

WAAS - Dépannage des conditions de surcharge

Chapitre : Dépannage des conditions de surcharge

Cet article décrit comment dépanner les conditions de surcharge.

Co

Art

Pré

WA

Dé

Op

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Contenu

- [1 Aperçu](#)
- [2 Comment surveiller les flux TFO et les conditions de surcharge](#)
 - [2.1 Vérification de la limite de connexion TCP](#)
 - [2.2 Vérification des connexions TCP optimisées](#)
- [3 L'accélérateur d'applications MAPI et les connexions réservées ont un impact sur la surcharge](#)
- [4 Solutions pour les conditions de surcharge](#)

Aperçu

Le réseau Cisco WAAS aurait été conçu pour optimiser un certain nombre de connexions TCP, en fonction des besoins du client. Selon le modèle du WAE, il peut y avoir des limitations de connexion supplémentaires pour les accélérateurs d'applications SSL et CIFS. Lorsque la limite de connexion globale ou une limite de connexion spécifique à l'accélérateur d'application est dépassée, le périphérique est surchargé. Dans cette situation, le trafic entrant sur le périphérique est plus important qu'il ne peut le gérer et il se peut donc que le trafic ne soit pas optimisé comme prévu (le trafic surchargé passe par le biais d'un trafic non optimisé).

Comment surveiller les flux TFO et les conditions de surcharge

Lorsqu'un accélérateur WAAS est surchargé, vous voyez généralement l'alarme suivante du Gestionnaire central : Saisie de l'état de surcharge en raison de connexions Max (*nnn*). Le nombre *nnn* est le nombre de fois où le WAE est devenu surchargé depuis le dernier redémarrage.

Le périphérique enregistre également un message d'erreur syslog similaire à ce qui suit : Sysmon : %WAAS-SYSMON-3-445015 : Défaillance détectée : L'accélérateur TFO est surchargé (limite de connexion)

Vous pouvez utiliser diverses commandes **show** au niveau de l'interface de ligne de commande pour déterminer le nombre de connexions autorisées et réelles et recueillir plus d'informations.

Vérification de la limite de connexion TCP

La première commande utile est **show tfo detail**, qui peut vous indiquer le nombre de connexions TFO optimisées que le périphérique peut gérer, comme suit :

```
wae-7341# show tfo detail
```

Policy Engine Config Item	Value	
-----	-----	
State	Registered	
Default Action	Use Policy	
Connection Limit	12000	<-----Maximum number of TFO optimized
connections		
Effective Limit	11988	
Keepalive timeout	3.0 seconds	

La valeur de la limite de connexion indique que ce périphérique WAAS peut prendre en charge 12000 connexions optimisées TFO.

La limite effective peut être inférieure à la limite de connexion si l'AO MAPI a réservé certaines connexions. Les connexions réservées sont soustraites de la limite de connexion pour obtenir la limite effective.

Vérification des connexions TCP optimisées

Pour comprendre les flux TCP sur le périphérique, vous pouvez utiliser la commande **show statistics connection** (dans la version 4.1.1, utilisez la commande **show statistics connection all**). Cette commande affiche les flux TFO/DRE/LZ actuellement gérés, les flux de transfert et les flux qui sont gérés par un accélérateur d'application spécifique. Voici un exemple de cette commande :

```
wae# show statistics connection
```

Current Active Optimized Flows:	5	
Current Active Optimized TCP Plus Flows:	5	
Current Active Optimized TCP Only Flows:	0	
Current Active Optimized TCP Preposition Flows:	0	
Current Active Auto-Discovery Flows:	0	
Current Reserved Flows:	12	<----- Added in 4.1.5
Current Active Pass-Through Flows:	0	
Historical Flows:	143	

D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel
92917	10.86.232.131:41197	70.70.7.11:3268	00:1a:64:69:19:fc	TDL
92918	10.86.232.131:41198	70.70.7.11:3268	00:1a:64:69:19:fc	TDL
92921	10.86.232.131:41216	70.70.7.11:3268	00:1a:64:69:19:fc	TDL
94458	10.86.232.131:45354	70.70.7.11:1026	00:1a:64:69:19:fc	TDL
36883	10.86.232.136:1857	10.86.232.131:1026	00:1a:64:69:19:fc	TDL

À partir de la première ligne du résultat (Flux Active Optimized actuels), vous pouvez voir que le périphérique a actuellement cinq flux optimisés actifs. À partir du deuxième compteur (Flux TCP Plus optimisés actifs actuels), vous pouvez voir qu'ils sont tous gérés avec l'optimisation TFO/DRE/LZ (TFO Plus signifie que l'optimisation DRE et/ou LZ est utilisée en plus de TFO). Le troisième compteur (Flux TCP uniquement optimisés actifs actuels) affiche les flux optimisés uniquement par TFO.

