

# WAAS - Risoluzione dei problemi relativi alle condizioni di sovraccarico

## Capitolo: Risoluzione dei problemi di sovraccarico

In questo articolo viene descritto come risolvere i problemi relativi alle condizioni di sovraccarico.

Co

Art

Arco

Ris

Ott

Ris

app

Ris

Ris

Ris

Ris

Ris

Ris

Ris

Ris

gen

Ris

Ris

Ris

Ris

Ris

Inli

Ris

Ris

Ris

## Sommario

- [1 Panoramica](#)
- [2 Come monitorare i flussi TFO e le condizioni di sovraccarico](#)
  - [2.1 Verifica del limite di connessioni TCP](#)
  - [2.2 Controllo delle connessioni TCP ottimizzate](#)
- [3 Connessioni riservate di MAPI Application Accelerator impatto sull'overload](#)
- [4 Soluzioni per le condizioni di sovraccarico](#)

## Panoramica

La rete WAAS Cisco sarebbe stata progettata per ottimizzare un certo numero di connessioni TCP, in base alle esigenze del cliente. A seconda del modello WAE, potrebbero essere previste ulteriori limitazioni di connessione per gli acceleratori applicazioni SSL e CIFS. Quando viene superato il limite complessivo di connessione o il limite specifico di connessione di un acceleratore

applicazione, il dispositivo è sovraccarico. In questa situazione, il traffico in entrata nel dispositivo è superiore a quello che può gestire e quindi non può essere ottimizzato come previsto (il traffico di sovraccarico viene trasmesso attraverso una modalità non ottimizzata).

## Come monitorare i flussi TFO e le condizioni di sovraccarico

Quando un acceleratore WAAS è sovraccarico, in genere viene visualizzato il seguente allarme di Central Manager: È in corso il passaggio allo stato di sovraccarico a causa di Max connections ( *nnn*). Il numero *nnn* è il numero di volte in cui WAE è diventata sovraccarica dall'ultimo riavvio.

Il dispositivo registra inoltre un messaggio di errore syslog simile al seguente: Sysmon: %WAAS-SYSMON-3-45015: Errore rilevato: L'acceleratore TFO è sovraccarico (limite connessione)

È possibile usare vari comandi **show** dalla CLI per determinare il numero di connessioni consentite ed effettive e raccogliere ulteriori informazioni.

### Verifica del limite di connessioni TCP

Il primo comando utile è **show tfo detail**, che può indicare il numero di connessioni TFO ottimizzate gestibili dal dispositivo, come indicato di seguito:

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

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

Il valore Connection Limit indica che il dispositivo WAAS può supportare 12000 connessioni TFO ottimizzate.

Il limite effettivo può essere inferiore al limite di connessione se l'oggetto attivazione MAPI ha riservato alcune connessioni. Le connessioni riservate vengono sottratte dal limite connessioni per ottenere il limite effettivo.

### Controllo delle connessioni TCP ottimizzate

Per comprendere i flussi TCP sul dispositivo, è possibile utilizzare il comando **show statistics connection** (nella versione 4.1.1, utilizzare il comando **show statistics connection all**). Con questo comando vengono visualizzati i flussi TFO/DRE/LZ attualmente gestiti, i flussi pass-through e i flussi gestiti da un acceleratore applicazione specifico. Di seguito è riportato un esempio di questo comando:

```
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

Dalla prima riga dell'output (Current Active Optimized Flows), è possibile vedere che il dispositivo ha attualmente cinque flussi ottimizzati attivi. Dal secondo contatore (Current Active Optimized TCP Plus Flows), si può vedere che sono tutti gestiti con l'ottimizzazione TFO/DRE/LZ (TFO Plus significa che l'ottimizzazione DRE e/o LZ è in uso in aggiunta a TFO). Il terzo contatore (Flussi correnti solo TCP ottimizzati) mostra i flussi ottimizzati solo da TFO.

Un altro utile contatore è il flusso di rilevamento automatico attivo corrente, che visualizza i flussi che non sono stati completamente impostati per diventare flussi ottimizzati o flussi pass-through. Per completare la configurazione, la connessione deve vedere l'handshake SYN, SYN ACK, ACK, utile per tenere presente quando si ha a che fare con una condizione di sovraccarico. Il contatore Flussi attivi pass-through correnti mostra le connessioni che il dispositivo ha determinato essere pass-through o in cui il dispositivo non ha visto le impostazioni SYN, SYN ACK, ACK. Questi flussi non saranno conteggiati come flussi ottimizzati. Per i flussi pass-through, un dispositivo deve essere in grado di gestire fino a 10 volte il numero di flussi ottimizzati per cui è classificato.

Il contatore Flussi riservati correnti visualizza il numero di connessioni riservate per l'acceleratore MAPI. Per ulteriori informazioni sulle connessioni MAPI riservate e sul relativo impatto sul sovraccarico del dispositivo, vedere la sezione [Impatto delle connessioni riservate di MAPI Application Accelerator sul sovraccarico](#).

La somma dei tre contatori seguenti indica quanto il dispositivo WAE si avvicina al limite di connessione:

- Flussi ottimizzati attivi correnti
- Flussi di individuazione automatica attivi correnti
- Flussi riservati correnti (disponibili solo in 4.1.5 e versioni successive)

Se la somma è uguale o maggiore del limite di connessione, il dispositivo è in una condizione di sovraccarico.

I dettagli sui cinque flussi ottimizzati sono visualizzati nella tabella sotto i contatori.

Un altro comando che è possibile utilizzare per visualizzare il numero di flussi TFO attualmente presenti su un dispositivo è il comando **show statistics tfo detail**. Due dei contatori più utili nell'output sono "N. di connessioni attive" e sotto le Statistiche del Motore criteri "Connessioni attive", come segue:

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

