

WAAS - Dépannage d'AppNav

Chapitre : Dépannage d'AppNav

Cet article décrit comment dépanner un déploiement AppNav.

Co

Art

Pré

WA

Dé

Op

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Dé

Contenu

- [1 Dépannage AppNav](#)
 - [1.1 Interception In-Path \(Inline\)](#)
 - [1.2 Interception hors chemin \(WCCP\)](#)
 - [1.2.1 Configuration et vérification de l'interception WCCP sur le routeur](#)
 - [1.2.2 Additional Information](#)
 - [1.3 Dépannage de la connectivité réseau](#)
 - [1.3.1 Passage par un trafic spécifique](#)
 - [1.3.2 Désactivation d'un ANC en ligne](#)
 - [1.3.3 Désactivation d'un ANC hors chemin](#)
 - [1.4 Dépannage du cluster AppNav](#)
 - [1.4.1 Alarmes AppNav](#)
 - [1.4.2 Surveillance du gestionnaire central](#)
 - [1.4.3 Commandes CLI AppNav pour la surveillance de l'état du cluster et du périphérique](#)
 - [1.4.4 Commandes CLI AppNav pour la surveillance des statistiques de distribution de flux](#)

- [1.4.5 Commandes CLI AppNav pour le débogage des connexions](#)
- [1.4.6 Suivi des connexions](#)
- [1.4.7 Journalisation du débogage AppNav](#)
- [1.5 Capture de paquets AppNav](#)

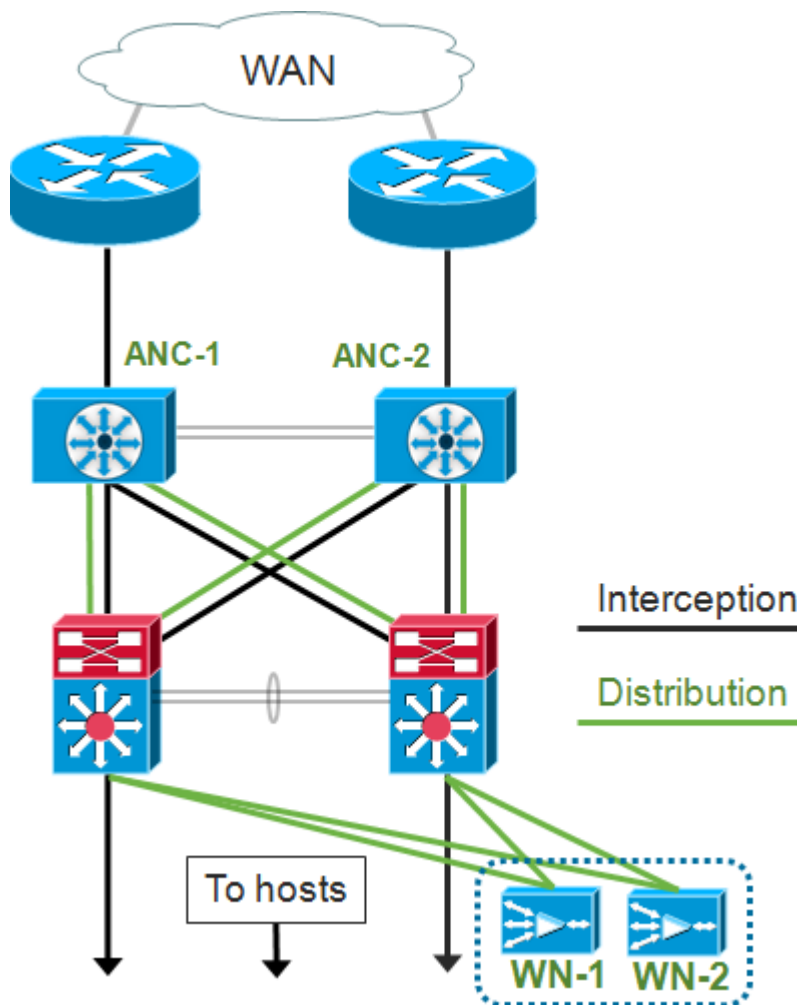
Dépannage AppNav

Cisco WAAS AppNav simplifie l'intégration réseau de l'optimisation WAN et réduit considérablement la dépendance vis-à-vis du commutateur ou du routeur d'interception en utilisant des contrôleurs AppNav (ANC) pour distribuer le trafic entre les noeuds WAAS (WN) afin de l'optimiser à l'aide d'un puissant mécanisme de classe et de politiques. Vous pouvez utiliser des noeuds WAAS (WN) pour optimiser le trafic en fonction des sites et/ou des applications. Cet article décrit comment dépanner AppNav.

NOTE: La fonctionnalité AppNav a été introduite dans WAAS version 5.0.1. Cette section ne s'applique pas aux versions WAAS antérieures.

Interception In-Path (Inline)

En mode inline, les ANC sont positionnés sur le chemin du trafic réseau où ils interceptent les paquets et les distribuent aux réseaux étendus.



La configuration d'interface d'un déploiement en ligne attribue les rôles d'interception et de distribution à des interfaces distinctes sur le module d'interface du contrôleur Cisco AppNav. Une interface de groupe de ponts est requise pour l'interception et se compose de deux interfaces physiques ou de canal de port ou une de chacune. L'interface de groupe de ponts ne manque pas

de capacité de câblage ; en d'autres termes, il ne s'ouvre pas et le trafic n'est pas ponté mécaniquement après une panne ou une perte d'énergie d'un périphérique. AppNav utilise le clustering pour fournir une haute disponibilité si le module d'interface du contrôleur AppNav, le chemin de liaison ou la connectivité au module d'interface du contrôleur AppNav est perdu ou s'il y a une panne d'alimentation.

Note: Les interfaces de pont ne bloquent pas les paquets BPDU (Bridge Protocol Data Unit) et, dans le cas d'interfaces redondantes qui créent des boucles, l'une des interfaces est bloquée par le protocole Spanning Tree.

Le dépannage de l'interception en ligne se compose des étapes suivantes :

- Vérifiez le positionnement en ligne correct de l'ANC en vérifiant la conception du réseau. Si nécessaire, utilisez des outils de base tels que ping et traceroute ou des outils ou applications de couche 7 pour confirmer que le chemin du trafic réseau est conforme aux attentes. Vérifiez le câblage physique de l'ANC.
- Vérifiez que l'ANC est configuré en mode d'interception en ligne.
- Vérifiez que l'interface de groupe de ponts est configurée correctement.

Les deux dernières étapes peuvent être effectuées dans Central Manager ou sur la ligne de commande, bien que Central Manager soit la méthode préférée et soit décrite en premier.

Dans le Gestionnaire central, choisissez **Périphériques** > *AppNavController*, puis choisissez **Configurer** > **Interception** > **Configuration de l'interception**. Vérifiez que la méthode d'interception est définie sur Inline.

Dans la même fenêtre, vérifiez qu'une interface de pont est configurée. Si une interface de pont est nécessaire, cliquez sur **Créer un pont** pour la créer. Vous pouvez affecter jusqu'à deux interfaces membres au groupe de pontage. Vous pouvez utiliser la calculatrice VLAN pour définir les entrées VLAN en fonction des opérations d'inclusion ou d'exclusion. Notez que l'interface de pont n'a pas d'adresse IP.

Utilisez le panneau Alarm ou la commande **show alarm** exec pour vérifier si des alarmes liées au pont sont déclenchées sur le périphérique. Une alarme bridge_down indique qu'une ou plusieurs interfaces membres du pont sont désactivées.

À partir de l'interface de ligne de commande, procédez comme suit pour configurer le fonctionnement en ligne :

1. Définissez la méthode d'interception en ligne :

```
wave# config
wave(config)# interception-method inline
```

2. Créez l'interface de groupe de ponts :

```
wave(config)# bridge 1 protocol interception
```

3. (Facultatif) Spécifiez la liste des VLAN à intercepter, le cas échéant :

```
wave(config)# bridge 1 intercept vlan-id all
```

4. Ajoutez deux interfaces logiques/physiques à l'interface de groupe de ponts :

```
wave(config)# interface GigabitEthernet 1/0
wave(config-if)# bridge-group 1
wave(config-if)# exit
wave(config)# interface GigabitEthernet 1/1
wave(config-if)# bridge-group 1
wave(config-if)# exit
```

Vous pouvez utiliser la commande **show bridge exec** pour vérifier l'état de fonctionnement de l'interface de pont et voir les statistiques du pont.

```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
  GigabitEthernet 1/0
  GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
  intercept vlan-id all                                     <<< VLANs to intercept

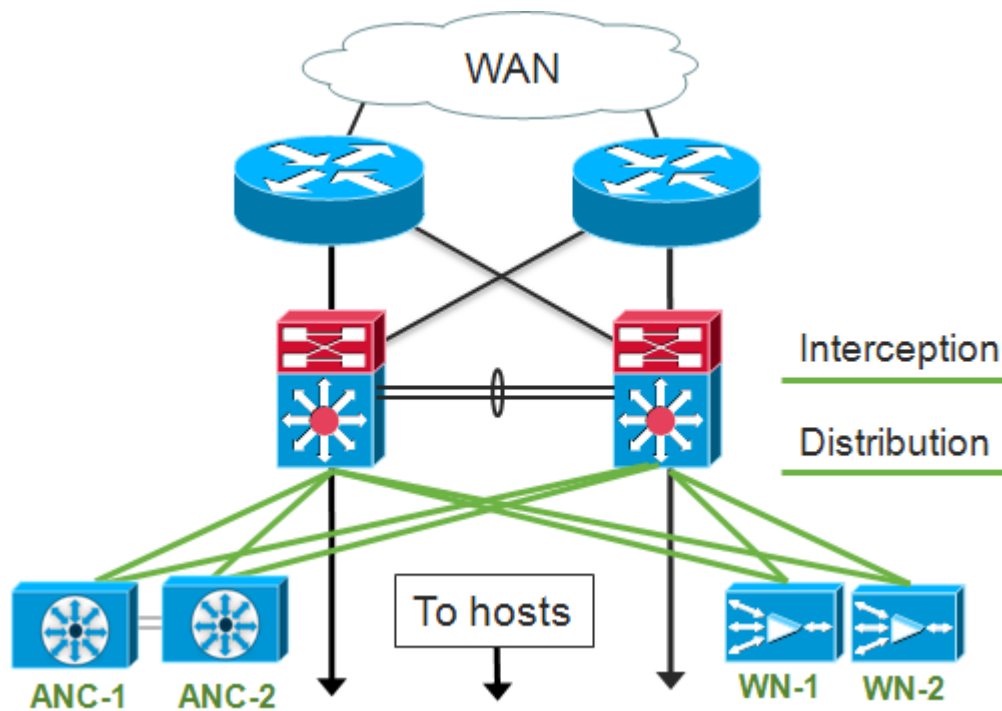
Interception Statistics:
                                GigabitEthernet 1/0      GigabitEthernet 1/1
Operation State                  :   Down              Down(lsp)          <<< Down due to LSP
Input Packets Forwarded/Bridged  :   16188          7845
Input Packets Redirected         :    5068           0
Input Packets Punted            :    1208           605
Input Packets Dropped           :     0              0
Output Packets Forwarded/Bridged :    7843          21256
Output Packets Injected         :    301            301
Output Packets Dropped          :     2              0
```

