WAAS - AppNav故障排除

章节：AppNav故障排除

本文介绍如何对AppNav部署进行故障排除。

指南

主要
了解
初步
故障
应用
排除
排除
排除
排除
排除
SSL
视频
排除
排除
排除
App
排除
串行
vWA
排除
排除

目录

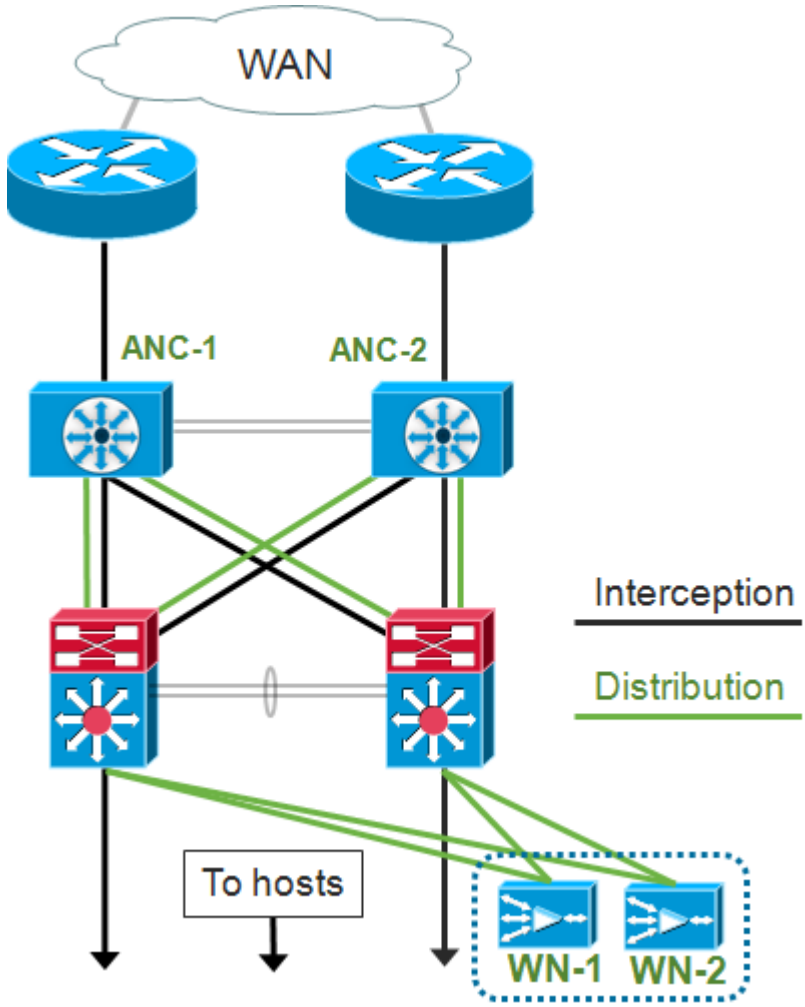
AppNav故障排除

Cisco WAAS AppNav通过使用AppNav控制器(ANC)在WAAS节点(WN)之间分配流量，以使用强大的类和策略机制进行优化，从而简化广域网优化的网络集成并大大降低对拦截交换机或路由器的依赖。您可以使用WAAS节点(WN)根据站点和/或应用优化流量。本文介绍如何对AppNav进行故障排除。

NOTE:WAAS版本5.0.1中引入了AppNav功能。此部分不适用于早期的WAAS版本。

内部路径（内联）拦截

在内联模式下，ANC位于网络流量路径中，在该路径中，ANC会拦截数据包并将其分发到WN。



内联部署的接口配置将侦听和分发角色分配给Cisco AppNav控制器接口模块上的独立接口。网桥组接口是拦截所必需的，它由两个或多个物理或端口通道接口或每个接口中的一个组成。网桥组接口没有无法布线的功能；即，在设备故障或断电后，它会失败，流量不会机械桥接。如果AppNav控制器接口模块、链路路径或与AppNav控制器接口模块的连接丢失或电源故障，AppNav会使用集群来提供高可用性。

注意：网桥接口不会阻止网桥协议数据单元(BPDU)数据包，如果冗余接口造成环路，其中一个接口会被生成树协议阻止。

排除内联拦截故障包括以下步骤：

- 通过检查网络设计，验证ANC的正确内联放置。如有必要，请使用基本工具（如ping和

traceroute）或第7层工具或应用程序来确认网络流量路径是否与预期一致。检查ANC的物理布线。
- 验证ANC是否已设置为内联侦听模式。
- 验证网桥组接口配置正确。

