

WAAS - Dépannage de WCCP

Chapitre : Dépannage de WCCP

Cet article décrit comment dépanner les problèmes WCCP.

Co

[Art](#)

[Pré](#)

[WA](#)

[Dé](#)

[Op](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

[Dé](#)

Contenu

- [1 Dépannage de WCCP sur le routeur](#)
 - [1.1 Dépannage de WCCP sur les commutateurs de la gamme Catalyst 6500 et les routeurs de la gamme ISR et 3700](#)
 - [1.2 Dépannage de WCCP sur les routeurs de la gamme ASR 1000](#)
- [2 Dépannage de WCCP sur le WAE](#)
- [3 Dépannage des ID de service configurables et des délais d'attente variables dans la version 4.4.1](#)

Les symptômes suivants indiquent des problèmes WCCP possibles :

- Le WAE ne reçoit pas de trafic (peut-être en raison d'une mauvaise configuration WCCP)
- Les utilisateurs finaux ne peuvent pas accéder à leurs applications serveur (peut-être en raison d'un blocage du trafic)
- La lenteur du réseau lorsque le protocole WCCP est activé (peut être due à la suppression de paquets par le routeur ou à l'utilisation élevée du processeur du routeur)
- Utilisation trop élevée du processeur du routeur (peut être due à une redirection dans le

logiciel plutôt que dans le matériel)

Les problèmes WCCP peuvent résulter de problèmes avec le routeur (ou le périphérique de redirection) ou du périphérique WAE. Il est nécessaire d'examiner la configuration WCCP à la fois sur le routeur et sur le périphérique WAE. Nous allons d'abord examiner la configuration WCCP sur le routeur, puis nous allons vérifier la configuration WCCP sur le WAE.

Dépannage de WCCP sur le routeur

Cette section traite du dépannage sur les périphériques suivants :

- [Commutateurs de la gamme Catalyst 6500 et routeurs ISR et 3700](#)
- [Routeurs de la gamme ASR 1000](#)

Dépannage de WCCP sur les commutateurs de la gamme Catalyst 6500 et les routeurs de la gamme ISR et 3700

Commencez le dépannage en vérifiant l'interception WCCPv2 sur le commutateur ou le routeur à l'aide de la commande IOS **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 plates-formes qui utilisent la redirection logicielle, vérifiez que les compteurs redirigés Total Packets s/w sont incrémentés dans la sortie de commande ci-dessus. Sur les plates-formes qui utilisent la redirection basée sur le matériel, ces compteurs ne devraient pas augmenter beaucoup. Si ces compteurs s'incrémentent de manière significative sur les plates-formes matérielles, WCCP peut être mal configuré sur le routeur (WCCP GRE est traité dans le logiciel par défaut), ou le routeur peut retomber dans la redirection logicielle en raison de problèmes de ressources matérielles tels que l'épuisement des ressources TCAM. Une enquête plus approfondie est nécessaire si vous voyez ces compteurs s'incrémenter sur une plate-forme

matérielle, ce qui pourrait entraîner une utilisation élevée du CPU.

Le compteur Total des paquets refusés Redirection s'incrémente pour les paquets qui correspondent au groupe de services mais ne correspondent pas à la liste de redirection.

Le compteur d'échecs d'authentification totale s'incrémente pour les paquets reçus avec le mot de passe incorrect du groupe de services.

Sur les routeurs où la redirection WCCP est effectuée dans le logiciel, continuez en vérifiant l'interception WCCPv2 sur le routeur à l'aide de la commande IOS **show ip wccp 61 detail** 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:  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                        FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  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 du groupe de services 61 est utilisable. Vérifiez que les compartiments de hachage sont affectés au périphérique WAE dans le champ Hash Allotissement. Le pourcentage indique le nombre total de compartiments de hachage gérés par ce WAE. La durée pendant laquelle le WAE a été dans le groupe de services est indiquée dans le champ Connect Time. La méthode d'affectation de hachage doit être utilisée avec la redirection logicielle.

Vous pouvez déterminer quel périphérique WAE de la batterie gèrera une requête particulière en utilisant la commande IOS cachée **show ip wccp service hash dst-ip src-ip dst-port src-port** 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 les routeurs où la redirection WCCP est effectuée dans le matériel, continuez en vérifiant l'interception WCCPv2 sur le routeur à l'aide de la commande IOS **show ip wccp 61 detail** 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 capables de redirection matérielle.

