Cisco Catalyst SD-WAN에서 AppQoE TCP 최적화 및 DRE 문제 해결

목차

소개

이 문서에서는 Cisco Catalyst SD-WAN에서 AppQoE TCP 최적화 및 DRE를 트러블슈팅하는 방법에 대해 설명합니다.

배경 정보

AppQoE 지원 TCP 흐름이 최적화되지 않았거나, 우회되거나, 전환 후 재설정되거나, 비정상 서비스 노드를 보고하거나, 예상보다 적은 DRE(Data Redundancy Elimination) 감소를 보이는 경우 이 가이드를 사용하십시오.

우선 10분 줄입니다. 서비스 노드 상태, 흐름 상태, 용량, TCP 전송 및 DRE-effectiveness 문제와 정책 및 경로 문제를 분리합니다. 흐름이 예상대로 작동하지 않는 위치를 확인한 후에만 증상 섹션을 계속합니다.

목적, 범위 및 안전

이 가이드에서는 통합 또는 외부 AppQoE 서비스 노드가 포함된 TCP 최적화 또는 DRE를 사용하는 Cisco IOS® XE Catalyst SD-WAN 디바이스에 대해 설명합니다.

검증 항목	상태
공개 행동 및 운영 CLI	최신 Cisco Catalyst SD-WAN AppQoE 26.x 설명서에 맞게 조정
내부 카운터 의미 체계	2026-07-15의 현재 Cisco IOS XE 소스와 다시 비교
게시에 사용되는 정확한 릴리스, 플랫폼 및 토폴로지	랩 캡처: C8000v의 Cisco IOS XE Catalyst SD-WAN 17.18.2, 외부 서비스 노드 AppQoE. AppNav Controller c8000v-appqoe-3, 서비스 노드 c8000v-appqoe-4, 외부 SN appqoe-service-node(SN IP 15.15.15.2). VPN 10의 SNG SNG-APPQOE, 데이터 정책 _vpn-10_appqoe-policy(TCP + DRE). 2026-07-15에 캡처됨.

명령의 가용성과 출력은 소프트웨어 릴리스, 플랫폼 및 역할에 따라 달라집니다. 대상 장치에 대한 명령 도움말을 사용하여 구문을 확인합니다. 이 가이드의 하위 레벨 QFP 명령은 읽기 전용이지만 플랫폼과 릴리스에 따라 다릅니다. 명령이 있는 경우에만 사용하십시오.

주요 릴리스 체크포인트는 다음과 같습니다. 플랫폼별 지원 및 확장 문서를 대체하지는 않습니다.

기능	최소 릴리스 검사점
DRE 및 자동화된 서비스 컨트롤러/서비스 노드 MTU 처	Cisco IOS XE Catalyst SD-WAN

기능	최소 릴리스 검사점
리	17.5.1a
향상된 AppQoE 문제 해결 및 하위 서비스 상태	17.6.1a
확장된 흐름 세부 문제 해결	17.9.1a
TLS 1.3을 사용하는 SSL 프록시	17.13.1a/관리자 20.13.1
구성 그룹을 통한 DRE	17.14.1a/관리자 20.14.1

DRE에는 양쪽 끝에서 지원되는 서비스 노드와 대칭 흐름 처리가 필요합니다. 서비스 컨트롤러 전용 역할의 디바이스에서는 실행되지 않으며 AppQoE는 동일한 연결에서 패킷 복제와 결합할 수 없습니다. 암호화된 트래픽의 페이로드를 최적화하려면 지원되는 SSL/TLS 처리가 필요합니다.

정책을 변경하거나, 통계를 지우거나, 서비스를 다시 시작하거나, 디버그를 활성화하기 전에 다음을 캡처합니다.