Un autre compteur utile est Current Active Auto-discovery Flows, qui affiche les flux qui n'ont pas été entièrement configurés pour devenir des flux optimisés ou des flux de transfert. Pour être entièrement configurée, la connexion doit voir SYN, SYN ACK, ACK handshake, ce qui est utile à noter lors de la gestion d'une surcharge. Le compteur Current Active Pass-Through Flows affiche les connexions que le périphérique a déterminées comme étant de transfert ou lorsque le périphérique n'a pas vu la configuration SYN, SYN ACK, ACK. Ces flux ne seront pas comptabilisés comme des flux optimisés. Pour les flux de transfert, un périphérique doit pouvoir gérer jusqu'à 10 fois le nombre de flux optimisés pour lesquels il est évalué.

Le compteur Flux actuellement réservés affiche le nombre de connexions réservées à l'accélérateur MAPI. Pour plus d'informations sur les connexions MAPI réservées et leur impact sur la surcharge des périphériques, consultez la section [Impact sur la surcharge des connexions réservées de l'accélérateur d'applications MAPI](#).

La somme des trois compteurs suivants vous indique à quel point le périphérique WAE est proche de sa limite de connexion :

- Flux actuellement actifs optimisés
- Flux de découverte automatique actifs actuels
- Flux actuellement réservés (disponibles uniquement dans les versions 4.1.5 et ultérieures)

Si cette somme est égale ou supérieure à la limite de connexion, le périphérique est en état de surcharge.

Les détails des cinq flux optimisés sont affichés dans le tableau sous les compteurs.

Une autre commande que vous pouvez utiliser pour voir le nombre de flux TFO actuellement sur un périphérique est la commande **show statistics tfo detail**. Deux des compteurs les plus utiles dans le résultat sont « Nombre de connexions actives » et sous Policy Engine Statistics, « Connexions actives », comme suit :

```
wae# show statistics tfo detail
```

```
Total number of connections           : 22915
No. of active connections              : 3
connections                            <-----Current optimized
```

```

No. of pending (to be accepted) connections      : 0
No. of bypass connections                        : 113
No. of normal closed conns                      : 19124
No. of reset connections                        : 3788
  Socket write failure                          : 2520
  Socket read failure                          : 0
  WAN socket close while waiting to write       : 1
  AO socket close while waiting to write       : 86
  WAN socket error close while waiting to read  : 0
  AO socket error close while waiting to read  : 80
  DRE decode failure                           : 0
  DRE encode failure                           : 0
  Connection init failure                      : 0
  WAN socket unexpected close while waiting to read : 1048
  Exceeded maximum number of supported connections : 0
  Buffer allocation or manipulation failed       : 0
  Peer received reset from end host            : 53
  DRE connection state out of sync            : 0
  Memory allocation failed for buffer heads    : 0
  Unoptimized packet received on optimized side : 0

```

Data buffer usages:

```

Used size:          0 B,  B-size:          0 B,  B-num: 0
Cloned size:       54584 B,  B-size:       73472 B,  B-num: 111

```

Buffer Control:

```

Encode size:        0 B,  slow:          0,  stop:          0
Decode size:        0 B,  slow:          0,  stop:          0

```

AckQ Control:

```

Total:              0,  Current:          0

```

Scheduler:

```

Queue Size: IO:          0,  Semi-IO:          0,  Non-IO:          0
Total Jobs: IO:        219110,  Semi-IO:      186629,  Non-IO:      49227

```

Policy Engine Statistics

```

Session timeouts: 0,  Total timeouts: 0
Last keepalive received 00.0 Secs ago
Last registration occurred 8:03:54:38.7 Days:Hours:Mins:Secs ago
Hits:              52125,  Update Released:          17945
Active Connections:          3,  Completed Connections:          37257 <-----Active

```

Connections

```

Drops:              0
Rejected Connection Counts Due To: (Total: 12)
  Not Registered      :          12,  Keepalive Timeout      :          0
  No License          :           0,  Load Level          :          0
Connection Limit      :           0,  Rate Limit          :          0 <-----Connection

