Guide de dépannage de Cisco WAAS pour la version 4.1.3 et ultérieures

Chapitre : Dépannage du WCCP

Cet article décrit comment dépanner des questions WCCP.

Contenu

Les symptômes suivants indiquent les questions possibles WCCP :

- Le WAE ne reçoit pas le trafic (pourrait être dû à la mauvaise configuration WCCP)
- Les utilisateurs finaux ne peuvent pas atteindre leurs serveurs d'application (pourrait être dû à blackholing du trafic)
- La lenteur de réseau quand le WCCP est activé (pourrait être due aux paquets de baisse de routeur ou à l'utilisation élevée de CPU de routeur)

- Utilisation excessivement élevée de CPU de routeur (pourrait être dû à la redirection en logiciel au lieu du matériel)

Les questions WCCP peuvent résulter des problèmes avec le routeur (ou réorienter le périphérique) ou du périphérique WAE. Il est nécessaire de regarder la configuration WCCP sur le routeur et sur le périphérique WAE. D'abord nous regarderons la configuration WCCP sur le routeur, puis nous vérifierons la configuration WCCP sur le WAE.

Dépannage du WCCP sur le routeur

Cette section couvre le dépannage sur les périphériques suivants :

- Commutateurs de gamme Catalyst 6500 et l'ISR et les Routeurs de gamme 3700
- Routeurs de la gamme ASR 1000

Dépannage du WCCP sur les Commutateurs de gamme Catalyst 6500 et l'ISR et les Routeurs de gamme 3700

Commencez le dépannage en vérifiant l'interception WCCPv2 sur le commutateur ou le routeur à l'aide de la commande IOS de **show ip wccp** comme suit :

```
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--
```

Sur les Plateformes qui utilisent la redirection articulée autour d'un logiciel, vérifiez que tout le s/w de paquets les compteurs réorientés incrémentent dans la sortie de commande ci-dessus. Sur les Plateformes qui utilisent la redirection réalisée par matériel, ces compteurs ne devraient pas incrémenter beaucoup. Si vous voyez que ces compteurs incrémentent de manière significative sur les Plateformes réalisées par matériel, le WCCP pourrait misconfigured sur le routeur (WCCP GRE est traité en logiciel par défaut), ou le routeur pourrait retomber à la redirection de logiciel due aux questions de ressources en matériel telles que l'exécution hors des ressources TCAM.

Plus d'enquête est exigée si vous voyez ces compteurs incrémenter sur une plate-forme réalisée par matériel, qui pourrait mener à l'utilisation du CPU élevée.

Tous les paquets refusés réorientent de contre- incréments pour les paquets qui apparient le groupe de service mais n'apparient pas la liste de réorientation.

Les échecs d'authentification totaux parent des incréments pour les paquets qui sont reçus avec le mot de passe de groupe incorrect de service.

Sur des Routeurs où la redirection WCCP est exécutée en logiciel, continuez en vérifiant l'interception WCCPv2 sur le routeur à l'aide de la commande IOS de **détail du show ip wccp 61** comme suit :

```
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
```

Vérifiez que l'état WAE dans le groupe de service 61 est utilisable. Vérifiez que des positions d'informations parasites sont assignées au WAE dans le domaine d'attribution d'informations parasites. Le pourcentage t'indique lesquelles de toutes les positions d'informations parasites sont manipulées par ce WAE. La durée que le WAE a été dans le groupe de service est signalée dans le domaine de temps de connexion. La méthode d'affectation d'informations parasites devrait être utilisée avec la redirection articulée autour d'un logiciel.

Vous pouvez déterminer quel WAE dans la batterie traitera une demande particulière à l'aide de la commande IOS masquée par***port du dst-port src-IP dst-IP d'informations parasites de service de show ip wccp*** sur le routeur comme suit :

```
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
```

Sur des Routeurs où la redirection WCCP est exécutée dans le matériel, continuez en vérifiant l'interception WCCPv2 sur le routeur à l'aide de la commande IOS de **détail du show ip wccp 61** comme suit :

```
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)
```

Vous voulez voir la méthode d'affectation de masque pour les Routeurs qui sont capables de la redirection de matériel.