- 소프트웨어 릴리스, 플랫폼 및 양단의 AppQoE 역할
- 소스 및 목적지 IP 주소, 포트, 프로토콜, VPN, UTC 테스트 시간
- 필요한 정책 시퀀스 및 서비스 노드 할당
- 증상이 하나의 플로우, 하나의 사이트 쌍 또는 모든 AppQoE 트래픽에 영향을 미치는지 여부
- 동일한 테스트 간격 동안 카운터 스냅숏 2개

참고: 초기 트러블슈팅 중에 DRE 캐시를 지우지 마십시오. 이를 지우면 DRE가 다시 시작되고 웜 캐시가 삭제되며, 이는 측정되는 조건이 변경됩니다.

여기서 시작: 10분 분류

1. AppQoE 상태 및 최근 오류 확인

참여 에지 디바이스 또는 서비스 컨트롤러에서 실행:

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

실습 샘플:

c8000v-appqoe-4(서비스 노드, 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 AO가 사용 중이 아니기 때문에 전체 상태가 노란색입니다(SSL 프록시가 지우기 모드). TCP, 서비스 체인 및 리소스 관리자 하위 서비스는 녹색입니다. PP가 삭제되거나 새 연결 오류가 발생하지 않습니다.

활성화된 서비스, 현재 서비스 노드 상태, 최근 플로우 오류 및 우회 또는 삭제 동작을 직접 설명하는 모든 이유를 확인합니다.

2. 양방향 정책 및 서비스 노드 할당 확인

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

실습 샘플:

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
```

이 작업은 SNG-APPQOE를 가리키는 tcp-optimization 및 dre-optimization을 모두 전달하며 SN은 tcp/dre GREEN으로 활성 상태입니다. ssl/http/utd는 RED/NOT AVAILABLE을 표시합니다. TCP+DRE 전용 테스트에 대해 이러한 AO가 구성되지 않았기 때문입니다.

의도된 시퀀스가 테스트 흐름의 양방향과 일치하며, 예상되는 TCP/DRE 작업을 포함하며, 의도된 서비스 노드 그룹을 가리키는지 확인합니다. DRE에는 양쪽 끝과 대칭 흐름 처리가 필요합니다.

3. 알려진 흐름 하나를 검사하고 이를 엔드 투 엔드로 추적

```
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
```

단일 흐름 추적

먼저 에지와 DC 라우터 모두에서 show sdwan appqoe flow vpn-id <vpn-id> server-ip <server-ip> server-port <port>를 실행합니다. 이 명령은 흐름 ID를 반환합니다. flow ID가 있으면 두 라우터에서 show sdwan appqoe flow-id <flow-id>를 실행합니다.

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

실습 샘플:

c8000v-appqoe-4(서비스 노드), 2026-07-15. 캡처 시간에 활성화된 플로우가 없으므로 기록(닫힌) 테이블이 표시됩니다.

```
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 = T는 이러한 플로우가 TCP에 최적화되었음을 의미합니다. DRE 최적화 플로우당 DRE 감소 비율이 보고되므로 RR%가 비어 있습니다(DRE 섹션 참조). 기록된 최적화/바이패스 상태를 직접 읽으려면 라이브 플로우에서 flow flow-id <id>를 사용하십시오. 위의 추적된 흐름은 서비스 = TD(TCP + DRE) 및 완전한 프록시 이벤트 시퀀스(SYN 옵션 교환, 수락/연결, DRE 흐름 생성 성공 및 데이터 활성화)를 보여 주며, 이를 통해 완전한 엔드 투 엔드 최적화가 확인됩니다.

플로우를 최적화, 우회/통과 또는 실패로 분류합니다. 하나의 집계 카운터에서 추론하는 것보다 흐름 또는 통과 사유의 기록된 상태를 선호합니다.

4. 서비스 노드 리소스 및 DRE 확인

디바이스 역할에 적용되는 명령을 실행합니다.

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

실습 샘플:

c8000v-appqoe-4(서비스 노드), 2026-07-15. 상태/용량 필드로 잘린 긴 DRE 출력입니다.

```
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
```

녹색, 경보 없음, 디스크 대기 시간 2ms, 전체 감소 비율 48% 정상 피어 테이블에서는 두 DRE 피어에 모두 연결할 수 있으며 버전이 호환되는지 확인합니다(aoim-statistics 참조).

