WAAS - Risoluzione dei problemi di AppNav

Capitolo: Risoluzione dei problemi di AppNav

In questo articolo viene descritto come risolvere i problemi relativi a una distribuzione di AppNav.

Co

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

Sommario

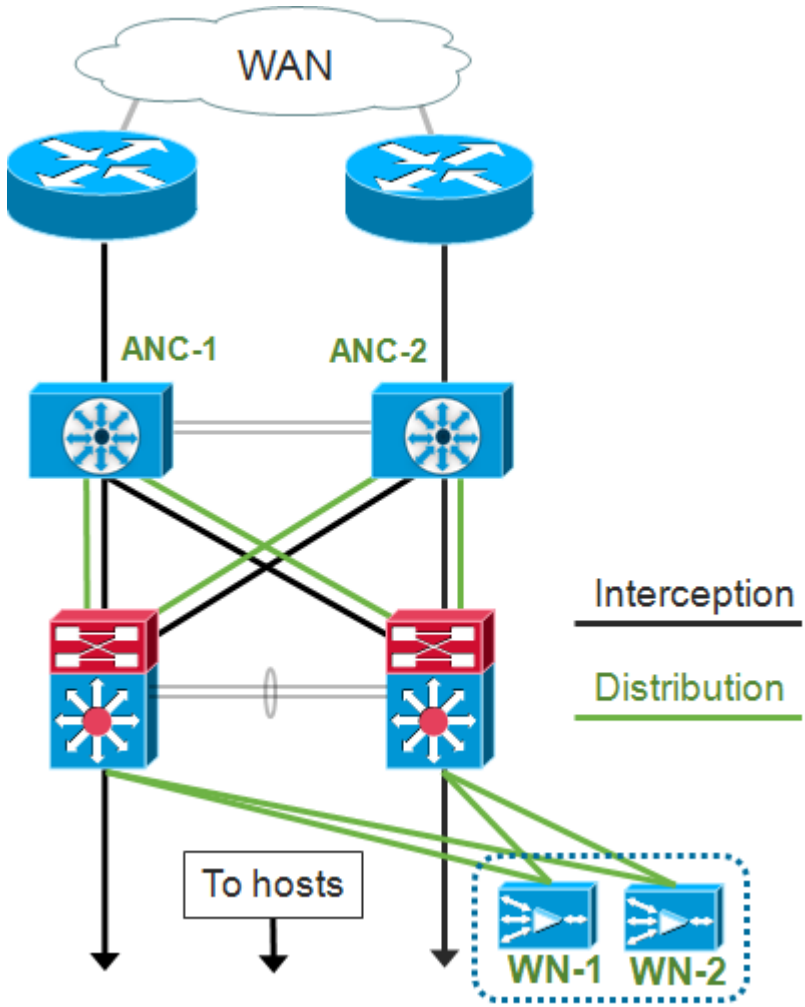
Risoluzione dei problemi di AppNav

Cisco WAAS AppNav semplifica l'integrazione in rete dell'ottimizzazione della WAN e riduce notevolmente la dipendenza dallo switch o dal router di intercettazione utilizzando i controller AppNav (ANC) per distribuire il traffico tra i nodi WAAS (WN) per l'ottimizzazione utilizzando un potente meccanismo di classe e policy. È possibile utilizzare i nodi WAAS (WN) per ottimizzare il traffico in base ai siti e/o alle applicazioni. In questo articolo viene descritto come risolvere i problemi relativi ad AppNav.

NOTA: La funzionalità AppNav è stata introdotta in WAAS versione 5.0.1. Questa sezione non è applicabile alle versioni precedenti di WAAS.

Intercettazione in-path (inline)

In modalità inline, le ANC vengono posizionate nel percorso del traffico di rete dove intercettano i pacchetti e li distribuiscono ai WAN.



La configurazione interfaccia per una distribuzione inline assegna i ruoli di intercettazione e distribuzione a interfacce separate sul modulo di interfaccia di Cisco AppNav Controller. Per l'intercettazione è necessaria un'interfaccia bridge-group costituita da due o più interfacce fisiche o di canale della porta o da una di ciascuna. l'interfaccia bridge-gruppo non ha capacità di

collegamento in errore; in altre parole, si apre in errore e il traffico non viene bloccato meccanicamente in seguito a un guasto del dispositivo o a una interruzione dell'alimentazione. AppNav utilizza il clustering per fornire alta disponibilità se il modulo di interfaccia di AppNav Controller, il percorso del collegamento o la connettività al modulo di interfaccia di AppNav Controller viene interrotta o si verifica un'interruzione dell'alimentazione.

Nota: Le interfacce bridge non bloccano i pacchetti BPDU (Bridge Protocol Data Unit) e, nel caso di interfacce ridondanti che creano loop, una delle interfacce è bloccata dallo Spanning Tree Protocol.

La risoluzione dei problemi relativi all'intercettazione in linea è costituita dai seguenti passaggi:

- Verificare il corretto posizionamento in linea dell'ANC controllando il progetto della rete. Se necessario, utilizzare strumenti di base come ping e traceroute o strumenti o applicazioni di livello 7 per verificare che il percorso del traffico di rete sia quello previsto. Controllare il cablaggio fisico dell'ANC.
- Verificare che l'ANC sia impostato sulla modalità di intercettazione in linea.
- Verificare che l'interfaccia bridge-group sia configurata correttamente.

Gli ultimi due passaggi possono essere eseguiti in Central Manager o sulla riga di comando, sebbene il metodo preferito sia Central Manager, che viene descritto per primo.

In Gestione centrale, scegliere **Dispositivi >** *AppNavController*, quindi scegliere **Configura > Intercettazione > Configurazione intercettazione**. Verificare che il metodo di intercettazione sia impostato su Inline.

Nella stessa finestra, verificare che sia configurata un'interfaccia bridge. Se è necessaria un'interfaccia bridge, fare clic su **Crea bridge** per crearla. È possibile assegnare al gruppo bridge fino a due interfacce membro. È possibile usare lo strumento di calcolo VLAN per definire le voci VLAN in base alle operazioni di inclusione o esclusione. Notare che all'interfaccia bridge non è assegnato un indirizzo IP.

Utilizzare il pannello Allarmi o il comando **show alarm** exec per verificare se sul dispositivo vengono generati allarmi relativi al bridge. Un allarme bridge_down indica che una o più interfacce membro nel bridge sono inattive.

Dalla CLI, seguire questi passaggi per configurare il funzionamento inline:

1. Impostare il metodo di intercettazione su inline:

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

2. Creare l'interfaccia bridge-group:

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

3. (Facoltativo) Specificare l'elenco di VLAN da intercettare, se necessario:

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

4. Aggiungere due interfacce logiche/fisiche all'interfaccia del gruppo-ponte:

```
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
```

Èpossibile utilizzare il comando **show bridge** exec per verificare lo stato operativo dell'interfaccia del bridge e visualizzare le statistiche relative al bridge.