最后两个步骤可在中央管理器中或命令行中执行，但中央管理器是首选方法，并且首先进行说明。

在中央管理器中，选择**Devices >** *AppNavController*，然后选择**Configure > Interction > Interction Configuration**。验证Intelcing Method是否设置为Inline。

在同一窗口中，检验是否配置了网桥接口。如果需要网桥接口，请单击“**创建网桥**”以创建它。您最多可以为网桥组分配两个成员接口。您可以使用VLAN计算器根据包含或排除操作定义VLAN条目。请注意，网桥接口未分配IP地址。

使用“警报”面板或**show alarm** exec命令检查设备上是否发出任何与网桥相关的警报。bridge_down警报表示网桥中的一个或多个成员接口已关闭。

在CLI中，按照以下步骤配置内联操作：

1.将拦截方法设置为内联：

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

2.创建网桥组接口：

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

3.（可选）指定要拦截的VLAN列表（如果需要）：

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

4.将两个逻辑/物理接口添加到网桥组接口：

```
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
```

您可以使用**show bridge** exec命令检验网桥接口的运行状态，并查看网桥的统计信息。

```
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
```

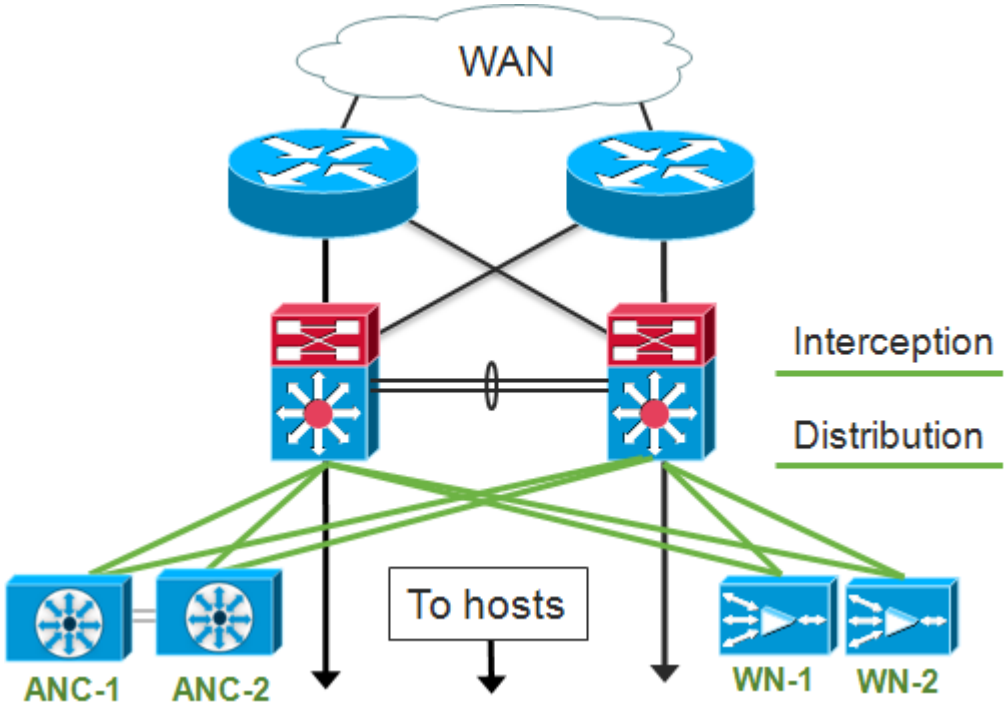
```
Interception Statistics:
                                GigabitEthernet 1/0    GigabitEthernet 1/1
Operation State                    :   Down           Down(lsp)           <<< Down due to LSP
Input Packets Forwarded/Bridged    :   16188          7845
Input Packets Redirected           :   5068           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
```

在上例中，Gig 1/0接口关闭，而Gig 1/1接口也因链路状态传播(LSP)而关闭。 您还可能看到Down(flow sync)，这意味着ANC正在加入集群并与集群中的其他ANC同步流信息。它会使拦截路径（网桥接口）关闭约两分钟，直到所有ANC都同步，以便能够正确分配现有流。