상태, 최대 및 활성 연결, 피어 호환성, 캐시 상태, 디스크 레이턴시 또는 경보, 원래 바이트 델타와 최적화된 바이트 델타를 확인합니다.

5. SC(Service Controller)와 SN(Service Node) 간의 트래픽 캡처

SC와 SN 간의 터널 인터페이스에서 모니터 캡처를 수행합니다. 캡슐화되지 않은 명확한 데이터를 제공합니다.

방법 1: CLI(Embedded Packet Capture — EPC)

디바이스 CLI에서 직접 Cisco IOS XE EPC(Embedded Packet Capture) 기능을 사용할 수 있습니다. 다음은 Tunnel2000000001을 사용한 단계별 컨피그레이션의 예입니다.

```
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
```

방법 2: GUI(Cisco SD-WAN Manager)

또는 Cisco SD-WAN Manager(이전의 vManage) GUI에서 직접 이 캡처를 수행할 수 있습니다. 그러면 다운로드할 .pcap 파일이 자동으로 출력됩니다.

1. Monitor(**모니터) > Devices(디바이스)로 이동합니다**.
2. 장치(**c8000v-appqoe-4**)를 선택합니다.
3. 왼쪽 **창**에서 Troubleshooting(문제 해결)을 클릭합니다.
4. **Traffic** 섹션 아래에서 **Packet** Capture를 **선택합니다**.
5. 인터페이스 선택 드롭다운에서 AppQoE 터널 인터페이스(예: Tunnel200000000001)**를** 선택합니다.
6. (선택 사항) 모든 소스/대상 IP 또는 포트 필터를 적용합니다.
7. 캡처를 시작하려면 **Start**(**시작**)를 클릭하고, 완료되면 **Stop(중지**)을 클릭합니다. 시스템에서 다운로드할 **.pcap** 파일을 준비합니다.

6. 다음 섹션을 선택합니다

첫 번째 이상 결과	계속
정책이 양방향으로 일치하지 않음	최적화 또는 전환 없음

첫 번째 이상 결과	계속
정상 또는 적격 서비스 노드가 할당되지 않았습니다.	서비스 노드 상태 및 할당
흐름이 우회되거나 통과 사유가 있음	전환 실패 및 우회
기존 흐름 재설정 또는 패킷 삭제	전환 후 삭제
버스트 중에는 새 연결만 실패함	SYN 폴리서 및 연결 속도
CFT/FID 장애 증가	CFT 및 용량
TCP 정지 및 PMTU/MSS 증거 있음	MTU 및 MSS
흐름이 최적화되어 있지만 감소가 미약함	DRE 유효성

TCP 최적화 및 DRE가 흐름을 처리하는 방법

듀얼 엔드 TCP 최적화 및 DRE를 사용하는 경우 원래 연결은 3개의 TCP 연결로 표시됩니다.

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

DRE는 오버레이 레그에서 반복된 데이터를 압축합니다. 원단 디바이스는 목적지로 전달하기 전에 원본 스트림을 재구성합니다. 외부 서비스 노드 토폴로지는 서비스 컨트롤러 간 서비스 노드 리디렉션을 추가하지만 동일한 체크포인트가 남아 있습니다. 정책, 경로 대칭, 서비스 노드 자격, 흐름 전환, 피어 호환성 및 DRE 상태.

용어	이 가이드의 의미
유지하도록 합니다	선택한 AppQoE 서비스가 흐름에 대해 활성 상태입니다.
우회 또는 통과	선택한 AppQoE 서비스 없이 트래픽이 계속됩니다. passthrough 이유를 검사합니다.
삭제	패킷이 계속되지 않습니다. 이는 사용자에게 영향을 미치며 삭제/오류 상관관계가 필요합니다.