Afin d'enregistrer les ressources TCAM sur le routeur, pensez à modifier le masque WCCP par défaut pour qu'il corresponde à votre environnement réseau. Examinez ces recommandations :

- Utilisez le plus petit nombre de bits de masque possible lors de l'utilisation de la liste de contrôle d'accès de redirection WCCP. Un plus petit nombre de bits de masque lorsqu'il est utilisé en conjonction avec la liste de contrôle d'accès Redirect entraîne une utilisation TCAM plus faible. S'il y a 1 à 2 clients WCCP dans un cluster, utilisez un bit. S'il existe 3 à 4 clients WCCP, utilisez 2 bits. S'il existe entre 5 et 8 clients WCCP, utilisez 3 bits, etc.
- Il est déconseillé d'utiliser le masque par défaut WAAS (0x1741). Dans le cas des déploiements de data center, l'objectif est d'équilibrer la charge des sites des filiales dans le data center plutôt que des clients ou des hôtes. Le masque de droite minimise l'appairage WAE du data center et, par conséquent, fait évoluer le stockage. Par exemple, utilisez 0x100 à 0x7F00 pour les data centers de détail qui ont des réseaux de filiales /24. Pour les grandes entreprises ayant un /16 par entreprise, utilisez 0x10000 à 0x7F0000 pour équilibrer la charge des entreprises dans le data center d'entreprise. Dans la filiale, l'objectif est d'équilibrer les clients qui obtiennent leurs adresses IP via DHCP. En règle générale, le protocole DHCP émet des adresses IP client qui s'incrémentent à partir de l'adresse IP la plus basse du sous-réseau. Pour équilibrer au mieux les adresses IP attribuées par DHCP avec le masque, utilisez 0x1 à 0x7F pour ne considérer que les bits d'ordre le plus bas de l'adresse IP du client pour obtenir la meilleure distribution.

Les ressources TCAM consommées par une liste d'accès de redirection WCCP sont un produit du contenu de cette liste de contrôle d'accès multipliée par rapport au masque de bit WCCP configuré. Par conséquent, il y a conflit entre le nombre de compartiments WCCP (créés en fonction du masque) et le nombre d'entrées dans la liste de contrôle d'accès de redirection. Par exemple, un masque de 0xF (4 bits) et une liste de contrôle d'accès d'autorisation de redirection de 200 lignes peuvent entraîner 3 200 entrées TCAM ($2^4 \times 200$). La réduction du masque à 0x7 (3 bits) réduit l'utilisation de la TCAM de 50 % ($2^3 \times 200 = 1600$).

Les plates-formes des gammes Catalyst 6500 et Cisco 7600 sont capables de gérer la redirection WCCP dans le logiciel et le matériel. Si des paquets sont redirigés par inadvertance dans le logiciel, lorsque vous prévoyez une redirection matérielle, cela pourrait entraîner une utilisation

trop élevée du processeur du routeur.

Vous pouvez examiner les informations TCAM pour déterminer si la redirection est gérée dans le logiciel ou le matériel. Utilisez la commande IOS **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 « Punt » représentent des demandes non traitées dans le matériel. Cette situation peut être causée par les erreurs suivantes :

- Affectation de hachage au lieu du masque
- Redirection sortante au lieu de trafic entrant
- Rediriger exclure dans
- Adresse MAC WAE inconnue
- Utilisation d'une adresse de bouclage pour la destination générique du tunnel GRE

Dans l'exemple suivant, les entrées policy-route indiquent que le routeur effectue une redirection matérielle complète :

```
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)
```

Le HIA (Here I Am) du WAE doit entrer la même interface que celle par laquelle le MAC WAE est connu. Nous vous recommandons d'utiliser une interface de bouclage et non une interface

connectée directement dans la liste des routeurs WAE.

Dépannage de WCCP sur les routeurs de la gamme ASR 1000

Les commandes de dépannage de WCCP sur les routeurs de la gamme Cisco ASR 1000 sont différentes des autres routeurs. Cette section présente les commandes que vous pouvez utiliser pour obtenir des informations WCCP sur l'ASR 1000.

