WAAS - Solucionando problemas de condições de sobrecarga

Capítulo: Troubleshooting de Condições de Sobrecarga

Este artigo descreve como solucionar problemas de condições de sobrecarga.

Co

Art
En
trá
So
Oti
Tro
Tro
Tro
Tro
Tro
Tro
Tro
Tro
So
Tro
Tro
Tro
So
So
So
So
So
Tro

Contents

Overview

A rede Cisco WAAS teria sido projetada para otimizar um certo número de conexões TCP, com base nos requisitos do cliente. Dependendo do modelo do WAE, pode haver limitações de conexão adicionais para os aceleradores de aplicativos SSL e CIFS. Quando o limite de conexão geral ou um limite de conexão específico do acelerador de aplicativos é excedido, o dispositivo é sobrecarregado. Nessa situação, há mais tráfego entrando no dispositivo do que ele pode manipular e, portanto, o tráfego pode não ser otimizado como esperado (o tráfego

sobrecarregado passa por não otimizado).

Como monitorar fluxos de TFO e condições de sobrecarga

Quando um dispositivo do acelerador WAAS está sobrecarregado, você normalmente vê o seguinte alarme do Central Manager: Entrando no estado de sobrecarga devido a conexões máximas (*nnn*). O número *nn* é o número de vezes que o WAE se sobrecarregou desde a última reinicialização.

O dispositivo também registra uma mensagem de erro de syslog semelhante à seguinte: Sysmon: %WAAS-SYSMON-3-445015: Falha detectada: O acelerador TFO está sobrecarregado (limite de conexão)

Você pode usar vários comandos **show** na CLI para determinar o número de conexões permitidas e reais e coletar mais informações.

Verificando o limite de conexão TCP

O primeiro comando útil é **show tfo detail**, que pode indicar quantas conexões TFO otimizadas o dispositivo pode lidar, da seguinte forma:

```
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
```

O valor do Limite de conexão informa que esse dispositivo WAAS pode suportar conexões otimizadas de 12000 TFO.

O limite efetivo pode ser inferior ao limite de conexão se o MAPI AO tiver reservado algumas conexões. As conexões reservadas são subtraídas do limite de conexão para obter o limite efetivo.

Verificando as conexões TCP otimizadas

Para entender os fluxos TCP no dispositivo, você pode usar o comando **show statistics connection** (na versão 4.1.1, use o **comando show statistics connection all**). Esse comando exibe os fluxos TFO/DRE/LZ tratados atualmente, fluxos de passagem e fluxos que estão sendo tratados por um acelerador de aplicativos específico. A seguir, um exemplo desse 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
```

A partir da primeira linha na saída (Fluxos Otimizados Atuais), você pode ver que o dispositivo tem atualmente cinco fluxos otimizados ativos. A partir do segundo contador (Fluxos TCP Plus Otimizados Atuais), você pode ver que todos estão sendo tratados com otimização TFO/DRE/LZ (TFO Plus significa que a otimização de DRE e/ou LZ está sendo usada além do TFO). O terceiro contador (Fluxos Somente TCP Otimizados Ativo Atual) mostra fluxos que são otimizados somente pelo TFO.

Outro contador útil são os Fluxos de Detecção Automática Ativa Atual, que exibem fluxos que não foram totalmente configurados para se tornarem fluxos otimizados ou fluxos de passagem. Para ser totalmente configurada, a conexão deve ver o handshake SYN, SYN ACK, ACK, que é útil observar ao lidar com uma condição de sobrecarga. O contador Fluxos de Passagem Ativa Atual mostra as conexões que o dispositivo determinou serem de passagem ou onde o dispositivo não viu a configuração SYN, SYN ACK, ACK. Esses fluxos não serão contados como fluxos otimizados. Para fluxos de passagem, um dispositivo deve ser capaz de lidar com até 10 vezes o número de fluxos otimizados para os quais está classificado.

O contador Fluxos Reservados Atuais mostra o número de conexões reservadas para o acelerador MAPI. Para obter mais detalhes sobre as conexões MAPI reservadas e seu impacto na sobrecarga de dispositivos, consulte a seção Impacto Reservado das Conexões do MAPI Application Accelerator na Sobrecarga.

A soma dos três contadores a seguir informa a proximidade do dispositivo WAE com seu limite de conexão:

- Fluxos Otimizados Atuais
- Fluxos atuais de detecção automática ativa
- Fluxos atuais reservados (disponível apenas em 4.1.5 e posteriores)

Se essa soma for igual ou maior que o limite de conexão, o dispositivo estará em uma condição de sobrecarga.

Detalhes sobre os cinco fluxos otimizados são exibidos na tabela abaixo dos contadores.

Outro comando que você pode usar para ver o número de fluxos TFO atualmente em um dispositivo é o comando **show statistics for detail**. Dois dos contadores mais úteis na saída são "Nº de conexões ativas" e, nas Estatísticas do Mecanismo de Política, "Conexões ativas", como a seguir:

```
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
```

Em alguns casos, os dois contadores serão diferentes e o motivo é que o "não". de conexões

ativas" exibe todos os fluxos atuais otimizados por TFO, TFO/DRE, TFO/DRE/LZ e TFO/DRE/LZ e um acelerador de aplicativos. As "Conexões Ativas" nas estatísticas do mecanismo de política incluem todos os fluxos no estado acima mais as conexões que são otimizadas apenas pelo TFO e por um acelerador de aplicativos. Essa situação significa que um fluxo TCP entrou e correspondeu a um classificador do application accelerator, mas o handshake SYN, SYN ACK e ACK não foi concluído.

Em muitos casos de sobrecarga de TFO, se o problema ainda estiver ocorrendo, você pode examinar esses comandos e determinar se o número de fluxos otimizados está relacionado ao número de conexões de TCP otimizadas para o hardware. Se estiver, você poderá visualizar os detalhes do fluxo e ver o que está usando todos os fluxos para determinar se esse tráfego é legítimo e se está sobrecarregando o dispositivo ou se há vírus, scanner de segurança ou algo mais que está ocorrendo na rede.

O contador "Limite de conexão" nas estatísticas do mecanismo de política relata o número de conexões rejeitadas e passadas porque o WAE excedeu seu número classificado de conexões TCP otimizadas. Se esse contador estiver alto, isso significa que o WAE está frequentemente obtendo mais conexões do que pode lidar.

Se o número de conexões otimizadas não estiver próximo do número nominal de conexões TCP otimizadas e você ainda estiver recebendo um alarme de sobrecarga, você deverá observar os fluxos atuais de descoberta automática ativa do comando **show statistics connection** ou "Ative Connections" em Policy Engine Statistics do comando **show statistics for detail**. Em alguns casos, o número de conexões otimizadas pode ser muito baixo, mas as Conexões Ativas sob as Estatísticas do Mecanismo de Política são aproximadamente iguais ao número nominal de fluxos otimizados para o hardware. Essa situação significa que há muitos fluxos que correspondem a um classificador, mas eles não estão totalmente estabelecidos. Quando um TCP SYN corresponde a um classificador, ele reservará uma conexão otimizada. Essa conexão não aparecerá na contagem de conexões TCP otimizadas até que o handshake TCP seja concluído e a otimização seja iniciada. Se o dispositivo determinar que o fluxo não deve ser otimizado, ele será removido da contagem de conexões ativas sob as Estatísticas do mecanismo de política.

Para solucionar ainda mais os casos em que a sobrecarga de TFO está ocorrendo e as Conexões ativas de estatísticas do mecanismo de política parecem estar usando todas as conexões de TCP otimizadas no dispositivo, use o comando **show statistics accelerator detail**. Na saída desse comando, examine as Conexões Ativas nas Estatísticas do Mecanismo de Política para cada acelerador de aplicativos para determinar qual acelerador de aplicativos está recebendo essas conexões que não estão totalmente estabelecidas. Em seguida, observe em que estado esses fluxos podem estar usando o comando **show statistics filtering**, que fornece o número de tuplas de filtragem no dispositivo, da seguinte forma:

```
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
```

O número de tuplas de filtragem é o número de fluxos no dispositivo que são otimizados, na passagem, no estado FIN WAIT, no estado setup e assim por diante. Cada fluxo estabelecido aparece como duas alças, uma para cada lado do fluxo, de modo que o número que você vê nessa saída pode ser muito maior que o número de fluxos que você está vendo nos outros comandos.

Para obter mais informações sobre os fluxos na lista de filtragem, você pode usar o comando **show filtering list da** seguinte maneira:

```
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  0xbc1aee00(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 o comando **show statistics accelerator all** mostrar qual acelerador de aplicativos está usando todas as conexões TFO otimizadas, você pode filtrar nessa porta ou tráfego. Por exemplo, se você quiser filtrar o tráfego na porta 80, use a **lista show filtering | I:80** comando.

Examine a legenda na coluna Estado. Se os fluxos estiverem no estado SYN, você poderá ver muitos fluxos com um estado S. Se o WAE tiver enviado de volta o SYN ACK com opções definidas, você poderá ver o estado SAsO. Essa indicação pode ajudá-lo a determinar o estado do fluxo e, a partir daí, você pode determinar se há um problema de roteamento, vírus ou um problema com o WAE não liberando conexões. Você pode precisar de rastreamentos para

determinar exatamente o que está acontecendo com os fluxos, mas os comandos acima devem fornecer uma ideia do que procurar.