용어	이 가이드의 의미
실패 닫기 흐름 상태	흐름을 검사/전환한 후에는 나중에 전환 실패가 정상적으로 일반 우회로 돌아갈 수 없습니다.
SC	서비스 컨트롤러
SN/ISN/ESN	서비스 노드/통합 서비스 노드/외부 서비스 노드
CFT	플로우 및 해당 기능 상태를 추적하는 데 사용되는 연결 플로우 테이블

최적화 또는 전환 없음

확인

1. 정책 일치 및 양방향의 작업을 확인합니다.
2. 예상되는 AppQoE 디바이스 쌍을 통해 대칭 라우팅을 확인합니다.
3. 서비스 노드 그룹 및 사이트 ID가 올바른지 확인합니다.
4. DRE가 배포되어 있고 양쪽 끝에서 정상 상태인지 확인합니다.
5. 대상 플로우 또는 통과 사유의 상태를 검사합니다.

해석

- 정책 일치가 없으면 일반적으로 분류, 방향, VPN 또는 첨부 파일이 잘못되었음을 의미합니다.
- 한면 일치는 한 에지에서 TCP/DRE 처리를 활성화할 수 있지만 올바른 양단 DRE 경로를 제공할 수는 없습니다.
- 트래픽이 이미 최적화되었거나, 지원되지 않는 흐름 유형이거나, 비대칭이거나, 자동 바이패스 조건과 일치하는 경우 흐름이 올바르게 우회할 수 있습니다.

수정 및 확인

올바른 정책, 방향, 노드 그룹, 사이트 ID 또는 라우팅 문제. 그런 다음 새 TCP 연결을 생성하고 양쪽 끝에서 플로우를 확인합니다. 기존 연결을 사용하여 정책 변경을 검증하지 마십시오.

전환 실패 및 우회

지원되는 AppQoE flow 및 error 명령으로 문제가 해결된 후에만 내부 QFP 통계를 사용합니다.

```
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
```

두 스냅샷 비교 이 카운터는 누적됩니다.

실습 샘플:

c8000v-appqoe-3(AppNav Controller), 2026-07-15. 정상 전환: sn 인덱스는 녹색이며 어떤 드롭 원인 카운터도 이전에 기록된 예상 SN 비정상 과도 상태를 넘어서지 않습니다.

```
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 및 appqoe_svc_on_appqoe_vpn_drop: 0은 CFT/FID 실패와 recursive-VPN 삭제를 배제합니다. SN Unhealthy로 삭제된 패킷: 10은 작은 기록 수이며, 활성 영향으로서 처리하기 전에 SN 상태 전환에 대한 상관관계를 나타냅니다.

전환 후 삭제

확인

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

릴리스 및 플랫폼에 있는 경우 통계 global 또는 한 번의 제어된 재생 전후의 통계를 비교합니다.

실습 샘플:

정상 기준, c8000v-appqoe-3(컨트롤러), 2026-07-15. 고장 종료 삭제는 발생하지 않습니다. sn이 Alive/Green이고 error recent는 PP로 인한 vPath 삭제를 보여줍니다. 0 및 vPath 새 연결 실패: 0. 데이터 경로 삭제 원인 스냅샷이 결정 증거입니다.

