Dépannage de l'optimisation TCP AppQoE et DRE dans Cisco Catalyst SD-WAN

Table des matières

- Introduction
- Informations générales
- Objectif, portée et sécurité
- Commencez ici : Triage de 10 minutes
  - 1. Vérifier l'état AppQoE et les erreurs récentes
  - 2. Vérification de l'affectation de la stratégie et du noeud de service dans les deux directions
  - 3. Inspectez un flux connu et effectuez son suivi de bout en bout
    - Traçage d'un flux unique
  - 4. Vérification des ressources du noeud de service et du DRE
  - 5. Capturer le trafic entre le contrôleur de service (SC) et le noeud de service (SN)
    - Méthode 1 : CLI (Embedded Packet Capture - EPC)
    - Méthode 2 : Interface utilisateur graphique (Cisco SD-WAN Manager)
  - 6. Choisissez la section suivante
- Comment l'optimisation TCP et le processus DRE traitent un flux
- Pas d'optimisation ni de déviation
  - Confirmer
  - Interpréter
  - Correction et vérification
- Échec et contournement de la dérivation
- Abandons après déviation
  - Confirmer
  - Interpréter
  - Correction et vérification
- État et affectation du noeud de service
- CFT et capacité
- Contrôleur SYN et débit de connexion
- MTU et MSS
  - Confirmer
- DRE est actif mais la réduction est faible
  - Confirmer l'état DRE et les homologues
  - Mesurer correctement
- Collecte et signalement des preuves
- Documentation Cisco associée

Introduction

Ce document décrit comment dépanner AppQoE TCP Optimization et DRE dans Cisco Catalyst SD-WAN.

Informations générales

Utilisez ce guide lorsqu'un flux TCP compatible AppQoE n'est pas optimisé, est contourné, se réinitialise après déroutement, signale un noeud de service défectueux ou affiche moins de réduction DRE (Data Redundancy Elimination) que prévu.

Commencez par le triage de 10 minutes. Il sépare les problèmes de stratégie et de chemin des problèmes d'état de service-noeud, d'état de flux, de capacité, de transport TCP et d'efficacité DRE. Passez à la section des symptômes uniquement après avoir déterminé où le flux cesse de se comporter comme prévu.

Objectif, portée et sécurité

Ce guide couvre les périphériques Cisco IOS® XE Catalyst SD-WAN utilisant l'optimisation TCP ou DRE avec des noeuds de service AppQoE intégrés ou externes.

Élément de validation	Status (état)
Comportement public et CLI opérationnelle	Aligné sur la documentation actuelle de Cisco Catalyst SD-WAN AppQoE 26.x
Contre-sémantique interne	Revérification par rapport à la source Cisco IOS XE actuelle le 2026-07-15
Version, plate-forme et topologie exactes utilisées pour la publication	Capture de TP : Cisco IOS XE Catalyst SD-WAN 17.18.2 sur C8000v, noeud de service externe AppQoE. Contrôleur AppNav c8000v-appqoe-3, noeud de service c8000v-appqoe-4, noeud de service externe SN appqoe-service-node (SN IP 15.15.15.2). SNG SNG-APPQOE, politique de données _vpn-10_appqoe-policy (TCP + DRE) sur VPN 10. Capturé le 15/07/2026.

La disponibilité et le résultat des commandes varient selon la version du logiciel, la plate-forme et le rôle. Confirmez la syntaxe avec l’aide des commandes sur l’équipement cible. Les commandes QFP de bas niveau de ce guide sont en lecture seule, mais elles sont spécifiques à la plate-forme et à la version ; utilisez-les uniquement lorsque la commande est présente.

Les points de contrôle de libération clés sont indiqués ci-dessous ; ils ne remplacent pas la

documentation de support et d'évolutivité propre à la plate-forme.