```

Limit

```

Minimum TFO          :           0,  Resource Manager    :          0
Global Config        :           0,  Server-Side        :          0
DM Deny              :           0,  No DM Accept       :          0

```

Auto-Discovery Statistics

```

Total Connections queued for accept: 22907
Connections queuing failures:        0
Socket pairs queued for accept:      0
Socket pairs queuing failures:       0
AO discovery successful:              0
AO discovery failure:                 0

```

Dans certains cas, les deux compteurs diffèrent et la raison est que le " no. de connexions actives " affiche tous les flux actuels optimisés par TFO, TFO/DRE, TFO/DRE/LZ et TFO/DRE/LZ et un accélérateur d'application. Les " Connexions actives " sous les statistiques du moteur de stratégie incluent tous les flux dans l'état ci-dessus plus les connexions qui sont optimisées uniquement par

TFO et un accélérateur d'application. Cette situation signifie qu'un flux TCP est entré et correspond à un classifieur d'accélérateur d'applications, mais que la connexion SYN, SYN ACK et ACK n'a pas été terminée.

Dans de nombreux cas de surcharge TFO, si le problème persiste, vous pouvez examiner ces commandes et déterminer si le nombre de flux optimisés est autour du nombre de connexions TCP optimisées pour le matériel. Si tel est le cas, vous pouvez afficher les détails du flux et voir ce qui utilise tous les flux pour déterminer si ce trafic est légitime et surcharge le périphérique ou s'il s'agit d'un virus, d'un analyseur de sécurité ou d'un autre élément se produisant sur le réseau.

Le compteur « Limite de connexion » sous les statistiques du moteur de stratégie indique le nombre de connexions rejetées et transmises car le WAE a dépassé son nombre de connexions TCP optimisées. Si ce compteur est élevé, cela signifie que le périphérique WAE obtient souvent plus de connexions qu'il ne peut gérer.

Si le nombre de connexions optimisées n'est pas proche du nombre évalué de connexions TCP optimisées et que vous recevez toujours une alarme de surcharge, vous devez consulter les flux de détection automatique actifs actuels de la commande **show statistics connection** ou " Active Connections " sous Policy Engine Statistics à partir de la commande **show statistics tfo detail**. Dans certains cas, le nombre de connexions optimisées peut être très faible, mais les connexions actives dans les statistiques du moteur de stratégie sont à peu près égales au nombre de flux optimisés pour le matériel. Cette situation signifie que de nombreux flux correspondent à un classifieur mais qu'ils ne sont pas entièrement établis. Lorsqu'un SYN TCP correspond à un classificateur, il réserve une connexion optimisée. Cette connexion n'apparaîtra pas dans le nombre de connexions TCP optimisées tant que la connexion TCP n'aura pas été terminée et que l'optimisation n'aura pas démarré. Si le périphérique détermine que le flux ne doit pas être optimisé, il sera supprimé du nombre de connexions actives sous Statistiques du moteur de stratégie.

Pour dépanner davantage les cas où une surcharge TFO se produit et où les connexions actives des statistiques du moteur de stratégie semblent utiliser toutes les connexions TCP optimisées sur le périphérique, utilisez la commande **show statistics Accelator detail**. Dans la sortie de cette commande, consultez les connexions actives sous Statistiques du moteur de stratégie pour chaque accélérateur d'application pour déterminer quel accélérateur d'application reçoit ces connexions qui ne sont pas entièrement établies. Examinez ensuite l'état de ces flux à l'aide de la commande **show statistics filter**, qui vous indique le nombre de tuples de filtrage sur le périphérique, comme suit :

```
wae# show statistics filtering
```

```
Number of filtering tuples: 18
Number of filtering tuple collisions: 0
Packets dropped due to filtering tuple collisions: 0
Number of transparent packets locally delivered: 965106
Number of transparent packets dropped: 0
Packets dropped due to ttl expiry: 0
Packets dropped due to bad route: 10
Syn packets dropped with our own id in the options: 0
Syn-Ack packets dropped with our own id in the options: 0
Internal client syn packets dropped: 0
Syn packets received and dropped on estab. conn: 0
Syn-Ack packets received and dropped on estab. conn: 0
Syn packets dropped due to peer connection alive: 525
Syn-Ack packets dropped due to peer connection alive: 0
Packets recvd on in progress conn. and not handled: 0
```

```

Packets dropped due to peer connection alive:          1614
Packets dropped due to invalid TCP flags:              0
Packets dropped by FB packet input notifier:          0
Packets dropped by FB packet output notifier:         0
Number of errors by FB tuple create notifier:         0
Number of errors by FB tuple delete notifier:         0
Dropped WCCP GRE packets due to invalid WCCP service: 0
Dropped WCCP L2 packets due to invalid WCCP service: 0
Number of deleted tuple refresh events:               0
Number of times valid tuples found on refresh list:   0