```
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
```

재설정을 fail-close로 지정하기 전에 이러한 델타에 대해 정확한 재생 시간의 상관관계를 분석합니다.

해석

서비스 노드를 사용할 수 없게 되거나 나중에 AppNav 리디렉션이 실패하는 경우 이전에 검사/전환된 흐름이 끊어질 수 있습니다. 이는 설정된 프록시 상태를 보호합니다. 프록시 경로가 사라진 후에는 원래 클라이언트-서버 연결을 항상 투명하게 재구성할 수 없습니다. 일반적인 우회가 체인 처리를 위반할 경우에도 서비스 체인 흐름이 중단될 수 있습니다.

모든 재설정에 대해 fail-close로 레이블을 지정하지 마십시오. 정확한 테스트 시간을 흐름 오류, 서비스 노드 상태 전환 및 카운터 델타와 상호 연결합니다.

수정 및 확인

안정적인 적격 서비스 노드를 복원하고 경로 또는 서비스 체인 오류를 수정합니다. 새 TCP 연결로 검증한 다음 관련 중단 카운터가 증가하지 않는지 확인합니다.

서비스 노드 상태 및 할당

상태는 역할과 서비스에 따라 다릅니다. 특정 AO(Application Optimizer)의 라이브니스, 리소스 용량 및 상태는 관련이 있지만 상호 교환이 불가능합니다.

상태	Datapath 동작 예상
초록색	신규 및 기존 플로우에 적합
노란색	기존 검사된 비 SYN 트래픽은 계속할 수 있습니다. 새 SYN은 해당 노드로 전환되지 않습니다. FULL 노드는 하나의 가능한 노란색 상태입니다
빨간색 또는 아래쪽	새 흐름/커밋되지 않은 흐름이 허용되는 경우 정상적으로 우회합니다. 이미 검사/장애 조치 완료 플로우는 감소할 수 있습니다. 서비스 체인 플로우는

실행:

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

노드 멤버십, 사이트 ID, 라이브니스, AO 상태, 로드/용량, DRE 경보 및 피어 연결성을 확인합니다. Cisco IOS XE Catalyst SD-WAN 릴리스 17.6.1a 이전에는 하위 서비스 상태 세부 정보가 제한될 수 있습니다. 그에 따라 이전 출력을 해석합니다.

실습 샘플:

Healthy node, 2026-07-15. 컨트롤러에서 SN은 AO당 상태 마커와 함께 Alive입니다. 노드에서 리소스 매니저가 녹색(헤드룸 있음)을 보고합니다.

```
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
```

로드는 0%이고 사용된 세션은 40000/750 제한 미만이므로 이 노드는 용량상의 이유로 가득 차거나 노란색이 아닙니다. show sdwan appqoe 상태에 표시된 노란색 전체 상태는 사용되지 않은 SSL AO에만 추적됩니다.

구성된 세션 용량에 근접하여 노드가 가득 찼거나 노란색이면 새 연결을 배포하거나, 플랫폼에서 허용하는 지원되는 AppQoE 리소스 프로필을 늘리거나, 용량을 추가합니다. 라우터 DRAM을 추가하면 지원되는 하드웨어 플로우 크기가 변경된다고 가정하지 마십시오.

CFT 및 용량

appqoe_cft_handle_pkt는 오류 카운터입니다. AppQoE가 CFT 처리에서 유효한 플로우 ID를 가져올 수 없는 경우 증가합니다. 값이 증가하면 CFT/FID 처리 실패의 증거가 됩니다. 총 트래픽에 비해 낮은 값은 포화 상태가 아닙니다.

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

서비스 노드 용량과 별도로 CFT 상태를 해석합니다.

실습 샘플:

c8000v-appqoe-3(컨트롤러), 2026-07-15. 긴 메모리 요소 테이블이 잘렸습니다.

