WAAS - Risoluzione dei problemi relativi a WCCP

Capitolo: Risoluzione dei problemi WCCP

In questo articolo viene descritto come risolvere i problemi relativi a WCCP.

Co

Art
Arc
Ris
Ott
Ris
app
Ris
Ris
Ris
Ris
Ris
Ris
Ris
Ris
Ris
ger
Ris
Ris
Ris
Ris
Ris
Inli
Ris
Ris
Ris
Ris

Sommario

I seguenti sintomi indicano possibili problemi WCCP:

- WAE non riceve traffico (probabilmente a causa di una configurazione errata di WCCP)
- Gli utenti finali non possono raggiungere le applicazioni server (probabilmente a causa di blocchi del traffico)

- Rallentamento della rete quando WCCP è abilitato (potrebbe essere dovuto alla perdita di pacchetti del router o all'utilizzo elevato della CPU del router)
- Utilizzo CPU router troppo elevato (potrebbe essere dovuto al reindirizzamento nel software anziché nell'hardware)

I problemi WCCP possono derivare da problemi con il router (o dispositivo di reindirizzamento) o dal dispositivo WAE. È necessario esaminare la configurazione WCCP sia sul router sia sul dispositivo WAE. Innanzitutto esamineremo la configurazione WCCP sul router, quindi verificheremo la configurazione WCCP sul server WAE.

Risoluzione dei problemi di WCCP sul router

In questa sezione vengono illustrati i problemi relativi ai seguenti dispositivi:

- Catalyst serie 6500 Switch e ISR serie 3700 Router
- ASR serie 1000 Router

Risoluzione dei problemi di WCCP sugli switch Catalyst serie 6500 e sui router ISR e serie 3700

Per iniziare la risoluzione dei problemi, verificare l'intercettazione WCCPv2 sullo switch o sul router usando il comando **show ip wcp** IOS come segue:

```
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--
```

Sulle piattaforme che utilizzano il reindirizzamento basato su software, verificare che i contatori Total Packets s/w Redirection siano in aumento nell'output del comando sopra riportato. Nelle piattaforme che utilizzano il reindirizzamento basato su hardware, questi contatori non dovrebbero aumentare molto. Se questi contatori aumentano in modo significativo su piattaforme basate su hardware, il protocollo WCCP potrebbe non essere configurato correttamente sul router (il

protocollo WCCP GRE viene elaborato nel software per impostazione predefinita) oppure il router potrebbe tornare al reindirizzamento del software a causa di problemi di risorse hardware, ad esempio l'esaurimento delle risorse TCAM. Se questi contatori aumentano su una piattaforma basata su hardware, è necessaria un'analisi più approfondita che potrebbe portare a un utilizzo elevato della CPU.

Il contatore Totale pacchetti non reindirizzati aumenta per i pacchetti che corrispondono al gruppo di servizi ma non all'elenco di reindirizzamento.

Il contatore Totale errori di autenticazione incrementa per i pacchetti ricevuti con la password del gruppo di servizi non corretta.

Sui router dove viene eseguito il reindirizzamento WCCP nel software, continuare a verificare l'intercettazione WCCPv2 sul router usando il comando **show ip wcp 61 detail** IOS come segue:

```
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
```

Verificare che lo stato WAE nel gruppo di servizi 61 sia utilizzabile. Verificare che i bucket di hash siano assegnati al WAE nel campo Assegnazione hash. La percentuale indica il numero totale di bucket di hash gestiti da WAE. La quantità di tempo per cui WAE è stata nel gruppo di servizi è indicata nel campo Tempo di connessione. Il metodo di assegnazione dell'hash deve essere utilizzato con il reindirizzamento basato su software.

Èpossibile determinare quale WAE nella farm gestirà una determinata richiesta utilizzando il comando **show ip wccp** *service* **hash** *dst-ip src-ip dst-port src-port* hidden IOS sul router come indicato di seguito:

```
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
```

Sui router con reindirizzamento WCCP nell'hardware, continuare a verificare l'intercettazione WCCPv2 sul router usando il comando **show ip wcp 61 detail** IOS come segue:

```
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)
```

Si desidera visualizzare il metodo di assegnazione delle maschere per i router che possono eseguire il reindirizzamento dell'hardware.

