Risoluzione dei problemi di ottimizzazione TCP e DRE AppQoE in Cisco Catalyst SD-WAN

Sommario

- Introduzione
- Premesse
- Scopo, ambito e sicurezza
- Inizia da qui: Triage di 10 minuti
  - 1. Verificare lo stato di AppQoE e gli errori recenti
  - 2. Verificare l'assegnazione dei criteri e dei nodi di servizio in entrambe le direzioni
  - 3. Ispezionare un flusso noto e tracciarlo da punto a punto
    - Traccia di un singolo flusso
  - 4. Verificare le risorse del nodo di servizio e il DRE
  - 5. Acquisire il traffico tra Service Controller (SC) e Service Node (SN)
    - Metodo 1: CLI (Embedded Packet Capture - EPC)
    - Metodo 2: GUI (Cisco SD-WAN Manager)
  - 6. Scegliere la sezione successiva
- Come l'ottimizzazione TCP e il DRE elaborano un flusso
- Nessuna ottimizzazione o deviazione
  - Conferma
  - Interpreta
  - Correggi e verifica
- Errore di deviazione e bypass
- Cadute dopo la deviazione
  - Conferma
  - Interpreta
  - Correggi e verifica
- Integrità e assegnazione del nodo del servizio
- CFT e capacità
- Policer SYN e velocità di connessione
- MTU e MSS
  - Conferma
- DRE è attivo ma la riduzione è debole
  - Conferma stato DRE e peer
  - Misura correttamente
- Raccolta delle prove e segnalazione dei problemi
- Documentazione correlata di Cisco

Introduzione

In questo documento viene descritto come risolvere i problemi di ottimizzazione TCP e DRE AppQoE in Cisco Catalyst SD-WAN.

Premesse

Utilizzare questa guida quando un flusso TCP abilitato per AppQoE non è ottimizzato, viene ignorato, reimpostato dopo la diversione, segnala un nodo di servizio non integro o mostra una riduzione DRE (Data Redundancy Elimination Elimination) inferiore al previsto.

Iniziate con il triage di 10 minuti. Separa i problemi di criteri e percorsi dai problemi di integrità dei nodi di servizio, di stato del flusso, di capacità, di trasporto TCP e di efficacia DRE. Passare a una sezione dei sintomi solo dopo aver individuato il punto in cui il flusso cessa di comportarsi come previsto.

Scopo, ambito e sicurezza

In questa guida vengono illustrati i dispositivi Cisco IOS® XE Catalyst SD-WAN che utilizzano l'ottimizzazione TCP o DRE con nodi di servizio AppQoE integrati o esterni.

Elemento di convalida	Stato
CLI operativa e di comportamento pubblico	In linea con la documentazione corrente di Cisco Catalyst SD-WAN AppQoE 26.x
Semantica contatori interni	Ricontrollato con l'origine Cisco IOS XE corrente il 15/07/2026
Versioni, piattaforme e topologie esatte utilizzate per la pubblicazione	Acquisizione in laboratorio: Cisco IOS XE Catalyst SD-WAN 17.18.2 su C800v, nodo di servizio esterno AppQoE. Controller AppNav c8000v-appqoe-3, nodo di servizio c8000v-appqoe-4, nodo di servizio applicazione SN esterno (SN IP 15.15.15.2). SNG SNG-APPQOE, data policy _vpn-10_appqoe-policy (TCP + DRE) su VPN 10. Acquisito il 15 luglio 2026.

La disponibilità e l'output dei comandi variano a seconda della versione del software, della piattaforma e del ruolo. Confermare la sintassi con la guida dei comandi sul dispositivo di destinazione. I comandi QFP di basso livello in questa guida sono di sola lettura, ma sono specifici della piattaforma e della versione; utilizzarli solo quando il comando è presente.

Di seguito sono riportati i checkpoint delle versioni principali; non sostituiscono il supporto specifico della piattaforma e la documentazione della scalabilità.