Pour afficher les informations WCCP du processeur de routage, utilisez les commandes **show platform software wccp rp active** 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 montre des commandes supplémentaires que vous pouvez utiliser pour examiner les informations du processeur de transfert :

```
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 les statistiques des paquets redirigés pour chaque interface, utilisez la commande **show platform software wccp interface counters** 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 la commande **show platform software wccp web-cache counters** pour 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 des détails de bas niveau, utilisez les commandes suivantes :

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

Pour plus d'informations, reportez-vous au livre blanc [« Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers »](#)

Dépannage de WCCP sur le WAE

Commencez le dépannage du WAE à l'aide de la commande **show wccp services**. Vous voulez que les services 61 et 62 soient configurés comme suit :

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

Vérifiez ensuite l'état WCCP à l'aide de la commande **show wccp status**. Vous voulez voir que WCCP version 2 est activé et actif comme suit :

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

Examinez les informations de la batterie WCCP à l'aide de la commande **show wccp wide-area-engine**. Cette commande indique le nombre de WAE dans la batterie, leurs adresses IP, qui est le WAE principal, les routeurs qui peuvent voir les WAE, 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
```


Vous pouvez également utiliser la version récapitulative de la commande pour afficher des informations similaires, ainsi que des informations de flux de contournement :

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

Utilisez la commande **show wcp gre** pour afficher les statistiques de paquets 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 des deux premiers compteurs doit être incrémenté.

Les paquets transparents non GRE reçus incrémentent le compteur pour les paquets qui sont redirigés à l'aide de la méthode de redirection de couche 2 WCCP.

Les paquets non WCCP transparents non GRE ont reçu des incréments de compteur pour les paquets qui sont redirigés par une méthode d'interception non WCCP (telle que ACE ou PBR).

Le compteur Total des paquets acceptés indique les paquets qui sont acceptés pour l'optimisation car la détection automatique a trouvé un périphérique WAE homologue.

Les paquets GRE envoyés au compteur du routeur (pas de contournement) indiquent les paquets qui ont été traités à l'aide de la méthode de sortie de retour négociée WCCP.

Les paquets envoyés à un autre compteur WAE indiquent qu'une protection de flux se produit lorsqu'un autre WAE est ajouté au groupe de services et commence à gérer une affectation de groupement qui était auparavant gérée par un autre WAE.

Vérifiez que les méthodes de sortie utilisées sont les méthodes attendues à l'aide de la commande **show egress-méthodes** comme suit :

```
WAE674# show egress-methods
```

```
Intercept method : WCCP
```

```
TCP Promiscuous 61 :
```

```
WCCP negotiated return method : WCCP GRE
```

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

```
TCP Promiscuous 62 :
```

```
WCCP negotiated return method : WCCP GRE
```

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

Les discordances de la méthode de sortie peuvent se produire dans les conditions suivantes :

- La méthode de sortie de retour négociée est configurée, mais WCCP négocie la méthode de retour de couche 2 et seul le retour GRE est pris en charge par WAAS.
- La méthode de sortie GRE générique est configurée, mais la méthode d'interception est de couche 2 et seule WCCP GRE est prise en charge comme méthode d'interception lorsque la sortie GRE générique est configurée.

Dans l'un ou l'autre de ces cas, une alarme mineure est déclenchée et est effacée lorsque l'incompatibilité est résolue en modifiant la méthode de sortie ou la configuration WCCP. Tant que l'alarme n'est pas effacée, la méthode de sortie de transfert IP par défaut est utilisée.

L'exemple suivant montre le résultat de la commande lorsqu'il existe une non-correspondance :

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

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

WARNING: WCCP has negotiated WCCP L2 as the intercept method for
mismatch occurs <-----Warning if
           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

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

WARNING: WCCP has negotiated WCCP L2 as the intercept method for
mismatch occurs <-----Warning if
           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 Catalyst 6500 Sup720 ou Sup32, nous vous recommandons d'utiliser la méthode générique de sortie GRE, qui est traitée dans le matériel. En outre, nous vous recommandons d'utiliser un tunnel multipoint pour faciliter la configuration, au lieu d'un tunnel point à point pour chaque WAE. Pour plus d'informations sur la configuration du tunnel, reportez-vous à la section [Configuration d'une interface de tunnel GRE sur un routeur](#) dans le *Guide de configuration des services d'application de réseau étendu Cisco*.