Per salvare le risorse TCAM sul router, si consiglia di modificare la maschera WCCP predefinita in base all'ambiente di rete. Tenere presenti le raccomandazioni seguenti:

- Usare il minor numero di bit della maschera possibile quando si usa l'ACL di reindirizzamento WCCP. Un numero inferiore di bit della maschera, se usato insieme all'ACL di reindirizzamento, riduce l'utilizzo del TCAM. Se in un cluster sono presenti 1-2 client WCCP, utilizzare un bit. Se sono presenti 3-4 client WCCP, utilizzare 2 bit. Se sono presenti 5-8 client WCCP, utilizzare 3 bit e così via.
- Si consiglia di non utilizzare la maschera predefinita WAAS (0x1741). Per le installazioni di centri dati, l'obiettivo è bilanciare il carico dei siti di filiali nel centro dati anziché nei client o negli host. La maschera giusta riduce al minimo il peering WAE del centro dati e, di conseguenza, lo storage è scalabile. Ad esempio, utilizzare da 0x100 a 0x7F00 per centri dati vendita al dettaglio con reti /24 filiali. Per le grandi aziende con /16 per azienda, utilizzare da 0x10000 a 0x7F0000 per bilanciare il carico delle aziende nel centro dati aziendale. Nelle filiali, l'obiettivo è bilanciare i client che ottengono i propri indirizzi IP tramite DHCP. In genere, DHCP invia indirizzi IP client incrementandoli dall'indirizzo IP più basso nella subnet. Per bilanciare al meglio gli indirizzi IP assegnati DHCP con la maschera, utilizzare da 0x1 a 0x7F per considerare solo i bit dell'ordine più basso dell'indirizzo IP del client e ottenere la distribuzione migliore.

Le risorse TCAM consumate da un elenco di accesso reindirizzato WCCP sono il prodotto del contenuto di quell'ACL moltiplicato per la maschera di bit WCCP configurata. Pertanto, esiste un conflitto tra il numero di bucket di WCCP (creati in base alla maschera) e il numero di voci nell'ACL di reindirizzamento. Ad esempio, una maschera di 0xF (4 bit) e un ACL di autorizzazione al reindirizzamento su 200 linee possono produrre 3200 voci TCAM (2^4 x 200). Riducendo la maschera a 0x7 (3 bit), l'utilizzo di TCAM si riduce del 50% (2^3 x 200 = 1600).

Le piattaforme Catalyst serie 6500 e Cisco serie 7600 sono in grado di gestire il reindirizzamento WCCP sia nel software che nell'hardware. Se i pacchetti vengono reindirizzati inavvertitamente nel software, quando ci si aspetta un reindirizzamento hardware, potrebbe verificarsi un utilizzo eccessivo della CPU del router.

Èpossibile esaminare le informazioni TCAM per determinare se il reindirizzamento viene gestito nel software o nell'hardware. Utilizzare il comando **show tcam** IOS come segue:

```
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
```

Le corrispondenze "Punt" rappresentano richieste non gestite nell'hardware. Questa situazione potrebbe essere causata dai seguenti errori:

- Assegnazione hash anziché maschera
- Reindirizzamento in uscita anziché in entrata
- Reindirizza esclusione in
- Indirizzo MAC WAE sconosciuto
- Utilizzo di un indirizzo di loopback per la destinazione generica del tunnel GRE

Nell'esempio seguente, le voci policy-route mostrano che il router sta eseguendo il reindirizzamento hardware completo:

```
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)
```

L'interfaccia Here I Am (HIA) di WAE deve entrare nella stessa interfaccia attraverso cui è noto WAE MAC. Si consiglia di utilizzare un'interfaccia di loopback e non un'interfaccia connessa direttamente nell'elenco dei router WAE.

Risoluzione dei problemi di WCCP su ASR serie 1000 Router

I comandi per la risoluzione dei problemi di WCCP sui router Cisco ASR serie 1000 sono diversi da quelli degli altri router. In questa sezione vengono illustrati i comandi che è possibile utilizzare per ottenere informazioni WCCP su ASR 1000.

Per visualizzare le informazioni WCCP del processore di routing, utilizzare i comandi **show platform software wccp rp active** come segue:

```
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
```

Nell'esempio seguente vengono illustrati comandi aggiuntivi che è possibile utilizzare per esaminare l'inoltro delle informazioni sul processore:

```
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>
```

Per visualizzare le statistiche dei pacchetti reindirizzati per ciascuna interfaccia, usare il comando **show platform software wccp interface counters** come segue:

```
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
```

Utilizzare il comando **show platform software wcp web-cache counters** per visualizzare le informazioni della cache WCCP come segue:

```
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
```

Per visualizzare i dettagli di basso livello, utilizzare i seguenti comandi:

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

Per ulteriori informazioni, vedere il white paper "Distribuzione e risoluzione dei problemi del protocollo di controllo Web Cache versione 2 su Cisco ASR serie 1000 Aggregation Services Router"