Dans l'exemple ci-dessus, l'interface Gig 1/0 est désactivée et l'interface Gig 1/1 est également désactivée en raison de la propagation à état de liens (LSP). Vous pouvez également voir Down(flow sync), ce qui signifie que l'ANC joint un cluster et synchronise les informations de flux avec d'autres ANC du cluster. Elle permet de maintenir le chemin d'interception (interface de pont) fermé pendant environ deux minutes jusqu'à ce que tous les ANC soient synchronisés afin que les flux existants puissent être correctement distribués.

La partie inférieure du résultat affiche les statistiques de trafic pour les interfaces membres.

Interception hors chemin (WCCP)

En mode WCCP, les routeurs WCCP sont placés dans le chemin du trafic réseau où ils interceptent les paquets et les redirigent vers des ANC, qui sont situés hors chemin. Comme AppNav gère le traitement d'interception, la distribution intelligente du flux et la prise en compte de la charge entre les accélérateurs WAAS, la configuration WCCP sur les routeurs est considérablement simplifiée.



Dans la configuration d'interface pour un déploiement hors chemin, les rôles d'interception et de distribution peuvent partager les mêmes interfaces sur le module d'interface du contrôleur Cisco AppNav, mais ce n'est pas nécessaire.

Le dépannage de l'interception hors chemin se compose des étapes suivantes :

- Vérifiez l'emplacement correct des routeurs WCCP pour vous assurer qu'ils se trouvent sur le chemin du trafic allant aux hôtes optimisés. Vous pouvez utiliser les commandes **show run** ou **show wccp** pour vérifier que ce sont les mêmes routeurs qui sont configurés pour WCCP. Si nécessaire, utilisez des outils de base tels que ping et traceroute, ou des outils ou applications de couche 7 pour confirmer que tout le trafic nécessitant une optimisation passe par les routeurs WCCP.
- Vérifiez la configuration WCCP sur les ANC WAAS, à l'aide du Gestionnaire central (préférée) ou de l'interface de ligne de commande.
- Vérifiez la configuration WCCP sur les routeurs de redirection à l'aide de l'interface de ligne de commande du routeur.

Pour vérifier la configuration WCCP sur les ANC, dans Central Manager, sélectionnez **Devices > AppNavController**, puis **Configure > Interception > Interception Configuration**.

- Vérifiez que la méthode d'interception est définie sur WCCP.
- Vérifiez que la case Activer le service WCCP est cochée.
- Vérifiez que la case Utiliser la passerelle par défaut comme routeur WCCP est cochée ou que les adresses IP du routeur WCCP sont répertoriées dans le champ Routeur WCCP.
- Vérifiez que les autres paramètres tels que le masque d'équilibrage de charge et la méthode de redirection sont configurés correctement pour votre déploiement.

Recherchez les alarmes WCCP associées sur les ANC qui font partie de la batterie WCCP du routeur. Dans le Gestionnaire central, cliquez sur le panneau Alarmes en bas de l'écran ou utilisez la commande **show alarm** sur chaque périphérique pour afficher les alarmes. Corrigez toutes les conditions d'alarme en modifiant la configuration de l'ANC ou du routeur, si nécessaire.

À partir de l'interface de ligne de commande, procédez comme suit pour configurer le

fonctionnement de WCCP :

1. Définissez la méthode d'interception sur wccp.

```
wave# config  
wave(config)# interception-method wccp
```

2. Configurez la liste des routeurs WCCP, qui contient les adresses IP des routeurs participant à la batterie de WCCP.

```
wave(config)# wccp router-list 1 10.10.10.21 10.10.10.22
```

3. Configurez l'ID de service WCCP. Un seul ID de service est préféré pour AppNav, bien que deux ID de service soient pris en charge.

```
wave(config)# wccp tcp-promiscuous 61
```

4. Associez la liste de routeurs configurée au service WCCP.

```
wave(config-wccp-service)# router-list-num 1
```

5. Configurez la méthode d'affectation WCCP (seule la méthode de masque est prise en charge sur un ANC). Si vous ne spécifiez pas les options dst-ip-mask ou src-ip-mask, le masque IP source par défaut est f et le masque IP de destination est 0.

```
wave(config-wccp-service)# assignment-method mask
```

6. Configurez la méthode de redirection WCCP (les méthodes de sortie et de retour sont définies automatiquement pour correspondre à la méthode de redirection et ne sont pas configurables pour un ANC). Vous pouvez choisir L2 (valeur par défaut) ou GRE. La couche 2 nécessite que l'ANC dispose d'une connexion de couche 2 avec le routeur et que le routeur est également configuré pour la redirection de couche 2.

```
wave(config-wccp-service)# redirect-method gre
```

7. Activez le service WCCP.

```
wave(config-wccp-service)# enable
```

Vérifiez l'interception WCCP sur chaque ANC à l'aide de la commande **show running-config**. Les deux exemples ci-dessous montrent la sortie de configuration en cours pour la redirection de couche 2 et la redirection de GRE.

Show running-config wccp (pour la redirection L2) :

```
wave# sh run wccp  
wccp router-list 1 10.10.10.21 10.10.10.22
```

```
wccp tcp-promiscuous service-pair 61
  router-list-num 1
  enable
running config
  exit
```

<<< L2 redirect is default so is not shown in

Show running-config wccp (pour GRE) :

```
wave# sh run wccp
wccp router-list 1 10.10.10.21 10.10.10.22
wccp tcp-promiscuous service-pair 61
  router-list-num 1
  redirect-method gre
  enable
  exit
```

<<< GRE redirect method is configured

Vérifiez l'état WCCP sur chaque ANC à l'aide de la commande **show wccp status**.

```
wave# show wccp routers
WCCP Interception :
Configured State : Enabled
Operational State : Enabled
  Services Enabled on this WAE:
    TCP Promiscuous 61
```

<<< Shows Disabled if WCCP is not configured
<<< Shows Disabled if WCCP is not enabled
<<< Shows NONE if no service groups are configured

Vérifiez les routeurs qui ont répondu aux messages keep-alive dans la batterie de serveurs WCCP à l'aide de la commande **show wccp routers**.

```
wave# show wccp routers
Router Information for Service Id: 61

  Routers Seeing this Wide Area Engine(2)
  Router Id      Sent To
  192.168.1.1    10.10.10.21
  192.168.1.2    10.10.10.22
  Routers not Seeing this Wide Area Engine
  -NONE-
  Routers Notified of from other WAE's
  -NONE-
```

<<< List of routers seen by this ANC
<<< List of routers not seen by this ANC
<<< List of routers notified of but not configured in router list

Vérifiez que chaque ANC affiche les autres ANC de la batterie WCCP et les routeurs accessibles par chacun d'entre eux à l'aide de la commande **show wccp clients**.

```
wave# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2
  IP address = 10.10.10.31  Lead WAE = NO  Weight = 0
```

<<< Number of ANCs in the farm
<<< Entry for each ANC in the farm

```
  Routers seeing this Wide Area Engine(2)
  192.168.1.1
  192.168.1.2
```

<<< List of routers seeing this ANC

```

IP address = 10.10.10.32   Lead WAE = YES   Weight = 0   <<< YES indicates ANC is serving
as the lead
Routers seeing this Wide Area Engine(2)
    192.168.1.1           <<< List of routers seeing this
ANC
    192.168.1.2

```

Vérifiez que les paquets sont reçus par chaque ANC à partir des routeurs de la batterie à l'aide de la commande **show statistics wccp**. Les statistiques du trafic reçu, transmis et envoyé à chaque routeur sont affichées. Les statistiques cumulées de tous les routeurs de la batterie sont affichées en bas. Une commande similaire est **show wccp statistics**. Notez que « OE » fait référence aux périphériques ANC ici.

```
wave# sh statistics wccp
```

```

WCCP Stats for Router      : 10.10.10.21
Packets Received from Router : 1101954
Bytes Received from Router   : 103682392
Packets Transmitted to Router : 1751072
Bytes Transmitted to Router   : 2518114618
Pass-thru Packets sent to Router : 0
Pass-thru Bytes sent to Router : 0
Redirect Packets sent to OE   : 1101954
Redirect Bytes sent to OE     : 103682392

```

```

WCCP Stats for Router      : 10.10.10.22
Packets Received from Router : 75264
Bytes Received from Router   : 10732204
Packets Transmitted to Router : 405193
Bytes Transmitted to Router   : 597227459
Pass-thru Packets sent to Router : 0
Pass-thru Bytes sent to Router : 0
Redirect Packets sent to OE   : 75264
Redirect Bytes sent to OE     : 10732204

```

```
Cummulative WCCP Stats:
```

```

Total Packets Received from all Routers : 1177218
Total Bytes Received from all Routers : 114414596
Total Packets Transmitted to all Routers : 2156265
Total Bytes Transmitted to all Routers : 3115342077
Total Pass-thru Packets sent to all Routers : 0
Total Pass-thru Bytes sent to all Routers : 0
Total Redirect Packets sent to OE : 1177218
Total Redirect Bytes sent to OE : 114414596

```

Configuration et vérification de l'interception WCCP sur le routeur

Pour configurer l'interception WCCP sur chaque routeur de la batterie WCCP, procédez comme suit.