Pour afficher les statistiques de tunnel GRE pour chaque routeur intercepteur, utilisez la commande **show statistics generic-gre** 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 fait de ne pas s'assurer que les paquets de sortie d'un WAE ne sont pas réinterceptés peut conduire à une boucle de redirection. Si un périphérique WAE détecte son propre ID retourné dans le champ Options TCP, une boucle de redirection s'est produite et donne le message syslog suivant :

```
%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.
```

Vous pouvez rechercher des instances de cette erreur dans le fichier syslog.txt à l'aide de la commande **find** comme suit :

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

Cette erreur apparaît également dans les statistiques de flux TFO disponibles dans la commande **show statistics filter** comme suit :

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

Si vous effectuez une redirection sortante sur le routeur, lorsque le trafic quitte le routeur, il sera redirigé vers le périphérique WAE, qui réacheminera le paquet vers le routeur, provoquant une boucle de routage. Si le périphérique WAE et les serveurs du data center se trouvent sur des VLAN différents et que le périphérique WAE et les clients se trouvent sur des VLAN différents, vous pouvez éviter une boucle de routage en utilisant la configuration de routeur suivante sur le VLAN WAE :

```
ip wccp redirect exclude in
```

Si le WAE partage le même VLAN avec ses clients ou serveurs adjacents, vous pouvez éviter les boucles de routage à l'aide de la méthode de retour négociée, ou le retour GRE générique pour les plates-formes où la redirection WCCP est effectuée dans le matériel. Lors de l'utilisation du retour GRE générique, le WAE utilise un tunnel GRE pour renvoyer le trafic au routeur.

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

NOTE: Les ID de service configurables WCCP et les fonctions de délai de détection des défaillances variables ont été introduits dans WAAS version 4.4.1. Cette section ne s'applique pas aux versions WAAS antérieures.

Tous les WAE d'une batterie WCCP doivent utiliser la même paire d'ID de service WCCP (la valeur par défaut est 61 et 62), et ces ID doivent correspondre à tous les routeurs qui prennent en charge la batterie. Un WAE avec des ID de service WCCP différents de ceux configurés sur les routeurs n'est pas autorisé à rejoindre la batterie et l'alarme existante « Router Unreachable » est déclenchée. De même, tous les WAE d'une batterie doivent utiliser la même valeur pour le délai de détection des défaillances. Un périphérique WAE déclenche une alarme si vous le configurez avec une valeur incorrecte.

Si vous voyez une alarme indiquant qu'un périphérique WAE ne peut pas joindre une batterie WCCP, vérifiez que les ID de service WCCP configurés sur le périphérique WAE et les routeurs de la batterie correspondent. Sur les WAE, utilisez la commande **show wccp wide-area-engine** pour vérifier les ID de service configurés. Sur les routeurs, vous pouvez utiliser la commande IOS

show ip wccp.

Pour vérifier si le périphérique WAE est connecté au routeur, utilisez les commandes **show wccp services detail** et **show wccp router detail**.

En outre, vous pouvez activer la sortie de débogage WCCP sur le WAE à l'aide des commandes **debug ip wccp event** ou **debug ip wccp packet**.

Si vous voyez une alarme mineure « Routeur inutilisable » pour un WAE, cela peut signifier que la valeur de délai de détection d'échec variable définie sur le WAE n'est pas prise en charge par le routeur. Utilisez la commande **show alarm minor detail** pour vérifier si la raison de l'alarme est « Incompatibilité de l'intervalle du minuteur 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 périphérique WAE, vérifiez le délai de détection d'échec configuré 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, vérifiez si la version IOS prend en charge le délai de détection des défaillances variables. Si oui, vous pouvez vérifier le paramètre configuré à l'aide de la commande **show ip wccp xx detail**, où xx est l'ID de service WCCP. Il existe trois résultats possibles :

- Le périphérique WAE utilise un délai de détection d'échec par défaut de 30 secondes et le routeur est configuré de la même manière ou ne prend pas en charge le délai d'attente variable : Le résultat du routeur n'indique aucun détail sur le paramètre de délai d'attente. Cette configuration fonctionne correctement.

- Le périphérique WAE utilise un délai d'attente de détection des défaillances autre que celui par défaut de 9 ou 15 secondes et le routeur ne prend pas en charge le délai d'attente variable : Le champ State indique « NOT Usable » et le WAE ne peut pas utiliser le routeur. Remplacez le délai d'attente de détection d'échec WAE par la valeur par défaut de 30 secondes à l'aide de la commande de configuration globale **wccp tcp fail-detection 30**.
- Le périphérique WAE utilise un délai d'attente de détection des défaillances autre que celui par défaut de 9 ou 15 secondes et le routeur prend en charge un délai d'attente variable : Le champ Client timeout indique le délai de détection d'échec configuré, qui correspond au périphérique WAE. Cette configuration fonctionne correctement.

Si la batterie de serveurs WCCP est instable en raison d'un battement de liaison, cela peut être dû au dépassement du délai de détection d'échec WCCP trop faible.