WAAS - WCCP故障排除

章節：WCCP故障排除

本文描述如何排除WCCP問題。

目錄

以下症狀指示可能的WCCP問題：

- WAE沒有接收流量（可能是由於WCCP配置錯誤）
- 終端使用者無法訪問其伺服器應用程式（可能是由於流量被黑洞）
- 啟用WCCP時的網路緩慢（可能由於路由器丟棄資料包或路由器CPU使用率高所致）
- 路由器CPU使用率過高（可能是由於軟體而非硬體的重新導向）

WCCP問題可能由路由器（或重定向裝置）或WAE裝置問題引起。必須檢視路由器和WAE裝置上的WCCP配置。首先我們將檢視路由器上的WCCP配置，然後檢查WAE上的WCCP配置。

路由器上的WCCP故障排除

本節介紹下列裝置的故障排除：

- Catalyst 6500系列交換機以及ISR和3700系列路由器
- ASR 1000系列路由器

排除Catalyst 6500系列交換機以及ISR和3700系列路由器上的WCCP故障

使用**show ip wccp** IOS命令在交換機或路由器上檢驗WCCPv2偵聽開始故障排除，如下所示：

```
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--
```

在使用基於軟體的重新導向的平台上，確認上述命令輸出中的Total Packets s/w Redirected計數器正在遞增。在使用基於硬體的重新導向的平台上，這些計數器不會增加太多。如果您看到這些計數器在基於硬體的平台上顯著增加，則可能會在路由器上錯誤配置WCCP（預設情況下，WCCP GRE在軟體中處理），或者路由器可能由於硬體資源問題（例如TCAM資源耗盡）而回退到軟體重新導向。如果看到這些計數器在基於硬體的平台上遞增，可能導致高CPU使用率，則需要更多調查。

與服務組匹配但不與重定向清單匹配的資料包的Total Packets Denied Redirect計數器增加。

Total Authentication failures計數器為使用不正確服務組密碼接收的資料包遞增。

在軟體中執行WCCP重定向的路由器上，繼續使用**show ip wccp 61 detail IOS命令驗證路由器上的WCCPv2攔截，**如下所示：

```
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
```

驗證服務組61中的WAE狀態是否為「Usable（可用）」。在Hash Allocation欄位中驗證是否已向WAE分配雜湊儲存段。該百分比告訴您此WAE處理的總雜湊桶數。WAE在服務組中的時間在「連線時間」欄位中報告。雜湊分配方法應與基於軟體的重定向一起使用。

通過在路由器上使用**show ip wccp** ***service*** **hash** ***dst-ip src-ip dst-port src-port src-port*** hidden IOS命令，可以確定伺服器場中的哪個WAE將處理特定請求，如下所示：

```
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
```

在硬體中執行WCCP重定向的路由器上，繼續使用**show ip wccp 61 detail IOS命令驗證路由器上的WCCPv2攔截**，如下所示：

```
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)
```

您希望看到支援硬體重定向的路由器的掩碼分配方法。

為了節省路由器上的TCAM資源，請考慮更改預設WCCP掩碼以適應您的網路環境。請考慮以下建議：

- 使用WCCP重新導向ACL時，請使用儘可能最小的掩碼位數。與重新導向ACL配合使用時，遮罩位元的數量越少，TCAM利用率就越低。如果群集中有1-2個WCCP客戶端，則使用位。如果有3-4個WCCP客戶端，則使用2位。如果有5-8個WCCP客戶端，則使用3位等。
- 建議不要使用WAAS預設掩碼(0x1741)。 對於資料中心部署，目標是將分支站點負載均衡到資料中心，而不是客戶端或主機。正確的掩碼將資料中心WAE對等降到最低，從而擴展儲存。例如，對於具有/24分支網路的零售資料中心，請使用0x100到0x7F00。對於每個企業具有/16的大型企業，請使用0x10000到0x7F000，將企業負載均衡到企業資料中心。在分支機構中，目標是平衡通過DHCP獲取其IP地址的客戶端。DHCP通常會發出客戶端IP地址，該地址從子網中的最低IP地址遞增。要最佳平衡DHCP分配的IP地址與掩碼，請使用0x1到0x7F僅考慮客戶端IP地址的最低位來實現最佳分配。