Afin d'économiser des ressources TCAM sur le routeur, envisagez de modifier le masque du par défaut WCCP pour adapter à votre environnement de réseau. Considérez ces recommandations :

- Utilisez le plus petit nombre de bits de masque possibles en utilisant le WCCP réorientent l'ACL. Un plus petit nombre de bits de masque une fois utilisé en même temps que réorientent des résultats d'ACL dans l'utilisation inférieure TCAM. S'il y a 1-2 clients WCCP dans une batterie, utilisez un bit. S'il y a 3-4 clients WCCP, utilisez 2 bits. S'il y a 5-8 clients WCCP, alors utilisez 3 bits et ainsi de suite.
- Nous ne recommandons pas utilisant le masque par défaut WAAS (0x1741). Pour des déploiements de centre de traitement des données, le but est d'équilibrer la charge les filiales dans le centre de traitement des données plutôt que des clients ou des hôtes. Le bon masque réduit le centre de traitement des données WAE scrutant et par conséquent mesure la mémoire. Par exemple, utilisation 0x100 à 0x7F00 pour les centres de traitement des données au détail qui ont des réseaux de branchement de /24. Pour de grandes entreprises avec /16 par entreprise, l'utilisation 0x10000 à 0x7F0000 d'équilibrer la charge les entreprises dans les informations de l'entreprise centrent. Dans la succursale, le but est d'équilibrer les clients qui obtiennent leurs adresses IP par l'intermédiaire du DHCP. Le DHCP émet généralement des adresses IP de client incrémentant de la plus basse adresse IP dans le sous-réseau. Au meilleur DHCP d'équilibre assigné des adresses IP avec le masque, utilisation 0x1 à 0x7F de considérer seulement les bits de poids faible de l'adresse IP de client pour réaliser la meilleure distribution.

Les ressources TCAM consommées par un redirect access-list WCCP est un produit du contenu de cet ACL multiplié contre le masque de bits configuré WCCP. Par conséquent, il y a conflit entre le nombre de positions WCCP (qui sont créées ont basé sur le masque) et le nombre d'entrées dans l'ACL de réorientation. Par exemple, un masque de 0xF (4 bits) et des 200 que la ligne l'ACL réorientent autorisation peut avoir comme conséquence 3200 (2^4 X 200) entrées TCAM. Ramener le masque à 0x7 (3 bits) réduit l'utilisation TCAM de 50% (2^3 X 200 = 1600).

Les Plateformes de gamme Catalyst 6500 et de gamme Cisco 7600 sont capables de manipuler la

redirection WCCP dans le logiciel et le matériel. Si des paquets par distraction sont réorientés en logiciel, quand vous vous attendez à la redirection de matériel, elle pourrait avoir comme conséquence l'utilisation excessivement élevée de CPU de routeur.

Vous pouvez examiner les informations TCAM pour déterminer si la redirection est manipulée dans le logiciel ou le matériel. Utilisez la commande IOS de **show tcam** comme suit :

```
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
```

Les correspondances de « coup de volée » représentent des demandes non traitées dans le matériel. Cette situation pourrait sont provoqué par par les erreurs suivantes :

- Affectation d'informations parasites au lieu de masque
- Redirection sortante au lieu d'arrivée
- Redirect les excluent dedans
- Adresse MAC inconnue WAE
- Utilisant une adresse de bouclage pour la destination générique de tunnel GRE

Dans l'exemple suivant, les entrées de stratégie-artère prouvent que le routeur fait la pleine redirection de matériel :

```
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)
```

Ici je suis (HIA) du WAE dois écrire la même interface que le MAC WAE est connu. Nous recommandons que vous utilisiez une interface de bouclage et pas une interface directement connectée dans la liste de routeur WAE.

Dépannage du WCCP sur les routeurs de la gamme ASR 1000

Les commandes pour dépanner le WCCP sur les Routeurs de gamme 1000 de Cisco ASR sont différentes des autres Routeurs. Cette section prouve à des commandes que vous pouvez utiliser pour obtenir les informations WCCP sur l'ASR 1000.

Pour afficher les informations du processeur WCCP d'artère, utilisez les commandes **actives du show platform software wccp RP** comme suit :

```
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
```

L'exemple suivant prouve à des commandes supplémentaires que vous pouvez utiliser pour examiner les informations de processeur d'expédition :

```
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>
```

Pour afficher a réorienté des statistiques de paquet pour chaque interface, utilisez les **compteurs d'interface de show platform software wccp** commandent comme suit :

```
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
```

Utilisez les **compteurs de Web-cache de show platform software wccp** commandent d'afficher les informations de cache WCCP comme suit :

```
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
```

Pour afficher les détails inférieurs, utilisez les commandes suivantes :

- **brief de show platform ainsi d'interface F0**
- **interface du show platform software wccp f0**
- **mettez au point la configuration de wccp de logiciel de plate-forme**

Le pour en savoir plus, voient le livre blanc « les déployer et dépannage de la version 2 de Control Protocol de cache de Web sur le Routeurs à services d'agrégation de la gamme Cisco ASR 1000 »

Dépannage du WCCP sur le WAE

Commencez le dépannage sur le WAE à l'aide de la commande de **services de wccp d'exposition** . Vous voulez voir les services 61 et 62 configurés, comme suit :