Capacité	Point de contrôle de libération minimale
Gestion de MTU DRE et de contrôleur de service/noeud de service automatisé	Cisco IOS XE Catalyst SD-WAN 17.5.1a
Dépannage AppQoE amélioré et intégrité des sous-services	17.6.1a
Dépannage détaillé des flux	17.9.1a
Proxy SSL avec TLS 1.3	17.13.1a/Manager 20.13.1
DRE via des groupes de configuration	17.14.1a/Manager 20.14.1

DRE nécessite des noeuds de service pris en charge aux deux extrémités et une gestion de flux symétrique. Il ne s'exécute pas sur un périphérique dans le rôle de contrôleur de service uniquement, et AppQoE ne peut pas être combiné avec la duplication de paquets sur la même connexion. Le trafic chiffré nécessite la gestion SSL/TLS prise en charge si sa charge utile doit être optimisée.

Avant de modifier la stratégie, d'effacer les statistiques, de redémarrer un service ou d'activer le débogage, procédez comme suit :

- Version logicielle, plate-forme et rôle AppQoE aux deux extrémités
- Adresses IP source et de destination, ports, protocole, VPN et temps de test UTC
- Séquence de stratégie et affectation de noeud de service attendues
- Indique si le symptôme affecte un flux, une paire de sites ou tout le trafic AppQoE
- Deux instantanés de compteur sur le même intervalle de test

---

Remarque : Ne videz pas le cache DRE lors du dépannage initial. L'effacement redémarre DRE et détruit le cache chaud, ce qui modifie l'état mesuré.

Commencez ici : Triage de 10 minutes

1. Vérifier l'état AppQoE et les erreurs récentes

Exécutez sur les périphériques de périphérie ou les contrôleurs de service participants :

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

Exemple de TP :

c8000v-appqoe-4 (noeud de service, 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)
```

Ici, l'état global est JAUNE uniquement parce que l'AO SSL n'est pas utilisé (le proxy SSL est en mode clair) ; Les sous-services TCP, de chaîne de services et de gestionnaire de ressources sont VERTS. Aucune interruption de PP ou échec de nouvelle connexion.

Recherchez les services activés, l'état actuel du noeud de service, les erreurs de flux récentes et toute raison expliquant directement le comportement de contournement ou d'abandon.

2. Vérification de l'affectation de la stratégie et du noeud de service dans les deux directions

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

Exemple de TP :

c8000v-appqoe-3 (contrôleur 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'action accept porte à la fois l'optimisation tcp et l'optimisation dre pointant sur SNG-APPQOE, et le SN est actif avec tcp/dre GREEN. ssl/http/utd show RED/NOT AVAILABLE parce que ces AO ne sont pas configurés — ce qui est attendu pour un test TCP+DRE uniquement.

Vérifiez que la séquence prévue correspond aux deux directions du flux de test, inclut les actions TCP/DRE attendues et pointe vers le groupe de noeuds de service prévu. DRE nécessite une gestion des deux extrémités et un flux symétrique.

3. Inspectez un flux connu et effectuez son suivi de bout en bout

```
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
```

Traçage d'un flux unique

Commencez par exécuter la commande show sdwan appqoe flow vpn-id <vpn-id> server-ip <server-ip> server-port <port> sur les routeurs de périphérie et de data center. Cette commande renvoie l'ID de flux. Une fois que vous avez l'ID de flux, exécutez show sdwan appqoe flow flow-id <flow-id> sur les deux routeurs.

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

Exemple de TP :

c8000v-appqoe-4 (noeud de service), 2026-07-15. Aucun flux n'étant actif au moment de la capture, la table historique (fermée) s'affiche.

```
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 signifie que ces flux ont été optimisés pour TCP ; RR% est vide car le taux de réduction du DRE est rapporté par flux optimisé du DRE (voir les sections DRE). Utilisez flow-id <id> sur un flux actif afin de lire directement son état optimisé/de contournement enregistré. Le flux suivi ci-dessus indique Service = TD (TCP + DRE) et une séquence d'événements proxy complète — les options SYN échangent, acceptent/se connectent, le flux DRE crée un succès et les données sont activées — confirmant l'optimisation complète de bout en bout.

Classez le flux comme étant optimisé, contourné/traversé ou en échec. Préférez l'état enregistré de la raison de flux ou de transit à une inférence d'un compteur d'agrégation.