输出的下部显示成员接口的流量统计信息。

离线(WCCP)拦截

在WCCP模式下，WCCP路由器位于网络流量路径中，在该路径中，它们会拦截数据包并将其重定向到位于路径外的ANC。由于AppNav处理WAAS加速器之间的侦听处理、智能流分配和负载考虑，因此路由器上的WCCP配置得到了显着简化。



在路径外部署的接口配置中，拦截和分发角色可以在Cisco AppNav控制器接口模块上共享相同的接口，但不是必需的。

排除路径外拦截故障包括以下步骤：

- 检验WCCP路由器的正确位置，确保它们位于进出优化主机的流量路径中。您可以使用**show run**或**show wccp**命令来验证这些路由器是否与为WCCP配置的路由器相同。如有必要，请使用基本工具（如ping和traceroute）或第7层工具或应用程序来确认所有需要优化的流量都通过WCCP路由器。
- 使用中央管理器（首选）或CLI验证WAAS ANC上的WCCP配置。
- 使用路由器CLI检验重定向路由器上的WCCP配置。

要验证ANC上的WCCP配置，请在中央管理器中，选择**Devices >** *AppNavController*，然后选择**Configure > Interction > Interction Configuration**。

- 验证拦截方法是否已设置为WCCP。
- 验证是否选中Enable WCCP Service复选框。
- 验证Use Default Gateway as WCCP Router复选框已选中或WCCP Router字段中已列出WCCP路由器IP地址。
- 验证其他设置（如负载均衡掩码和重定向方法）是否已为部署正确配置。

在属于路由器WCCP场的ANC上检查是否存在任何与WCCP相关的警报。在中央管理器上，单击屏幕底部的“警报”面板，或在每台设备上使用**show alarm**命令查看警报。根据需要更改ANC或路由器上的配置，以更正任何警报情况。

在CLI中，按照以下步骤配置WCCP操作：

1.将拦截方法设置为wccp。

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

2.配置WCCP路由器列表，该列表包含参与WCCP场的路由器的IP地址。

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

3.配置WCCP服务ID。AppNav首选使用单个服务ID，但支持两个服务ID。

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

4.将已配置的路由器列表与WCCP服务关联。

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

5.配置WCCP分配方法（ANC仅支持掩码方法）。 如果未指定dst-ip-mask或src-ip-mask选项，则默认源IP掩码设置为f，目标IP掩码设置为0。

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

6.配置WCCP重定向方法（出口和返回方法自动设置为与重定向方法匹配，且不可为ANC配置）。您可以选择L2（默认）或GRE。L2要求ANC与路由器具有第2层连接，并且路由器也配置为进行第2层重定向。

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

7.启用WCCP服务。

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

使用show running-config命令检验每个ANC上**的WCCP拦**截。以下两个示例显示L2重定向和GRE重

定向的运行配置输出。

Show running-config wccp（用于L2重定向）：

```
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
```

显示running-config wccp（用于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
```

使用show wccp status命令验证每个ANC上的WCCP状态。

```
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
```

使用show wccp routers命令检验已响应WCCP场中的保持连接消息的路由器。

```
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-
```

使用show wccp clients命令验证WCCP场中每个ANC对其他ANC的视图，以及每个ANC可访问的路由器。

```
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
```

使用show statistics wccp命令验证每个ANC从场中的路由器接收**了数据包。**显示从每台路由器接收、通过和发送到每台路由器的流量的统计信息。场中所有路由器的累积统计信息显示在底部。类似的命令是**show wccp statistics**。请注意，“OE”是指此处的ANC设备。

```
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
```

在路由器上配置和检验WCCP拦截

要在WCCP场中的每台路由器上配置WCCP拦截，请执行以下步骤。

1.使用ip wccp router命令在路由器上配置**WCCP**服务。

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

2.在路由器LAN和WAN接口上配置WCCP拦截。如果在ANC上使用单个服务ID，则可以在两个接口

上配置相同的服务ID。

```
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.（可选）如果使用通用GRE出口，请配置隧道接口（仅当为ANC WCCP重定向方法选择GRE时）。

```
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
```

使用show wccp 命令检验场中每台路由器上的WCCP**配置。**

```
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
```

其他信息

有关其他信息，请参阅以下文档：

- WCCP网络与Cisco Catalyst 6500集成：成功部署的最佳实践建议
- 思科广域应用服务Web缓存通信协议重定向：思科路由器平台支持
- 在路由器上配置高级WCCP功能，请参阅《思*科广域应用服务配置指南*》
- 在WAE上配置WCCP，请参阅《思*科广域应用服务配置指南*》