Risoluzione dei problemi di WCCP su WAE

Iniziare la risoluzione dei problemi su WAE utilizzando il comando **show wccp services**. Si desidera visualizzare entrambi i servizi 61 e 62 configurati, come segue:

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

Verificare quindi lo stato WCCP utilizzando il comando **show wcp status**. Si desidera verificare che WCCP versione 2 è abilitato e attivo come segue:

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

Verificare le informazioni della farm WCCP utilizzando il comando **show wcp wide-area-engine**. Con questo comando viene visualizzato il numero di WAE nella farm, i relativi indirizzi IP, ovvero il WAE principale, i router che possono visualizzare i WAE e altre informazioni, come indicato di seguito:

```
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
. . .
```

Controllare le informazioni sul router utilizzando il comando **show wccp router**. Verificare che esista una comunicazione bidirezionale con i router abilitati per WCCP e che tutti i router mostrino lo stesso KeyIP e lo stesso KeyCN (numero di modifica), come indicato di seguito:

```
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-
. . .
```

Nei casi in cui il server WAE non è adiacente al router di livello 2 o viene utilizzato un indirizzo di loopback, è necessario disporre di route statiche o di un gateway predefinito per supportare WCCP.

Per esaminare la distribuzione del bucket di hash nel gruppo di servizi, utilizzare il comando **show wccp flows tcp-promiscuous** come segue:

```
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
```

In alternativa, è possibile utilizzare la versione di riepilogo del comando per visualizzare informazioni simili e ignorare le informazioni sul flusso:

```
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: .......... ......
. . .
```

Utilizzare il comando **show wccp gre** per visualizzare le statistiche del pacchetto GRE come segue:

```
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--
```

Se il reindirizzamento WCCP funziona, uno dei primi due contatori deve essere incrementale.

I pacchetti non GRE trasparenti hanno ricevuto incrementi del contatore per i pacchetti reindirizzati con il metodo di inoltro di reindirizzamento WCCP Layer 2.

I pacchetti non GRE non WCCP trasparenti hanno ricevuto incrementi del contatore per i pacchetti reindirizzati con un metodo di intercettazione non WCCP (come ACE o PBR).

Il contatore Totale pacchetti accettati indica i pacchetti accettati per l'ottimizzazione perché l'individuazione automatica ha trovato un WAE peer.

Il contatore GRE dei pacchetti inviati al router (non da bypass) indica i pacchetti gestiti tramite il metodo di uscita di ritorno negoziato WCCP.

I pacchetti inviati a un altro contatore WAE indicano che la protezione del flusso si verifica quando un altro WAE viene aggiunto al gruppo di servizi e inizia a gestire un'assegnazione di bucket precedentemente gestita da un altro WAE.

Verificare che i metodi di uscita utilizzati siano quelli previsti utilizzando il comando **show egress-methods** come indicato di seguito:

```
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
```

La mancata corrispondenza del metodo di uscita può verificarsi nelle seguenti condizioni:

- Il metodo di uscita di ritorno negoziato è configurato, ma WCCP negozia il metodo di ritorno di layer 2 e WAAS supporta solo la restituzione GRE.
- Il metodo di uscita GRE generico è configurato, ma il metodo di intercettazione è Layer 2 e solo il metodo di intercettazione WCCP GRE è supportato quando è configurato il metodo di uscita GRE generico.

In entrambi i casi, viene generato un piccolo allarme che viene cancellato quando la mancata corrispondenza viene risolta modificando il metodo di uscita o la configurazione WCCP. Finché

l'allarme non viene cancellato, viene utilizzato il metodo di uscita predefinito per l'inoltro IP.

L'esempio seguente mostra l'output del comando quando esiste una mancata corrispondenza:

```
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.
```

Per i router Catalyst 6500 Sup720 o Sup32, si consiglia di utilizzare il metodo generico di uscita GRE, elaborato nell'hardware. Inoltre, si consiglia di utilizzare un tunnel multipoint per semplificare la configurazione, anziché un tunnel point-to-point per ciascun WAE. Per i dettagli sulla configurazione del tunnel, fare riferimento alla sezione Configurazione di un'interfaccia del tunnel GRE su un router nella *Guida alla configurazione dei servizi delle applicazioni ad ampio raggio Cisco*.