4. Vérification des ressources du noeud de service et du DRE

Exécutez les commandes qui s'appliquent au rôle de périphérique :

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

Exemple de TP :

c8000v-appqoe-4 (noeud de service), 2026-07-15. Sortie DRE longue réduite aux champs d’intégrité/de capacité.

```
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
```

VERT santé, aucune alarme, latence de disque de 2 ms et taux de réduction global de 48 % sain. La table des homologues confirme que les deux homologues DRE sont accessibles et compatibles avec la version (voir aoim-statistics).

Vérifiez l'intégrité, le nombre maximal de connexions actives, la compatibilité des homologues, l'état du cache, la latence ou les alarmes du disque, ainsi que les deltas d'octets d'origine par rapport aux octets optimisés.

5. Capturer le trafic entre le contrôleur de service (SC) et le noeud de service (SN)

Effectuez une capture de surveillance sur l'interface du tunnel entre le SC et le SN. Il fournit des données claires et non encapsulées.

Méthode 1 : CLI (Embedded Packet Capture - EPC)

Vous pouvez utiliser la fonctionnalité Cisco IOS XE Embedded Packet Capture (EPC) directement sur l'interface de ligne de commande du périphérique. Voici la configuration étape par étape en utilisant Tunnel2000000001 comme exemple :

```
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
```

Méthode 2 : Interface utilisateur graphique (Cisco SD-WAN Manager)

Vous pouvez également effectuer cette capture directement à partir de l'interface utilisateur graphique de Cisco SD-WAN Manager (anciennement vManage), qui affichera automatiquement un fichier .pcap à télécharger :

1. Accédez à **Monitor > Devices**.
2. Choisissez votre périphérique (**c8000v-appqoe-4**).
3. Cliquez sur **Dépannage** dans le volet de gauche.
4. Dans la section **Traffic**, choisissez **Packet Capture**.

5. Dans la liste déroulante de sélection d'interface, choisissez l'interface de tunnel AppQoE (par exemple, **Tunnel200000001**).
6. (Facultatif) Appliquez les filtres IP source/de destination ou de port.
7. Cliquez sur **Start** pour commencer la capture et sur **Stop** lorsque vous avez terminé. Le système prépare un fichier **.pcap** pour le téléchargement.

6. Choisissez la section suivante

Premier Résultat Anormal	Continuer vers
La stratégie ne correspond pas dans les deux directions	Aucune optimisation ou déviation
Aucun noeud de service sain ou éligible n'est attribué	Intégrité et affectation des noeuds de service
Le flux est contourné ou a une raison de passage	Échec et contournement de la dérivation
Réinitialisations de flux ou abandon de paquets existants	Abandon après déviation
Seules les nouvelles connexions échouent pendant une rafale	Régulateur SYN et débit de connexion
Augmentation des défaillances CFT/FID	CFT et capacité
TCP est bloqué et des preuves PMTU/MSS sont présentes	MTU et MSS
Le flux est optimisé mais la réduction est faible	efficacité du DRE

Comment l'optimisation TCP et le processus DRE traitent un flux

Avec l'optimisation TCP à double extrémité et le DRE, la connexion d'origine est représentée par trois connexions TCP :

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

DRE compresse les données répétées sur le segment de superposition. Le périphérique distant reconstruit le flux d'origine avant de le transmettre à la destination. Une topologie de noeud de service externe ajoute la redirection de contrôleur de service vers noeud de service, mais les mêmes points de contrôle restent : politique, symétrie de chemin, éligibilité des noeuds de service, détournement de flux, compatibilité des homologues et état DRE.