网络连接故障排除

排除WAAS故障时，确定网络在禁用WAAS的情况下的行为可能会有所帮助。当流量不仅未能优化，而且根本无法通过时，这非常有帮助。在这些情况下，问题可能与WAAS无关。即使流量通过，此技术也可能有助于确定哪些WAAS设备需要进行故障排除。

在测试第3层连接之前，请验证AppNav控制器接口模块是否连接到正确的交换机端口。如果连接的交换机支持并启用了思科发现协议(CDP)，请运行命令**show cdp neighbors detail**，以验证与网络交换机的连接是否正确。

禁用WAAS可能并非在所有情况下都适用。如果某些流量正在优化，而某些流量未优化，则禁用WAAS可能是不可接受的，从而中断正在成功优化的流量。在这种情况下，拦截ACL或AppNav策略可用于通过遇到问题的特定类型的流量。有关详细信息，请参阅通过特定流量部分。

要禁用WAAS，内联模式和离开路径模式的步骤不同：

- 内联模式要求将拦截网桥置于直通状态。有关详细信息，请参阅禁用内联ANC部分。
- 离开路径模式需要禁用WCCP协议。有关详细信息，请参阅禁用非路径ANC部分。

在AppNav环境中，只需禁用ANC。WN无需禁用，因为它们不参与拦截。

禁用WAAS后，使用标准方法检查网络连接。

- 使用ping和traceroute等工具检查第3层连接。
- 检查应用行为以确定上层连接
- 如果网络遇到与启用WAAS时相同的连接问题，则问题很可能与WAAS无关。
- 如果网络在禁用WAAS的情况下工作正常，但启用WAAS时出现连接问题，则可能有一个或多个WAAS设备需要注意。下一步是将问题隔离到特定WAAS设备。
- 如果网络具有启用和不启用WAAS的连接，但没有优化，则可能有一个或多个WAAS设备需要注意。下一步是将问题隔离到特定WAAS设备。

要检查启用WAAS的网络行为，请执行以下步骤：

1.在WAAS ANC和WCCP路由器（如果适用）上重新启用WAAS功能。

2.如果您确定存在与WAAS相关的问题，请分别启用每个AppNav集群和/或ANC，将其隔离为所观察到问题的潜在原因。

3.启用每个ANC后，执行与前面步骤相同的基本网络连接测试，并注意此特定ANC是否似乎正常运行。在此阶段，不要关注单个WN。此阶段的目标是确定哪些群集以及哪些特定ANC正在经历期望或不期望的行为。

4.在启用和测试每个ANC时，请再次禁用它，以便启用下一个ANC。依次启用和测试每个ANC，可确定哪些ANC需要进一步故障排除。

此故障排除技术最适用于WAAS配置不仅未能优化，而且导致正常网络连接问题的情况。

通过特定流量

您可以通过使用拦截ACL或配置AppNav策略来通过特定流量。

- 创建ACL，拒绝要通过的特定流量并允许其他所有流量。在本例中，我们要通过HTTP流量（目标端口80）。 将ANC拦截访问列表设置为已定义的ACL。发往端口80的连接会通过。您可以使用**show statistics pass-throug type appnav**命令通过检查PT拦截ACL计数器是否在增加来验证是否发生了直通。

```
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
```

- 配置ANC策略以通过匹配特定类的流量。

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

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

禁用内联ANC

通过将内联ANC置于直通状态，可以通过以下几种方法禁用该ANC:

- 将侦听网桥VLAN列表设置为无。在中央管理器中，选择ANC设备，然后选择**Configure > Interction > Interction Configuration**。选择网桥接口并单击“编辑”**任务栏**图标。将VLAN字段设置为值“none”。
- 禁用包含ANC的服务上下文。在中央管理器中，选择一个集群，然后单击AppNav控制器选项卡

，选择ANC，然后单击禁用任**务栏**图标。
- 应用具有“拒绝所有”条件的拦截ACL。首选此方法。（前两种方法会中断现有的优化连接。）使用deny ALL条件定义ACL。在中央管理器中，选择ANC设备，然后选择**Configure > Interction > Interction Access List**，并在AppNav Controller Intercing Access List下拉列表中选择deny ALL access列表。

要从CLI禁用ACL拦截，请使用以下命令：

```
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
```