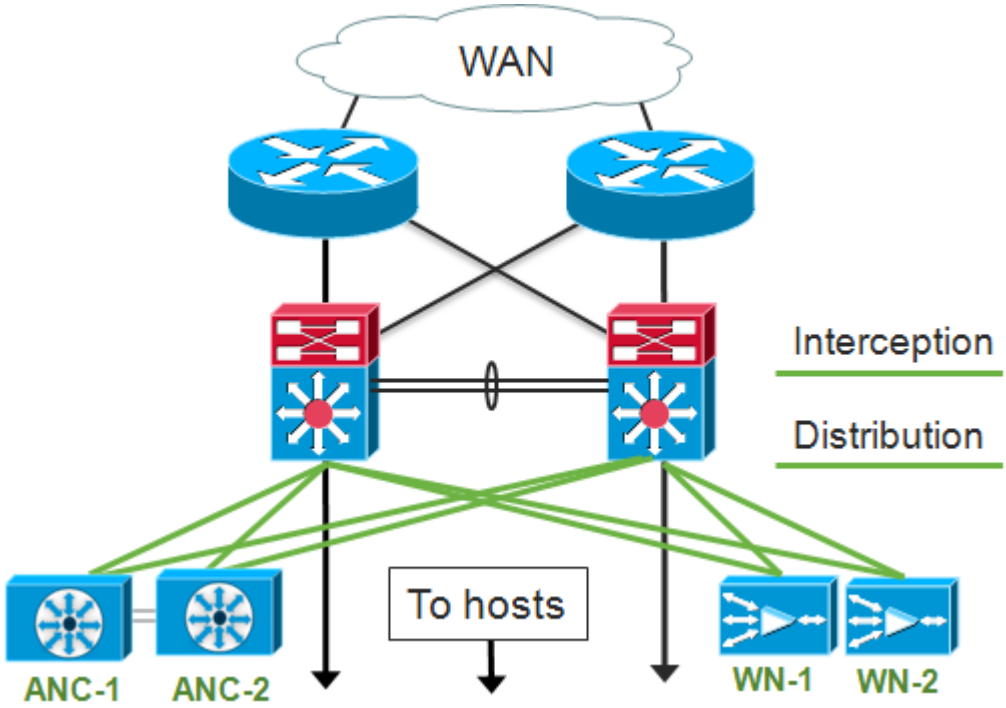
```
wave# show bridge 1
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Member Interfaces:
 GigabitEthernet 1/0
 GigabitEthernet 1/1
Link state propagation: Enabled
VLAN interception:
 intercept vlan-id all                                                    <<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

Nell'esempio precedente, l'interfaccia Gig 1/0 è inattiva e anche l'interfaccia Gig 1/1 è inattiva a causa della propagazione dello stato del collegamento (LSP). È inoltre possibile che venga visualizzato Down(flow sync), ovvero l'ANC viene aggiunto a un cluster e sincronizza le informazioni sul flusso con altre ANC nel cluster. Mantiene il percorso di intercettazione (interfaccia bridge) chiuso per circa due minuti finché tutti gli ANC non sono sincronizzati in modo che i flussi esistenti possano essere distribuiti correttamente.

Nella parte inferiore dell'output vengono visualizzate le statistiche del traffico per le interfacce membro.

Intercettazione off-path (WCCP)

In modalità WCCP, i router WCCP sono posizionati nel percorso del traffico di rete dove intercettano i pacchetti e li reindirizzano agli ANC, che si trovano all'esterno del percorso. Poiché AppNav gestisce l'elaborazione delle intercettazioni, la distribuzione intelligente del flusso e la considerazione del carico tra acceleratori WAAS, la configurazione WCCP sui router è notevolmente semplificata.



Nella configurazione interfaccia per una distribuzione off-path, i ruoli di intercettazione e distribuzione possono condividere le stesse interfacce sul modulo di interfaccia di Cisco AppNav Controller, ma non è necessario.

La risoluzione dei problemi relativi all'intercettazione fuori percorso è costituita dai seguenti passaggi:

- Verificare che i router WCCP siano posizionati correttamente per verificare che si trovino nel percorso del traffico tra gli host ottimizzati e che parta da essi. È possibile utilizzare i comandi **show run** o **show wcp** per verificare che si tratti degli stessi router configurati per WCCP. Se necessario, utilizzare strumenti di base come ping e traceroute o strumenti o applicazioni di livello 7 per verificare che tutto il traffico che richiede ottimizzazione passi attraverso i router WCCP.
- Verificare la configurazione WCCP sulle ANC WAAS, utilizzando Central Manager (preferito) o la CLI.
- Verificare la configurazione WCCP sui router di reindirizzamento, usando la CLI del router.

Per verificare la configurazione WCCP sulle ANC, in Central Manager, scegliere **Devices >** *AppNavController*, quindi **Configure > Interception > Interception Configuration**.

- Verificare che il metodo di intercettazione sia impostato su WCCP.
- Verificare che la casella di controllo Abilita servizio WCCP sia selezionata.
- Verificare che la casella di controllo Usa gateway predefinito come router WCCP sia selezionata o che gli indirizzi IP del router WCCP siano elencati nel campo Router WCCP.
- Verificare che le altre impostazioni, ad esempio la maschera di bilanciamento del carico e il metodo di reindirizzamento, siano configurate correttamente per la distribuzione.

Verificare la presenza di eventuali allarmi relativi ai WCCP sui controller di dominio di rete (ANC) che facciano parte della farm WCCP del router. In Gestione centrale, fare clic sul pannello Allarmi nella parte inferiore della schermata o usare il comando **show alarm** su ciascun dispositivo per visualizzare gli allarmi. Correggere eventuali condizioni di allarme modificando la configurazione sull'ANC o sul router, in base alle esigenze.

Dalla CLI, seguire questi passaggi per configurare il funzionamento di WCCP:

1. Impostare il metodo di intercettazione su wccp.

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

2. Configurare l'elenco dei router WCCP, contenente gli indirizzi IP dei router che partecipano alla farm WCCP.

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

3. Configurare l'ID servizio WCCP. Per AppNav è preferibile un unico ID di servizio, sebbene siano supportati due ID di servizio.

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

4. Associare l'elenco di router configurato al servizio WCCP.

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

5. Configurare il metodo di assegnazione WCCP (solo il metodo mask è supportato su un sistema ANC). Se non si specificano le opzioni dst-ip-mask o src-ip-mask, la maschera IP di origine predefinita viene impostata su f e la maschera IP di destinazione su 0.

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

6. Configurare il metodo di reindirizzamento WCCP (i metodi di uscita e di ritorno vengono impostati automaticamente in modo da corrispondere al metodo di reindirizzamento e non sono configurabili per un'ANC). È possibile scegliere L2 (impostazione predefinita) o GRE. L2 richiede che l'ANC abbia una connessione di layer 2 con il router e che il router sia configurato anche per il reindirizzamento di layer 2.

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

7. Abilitare il servizio WCCP.

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

Verificare l'intercettazione WCCP su ciascun ANC utilizzando il comando **show running-config**. I due esempi seguenti mostrano l'output della configurazione in esecuzione per il reindirizzamento L2 e il reindirizzamento GRE.

Show running-config wccp (per reindirizzamento 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                                        <<< L2 redirect is default so is not shown in
running config
  exit
```

Show running-config wccp (per 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                            <<< GRE redirect method is configured
 enable
 exit
```

Verificare lo stato WCCP su ciascun ANC utilizzando il comando **show wcp status**.