Terme	Signification dans ce guide
Optimisé	Le service AppQoE sélectionné est actif pour le flux.
Contournement ou transfert	Le trafic continue sans le service AppQoE choisi ; inspectez la raison de la transmission.
Goutte	Le paquet ne continue pas ; cela a un impact sur l'utilisateur et nécessite une corrélation d'abandon/erreur.
État de flux de fermeture après panne	Une fois qu'un flux a été inspecté/dévié, certaines défaillances de déviation ultérieures ne peuvent pas être ramenées en toute sécurité à une dérivation ordinaire.
SC	Contrôleur de service
SN/ISN/ESN	Noeud de service/Noeud de service intégré/Noeud de service externe
CFT	Table de flux de connexion utilisée pour suivre les flux et leur état de fonctionnalité

Pas d'optimisation ni de déviation

Confirmer

1. Confirmez la correspondance de stratégie et les actions dans les deux directions.
2. Confirmez le routage symétrique via la paire de périphériques AppQoE attendue.
3. Vérifiez que le groupe de noeuds de service et les ID de site sont corrects.
4. Vérifiez que le DRE est déployé et qu'il fonctionne correctement aux deux extrémités.
5. Inspectez l'état du motif de flux ou de transit cible.

Interpréter

- Aucune correspondance de stratégie signifie généralement que la classification, la direction, le VPN ou la connexion est incorrecte.
- Une correspondance unilatérale peut activer la gestion TCP/DRE sur une périphérie, mais ne peut pas fournir un chemin DRE à deux extrémités valide.
- Un flux peut être correctement contourné lorsque le trafic est déjà optimisé, qu'il s'agit d'un type de flux non pris en charge, qu'il est asymétrique ou qu'il correspond à une condition de contournement automatique.

Correction et vérification

Les problèmes de stratégie, de direction, de groupe de noeuds, d'ID de site ou de routage sont corrects. Créez ensuite une nouvelle connexion TCP et vérifiez le flux aux deux extrémités. N'utilisez pas de connexion existante pour valider une modification de stratégie.

Échec et contournement de la dérivation

Utilisez les statistiques QFP internes uniquement après que les commandes de flux et d'erreur AppQoE prises en charge ont réduit le problème :

```
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
```

Comparer deux instantanés ; ces compteurs sont cumulatifs.

Exemple de TP :

c8000v-appqoe-3 (contrôleur AppNav), 2026-07-15. l'indice SN est vert et aucun compteur de cause de chute ne dépasse le nombre de transitoires SN malsains attendu enregistré précédemment.

```
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 et appqoe_svc_on_appqoe_vpn_drop : 0 pour exclure une défaillance CFT/FID et une perte de VPN récursive. Les paquets abandonnés comme SN malsain : 10 est un petit décompte historique — corrélé avec les transitions de santé SN avant de le traiter comme un impact actif.

Abandons après déviation

Confirmer

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

Si présent sur la version et la plate-forme, comparez les statistiques globales ou les statistiques avant et après une reproduction contrôlée.

Exemple de TP :

Saine ligne de base, c8000v-appqoe-3 (contrôleur), 2026-07-15. Aucune perte de fermeture en cas de panne ne se produit ; le numéro de série est actif/vert et l'erreur récente indique une perte vPath due aux PP : Échec de la nouvelle connexion 0 et vPath : 0. Le cliché de cause d'abandon

du chemin de données constitue la preuve déterminante :

```
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
```

Corrélez le temps de reproduction exact avec ces deltas avant d'étiqueter une réinitialisation comme fail-close.

Interpréter

Un flux précédemment inspecté/dévié peut être abandonné lorsque le noeud de service devient inutilisable ou qu'une redirection AppNav ultérieure échoue. Cela protège l'état du proxy établi ; la connexion client-serveur d'origine ne peut pas toujours être reconstruite de manière transparente après la disparition d'un chemin proxy. Les flux de la chaîne de services peuvent également chuter lorsque le contournement ordinaire viole le traitement de la chaîne.

N'étiquetez pas chaque réinitialisation comme une fermeture en cas d'échec. Corrélez l'heure exacte du test avec l'erreur de flux, la transition d'intégrité du noeud de service et le delta du compteur.

Correction et vérification

Restaurer un noeud de service éligible stable et corriger le chemin ou la défaillance de la chaîne de services. Effectuez la validation avec une nouvelle connexion TCP, puis vérifiez que le compteur d'abandon concerné cesse d'augmenter.

État et affectation du noeud de service

La santé est spécifique au rôle et au service. L'activité, la capacité des ressources et l'intégrité d'un Optimiseur d'applications (AO) particulier sont liées, mais non interchangeables.

Province	Comportement de Datapath attendu
Vert	Éligibilité aux flux nouveaux et existants

Province	Comportement de Datapath attendu
Jaune	Le trafic non SYN inspecté existant peut continuer ; Les nouveaux SYN ne sont pas transférés vers ce noeud. Un noeud FULL est une condition possible de couleur jaune
Rouge ou Bas	Les flux nouveaux/non engagés sont normalement contournés lorsqu'ils sont autorisés ; les flux déjà inspectés/dont la fermeture a échoué peuvent chuter ; les flux de la chaîne de services peuvent chuter

Exécutez la commande :

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

Vérifiez l'appartenance des noeuds, l'ID de site, l'activité, l'état AO, la charge/capacité, les alarmes DRE et l'accessibilité des homologues. Avant Cisco IOS XE Catalyst SD-WAN version 17.6.1a, les détails d'intégrité de sous-service peuvent être limités ; interpréter les résultats plus anciens en conséquence.

Exemple de TP :

Noeud sain, 2026-07-15. Sur le contrôleur, le numéro de série est actif avec des marqueurs d'intégrité par AO ; sur le noeud, le gestionnaire de ressources signale Vert avec réserve :

