindungen dargestellt:

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

DRE komprimiert wiederholte Daten auf dem Overlay-Standbein. Das Gerät am anderen Ende rekonstruiert den ursprünglichen Stream, bevor er an das Ziel weitergeleitet wird. Eine externe Serviceknoten-Topologie fügt eine Service-Controller-zu-Service-Knoten-Umleitung hinzu, aber es bleiben dieselben Prüfpunkte erhalten: Richtlinie, Pfadsymmetrie, Serviceknoten-Berechtigung, Datenflussumleitung, Peer-Kompatibilität und DRE-Status.

Begriff	Bedeutung in diesem Leitfaden
im optimalen Zustand zu halten	Der ausgewählte AppQoE-Dienst ist für den Datenfluss aktiv.
Umgehung oder Passthrough	Der Datenverkehr wird ohne den ausgewählten AppQoE-Service fortgesetzt. den Grund für den Passthrough überprüfen.
Verwerfen	Das Paket wird nicht fortgesetzt. Dies wirkt sich auf den Benutzer aus und erfordert eine Drop-and-Error-Korrelation.
Fail-Close-Flow-Status	Nachdem ein Fluss überprüft/umgeleitet wurde, können einige spätere Umleitungsfehler nicht sicher auf den normalen Bypass zurückfallen.
SC	Service-Controller
SN/ISN/ESN	Service Node/Integrated Service Node/External Service Node
CFT	Connection Flow Table zum Verfolgen von Flows und deren Funktionsstatus

Keine Optimierung oder Ablenkung

Bestätigen

1. Bestätigen Sie die Übereinstimmung mit den Richtlinien und die Aktionen in beide Richtungen.
2. Bestätigen Sie ein symmetrisches Routing durch das erwartete Paar AppQoE-Geräte.
3. Bestätigen Sie, dass die Serviceknotengruppe und die Standort-IDs korrekt sind.
4. Vergewissern Sie sich, dass die DRE-Komprimierung an beiden Enden eingesetzt wird und fehlerfrei ist.

5. Überprüfen Sie den Status des Zieldatenflusses oder des Durchlassgrundes.

Interpretieren

- Keine Richtlinienübereinstimmung bedeutet in der Regel, dass Klassifizierung, Richtung, VPN oder Anhang falsch sind.
- Eine einseitige Übereinstimmung kann die TCP/DRE-Verarbeitung an einem Edge aktivieren, jedoch keinen gültigen zweiseitigen DRE-Pfad bereitstellen.
- Ein Datenfluss kann korrekt umgangen werden, wenn der Datenverkehr bereits optimiert ist, ein nicht unterstützter Datenflusstyp ist, asymmetrisch ist oder eine automatische Umgehungsbedingung erfüllt.

Korrigieren und Überprüfen

Korrigieren Sie Richtlinien-, Direktions-, Knotengruppen-, Standort-ID- oder Routing-Probleme. Erstellen Sie dann eine neue TCP-Verbindung, und überprüfen Sie den Datenfluss an beiden Enden. Verwenden Sie keine bestehende Verbindung, um eine Richtlinienänderung zu validieren.

Umleitungsfehler und Umgehung

Verwenden Sie interne QFP-Statistiken erst, nachdem die unterstützten AppQoE-Fließ- und -Fehlerbefehle das Problem eingegrenzt haben:

```
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
```

Vergleichen Sie zwei Snapshots Diese Leistungsindikatoren sind kumulativ.

Laborbeispiel:

c8000v-appqoe-3 (AppNav-Controller), 2026-07-15. Gesunde Umleitung: Der SN-Index ist Grün, und es gibt keine Zähler für Absturzursachen, die über die erwarteten, zuvor aufgezeichneten SN-ungesunden Transienten hinausgehen.

```
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 und appqoe_svc_on_appqoe_vpn_drop: 0 CFT/FID-Ausfall und rekursives VPN-Verwerfen ausschließen. Pakete, die als SN Unhealth verworfen wurden: 10 ist eine kleine historische Zahl - korrelieren Sie mit den SN-Gesundheitsveränderungen, bevor Sie es als aktive Auswirkung behandeln.

Drops nach der Umleitung

Bestätigen

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

Wenn auf der Version und Plattform vorhanden, vergleichen Sie Statistiken global oder Statistiken alle vor und nach einer kontrollierten Reproduktion.

Laborbeispiel:

Gute Ausgangswerte, c8000v-appqoe-3 (Controller), 2026-07-15. Es treten keine Fail-Close-Verluste auf. Die SN ist "Alive/Green", und der kürzlich aufgetretene Fehler zeigt, dass vPath aufgrund von PPs verworfen wurde: 0 und neue vPath-Verbindung fehlgeschlagen: 0. Der datapath-Fallursachenmomentaufnahme ist der entscheidende Beweis:

```
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
```

Korrelieren Sie die genaue Reproduktionszeit mit diesen Deltas, bevor Sie einen Reset als Fail-Close kennzeichnen.

Interpretieren

Ein zuvor überprüfter/umgeleiteter Datenfluss kann verloren gehen, wenn der Serviceknoten unbrauchbar wird oder eine spätere AppNav-Umleitung fehlschlägt. Dadurch wird der etablierte Proxystatus geschützt. Die ursprüngliche Client-Server-Verbindung kann nicht immer transparent wiederhergestellt werden, nachdem ein Proxypfad nicht mehr vorhanden ist. Serviceabläufe können ebenfalls abnehmen, wenn eine normale Umgehung die Kettenverarbeitung verletzt.

Bezeichnen Sie nicht jede Zurücksetzung als Fail-Close. Korrelation der genauen Testzeit mit dem Datenflussfehler, dem Service-Node-Integritätsübergang und dem Zählerdelta

Korrigieren und Überprüfen

Stellen Sie einen stabilen, qualifizierten Serviceknoten wieder her, und korrigieren Sie den Pfad- oder Servicekettenfehler. Mit einer neuen TCP-Verbindung validieren und anschließend bestätigen, dass der entsprechende Zähler nicht mehr ansteigt.

Serviceknoten-Zustand und -Zuweisung

Gesundheit ist rollen- und dienstleistungsspezifisch. Die Lebensdauer, die Ressourcenkapazität und der Status eines bestimmten Anwendungsoptimierers (Application Optimizer, AO) sind zwar miteinander verknüpft, können jedoch nicht ausgetauscht werden.

Status	Erwartetes Datenpfad-Verhalten
Grün	Qualifiziert für neue und bestehende Flows
Gelb	Bestehender überprüfter Verkehr ohne SYN kann fortgesetzt werden; neue SYNs werden nicht zu diesem Knoten umgeleitet. Ein FULL-Knoten ist eine mögliche gelbe Bedingung.
Rot oder Unten	Neue/nicht zugesicherte Datenflüsse werden normalerweise umgangen, wenn dies zulässig ist; Bereits überprüfte/nicht behobene Datenflüsse können abnehmen. Serviceabläufe können abnehmen

Ausgeführt:

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

Überprüfen Sie die Knotenmitgliedschaft, die Standort-ID, die Lebensdauer, den AO-Status, die Last/Kapazität, die DRE-Alarme und die Peer-Erreichbarkeit. Vor der Cisco IOS XE Catalyst SD-WAN-Version 17.6.1a können Details zum Zustand von Subservices eingeschränkt werden. ältere Ausgabe entsprechend interpretieren.

Laborbeispiel:

"Healthy node", 2026-07-15. Auf dem Controller ist die SN "Alive" mit Gesundheitsmarkern pro AO; auf dem Knoten meldet der Ressourcen-Manager Grün mit Headroom:

```
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
```

Die Auslastung beträgt 0 % und verwendete Sitzungen liegen deutlich unter den Grenzwerten von 40000/750, daher ist dieser Knoten aus Kapazitätsgründen weder voll noch gelb. Der gelbe Gesamtstatus in show sdwan appqoe verfolgt nur den nicht verwendeten SSL AO.

Wenn ein Knoten voll oder gelb ist, weil er sich in der Nähe seiner konfigurierten Sitzungskapazität befindet, stellen Sie neue Verbindungen bereit, erhöhen Sie das unterstützte AppQoE-Ressourcenprofil, sofern die Plattform dies zulässt, oder fügen Sie Kapazität hinzu. Gehen Sie nicht davon aus, dass sich durch das Hinzufügen von Router-DRAM die unterstützte Hardware-Ablaufskalierung ändert.

CFT und Kapazität

appqoe_cft_handle_pkt ist ein Fehlerzähler. Er wird erhöht, wenn AppQoE von der CFT-Verarbeitung keine gültige Flow-ID abrufen kann. Ein steigender Wert ist ein Beleg für einen Fehler bei der Handhabung von CFT/FID; ein geringer Wert im Verhältnis zum Gesamtverkehr ist kein Beweis für eine Sättigung.

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

CFT-Status getrennt von der Serviceknoten-Kapazität interpretieren:

Laborbeispiel:

c8000v-appqoe-3 (controller), 2026-07-15. Lange Speicherelementtabelle getrimmt.