将非国大置于传递状态：

- 禁用WAAS拦截，而不是接口。
- 禁用所有WAAS优化。
- 导致所有流量不受影响地通过。

禁用离线ANC

要禁用在离开路径模式下运行的ANC，请禁用ANC的WCCP协议。您可以在ANC上或在重定向路由器上或在两者上执行此操作。在ANC上，可以禁用或删除WCCP服务，或者可以删除侦听方法或将其从WCCP更改为其他方法。

要禁用WCCP拦截，请在中央管理器中选择ANC设备，然后选择**Configure > Interction > Interction Configuration**。取消选中Enable WCCP Service复选框或点击Remove Settings任务栏图标以完全删除WCCP拦截设置（它们将丢失）。

要从CLI禁用WCCP拦截，请使用以下命令：

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

在某些情况下，可能有多个ANC从同一路由器接收重定向流量。为方便起见，您可以选择在路由器上禁用WCCP，而不是ANC。优点是，您只需一个步骤即可从WCCP场中删除多个ANC。缺点是您无法从WAAS Central Manager执行此操作。

要在路由器上禁用WCCP，请使用以下语法：

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

要在路由器上重新启用WCCP，请使用以下语法：

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

在每台WCCP路由器上，验证您选择禁用的ANC是否未显示为WCCP客户端。在路由器上删除WCCP服务时，将显示以下输出。

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

AppNav集群故障排除

要对AppNav集群进行故障排除，您可以使用以下工具：

- AppNav警报
- 中央管理器监控
- 用于监控集群和设备状态的AppNav CLI命令
- 用于监控流分布统计信息的AppNav CLI命令
- 连接跟踪
- AppNav调试日志记录

AppNav警报

集群成员管理器(CMM)因错误情况引发以下警报：

- 降级集群（严重） — ANC之间的部分可见性ANC将通过新连接。
- 收敛失败（严重） — ANC无法在ANC和WN的稳定视图上收敛。ANC将通过新连接。
- ANC加入失败（严重） — 由于集群中包含ANC的潜在降级，ANC无法加入现有集群。
- ANC混合场（次要） — 集群中的ANC运行不同但兼容的集群协议版本。
- ANC Unreachable(Major) — 配置的ANC无法访问。
- WN Unreachable(Major) — 已配置的WN不可达。此WN不用于流量重定向。
- WN Excluded(Major) — 已配置的WN可访问，但已排除，因为一个或多个其他ANC无法看到它。此WN不用于流量重定向（新连接）。

您可以在“中央管理器警报”面板中看到警报，或在设备上**使用show alarms** EXEC命令来查看警报。

注意：CMM是内部AppNav组件，用于管理ANC和WN的分组，将其分组到与服务上下文关联的AppNav集群中。

中央管理器监控

您可以使用中央管理器来验证、监控AppNav集群并排除其故障。Central Manager可以查看您网络中所有已注册的WAAS设备的全局视图，并可以快速帮助您找到大多数AppNav问题。

从“中央管理器”菜单中，选**择AppNav集群>*集群名称***。集群主窗口显示集群拓扑（包括WCCP和网关路由器）、整体集群状态、设备状态、设备组状态和链路状态。