WCCP重定向訪問清單所消耗的TCAM資源是該ACL的內容與配置的WCCP位掩碼相乘的乘積。因此，WCCP儲存段數（根據掩碼建立）與重定向ACL中的條目數之間存在爭用。例如，掩碼0xF（4位）和200線路重定向允許ACL可能會產生3200(2^4 x 200)個TCAM條目。將掩碼縮減為0x7（3位）可減少50%的TCAM使用率(2^3 x 200 = 1600)。

Catalyst 6500系列和Cisco 7600系列平台能夠在軟體和硬體中處理WCCP重定向。如果在軟體中無意中重定向資料包，則在預計硬體重定向時，可能會導致路由器CPU使用率過高。

您可以檢查TCAM資訊，以確定是否在軟體或硬體中處理重定向。按如下說明使用**show tcam** IOS命令：

```
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
```

「點選」匹配表示未在硬體中處理的請求。出現這種情況的原因可能是以下錯誤：

- 雜湊分配而不是掩碼
- 傳出重新導向（而不是傳入）
- 重定向排除
- 未知WAE MAC地址
- 對通用GRE通道目標使用環回地址

在以下示例中，策略路由條目顯示路由器正在執行完全硬體重定向：

```
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)
```

來自WAE的Here I Am(HIA)必須進入與WAE MAC通過相同的介面。我們建議在WAE路由器清單中使用環回介面，而不是直連介面。

排除ASR 1000系列路由器上的WCCP故障

Cisco ASR 1000系列路由器上的WCCP故障排除命令與其他路由器不同。本節介紹可用於獲取ASR 1000上WCCP資訊的命令。

要顯示路由處理器WCCP資訊，請使用**show platform software wccp rp active**命令，如下所示：

```
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
```

以下示例顯示可用於檢查轉發處理器資訊的其他命令：

```
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>
```

要顯示每個介面的重定向資料包統計資訊，請使用**show platform software wccp interface counters**命令，如下所示：

```
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
```

使用**show platform software wccp web-cache counters**命令顯示WCCP快取資訊，如下所示：

```
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
```

要顯示低級詳細資訊，請使用以下命令：

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

有關詳細資訊，請參閱白皮書「在Cisco ASR 1000系列聚合服務路由器上部署和故障排除Web快取控制協定版本2」

排除WAE上的WCCP故障

使用**show wccp services**命令開始對WAE進行故障排除。您希望看到服務61和62都已配置，如下所示：

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

接下來，使用**show wccp status**命令檢查WCCP狀態。您希望看到WCCP第2版已啟用且處於活動狀態，如下所示：

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

使用**show wccp wide-area-engine**命令檢視WCCP場資訊。此命令顯示伺服器場中的WAE數量、其IP地址（一個是主要WAE）、可檢視WAE的路由器和其他資訊，如下所示：

```
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
. . .
```

使用**show wccp routers**命令檢視路由器資訊。驗證與啟用WCCP的路由器是否存在雙向通訊，並且所有路由器顯示相同的KeyIP和KeyCN（更改編號），如下所示：

```
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-
. . .
```

如果WAE不是第2層路由器鄰接或使用環回地址，則需要靜態路由或預設網關來支援WCCP。

要檢查服務組中的雜湊桶分佈，請使用**show wccp flows tcp-promiscuous**命令，如下所示：

```
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
```

或者，您可以使用命令的摘要版本來檢視類似資訊以及旁路流資訊：

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

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

BYP  = 0

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

AWAY = 0

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

使用show wccp gre命令以顯示GRE資料包統計資訊，如下所示：

```
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--
```

如果WCCP重新導向有效，前兩個計數器中的任何一個應該遞增。

對於使用WCCP第2層重定向轉發方法重定向的資料包，接收的透明非GRE資料包計數器增加。

對於通過非WCCP偵聽方法（例如ACE或PBR）重定向的資料包，接收的透明非GRE非WCCP資料包的計數器增量為。

Total packets accepted計數器表示由於自動發現找到對等WAE而被接受進行最佳化的資料包。

傳送到路由器的GRE資料包（非旁路）計數器表示使用WCCP協商的返回出口方法處理的資料包。

傳送到另一個WAE計數器的資料包表示在將另一個WAE新增到服務組並開始處理之前由另一個WAE處理的桶分配時，流量保護正在發生。

使用**show egress-methods**命令驗證正在使用的輸出方法是否為預期方法，如下所示：

```
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
```

在下列情況下可能會發生輸出方法不匹配：

- 已配置協商的返回出口方法，但WCCP會協商第2層返回方法，而且WAAS僅支援GRE返回。
- 已配置通用GRE出口方法，但偵聽方法為第2層，並且當配置通用GRE出口時，僅支援WCCP GRE作為偵聽方法。