```
wave# show wccp routers
WCCP Interception :
Configured State :  Enabled                     <<< Shows Disabled if WCCP is not configured
Operational State : Enabled                     <<< Shows Disabled if WCCP is not enabled
 Services Enabled on this WAE:
        TCP Promiscuous 61                      <<< Shows NONE if no service groups are
configured
```

Verificare i router che hanno risposto ai messaggi keep-alive nella farm WCCP utilizzando il comando **show wcp router**.

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

       Routers Seeing this Wide Area Engine(2)
       Router Id       Sent To                  <<< List of routers seen by this ANC
       192.168.1.1     10.10.10.21
       192.168.1.2     10.10.10.22
       Routers not Seeing this Wide Area Engine   <<< List of routers not seen by this ANC
               -NONE-
       Routers Notified of from other WAE's       <<< List of routers notified of but not
configured in router list
               -NONE-
```

Verificare la vista di ciascun ANC degli altri ANC nella farm WCCP e dei router raggiungibili da ciascuno di essi utilizzando il comando **show wcp clients**.

```
wave# show wccp clients
Wide Area Engine List for Service: 61
Number of WAE's in the Cache farm: 2                            <<< Number of ANCs in the farm
       IP address = 10.10.10.31   Lead WAE = NO   Weight = 0   <<< Entry for each ANC in the
farm
       Routers seeing this Wide Area Engine(2)
               192.168.1.1                                      <<< List of routers seeing this
ANC
               192.168.1.2

       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
```

Verificare che ogni ANC riceva i pacchetti dai router della farm utilizzando il comando **show statistics wccp**. Vengono visualizzate le statistiche per il traffico ricevuto, passato e inviato a ciascun router. Nella parte inferiore vengono visualizzate le statistiche cumulative per tutti i router della farm. Un comando simile è **show wccp statistics**. Notare che "OE" si riferisce ai dispositivi ANC qui.

```
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
```

Configurazione e verifica dell'intercettazione WCCP sul router

Per configurare l'intercettazione WCCP su ogni router della farm WCCP, eseguire la procedura seguente.

1. Configurare il servizio WCCP sul router utilizzando il comando **ip wcp** router.

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

2. Configurare l'intercettazione WCCP sulle interfacce LAN e WAN del router. È possibile configurare lo stesso ID servizio su entrambe le interfacce se si utilizza un unico ID servizio sugli 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. (Facoltativo) Configurare un'interfaccia tunnel se si utilizza un'uscita GRE generica (solo se si è scelto GRE per il metodo di reindirizzamento 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
```

Verificare la configurazione WCCP su ciascun router della farm utilizzando il comando **show wcp**.

```
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
```

Ulteriori informazioni

Per ulteriori informazioni, vedere i seguenti documenti:

- Integrazione della rete WCCP con Cisco Catalyst 6500: Suggerimenti sulle procedure ottimali per le distribuzioni riuscite
- Reindirizzamento protocollo di comunicazione Web Cache per servizi applicativi ad ampio raggio Cisco: Supporto piattaforma router Cisco
- configurazione delle funzionalità WCCP avanzate sui router dalla *guida alla configurazione dei servizi delle applicazioni ad ampio raggio Cisco*
- Configurazione di WCCP su WAE, dalla *Guida alla configurazione dei servizi delle applicazioni ad ampio raggio Cisco*

Risoluzione dei problemi di connettività di rete

Quando si esegue la risoluzione dei problemi di WAAS, può essere utile determinare il comportamento della rete con WAAS disattivato. Questo è utile quando il traffico non solo non riesce ad essere ottimizzato, ma non riesce a passare. In questi casi, potrebbe risultare che il problema non è WAAS. Anche nei casi in cui il traffico attraversi, questa tecnica può aiutare a determinare quali dispositivi WAAS richiedono la risoluzione dei problemi.

Prima di verificare la connettività di layer 3, verificare che il modulo di interfaccia del controller AppNav sia collegato alle porte corrette dello switch. Se lo switch connesso supporta e ha il protocollo CDP (Cisco Discovery Protocol) abilitato, eseguire il comando **show cdp neighbors detail** per verificare la corretta connettività allo switch di rete.

La disattivazione di WAAS potrebbe non essere applicabile in tutti i casi. Se parte del traffico è in fase di ottimizzazione e parte non lo è, potrebbe essere inaccettabile disabilitare WAAS, interrompendo in tal modo il traffico in fase di ottimizzazione. In questo caso, è possibile utilizzare l'ACL di intercettazione o il criterio AppNav per passare attraverso il tipo specifico di traffico che presenta problemi. Per i dettagli, vedere la sezione Passaggio attraverso un traffico specifico.

Per disabilitare WAAS, vengono eseguiti passaggi diversi per la modalità in linea rispetto alla modalità off-path:

- La modalità inline richiede che il bridge di intercettazione sia in stato pass-through. Per ulteriori informazioni, vedere la sezione Disattivazione di un ANC inline.
- La modalità off-path richiede la disabilitazione del protocollo WCCP. Per ulteriori informazioni, vedere la sezione Disattivazione di un'ANC fuori percorso.

Negli ambienti AppNav, solo le ANC devono essere disabilitate. Non è necessario che i nomi principali siano disabilitati, in quanto non partecipano all'intercettazione.

Dopo aver disattivato WAAS, controllare la connettività di rete utilizzando i metodi standard.

- Verificare la connettività di layer 3 utilizzando strumenti quali ping e traceroute.
- Controllare il comportamento dell'applicazione per determinare la connettività di livello superiore
- Se nella rete si verificano gli stessi problemi di connettività riscontrati con WAAS abilitato, è molto probabile che il problema non sia correlato a WAAS.
- Se la rete funziona correttamente con WAAS disabilitato, ma sono stati riscontrati problemi di connessione con WAAS abilitato, è probabile che vi siano uno o più dispositivi WAAS che richiedono attenzione. Il passo successivo è isolare il problema da dispositivi WAAS specifici.
- Se la rete è connessa con e senza WAAS abilitato, ma non è ottimizzata, probabilmente ci sono uno o più dispositivi WAAS che richiedono attenzione. Il passo successivo è isolare il problema da dispositivi WAAS specifici.

Per verificare il comportamento della rete con WAAS abilitato, eseguire la procedura seguente:

1. Riattivare la funzionalità WAAS sui CNA WAAS e, se applicabile, sui router WCCP.

2. Se si è determinato che esiste un problema relativo a WAAS, abilitare ogni cluster AppNav e/o ANC singolarmente, per isolarlo come possibile causa del problema osservato.

3. Dopo aver abilitato ciascun ANC, eseguire gli stessi test di base della connettività di rete descritti nelle fasi precedenti e verificare se lo specifico ANC funziona correttamente. In questa fase, non devono preoccuparsi dei singoli nomi distinti. L'obiettivo in questa fase è determinare quali cluster e quali ANC specifiche stanno sperimentando un comportamento desiderato o indesiderato.

4. Una volta attivato e verificato ciascun ANC, disabilitarlo di nuovo in modo da poter abilitare quello successivo. L'attivazione e il test di ciascun ANC a turno consente di determinare quali richiedono ulteriore risoluzione dei problemi.

Questa tecnica di risoluzione dei problemi è applicabile soprattutto nelle situazioni in cui la configurazione WAAS sembra non solo non riuscire a ottimizzare, ma anche causare problemi con la normale connettività di rete.

Passaggio Di Un Traffico Specifico

Èpossibile passare attraverso un traffico specifico utilizzando un ACL di intercettazione o configurando il criterio AppNav per l'accesso.

- Creare un ACL che impedisca al traffico specifico di passare attraverso il router e autorizzi tutto il resto. In questo esempio, si desidera passare attraverso il traffico HTTP (porta di destinazione 80). Impostare l'elenco degli accessi alle intercettazioni ANC sull'ACL definito. Le connessioni destinate alla porta 80 vengono passate. È possibile utilizzare il comando **show statistics pass-through type appnav** per verificare che l'accesso sia in corso verificando che i contatori PT Intercept ACL siano in aumento.