首先，检验整个集群状态是否运行正常。

请注意，此图中显示的ANC和WN图标具有相同的设备名称，因为它们位于同一设备上。在同时作为WN优化流量的ANC上，这两个功能在拓扑图上显示为单独的图标。

在中央管理器可能没有当前信息的任何设备上显示橙色三角形警告指示器，因为设备在过去30秒内未响应（设备可能脱机或无法访问）。

通过将光标悬停在设备图标上，可以获得任何ANC或WN设备的详细360度状态视图。第一个选项卡显示设备上的警报。您应该解决阻止正确群集操作的任何警报。

单击Insection选项卡，验证每个ANC上的设备拦截方法。

如果侦听关闭，状态显示如下：

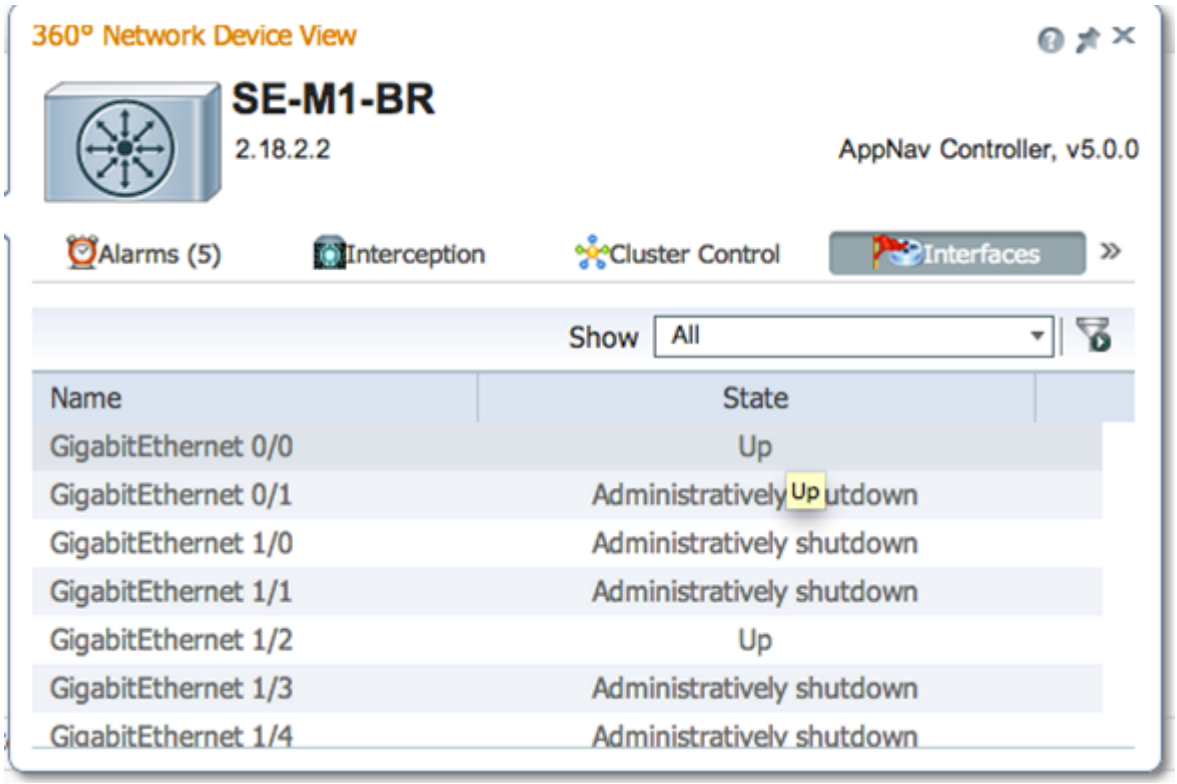
单击Cluster Control（集群控制）选项卡，查看此ANC可以看到的集群中每台设备的IP地址和状态。集群中的每个ANC应具有相同的设备列表。否则，表示配置或网络问题。