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

Prochain contrôle l'état WCCP à l'aide de la commande d'**état de wccp d'exposition**. Vous voulez voir que la version 2 WCCP est activée et active comme suit :

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

Regardez les informations de ferme WCCP à l'aide de la commande de large-zone-**engine de wccp d'exposition**. Cette commande montre le nombre de WAEs dans la batterie, leurs adresses IP, lesquels est le pôle WAE, des Routeurs qui peuvent voir le WAEs, et d'autres informations, comme suit :

```
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
. . .
```

Regardez les informations de routeur à l'aide de l'ordre de **Routeurs de wccp d'exposition**. Vérifiez qu'il y a transmission bidirectionnelle avec les Routeurs WCCP-activés et tous les Routeurs affichent le mêmes KeyIP et KeyCN (nombre de modification), comme suit :

```
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-
. . .
```

Dans les cas où le WAE n'est pas la couche 2-adjacent au routeur, ou une adresse de bouclage est utilisée, des artères de charge statique ou une passerelle par défaut est exigée pour prendre en charge le WCCP.

Pour examiner la distribution de position d'informations parasites dans le groupe de service, utilisez la commande TCP-**promiscueuse d'écoulements de wccp d'exposition** comme suit :

```
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
```

Alternativement, vous pouvez utiliser la version récapitulative de la commande de voir les informations semblables, aussi bien que les informations d'écoulement de contournement :

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

Utilisez la commande de **gre de wccp d'exposition** d'afficher des statistiques de paquet GRE comme suit :

```
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 redirection WCCP fonctionne, l'un ou l'autre des deux premiers compteurs devrait incrémenter.

Incréments reçus par paquets transparents de non-GRE les contre- pour les paquets qui sont réorientés utilisant la couche 2 WCCP réorientent la méthode d'expédition.

Incréments reçus par paquets transparents du non-GRE non-WCCP les contre- pour les paquets qui sont réorientés par une méthode de l'interception non-WCCP (telle qu'ACE ou PBR).

Le compteur reçu par paquets totaux indique les paquets qui sont reçus pour l'optimisation parce que la détection automatique fondent un pair WAE.

Les paquets GRE envoyés au compteur de routeur (pas contournement) indique les paquets qui ont été manipulés suivre la méthode de retour négociée par WCCP de sortie.

Les paquets envoyés à un autre compteur WAE indique que la protection d'écoulement se produit quand un autre WAE est ajouté au groupe de service et commence manipulant une affectation de position qui précédemment était manipulée par un autre WAE.

Vérifiez que les méthodes de sortie qui sont utilisées sont prévues à l'aide des de sortie-**méthodes d'exposition** commandent comme suit :

```
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
```

Les non-concordances de méthode de sortie peuvent se produire dans les conditions suivantes :

- La méthode de retour négociée de sortie est configurée, mais le WCCP négocie la méthode de retour de la couche 2 et seulement le retour GRE est pris en charge par WAAS.

- La méthode générique de sortie GRE est configurée, mais la méthode d'interception est la couche 2 et seulement WCCP GRE est pris en charge comme méthode d'interception quand le de sortie générique GRE est configuré.

Dans l'un ou l'autre de ces cas, une alarme mineure est donnée et est effacée quand la non-concordance est résolue en changeant la méthode de sortie ou la configuration WCCP. Jusqu'à ce que l'alarme soit effacée, l'IP par défaut expédiant la méthode de sortie est utilisé.

L'exemple suivant affiche la sortie de commande quand une non-concordance existe :

```
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.
```

Pour les Routeurs Sup720 ou Sup32 de Catalyst 6500, nous recommandons suivre la méthode générique de sortie GRE, qui est traitée dans le matériel. Supplémentaire, nous recommandons utilisant un tunnel multipoint pour la facilité de la configuration, au lieu d'un tunnel point par point pour chaque WAE. Pour des détails de configuration de tunnel, référez-vous à la section configurant une interface de tunnel GRE sur un routeur dans le *guide de configuration de Cisco Wide Area Application Services*.

Pour visualiser les statistiques de tunnel GRE pour chaque routeur interceptant, utilisez la commande **générique-gre de statistiques d'exposition** comme suit :

```
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
```

Le manque de s'assurer que des paquets de sortie d'un WAE pas reintercepted peut mener à une boucle de redirection. Si un WAE détecte son propre ID retourné dans le domaine d'options de TCP, une boucle de redirection s'est produite et a comme conséquence le message suivant de Syslog :