Funzionalità	Checkpoint rilascio minimo
Gestione DRE e MTU controller/nodo di servizio automatizzata	Cisco IOS XE Catalyst SD-WAN 17.5.1a
Risoluzione dei problemi e integrità dei sottoservizi AppQoE migliorata	17.6.1a
Risoluzione estesa dei problemi relativi al flusso di lavoro	17.9.1 bis
Proxy SSL con TLS 1.3	17.13.1a/Manager 20.13.1
DRE tramite i gruppi di configurazione	17.14.1a/Manager 20.14.1

Il DRE richiede nodi di servizio supportati a entrambe le estremità e la gestione del flusso simmetrico. Non viene eseguito su un dispositivo con ruolo di solo controller del servizio e non è possibile combinare AppQoE con Duplicazione pacchetti nella stessa connessione. Il traffico crittografato richiede la gestione SSL/TLS supportata se si desidera ottimizzare il payload.

Prima di modificare i criteri, cancellare le statistiche, riavviare un servizio o abilitare il debug, acquisire:

- Rilascio software, piattaforma e ruolo AppQoE a entrambe le estremità
- Indirizzi IP di origine e destinazione, porte, protocollo, VPN e ora UTC di test
- Prevista sequenza di criteri e assegnazione del nodo del servizio
- Se il sintomo influenza un flusso, una coppia di siti o tutto il traffico AppQoE
- Due istantanee dei contatori nello stesso intervallo di test

---

Nota: Non cancellare la cache DRE durante la risoluzione iniziale dei problemi. Cancellandolo, il DRE viene riavviato e la cache a caldo viene distrutta, modificando così la condizione da misurare.

Inizia da qui: Triage di 10 minuti

1. Verificare lo stato di AppQoE e gli errori recenti

Esegui sui dispositivi periferici o sui controller di servizio partecipanti:

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

Esempio di laboratorio:

c800v-appqoe-4 (nodo di servizio, C800v, 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)
```

Lo stato complessivo è GIALLO solo perché l'oggetto attivazione SSL non è in uso (il proxy SSL è in modalità non crittografata); I servizi secondari TCP, service-chain e resource-manager sono di tipo GREEN. Nessuna perdita di PP o errori di nuova connessione.

Cercare i servizi abilitati, lo stato corrente del nodo del servizio, gli errori di flusso recenti e qualsiasi motivo che spieghi direttamente il comportamento di bypass o eliminazione.

2. Verificare l'assegnazione dei criteri e dei nodi di servizio in entrambe le direzioni

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

Esempio di laboratorio:

c8000v-appqoe-3 (controller 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
```

L'azione accetta porta sia l'ottimizzazione tcp che l'ottimizzazione dre a SNG-APPQOE e il numero di serie è attivo con tcp/dre GREEN. ssl/http/utd mostra RED/NOT AVAILABLE perché questi oggetti attivazione non sono configurati. Previsto per un test solo TCP+DRE.

Confermare che la sequenza desiderata corrisponda a entrambe le direzioni del flusso di test, includa le azioni TCP/DRE previste e punti al gruppo di nodi di servizio desiderato. Il DRE richiede sia le estremità che la gestione del flusso simmetrico.

3. Ispezionare un flusso noto e tracciarlo da punto a punto

```
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
```

Traccia di un singolo flusso

Eseguire innanzitutto il comando show sdwan appqoe flow vpn-id <vpn-id> server-ip <server-ip> server-port <port> sui router perimetrali e su quello DC. Questo comando restituisce l'ID di flusso. Dopo aver ottenuto l'ID di flusso, eseguire show sdwan appqoe flow-id <flow-id> su entrambi i router.