如果所有ANC无法彼此看到，则集群无法运行，并且由于集群无法同步流，所有流量都会通过。

如果所有ANC都已连接，但WN的视图不同，则集群处于降级状态。流量仍然分布，但仅分布到所有ANC看到的WN。

所有ANC未看到的所有WN均被排除。

单击Interfaces（接口）选项卡，验证ANC上物理接口和逻辑接口的状态。



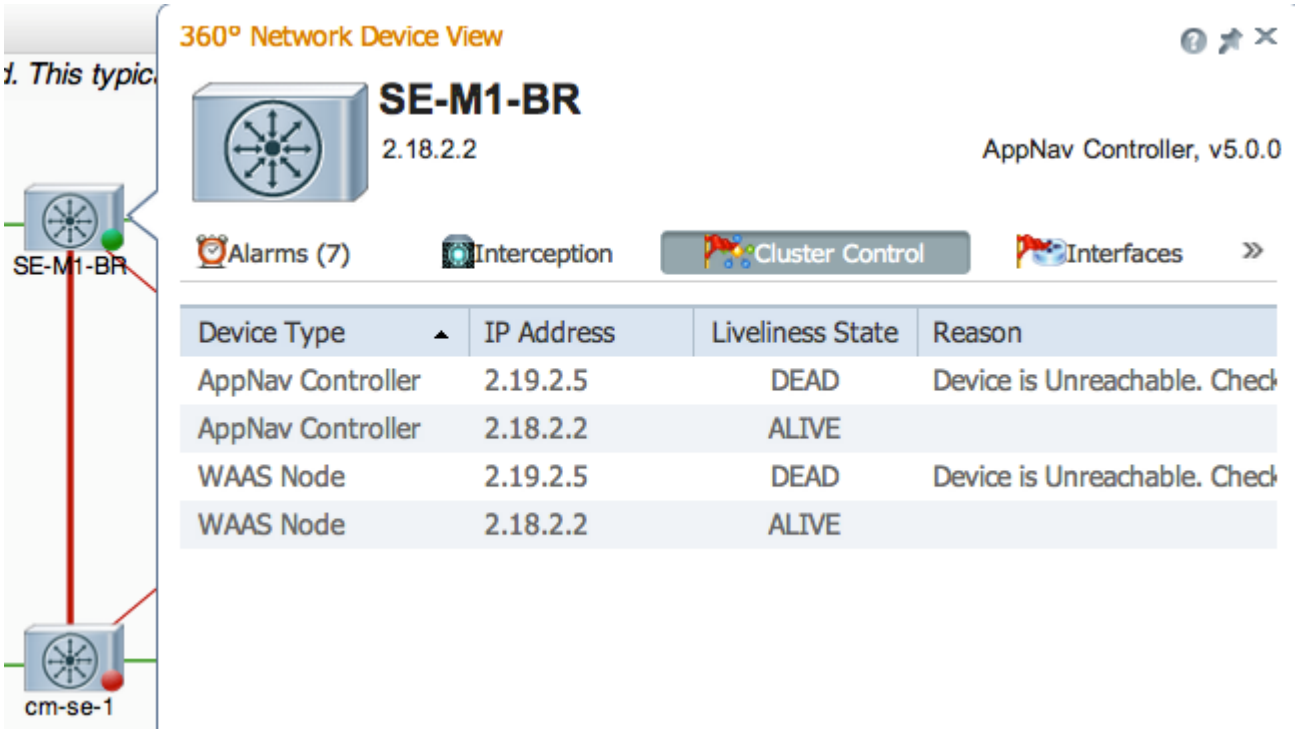
查看集群中每个WN的360度视图，并在“优化”选项卡中验证所有加速器的绿色状态。加速器的黄色状态表示加速器正在运行，但无法为新连接提供服务，例如，由于加速器过载或其许可证已被删除。红色状态表示加速器未运行。如果任何加速器为黄色或红色，则必须对这些加速器进行单独的故障排除。如果缺少企业许可证，说明将写明系统许可证已撤销。在Admin > History > License Management **device页面安装企业**许可证。

分割集群由集群中ANC之间的连接问题导致。如果中央管理器可以与所有ANC通信，则它可以检测拆分集群，但是，如果它无法与某些ANC通信，则它无法检测拆分。如果中央管理器与任何设备失去连接，并且该设备在中央管理器中显示为脱机，则会发出“管理状态为脱机”警报。

最好将管理接口与数据接口分开，以便即使数据链路断开也保持管理连接。

在分割集群中，ANC的每个子集群将流独立地分发到它可以看到的WNG，但由于子集群之间的流不协调，它可能导致重置连接，并降低集群整体性能。

检查每个ANC的Cluster Control（集群控制）选项卡，查看是否无法访问一个或多个ANC。如果两个ANC之间曾经可以相互通信，但此情况并非拆分集群的唯一原因，因此最好检查每个ANC的Cluster Control（集群控制）选项卡，则会发出“Service controller is unreachable”警报。



如果ANC的状态指示灯为灰色，则可能会将其禁用。单击拓扑图下方的AppNav Controllers选项卡，检查是否已启用所有ANC。如果未启用ANC，则其“已启用”状态为“否”。您可以单击“启用”任**务栏**图标以启用ANC。