```
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)
```

Gesamtanzahl der aktuell zugeordneten Flows: 8 gegen eine maximale Anzahl von 1.000.000 bedeutet keinen Tabellendruck, und cft_handle_pkt: 0 in den AppQoE-Statistiken bestätigt, dass keine FID-Übernahme fehlschlägt. Ein steigender cft_handle_pkt - nicht nur die Belegung des

Tisches - weist auf ein CFT/FID-Problem hin.

- Der CFT-Status identifiziert die Kantenflusstabelle oder den Druck/die Fehler der Flowkennung.
- rm-resources identifiziert die AppQoE-Serviceknoten-Sitzungskapazität.
- Vollständige Tabellen oder Speicherdruck sind mögliche Ursachen für FID-Erfassungsfehler, aber nicht die einzigen Ursachen.

Wenn der Fehler während des Testintervalls zunimmt, erfassen Sie den CFT-Fehler/-Status, die Plattformskalierung, aktive Verbindungen und Knotenressourcen. Verringerung des Verbindungsdrucks, Neuausrichtung der Serviceknoten, Änderung des unterstützten Ressourcenprofils oder Wechsel zu einer Plattform mit der erforderlichen Skalierbarkeit Wenden Sie sich an das Cisco TAC, bevor Sie einen allgemeinen CFT-Fehler als Schlussfolgerung zur Hardwarekapazität behandeln.

SYN-Überwachung und Verbindungsrate

Vollständigen Status und dokumentierte Zähler verwenden. "SDVT_DROP_ERROR" ist eine Fehlerklasse; an sich ist es kein Beweis dafür, dass der SYN-Policer ausgelöst wurde.

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

Neue Verbindungsfehler werden miteinander in Beziehung gesetzt: Syn Drop Max PPs erreicht, vPath aufgrund von PPs unterbrochen und dasselbe Testintervall. Langlebige Kapitalflüsse, die gesund bleiben, während nur neue SYNs scheitern, stärken die Policer-Hypothese.

Laborbeispiel:

c8000v-appqoe-4 (Serviceknoten), 2026-07-15. libuinet-statistics is long; Der für die Richtlinienvergabe relevante Vpath-Statistikblock wird angezeigt.

```
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
```

Maximale Anzahl an Syn-Drop-Paketen erreicht: 0 (und vPath-Verwerfen aufgrund von PPs: 0 in error (kürzlich) den SYN-Policer hier. Die konfigurierte Rate auf dem Controller lautet syn_policer_rate: 2700 (von interner alle); vergleichen Sie diese mit Ihrem SYN-Tarif, bevor Sie handeln.

Reduzieren Sie wenn möglich die Burst-Rate, verteilen Sie neue Verbindungen über eine intakte Kapazität, und stellen Sie sicher, dass die dokumentierten Zähler für die Richtlinienvergabe nicht mehr zunehmen. Keine Sicherheitsgrenzwerte aus einem allgemeinen Leitfaden anpassen oder umgehen; Verwenden Sie die Skalenanleitung der Plattform und des TAC, wenn sich nachhaltige Quoten den unterstützten Grenzwerten annähern.

MTU und MSS

Die MSS-Anpassung ist für sich genommen kein direkter AppQoE-SYN-Drop-Pfad. Der Datenpfad berechnet eine MSS aus der Service-Knoten-Adjacency-MTU und dem Kapselungs-Overhead. Wenn möglich, passt er die Client-MSS an und speichert eine serverseitige MSS. Wenn MTU-Informationen nicht verfügbar sind, kann sie ohne diese Anpassung fortgesetzt werden.

Verwenden Sie daher nicht nur sdvt_drop_appnav_divert als Beweis für einen Fehler bei der MSS-Berechnung.

Bestätigen

- Aufzeichnung der Softwareversion; Die automatisierte SC-to-SN-MTU-Verarbeitung wurde in 17.5.1a eingeführt.
- Überprüfen Sie eine einheitliche unterstützte MTU für den Service-Controller-/Service-Node-Pfad und das SD-WAN-Underlay.
- Verwenden Sie DF-Bit-Pfad-MTU-Tests und synchronisierte SYN/SYN-ACK-Erfassungen an den entsprechenden Flanken.
- angebotene und angepasste MSS-Werte vergleichen und auf Fragmentierung oder Blackholing prüfen.

Nützlicher Plattformbefehl, sofern unterstützt:

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

Laborbeispiel:

c8000v-appqoe-3 (Controller), 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
```

Die IPsec-Overlay-Sitzungen melden eine einheitliche PMTU 1442. Eine konsistente PMTU über die SC/SN-Tunnel hinweg (und kein Blackholing in DF-Bit-Tests) bedeutet, dass die MSS von einer stabilen Adjazenz-MTU abgeleitet wird. Schließen Sie dies aus, bevor Sie die Tunnel-MTU berühren.

