WAAS - Resolución de problemas de WCCP

Capítulo: Resolución de problemas de WCCP

En este artículo se describe cómo resolver problemas de WCCP.

Co

Art
Intr
trát
Re
Op
Re
apl
Re
Re
Re
Re
Re
Re
Re
Re
Re
sob
Re
Re
Re
Re
Re
Re
Re

Contenido

Los siguientes síntomas indican posibles problemas de WCCP:

- WAE no está recibiendo tráfico (podría deberse a una configuración incorrecta de WCCP)
- Los usuarios finales no pueden acceder a sus aplicaciones de servidor (podría deberse a la retención de tráfico)
- Lentitud de la red cuando WCCP está habilitado (puede deberse a que el router descarta paquetes o a un uso elevado de la CPU del router)

- Uso excesivo de la CPU del router (podría deberse a la redirección en el software en lugar del hardware)

Los problemas de WCCP pueden ser el resultado de problemas con el router (o el dispositivo de redirección) o desde el dispositivo WAE. Es necesario observar la configuración WCCP tanto en el router como en el dispositivo WAE. Primero, veremos la configuración WCCP en el router y luego comprobaremos la configuración WCCP en el WAE.

Resolución de problemas de WCCP en el router

Esta sección trata sobre la resolución de problemas en los siguientes dispositivos:

- Switches Catalyst serie 6500 y routers ISR y serie 3700
- Routers de la serie ASR 1000

Resolución de problemas de WCCP en los switches Catalyst serie 6500 y los routers ISR y serie 3700

Comience a solucionar problemas verificando la intercepción WCCPv2 en el switch o router usando el comando **show ip wccp** IOS como se muestra a continuación:

```
Router# show ip wccp
Global WCCP information:
   Router information:
       Router Identifier:                  10.88.81.242
       Protocol Version:                   2.0

   Service Identifier: 61
       Number of Service Group Clients:    1                   <-----Client = WAE
       Number of Service Group Routers:    1
       Total Packets s/w Redirected:       68755               <-----Increments for software-
based redirection
         Process:                          2                   <-----
         Fast:                             0                   <-----
         CEF:                              68753               <-----
       Service mode:                       Open
       Service access-list:                -none-
       Total Packets Dropped Closed:       0
       Redirect access-list:               -none-
       Total Packets Denied Redirect:      0                   <-----Match service group but not
redirect list
       Total Packets Unassigned:           0
       Group access-list:                  -none-
       Total Messages Denied to Group:     0
       Total Authentication failures:      0                   <-----Packets have incorrect
service group password
       Total Bypassed Packets Received:    0
--More--
```

En las plataformas que utilizan redirección basada en software, verifique que los contadores de Total Packets s/w Redirected aumenten en el resultado del comando anterior. En las plataformas que utilizan redirección basada en hardware, estos contadores no deberían aumentar mucho. Si observa que estos contadores aumentan significativamente en las plataformas basadas en hardware, WCCP podría estar mal configurado en el router (WCCP GRE se procesa en el software de forma predeterminada), o el router podría estar cayendo de nuevo en la redirección de software debido a problemas de recursos de hardware, como el agotamiento de los recursos

TCAM. Se requiere más investigación si ve que estos contadores aumentan en una plataforma basada en hardware, lo que podría conducir a un uso elevado de la CPU.

El contador Total Packets Denied Redirect aumenta para los paquetes que coinciden con el grupo de servicio pero no coinciden con la lista de redirección.

El contador de fallas de autenticación total aumenta para los paquetes que se reciben con la contraseña incorrecta del grupo de servicios.

En los routers donde se realiza la redirección WCCP en el software, continúe verificando la intercepción WCCPv2 en el router mediante el comando **show ip wccp 61 detail** IOS de la siguiente manera:

```
Router# show ip wccp 61 detail
WCCP Client information:
       WCCP Client ID:          10.88.81.4
       Protocol Version:        2.0
       State:                   Usable                                  <-----Should be Usable
       Initial Hash Info:       00000000000000000000000000000000
                                00000000000000000000000000000000
       Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
       Hash Allotment:          256 (100.00%)                           <-----Buckets handled by
this WAE
       Packets s/w Redirected:  2452
       Connect Time:            01:19:46                                <-----Time WAE has been
in service group
       Bypassed Packets
         Process:               0
         Fast:                  0
         CEF:                   0
```

Verifique que el estado WAE en el grupo de servicio 61 sea Usable. Verifique que las cubetas de troceo estén asignadas al WAE en el campo Asignación de hash. El porcentaje indica cuántos de los bloques de hash totales se controlan con este WAE. La cantidad de tiempo que WAE ha estado en el grupo de servicios se informa en el campo Tiempo de conexión. El método de asignación de hash debe utilizarse con redirección basada en software.