```
c8000v-appqoe-3#show service-insertion type appqoe service-node-group | begin Health
Health Markers:
              AO       Load State
             tcp           GREEN 0%
             ssl  RED/NOT AVAILABLE
             dre           GREEN 0%

c8000v-appqoe-4#show sdwan appqoe rm-resources | include Status|Max Sessions|Used Sessions
 System Memory Status        : GREEN
 Num sessions Status         : GREEN
 Overall HTX health Status   : GREEN
TCP Resources:  Max Sessions : 40000   Used Sessions : 0
DRE Resources:  Max Sessions : 750     Used Sessions : 0
```

La charge est de 0 % et les sessions utilisées sont bien inférieures aux limites 40000/750. Ce noeud n'est donc ni plein ni jaune pour des raisons de capacité. L'état global jaune affiché dans la commande show sdwan appqoe status ne trace que l'AO SSL inutilisé.

Lorsqu'un noeud est plein ou jaune parce qu'il est proche de sa capacité de session configurée, distribuez les nouvelles connexions, augmentez le profil de ressources AppQoE pris en charge là où la plate-forme le permet ou ajoutez de la capacité. Ne supposez pas que l'ajout de la DRAM du routeur modifie l'échelle de flux matériel prise en charge.

CFT et capacité

appqoe_cft_handle_pkt est un compteur d'erreurs. Elle est incrémentée lorsque AppQoE ne peut pas obtenir un ID de flux valide à partir de la gestion CFT. Une valeur croissante est la preuve d'une défaillance de manipulation CFT/FID ; une valeur faible par rapport au trafic total ne constitue pas une preuve de saturation.

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

Interpréter l'état CFT séparément de la capacité du noeud de service :

Exemple de TP :

c8000v-appqoe-3 (contrôleur), 2026-07-15. Table d'éléments de mémoire longue raccourcie.

```
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)
```

Nombre total de flux actuellement alloués : 8 contre un maximum de 1 000 000 signifie aucune pression de table, et cft_handle_pkt : 0 dans les statistiques AppQoE confirme l'absence d'échec d'acquisition FID. Une augmentation de cft_handle_pkt — et non pas uniquement l'occupation de la table — est ce qui indique un problème CFT/FID.

- L'état CFT identifie les erreurs/pressions de la table d'écoulement ou de l'ID d'écoulement.
- rm-resources identifie la capacité de session du noeud de service AppQoE.
- Les tables complètes ou la pression de la mémoire sont des causes possibles d'échec

d'acquisition FID, mais pas les seules causes.

Si l'erreur augmente au cours de l'intervalle de test, capturez l'état/l'erreur CFT, l'échelle de la plate-forme, les connexions actives et les ressources du noeud. Réduisez la pression de connexion, rééquilibrez les noeuds de service, modifiez le profil de ressources pris en charge ou passez à une plate-forme à l'échelle requise. Contactez le TAC Cisco avant de considérer une erreur CFT générique comme une conclusion de capacité matérielle.

Contrôleur SYN et débit de connexion

Utilisez l'état complet et les compteurs documentés. "SDVT_DROP_ERROR" est une classe d'erreur ; en soi, ce n'est pas la preuve que le régulateur SYN a tiré.

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

Corrélez les échecs de nouvelle connexion avec les points de présence max. Syn Drop, la perte vPath due aux points de présence et le même intervalle de test. Les flux à longue durée de vie restant sains alors que seuls les nouveaux SYN échouent renforcent l'hypothèse du régulateur.

Exemple de TP :

c8000v-appqoe-4 (noeud de service), 2026-07-15. libuinet-statistics est long ; le bloc de statistiques Vpath relatif au régulateur est affiché.