1. Configurez le service WCCP sur le routeur à l'aide de la commande **ip wccp router**.

```

Core-Router1 configure terminal
Core-Router1(config)# ip wccp 61

```

2. Configurez l'interception WCCP sur les interfaces LAN et WAN du routeur. Vous pouvez configurer le même ID de service sur les deux interfaces si vous utilisez un seul ID de service sur les ANC.


```
Core-Router1(config)# interface GigabitEthernet0/0
Core-Router1(config-subif)# ip address 10.20.1.1 255.255.255.0
Core-Router1(config-subif)# ip wccp 61 redirect in
Core-Router1(config-subif)# ip router isis inline_wccp_pod
Core-Router1(config-subif)# exit
```

```
Core-Router1(config)# interface GigabitEthernet0/1
Core-Router1(config-subif)# ip address 10.19.1.1 255.255.255.0
Core-Router1(config-subif)# ip wccp 61 redirect in
Core-Router1(config-subif)# ip router isis inline_wccp_pod
Core-Router1(config-subif)# glbp 701 ip 10.19.1.254
Core-Router1(config-subif)# duplex auto
Core-Router1(config-subif)# speed auto
Core-Router1(config-subif)# media-type rj45
Core-Router1(config-subif)# exit
```

3. (Facultatif) Configurez une interface de tunnel si vous utilisez une sortie GRE générique (uniquement si vous avez choisi GRE pour la méthode de redirection WCCP ANC).

```
Core-Router1(config)# interface Tunnel1
Core-Router1(config-subif)# ip address 192.168.1.1 255.255.255.0
Core-Router1(config-subif)# no ip redirects
Core-Router1(config-subif)# tunnel source GigabitEthernet0/0.3702
Core-Router1(config-subif)# tunnel mode gre multipoint
```

Vérifiez la configuration WCCP sur chaque routeur de la batterie à l'aide de la commande **show wccp**.

```
Core-Router1 sh ip wccp 61 detail
WCCP Client information:
  WCCP Client ID:      10.10.10.31          <<< ANC IP address
  Protocol Version:    2.00
  State:               Usable
  Redirection:         GRE                  <<< Negotiated WCCP parameters
  Packet Return:       GRE                  <<<
  Assignment:          MASK                 <<<
  Connect Time:        00:31:27
  Redirected Packets:
    Process:           0
    CEF:               0
  GRE Bypassed Packets:
    Process:           0
    CEF:               0
  Mask Allotment:      16 of 16 (100.00%)
  Assigned masks/values: 1/16

  Mask  SrcAddr  DstAddr  SrcPort DstPort
  ----  -
  0000: 0x0000000F 0x00000000 0x0000 0x0000          <<< Configured mask

  Value SrcAddr  DstAddr  SrcPort DstPort
  ----  -
  0000: 0x00000000 0x00000000 0x0000 0x0000          <<< Mask assignments
  0001: 0x00000001 0x00000000 0x0000 0x0000
  0002: 0x00000002 0x00000000 0x0000 0x0000
  0003: 0x00000003 0x00000000 0x0000 0x0000
  0004: 0x00000004 0x00000000 0x0000 0x0000
```

```
0005: 0x00000005 0x00000000 0x0000 0x0000
0006: 0x00000006 0x00000000 0x0000 0x0000
0007: 0x00000007 0x00000000 0x0000 0x0000
0008: 0x00000008 0x00000000 0x0000 0x0000
0009: 0x00000009 0x00000000 0x0000 0x0000
0010: 0x0000000A 0x00000000 0x0000 0x0000
0011: 0x0000000B 0x00000000 0x0000 0x0000
0012: 0x0000000C 0x00000000 0x0000 0x0000
0013: 0x0000000D 0x00000000 0x0000 0x0000
0014: 0x0000000E 0x00000000 0x0000 0x0000
0015: 0x0000000F 0x00000000 0x0000 0x0000
```

Additional Information

Pour plus d'informations, reportez-vous aux documents suivants :

- [Intégration réseau WCCP avec Cisco Catalyst 6500 : Recommandations relatives aux meilleures pratiques pour les déploiements réussis](#)
- [Redirection du protocole de communication du cache Web des services d'applications de réseau étendu Cisco : Prise en charge de la plate-forme de routeur Cisco](#)
- [Configuration des fonctionnalités WCCP avancées sur les routeurs, à partir du *Guide de configuration des services d'application de réseau étendu Cisco*](#)
- [Configuration de WCCP sur des WAE, à partir du *Guide de configuration des services d'application de réseau étendu Cisco*](#)

Dépannage de la connectivité réseau

Lors du dépannage de WAAS, il peut être utile de déterminer le comportement du réseau avec WAAS désactivé. Cela est utile lorsque le trafic ne parvient pas seulement à être optimisé, mais qu'il ne parvient pas du tout à passer. Dans ces cas, il peut s'avérer que le problème n'est pas lié à WAAS. Même dans les cas où le trafic passe, cette technique peut aider à déterminer quels périphériques WAAS nécessitent un dépannage.

Avant de tester la connectivité de couche 3, vérifiez que le module d'interface du contrôleur AppNav est connecté aux ports de commutateur appropriés. Si le commutateur connecté prend en charge et que le protocole CDP (Cisco Discovery Protocol) est activé, exécutez la commande **show cdp neighbors detail** pour vérifier la connectivité correcte au commutateur réseau.

La désactivation de WAAS peut ne pas être applicable dans tous les cas. Si un certain trafic est optimisé et que d'autres ne le sont pas, il peut être inacceptable de désactiver WAAS, perturbant ainsi le trafic qui est optimisé avec succès. Dans ce cas, la liste de contrôle d'accès d'interception ou la stratégie AppNav peuvent être utilisées pour traverser le type de trafic spécifique qui rencontre des problèmes. Pour plus de détails, consultez la section [Passage par un trafic spécifique](#).

Pour désactiver WAAS, différentes étapes sont effectuées pour le mode en ligne plutôt que pour le mode hors chemin :

- Le mode en ligne nécessite de placer le pont d'interception à l'état de passage. Pour plus d'informations, reportez-vous à la section [Désactivation d'un ANC en ligne](#).
- Le mode hors chemin nécessite la désactivation du protocole WCCP. Pour plus d'informations, reportez-vous à la section [Désactivation d'un ANC hors chemin](#).

Dans les environnements AppNav, seuls les ANC doivent être désactivés. Il n'est pas nécessaire

de désactiver les noms de réseau, car ils ne participent pas à l'interception.

Une fois le WAAS désactivé, vérifiez la connectivité réseau à l'aide de méthodes standard.

- Vérifiez la connectivité de couche 3 à l'aide d'outils tels que ping et traceroute.
- Vérifier le comportement des applications pour déterminer la connectivité de couche supérieure
- Si le réseau rencontre les mêmes problèmes de connectivité qu'avec WAAS activé, le problème n'est probablement pas lié à WAAS.
- Si le réseau fonctionne correctement avec WAAS désactivé, mais que des problèmes de connexion avec WAAS activé sont rencontrés, il y a probablement un ou plusieurs périphériques WAAS qui nécessitent une attention particulière. L'étape suivante consiste à isoler le problème sur des périphériques WAAS spécifiques.
- Si la connectivité avec et sans WAAS est activée sur le réseau, mais qu'il n'y a pas d'optimisation, il y a probablement un ou plusieurs périphériques WAAS nécessitant une attention particulière. L'étape suivante consiste à isoler le problème sur des périphériques WAAS spécifiques.

Pour vérifier le comportement du réseau avec WAAS activé, procédez comme suit :

1. Réactivez la fonctionnalité WAAS sur les ANC WAAS et, le cas échéant, sur les routeurs WCCP.
2. Si vous avez déterminé qu'il existe un problème lié à WAAS, activez chaque cluster AppNav et/ou ANC individuellement pour l'isoler comme cause potentielle du problème observé.
3. Lorsque chaque ANC est activé, effectuez les mêmes tests de connectivité réseau de base que lors des étapes précédentes et notez si ce ANC spécifique semble fonctionner correctement. Ne vous souciez pas des noms individuels à ce stade. L'objectif à ce stade est de déterminer quels clusters et quels ANC spécifiques subissent un comportement souhaité ou non souhaité.
4. Lorsque chaque ANC est activé et testé, désactivez-le à nouveau afin que le suivant puisse être activé. L'activation et le test de chaque ANC vous permettent de déterminer ceux qui nécessitent un dépannage supplémentaire.

Cette technique de dépannage est la plus applicable dans les situations où la configuration WAAS semble non seulement échouer à optimiser, mais également causer des problèmes avec la connectivité réseau normale.

Passage par un trafic spécifique

Vous pouvez passer par un trafic spécifique soit en utilisant une liste de contrôle d'accès d'interception, soit en configurant la stratégie AppNav pour passer.

- Créez une liste de contrôle d'accès refusant le trafic spécifique à passer et autorisant tout le reste. Dans cet exemple, nous voulons passer par le trafic HTTP (dest port 80). Définissez la liste d'accès d'interception ANC sur la liste de contrôle d'accès définie. Les connexions destinées au port 80 sont transmises. Vous pouvez utiliser la commande **show statistics pass-through type appnav** pour vérifier que le pass-through se produit en vérifiant que les compteurs de la liste de contrôle d'accès Intercept PT sont en train d'augmenter.

```
anc# config
anc(config)# ip access-list extended pt_http
anc(config-ext-nacl)# deny tcp any any eq 80
anc(config-ext-nacl)# permit ip any any
anc(config-ext-nacl)# exit
anc(config)# interception appnav-controller access-list pt_http
```

- Configurez la stratégie ANC pour passer par le trafic correspondant à des classes spécifiques.

```
class-map type appnav HTTP
  match tcp dest port 80

policy-map type appnav my_policy
.
.
.
class HTTP
  pass-through
```

Désactivation d'un ANC en ligne

Il existe plusieurs façons de désactiver une ANC en ligne en la plaçant dans l'état de transmission :

- Définissez la liste VLAN du pont d'interception sur none. Dans Central Manager, sélectionnez un périphérique ANC, puis choisissez **Configure > Interception > Interception Configuration**. Sélectionnez l'interface du pont et cliquez sur l'icône **Modifier** la barre des tâches. Définissez le champ VLAN sur la valeur « none ».
- Désactivez le contexte de service contenant l'ANC. Dans le Gestionnaire central, sélectionnez un cluster, puis cliquez sur l'onglet Contrôleurs AppNav, sélectionnez un ANC, puis cliquez sur l'icône **Désactiver** la barre des tâches.
- Appliquez une liste de contrôle d'accès d'interception avec les critères « deny ALL ». Cette méthode est préférée. (Les deux premières méthodes perturbent les connexions optimisées existantes.) Définissez une liste de contrôle d'accès avec les critères de refus ALL. Dans Central Manager, choisissez un périphérique ANC, puis choisissez **Configure > Interception > Interception Access List**, puis choisissez la liste d'accès deny ALL dans la liste déroulante AppNav Controller Interception Access List.