```

Le nombre de tuples de filtrage est le nombre de flux sur le périphérique qui sont optimisés, dans l'intercommunication, dans l'état FIN WAIT, dans l'état de configuration, etc. Chaque flux établi apparaît sous la forme de deux tuples, un pour chaque côté du flux, de sorte que le nombre que vous voyez dans cette sortie peut être beaucoup plus grand que le nombre de flux que vous voyez dans les autres commandes.

Pour obtenir plus d'informations sur les flux de la liste de filtrage, vous pouvez utiliser la commande **show filter list** comme suit :

```
wae# show filtering list
```

```

E: Established, S: Syn, A: Ack, F: Fin, R: Reset
s: sent, r: received, O: Options, P: Passthrough
B: Bypass, L: Last Ack, W: Time Wait, D: Done
T: Timedout, C: Closed

```

Local-IP:Port	Remote-IP:Port	Tuple(Mate)	State
10.86.232.82:23	10.86.232.134:41784	0xbclae980(0x0)	E
10.86.232.131:58775	70.70.7.11:3268	0x570b2900(0x570b2b80)	EW
70.70.7.11:3268	10.86.232.131:58775	0x570b2b80(0x570b2900)	EDL
70.70.7.11:3268	10.86.232.131:57920	0x570b2d80(0x570b2800)	E
10.86.232.131:57920	70.70.7.11:3268	0x570b2800(0x570b2d80)	E
10.86.232.82:23	161.44.67.102:4752	0xbclae00(0x0)	E
10.86.232.131:58787	70.70.7.11:1026	0x570b2080(0x570b2e80)	EW
70.70.7.11:1026	10.86.232.131:58787	0x570b2e80(0x570b2080)	EDL
10.86.232.131:48698	70.70.7.11:1026	0x570b2f00(0x570b2880)	PE
10.86.232.131:58774	70.70.7.11:389	0x570b2300(0x570b2180)	EW
70.70.7.11:389	10.86.232.131:58774	0x570b2180(0x570b2300)	EDL
10.86.232.131:58728	70.70.7.11:1026	0x570b2380(0x570b2a00)	E
10.86.232.131:58784	70.70.7.11:1026	0x570b2e00(0x570b2980)	EW
70.70.7.11:1026	10.86.232.131:58784	0x570b2980(0x570b2e00)	EDL
70.70.7.11:1026	10.86.232.131:48698	0x570b2880(0x570b2f00)	PE
10.86.232.131:58790	70.70.7.11:3268	0x570b2100(0x570b2c80)	EW
70.70.7.11:3268	10.86.232.131:58790	0x570b2c80(0x570b2100)	EDL

Si la commande **show statistics Accelerator all** vous indique quel accélérateur d'application utilise toutes les connexions TFO optimisées, vous pouvez filtrer sur ce port ou trafic. Par exemple, si vous voulez filtrer sur le trafic du port 80, utilisez la liste **show filter | I** : commande **80**.

Regardez la légende dans la colonne État. Dans le cas où les flux sont à l'état SYN, vous pouvez voir beaucoup de flux avec un état S. Si le WAE a renvoyé l'ACK SYN avec les options définies, vous pouvez voir l'état SAsO. Cette indication peut vous aider à déterminer l'état du flux et à partir de là, vous pouvez déterminer s'il y a un problème de routage, un virus ou un problème avec le WAE qui ne libère pas les connexions. Il se peut que vous ayez besoin de traces pour déterminer exactement ce qui arrive aux flux, mais les commandes ci-dessus devraient vous donner une idée de ce qu'il faut rechercher.

L'accélérateur d'applications MAPI et les connexions réservées ont un impact sur la surcharge

Souvent, une surcharge TFO peut être causée par les connexions réservées à l'accélérateur d'application MAPI. Il est donc utile de comprendre comment l'accélérateur d'application MAPI réserve les connexions.