Impacto das conexões reservadas do MAPI Application Accelerator na sobrecarga

Frequentemente, uma sobrecarga de TFO pode ser causada pelas conexões reservadas do MAPI application accelerator, portanto, é útil entender o processo de como o MAPI application accelerator reserva conexões.

O acelerador de aplicativos MAPI reserva conexões TFO para garantir que ele tenha conexões suficientes disponíveis para acelerar todas as conexões atuais e futuras que os clientes farão com os servidores Exchange. É normal que um cliente MAPI faça várias conexões. Se um cliente fizer a conexão inicial através do MAPI application accelerator, mas as conexões subsequentes falharem no MAPI application accelerator, há um risco de a conexão do cliente falhar.

Para evitar essas possíveis falhas de conexão, o acelerador de aplicativos MAPI reserva recursos de conexão da seguinte maneira:

- Antes de qualquer conexão de cliente começar, ela reserva 10 conexões para si mesma, como um buffer para novas conexões antecipadas.
- Para cada conexão cliente com o servidor, ele reserva três conexões TFO para esse par cliente-servidor e uma das três é usada como uma conexão ativa para essa primeira conexão. Se o mesmo cliente fizer uma segunda ou terceira conexão com o mesmo servidor, elas serão tratadas do pool de conexões reservadas. Se um cliente fizer apenas uma única conexão com o servidor, essas duas conexões reservadas serão não utilizadas e permanecerão no pool reservado. Se o cliente fizer uma conexão com um servidor diferente, três novas conexões serão novamente reservadas para esse par cliente-servidor.

Todas essas conexões reservadas foram projetadas para melhorar o desempenho e reduzir a possibilidade de falha de conexão de um cliente devido à incapacidade de fazer conexões adicionais através do acelerador de aplicativos MAPI.

A sobrecarga ocorre quando os fluxos atuais otimizados ativos + fluxos atuais de descoberta automática ativa + fluxos reservados de corrente são maiores que o limite de conexão fixa do dispositivo. Em geral, novas conexões seriam então passadas. Mas algumas novas conexões MAPI podem ainda ser otimizadas. Quando o dispositivo está no ponto de sobrecarga, se um cliente faz uma solicitação adicional a um servidor MAPI ao qual ele já está conectado, então conexões reservadas são usadas. Mas se não houver conexões reservadas suficientes (por exemplo, se um cliente fizer uma quarta conexão com o mesmo servidor MAPI e o WAE já estiver em sobrecarga), uma condição de conexão escapada poderá ocorrer, o que pode levar a um comportamento errado, como um cliente que recebe muitas cópias duplicadas da mesma mensagem de correio único.

Se o sistema não encaminhou a conexão ao acelerador de aplicativos MAPI, você deve ver "PT Rjct Resources" ou "PT in progress", dependendo se há atividade na conexão. Se a conexão foi encaminhada ao acelerador de aplicativos MAPI e a reserva falhou, a conexão será marcada com um "G" para o Accelerator, em vez de um "M" (na saída do comando **show statistics connection otimized mapi**). Para obter um exemplo desse comando, consulte o artigo Troubleshooting the MAPI AO.

Se você estiver passando por condições frequentes de sobrecarga, é importante entender como

os clientes do Outlook estão fazendo conexões (quantas conexões com quantos servidores Exchange). Com o Outlook sendo executado em um cliente, mantenha pressionada a tecla **Ctrl** enquanto clica com o botão direito do mouse no ícone do Outlook na bandeja do sistema na barra de tarefas. Escolha **Status da Conexão** para exibir a lista de servidores aos quais o cliente do Outlook se conectou. A partir daí, você pode ver quantas conexões o cliente está fazendo e quantos servidores Exchange diferentes. Se o cliente estiver fazendo conexões com vários servidores diferentes, seria útil investigar maneiras de consolidar e-mails para que um usuário abra apenas conexões MAPI em um único servidor Exchange e use várias conexões para esse servidor.

Também é útil investigar se há outros aplicativos que possam estar fazendo conexões MAPI.

Soluções para condições de sobrecarga

Examine as conexões otimizadas para ver se são legítimas. Em muitos casos, um ataque de negação de serviço (DoS) encontrado na rede pode estar fazendo com que o WAE tente otimizar as conexões. Em caso afirmativo, empregue um mecanismo de proteção DoS na rede para fechar as conexões de forma proativa.

Nos casos em que as conexões são legítimas, o WAE implantado no local está abaixo do tamanho e pode precisar ser atualizado, ou um WAE adicional pode ser implantado para aumentar a escalabilidade nesse local.