Pour désactiver l'interception à l'aide d'une liste de contrôle d'accès à partir de l'interface de ligne de commande, utilisez les commandes suivantes :

```
anc# config
anc(config)# ip access-list standard deny
anc(config-std-nacl)# deny any
anc(config-std-nacl)# exit
anc(config)# interception appnav-controller access-list deny
```

Placement d'un ANC en état de transmission :

- Désactive l'interception WAAS, et non les interfaces.
- Désactive l'optimisation WAAS.
- Fait passer tout le trafic sans incidence.

Désactivation d'un ANC hors chemin

Pour désactiver un ANC qui s'exécute en mode hors chemin, désactivez le protocole WCCP pour l'ANC. Vous pouvez effectuer cette action sur l'ANC ou sur le routeur de redirection ou sur les deux. Sur l'ANC, vous pouvez désactiver ou supprimer les services WCCP, ou supprimer la méthode d'interception ou la remplacer par une autre méthode.

Pour désactiver l'interception WCCP, dans Central Manager, sélectionnez un périphérique ANC, puis choisissez **Configure > Interception > Interception Configuration**. Désactivez la case à cocher Activer le service WCCP ou cliquez sur l'icône Supprimer les paramètres de la barre des tâches pour supprimer complètement les paramètres d'interception WCCP (ils seront perdus).

Pour désactiver l'interception WCCP à partir de l'interface de ligne de commande, utilisez les commandes suivantes :

```
anc# config
anc(config)# wccp tcp-promiscuous service-pair 61
anc(config-wccp-service)# no enable
```

Dans certains cas, plusieurs ANC peuvent recevoir le trafic redirigé du même routeur. Pour plus de commodité, vous pouvez choisir de désactiver WCCP sur le routeur, plutôt que sur les ANC. L'avantage est que vous pouvez supprimer plusieurs ANC d'une batterie WCCP en une seule étape. L'inconvénient est que vous ne pouvez pas le faire à partir du Gestionnaire central WAAS.

Pour désactiver WCCP au niveau du routeur, utilisez la syntaxe suivante :

```
RTR1(config)# no ip wccp 61
RTR1(config)# no ip wccp 62 <<< Only needed if you are using two WCCP service IDs
```

Pour réactiver WCCP au niveau du routeur, utilisez la syntaxe suivante :

```
RTR1(config)# ip wccp 61
RTR1(config)# ip wccp 62 <<< Only needed if you are using two WCCP service IDs
```

Sur chaque routeur WCCP, vérifiez que les ANC que vous avez choisi de désactiver ne s'affichent pas en tant que clients WCCP. Le résultat suivant s'affiche lorsque les services WCCP ont été supprimés sur le routeur.

```
RTR1# show ip wccp 61
The WCCP service specified is not active.
```

Dépannage du cluster AppNav

Pour dépanner un cluster AppNav, vous pouvez utiliser les outils suivants :

- [Alarmes AppNav](#)
- [Surveillance du gestionnaire central](#)

- [Commandes CLI AppNav pour la surveillance de l'état du cluster et du périphérique](#)
- [Commandes CLI AppNav pour la surveillance des statistiques de distribution de flux](#)
- [Suivi des connexions](#)
- [Journalisation du débogage AppNav](#)

Alarmes AppNav

Le Gestionnaire d'appartenance au cluster (CMM) émet les alarmes suivantes en raison de conditions d'erreur :

- Cluster dégradé (critique) : visibilité partielle entre les ANC. ANC passera par de nouvelles connexions.
- Échec de la convergence (critique) : l'ANC n'a pas pu converger vers une vue stable des ANC et des WAN. ANC passera par de nouvelles connexions.
- Échec de la jointure ANC (critique) : ANC n'a pas pu rejoindre un cluster existant en raison d'une dégradation potentielle du cluster avec l'ANC dans celui-ci.
- Batterie mixte ANC (mineure) : les ANC du cluster exécutent des versions différentes mais compatibles du protocole de cluster.
- ANC Unreachable (Major) : un ANC configuré est inaccessible.
- WN Unreachable (Major) : un WN configuré est inaccessible. Ce nom n'est pas utilisé pour la redirection du trafic.
- WN Excluded (Major) : un WN configuré est accessible mais exclu car un ou plusieurs autres ANC ne le voient pas. Ce nom n'est pas utilisé pour la redirection du trafic (nouvelles connexions).

Vous pouvez voir des alarmes dans le panneau d'alarmes du Gestionnaire central ou à l'aide de la commande EXEC **show alarms** sur un périphérique.

Note: Le CMM est un composant AppNav interne qui gère le regroupement des ANC et des noms d'utilisateur dans un cluster AppNav associé à un contexte de service.

Surveillance du gestionnaire central

Vous pouvez utiliser le Gestionnaire central pour vérifier, surveiller et dépanner les clusters AppNav. Le Gestionnaire central a une vue globale de tous les périphériques WAAS enregistrés sur votre réseau et peut vous aider rapidement à localiser la plupart des problèmes AppNav.

Dans le menu Central Manager, sélectionnez **AppNav Clusters > nom de cluster**. La fenêtre d'accueil du cluster affiche la topologie du cluster (y compris les routeurs WCCP et de passerelle), l'état global du cluster, l'état du périphérique, l'état du groupe de périphériques et l'état de la liaison.

Tout d'abord, vérifiez que l'état global du cluster est opérationnel.

Notez que les icônes ANC et WN de ce schéma ont le même nom de périphérique car elles résident sur le même périphérique. Sur un ANC qui optimise également le trafic en tant que WN, ces deux fonctions sont affichées sous forme d'icônes distinctes sur le schéma de topologie.

Un indicateur d'avertissement en triangle orange est affiché sur tout périphérique pour lequel le Gestionnaire central ne dispose peut-être pas d'informations actuelles, car le périphérique n'a pas répondu au cours des 30 dernières secondes (le périphérique peut être hors connexion ou inaccessible).

Vous pouvez obtenir une vue détaillée de l'état à 360 degrés de tout périphérique ANC ou WN en plaçant le curseur sur l'icône du périphérique. Le premier onglet affiche des alarmes sur le périphérique. Vous devez résoudre toutes les alarmes qui empêchent le bon fonctionnement du cluster.

Cliquez sur l'onglet Interception pour vérifier la méthode d'interception de périphérique sur chaque ANC.

Si l'interception est désactivée, l'état s'affiche comme suit :

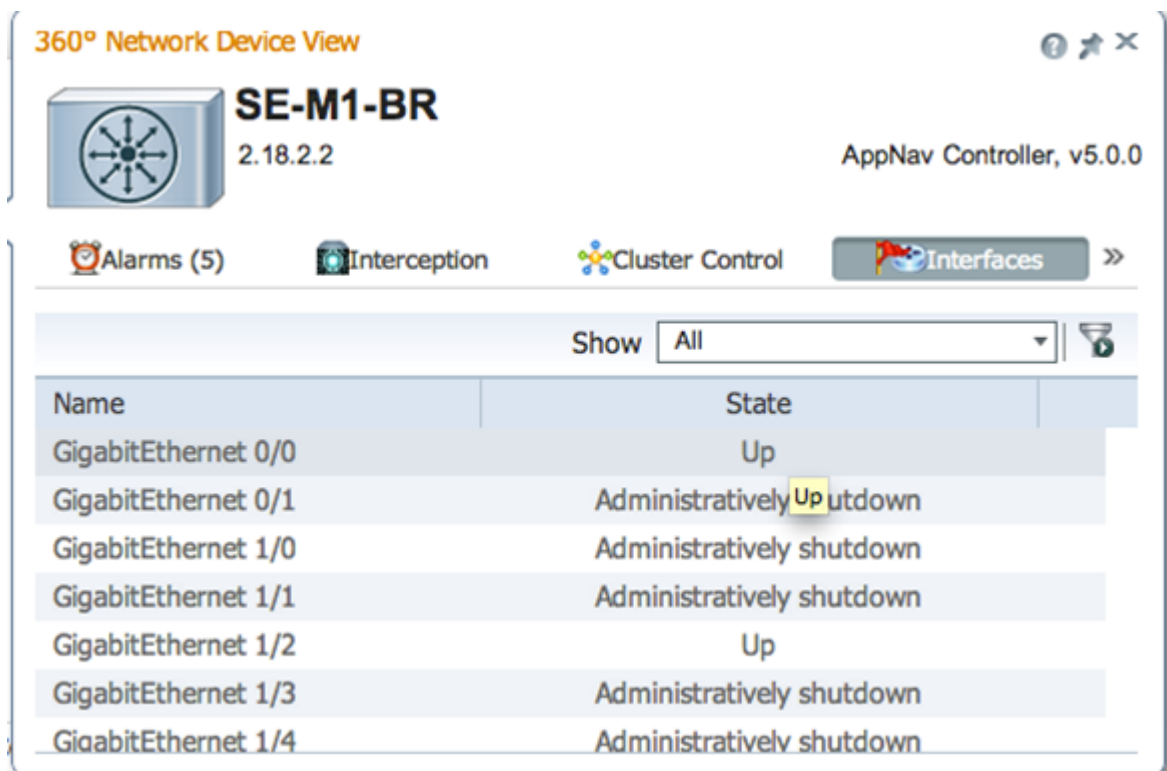
Cliquez sur l'onglet Cluster Control pour afficher l'adresse IP et l'état de chaque périphérique du cluster que ce contrôleur ANC peut voir. Chaque ANC du cluster doit avoir la même liste de périphériques. Si ce n'est pas le cas, cela indique un problème de configuration ou de réseau.