Puede determinar qué WAE en la granja controlará una solicitud determinada usando el comando **show ip wccp** *service* **hash** *dst-ip src-ip dst-port src-port* **hidden IOS en el router de la siguiente manera:**

```
Router# show ip wccp 61 hash 0.0.0.0 10.88.81.10 0 0
WCCP hash information for:
   Primary Hash:   Src IP: 10.88.81.10
   Bucket:   9
   WCCP Client: 10.88.81.12                                  <-----Target WAE
```

En los routers donde se realiza la redirección WCCP en el hardware, continúe verificando la intercepción WCCPv2 en el router mediante el comando **show ip wccp 61 detail** IOS de la siguiente manera:

```
Cat6k# sh ip wccp 61 detail
WCCP Client information:
   WCCP Client ID:          10.88.80.135
```

```
   Protocol Version:        2.0
   State:                   Usable
   Redirection:             L2
   Packet Return:           GRE                    <-----Use generic GRE for hardware-based
platforms
   Packets Redirected:    0
   Connect Time:          1d18h
   Assignment:            MASK                     <-----Use Mask for hardware-based
redirection

   Mask  SrcAddr    DstAddr    SrcPort DstPort
   ----  -------    -------    ------- -------
   0000: 0x00001741 0x00000000 0x0000  0x0000       <-----Default mask

   Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
   ----- -------    -------    ------- ------- -----
   0000: 0x00000000 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0001: 0x00000001 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0002: 0x00000040 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
   0003: 0x00000041 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

Desea ver el método de asignación de máscara para los routers que son capaces de redireccionar el hardware.

Para guardar los recursos TCAM en el router, considere cambiar la máscara WCCP predeterminada para que se adapte a su entorno de red. Tenga en cuenta estas recomendaciones:

- Utilice el menor número posible de bits de máscara al utilizar la ACL de redirección WCCP. Un número menor de bits de máscara cuando se utiliza junto con la ACL de redireccionamiento da como resultado un menor uso de TCAM. Si hay 1-2 clientes WCCP en un clúster, utilice un bit. Si hay 3-4 clientes WCCP, utilice 2 bits. Si hay 5-8 clientes WCCP, utilice 3 bits y así sucesivamente.
- No recomendamos utilizar la máscara predeterminada WAAS (0x1741). Para las implementaciones de Data Center, el objetivo es equilibrar la carga de las sucursales en el Data Center en lugar de en los clientes o los hosts. La máscara derecha minimiza el peering WAE del Data Center y, por lo tanto, amplía el almacenamiento. Por ejemplo, utilice 0x100 a 0x7F00 para los Data Centers minoristas que tienen redes de sucursales /24. En el caso de las grandes empresas con un /16 por empresa, utilice 0x10000 a 0x7F0000 para equilibrar la carga de las empresas en el Data Center empresarial. En la sucursal, el objetivo es equilibrar los clientes que obtienen sus direcciones IP a través de DHCP. Por lo general, DHCP emite direcciones IP del cliente que aumentan desde la dirección IP más baja de la subred. Para equilibrar mejor las direcciones IP asignadas por DHCP con la máscara, utilice 0x1 a 0x7F para considerar solamente los bits de orden más bajo de la dirección IP del cliente para lograr la mejor distribución.

Los recursos TCAM consumidos por una lista de acceso de redirección WCCP son un producto del contenido de esa ACL multiplicado contra la máscara de bits WCCP configurada. Por lo tanto, hay contención entre el número de cubos WCCP (que se crean en función de la máscara) y el número de entradas en la ACL de redirección. Por ejemplo, una máscara de 0xF (4 bits) y una ACL de permiso de redirección de línea de 200 pueden dar como resultado 3200 entradas TCAM (2^4 x 200). La reducción de la máscara a 0x7 (3 bits) reduce el uso de TCAM en un 50% (2^3 x 200 = 1600).

Las plataformas Catalyst serie 6500 y Cisco serie 7600 son capaces de gestionar la redirección

WCCP tanto en el software como en el hardware. Si los paquetes se redirigen inadvertidamente en el software, cuando se espera una redirección del hardware, podría resultar en un uso excesivo de la CPU del router.

Puede inspeccionar la información de TCAM para determinar si la redirección se está manejando en el software o en el hardware. Utilice el comando **show tcam** IOS de la siguiente manera:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

    permit       tcp host 10.88.80.135 any
    punt         ip any any (8 matches)              <-----Packets handled in software
```