```

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

```

In alcuni casi, i due contatori differiranno e la ragione è che il "No. di connessioni attive" visualizza

tutti i flussi di corrente ottimizzati da TFO, TFO/DRE, TFO/DRE/LZ e TFO/DRE/LZ e da un acceleratore di applicazioni. La sezione "Connessioni attive" delle statistiche del motore delle policy include tutti i flussi nello stato precedente più le connessioni ottimizzate solo da TFO e da un acceleratore di applicazione. In questo caso, è stato rilevato un flusso TCP corrispondente a un classificatore di acceleratori di applicazioni, ma l'handshake SYN, SYN ACK e ACK non è stato completato.

In molti casi di sovraccarico TFO, se il problema persiste, è possibile esaminare questi comandi e determinare se il numero di flussi ottimizzati si avvicina al numero nominale di connessioni TCP ottimizzate per l'hardware. In questo caso, è possibile visualizzare i dettagli del flusso e verificare che cosa sta utilizzando tutti i flussi per determinare se il traffico è legittimo e sovraccarica il dispositivo oppure se si tratta di un virus, di un programma di protezione o di un altro evento che si verifica in rete.

Il contatore "Limite connessione" nelle statistiche del modulo criteri indica il numero di connessioni rifiutate e passate perché WAE ha superato il numero di connessioni TCP ottimizzate. Se questo contatore è alto, significa che WAE riceve spesso più connessioni di quante ne possa gestire.

Se il numero di connessioni ottimizzate non si avvicina al numero nominale di connessioni TCP ottimizzate e si riceve ancora un allarme di sovraccarico, è necessario esaminare i flussi di rilevamento automatico attivi correnti dal comando **show statistics connection** o dal comando "Active Connections" in Policy Engine Statistics dal comando **show statistics tfor detail**. In alcuni casi, il numero di connessioni ottimizzate può essere molto basso, ma le connessioni attive nelle statistiche del motore delle policy sono all'incirca uguali al numero nominale di flussi ottimizzati per l'hardware. Questa situazione significa che esistono molti flussi che corrispondono a un classificatore ma non sono completamente stabiliti. Quando un TCP SYN corrisponde a un classificatore, riserva una connessione ottimizzata. Questa connessione non verrà visualizzata nel conteggio delle connessioni TCP ottimizzate fino al termine dell'handshake TCP e all'avvio dell'ottimizzazione. Se il dispositivo determina che il flusso non deve essere ottimizzato, verrà rimosso dal conteggio delle connessioni attive nelle statistiche del motore dei criteri.

Per ulteriori informazioni sui casi in cui si verifica un sovraccarico TFO e le connessioni attive alle statistiche del motore dei criteri sembrano utilizzare tutte le connessioni TCP ottimizzate sul dispositivo, utilizzare il comando **show statistics accelerator detail**. Nell'output di questo comando, esaminare Connessioni attive in Statistiche motore dei criteri per ogni acceleratore applicazione per determinare quale acceleratore applicazioni riceve queste connessioni non completamente stabilite. Verificare quindi lo stato di questi flussi utilizzando il comando **show statistics filtering**, che fornisce il numero di tuple di filtro nel dispositivo, come indicato di seguito:

```
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

```

Il numero di tuple di filtraggio è il numero di flussi nel dispositivo che sono ottimizzati, in pass-through, in stato FIN WAIT, in stato setup e così via. Ogni flusso stabilito viene visualizzato come due tuple, una per ogni lato del flusso, quindi il numero visualizzato in questo output potrebbe essere molto maggiore del numero di flussi visualizzato negli altri comandi.

Per ulteriori informazioni sui flussi nell'elenco di filtro, è possibile utilizzare il comando **show filtering list** nel modo seguente:

```
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	0xbc1ae980(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	0xbc1ae00(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

Se il comando **show statistics accelerator all** mostra l'acceleratore applicazione che sta utilizzando tutte le connessioni TFO ottimizzate, è possibile filtrare il traffico o la porta. Ad esempio, se si desidera filtrare il traffico sulla porta 80, utilizzare l'**elenco show filtering | I :80**.

Osservare la legenda nella colonna Stato. Se i flussi si trovano nello stato SYN, è possibile che vengano visualizzati molti flussi con uno stato S. Se WAE ha restituito il SYN ACK con le opzioni impostate, è possibile che vengano visualizzate le associazioni di protezione dello stato. Questa indicazione può aiutare a determinare lo stato del flusso e da qui è possibile determinare se vi è un problema di routing, un virus o un problema con WAE che non rilascia le connessioni. Potrebbero essere necessarie tracce per determinare esattamente cosa sta accadendo ai flussi, ma i comandi sopra riportati dovrebbero darvi un'idea di cosa cercare.