Si tous les ANC ne peuvent pas se voir, le cluster n'est pas opérationnel et tout le trafic passe par en raison de l'incapacité du cluster à synchroniser les flux.

Si tous les ANC sont connectés mais ont des vues différentes des WN, le cluster est dans un état dégradé. Le trafic est toujours distribué, mais uniquement aux noms de réseau visibles par tous les ANC.

Tous les noms de réseau non vus par tous les ANC sont exclus.

Cliquez sur l'onglet Interfaces pour vérifier l'état des interfaces physiques et logiques sur l'ANC.



360° Network Device View

SE-M1-BR
2.18.2.2

AppNav Controller, v5.0.0

Alarms (5) Interception Cluster Control Interfaces >>

Show All

Name	State
GigabitEthernet 0/0	Up
GigabitEthernet 0/1	Administratively Up shutdown
GigabitEthernet 1/0	Administratively shutdown
GigabitEthernet 1/1	Administratively shutdown
GigabitEthernet 1/2	Up
GigabitEthernet 1/3	Administratively shutdown
GigabitEthernet 1/4	Administratively shutdown

Examinez la vue à 360 degrés de chaque nom de réseau du cluster et vérifiez l'état vert de tous les accélérateurs dans l'onglet Optimisation. L'état jaune d'un accélérateur signifie que l'accélérateur est en cours d'exécution mais qu'il ne peut pas entretenir de nouvelles connexions, par exemple parce qu'il est surchargé ou parce que sa licence a été supprimée. Un état rouge indique que l'accélérateur ne fonctionne pas. Si des accélérateurs sont jaunes ou rouges, vous

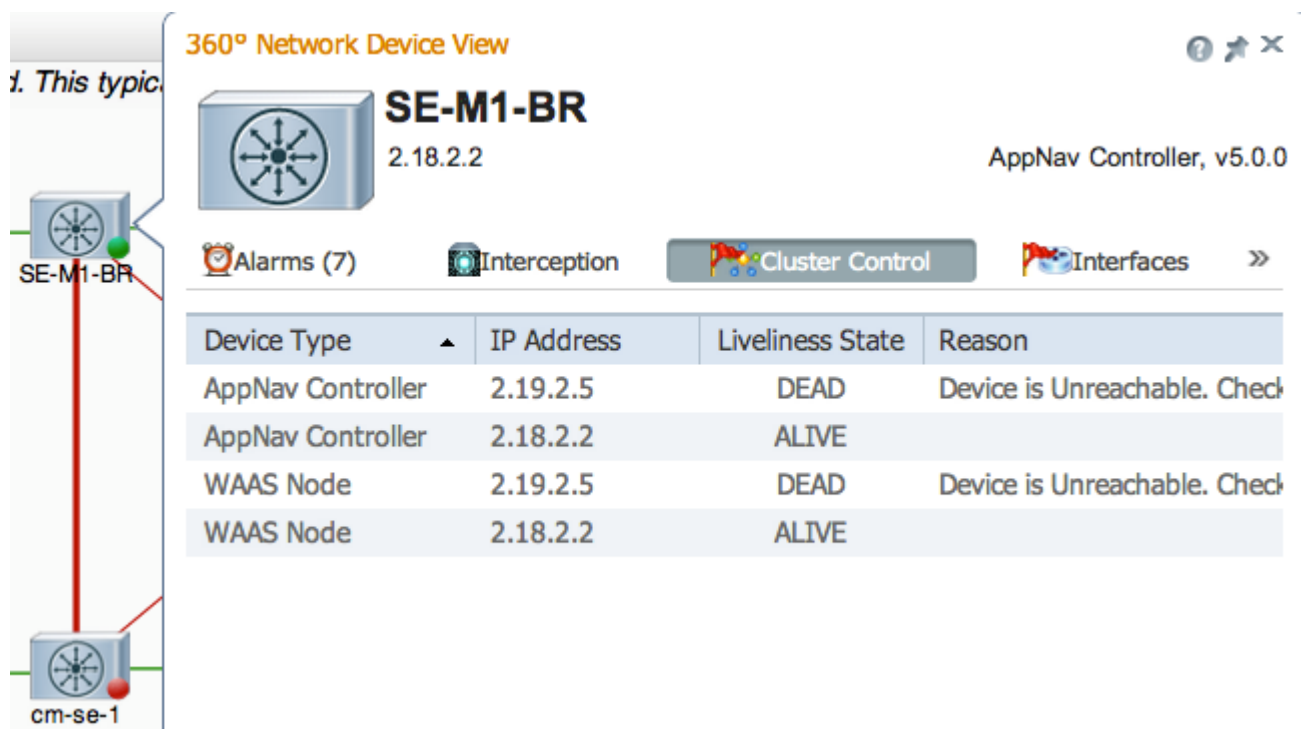
devez les dépanner séparément. Si la licence Enterprise est manquante, la description indique que la licence System a été révoquée. Installez la licence Enterprise dans la page **Admin > History > License Management** device.

Un cluster divisé résulte de problèmes de connectivité entre les ANC du cluster. Si le Gestionnaire central peut communiquer avec tous les ANC, il peut détecter un cluster partagé, mais s'il ne peut pas communiquer avec certains ANC, il ne peut pas détecter le fractionnement. L'alarme d'« état de gestion hors connexion » est déclenchée si le Gestionnaire central perd la connectivité avec n'importe quel périphérique et que le périphérique est affiché hors connexion dans le Gestionnaire central.

Il est préférable de séparer les interfaces de gestion des interfaces de données pour maintenir la connectivité de gestion même en cas de panne d'une liaison de données.

Dans un cluster partagé, chaque sous-cluster des ANC distribue indépendamment les flux aux WNG qu'il peut voir, mais comme les flux entre les sous-clusters ne sont pas coordonnés, il peut provoquer des connexions de réinitialisation et la performance globale du cluster est dégradée.

Vérifiez l'onglet Cluster Control de chaque ANC pour voir si un ou plusieurs ANC sont inaccessibles. L'alarme « Le contrôleur de service est inaccessible » est déclenchée si deux ANC qui pouvaient autrefois communiquer entre eux perdent la connectivité entre eux, mais cette situation n'est pas la seule cause d'un cluster partagé. Il est donc préférable de vérifier l'onglet Contrôle de cluster de chaque ANC.



Device Type	IP Address	Liveliness State	Reason
AppNav Controller	2.19.2.5	DEAD	Device is Unreachable. Check
AppNav Controller	2.18.2.2	ALIVE	
WAAS Node	2.19.2.5	DEAD	Device is Unreachable. Check
WAAS Node	2.18.2.2	ALIVE	

Si un ANC a un voyant d'état gris, il peut être désactivé. Vérifiez que tous les ANC sont activés en cliquant sur l'onglet Contrôleurs AppNav sous le diagramme de topologie. Si un ANC n'est pas activé, son état Activé est Non. Vous pouvez cliquer sur l'icône **Activer** la barre des tâches pour activer un ANC.

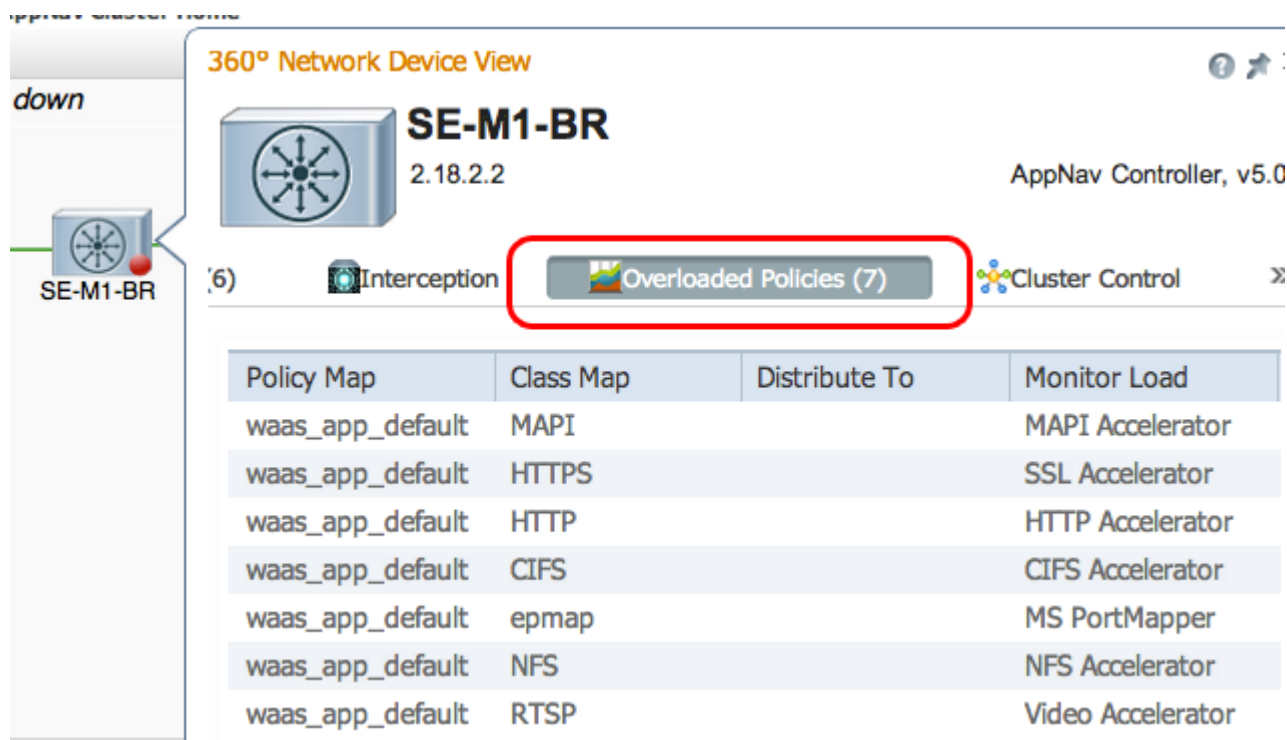
Vérifiez la stratégie AppNav sur chaque ANC qui a autre chose qu'un voyant d'état vert. Si vous placez le curseur sur le voyant d'état d'un périphérique, une info-bulle vous indique l'état ou le problème, si un problème est détecté.