```
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
```

- Configurare il criterio ANC in modo che il traffico di transito corrisponda a classi specifiche.

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

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

Disattivazione di un ANC inline

Esistono diversi modi per disabilitare un ANC inline mettendolo in stato pass-through:

- Impostare l'elenco delle VLAN del bridge di intercettazione su none (nessuno). In Central Manager, scegliete un dispositivo ANC, quindi scegliete **Configura > Intercettazione > Configurazione intercettazione**. Selezionare l'interfaccia bridge e fare clic sull'icona **Modifica** barra delle applicazioni. Impostare il campo VLAN sul valore "none" (nessuno).
- Disabilitare il contesto di servizio contenente l'ANC. In Gestione centrale, scegliere un cluster, quindi fare clic sulla scheda Controller di AppNav, selezionare un ANC e fare clic sull'icona **Disabilita** barra delle applicazioni.
- Applicare un ACL di intercettazione con i criteri "deny ALL". Questo metodo è preferito. I primi due metodi interrompono le connessioni ottimizzate esistenti. Definire un ACL con i criteri deny ALL. In Central Manager, scegliere un dispositivo ANC, quindi **Configura > Intercettazione > Elenco accessi intercettazione** e selezionare l'elenco degli accessi negati all nell'elenco a discesa Elenco accessi intercettazione di AppNav Controller.

Per disabilitare l'intercettazione con un ACL dalla CLI, usare i seguenti comandi:

```
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
```

Attivazione dello stato pass-through per un ANC:

- Disabilita l'intercettazione WAAS, non le interfacce.
- Disabilita l'ottimizzazione WAAS.
- Impedisce il passaggio di tutto il traffico.

Disattivazione di un'ANC fuori percorso

Per disabilitare un ANC in esecuzione in modalità off-path, disabilitare il protocollo WCCP per l'ANC. È possibile eseguire questa azione sull'ANC o sul router di reindirizzamento o su entrambi. Nell'ANC è possibile disabilitare o eliminare i servizi WCCP oppure rimuovere il metodo di intercettazione o modificarlo da WCCP a un altro metodo.

Per disabilitare l'intercettazione WCCP, in Gestione centrale scegliere un dispositivo ANC, quindi

Configura > Intercettazione > Configurazione intercettazione. Deselezionare la casella di controllo Abilita servizio WCCP o fare clic sull'icona Rimuovi impostazioni nella barra delle applicazioni per rimuovere completamente le impostazioni di intercettazione WCCP (andranno perse).

Per disabilitare l'intercettazione WCCP dalla CLI, utilizzare i seguenti comandi:

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

In alcuni casi, è possibile che più ANC ricevano il traffico reindirizzato dallo stesso router. Per comodità, è possibile scegliere di disabilitare il protocollo WCCP sul router anziché sugli ANC. Il vantaggio è che è possibile rimuovere più ANC da una farm WCCP in un'unica operazione. Lo svantaggio è che non è possibile eseguire questa operazione da Gestione centrale WAAS.

Per disabilitare WCCP sul router, utilizzare la sintassi seguente:

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

Per riattivare WCCP sul router, utilizzare la sintassi seguente:

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

Su ciascun router WCCP, verificare che gli ANC che si è scelto di disabilitare non vengano visualizzati come client WCCP. Quando i servizi WCCP sono stati eliminati sul router, viene visualizzato l'output seguente.

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

Risoluzione dei problemi del cluster AppNav

Per risolvere i problemi relativi a un cluster AppNav, è possibile utilizzare gli strumenti seguenti:

- Avvisi di AppNav
- Monitoraggio del gestore centrale
- Comandi CLI di AppNav per il monitoraggio dello stato di cluster e dispositivi
- Comandi CLI di AppNav per il monitoraggio delle statistiche di distribuzione del flusso
- Traccia connessione
- Registrazione debug AppNav

Avvisi di AppNav

Cluster Membership Manager (CMM) genera i seguenti allarmi a causa di condizioni di errore:

- Cluster degradato (critico) - Visibilità parziale tra gli ANC. ANC passerà attraverso nuove connessioni.
- Convergenza non riuscita (critica) - Impossibile eseguire la convergenza su una vista stabile di ANC e WN. ANC passerà attraverso nuove connessioni.

- Join ANC non riuscito (critico): ANC non è riuscito a unirsi a un cluster esistente a causa del potenziale deterioramento del cluster con l'ANC in esso contenuto.
- Farm mista ANC (secondaria): le ANC nel cluster eseguono versioni diverse ma compatibili del protocollo del cluster.
- ANC non raggiungibile (principale): un'ANC configurata non è raggiungibile.
- WN non raggiungibile (principale): un WN configurato non è raggiungibile. Questo nome di dominio non viene utilizzato per il reindirizzamento del traffico.
- WN escluso (principale) - Un WN configurato è raggiungibile ma escluso perché uno o più ANC non lo possono vedere. Questo nome distinto non viene utilizzato per il reindirizzamento del traffico (nuove connessioni).

Gli allarmi possono essere visualizzati nel pannello Allarmi di Central Manager o utilizzando il comando **show alarms** EXEC su un dispositivo.

Nota: CMM è un componente interno di AppNav che gestisce il raggruppamento di ANC e WN in un cluster AppNav associato a un contesto del servizio.

Monitoraggio del gestore centrale

Èpossibile utilizzare Gestione centrale per verificare, monitorare e risolvere i problemi relativi ai cluster AppNav. Central Manager dispone di una vista globale di tutti i dispositivi WAAS registrati nella rete e consente di individuare rapidamente la maggior parte dei problemi di AppNav.

Dal menu Gestione centrale, scegliere **Cluster di AppNav >** *nome-cluster*. Nella finestra Home cluster vengono visualizzati la topologia del cluster (inclusi router WCCP e gateway), lo stato globale del cluster, lo stato del dispositivo, lo stato del gruppo di dispositivi e lo stato del collegamento.

Verificare innanzitutto che lo stato complessivo del cluster sia operativo.

Si noti che le icone ANC e WN mostrate in questo diagramma hanno lo stesso nome di dispositivo in quanto risiedono sullo stesso dispositivo. Su un'ANC che ottimizza anche il traffico come WAN, queste due funzioni sono mostrate come icone separate nel diagramma della topologia.

Un indicatore di avviso triangolare arancione viene visualizzato su qualsiasi dispositivo per il quale Central Manager potrebbe non disporre di informazioni aggiornate perché il dispositivo non ha risposto negli ultimi 30 secondi (potrebbe essere offline o irraggiungibile).

Èpossibile visualizzare in dettaglio lo stato a 360 gradi di qualsiasi dispositivo ANC o WAN posizionando il cursore sull'icona del dispositivo. La prima scheda visualizza gli allarmi sul dispositivo. È consigliabile risolvere gli eventuali allarmi che impediscono il corretto funzionamento del cluster.

Fare clic sulla scheda Intercettazione per verificare il metodo di intercettazione su ciascun ANC.

Se l'intercettazione non è attiva, lo stato viene visualizzato come segue:

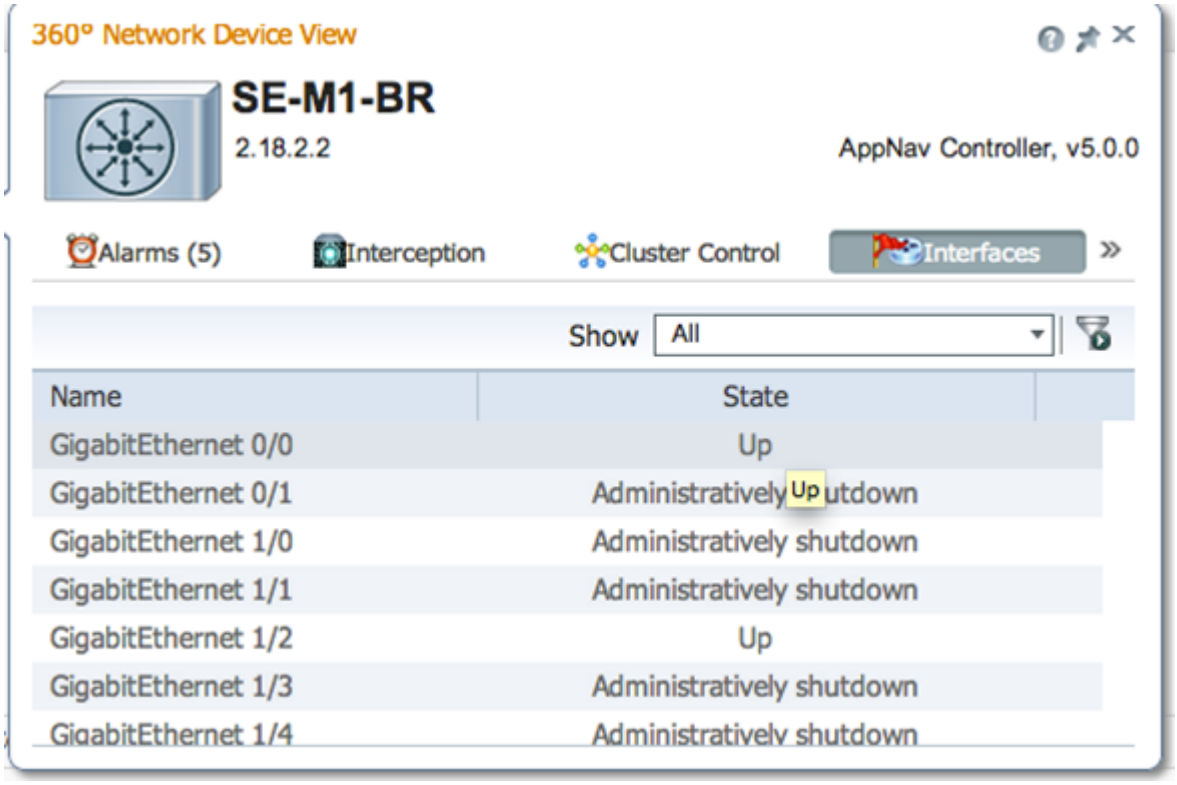
Fare clic sulla scheda Controllo cluster per visualizzare l'indirizzo IP e lo stato di ogni dispositivo del cluster che può essere visualizzato da questa scheda ANC. Ogni dispositivo ANC nel cluster deve avere lo stesso elenco di dispositivi. In caso contrario, indica un problema di configurazione o di rete.