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

Esempio di laboratorio:

c8000v-appqoe-4 (service node), 2026-07-15. Nessun flusso attivo al momento dell'acquisizione, pertanto viene visualizzata la tabella cronologica (chiusa).

```
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 indica che questi flussi sono stati ottimizzati per TCP; RR% è vuoto in quanto il rapporto di riduzione DRE è riportato per flusso ottimizzato per DRE (vedere le sezioni DRE). Usare flow-id <id> su un flusso in diretta per leggere direttamente lo stato registrato come ottimizzato/ignorato. Il flusso tracciato sopra riportato mostra Service = TD (TCP + DRE) e una sequenza di eventi proxy completa — scambio di opzioni SYN, accettazione/connessione, creazione del flusso DRE riuscita e dati abilitati — a conferma dell'ottimizzazione completa end-to-end.

Classificare il flusso come ottimizzato, ignorato/passthrough o non riuscito. Preferire lo stato registrato del motivo di flusso o di passthrough a un'inferenza da un contatore aggregato.

4. Verificare le risorse del nodo di servizio e il DRE

Eseguire i comandi applicabili al ruolo del dispositivo:

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

Esempio di laboratorio:

c8000v-appqoe-4 (service node), 2026-07-15. Output DRE lungo tagliato in base ai campi di stato/capacità.

```
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
```

Integrità VERDE, nessun allarme, latenza del disco 2 ms e un rapporto di riduzione complessiva del 48%. La tabella dei peer conferma che i peer DRE sono raggiungibili e compatibili con le versioni (vedere aoim-statistics).

Verificare lo stato, le connessioni massime e attive, la compatibilità peer, lo stato della cache, la latenza o gli allarmi del disco e i differenziali tra byte originali e ottimizzati.

5. Acquisire il traffico tra Service Controller (SC) e Service Node (SN)

Acquisire un monitor sull'interfaccia del tunnel tra il CS e il SN. Fornisce dati chiari e non incapsulati.

Metodo 1: CLI (Embedded Packet Capture - EPC)

È possibile usare la funzione Cisco IOS XE Embedded Packet Capture (EPC) direttamente sulla CLI del dispositivo. Di seguito viene riportata la configurazione dettagliata utilizzando Tunnel2000000001 come esempio:

```
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
```

Metodo 2: GUI (Cisco SD-WAN Manager)

In alternativa, è possibile eseguire questa acquisizione direttamente dalla GUI di Cisco SD-WAN Manager (in precedenza vManage), che emette automaticamente un file .pcap da scaricare:

1. Passare a **Monitor > Dispositivi**.
2. Scegliere il dispositivo (**c8000v-appqoe-4**).
3. Fare clic su **Risoluzione dei problemi** nel riquadro di sinistra.
4. Nella sezione **Traffico**, scegliere **Packet Capture** (Acquisizione pacchetti).
5. Nell'elenco a discesa per la selezione dell'interfaccia, scegliere l'interfaccia del tunnel AppQoE (ad esempio, **Tunnel200000001**).

6. (Facoltativo) Applicare i filtri IP o delle porte di origine/destinazione.
7. Fare clic su **Start** per iniziare l'acquisizione e su **Stop** al termine. Il sistema preparerà un file **.pcap** per il download.

6. Scegliere la sezione successiva

Primo risultato anomalo	Vai a
Il criterio non corrisponde in entrambe le direzioni	Nessuna ottimizzazione o deviazione
Nessun nodo del servizio integro o idoneo assegnato	Integrità e assegnazione dei nodi di servizio
Flusso ignorato o con un motivo di superamento	Errore di deviazione e bypass
Reset di flusso esistenti o pacchetti ignorati	Cadute dopo la diversione
Durante una frammentazione si verificano errori solo nelle nuove connessioni	Policer SYN e velocità di connessione
Aumento degli errori CFT/FID	CFT e capacità
Sono presenti blocchi TCP e prove PMTU/MSS	MTU e MSS
Il flusso è ottimizzato, ma la riduzione è debole	Efficacia DRE

Come l'ottimizzazione TCP e il DRE elaborano un flusso

Con l'ottimizzazione TCP dual-ended e DRE, la connessione originale è rappresentata da tre connessioni TCP:

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

DRE comprime i dati ripetuti sulla gamba di sovrapposizione. Il dispositivo più lontano ricostruisce il flusso originale prima di inoltrarlo alla destinazione. Una topologia di nodo di servizio esterno

aggiunge il reindirizzamento da controller di servizio a nodo di servizio, ma rimangono gli stessi checkpoint: criteri, simmetria dei percorsi, idoneità dei nodi di servizio, deviazione del flusso, compatibilità peer e stato DRE.

Termine	Significato della presente Guida
A livelli ottimali	Il servizio AppQoE selezionato è attivo per il flusso.
Bypass o passthrough	Il traffico continua senza il servizio AppQoE scelto; esaminare il motivo della trasmissione.
Drop	Il pacchetto non continua; questo ha un impatto per l'utente e richiede una correlazione drop/error.
Stato del flusso di chiusura con errore	Dopo che un flusso è stato ispezionato/deviato, alcuni errori di deviazione successivi non possono tornare in modo sicuro al bypass ordinario.
SC	Controller servizi
SN/ISDN/ESN	Service Node/Integrated Service Node/External Service Node
CFT	Tabella Flusso di connessione utilizzata per tenere traccia dei flussi e del relativo stato delle caratteristiche

Nessuna ottimizzazione o deviazione

Conferma

1. Confermare la corrispondenza dei criteri e le azioni in entrambe le direzioni.
2. Confermare il routing simmetrico tramite la coppia di dispositivi AppQoE prevista.
3. Confermare che il gruppo del nodo di servizio e gli ID del sito siano corretti.
4. Verificare che il DRE sia stato distribuito e integro su entrambe le estremità.
5. Esaminare lo stato del flusso di destinazione o il motivo della trasmissione.

Interpreta

- In genere, nessuna corrispondenza tra i criteri indica che la classificazione, la direzione, la VPN o l'allegato sono errati.

- Una corrispondenza unilaterale può abilitare la gestione TCP/DRE su un lato ma non può fornire un percorso DRE a due estremità valido.
- Un flusso può essere ignorato correttamente quando il traffico è già ottimizzato, è un tipo di flusso non supportato, è asimmetrico o corrisponde a una condizione di ignoramento automatico.

Correggi e verifica

Correggere i problemi relativi a criteri, direzione, gruppi di nodi, ID sito o routing. Creare quindi una nuova connessione TCP e verificare il flusso su entrambe le estremità. Non utilizzare una connessione esistente per convalidare una modifica dei criteri.

Errore di deviazione e bypass

Utilizzare le statistiche QFP interne solo dopo che il flusso AppQoE supportato e i comandi di errore hanno ridotto il 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
```