Pour vérifier les stratégies définies, dans le menu Gestionnaire central, sélectionnez **Configurer > Stratégies AppNav**, puis cliquez sur le bouton **Gérer**.

En règle générale, une seule stratégie doit être affectée à tous les ANC du cluster. La stratégie par défaut est appnav_default. Sélectionnez la case d'option en regard d'une stratégie et cliquez sur l'icône **Modifier** la barre des tâches. Le volet Stratégie AppNav affiche les ANC auxquels la stratégie sélectionnée est appliquée. Si tous les ANC ne sont pas cochés, cochez la case en regard de chaque ANC non coché pour lui attribuer la stratégie. Cliquez sur **OK** pour enregistrer les modifications.

Après avoir vérifié les affectations de stratégie, vous pouvez vérifier les règles de stratégie dans la page Stratégies AppNav qui reste affichée. Sélectionnez une règle de stratégie et cliquez sur l'icône **Modifier** la barre des tâches pour modifier sa définition.

Un ANC peut avoir un voyant d'état jaune ou rouge si une ou plusieurs stratégies sont surchargées. Cochez l'onglet Surcharge Politiques de la vue des périphériques à 360 degrés pour afficher la liste des stratégies surveillées surchargées.



360° Network Device View

SE-M1-BR
2.18.2.2
AppNav Controller, v5.0

(6) Interception **Overloaded Policies (7)** Cluster Control

Policy Map	Class Map	Distribute To	Monitor Load
waas_app_default	MAPI		MAPI Accelerator
waas_app_default	HTTPS		SSL Accelerator
waas_app_default	HTTP		HTTP Accelerator
waas_app_default	CIFS		CIFS Accelerator
waas_app_default	epmap		MS PortMapper
waas_app_default	NFS		NFS Accelerator
waas_app_default	RTSP		Video Accelerator

Si un ANC se joint au cluster, il s'affiche avec un voyant d'état jaune et un état de jointure.

L'onglet Interception de la vue périphérique à 360 degrés indique que le chemin d'interception est en panne en raison de l'état de jonction. L'interception est bloquée jusqu'à ce que l'ANC ait synchronisé ses tables de flux avec les autres ANC et qu'il soit prêt à accepter le trafic. Ce processus ne prend généralement pas plus de deux minutes.

Si vous supprimez un ANC d'un cluster, il est toujours affiché pendant quelques minutes dans le schéma de topologie et comme actif dans l'onglet Contrôle de cluster, jusqu'à ce que tous les ANC conviennent de la nouvelle topologie de cluster. Il ne reçoit aucun nouveau flux dans cet état.

Commandes CLI AppNav pour la surveillance de l'état du cluster et du périphérique

Plusieurs commandes CLI sont utiles pour le dépannage d'un ANC :

- **show run service-insertion**
- **show service-insertion service-context**
- **show service-insertion appnav-controller-group**
- **show service-insertion service-node-group all**
- **show service-insertion appnav-controller *adresse IP***
- **show service-insertion service-node [*adresse IP*]**
- **show service-insertion service-node-group *nom-groupe***

Utilisez ces commandes sur un nom de réseau :

- **show run service-insertion**
- **show service-insertion service-node**

Vous pouvez utiliser la commande **show service-insertion service-context** sur un ANC pour voir l'état du contexte de service et la vue stable des périphériques dans le cluster :

```
ANC# show service-insertion service-context
Service Context                : test
Service Policy                 : appnav_default          <<< Active AppNav
policy
Cluster protocol ICIMP version : 1.1
Cluster protocol DMP version  : 1.1
Time Service Context was enabled : Wed Jul 11 02:05:23 2012
Current FSM state              : Operational             <<< Service context
status
Time FSM entered current state : Wed Jul 11 02:05:55 2012
Last FSM state                 : Converging
Time FSM entered last state    : Wed Jul 11 02:05:45 2012
Joining state                  : Not Configured
Time joining state entered     : Wed Jul 11 02:05:23 2012
Cluster Operational State      : Operational             <<< Status of this
ANC
Interception Readiness State   : Ready
Device Interception State      : Not Shutdown          <<< Interception is
```

not shut down by CMM

```
Stable AC View:                                     <<< Stable view of
converged ANCs
    10.1.1.1          10.1.1.2
Stable SN View:                                     <<< Stable view of
converged WNs
    10.1.1.1          10.1.1.2
Current AC View:
    10.1.1.1          10.1.1.2
Current SN View:
    10.1.1.1          10.1.1.2          10.1.1.3
```

Si le champ Device Interception State (ci-dessus) indique Shutdown (Arrêt), cela signifie que le CMM a arrêté l'interception en raison du fait que ce contrôleur ANC n'est pas prêt à recevoir les flux de trafic. Par exemple, l'ANC peut encore être dans le processus de jointure et le cluster n'a pas encore synchronisé les flux.

Les champs Stable View (ci-dessus) répertorient les adresses IP des ANC et des noms de réseau vus par ce périphérique ANC dans sa dernière vue convergente du cluster. Vue utilisée pour les opérations de distribution. Les champs Current View répertorient les périphériques annoncés par cette ANC dans ses messages de pulsation.

Vous pouvez utiliser la commande **show service-insertion appnav-controller-group** sur un ANC pour voir l'état de chaque ANC dans le groupe ANC :

```
ANC# show service-insertion appnav-controller-group
All AppNav Controller Groups in Service Context
Service Context                               : test
Service Context configured state              : Enabled

AppNav Controller Group : scg
Member AppNav Controller count : 2
  Members:
    10.1.1.1          10.1.1.2

AppNav Controller                               : 10.1.1.1
AppNav Controller ID                           : 1
Current status of AppNav Controller            : Alive                <<< Status of this ANC
Time current status was reached                 : Wed Jul 11 02:05:23 2012
Joining status of AppNav Controller            : Joined                  <<< Joining means ANC
is still joining
Secondary IP address                            : 10.1.1.1                <<< Source IP used in
cluster protocol packets
Cluster protocol ICIMP version                 : 1.1
Cluster protocol Incarnation Number           : 2
Cluster protocol Last Sent Sequence Number     : 0
Cluster protocol Last Received Sequence Number: 0

Current AC View of AppNav Controller:         <<< ANC and WN
devices advertised by this ANC
    10.1.1.1          10.1.1.2
Current SN View of AppNav Controller:
    10.1.1.1          10.1.1.2

AppNav Controller                               : 10.1.1.2 (local)        <<< local indicates
this is the local ANC
AppNav Controller ID                           : 1
Current status of AppNav Controller            : Alive
```

Time current status was reached : Wed Jul 11 02:05:23 2012
Joining status of AppNav Controller : Joined
Secondary IP address : 10.1.1.2
Cluster protocol ICIMP version : 1.1
Cluster protocol Incarnation Number : 2
Cluster protocol Last Sent Sequence Number : 0
Cluster protocol Last Received Sequence Number: 0

Current AC View of AppNav Controller: <<< ANC and WN

devices advertised by this ANC

10.1.1.1 10.1.1.2

Current SN View of AppNav Controller:

10.1.1.1 10.1.1.2 10.1.1.3

Pour obtenir la liste des états ANC possibles et des états de jointure, reportez-vous à la commande **show service-insertion** dans le *Guide de référence des commandes des services d'application de réseau étendu Cisco*.

Vous pouvez utiliser la commande **show service-insertion service-node** sur un ANC pour voir l'état d'un nom de domaine particulier dans le cluster :

ANC# **show service-insertion service-node 10.1.1.2**

Service Node: : 20.1.1.2
Service Node belongs to SNG : sng2
Service Context : test
Service Context configured state : Enabled

Service Node ID : 1
Current status of Service Node : Alive <<< WN is visible
Time current status was reached : Sun May 6 11:58:11 2011
Cluster protocol DMP version : 1.1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1692060441
Cluster protocol last received sequence number: 1441393061

AO state

AO	State	For	
--	----	---	
tfo	GREEN	3d 22h 11m 17s	<<< Overall/TFO state
reported by WN			
epm	GREEN	3d 22h 11m 17s	<<< AO states
reported by WN			
cifs	GREEN	3d 22h 11m 17s	
mapi	GREEN	3d 22h 11m 17s	
http	RED	3d 22h 14m 3s	
video	RED	11d 2h 2m 54s	
nfs	GREEN	3d 22h 11m 17s	
ssl	YELLOW	3d 22h 11m 17s	
ica	GREEN	3d 22h 11m 17s	

Vous pouvez utiliser la commande **show service-insertion service-node-group** sur un ANC pour voir l'état d'un WNG particulier dans le cluster :

ANC# **show service-insertion service-node-group sng2**

Service Node Group name : sng2
Service Context : scxt1
Member Service Node count : 1
Members:

10.1.1.1 10.1.1.2

Service Node: : 10.1.1.1
Service Node belongs to SNG : sng2
Current status of Service Node : Excluded <<< WN status
Time current status was reached : Sun Nov 6 11:58:11 2011
Cluster protocol DMP version : 1.1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1692061851
Cluster protocol last received sequence number: 1441394001

AO state

AO	State	For
--	-----	---
tfo	GREEN	3d 22h 12m 52s
epm	GREEN	3d 22h 12m 52s
cifs	GREEN	3d 22h 12m 52s
mapi	GREEN	3d 22h 12m 52s
http	RED	3d 22h 15m 38s
video	RED	11d 2h 4m 29s
nfs	GREEN	3d 22h 12m 52s
ssl	YELLOW	3d 22h 12m 52s
ica	GREEN	3d 22h 12m 52s

Service Node: : 10.1.1.2
Service Node belongs to WNG : sng2
Current status of Service Node : Alive <<< WN status
Time current status was reached : Sun Nov 6 11:58:11 2011
Cluster protocol DMP version : 1.1
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1692061851
Cluster protocol last received sequence number: 1441394001

AO state

AO	State	For
--	-----	---
tfo	GREEN	3d 22h 12m 52s
epm	GREEN	3d 22h 12m 52s
cifs	GREEN	3d 22h 12m 52s
mapi	GREEN	3d 22h 12m 52s
http	RED	3d 22h 15m 38s
video	RED	11d 2h 4m 29s
nfs	GREEN	3d 22h 12m 52s
ssl	YELLOW	3d 22h 12m 52s
ica	GREEN	3d 22h 12m 52s

SNG Availability per AO <<< AO status for entire

WNG

AO	Available	Since
--	-----	-----
tfo	Yes	3d 22h 12m 52s
epm	Yes	3d 22h 12m 52s
cifs	Yes	3d 22h 12m 52s
mapi	Yes	3d 22h 12m 52s
http	No	3d 22h 15m 38s
video	No	11d 2h 4m 29s
nfs	Yes	3d 22h 12m 52s
ssl	No	11d 2h 4m 29s
ica	Yes	3d 22h 12m 52s

Le premier nom dans l'exemple ci-dessus a le statut Excluded, ce qui signifie que le nom est visible par l'ANC mais qu'il est exclu du cluster car un ou plusieurs autres ANC ne le voient pas.