Las coincidencias "Punt" representan solicitudes que no se manejan en el hardware. Esta situación podría deberse a los siguientes errores:

- Asignación de hash en lugar de máscara
- Redirección saliente en lugar de entrante
- Redirigir excluir en
- Dirección MAC WAE desconocida
- Uso de una dirección de loopback para el destino de túnel GRE genérico

En el siguiente ejemplo, las entradas de ruta de política muestran que el router está realizando una redirección de hardware completa:

```
Cat6k# show tcam interface vlan 900 acl in ip

* Global Defaults not shared


Entries from Bank 0


Entries from Bank 1

   permit       tcp host 10.88.80.135 any
   policy-route tcp any 0.0.0.0 255.255.232.190 (60 matches)         <-----These entries show
hardware redirection
   policy-route tcp any 0.0.0.1 255.255.232.190 (8 matches)
   policy-route tcp any 0.0.0.64 255.255.232.190 (16 matches)
   policy-route tcp any 0.0.0.65 255.255.232.190 (19 matches)
   policy-route tcp any 0.0.1.0 255.255.232.190
   policy-route tcp any 0.0.1.1 255.255.232.190
   policy-route tcp any 0.0.1.64 255.255.232.190
   policy-route tcp any 0.0.1.65 255.255.232.190
   policy-route tcp any 0.0.2.0 255.255.232.190
   policy-route tcp any 0.0.2.1 255.255.232.190
   policy-route tcp any 0.0.2.64 255.255.232.190
   policy-route tcp any 0.0.2.65 255.255.232.190 (75 matches)
   policy-route tcp any 0.0.3.0 255.255.232.190 (222195 matches)
```

El valor Aquí Soy (HIA) del WAE debe introducir la misma interfaz a través de la cual se conoce el WAE MAC. Le recomendamos que utilice una interfaz de loopback y no una interfaz conectada directamente en la lista de routers WAE.

Resolución de problemas de WCCP en los routers de la serie ASR 1000

Los comandos para la resolución de problemas de WCCP en los routers Cisco ASR 1000 Series son diferentes de los otros routers. Esta sección muestra los comandos que puede utilizar para obtener información de WCCP sobre ASR 1000.

Para mostrar la información de WCCP del procesador de ruta, utilice los comandos **show platform software wccp rp active** de la siguiente manera:

```
ASR1000# sh platform software wccp rp active
Dynamic service 61
Priority: 34, Number of clients: 1                          <-----Number of WAE clients
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----Assignment, forwarding, and
return methods
L4 proto: 6, Use Source Port: No, Is closed: No
Dynamic service 62
Priority: 34, Number of clients: 1                          <-----
Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE       <-----
L4 proto: 6, Use Source Port: No, Is closed: No
```

El siguiente ejemplo muestra comandos adicionales que puede utilizar para examinar la información del procesador de reenvío:

```
ASR1000# sh platform software wccp fp active ?
  <0-255>     service ID
  cache-info  Show cache-engine info
  interface   Show interface info
  statistics  Show messaging statistics
  web-cache   Web-cache type
  |           Output modifiers
  <cr>
```

Para mostrar las estadísticas de paquetes redirigidos para cada interfaz, utilice el comando **show platform software wccp interface counters** de la siguiente manera:

```
ASR1000# sh platform software wccp interface counters
Interface GigabitEthernet0/1/2
       Input Redirect Packets  = 391
       Output Redirect Packets  = 0
Interface GigabitEthernet0/1/3
       Input Redirect Packets  = 1800
       Output Redirect Packets  = 0
```