```
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
```

Nombre maximal de PP de rejet Syn atteint : 0 (et perte vPath due aux PP : 0 (erreur récente) règle le régulateur SYN ici. Le débit configuré sur le contrôleur est syn_policer_rate : 2700 (à partir de l'appel interne) ; comparez-le à votre taux SYN offert avant d'agir.

Si possible, réduisez le débit en rafale, distribuez les nouvelles connexions sur une capacité saine

et confirmez que les compteurs du régulateur documentés cessent d'augmenter. Ne pas ajuster ou contourner les limites de protection d'un guide générique ; utiliser le guide d'échelle de la plate-forme et du TAC lorsque les débits soutenus approchent les limites prises en charge.

MTU et MSS

L'ajustement MSS n'est pas, en soi, un chemin direct de suppression SYN AppQoE. Le chemin de données calcule un MSS à partir du MTU de contiguïté de noeud de service et de la surcharge d'encapsulation. Lorsqu'il le peut, il ajuste le MSS client et stocke un MSS côté serveur ; lorsque les informations MTU ne sont pas disponibles, il peut continuer sans cet ajustement.

Par conséquent, n'utilisez pas sdvt_drop_appnav_divert seul comme preuve d'un échec de calcul MSS.

Confirmer

- Enregistrer la version du logiciel ; la gestion automatisée des MTU SC-à-SN a été introduite dans la version 17.5.1a.
- Vérifiez une unité de transmission maximale (MTU) uniforme prise en charge sur le chemin contrôleur de service/noeud de service et sur le sous-réseau SD-WAN.
- Utilisez le test de MTU de chemin de bit DF et les captures SYN/SYN-ACK synchronisées au niveau des arêtes appropriées.
- Comparer les valeurs MSS offertes et ajustées et vérifier la fragmentation ou le trou noir.

Commande de plate-forme utile si prise en charge :

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

Exemple de TP :

c8000v-appqoe-3 (contrôleur), 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
```

Les sessions de superposition IPsec signalent une PMTU 1442 uniforme. Une PMTU cohérente dans les tunnels SC/SN (et aucun trou noir dans les tests DF-bit) signifie que MSS est dérivée d'une MTU de contiguïté stable ; excluez ceci avant de toucher la MTU du tunnel.

Corrigez la stratégie MTU ou MSS du chemin uniquement après avoir confirmé le saut défaillant. N'augmentez pas le MTU d'un tunnel à moins que le chemin sous-jacent complet ne puisse le transporter.

DRE est actif mais la réduction est faible

Une faible réduction ne signifie pas automatiquement que le DRE est rompu. Des données de premier passage uniques, un cache froid, des données utiles déjà compressées, un trafic chiffré sans la gestion SSL/TLS requise, des flux asymétriques, une incompatibilité des homologues ou un contournement automatique peuvent tous produire peu ou pas de réduction.