Le tableau Disponibilité SNG par AO indique si chaque AO est capable de gérer de nouvelles connexions. Un AO est disponible si au moins un WN du WNG a un statut VERT pour l'AO.

Vous pouvez utiliser la commande **show service-insertion service-node** sur un nom d'utilisateur pour voir l'état du nom d'utilisateur :

WAE# **show service-insertion service-node**

Cluster protocol DMP version : 1.1
Service started at : Wed Jul 11 02:05:45 2012
Current FSM state : Operational <<< WN is responding to

health probes

Time FSM entered current state : Wed Jul 11 02:05:45 2012
Last FSM state : Admin Disabled
Time FSM entered last state : Mon Jul 2 17:19:15 2012
Shutdown max wait time:
Configured : 120
Operational : 120

Last 8 AppNav Controllers

AC IP	My IP	DMP Version	Incarnation	Sequence	Time Last Heard
-----	-----	-----	-----	-----	---

Reported state

<<< TFO and AO reported states

Accl	State	For	Reason
-----	-----	---	-----
TFO (System)	GREEN	43d 7h 45m 8s	
EPM	GREEN	43d 7h 44m 40s	
CIFS	GREEN	43d 7h 44m 41s	
MAPI	GREEN	43d 7h 44m 43s	
HTTP	GREEN	43d 7h 44m 45s	
VIDEO	GREEN	43d 7h 44m 41s	
NFS	GREEN	43d 7h 44m 44s	
SSL	RED	43d 7h 44m 21s	
ICA	GREEN	43d 7h 44m 40s	

Monitored state of Accelerators

<<< TFO and AO actual states

TFO (System)
Current State: GREEN
Time in current state: 43d 7h 45m 8s
EPM
Current State: GREEN
Time in current state: 43d 7h 44m 40s
CIFS
Current State: GREEN
Time in current state: 43d 7h 44m 41s
MAPI
Current State: GREEN
Time in current state: 43d 7h 44m 43s
HTTP
Current State: GREEN
Time in current state: 43d 7h 44m 45s
VIDEO

```
Current State: GREEN
Time in current state: 43d 7h 44m 41s
NFS
Current State: GREEN
Time in current state: 43d 7h 44m 44s
SSL
Current State: RED
Time in current state: 43d 7h 44m 21s
Reason:
AO is not configured
ICA
Current State: GREEN
Time in current state: 43d 7h 44m 40s
```

L'état surveillé d'un accélérateur est son état réel, mais l'état signalé peut différer, car il s'agit de l'état le plus bas du système ou de l'état de l'accélérateur.

Pour plus d'informations sur le dépannage de l'optimisation sur un réseau étendu, consultez les articles [Dépannage de l'optimisation](#) et [Dépannage de l'accélération des applications](#).

Commandes CLI AppNav pour la surveillance des statistiques de distribution de flux

Plusieurs commandes CLI sont utiles pour le dépannage des politiques et la distribution de flux sur un ANC :

- **show policy-map type appnav *polycymap-name*** — Affiche les règles de stratégie et le nombre d'occurrences pour chaque classe de la carte de stratégie.
- **show class-map type appnav *class-name*** — Affiche les critères de correspondance et le nombre de résultats pour chaque condition de correspondance dans la carte de classe.
- **show policy-sub-class type appnav *level1-class-name level2-class-name*** — Affiche les critères de correspondance et le nombre de résultats pour chaque condition de correspondance dans une carte de classe dans une carte de stratégie AppNav imbriquée.
- **show statistics class-map type appnav *class-name*** — Affiche les statistiques d'interception et de distribution du trafic pour une carte de classe.
- **show statistics policy-sub-class type appnav *level1-class-name level2-class-name*** — Affiche les statistiques d'interception et de distribution du trafic pour une carte de classe dans une carte de stratégie AppNav imbriquée.
- **show statistics pass-through type appnav** — Affiche les statistiques de trafic AppNav pour chaque raison de transfert.
- **show appnav-controller flow-distribution** — Montre comment un flux hypothétique spécifique serait classifié et distribué par un ANC, en fonction de la politique définie et des conditions de charge dynamique. Cette commande peut être utile pour vérifier comment un flux particulier sera traité sur un ANC et à quelle classe il appartient.

Utilisez ces commandes sur un réseau étendu pour dépanner la distribution de flux :

- **show statistics service-insertion service-node *ip-address*** — Affiche les statistiques pour les accélérateurs et le trafic distribué au réseau local virtuel.
- **show statistics service-insertion service-node-group name *group-name*** — Affiche les statistiques pour les accélérateurs et le trafic distribué au WNG.

Vous pouvez utiliser la commande **show statistics class-map type appnav *class-name*** sur un ANC pour dépanner la distribution de flux, par exemple pour déterminer pourquoi le trafic peut être lent pour une classe particulière. Il peut s'agir d'un mappage de classe d'application tel que HTTP ou,

si tout le trafic vers une branche semble lent, il peut s'agir d'un mappage de classe d'affinité de branche. Voici un exemple pour la classe HTTP :

```

ANC# show statistics class-map type appnav HTTP
Class Map                               From Network to SN   From SN to Network
-----
HTTP
  Redirected Client->Server:
    Bytes                                3478104              11588180
    Packets                               42861               102853
  Redirected Server->Client:
    Bytes                                1154109763          9842597
    Packets                               790497              60070

Connections
-----
  Intercepted by ANC                      4                    <<< Are connections
being intercepted?
  Passed through by ANC                   0                    <<< Passed-through
connections
  Redirected by ANC                       4                    <<< Are connections
being distributed to WNs?
  Accepted by SN                          4                    <<< Connections accepted
by WNs
  Passed through by SN (on-Syn)           0                    <<< Connections might be
passed through by WNs
  Passed through by SN (post-Syn)        0                    <<< Connections might be
passed through by WNs

Passthrough Reasons                      Packets              Bytes                <<< Why is ANC passing
through connections?
-----
  Collected by ANC:
    PT Flow Learn Failure                  0                    0                    <<< Asymmetric
connection; interception problem
    PT Cluster Degraded                   0                    0                    <<< ANCs cannot
communicate
    PT SNG Overload                       0                    0                    <<< All WNs in the WNG
are overloaded
    PT AppNav Policy                      0                    0                    <<< Connection policy is
pass-through
    PT Unknown                             0                    0                    <<< Unknown passthrough

  Indicated by SN:                        <<< Why are WNs passing
through connections?
    PT No Peer                             0                    0                    <<< List of WN pass-
through reasons
  ...

```

Les raisons de transfert du nom de domaine dans la section Indiqué par le numéro de série ne s'incrémentent que si le déchargement du transfert est configuré sur un nom de domaine. Sinon, l'ANC ne sait pas que le WN passe par une connexion et ne le compte pas.

Si les connexions : Intercepté par le compteur ANC n'augmente pas, il y a un problème d'interception. Vous pouvez utiliser l'utilitaire WAAS TcpTraceroute pour dépanner l'emplacement de l'ANC dans le réseau, trouver des chemins asymétriques et déterminer la stratégie appliquée à une connexion. Pour plus d'informations, consultez la section [Suivi des connexions](#).

Commandes CLI AppNav pour le débogage des connexions

Pour déboguer une connexion individuelle ou un ensemble de connexions sur un ANC, vous pouvez utiliser la commande **show statistics appnav-controller connection** pour afficher la liste des connexions actives.

```
anc# show statistics appnav-controller connection
Collecting Records. Please wait...
Optimized Flows:
-----
Client                Server                SN-IP                AC Owned
2.30.5.10:38111      2.30.1.10:5004      2.30.1.21            Yes
2.30.5.10:38068      2.30.1.10:5003      2.30.1.21            Yes
2.30.5.10:59861      2.30.1.10:445       2.30.1.21            Yes
2.30.5.10:59860      2.30.1.10:445       2.30.1.21            Yes
2.30.5.10:43992      2.30.1.10:5001      2.30.1.5             Yes
2.30.5.10:59859      2.30.1.10:445       2.30.1.21            Yes
2.30.5.10:59858      2.30.1.10:445       2.30.1.21            Yes
2.30.5.10:59857      2.30.1.10:445       2.30.1.21            Yes
2.30.5.10:59856      2.30.1.10:445       2.30.1.21            Yes

Passthrough Flows:
-----
Client                Server                Passthrough Reason
2.30.5.10:41911      2.30.1.10:5002      PT Flowswitch Policy
```

Vous pouvez filtrer la liste en spécifiant l'adresse IP du client ou du serveur et/ou les options de port et vous pouvez afficher des statistiques détaillées sur les connexions en spécifiant le mot clé **detail**.

```
anc# show statistics appnav-controller connection server-ip 2.30.1.10 detail
Collecting Records. Please wait...

Optimized Flows
-----
Client: 2.30.5.10:55330
Server: 2.30.1.10:5001
AppNav Controller Owned: Yes          <<< This ANC is seeing activity on this connection
Service Node IP:2.30.1.5              <<< Connection is distributed to this SN
Classifier Name: se_policy:p5001      <<< Name of matched class map
Flow association: 2T:No,3T:No         <<< Connection is associated with dynamic app or session
(MAPI and ICA only)?
Application-ID: 0                     <<< AO that is optimizing the connection
Peer-ID: 00:14:5e:84:41:31           <<< ID of the optimizing peer

Client: 2.30.5.10:55331
Server: 2.30.1.10:5001
AppNav Controller Owned: Yes
Service Node IP:2.30.1.5
Classifier Name: se_policy:p5001
Flow association: 2T:No,3T:No
Application-ID: 0
Peer-ID: 00:14:5e:84:41:31
...
```

Vous pouvez spécifier l'option de résumé pour afficher le nombre de connexions distribuées et directes actives.

```
anc# show statistics appnav-controller connection summary
Number of optimized flows      = 2
Number of pass-through flows = 17
```

Suivi des connexions

Pour vous aider à dépanner les flux AppNav, vous pouvez utiliser l'outil de suivi des connexions dans le Gestionnaire central. Cet outil affiche les informations suivantes pour une connexion particulière :

- Si la connexion a été transmise ou distribuée à un WNG
- Motif de transmission, le cas échéant
- WNG et WN auxquels la connexion a été distribuée
- Accélérateur surveillé pour la connexion
- Mise en correspondance de classes appliquée

Pour utiliser l'outil de trace de connexion, procédez comme suit :

1. Dans le menu Gestionnaire central, choisissez **AppNav Clusters** > *nom de cluster*, puis choisissez **Monitor** > **Tools** > **Connection Trace**.
2. Choisissez l'ANC, le périphérique WAAS homologue, et spécifiez les critères de correspondance de connexion.
3. Cliquez sur **Trace** pour afficher les connexions correspondantes.