Confrontare due istantanee. questi contatori sono cumulativi.

Esempio di laboratorio:

c8000v-appqoe-3 (controller AppNav), 2026-07-15. Diversione integra: l'indice SN è verde e nessun contatore di drop-cause è in aumento oltre il numero previsto di transitori non integri SN registrati in precedenza.

```
c8000v-appqoe-3#show platform hardware qfp active feature appqoe stats all
 APPQOE Feature Statistics:
 Global:
     ip-non-tcp-pkts: 1354682
     cft_handle_pkt: 0
     sdvt_divert_req_fail: 1374
     appqoe_svc_on_appqoe_vpn_drop: 0
     appqoe_sng_not_configured: 0
   SDVT Global stats:
     within SDVT syn policer limit: 71660
 SNG: 0 SN Index [0 (Green)], IP: 15.15.15.2, oce_id: 221252816
     APPNAV STATS: toSN 85540403 / 75619122643 fromSN 105667460 / 109985814214
                   NoFoDrop 0 / 0
   SDVT Count stats:
```

```
     Active Connections: 4
     decaps: 58388600   encaps: 47119306
   SDVT Packet stats:
     Divert packets / bytes   47119306 / 34139250226
     Reinject packets / bytes 58388600 / 52530512355
     Pkts dropped packets / bytes 10 / 690
   SDVT Drop Cause stats:
     Packets Dropped as SN Unhealthy: 10

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

cft_handle_pkt: 0 e appqoe_svc_on_appqoe_vpn_drop: 0 Escludere un errore CFT/FID e una perdita di VPN ricorsiva. Pacchetti scartati come SN non integri: 10 è un piccolo conteggio storico — correlato con le transizioni dello stato di salute SN prima di trattarlo come impatto attivo.

Cadute dopo la deviazione

Conferma

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

Se presenti sulla release e sulla piattaforma, confrontate le statistiche globali o le statistiche prima e dopo una riproduzione controllata.

Esempio di laboratorio:

Linea di base integra, c8000v-appqoe-3 (controller), 2026-07-15. Non si stanno accumulando perdite di fail-close; il numero di serie è Attivo/Verde e un errore recente indica che vPath è stato interrotto a causa di Ps: 0 e vPath new connection non riusciti: 0. L'istantanea della causa di rilascio del datapath è la prova 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
```

