Cisco Catalyst SD-WANのAppQoE TCP最適化およびDREのトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco Catalyst SD-WANでのAppQoE TCP最適化およびDREのトラブルシューティング方法について説明します。

バックグラウンド情報

このガイドは、AppQoE対応TCPフローが最適化されていない場合、バイパスされる場合、転送後にリセットされる場合、異常なサービスノードを報告する場合、またはデータ冗長性排除(DRE)の低下が予想よりも少ない場合に使用します。

10分間のトリアージから開始します。ポリシーとパスの問題を、サービスノードの状態、フロー状態、容量、TCP転送、およびDRE効果の問題から切り離します。「症状」のセクションに進むのは、フローが期待どおりに動作しなくなった場所がわかったときだけです。

目的、範囲、安全性

このガイドでは、Cisco IOS® XE Catalyst SD-WANデバイスについて説明します。このデバイスは、統合された、または外部のAppQoEサービスノードでTCP最適化またはDREを使用します。

検証項目	ステータス
パブリック動作と運用CLI	現行のCisco Catalyst SD-WAN AppQoE 26.xドキュメントとの整合
内部カウンターセマンティクス	2026-07-15で現在のCisco IOS XEソースに対して再確認
公開に使用される正確なリリース、プラットフォーム、トポロジ	ラボキャプチャ：Cisco IOS XE Catalyst SD-WAN 17.18.2 on C8000v、外部サービスノードAppQoEAppNavコントローラc8000v-appqoe-3、サービスノードc8000v-appqoe-4、外部SN appqoe-service-node(SN IP 15.15.15.2)。 VPN 10上のSNG SNG-APPQOE、データポリシー_vpn-10_appqoe-policy(TCP + DRE)。2026年7月15日に取得。

コマンドのアベイラビリティと出力は、ソフトウェアリリース、プラットフォーム、およびロールによって異なります。ターゲット・デバイスでコマンド・ヘルプを使用して構文を確認します。このガイドの低レベルQFPコマンドは読み取り専用ですが、プラットフォームおよびリリースに固有です。コマンドが存在する場合にのみ使用してください。

主なリリースのチェックポイントは次のとおりです。これらは、プラットフォーム固有のサポートおよびスケールに関するドキュメントに取って代わるものではありません。

機能	最小リリースチェックポイント
DREおよび自動化されたサービスコントローラ/サービスノードMTU処理	Cisco IOS XE Catalyst SD-WAN 17.5.1a
AppQoEのトラブルシューティングとサブサービス状態の強化	17.6.1a
拡張されたフロー詳細のトラブルシューティング	17.9.1a
TLS 1.3のSSLプロキシ	17.13.1a/マネージャ20.13.1
設定グループを使用したDRE	17.14.1a/マネージャ20.14.1

DREでは、両端でサポートされているサービスノードと対称フロー処理が必要です。サービスコントローラのみのロールのデバイスでは実行されず、同じ接続でAppQoEをパケット複製と組み合わせることはできません。暗号化されたトラフィックのペイロードを最適化する場合は、サポートされているSSL/TLS処理が必要です。

ポリシーを変更する前、統計情報をクリアする前、サービスを再起動する前、またはデバッグを有効にする前に、次の項目をキャプチャします。

- ソフトウェアリリース、プラットフォーム、および両端でのAppQoEロール
- 送信元および宛先IPアドレス、ポート、プロトコル、VPN、およびUTCテスト時間
- 予想されるポリシーシーケンスとサービスノード割り当て
- 症状が1つのフロー、1つのサイトペア、またはすべてのAppQoEトラフィックに影響するかどうか
- 同じテスト間隔で2つのカウンタースナップショット

注：最初のトラブルシューティングでは、DREキャッシュをクリアしないでください。これをクリアすると、DREが再起動され、ウォームキャッシュが破棄されて、測定条件が変更されます。