# Connessioni riservate di MAPI Application Accelerator impatto sull'overload

Spesso un sovraccarico TFO può essere causato dalle connessioni riservate dell'acceleratore applicazione MAPI, quindi è utile comprendere il processo di riserva delle connessioni da parte dell'acceleratore applicazione MAPI.

L'acceleratore applicazioni MAPI riserva le connessioni TFO per assicurarsi che disponga di connessioni sufficienti per accelerare tutte le connessioni correnti e future che i client effettueranno ai server Exchange. È normale per un client MAPI effettuare più connessioni. Se un client esegue la connessione iniziale tramite l'acceleratore applicazioni MAPI, ma le connessioni successive non riescono nell'acceleratore applicazioni MAPI, esiste il rischio che la connessione del client non riesca.

Per evitare questi potenziali errori di connessione, l'acceleratore applicazioni MAPI riserva le risorse di connessione nel modo seguente:

- Prima di iniziare qualsiasi connessione client, riserva 10 connessioni per se stesso, come buffer per le nuove connessioni previste.
- Per ogni connessione client al server, riserva tre connessioni TFO per quella coppia client-server e una delle tre viene utilizzata come connessione attiva per questa prima connessione. Se lo stesso client stabilisce una seconda o una terza connessione allo stesso server, tali connessioni vengono gestite all'esterno del connection pool riservato. Se un client effettua una sola connessione al server, queste due connessioni riservate non verranno utilizzate e rimarranno nel pool riservato. Se il client stabilisce una connessione a un server diverso, tre nuove connessioni sono ancora riservate per quella coppia client-server.

Tutte queste connessioni riservate sono progettate per migliorare le prestazioni e ridurre la possibilità che una connessione client venga interrotta a causa dell'impossibilità di creare connessioni aggiuntive tramite l'acceleratore applicazioni MAPI.

L'overload si verifica quando il valore di Current Active Optimized Flows + Current Active Auto-Discovery Flows + Current Reserved Flows è maggiore del limite di connessione fisso della periferica. In generale, le nuove connessioni vengono passate attraverso di esse. Tuttavia, alcune nuove connessioni MAPI potrebbero essere ancora ottimizzate. Quando il dispositivo si trova nel punto di sovraccarico, se un client effettua una richiesta aggiuntiva a un server MAPI a cui si è già connesso, vengono utilizzate connessioni riservate. Tuttavia, se non vi sono sufficienti connessioni riservate (ad esempio, se un client effettua una quarta connessione allo stesso server MAPI e WAE è già in sovraccarico), potrebbe verificarsi una condizione di escape della connessione, che potrebbe portare a un comportamento errato, ad esempio un client che riceve molte copie duplicate dello stesso messaggio di posta elettronica.

Se la connessione non viene inoltrata all'acceleratore applicazioni MAPI, a seconda che la connessione sia attiva o meno, verrà visualizzato "PT risorse rifiutate" o "PT in corso". Se la connessione è stata inoltrata all'acceleratore applicazione MAPI e la prenotazione non è riuscita, la connessione verrà contrassegnata con una "G" per l'acceleratore, anziché con una "M" (nell'output del comando **show statistics connection optimized mapi**). Per un esempio di questo comando, vedere l'articolo [Risoluzione dei problemi relativi all'oggetto attivazione MAPI](#).

Se si verificano condizioni di sovraccarico frequenti, è importante comprendere in che modo i client di Outlook eseguono le connessioni (il numero di connessioni al numero di server Exchange). Se Outlook è in esecuzione su un client, tenere premuto il tasto **Ctrl** mentre si fa clic

con il pulsante destro del mouse sull'icona di Outlook nella barra delle applicazioni. Scegliere **Stato connessione** per visualizzare l'elenco dei server a cui il client Outlook si è connesso. Da questo si può vedere quante connessioni sta effettuando il client e a quanti server Exchange differenti. Se il client effettua connessioni a diversi server, potrebbe essere utile esaminare come consolidare la posta in modo che un utente apra solo le connessioni MAPI a un singolo server di Exchange e utilizzi più connessioni a tale server.

È inoltre utile verificare se sono presenti altre applicazioni che potrebbero creare connessioni MAPI.

## **Soluzioni per le condizioni di sovraccarico**

Esaminare le connessioni ottimizzate per verificare se sono legittime. In molti casi, un attacco Denial of Service (DoS) riscontrato nella rete può causare un tentativo di ottimizzazione delle connessioni da parte di WAE. In tal caso, utilizzare un meccanismo di protezione DoS nella rete per chiudere in modo proattivo le connessioni.

Nei casi in cui le connessioni sono legittime, il WAE installato nel sito è di dimensioni insufficienti e potrebbe richiedere un aggiornamento oppure è possibile installare un WAE aggiuntivo per aumentare la scalabilità del sito.