Correlare il tempo di riproduzione esatto rispetto a questi delta prima di etichettare un reset come fail-close.

Interpreta

Un flusso precedentemente ispezionato/deviato può essere interrotto quando il nodo del servizio diventa inutilizzabile o un reindirizzamento AppNav successivo non riesce. Questo protegge lo stato proxy stabilito; la connessione client-server originale non può sempre essere ricostruita in modo trasparente dopo la scomparsa di un percorso proxy. I flussi della catena di servizi possono inoltre diminuire quando un bypass ordinario viola l'elaborazione della catena.

Non etichettare ogni ripristino come chiusura con errore. Correlare l'ora esatta del test con l'errore di flusso, la transizione dello stato del nodo di servizio e il delta del contatore.

Correggi e verifica

Ripristinare un nodo di servizio stabile e idoneo e correggere il percorso o l'errore della catena di servizio. Eseguire la convalida con una nuova connessione TCP, quindi verificare che il contatore di rilascio pertinente smetta di aumentare.

Integrità e assegnazione del nodo del servizio

L'integrità è specifica del ruolo e del servizio. La vita, la capacità delle risorse e lo stato di un particolare Application Optimizer (AO) sono correlati ma non intercambiabili.

State	Comportamento del percorso dati previsto
Verde	Idoneo per flussi nuovi ed esistenti
Giallo	Il traffico non SYN ispezionato esistente può continuare; i nuovi SYN non vengono deviati a tale nodo. Un nodo FULL è una possibile condizione gialla
Rosso o	i flussi nuovi/non impegnati normalmente non vengono eseguiti quando consentito; i

State	Comportamento del percorso dati previsto
Giù	flussi già ispezionati/di chiusura con esito negativo possono scendere; i flussi della catena di servizi possono diminuire

Lanciare:

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

Verificare l'appartenenza al nodo, l'ID del sito, l'integrità degli oggetti attivazione, il carico/la capacità, gli allarmi DRE e la raggiungibilità dei peer. Prima della release 17.6.1a di Cisco IOS XE Catalyst SD-WAN, i dettagli sullo stato del servizio secondario possono essere limitati; interpretare l'output precedente di conseguenza.

Esempio di laboratorio:

Nodo sano, 2026-07-15. Sul controller il numero di serie è Vivo con indicatori di integrità per-AO; sul nodo il gestore delle risorse segnala Verde con spazio di crescita:

```
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
```

Il carico è pari a 0% e le sessioni utilizzate sono ben al di sotto dei limiti 40000/750, quindi questo nodo non è né pieno né giallo per motivi di capacità. Lo stato complessivo giallo visualizzato in show sdwan appqoe status fa riferimento solo all'oggetto attivazione del protocollo SSL non utilizzato.

Quando un nodo è pieno o giallo perché si trova vicino alla capacità della sessione configurata, distribuire nuove connessioni, aumentare il profilo di risorse AppQoE supportato dove la

piattaforma lo consente oppure aggiungere capacità. L'aggiunta della memoria DRAM del router non modifica la scala di flusso hardware supportata.

CFT e capacità

appqoe_cft_handle_pkt è un contatore di errori. Aumenta quando AppQoE non riesce a ottenere un ID di flusso valido dalla gestione CFT. un valore crescente è la prova di un'anomalia nella gestione di CFT/FID; un valore basso rispetto al traffico totale non è la prova della saturazione.