ここから開始：10分間のトリアージ

1. AppQoEの状態と最近のエラーの確認

参加しているエッジデバイスまたはサービスコントローラで実行します。

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

ラボのサンプル：

c8000v-appqoe-4（サービスノード、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)
```

SSL AOが使用されていない（SSLプロキシがクリアモードである）ため、全体のステータスは黄色で、TCP、サービスチェーン、およびリソースマネージャサブサービスは緑色です。PPのドロップや新しい接続の障害は発生しません。

有効なサービス、現在のサービスノードの状態、最近のフローエラー、およびバイパス動作またはドロップ動作の直接的な原因を探します。

2. 双方向のポリシーおよびサービスノード割り当ての確認

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

ラボのサンプル：

c8000v-appqoe-3（AppNavコントローラ）、2026年7月15日。

```
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
```

action acceptは、SNG-APPQOEをポイントするtcp-optimizationとdre-optimizationの両方を伝送し、SNはtcp/dre GREENで動作しています。ssl/http/utdはRED/NOT AVAILABLEと表示されますが、これらのAOは設定されていないため、TCP+DREのみのテストが想定されています。

目的のシーケンスがテストフローの両方向に一致し、予期されるTCP/DREアクションを含み、目的のサービスノードグループを指していることを確認します。DREには、両端および対称フロー処理が必要です。

3. 1つの既知のフローを検査し、エンドツーエンドでトレースする

```
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
```

単一のフローのトレース

まず、エッジルータとDCルータの両方でshow sdwan appqoe flow vpn-id <vpn-id> server-ip <server-ip> server-port <port>を実行します。このコマンドは、フローIDを返します。フローIDを取得したら、両方のルータでshow sdwan appqoe flow flow-id <flow-id>を実行します。

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

ラボのサンプル：

c8000v-appqoe-4（サービスノード）、2026-07-15。キャプチャ時にアクティブだったフローはないため、履歴（閉じた）テーブルが表示されます。

```
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は、これらのフローがTCP最適化されたことを意味します。DRE最適化フローごとにDRE削減率が報告されるため、RR %は空白です（DREのセクションを参照）。 ライブフローでflow flow-id <id>を使用し、記録されている最適化/バイパスステータスを直接読み取ります。上記のトレースフローは、サービス= TD(TCP + DRE)と完全なプロキシイベントシーケンス（SYNオプションの交換、受け入れ/接続、DREフロー作成の成功、およびデータの有効化）を示し、完全なエンドツーエンドの最適化を確認しています。

フローを最適化済み、バイパス/パススルー、または障害発生済みとして分類します。1つの集約カウンタからの推定よりも、フローまたはパススルーの記録されたステータスが優先されます。

4. サービスノードリソースとDREの確認

デバイスロールに適用するコマンドを実行します。

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

```
show sdwan appqoe dreopt statistics peer
```

ラボのサンプル：

c8000v-appqoe-4（サービスノード）、2026-07-15。長いDRE出力はhealth/capacityフィールドにトリミングされます。

```
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
```

ヘルスグリーン、アラームなし、ディスク遅延2ミリ秒、全体的に健全な48 %の削減率ピアテーブルは、両方のDREピアが到達可能で、バージョン互換であることを確認します（aoim-

statisticsを参照）。

状態、最大接続とアクティブ接続、ピアの互換性、キャッシュ状態、ディスク遅延またはアラーム、および元のバイトと最適化されたバイトの差分を確認します。

5. サービスコントローラ(SC)とサービスノード(SN)間のトラフィックのキャプチャ

SCとSNの間のトンネルインターフェイスでモニタキャプチャを取得します。カプセル化されていない明確なデータを提供する

方法1:CLI(Embedded Packet Capture — EPC)

Cisco IOS XE Embedded Packet Capture(EPC)機能は、デバイスのCLIで直接使用できます。Tunnel2000000001を例として使用した段階的な設定を次に示します。

```
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
```

方法2:GUI(Cisco SD-WAN Manager)