Le protocole WAAS TCP Traceroute est un autre outil non spécifique à AppNav qui peut vous aider à résoudre les problèmes de réseau et de connexion, y compris les chemins asymétriques. Vous pouvez l'utiliser pour trouver une liste de noeuds WAAS entre le client et le serveur, ainsi que les stratégies d'optimisation configurées et appliquées pour une connexion. Dans Central Manager, vous pouvez choisir n'importe quel périphérique de votre réseau WAAS à partir duquel exécuter la commande traceroute. Pour utiliser l'outil Traceroute TCP du Gestionnaire central WAAS, procédez comme suit :

1. Dans le menu Gestionnaire central WAAS, sélectionnez **Monitor** > **Troubleshoot** > **WAAS Tcpttraceroute**. Vous pouvez également choisir un périphérique d'abord, puis choisir cet élément de menu pour exécuter la commande traceroute à partir de ce périphérique.
2. Dans la liste déroulante Noeud WAAS, sélectionnez un périphérique WAAS à partir duquel exécuter la commande traceroute. (Cet élément n'apparaît pas si vous vous trouvez dans le contexte du périphérique.)
3. Dans les champs Destination IP et Destination Port, saisissez l'adresse IP et le port de destination vers lesquels vous souhaitez exécuter la commande traceroute.
4. Cliquez sur **Exécuter TCPTraceroute** pour afficher les résultats.

Les noeuds WAAS du chemin tracé sont affichés dans le tableau sous les champs. Vous pouvez également exécuter cet utilitaire à partir de l'interface de ligne de commande à l'aide de la commande **waas-tcptrace**.

Journalisation du débogage AppNav

Le fichier journal suivant est disponible pour le dépannage des problèmes du gestionnaire de

cluster AppNav :

- Fichiers journaux de débogage : /local1/errorlog/cmm-errorlog.current (et cmm-errorlog.*)

Pour configurer et activer la journalisation de débogage du gestionnaire de cluster AppNav, utilisez les commandes suivantes.

NOTE: La journalisation de débogage est gourmande en CPU et peut générer une grande quantité de sortie. Utilisez-le judicieusement et avec parcimonie dans un environnement de production.

Vous pouvez activer la journalisation détaillée sur le disque :

```
WAE(config)# logging disk enable
WAE(config)# logging disk priority detail
```

Les options de débogage du gestionnaire de cluster (sur 5.0.1 et versions ultérieures) sont les suivantes :

```
WAE# debug cmm ?
all          enable all CMM debugs
cli          enable CMM cli debugs
events       enable CMM state machine events debugs
ipc          enable CMM ipc messages debugs
misc         enable CMM misc debugs
packets      enable CMM packet debugs
shell        enable CMM infra debugs
timers       enable CMM state machine timers debugs
```

Vous pouvez activer la journalisation du débogage pour le gestionnaire de cluster, puis afficher la fin du journal des erreurs de débogage comme suit :

```
WAE# debug cmm all
WAE# type-tail errorlog/cmm-errorlog.current follow
```

Vous pouvez également activer la journalisation de débogage pour le gestionnaire de distribution de flux (FDM) ou l'agent de distribution de flux (FDA) avec les commandes suivantes :

```
WAE# debug fdm all
WAE# debug fda all
```

Le FDM détermine où distribuer les flux en fonction des conditions de charge dynamique et de stratégie des noms d'utilisateur. La FDA recueille des informations sur la charge du WWN. Les fichiers journaux suivants sont disponibles pour le dépannage des problèmes FDM et FDA :

- Fichiers journaux de débogage : /local1/errorlog/fdm-errorlog.current (et fdm-errorlog.*)
- Fichiers journaux de débogage : /local1/errorlog/fda-errorlog.current (et fda-errorlog.*)

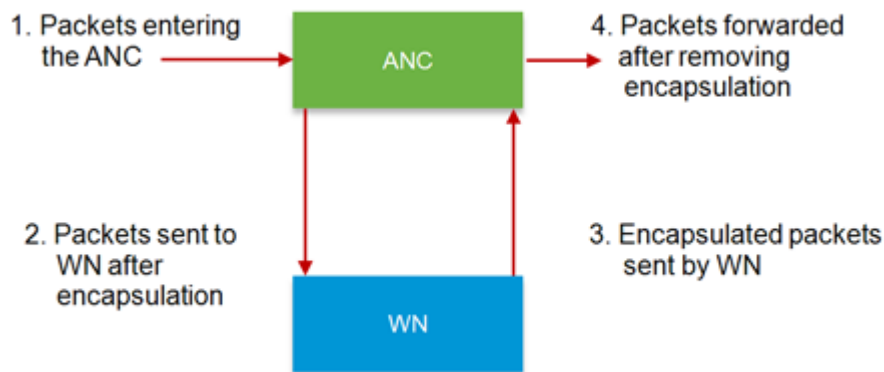
Capture de paquets AppNav

Une nouvelle commande **packet-capture** est introduite pour permettre la capture de paquets de données sur les interfaces du module d'interface du contrôleur Cisco AppNav. Cette commande peut également capturer des paquets sur d'autres interfaces et décoder les fichiers de capture de

paquets. La commande **packet-capture** est préférée aux commandes déconseillées **tcpdump** et **tethéal**, qui ne peuvent pas capturer les paquets sur le module d'interface du contrôleur Cisco AppNav. Reportez-vous au *Guide de référence des commandes des services d'application de réseau étendu de Cisco* pour plus de détails sur la syntaxe des commandes.

Note: La capture de paquets ou la capture de débogage peuvent être actives, mais pas les deux simultanément.

Les paquets de données envoyés entre les ANC et les WAN sont encapsulés, comme illustré dans le schéma suivant.



Si vous capturez des paquets aux points 1 ou 4 du schéma, ils ne sont pas encapsulés. Si vous capturez des paquets aux points 2 ou 3, ils sont encapsulés.

Voici un exemple de sortie pour une capture de paquets encapsulée :

```
anc# packet-capture appnav-controller interface GigabitEthernet 1/0 access-list all
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth14
0.000000    2.58.2.11 -> 2.1.6.122    TCP https > 2869 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4.606723    2.58.2.175 -> 2.43.64.21    TELNET Telnet Data ...
...
37.679587    2.58.2.40 -> 2.58.2.35    GRE Encapsulated 0x8921 (unknown)
37.679786    2.58.2.35 -> 2.58.2.40    GRE Encapsulated 0x8921 (unknown)
```

Voici un exemple de sortie pour une capture de paquets non encapsulée :

```
anc# packet-capture appnav-controller access-list all non-encapsulated
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth14
0.751567    2.58.2.175 -> 2.43.64.21    TELNET Telnet Data ...
1.118363    2.58.2.175 -> 2.43.64.21    TELNET Telnet Data ...
1.868756    2.58.2.175 -> 2.43.64.21    TELNET Telnet Data ...
...
```

Instructions de capture de paquets :

- Une liste de contrôle d'accès de capture de paquets est toujours appliquée au paquet IP interne pour les paquets encapsulés WCCP-GRE et SIA.
- La capture de paquets est effectuée sur toutes les interfaces ANC si l'interface ANC pour la

capture de paquets n'est pas fournie.

Voici un exemple de sortie pour une capture de paquets sur une interface WAN :

```
anc# packet-capture interface GigabitEthernet 0/0 access-list 10
Packet-Capture: Setting virtual memory/file size limit to 419430400
Running as user "admin" and group "root". This could be dangerous.
Capturing on eth0
 0.000000      2.1.8.4 -> 2.64.0.6      TELNET Telnet Data ...
 0.000049      2.64.0.6 -> 2.1.8.4      TELNET Telnet Data ...
 0.198908      2.1.8.4 -> 2.64.0.6      TCP 18449 > telnet [ACK] Seq=2 Ack=2 Win=3967 Len=0
 0.234129      2.1.8.4 -> 2.64.0.6      TELNET Telnet Data ...
 0.234209      2.64.0.6 -> 2.1.8.4      TELNET Telnet Data ...
```

Voici un exemple de décodage d'un fichier de capture de paquets :

```
anc# packet-capture decode /local1/se_flow_add.cap
Running as user "admin" and group "root". This could be dangerous.  1  0.000000
 100.1.1.2 -> 100.1.1.1      GRE Encapsulated SWIRE  2  0.127376
 100.1.1.2 -> 100.1.1.1      GRE Encapsulated SWIRE
```

Vous pouvez spécifier un port src-ip/dst-ip/src-port/dst-port pour le filtrage des paquets :

```
anc# packet-capture decode source-ip 2.64.0.33 /local1/hari_pod_se_flow.cap
```

```
Running as user "admin" and group "root". This could be dangerous.
 3  0.002161      2.64.0.33 -> 2.64.0.17      TCP 5001 > 33165 [SYN, ACK] Seq=0 Ack=1
Win=5792 Len=0 MSS=1460 TSV=326296092 TSER=326296080 WS=4
 4  0.002360      2.64.0.33 -> 2.64.0.17      TCP 5001 > 33165 [SYN, ACK] Seq=0 Ack=1
Win=5792 Len=0 MSS=1406 TSV=326296092 TSER=326296080 WS=4
```