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

Interpreta lo stato CFT separatamente dalla capacità del nodo di servizio:

Esempio di laboratorio:

c8000v-appqoe-3 (controller), 2026-07-15. Tabella con elementi di memoria lunghi tagliata.

```
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)
```

Numero totale di flussi attualmente allocati: 8 contro un valore massimo di 1.000.000 significa nessuna pressione sulla tavola e cft_handle_pkt: 0 nello stato AppQoE conferma che non si è verificato alcun errore di acquisizione FID. L'aumento di cft_handle_pkt, non solo l'occupazione delle tabelle, indica un problema di CFT/FID.

- Lo stato CFT identifica la pressione/gli errori della tabella di flusso del bordo o dell'ID del flusso.
- rm-resources identifica la capacità della sessione del nodo del servizio AppQoE.
- Le tabelle complete o la pressione della memoria sono possibili cause di un errore di acquisizione del FID, ma non le uniche cause.

Se l'errore aumenta durante l'intervallo di test, acquisire l'errore/stato CFT, la scala della piattaforma, le connessioni attive e le risorse del nodo. Ridurre la pressione di connessione, ribilanciare i nodi di servizio, modificare il profilo di risorsa supportato o passare a una piattaforma con la scalabilità richiesta. Coinvolgere Cisco TAC prima di considerare un errore CFT generico come una conclusione relativa alla capacità hardware.

Policer SYN e velocità di connessione

Utilizzare lo stato completo e i contatori documentati. "SDVT_DROP_ERROR" è una classe di errore; di per sé non è la prova che il poliziotto SYN abbia sparato.

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

Correlazione tra gli errori di nuova connessione e il numero massimo di PPP Syn Drop, il calo di vPath dovuto alle PPP e lo stesso intervallo di test. Flussi di lunga durata che rimangono sani mentre solo i nuovi SYN falliscono rafforza l'ipotesi del policer.

Esempio di laboratorio:

c8000v-appqoe-4 (service node), 2026-07-15. libuinet-statistics è long; viene visualizzato il blocco di statistiche Vpath relativo al policer.

```
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
```

Numero massimo di PPP Syn Drop raggiunto: 0 (e vPath viene eliminato a causa di PP: 0 (errore recente) regola il policer SYN qui. La velocità configurata sul controller è syn_policer_rate: 2700 (dall'interno all); confrontalo con il tuo tasso di SYN offerto prima di agire.

Ridurre la velocità di burst, se possibile, distribuire nuove connessioni su una capacità sana e confermare che i contatori di policer documentati non aumentano più. non sintonizzarsi o eludere i limiti di protezione da una guida generica; utilizzare le linee guida della piattaforma e il TAC

quando i tassi sostenuti si avvicinano ai limiti supportati.

MTU e MSS

La regolazione MSS non è di per sé un percorso SYN-drop diretto di AppQoE. Il datapath calcola un valore MSS dall'MTU di adiacenza del nodo di servizio e dal sovraccarico dell'incapsulamento. Quando è possibile, regola il valore MSS del client e lo memorizza sul lato server; quando le informazioni MTU non sono disponibili, possono continuare senza quella regolazione.

Pertanto, non utilizzare sdvt_drop_appnav_divert da solo come prova di un errore di calcolo MSS.

Conferma

- Registrare la release del software; la gestione automatica dell'MTU da SC a SN è stata introdotta nella versione 17.5.1a.
- Verificare un'MTU uniforme supportata sul percorso del controller del servizio/nodo del servizio e sul supporto SD-WAN.
- Usare il test DF-bit path-MTU e le acquisizioni SYN/SYN-ACK sincronizzate sui bordi rilevanti.
- Confronta i valori MSS offerti e regolati e verifica la frammentazione o il black-holing.