または、Cisco SD-WAN Manager（以前のvManage）のGUIを使用して、このキャプチャを直接実行することもできます。このGUIは、.pcapファイルを自動的に出力するため、ダウンロードが可能です。

1. **Monitor > Devices**の順に移動します。
2. デバイス(**c8000v-appqoe-4**)を選択します。
3. 左側のペインで**Troubleshooting**をクリックします。
4. **Traffic**セクションで、**Packet Capture**を選択します。
5. インターフェイスの選択ドロップダウンで、AppQoEトンネルインターフェイス（**Tunnel2000000001**など）を選択します。
6. （オプション）送信元/宛先IPまたはポートフィルタを適用します。
7. **Start**をクリックしてキャプチャを開始し、終了したら**Stop**をクリックします。ダウンロードする**.pcap**ファイルが準備されます。

6. 「次のセクション」を選択します

最初の異常結果	次へ
両方向でポリシーが一致しません	最適化または転用なし
正常または適格なサービスノードが割り当てられていません	サービスノードの状態と割り当て
フローがバイパスされているか、またはパススルーの理由がある	転用の失敗およびバイパス
既存のフローリセットまたはパケットのドロップ	流用後のドロップ
バースト中に失敗するのは新しい接続だけです	SYNポリサーおよび接続レート
CFT/FID障害が増加する	CFTとキャパシティ
TCPが停止しており、PMTU/MSSの証拠がある	MTUおよびMSS
フローは最適化されているが、削減は弱い	DREの効果

TCP最適化およびDREによるフローの処理方法

デュアルエンドのTCP最適化とDREを使用すると、元の接続は3つのTCP接続で表されます。

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

DREは、オーバーレイレッグ上の繰り返しデータを圧縮します。遠端デバイスは、宛先に転送する前に元のストリームを再構築します。外部サービスノードトポロジでは、サービスコントローラからサービスノードへのリダイレクションが追加されますが、同じチェックポイント（ポリシー、パスの対称性、サービスノードの適格性、フロー転送、ピアの互換性、およびDRE状態）が残ります。

用語	このガイドでの意味
最適化	選択したAppQoEサービスはフローに対してアクティブです。
バイパスまたはパススルー	トラフィックは、選択されたAppQoEサービスなしで続行されます。パススルーの理由を調べてください。
[Drop]	パケットは続行されません。これはユーザに影響を与えるため、ドロップ/エラーの関連付けが必要です。
フェールクローズのフロー状態	フローが検査/転送された後、その後の転送の失敗の中には、通常のバイパスに安全にフォールバックできないものがあります。
SC	サービスコントローラ
シリアル番号/ISN/ESN	サービスノード/統合サービスノード/外部サービスノード
CFT	フローとその機能の状態を追跡するために使用される接続フローテーブル

最適化または転用なし

Confirm

1. 両方向でポリシーの一致とアクションを確認します。
2. 想定されるAppQoEデバイスのペアを使用して対称ルーティングを確認します。
3. サービスノードグループとサイトIDが正しいことを確認します。
4. DREが導入されていて、両端が正常であることを確認します。
5. ターゲットフローのステータスまたはパススルーの理由を調べます。

解釈

- ポリシーが一致しない場合は、通常、分類、方向、VPN、または添付ファイルが間違っていることを意味します。
- 片側一致では、一方のエッジでTCP/DRE処理を有効にできますが、有効な両端DREパスを指定することはできません。
- トラフィックがすでに最適化されている場合、サポートされていないフロータイプの場合、非対称の場合、または自動バイパスの条件に一致する場合は、フローが正しくバイパスできます。

修正と検証

ポリシー、方向、ノードグループ、サイトID、またはルーティングの問題を修正します。次に、新しいTCP接続を作成し、両端のフローを確認します。既存の接続を使用してポリシーの変更を検証しないでください。

転送の失敗とバイパス

内部QFP統計情報は、サポートされているAppQoE flowおよびerrorコマンドによって問題が絞り込まれた後にのみ使用してください。

```
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
```