Utilice el comando **show platform software wccp web-cache counters** para mostrar la información de caché de WCCP de la siguiente manera:

```
ASR1000# sh platform software wccp web-cache counters
Service Group (0, 0) counters
       unassigned_count = 0
       dropped_closed_count = 0
```

```
        bypass_count = 0
        bypass_failed_count = 0
        denied_count = 0
        redirect_count = 0
```

Para mostrar detalles de nivel bajo, utilice los siguientes comandos:

- **show platform so interface F0 brief**
- **show platform software wccp f0 interface**
- **debug platform software wccp configuration**

Para obtener más información, vea el informe técnico "Implementación y resolución de problemas de Web Cache Control Protocol versión 2 en Cisco ASR 1000 Series Aggregation Services Routers"

Resolución de problemas de WCCP en WAE

Empiece a resolver problemas en WAE usando el comando **show wccp services**. Desea que se configuren los servicios 61 y 62 de la siguiente manera:

```
WAE-612# show wccp services
Services configured on this File Engine
        TCP Promiscuous 61
        TCP Promiscuous 62
```

A continuación, verifique el estado de WCCP usando el comando **show wccp status**. Desea ver que WCCP versión 2 está habilitado y activo de la siguiente manera:

```
WAE-612# show wccp status
WCCP version 2 is enabled and currently active
```

Observe la información de la granja WCCP usando el comando **show wccp wide-area-engine**. Este comando muestra el número de WAE en la granja, sus direcciones IP, que es el WAE principal, los routers que pueden ver los WAEs, y otra información, de la siguiente manera:

```
WAE612# show wccp wide-area-engine
Wide Area Engine List for Service: TCP Promiscuous 61

Number of WAE's in the Cache farm: 3
Last Received Assignment Key IP address: 10.43.140.162     <-----All WAEs in farm should have
same Key IP
Last Received Assignment Key Change Number: 17
Last WAE Change Number: 16
Assignment Made Flag = FALSE

        IP address = 10.43.140.162       Lead WAE = YES  Weight = 0
        Routers seeing this Wide Area Engine(3)
                10.43.140.161
                10.43.140.166
                10.43.140.168

        IP address = 10.43.140.163       Lead WAE = NO  Weight = 0
        Routers seeing this Wide Area Engine(3)
                10.43.140.161
```

```
               10.43.140.166
               10.43.140.168

       IP address = 10.43.140.164       Lead WAE = NO  Weight = 0
       Routers seeing this Wide Area Engine(3)
               10.43.140.161
               10.43.140.166
               10.43.140.168
. . .
```

Observe la información del router mediante el comando **show wccp routers**. Verifique que haya comunicación bidireccional con los routers habilitados para WCCP y que todos los routers muestren los mismos KeyIP y KeyCN (número de cambio), como se indica a continuación:

```
WAE-612# show wccp routers

Router Information for Service: TCP Promiscuous 61
       Routers Seeing this Wide Area Engine(1)
       Router Id       Sent To         Recv ID     KeyIP         KeyCN  MCN
       10.43.140.161   10.43.140.161   00203A21    10.43.140.162  17    52   <-----Verify
routers have same KeyIP and KeyCN
       10.43.140.166   10.43.140.166   00203A23    10.43.140.162  17    53
       10.43.140.168   10.43.140.165   00203A2D    10.43.140.162  17    25
       Routers not Seeing this Wide Area Engine
               -NONE-
       Routers Notified of from other WAE's
               -NONE-
       Multicast Addresses Configured
               -NONE-
. . .
```

En los casos en que el WAE no es adyacente a la Capa 2 del router o se utiliza una dirección de loopback, se requieren rutas estáticas o un gateway predeterminado para soportar WCCP.