Comando di piattaforma utile, se supportato:

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

Esempio di laboratorio:

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
```

Le sessioni di sovrimpressione IPsec segnalano una PMTU 1442 uniforme. Una PMTU coerente sui tunnel SC/SN (e nessuna black-holing nei test DF-bit) indica che il valore MSS deriva da una

MTU stabile nelle adiacenze. Escludere questa condizione prima di toccare l'MTU del tunnel.

Correggere il criterio MTU o MSS del percorso solo dopo aver confermato l'hop che ha generato l'errore. Non aumentare l'MTU di un tunnel a meno che il percorso completo dell'underlay non possa trasportarlo.

DRE è attivo ma la riduzione è debole

Una riduzione bassa non significa automaticamente che il DRE sia interrotto. Dati di primo passaggio univoci, una cache a freddo, payload già compressi, traffico crittografato senza la gestione SSL/TLS richiesta, flussi asimmetrici, incompatibilità peer o bypass automatico possono tutti produrre una riduzione minima o nulla.

Conferma stato DRE e peer

```
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
```

Esempio di laboratorio:

c8000v-appqoe-4 (service node), 2026-07-15. Lo stato/le statistiche/il peer DRE vengono visualizzati nella fase di valutazione 4. esempio precedente; i comandi rimanenti:

```
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
```

Nessun elemento è in modalità di bypass automatico, la negoziazione AD è in corso di completamento e le statistiche aoim mostrano 0 passthrough dalla mancata corrispondenza delle versioni con entrambi i peer DRE contrassegnati come incompatibili = N. Lo stato sslproxy indica la modalità di cancellazione: TRUE, quindi i payload HTTPS attraversano il traffico senza decrittografia (prevista riduzione DRE debole sul traffico già crittografato) a meno che non sia abilitato il proxy SSL. La riduzione misurata del 48% (passaggio di selezione 4.) è un reale vantaggio DRE sui flussi in chiaro.

Verifica:

1. Il criterio DRE corrisponde a entrambe le direzioni su entrambe le estremità.
2. Il flusso è simmetrico e utilizza i peer previsti.
3. Lo stato di integrità del DRE e lo stato della cache sono attivi senza alcun allarme rilevante.
4. Versioni peer e funzionalità AO compatibili.
5. La latenza del disco e l'utilizzo delle risorse rientrano nell'intervallo supportato.
6. Il flusso non è nel bypass automatico.
7. Il traffico crittografato dispone della decrittografia SSL/TLS richiesta e della configurazione dell'ottimizzazione dual-ended.

Misura correttamente

Utilizzare un set di dati rappresentativo e lo stesso intervallo di tempo a entrambe le estremità. Acquisire i contatori di byte originali e ottimizzati prima e dopo il test. Preferire i differenziali di intervallo a un rapporto di riduzione della durata. Se si verifica il vantaggio della cache, documentare se l'esecuzione è a cache fredda o a caldo e ripetere lo stesso contenuto.

Raccolta delle prove e segnalazione dei problemi

Utilizzare prima i comandi operativi supportati. Se la causa non è chiara, raccogli:

- Finestra di riproduzione UTC e tupla/VPN interessata
- Un errore e un flusso riconosciuto valido dalla stessa coppia di siti
- Stato AppQoE, errori recenti, criteri, gruppo del nodo di servizio e output di flusso da entrambe le estremità
- Stato DRE, statistiche peer, stato delle risorse e delta di byte di intervallo

- Statistiche di stato CFT e QFP AppQoE quando questi comandi esistono
- Tecnologia di amministrazione acquisita prima di cancellare i contatori o riavviare i servizi

show sdwan appqoe flow all debug è espanso show output, non una licenza per abilitare il debug su un'ampia piattaforma. Può essere costoso e può esporre tuple di flusso; utilizzarlo solo per una raccolta con ambito breve quando i comandi di flusso di destinazione sono insufficienti.

Non pubblicare un comando platform-debug generico senza una release/piattaforma convalidata, una durata di acquisizione, una destinazione di output e una procedura di arresto verificata. Utilizzare le linee guida di Cisco TAC per il debug attivo o la raccolta di tracce di pacchetti su un dispositivo di produzione occupato.

Documentazione correlata di Cisco

- Verifica e risoluzione dei problemi di AppQoE
- Ottimizzazione TCP
- Ottimizzazione del traffico con DRE
- Nodi di servizi esterni per servizi AppQoE
- Catalyst SD-WAN AppQoE DRE: Topologia, configurazione, verifica
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).