2つのスナップショットを比較します。これらのカウンタは累積的です。

ラボのサンプル：

c8000v-appqoe-3（AppNavコントローラ）、2026年7月15日。正常な転送：SNインデックスが緑になり、ドロップ原因カウンタが以前に記録された正常でないSNの推移値を超えつつあります。

```
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およびappqoe_svc_on_appqoe_vpn_drop: 0は、CFT/FID障害と再帰VPNドロップを除外します。SN Unhealthyとしてドロップされたパケット：10は小さな履歴カウントで、アクティブな影響として扱う前にSNのヘルス遷移に対して相関します。

転送の後のドロップ

Confirm

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

リリースおよびプラットフォーム上に存在する場合、制御された1回の複製の前後にstats globalまたはstats allを比較します。

ラボのサンプル：

正常なベースライン、c8000v-appqoe-3（コントローラ）、2026-07-15。フェールクローズによる廃棄は発生していません。SNはAlive/Greenで、エラーrecentはPPs:0によるvPathの廃棄とvPath new connection failed:0を示しています。データパスドロップの原因のスナップショットが決定的な証拠となります。

```
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
```

正確な再生時間とデルタを関連付けてから、リセットにフェールクローズのラベルを付ける

解釈

以前に検査/転送されたフローは、サービスノードが使用不能になるか、以降のAppNavリダイレクトが失敗するとドロップする可能性があります。これにより、確立されたプロキシの状態が保護されます。プロキシパスが消失した後は、元のクライアントとサーバ間の接続を常に透過的に再構築できるとは限りません。サービスチェーンフローは、通常のバイパスがチェーン処理に違反した場合にもドロップする可能性があります。

すべてのリセットにfail-closeというラベルを付けないでください。正確なテスト時間を、フローエラー、サービスノードの状態遷移、およびカウンタの差分と関連付けます。

修正と検証

安定した適格なサービスノードを復元し、パスまたはサービスチェーンの障害を修正します。新しいTCP接続で検証し、関連するドロップカウンタの増加が止まることを確認します。

サービスノードの健全性と割り当て

健全性はロールとサービスに固有です。特定のApplication Optimizer(AO)の活性、リソース容量、および健全性は相互に関連していますが、互換性はありません。

State	期待されるデータパスの動作
緑	新規および既存のフローの対象
黄色	既存の検査済み非SYNトラフィックは続行できます。新しいSYNはそのノードに転送されません。FULLノードは、黄色の状態の1つです
赤または下	新しい/コミットされていないフローは通常、許可されるとバイパスされる。検査済み/フェールクローズ済みのフローはドロップされる。サービスチェーンフローはドロップされる

次のコマンドを実行します。

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

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

ノードのメンバーシップ、サイトID、活性、AOの状態、負荷/容量、DREアラーム、およびピア到達可能性を確認します。Cisco IOS XE Catalyst SD-WANリリース17.6.1aより前では、サブサービスの状態の詳細は制限される可能性があり、古い出力を適宜解釈してください。

ラボのサンプル：

正常なノード、2026-07-15。コントローラでは、SNはAO単位のヘルスマーカーで有効になっています。ノードでは、リソースマネージャがヘッドルームが緑に表示されています。

```
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
```

負荷は0 %であり、使用されているセッションは40000/750の制限の下にあるため、このノードは容量の理由からフルでも黄色でもありません。show sdwan appqoe statusで確認できる黄色の全体的なステータスは、未使用のSSL AOのみをトレースします。

ノードがセッション容量の上限に近いためにフルまたはイエローになった場合は、新しい接続を分散するか、プラットフォームが許可する場所でサポートされているAppQoEリソースプロファイルを増やすか、容量を追加します。ルータのDRAMを追加すると、サポートされるハードウェアのフロースケールが変更されるとは想定しないでください。

CFTとキャパシティ

appqoe_cft_handle_pktはエラーカウンタです。このカウンタは、AppQoEがCFT処理から有効なフローIDを取得できない場合に増加します。CFT/FID処理の失敗を示す値が上昇しています。トラフィック全体に対して低い値を設定しても、飽和状態の証明にはなりません。