Per visualizzare le statistiche del tunnel GRE per ciascun router intercettante, usare il comando **show statistics generic-gre** come segue:

```
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
```

Se non si garantisce che i pacchetti in uscita da un WAE non vengano reintercettati, è possibile che si crei un loop di reindirizzamento. Se un WAE rileva il proprio ID restituito nel campo delle opzioni TCP, si è verificato un loop di reindirizzamento e viene visualizzato il seguente messaggio

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.
```

Èpossibile cercare le istanze di questo errore nel file syslog.txt utilizzando il comando **find** come segue:

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

Questo errore viene visualizzato anche nelle statistiche di flusso TFO disponibili nel comando **show statistics filtering** come segue:

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

Se si sta eseguendo il reindirizzamento in uscita sul router, quando il traffico esce dal router, viene reindirizzato nuovamente al server WAE, che reindirizza il pacchetto in uscita dal router, causando un loop di routing. Se il server WAE del data center si trova su VLAN diverse e il server WAE della filiale e i client si trovano su VLAN diverse, è possibile evitare un loop di routing utilizzando la seguente configurazione del router sulla VLAN WAE:

```
ip wccp redirect exclude in
```

Se WAE condivide la stessa VLAN con i client o i server adiacenti, è possibile evitare i loop di routing utilizzando il metodo di ritorno negoziato o il metodo GRE generico per le piattaforme in cui viene eseguito il reindirizzamento WCCP nell'hardware. Quando si usa il comando generico di ritorno GRE, WAE usa un tunnel GRE per restituire il traffico al router.

Risoluzione dei problemi relativi agli ID dei servizi configurabili e ai timeout delle variabili nella versione 4.4.1

NOTA: Gli ID dei servizi configurabili WCCP e le funzionalità di timeout per il rilevamento degli errori delle variabili sono stati introdotti in WAAS versione 4.4.1. Questa sezione non è applicabile alle versioni precedenti di WAAS.

Tutti i WAE in una farm WCCP devono utilizzare la stessa coppia di ID servizio WCCP (l'impostazione predefinita è 61 e 62) e questi ID devono corrispondere a tutti i router che supportano la farm. A un server WAE con ID servizio WCCP diversi da quelli configurati sui router non è consentito l'accesso alla farm e viene generato l'allarme "Router Unreachable" esistente. Analogamente, tutti i WAE di una farm devono utilizzare lo stesso valore per il timeout di rilevamento errori. WAE genera un allarme se viene configurato con un valore non corrispondente.

Se viene visualizzato un avviso che indica che un server WAE non è in grado di unirsi a una farm WCCP, verificare che gli ID del servizio WCCP configurati nel server WAE e i router della farm corrispondano. Sui server WAE, usare il comando **show wccp wide-area-engine** per controllare gli ID del servizio configurati. Sui router, è possibile usare il comando **show ip wccp** IOS.

Per verificare se WAE è connesso al router, usare i comandi **show wccp services detail** e **show wccp router detail**.

Inoltre, è possibile abilitare l'output del debug WCCP sul server WAE usando i comandi **debug ip wccp event** o **debug ip wccp packet**.

Se viene visualizzato un allarme "Router Unusable" (Inutilizzabile dal router) per un WAE, è possibile che il valore di timeout di rilevamento degli errori variabili impostato su WAE non sia supportato dal router. Usare il comando **show alarm minor detail** per verificare se la causa dell'allarme è "Mancata corrispondenza dell'intervallo del timer con il 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                                                                 <-----
```

In WAE, controllare il timeout di rilevamento errori configurato come segue:

```
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
. . .
```

Sul router, verificare se la versione IOS supporta il timeout di rilevamento degli errori variabili. In questo caso, è possibile controllare l'impostazione configurata utilizzando il comando **show ip wccp *xx* detail**, dove *xx* è l'ID del servizio WCCP. I risultati possibili sono tre:

- WAE utilizza un timeout predefinito di rilevamento errori di 30 secondi e il router è configurato allo stesso modo o non supporta il timeout variabile: L'output del router non visualizza dettagli sull'impostazione del timeout. Questa configurazione funziona correttamente.
- WAE utilizza un timeout di rilevamento errori non predefinito di 9 o 15 secondi e il router non supporta il timeout variabile: Nel campo State (Stato) viene visualizzato "NOT Usable" (Non utilizzabile) e WAE non può utilizzare il router. Modificare il timeout di WAE failure detection

sul valore predefinito di 30 secondi utilizzando il comando di configurazione globale **wccp tcp failure-detection 30**.

- WAE utilizza un timeout di rilevamento errori non predefinito di 9 o 15 secondi e il router supporta un timeout variabile: Il campo Timeout client visualizza il timeout di rilevamento errori configurato, corrispondente al valore WAE. Questa configurazione funziona correttamente.

Se la farm WCCP è instabile a causa di instabilità dei collegamenti, è possibile che il timeout di rilevamento errori WCCP sia troppo basso.