在這兩種情況下，都會發出輕微警報，當通過更改輸出方法或WCCP配置解決不相符時，會清除該警報。在清除警報之前，使用預設的IP轉發出口方法。

以下示例顯示存在不匹配時的命令輸出：

```
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.
```

對於Catalyst 6500 Sup720或Sup32路由器，我們建議使用通用的GRE輸出方法，該方法在硬體中處理。此外，我們建議使用一條多點隧道來簡化配置，而不是為每個WAE使用一條點對點隧道。有關通道組態詳細資訊，請參閱*思科廣域應用程式服務組態設定指南*中的在路由器上設定GRE通道介面一節。

要檢視每個攔截路由器的GRE隧道統計資訊，請使用**show statistics generic-gre**命令，如下所示：

```
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
```

如果無法確保來自WAE的出口資料包不被重新攔截，可能會導致重定向環路。如果WAE檢測到TCP選項欄位中返回的自身ID，則會發生重定向循環，並導致以下系統日誌消息：

```
%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.
```

可以使用**find**命令在syslog.txt檔案中搜尋此錯誤的例項，如下所示：

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

此錯誤也會顯示在**show statistics filtering**命令中可用的TFO流統計資訊中，如下所示：

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

如果您在路由器上進行傳出重新導向，當流量離開路由器時，它會重新導向回WAE，而後者會將封包重新路由到路由器之外，導致路由回圈。如果資料中心WAE和伺服器位於不同的VLAN中，而分支WAE和客戶端位於不同的VLAN中，則可以在WAE VLAN上使用以下路由器配置來避免路由環路：

```
ip wccp redirect exclude in
```

如果WAE與其相鄰客戶端或伺服器共用同一個VLAN，則可以使用協商的返回方法或針對在硬體中執行WCCP重定向的平台的通用GRE返回來避免路由環路。使用通用GRE返回時，WAE使用GRE隧道將流量返迴路由器。

4.4.1版中的可配置服務ID和可變超時故障排除

附註：WCCP可配置服務ID和可變故障檢測超時功能是在WAAS版本4.4.1中引入的。本節不適用於較早的WAAS版本。

WCCP場中的所有WAE必須使用同一對WCCP服務ID（預設值為61和62），並且這些ID必須與支援場的所有路由器匹配。WCCP服務ID與路由器上配置的WCCP服務ID不同的WAE不允許加入伺服器群，並且會發出現有的「路由器無法到達」警報。同樣，場中的所有WAE都必須使用相同的故障檢測超時值。如果使用不匹配值配置WAE會觸發警報。

如果您看到WAE無法加入WCCP場的警報，請檢查WAE上配置的WCCP服務ID和場中的路由器是否匹配。在WAE上，使用**show wccp wide-area-engine**命令檢查已配置的服務ID。在路由器上，可以使用**show ip wccp** IOS命令。

要檢查WAE是否連線到路由器，請使用**show wccp services detail**和**show wccp router detail**命令。

此外，可以使用**debug ip wccp event**或**debug ip wccp packet**命令在WAE上啟用WCCP調試輸出。

如果您看到WAE的「路由器不可用」次要警報，可能表示路由器不支援在WAE上設定的可變故障檢測超時值。使用**show alarm minor detail**命令檢查警報原因是否為「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                                                    <-----
```

在WAE上，檢查配置的故障檢測超時，如下所示：

```
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
. . .
```

在路由器上，檢查IOS版本是否支援可變故障檢測超時。如果是，可以使用**show ip wccp *xx*** detail命令檢查已配置的設定，其中*xx*是WCCP服務ID。有三種可能的結果：

- WAE使用預設故障檢測超時30秒，並且路由器配置相同或不支援可變超時：路由器輸出未顯示有關超時設定的詳細資訊。此組態運作良好。
- WAE使用9或15秒的非預設故障檢測超時，而路由器不支援可變超時：狀態欄位顯示「不可用」，並且WAE無法使用路由器。使用**wccp tcp failure-detection 30**全域性配置命令，將WAE故障檢測超時更改為預設值30秒。
- WAE使用9或15秒的非預設故障檢測超時，並且路由器支援可變超時：客戶端超時欄位顯示配置的故障檢測超時，該超時與WAE匹配。此組態運作良好。

如果WCCP場由於鏈路擺動而不穩定，則可能因為WCCP故障檢測超時太低。