Korrigieren Sie die Pfad-MTU- oder MSS-Richtlinie erst, nachdem Sie den fehlerhaften Hop bestätigt haben. Erhöhen Sie eine Tunnel-MTU nur, wenn der komplette Underlay-Pfad sie tragen kann.

DRE ist aktiv, aber die Reduzierung ist schwach

Geringe Reduzierung bedeutet nicht automatisch, dass die DRE-Komprimierung unterbrochen wird. Einzigartige First-Pass-Daten, ein Cold-Cache, bereits komprimierte Payloads, verschlüsselter Datenverkehr ohne die erforderliche SSL/TLS-Verarbeitung, asymmetrische Datenflüsse, Peer-Inkompatibilität oder Auto-Bypass können allesamt zu geringen oder keinen Reduzierungen führen.

DRE-Status und Peers bestätigen

```
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
```

Laborbeispiel:

c8000v-appqoe-4 (Serviceknoten), 2026-07-15. DRE-Status/Statistiken/Peer erscheinen in der Triage Schritt 4. Beispiel oben; die übrigen Befehle:

```
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
```

Nichts ist in Auto-Bypass, die AD-Aushandlung wird abgeschlossen, und die AOIM-Statistik zeigt 0 Passthrough von Versionskonflikten mit beiden als inkompatibel markierten DRE-Peers an = N. Der SSL-Proxy-Status zeigt den Clear Mode an: TRUE, damit HTTPS-Payloads ohne Entschlüsselung übertragen werden - erwartete schwache DRE-Reduzierung für bereits - verschlüsselter Datenverkehr, sofern kein SSL-Proxy aktiviert ist. Die gemessene Reduktion von 48% (Triage Step 4.) ist ein echter DRE-Vorteil auf den Klartext-Flüssen.

Überprüfung:

1. Die DRE-Richtlinie stimmt mit beiden Richtungen überein.
2. Der Fluss ist symmetrisch und verwendet die erwarteten Peers.
3. DRE-Status und Cache-Status sind aktiv, es besteht kein relevanter Alarm.
4. Peer-Versionen und AO-Funktionen sind kompatibel.
5. Die Festplattenlatenz und die Ressourcennutzung liegen innerhalb des unterstützten Bereichs.
6. Der Fluss ist nicht automatisch umgangen.
7. Für verschlüsselten Datenverkehr werden SSL-/TLS-Verschlüsselung und eine zweiseitige Optimierungskonfiguration benötigt.

Richtig messen

Verwenden Sie einen repräsentativen Datensatz und das gleiche Zeitintervall an beiden Enden. Erfassen Sie die ursprünglichen und optimierten Bytezähler vor und nach dem Test. Intervall-Deltas über Lebenszeitverkürzung vorziehen. Wenn Sie den Cache-Vorteil testen, dokumentieren

Sie, ob der Run im Kaltcache oder im Warmcache ausgeführt wird, und wiederholen Sie den gleichen Inhalt.

Evidenzsammlung und Eskalation

Verwenden Sie zuerst unterstützte Betriebsbefehle. Wenn die Ursache unklar bleibt, sammeln Sie:

- UTC-Wiedergabefenster und betroffenes Tupel/VPN
- Ein fehlerhafter und ein zweifelsfrei funktionierender Datenfluss vom gleichen Standortpaar
- AppQoE-Status, Fehler der letzten Zeit, Richtlinie, Service-Node-Gruppe und Flow-Ausgabe von beiden Seiten
- DRE-Status, Peer-Statistiken, Ressourcenstatus und Intervallbyte-Deltas
- CFT-Status und QFP AppQoE-Statistiken, wenn diese Befehle vorhanden sind
- Erfassung durch Admin-Techniker vor dem Löschen von Zählern oder Neustarten von Services

show sdwan appqoe flow all debug is extended show output, not a license to enable wide platform debugging. Es kann teuer sein und kann Strömungstupel freilegen; Verwenden Sie sie nur für eine kurze, umfangreiche Auflistung, wenn die Zielflussbefehle nicht ausreichen.

Veröffentlichen Sie keinen generischen Plattformdebugbefehl ohne eine validierte Version/Plattform, eine Erfassungsdauer, ein Ausgabeziel und eine getestete Stoppprozedur. Nutzen Sie die Anleitung des Cisco TAC für aktives Debuggen oder zur Paket-Nachverfolgung auf einem ausgelasteten Produktionsgerät.

Zugehörige Cisco Dokumentation

- AppQoE-Überprüfung und Fehlerbehebung
- TCP-Optimierung
- Datenverkehrsoptimierung mit DRE
- Externe Service-Knoten für AppQoE-Services
- Catalyst SD-WAN AppQoE DRE: Topologie, Konfiguration, Verifizierung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.