Para examinar la distribución de la cubeta de troceo en el grupo de servicio, utilice el comando **show wccp flows tcp-promiscuous** de la siguiente manera:

```
wae# sh wccp flows tcp-promiscuous
Flow counts for service: TCP Promiscuous 61
Bucket                              Flow Counts
  0- 11:     0     0     0     0     0     0     0     0     0     0     0     0
 12- 23:     0     0     0     0     0     0     0     0     0     0     0     0
 24- 35:     0     0     0     0     0     0     0     0     0     0     0     0
 36- 47:     0     0     0     0     0     0     0     0     0     0     0     0
 48- 59:     0     0     0     0     0     0     0     0     0     0     0     0
 60- 71:     0     0     0     0     0     0     0     0     0     0     0     0
 72- 83:     0     0     0     0     0     0     0     0     0     0     0     0
 84- 95:     0     0     0     0     0     0     0     0     0     0     0     0
 96-107:     0     0     0     0     0     0     0     0     0     0     0     0
108-119:     0     0     0     0     0     0     0     0     0     0     0     0
120-131:     0     0     0     0     0     0     0     0     0     0     0     0
132-143:     0     0     0     0     0     0     0     0     0     0     0     0
144-155:     0     0     0     0     0     0     0     0     0     0     0     0
156-167:     0     0     0     0     0     0     0     0     0     0     0     0
168-179:     0     0     0     0     0     0     0     0     0     0     0     0
180-191:     0     0     0     0     0     0     0     0     0     0     0     0
192-203:     0     0     0     0     0     0     0     0     0     0     0     0
204-215:     0     0     0     0     0     0     0     0     0     0     0     0
216-227:     0     0     0     0     0     0     0     0     0     0     0     0
```

```
228-239:     0     0     0     0     0     0     0     0     0     3     0     0
240-251:     0     0     0     0     0     0     0     0     0     0     0     0
252-255:     0     0     0     0
```

Alternativamente, puede utilizar la versión de resumen del comando para ver información similar, así como para omitir la información de flujo:

```
wae# sh wccp flows tcp-promiscuous summary
Flow summary for service: TCP Promiscuous 61
Total Buckets
OURS = 256

  0- 59: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
 60-119: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
120-179: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
180-239: 0000000000 0000000000 0000000000 0000000000 0000000000 0000000000
240-255: 0000000000 000000

BYP  = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......

AWAY = 0

  0- 59: .......... .......... .......... .......... .......... ..........
 60-119: .......... .......... .......... .......... .......... ..........
120-179: .......... .......... .......... .......... .......... ..........
180-239: .......... .......... .......... .......... .......... ..........
240-255: .......... ......
. . .
```

Utilice el comando **show wccp gre** para mostrar las estadísticas de paquetes GRE de la siguiente manera:

```
WAE-612# show wccp gre
Transparent GRE packets received:              5531561         <-----Increments for WCCP GRE
redirection
Transparent non-GRE packets received:          0               <-----Increments for WCCP L2
redirection
Transparent non-GRE non-WCCP packets received: 0               <-----Increments for ACE or PBR
redirection
Total packets accepted:                        5051            <-----Accepted for optimization;
peer WAE found
Invalid packets received:                      0
Packets received with invalid service:         0
Packets received on a disabled service:        0
Packets received too small:                    0
Packets dropped due to zero TTL:               0
Packets dropped due to bad buckets:            0
Packets dropped due to no redirect address:    0
Packets dropped due to loopback redirect:      0
Pass-through pkts dropped on assignment update:0
Connections bypassed due to load:              0
Packets sent back to router:                   0
GRE packets sent to router (not bypass)        0               <-----Handled with WCCP
```

```
negotiated return egress
Packets sent to another WAE:                    0
GRE fragments redirected:                       0
GRE encapsulated fragments received:            0
Packets failed encapsulated reassembly:         0
Packets failed GRE encapsulation:               0
--More--
```

Si la redirección WCCP funciona, cualquiera de los dos primeros contadores debería aumentar.

Los paquetes transparentes que no son GRE recibieron incrementos de contador para los paquetes que se redirigen usando el método de reenvío de redirección de capa 2 de WCCP.

Los paquetes sin GRE transparente que no son de WCCP recibieron incrementos de contador para los paquetes que son redirigidos por un método de intercepción que no es de WCCP (como ACE o PBR).

El contador Total de paquetes aceptados indica los paquetes que se aceptan para la optimización porque la detección automática encontró un WAE de peer.

Los paquetes GRE enviados al contador de router (no de desvío) indican los paquetes que se manejaron usando el método de salida de retorno negociado WCCP.

Los paquetes enviados a otro contador WAE indican que la protección de flujo se produce cuando se agrega otro WAE al grupo de servicios y comienza a gestionar una asignación de depósito que anteriormente estaba siendo manejada por otro WAE.