```
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
```

Vous pouvez rechercher le fichier de syslog.txt pour des exemples de cette erreur à l'aide de la commande de **découverte** comme suit :

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

Cette erreur révèle également dans le TFO flux la statistique disponible dans la commande de **filtrage de statistiques d'exposition** comme suit :

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

Si vous faites la redirection sortante sur le routeur, car le trafic laisse le routeur il obtiendra réorienté de nouveau au WAE, qui reroutera le paquet le routeur, entraînant une boucle de routage. Si le centre de traitement des données WAE et les serveurs sont sur différents VLAN et le branchement WAE et les clients sont sur différents VLAN, vous pouvez éviter une boucle de routage à l'aide de la configuration de routeur suivante sur le WAE VLAN :

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

Si le WAE partage le même VLAN avec ses clients ou serveurs adjacents, vous pouvez éviter des boucles de routage à l'aide de la méthode de retour négociée, ou le retour générique GRE pour des Plateformes où la redirection WCCP est exécutée dans le matériel. En utilisant le retour générique GRE, le WAE utilise un tunnel GRE pour renvoyer le trafic au routeur.

Dépannage des id configurables de service et des délais d'attente variables dans la version 4.4.1

REMARQUE: Les id configurables de service WCCP et les caractéristiques variables de délai d'attente de détection de panne ont été introduits dans la version 4.4.1 WAAS. Cette section s'applique pas applicable à des versions plus tôt WAAS.

Tout le WAEs dans une batterie WCCP doit utiliser les mêmes paires d'id de service WCCP (le par défaut est 61 et 62), et ces id doivent apparier tous les Routeurs qui prennent en charge la batterie. Un WAE avec différents id de service WCCP que ceux configurés sur les Routeurs n'est pas permis pour joindre la batterie et l'alarme inaccessible existante de « routeur » est donnée. De même, tout le WAEs dans une batterie doit utiliser la même valeur pour le délai d'attente de détection de panne. Un WAE donne une alarme si vous la configurez avec une valeur de non-adaptation.

Si vous voyez une alarme qu'un WAE ne peut pas joindre une batterie WCCP, vérifiez que les id de service WCCP configurés sur le WAE et les Routeurs dans la batterie s'assortissent. Sur le WAEs, utilisez la commande de large-zone-**engine de wccp d'exposition** de vérifier les id configurés de service. Sur les Routeurs, vous pouvez utiliser la commande IOS de **show ip wccp**.

Pour vérifier si le WAE a la Connectivité au routeur, utilisez le **détail de services de wccp d'exposition** et **affichez les** ordres de **petit groupe de routeur de wccp**.

Supplémentaire, vous pouvez activer la sortie de débogage WCCP sur le WAE à l'aide de l' **événement d'ip wccp de débogage** ou **mettre au point des** commandes de **paquet d'ip wccp**.

Si vous voyez une alarme mineure inutilisable de « routeur » pour un WAE, il pourrait signifier que le positionnement variable de valeur du dépassement de durée de détection de panne sur le WAE n'est pas pris en charge par le routeur. Utilisez la commande **mineure de détail d'alarme d'exposition** de vérifier si la raison pour l'alarme est « non-concordance d'intervalle de compteur avec le routeur » :

```
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                                                                 <-----
```

Sur le WAE, vérifiez le délai d'attente configuré de détection de panne comme suit :

```
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
. . .
```

Sur le routeur, contrôle si la version IOS prend en charge le délai d'attente variable de détection de panne. Si oui, vous pouvez vérifier la configuration configurée à l'aide de la commande de **détail du show ip wccp *xx***, où *xx* est l'ID de service WCCP. Il y a trois résultats possibles :

- WAE utilise le délai d'attente par défaut de détection de panne de 30 secondes et le routeur est configuré les mêmes ou ne prend en charge pas le délai d'attente variable : La sortie de routeur n'affiche aucun détail au sujet de la configuration de délai d'attente. Cette configuration fonctionne bien.
- WAE utilise le délai d'attente de détection de panne de non-par défaut de 9 ou 15 secondes et le routeur ne prend en charge pas le délai d'attente variable : Les expositions de champ d'état « non utilisables » et le WAE ne peuvent pas utiliser le routeur. Changez le délai d'attente de détection de panne WAE à la valeur par défaut de 30 secondes à l'aide de la commande de configuration globale de la **détection de panne 30 de TCP de wccp**.
- WAE utilise le délai d'attente de détection de panne de non-par défaut de 9 ou 15 secondes et le routeur prend en charge le délai d'attente variable : Le champ de délai d'attente de client affiche le délai d'attente configuré de détection de panne, qui apparie le WAE. Cette configuration fonctionne bien.

Si la batterie WCCP doit instable joindre le lien instable, elle pourrait être parce que le délai d'attente de détection de panne WCCP est si bas.