L'accélérateur d'application MAPI réserve les connexions TFO pour s'assurer qu'il dispose de suffisamment de connexions pour accélérer toutes les connexions actuelles et futures que les clients établiront avec les serveurs Exchange. Il est normal qu'un client MAPI établisse plusieurs connexions. Si un client établit la connexion initiale via l'accélérateur d'application MAPI, mais que les connexions suivantes échouent dans l'accélérateur d'application MAPI, la connexion du client risque d'échouer.

Afin d'éviter ces échecs de connexion potentiels, l'accélérateur d'application MAPI réserve les ressources de connexion comme suit :

- Avant le début des connexions client, il réserve 10 connexions pour lui-même, en tant que tampon pour les nouvelles connexions anticipées.
- Pour chaque connexion client au serveur, il réserve trois connexions TFO pour cette paire client-serveur et l'une des trois est utilisée comme connexion active pour cette première connexion. Si le même client établit une deuxième ou une troisième connexion au même serveur, celles-ci sont traitées hors du pool de connexions réservé. Si un client établit une seule connexion au serveur, ces deux connexions réservées seront inutilisées et resteront dans le pool réservé. Si le client établit une connexion à un autre serveur, trois nouvelles connexions sont à nouveau réservées à cette paire client-serveur.

Toutes ces connexions réservées sont conçues pour améliorer les performances et réduire les risques d'échec de connexion client en raison de l'incapacité à établir des connexions supplémentaires via l'accélérateur d'application MAPI.

La surcharge se produit lorsque les flux actuels actifs optimisés + les flux actifs de détection automatique + les flux actuels réservés sont supérieurs à la limite de connexion fixe du périphérique. En général, de nouvelles connexions seraient alors transmises. Mais certaines nouvelles connexions MAPI peuvent encore être optimisées. Lorsque le périphérique se trouve au point de surcharge, si un client fait une demande supplémentaire à un serveur MAPI auquel il est déjà connecté, les connexions réservées sont utilisées. Mais s'il n'y a pas assez de connexions réservées (par exemple, si un client établit une quatrième connexion au même serveur MAPI et que le WAE est déjà en surcharge), une condition de connexion échappée peut se produire, ce qui peut conduire à un comportement erroné tel qu'un client recevant de nombreuses copies dupliquées du même message de messagerie unique.

Si le système n'a pas transféré la connexion à l'accélérateur d'application MAPI, vous devriez voir « PT Rjct Resources » ou « PT en cours », selon qu'il y a une activité sur la connexion. Si la connexion a été transférée à l'accélérateur d'application MAPI et que la réservation a échoué, la connexion sera marquée d'un « G » pour l'accélérateur, au lieu d'un « M » (dans la sortie de la commande **show statistics connection optimized mapi**). Pour un exemple de cette commande, consultez l'article [Dépannage de l'AO MAPI](#).

Si vous rencontrez des conditions de surcharge fréquentes, il est important de comprendre comment les clients Outlook établissent des connexions (combien de connexions au nombre de serveurs Exchange). Lorsque Outlook est exécuté sur un client, maintenez la touche **Ctrl**

enfoncée tout en cliquant avec le bouton droit sur l'icône Outlook dans la barre d'état système de la barre des tâches. Choisissez **État de la connexion** pour afficher la liste des serveurs auxquels le client Outlook s'est connecté. À partir de cela, vous pouvez voir combien de connexions le client établit et combien de serveurs Exchange différents. Si le client établit des connexions à plusieurs serveurs différents, il serait utile d'étudier les moyens de consolider le courrier afin qu'un utilisateur ouvre uniquement des connexions MAPI à un seul serveur Exchange et utilise plusieurs connexions à ce serveur.

Il est également utile d'examiner s'il existe d'autres applications susceptibles d'établir des connexions MAPI.

Solutions pour les conditions de surcharge

Examinez les connexions optimisées pour voir si elles sont légitimes. Dans de nombreux cas, une attaque par déni de service (DoS) rencontrée sur le réseau peut amener le WAE à tenter d'optimiser les connexions. Si c'est le cas, utilisez un mécanisme de protection DoS dans le réseau pour fermer proactivement les connexions.

Dans les cas où les connexions sont légitimes, le périphérique WAE déployé sur le site est de taille insuffisante et peut nécessiter une mise à niveau, ou un périphérique WAE supplémentaire peut être déployé pour accroître l'évolutivité au sein de ce site.