Se tutte le ANC non possono vedersi, il cluster non è operativo e tutto il traffico viene trasmesso a causa dell'impossibilità del cluster di sincronizzare i flussi.

Se tutti gli ANC sono connessi ma hanno visualizzazioni diverse dei nomi principali, il cluster è in uno stato degradato. Il traffico è ancora distribuito, ma solo ai WN visibili da tutte le ANC.

Sono esclusi i nomi propri non visibili da tutti gli ANC.

Fare clic sulla scheda Interfacce per verificare lo stato delle interfacce fisiche e logiche nell'ANC.



Osservare la vista a 360 gradi su ogni nodo del cluster e verificare lo stato verde di tutti gli acceleratori nella scheda Ottimizzazione. Lo stato giallo di un acceleratore indica che l'acceleratore è in esecuzione ma non è in grado di servire nuove connessioni, ad esempio perché è sovraccarico o perché la relativa licenza è stata rimossa. Lo stato rosso indica che l'acceleratore non è in esecuzione. Se un acceleratore è giallo o rosso, è necessario risolverlo separatamente. Se la licenza Enterprise è mancante, la descrizione indica che la licenza System è stata revocata. Installare la licenza Enterprise nella pagina del dispositivo **Admin > History > License Management**.

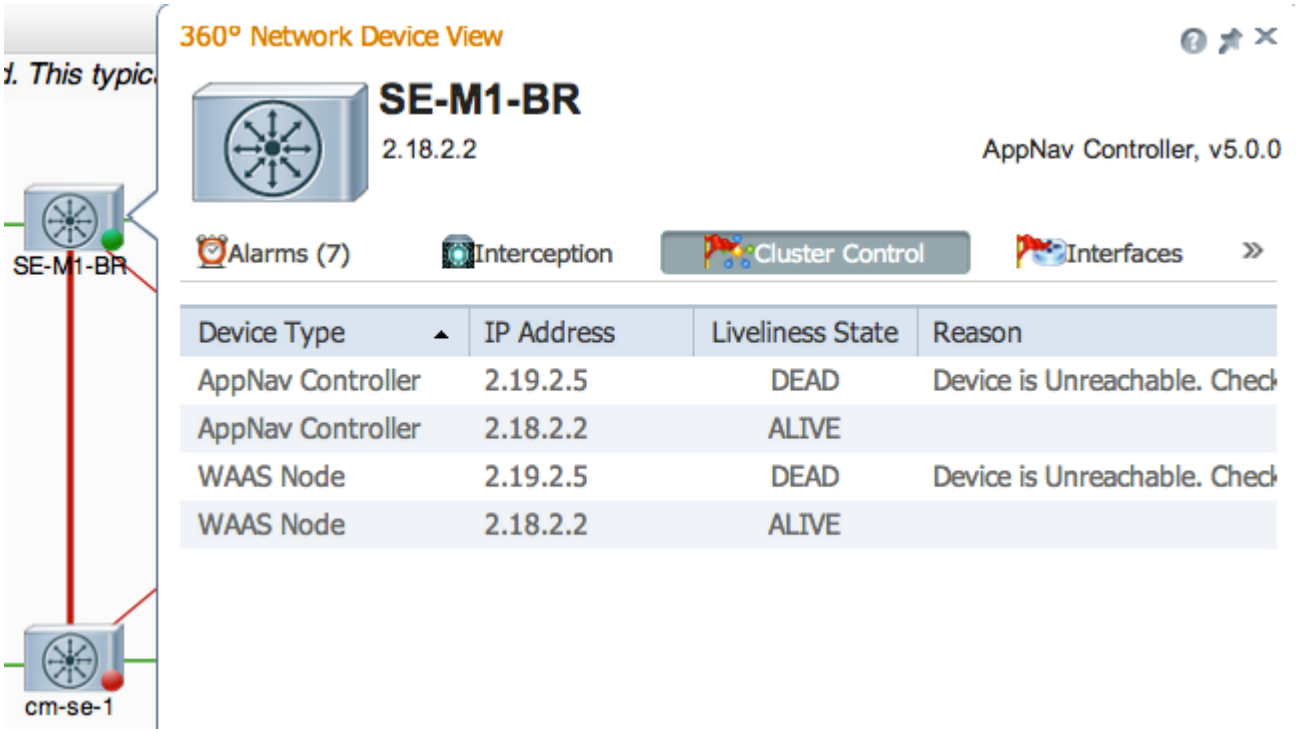
Un cluster diviso è il risultato di problemi di connettività tra le schede ANC nel cluster. Se il gestore centrale è in grado di comunicare con tutti gli ANC, può rilevare un cluster suddiviso, tuttavia, se non è in grado di comunicare con alcuni ANC, non può rilevare la suddivisione. L'allarme "Stato di

gestione non in linea" viene generato se il gestore centrale perde la connettività con qualsiasi dispositivo e il dispositivo viene visualizzato come non in linea in Gestione centrale.

Èconsigliabile separare le interfacce di gestione dalle interfacce dati per mantenere la connettività di gestione anche se un collegamento dati non è attivo.

In un cluster suddiviso, ogni sottocapitolo di ANC distribuisce in modo indipendente i flussi ai WNG che può vedere, ma poiché i flussi tra i sottocluster non sono coordinati, può causare la reimpostazione delle connessioni e una riduzione delle prestazioni complessive del cluster.

Controllare la scheda Controllo cluster di ciascun ANC per verificare se uno o più ANC non sono raggiungibili. L'allarme "Controller del servizio non raggiungibile" viene generato se due ANC che una volta potevano comunicare tra loro perdono la connettività, ma questa situazione non è l'unica causa di un cluster diviso, quindi è meglio controllare la scheda Controllo cluster di ogni ANC.



Se la spia di stato di un ANC è grigia, potrebbe essere disattivata. Verificare che tutti gli ANC siano abilitati facendo clic sulla scheda Controller di AppNav sotto il diagramma della topologia. Se un ANC non è abilitato, il suo stato è No. Per abilitarlo, fare clic sull'icona **Abilita** barra delle applicazioni.

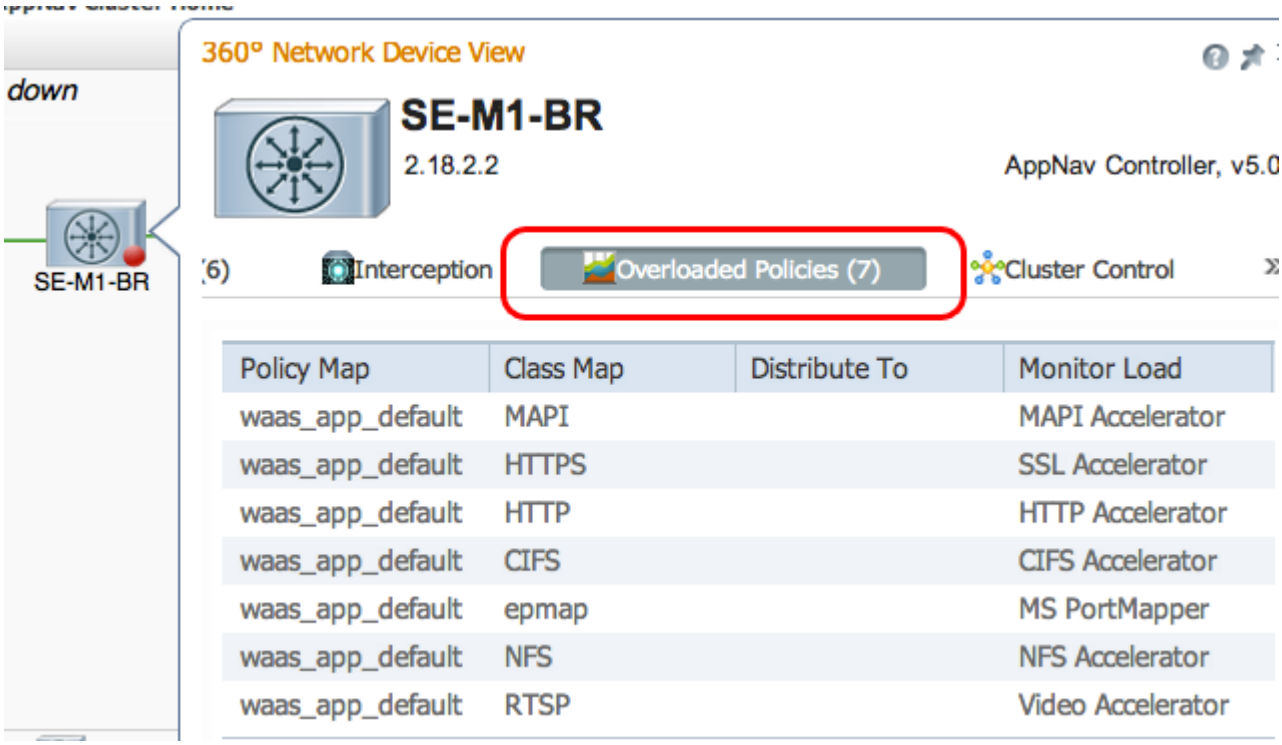
Controllare i criteri di AppNav su ogni ANC che non abbia una spia verde di stato. Se si posiziona il cursore sulla spia di stato di un dispositivo, viene visualizzata una descrizione dello stato o del problema, se rilevato.

Per controllare i criteri definiti, dal menu di Central Manager, scegliere **Configura > Criteri di AppNav** e fare clic sul pulsante **Gestisci**.

In genere è necessario assegnare un unico criterio a tutti gli ANC nel cluster. Il criterio predefinito è appnav_default. Selezionare il pulsante di opzione accanto a un criterio e fare clic sull'icona **Modifica** sulla barra delle applicazioni. Nel riquadro Criteri di AppNav vengono visualizzati gli ANC a cui è applicato il criterio selezionato. Se tutti gli ANC non sono visualizzati con un segno di spunta, fare clic sulla casella di spunta accanto a ciascun ANC non selezionato per assegnargli il criterio. Fare clic su **OK** per salvare le modifiche.

Dopo aver verificato le assegnazioni dei criteri, è possibile verificare le regole dei criteri nella pagina Criteri di AppNav che rimane visualizzata. Selezionare una regola dei criteri e fare clic sull'icona **Modifica** sulla barra delle applicazioni per modificarne la definizione.

Se uno o più criteri sono sovraccarichi, un'ANC potrebbe avere una spia di stato gialla o rossa. Controllare la scheda Criteri di overload della vista del dispositivo a 360 gradi per visualizzare un elenco dei criteri monitorati di overload.



Se un'ANC si unisce al cluster, viene visualizzata con una luce di stato gialla e lo stato di unione.

La scheda Intercettazione (Interception) della vista del dispositivo a 360 gradi mostra che il percorso di intercettazione è inattivo a causa dello stato di unione. L'intercettazione viene sospesa finché l'ANC non ha sincronizzato le proprie tabelle di flusso con le altre ANC ed è pronta ad accettare il traffico. Questo processo richiede in genere non più di due minuti.

Se si rimuove un ANC da un cluster, questo viene ancora visualizzato per alcuni minuti nel diagramma della topologia e come attivo nella scheda Controllo cluster, finché tutti gli ANC non concordano sulla nuova topologia del cluster. Non riceve alcun nuovo flusso in questo stato.

Comandi CLI di AppNav per il monitoraggio dello stato di cluster e dispositivi

Diversi comandi CLI sono utili per la risoluzione dei problemi su 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** *indirizzo-ip*
- **show service-insertion service-node** [*indirizzo-ip*]
- **show service-insertion service-node-group** *nome-gruppo*

Utilizzare i seguenti comandi su un WAN:

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

Èpossibile utilizzare il comando **show service-insertion service-context** su un CNA per verificare lo stato del contesto del servizio e la visualizzazione stabile dei dispositivi nel 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
```