```
show platform hardware qfp active infrastructure cft status
```

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

CFT状態をサービスノードのキャパシティとは別に解釈します。

ラボのサンプル：

c8000v-appqoe-3（コントローラ）、2026-07-15。長いメモリ要素のテーブルが削除されました。

```
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)
```

現在割り当てられているフローの総数：8（最大1,000,000に対して）はテーブルのプレッシャーがないことを意味し、AppQoE統計のcft_handle_pkt:0はFID取得エラーがないことを確認します。テーブル占有だけではなく、上昇するcft_handle_pktが、CFT/FIDの問題を示しています。

- CFTステータスは、エッジフローテーブルまたはフローIDの圧力/エラーを示します。
- rm-resourcesは、AppQoEサービスノードセッション容量を識別します。
- FID取得の失敗の原因としてはテーブルがいっぱいであるか、メモリ不足が考えられますが、それが唯一の原因ではありません。

テスト間隔中にエラーが増加した場合は、CFTエラー/状態、プラットフォームスケール、アクティブな接続、およびノードリソースをキャプチャします。接続圧力の軽減、サービスノードの再調整、サポートされるリソースプロファイルの変更、または必要な規模のプラットフォームへの移行。一般的なCFTエラーをハードウェア容量の結論として扱う前に、Cisco TACに連絡してください。

SYNポリサーと接続レート

完全なステータスと文書化されたカウンタを使用します。「SDVT_DROP_ERROR」はエラークラスであり、それ自体はSYNポリサーが起動したことを示すものではありません。

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

Syn Drop Max PPs reached、PPによるvPathドロップ、および同じテスト間隔を使用した、新しい接続の共関連障害新しいSYNに障害が発生しただけでポリサーの仮説が強化される一方で、長期間持続するフローは正常なままです。

ラボのサンプル：

c8000v-appqoe-4（サービスノード）、2026-07-15。libuinet-statisticsは長く、ポリサー関連のVpath統計ブロックが表示されます。

```
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
```

Syn Drop Max PPs reached: 0（およびPPによるvPathドロップ：最近のエラーでは0）。SYNポリサーはここでルールされます。コントローラで設定されているレートはsyn_policer_rate: 2700（internal allから）です。アクションを実行する前に、提示されたSYNレートと比較してください。

可能であればバーストレートを減らし、正常なキャパシティに新しい接続を分散し、文書化されたポリサーカウンタの増加が止まることを確認します。一般的なガイドの保護制限を調整したり、回避したりしないでください。持続レートがサポート制限に近づいたら、プラットフォームとTACのスケールガイダンスを使用してください。

MTUおよびMSS

MSSの調整は、それ自体では、直接のAppQoE SYNドロップパスではありません。データパスは、サービスノード隣接関係MTUとカプセル化オーバーヘッドからMSSを計算します。可能な場合は、クライアントMSSを調整し、サーバ側MSSを保存します。MTU情報が使用できない場合は、調整せずに続行できます。

したがって、MSS計算の失敗の証明としてsdvt_drop_appnav_divertだけを使用しないでください。

Confirm

- ソフトウェアリリースを記録します。17.5.1aでは、SC-to-SN MTUの自動処理が導入されました。
- サービスコントローラ/サービスノードパスとSD-WANアンダーレイでサポートされるMTUが均一であることを確認します。
- 関連するエッジで、DFビットパスMTUテストと同期SYN/SYN-ACKキャプチャを使用します。
- 提示されたMSS値と調整されたMSS値を比較し、フラグメンテーションまたはブラックホール化の有無を確認します。

役に立つplatformコマンド（サポートされている場合）:

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

ラボのサンプル：

c8000v-appqoe-3（コントローラ）、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
```