```
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)
```

현재 할당된 총 플로우 수: 최대 1,000,000에 대해 8은 테이블 압력이 없음을 의미하며 cft_handle_pkt: AppQoE 통계에서 0이(가) FID 획득 실패를 확인하지 않습니다. 테이블 점유만 있는 것이 아니라 cft_handle_pkt의 상승이 CFT/FID 문제를 가리키는 것입니다.

- CFT 상태는 에지 플로우 테이블 또는 플로우 ID 압력/오류를 식별합니다.
- rm-resources는 AppQoE 서비스 노드 세션 용량을 식별합니다.
- 전체 테이블 또는 메모리 압력은 FID 획득 실패의 가능한 원인일 수 있지만 유일한 원인은 아닙니다.

테스트 간격 동안 오류가 증가하는 경우 CFT 오류/상태, 플랫폼 규모, 활성 연결 및 노드 리소스를 캡처합니다. 연결 압력을 줄이고, 서비스 노드의 균형을 다시 맞추거나, 지원되는 리소스 프로필을 변경하거나, 필요한 규모의 플랫폼으로 이동하십시오. 일반적인 CFT 오류를 하드웨어 용량 결론으로 처리하기 전에 Cisco TAC를 활용하십시오.

SYN 폴리서 및 연결 속도

전체 상태 및 문서화된 카운터를 사용합니다. "SDVT_DROP_ERROR"는 오류 클래스입니다. 그 자체로는 SYN 폴리서가 작동했다는 증거가 아닙니다.

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

Syn Drop Max PP에 도달하고, PP로 인한 vPath Drop 및 동일한 테스트 간격을 사용하여 새 연결 실패를 공동 연결합니다. 새로운 SYN만 실패하는 동안 수명이 긴 플로우는 건강하게 유지되어 정책 가설이 강화됩니다.

실습 샘플:

c8000v-appqoe-4(서비스 노드), 2026-07-15. libuinet-statistics는 깁니다. policer 관련 Vpath 통계 블록이 표시됩니다.

```
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 PP 도달: 0(PP로 인한 vPath 중단: 0의 오류 최근) 여기서 SYN 폴리서를 제어합니다. 컨트롤러에서 구성된 속도는 syn_policer_rate입니다. 2700(내부 전체에서); 작업을 수행하기 전에 제공된 SYN 비율과 비교합니다.

가능한 경우 버스트 속도를 줄이고, 정상적인 용량에 새 연결을 배포하고, 문서화된 폴리서 카운터의 증가가 중지되었는지 확인합니다. 일반 가이드에서 보호 제한을 조정하거나 우회하지 마십시오. 지속적인 속도가 지원되는 한계에 도달할 경우 플랫폼 및 TAC의 규모 지침을 사용하십시오.

MTU 및 MSS

MSS 조정은 그 자체로 직접 AppQoE SYN-drop 경로가 아닙니다. 데이터 경로는 서비스 노드 인접성 MTU 및 캡슐화 오버헤드로부터 MSS를 계산합니다. 가능하다면 클라이언트 MSS를 조정하고 서버측 MSS를 저장합니다. mtu 정보를 사용할 수 없는 경우, 이를 조정하지 않고 계속할 수 있습니다.

따라서 sdvt_drop_appnav_divert만 MSS 계산 실패의 증거로 사용하지 마십시오.

확인

- 소프트웨어 릴리스 기록 자동화된 SC-SN MTU 처리는 17.5.1a에 도입되었습니다.
- 서비스 컨트롤러/서비스 노드 경로 및 SD-WAN 언더레이에서 지원되는 MTU를 동일하게 확인합니다.
- 관련 에지에서 DF 비트 경로 MTU 테스트 및 동기화된 SYN/SYN-ACK 캡처를 사용합니다.
- 제공된 MSS 값과 조정된 MSS 값을 비교하고 프래그먼트화 또는 블랙홀링을 확인합니다.

지원되는 경우 유용한 플랫폼 명령:

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

실습 샘플:

c8000v-appqoe-3(컨트롤러), 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 오버레이 세션은 균일한 PMTU 1442를 보고합니다. SC/SN 터널 전반에 걸쳐 일관된 PMTU가 적용되며 DF 비트 테스트에서는 블랙홀이 발생하지 않는다는 의미는 MSS가 안정적인 인접성 MTU에서 파생됨을 의미합니다. 터널 MTU를 건드리기 전에 이 기능을 사용하지 마십시오.

실패한 홉을 확인한 후에만 경로 MTU 또는 MSS 정책을 수정합니다. 전체 언더레이 경로가 터널 MTU를 전달할 수 있는 경우가 아니면 터널 MTU를 늘리지 마십시오.

DRE가 활성 상태이지만 감소가 약함

감소율이 낮다고 해서 DRE가 자동으로 손상되는 것은 아닙니다. 고유한 첫 번째 패스 데이터, 콜드 캐시, 이미 압축된 페이로드, 필요한 SSL/TLS 처리 없이 암호화된 트래픽, 비대칭 플로우, 피어 비호환성 또는 자동 우회로 인해 거의 또는 전혀 감소되지 않습니다.