Se il campo Stato intercettazione dispositivo (sopra) visualizza Arresto, significa che il CMM ha arrestato l'intercettazione perché l'ANC non è pronta a ricevere i flussi di traffico. Ad esempio, l'ANC potrebbe essere ancora nel processo di unione e il cluster non ha ancora sincronizzato i flussi.

I campi Vista stabile (sopra) elencano gli indirizzi IP degli ANC e dei WAN rilevati dal dispositivo ANC nell'ultima vista convergente del cluster. Vista utilizzata per le operazioni di distribuzione. I campi Visualizzazione corrente elencano i dispositivi annunciati dall'ANC nei messaggi heartbeat.

Èpossibile utilizzare il comando **show service-insertion appnav-controller-group** su un ANC per verificare lo stato di ciascun ANC del gruppo:

```
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
```

Per un elenco dei possibili stati ANC e join, vedere il comando **show service-insertion** nella *guida di riferimento dei comandi di Cisco Wide Area Application Services*.

Èpossibile utilizzare il comando **show service-insertion service-node** su un server ANC per visualizzare lo stato di un determinato server WAN nel 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
```

Èpossibile utilizzare il comando **show service-insertion service-node-group** su un server ANC per visualizzare lo stato di un determinato server WNG nel 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
```

Lo stato del primo WN dell'esempio precedente è Escluso, il che significa che il WN è visibile all'ANC ma viene escluso dal cluster perché uno o più ANC non possono visualizzarlo.

La tabella Disponibilità SNG per oggetto attivazione mostra se ogni oggetto attivazione è in grado di servire nuove connessioni. Un oggetto attivazione (AO) è disponibile se almeno un oggetto attivazione (WN) nel WNG ha lo stato VERDE per l'oggetto attivazione (AO).

Èpossibile utilizzare il comando **show service-insertion service-node** su un WN per visualizzare lo stato del WN:

```
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        Tim
e 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
```

Lo stato monitorato di un acceleratore è lo stato effettivo, ma lo stato riportato può essere diverso perché è il valore più basso dello stato del sistema o dello stato dell'acceleratore.

Per ulteriori informazioni sull'ottimizzazione della risoluzione dei problemi in un sito Web globale, vedere gli articoli Risoluzione dei problemi di ottimizzazione e Risoluzione dei problemi di accelerazione delle applicazioni.

Comandi CLI di AppNav per il monitoraggio delle statistiche di distribuzione del flusso

Diversi comandi CLI sono utili per la risoluzione dei problemi relativi ai criteri e alla distribuzione del flusso su un cavo ANC:

- **show policy-map type appnav** *policymap-name*: visualizza le regole dei criteri e il numero di accessi per ogni classe nella mappa dei criteri.
- **show class-map type appnav** *class-name*: visualizza i criteri di corrispondenza e i conteggi delle corrispondenze per ogni condizione di corrispondenza nella mappa di classe.
- **show policy-sub-class type appnav** *level1-class-name level2-class-name* — Mostra i criteri di corrispondenza e i conteggi delle corrispondenze per ogni condizione di corrispondenza in

una mappa di classe in una mappa di criteri AppNav nidificata.
- **show statistics class-map type appnav** *class-name*: visualizza le statistiche di intercettazione del traffico e distribuzione per una mappa di classe.
- **show statistics policy-sub-class type appnav** *level1-class-name level2-class-name* — Mostra le statistiche di intercettazione del traffico e distribuzione per una mappa di classe in una mappa di criteri AppNav nidificata.
- **show statistics pass-through type appnav**: visualizza le statistiche del traffico di AppNav per ciascun motivo di pass-through.
- **show appnav-controller flow-distribution**: visualizza il modo in cui un flusso ipotetico specifico viene classificato e distribuito da un'ANC in base alle condizioni di carico dinamico e ai criteri definiti. Questo comando può essere utile per verificare come un particolare flusso verrà gestito su un ANC e a quale classe appartiene.

Utilizzare questi comandi su un WAN per risolvere i problemi relativi alla distribuzione del flusso:

- **show statistics service-insertion service-node** *ip-address*: visualizza le statistiche degli acceleratori e del traffico distribuiti al server principale.
- **show statistics service-insertion service-node-group name** *group-name* — Mostra le statistiche per gli acceleratori e il traffico distribuiti al WNG.

Èpossibile utilizzare il comando **show statistics class-map type appnav** *class-name* su un ANC per risolvere i problemi di distribuzione del flusso, ad esempio per determinare il motivo per cui il traffico potrebbe essere lento per una determinata classe. Può trattarsi di una mappa di classe di applicazione come HTTP oppure, se tutto il traffico verso un ramo sembra lento, di una mappa di classe di affinità ramo. Di seguito è riportato un esempio per 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
  ...
```

I motivi di pass-through WAN nella sezione Indicato da SN vengono incrementati solo se l'offload pass-through è configurato su un WAN. In caso contrario, l'ANC non è a conoscenza del fatto che il nome del dominio sta passando attraverso una connessione e non lo conta.

Se l'opzione Connections: Intercettato dal contatore ANC non aumenta, c'è un problema di intercettazione. È possibile utilizzare l'utilità WAAS TcpTraceroute per risolvere i problemi relativi alla posizione dell'ANC nella rete, trovare percorsi asimmetrici e determinare il criterio applicato a una connessione. Per ulteriori informazioni, vedere la sezione Analisi connessione.

Comandi CLI di AppNav per il debug delle connessioni

Per eseguire il debug di una singola connessione o di un insieme di connessioni su un ANC, è possibile utilizzare il comando **show statistics appnav-controller connection** per visualizzare l'elenco delle connessioni attive.