IPsecオーバーレイセッションは、均一PMTU 1442を報告します。SC/SNトンネル間で一貫性のあるPMTU（およびDFビットテストではブラックホール化なし）は、MSSが安定した隣接関係MTUから派生していることを意味します。トンネルMTUに触れる前にこれを除外してください。

パスMTUまたはMSSポリシーは、障害のあるホップを確認した後にのみ修正してください。完全なアンダーレイパスで伝送できない場合は、トンネルMTUを増やさないでください。

DREはアクティブだがリダクションが弱い

低い削減は、DREの故障を自動的に意味するわけではありません。一意のファーストパスデータ、コールドキャッシュ、すでに圧縮されているペイロード、必要なSSL/TLS処理のない暗号化されたトラフィック、非対称フロー、ピア非互換性、または自動バイパスはすべて、ほとんど、またはまったく削減されない可能性があります。

DRE状態とピアの確認

```
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
```

ラボのサンプル：

c8000v-appqoe-4（サービスノード）、2026-07-15。DRE status/statistics/peerが、上記のトリアージ手順4の例に示されています。残りのコマンドは次のとおりです。

```
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
```

自動バイパスでは何も行われず、ADネゴシエーションが完了し、aoim-statisticsで、両方のDREピアがincompatible = Nとマークされたバージョン不一致による0パススルーが表示されます。sslproxyステータスはClear Mode: TRUEを示すため、HTTPSペイロードは復号化なしで通過します。SSLプロキシが有効でない限り、すでに暗号化されたトラフィックのDRE削減は見込まれます。測定された48 %の削減（トリアージステップ4）は、クリアテキストフローに対する実際のDREの利点です。

確認：

1. DREポリシーは両端で両方向に一致します。
2. フローは対称であり、予期されるピアを使用します。
3. DREの健全性とキャッシュ状態がアクティブで、関連するアラームはありません。
4. ピアのバージョンとAO機能には互換性があります。
5. ディスクの遅延とリソースの使用率がサポートされている範囲内です。
6. フローが自動バイパス内にない。
7. 暗号化されたトラフィックには、必要なSSL/TLS復号化とデュアルエンド最適化設定が適用されます。

正しく測定する

1つの代表的なデータセットを使用し、両端で同じ時間間隔を使用します。テストの前後に、元のバイトカウンタおよび最適化されたバイトカウンタをキャプチャします。ライフタイム短縮率よりもインターバル遅延が優先されます。キャッシュの利点をテストする場合は、コールドキャッシュとウォームキャッシュのどちらを実行するかを文書化し、同じ内容を繰り返します。

証拠の収集とエスカレーション

最初に、サポートされている運用コマンドを使用します。原因が依然として不明な場合は、以下の情報を収集する：

- UTC再現期間と影響を受けるタプル/VPN
- 同じサイトペアからの1つの障害フローと1つの正常なフロー
- AppQoEステータス、最近のエラー、ポリシー、サービスノードグループ、および両端からのフロー出力
- DREステータス、ピア統計情報、リソース状態、およびインターバルバイト差分
- CFTステータスおよびQFP AppQoE統計（これらのコマンドが存在する場合）
- カウンタをクリアする前、またはサービスを再起動する前にキャプチャされたAdmin-tech

show sdwan appqoe flow all debugは拡張されたshow出力であり、広範なプラットフォームデバッグを可能にするライセンスではありません。これはコストが高く、フロータプルが公開される可能性があります。対象フローコマンドが不十分な場合は、短いスコープのコレクションにのみ使用してください。

検証済みのリリース/プラットフォーム、キャプチャ期間、出力先、およびテスト済みの停止手順がない場合は、generic platform-debugコマンドを発行しないでください。ビジー状態の実稼働デバイスでアクティブなデバッグまたはパケットトレース収集を行うには、Cisco TACガイダンスを使用してください。

シスコの関連資料

- AppQoEの検証とトラブルシューティング
- TCP最適化
- DREによるトラフィックの最適化
- AppQoEサービスの外部サービスノード
- Catalyst SD-WAN AppQoE DRE：トポロジ、設定、検証
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。