Verifique que los métodos de egreso que se utilizan sean los esperados usando el comando **show egress-method** de la siguiente manera:

```
WAE674# show egress-methods

Intercept method : WCCP

 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected

 TCP Promiscuous 62 :
     WCCP negotiated return method : WCCP GRE

                       Egress Method      Egress Method
     Destination        Configured            Used
     -----------  ----------------------  -------------
     any          WCCP Negotiated Return  WCCP GRE               <-----Verify these are
expected
```

Las discordancias del método de egreso pueden ocurrir en las siguientes condiciones:

- Se configura el método de salida de retorno negociado, pero WCCP negocia el método de retorno de Capa 2 y WAAS sólo admite la devolución de GRE.
- Se configura el método de salida GRE genérico, pero el método de intercepción es Capa 2 y sólo se admite WCCP GRE como método de intercepción cuando se configura la salida GRE genérica.

En cualquiera de estos casos, se provoca una alarma menor y se borra cuando se resuelve la discordancia cambiando el método de egreso o la configuración WCCP. Hasta que se borre la alarma, se utiliza el método de salida de reenvío IP predeterminado.

El siguiente ejemplo muestra el resultado del comando cuando existe una discordancia:

```
WAE612# show egress-methods
Intercept method : WCCP
 TCP Promiscuous 61 :
     WCCP negotiated return method : WCCP GRE

                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
 TCP Promiscuous 62 :

     WCCP negotiated return method : WCCP GRE
                      Egress Method      Egress Method
     Destination       Configured           Used
     -----------  ---------------------  -------------
     any          Generic GRE            IP Forwarding                    <-----Mismatch

     WARNING:  WCCP has negotiated WCCP L2 as the intercept method for     <-----Warning if
mismatch occurs
               which generic GRE is not supported as an egress method
               in this release. This device uses IP forwarding as the
               egress method instead of the configured generic GRE
               egress method.
```

Para los routers Catalyst 6500 Sup720 o Sup32, recomendamos utilizar el método de salida GRE genérico, que se procesa en el hardware. Además, se recomienda utilizar un túnel multipunto para facilitar la configuración, en lugar de un túnel punto a punto para cada WAE. Para ver los detalles de la configuración del túnel, consulte la sección Configuración de una Interfaz de Túnel GRE en un Router en la *Guía de Configuración de Servicios de Aplicación de Área Amplia de Cisco*.

Para ver las estadísticas del túnel GRE para cada router interceptador, utilice el comando **show statistics generic-gre** de la siguiente manera:

```
WAE# sh stat generic
Tunnel Destination:                          10.10.14.16
Tunnel Peer Status:                          N/A
Tunnel Reference Count:                      2
Packets dropped due to failed encapsulation:    0
Packets dropped due to no route found:          0
Packets sent:                                0
Packets sent to tunnel interface that is down:  0
Packets fragmented:                          0
```

Si no se garantiza que los paquetes de salida de un WAE no se reinterceptan, se puede producir

un loop de redirección. Si un WAE detecta su propia ID devuelta en el campo de opciones de TCP, se ha producido un loop de redirección y da como resultado el siguiente mensaje de syslog:

```
%WAAS-SYS-3-900000: 137.34.79.11:1192 - 137.34.77.196:139 - opt_syn_rcv: Routing Loop detected -
Packet has our own devid. Packet dropped.
```

Puede buscar instancias de este error en el archivo syslog.txt utilizando el comando **find** de la siguiente manera:

```
WAE-612# find match “Routing Loop” syslog.txt
```

Este error también se muestra en las estadísticas de flujo de TFO disponibles en el comando **show statistics filter** de la siguiente manera:

```
WAE-612# show statistics filtering
. . .
Syn packets dropped with our own id in the options:   8         <-----Indicates a redirection
loop
. . .
```

Si está realizando una redirección saliente en el router, a medida que el tráfico abandone el router se redirigirá de nuevo al WAE, que volverá a enrutar el paquete fuera del router, lo que provocará un loop de ruteo. Si el Data Center WAE y los servidores están en diferentes VLAN y la sucursal WAE y los clientes están en diferentes VLAN, puede evitar un loop de ruteo usando la siguiente configuración del router en la VLAN WAE:

```
ip wccp redirect exclude in
```

Si el WAE comparte la misma VLAN con sus clientes o servidores adyacentes, puede evitar los loops de ruteo usando el método de retorno negociado, o el retorno GRE genérico para las plataformas donde se realiza la redirección WCCP en el hardware. Cuando se utiliza la devolución genérica de GRE, WAE utiliza un túnel GRE para devolver el tráfico al router.