Confirmer l'état DRE et les homologues

```
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
```

Exemple de TP :

c8000v-appqoe-4 (noeud de service), 2026-07-15. L'état DRE/les statistiques/l'homologue apparaissent dans le triage Étape 4. exemple ci-dessus ; les commandes restantes :

```
c8000v-appqoe-4#show sdwan appqoe dreopt auto-bypass
c8000v-appqoe-4#
                                (empty — no flows in DRE auto-bypass)

c8000v-appqoe-4#show sdwan appqoe ad-statistics
 [Edge] AD Negotiation Start                 : 21513
 [Edge] AD Negotiation Done                  : 21215
 [Edge] Rcvd SYN-ACK w/o AD options          : 21167
 [Core] AD Negotiation Start                 : 55
 [Core] AD Negotiation Done                  : 55

c8000v-appqoe-4#show sdwan appqoe aoim-statistics
 Total Number Of Peer Syncs      : 2
 Total Passthrough Connections Due to Peer Version Mismatch   : 0
 LOCAL AO Statistics:  SSL 1.3 (Y),  DRE 0.23 (Y)
```

```
 PEER 10.20.0.1:  SSL 1.3 InCompatible=N,  DRE 0.23 InCompatible=N
 PEER 10.30.0.1:  SSL 1.3 InCompatible=N,  DRE 0.23 InCompatible=N

c8000v-appqoe-4#show sslproxy status
CA TP Label                    : PROXY-SIGNING-CA
Dual-Side Optimization         : TRUE
Min TLS Ver                    : TLS Version 1
Clear Mode                     : TRUE
```

Il n'y a rien dans le contournement automatique, la négociation Active Directory est en cours et aoim-statistics montre 0 passthroughs de non-concordance de version avec les deux homologues DRE marqués incompatibles = N. sslproxy status montre Clear Mode : VRAI, donc les charges utiles HTTPS traversent sans déchiffrement — réduction DRE faible attendue sur déjà - trafic chiffré sauf si le proxy SSL est activé. La réduction de 48 % mesurée (étape 4 du triage) est un avantage réel de l'ERD sur les flux en texte clair.

Vérifier :

1. La politique DRE correspond aux deux directions aux deux extrémités.
2. Le flux est symétrique et utilise les homologues attendus.
3. L'état du cache et de l'intégrité DRE sont actifs sans alarme pertinente.
4. Les versions homologues et les fonctionnalités AO sont compatibles.
5. La latence du disque et l'utilisation des ressources sont comprises dans la plage prise en charge.
6. Le flux n'est pas en contournement automatique.
7. Le trafic chiffré dispose du déchiffrement SSL/TLS requis et d'une configuration d'optimisation à double extrémité.

Mesurer correctement

Utilisez un ensemble de données représentatif et le même intervalle de temps aux deux extrémités. Capturez les compteurs d'octets originaux et optimisés avant et après le test. Préférez les deltas d'intervalle à un rapport de réduction à vie. Si vous testez l'avantage du cache, indiquez si l'exécution est en cache à froid ou en cache à chaud et répétez le même contenu.

Collecte et signalement des preuves

Commencez par utiliser les commandes opérationnelles prises en charge. Si la cause n'est pas claire, collectez :

- Fenêtre de reproduction UTC et tuple/VPN affecté
- Un flux défaillant et un flux dont le fonctionnement a été vérifié provenant de la même paire

de sites
- État AppQoE, erreurs récentes, stratégie, groupe de noeuds de service et flux de sortie des deux extrémités
- État DRE, statistiques d'homologues, état des ressources et deltas d'octets d'intervalle
- État CFT et statistiques QFP AppQoE lorsque ces commandes existent
- Technologie d'administration capturée avant le déblocage des compteurs ou le redémarrage des services

show sdwan appqoe flow all debug est développé par show output et n'est pas une licence permettant le débogage d'une plate-forme étendue. Elle peut être coûteuse et exposer des tuples d'écoulement ; utilisez-le uniquement pour une collection courte et étendue lorsque les commandes de flux ciblées sont insuffisantes.

Ne publiez pas de commande platform-debug générique sans version/plate-forme validée, durée de capture, destination de sortie et procédure d'arrêt testée. Utilisez les conseils du TAC Cisco pour le débogage actif ou la collecte de suivi de paquets sur un périphérique de production occupé.

Documentation Cisco associée

- Vérification et dépannage de la QoE des applications
- Optimisation TCP
- Optimisation du trafic avec DRE
- Noeuds de service externes pour les services AppQoE
- Catalyst SD-WAN AppQoE DRE : Topologie, configuration, vérification
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.