```
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
```

Èpossibile filtrare l'elenco specificando l'indirizzo IP e/o le opzioni della porta del client o del server e visualizzare statistiche dettagliate sulle connessioni specificando la parola chiave **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
...
```

Èpossibile specificare l'opzione di riepilogo per visualizzare il numero di connessioni distribuite e pass-through attive.

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

Traccia connessione

Per facilitare la risoluzione dei problemi dei flussi di AppNav, è possibile utilizzare lo strumento Traccia connessione in Gestione centrale. Questo strumento mostra le seguenti informazioni per una connessione specifica:

- Se la connessione è stata passata o distribuita a un WNG
- Motivo di trasmissione, se applicabile
- WNG e WN a cui è stata distribuita la connessione
- Acceleratore monitorato per la connessione
- Mapping classi applicato

Per utilizzare lo strumento Traccia connessione, eseguire la procedura seguente:

1. Dal menu Central Manager, scegliere **AppNav Clusters >** *nome-cluster*, quindi scegliere **Monitor > Strumenti > Traccia connessione**.

2. Scegliere l'ANC, il dispositivo WAAS peer e specificare i criteri di corrispondenza della connessione.

3. Fare clic su **Trace** per visualizzare le connessioni corrispondenti.

WAAS TCP Traceroute è un altro strumento non specifico di AppNav che consente di risolvere i problemi relativi alla rete e alla connessione, inclusi i percorsi asimmetrici. È possibile utilizzarlo per trovare un elenco di nodi WAAS tra il client e il server e i criteri di ottimizzazione configurati e

applicati per una connessione. Da Central Manager, è possibile scegliere qualsiasi dispositivo nella rete WAAS da cui eseguire il traceroute. Per utilizzare lo strumento WAAS Central Manager TCP Traceroute, attenersi alla seguente procedura:

1. Dal menu WAAS Central Manager, scegliere **Monitor > Risoluzione dei problemi > WAAS Tcptraceroute**. In alternativa, è possibile scegliere prima un dispositivo e quindi questa voce di menu per eseguire il traceroute da quel dispositivo.

2. Dall'elenco a discesa Nodo WAAS, scegliere un dispositivo WAAS da cui eseguire il traceroute. (Questo elemento non viene visualizzato se il contesto del dispositivo è attivo.)

3. Nei campi IP destinazione e Porta destinazione, inserire l'indirizzo IP e la porta della destinazione verso cui si desidera eseguire il traceroute

4. Fare clic su **Esegui TCPTraceroute** per visualizzare i risultati.

I nodi WAAS nel percorso tracciato vengono visualizzati nella tabella sotto i campi. è possibile eseguire questa utility anche dalla CLI con il comando **waas-tcptrace**.

Registrazione debug AppNav

Il seguente file di registro è disponibile per la risoluzione dei problemi relativi a Gestione cluster AppNav:

- File registro di debug: /local1/errorlog/cmm-errorlog.current (e cmm-errorlog.*)

Per configurare e abilitare la registrazione di debug di Gestione cluster AppNav, utilizzare i comandi seguenti.

NOTA: La registrazione del debug richiede un utilizzo intensivo della CPU e può generare un'elevata quantità di output. Utilizzarlo con cautela e moderazione in un ambiente di produzione.

Èpossibile abilitare la registrazione dettagliata sul disco:

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

Di seguito sono riportate le opzioni per il debug di Gestione cluster (nella versione 5.0.1 e successive).

```
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
```

Èpossibile abilitare la registrazione di debug per Gestione cluster e quindi visualizzare la fine del registro degli errori di debug come indicato di seguito:

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

Èinoltre possibile abilitare il log di debug per FDM (Flow Distribution Manager) o FDA (Flow Distribution Agent) con i seguenti comandi:

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

FDM determina dove distribuire i flussi in base alle condizioni di carico dinamico e ai criteri dei nomi univoci. L'FDA raccoglie le informazioni sul carico WAN. I seguenti file di log sono disponibili per la risoluzione dei problemi relativi a FDM e FDA:

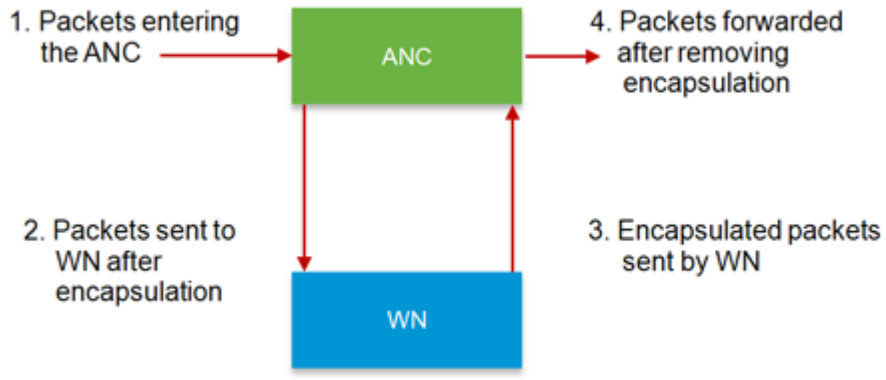
- File registro di debug: /local1/errorlog/fdm-errorlog.current (e fdm-errorlog.*)
- File registro di debug: /local1/errorlog/fda-errorlog.current (e fda-errorlog.*)

AppNav Packet Capture

Èstato introdotto un nuovo comando **packet-capture** per consentire l'acquisizione di pacchetti di dati sulle interfacce sul modulo di interfaccia del controller Cisco AppNav. Questo comando può anche acquisire pacchetti su altre interfacce e decodificare file di acquisizione pacchetti. Il comando **packet-capture** è preferito ai comandi deprecati **tcpdump** e **terminal**, che non possono acquisire pacchetti sul modulo di interfaccia di Cisco AppNav Controller. Per ulteriori informazioni sulla sintassi dei comandi, vedere la *guida di riferimento dei comandi di Cisco Wide Area Application Services*.

Nota: L'acquisizione del pacchetto o l'acquisizione del debug possono essere attive, ma non entrambe contemporaneamente.

I pacchetti di dati inviati tra gli ANC e i WAN sono incapsulati, come mostrato nel diagramma seguente.



Se si catturano i pacchetti nei punti 1 o 4 del diagramma, essi non sono incapsulati. Se si catturano i pacchetti ai punti 2 o 3, essi vengono incapsulati.

Di seguito è riportato un esempio di output per un'acquisizione del pacchetto incapsulato:

```
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)
```

Di seguito è riportato un esempio di output per un'acquisizione del pacchetto non incapsulato:

```
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 ...
...
```

Linee guida per l'acquisizione dei pacchetti:

- Un ACL di acquisizione dei pacchetti viene sempre applicato al pacchetto IP interno per i pacchetti incapsulati WCCP-GRE e SIA.
- L'acquisizione del pacchetto viene effettuata su tutte le interfacce ANC se non viene fornita l'interfaccia ANC per l'acquisizione del pacchetto.

Di seguito è riportato un esempio di output per un'acquisizione pacchetto su un'interfaccia 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 ...
```

Di seguito è riportato un esempio di decodifica di un file di acquisizione dei pacchetti:

```
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
```

Èpossibile specificare una porta src-ip/dst-ip/src-port/dst-port per filtrare i pacchetti:

anc# packet-capture decode source-ip 2.64.0.3 /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
```