Resolución de problemas de ID de servicio configurables y tiempos de espera variables en la versión 4.4.1

NOTE: Las ID de servicio configurables WCCP y las funciones de tiempo de espera de detección de fallas variables se introdujeron en la versión 4.4.1 de WAAS. Esta sección no se aplica a las versiones anteriores de WAAS.

Todos los WAEs de una granja WCCP deben utilizar el mismo par de ID de servicio WCCP (el valor predeterminado es 61 y 62), y estos ID deben coincidir con todos los routers que admiten la granja. No se permite que un WAE con ID de servicio WCCP diferentes de los configurados en los routers se una a la granja y se produce la alarma existente "Router Inalcanzable". Asimismo, todos los WAE de una granja deben utilizar el mismo valor para el tiempo de espera de detección de fallas. Un WAE provoca una alarma si la configura con un valor que no coincide.

Si ve una alarma de que un WAE no puede unirse a un bloque WCCP, verifique que los ID de servicio WCCP configurados en el WAE y los routers en el bloque coincidan. En los WAE, utilice el comando **show wccp wide-area-engine** para verificar los ID de servicio configurados. En los

routers, puede utilizar el comando **show ip wccp** IOS.

Para verificar si WAE tiene conectividad con el router, utilice los comandos **show wccp services detail** y **show wccp router detail**.

Además, puede habilitar la salida de depuración de WCCP en WAE mediante los comandos **debug ip wccp event** o **debug ip wccp packet**.

Si ve una alarma menor "Router inutilizable" para un WAE, podría significar que el valor de tiempo de espera de detección de falla variable establecido en el WAE no es soportado por el router. Utilice el comando **show alarm secondary detail** para verificar si la razón de la alarma es "Timer interval mismatch with router":

```
WAE# show alarm minor detail

Minor Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 rtr_unusable              WCCP/svc051/rtr2.192.9.161

    Jan 11 23:18:41.885 UTC, Communication Alarm, #000005, 17000:17003
    WCCP router 2.192.9.161 unusable for service id: 51 reason: Timer interval       <-----Check
reason
mismatch with router                                                                 <-----
```

En WAE, verifique el tiempo de espera de detección de fallas configurado como sigue:

```
WAE# show wccp services detail

Service Details for TCP Promiscuous 61 Service
       Service Enabled                    : Yes
       Service Priority                   : 34
       Service Protocol                   : 6
       Application                        : Unknown
       Service Flags (in Hex)             : 501
       Service Ports                      :      0     0     0     0
                                          :      0     0     0     0
       Security Enabled for Service       : No
       Multicast Enabled for Service      : No
       Weight for this Web-CE             : 1
       Negotiated forwarding method       : GRE
       Negotiated assignment method       : HASH
       Negotiated return method           : GRE
       Negotiated HIA interval            : 2 second(s)
       Negotiated failure-detection timeout  : 30 second(s)          <-----Failure detection
timeout configured
. . .
```

En el router, verifique si la versión del IOS soporta el tiempo de espera de la detección de falla variable. Si es así, puede verificar la configuración mediante el comando **show ip wccp *xx* detail**, donde *xx* es la ID de servicio WCCP. Hay tres posibles resultados:

- WAE está utilizando el tiempo de espera predeterminado de detección de fallas de 30 segundos y el router está configurado igual o no admite el tiempo de espera de variables: La salida del router no muestra detalles sobre la configuración del tiempo de espera. Esta configuración funciona bien.

- WAE está utilizando un tiempo de espera de detección de fallas no predeterminado de 9 o 15 segundos y el router no soporta el tiempo de espera variable: El campo Estado muestra "NO utilizable" y el WAE no puede utilizar el router. Cambie el tiempo de espera de detección de fallas WAE por el valor predeterminado de 30 segundos usando el comando de configuración global **wccp tcp failure-detection 30**.
- WAE utiliza un tiempo de espera de detección de fallas no predeterminado de 9 o 15 segundos y el router admite el tiempo de espera variable: El campo de tiempo de espera del cliente muestra el tiempo de espera de detección de fallas configurado, que coincide con el WAE. Esta configuración funciona bien.

Si la granja WCCP es inestable debido a la inestabilidad del link, podría ser porque el tiempo de espera de detección de fallas WCCP es demasiado bajo.