DRE 상태 및 피어 확인

```
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
```

실습 샘플:

c8000v-appqoe-4 (서비스 노드), 2026-07-15. DRE 상태/통계/피어는 4단계 트리지에 나타납니다. 위의 샘플; 나머지 명령:

```
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
```

자동 우회에 아무 것도 없고, AD 협상이 완료되고 있으며, aoim-statistics는 버전 불일치에서 두 DRE 피어 모두 비호환됨으로 표시된 0개의 통과를 표시합니다. = N. sslproxy 상태는 지우기 모드를 표시합니다. TRUE이므로 SSL 프록시가 활성화되지 않은 경우 HTTPS 페이로드가 암호 해독 없이 통과합니다. 즉, 이미 암호화된 트래픽에서 DRE가 약하게 감소할 것으로 예상됩니다. 측정된 48% 감소(4단계 분류)는 일반 텍스트 흐름에 대한 실제 DRE 혜택입니다.

확인:

1. DRE 정책은 양쪽 끝에서 양방향과 일치합니다.
2. 흐름은 대칭이며 예상 피어를 사용합니다.
3. DRE 상태 및 캐시 상태는 관련 경보 없이 활성 상태입니다.
4. 피어 버전 및 AO 기능은 호환됩니다.
5. 디스크 레이턴시 및 리소스 사용률이 지원되는 범위 내에 있습니다.
6. 흐름이 자동 바이패스에 있지 않습니다.
7. 암호화된 트래픽에는 필수 SSL/TLS 암호 해독 및 듀얼 엔드 최적화 컨피그레이션이 있습니다.

올바르게 측정

하나의 대표 데이터 세트와 양쪽 끝에서 동일한 시간 간격을 사용합니다. 테스트 전후에 원본 및 최적화된 바이트 카운터를 캡처합니다. 수명 감소 비율보다 간격 델타를 선호합니다. 캐시 이점을 테스트하는 경우 실행이 콜드 캐시인지 아니면 웜 캐시인지를 문서화하고 동일한 내용을 반복합니다.

증거 수집 및 에스컬레이션

지원되는 작동 명령을 먼저 사용하십시오. 원인이 불분명한 경우 다음을 수집합니다.

- UTC 재생 창 및 영향을 받는 튜플/VPN
- 동일한 사이트 쌍에서 1개의 실패와 1개의 정상 작동이 확인된 플로우
- AppQoE 상태, 최근 오류, 정책, 서비스 노드 그룹, 양단의 흐름 출력
- DRE 상태, 피어 통계, 리소스 상태 및 간격 바이트 델타
- 해당 명령이 있는 경우 CFT 상태 및 QFP AppQoE 통계
- 카운터를 지우거나 서비스를 다시 시작하기 전에 Admin-tech가 캡처됨

show sdwan appqoe flow all debug는 광범위한 플랫폼 디버깅을 활성화하는 라이센스가 아니라 show output으로 확장됩니다. 비용이 많이 들 수 있으며 유동이 노출될 수 있습니다. 대상이 지정된 flow 명령이 부족한 경우 범위가 지정된 짧은 수집에만 이 명령을 사용합니다.

검증된 릴리스/플랫폼, 캡처 기간, 출력 대상 및 테스트된 중지 프로시저 없이 일반 platform-debug 명령을 게시하지 마십시오. 사용 중인 프로덕션 디바이스에서 활성 디버그 또는 패킷 추적 수집에 Cisco TAC 지침을 사용합니다.

관련 Cisco 문서

- AppQoE 확인 및 문제 해결
- TCP 최적화
- DRE를 사용한 트래픽 최적화
- AppQoE 서비스를 위한 외부 서비스 노드
- Catalyst SD-WAN AppQoE DRE: 토폴로지, 컨피그레이션, 확인
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.