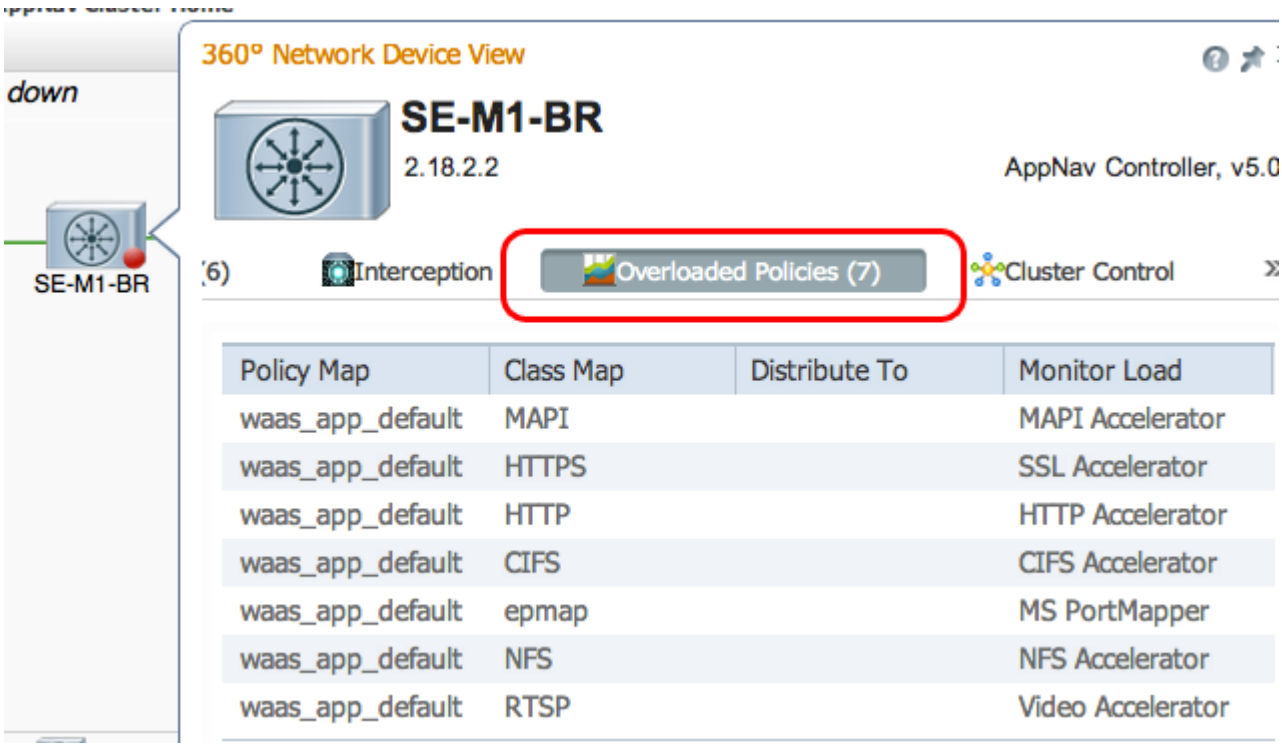
检查每个ANC上除绿色状态指示灯以外的其他ANC的AppNav策略。如果将光标悬停在设备上的状态指示灯上，则工具提示会告诉您状态或问题（如果检测到）。

要检查已定义的策略，请从Central Manager菜单中选择Configure **> AppNav Policies，**然后单击Manage**按**钮。

通常应该为集群中的所有ANC分配一个策略。默认策略名为appnav_default。选择策略旁边的单选按钮，然后单击“编辑”**任务栏**图标。AppNav Policy窗格将显示应用所选策略的ANC。如果所有ANC未显示复选标记，请点击每个未选中的ANC旁的复选框，将策略分配给它。点击 **确定，保存更改。**

在验证策略分配后，您可以验证AppNav Policies页面中保留显示的策略规则。选择任何策略规则，然后单击“编**辑”**任务栏图标以更改其定义。

如果一个或多个策略超载，ANC可能会显示黄色或红色状态指示灯。检查360度设备视图的过载策略选项卡，查看过载的受监控策略列表。



如果ANC正在加入集群，则显示为黄色状态指示灯和加入状态。

360度设备视图的“拦截”(Istection)选项卡显示，由于连接状态，拦截路径已关闭。拦截将保持不变，直到ANC将其流表与其他ANC同步并准备好接受流量。此过程通常不超过两分钟。

如果从集群中删除ANC，则拓扑图中仍会显示该ANC几分钟，并在“集群控制”选项卡中显示为活动状态，直到所有ANC都同意新集群拓扑。在此状态下，它不会收到任何新流。

用于监控集群和设备状态的AppNav CLI命令

几个CLI命令对ANC上的故障排除非常有用：

- **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** *IP地址*
- **show service-insertion service-node** [*ip-address*]
- **show service-insertion service-node-group** *组名*

在WN上使用以下命令：

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

在ANC上，可以**使用show service-insertion service-context**命令查看集群中设备的服务上下文状态和稳定视图：

```
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
```

如果Device Insection State字段（以上）显示Shutdown，则表示CMM已关闭拦截，因为此ANC未准备好接收流量。例如，ANC可能仍在加入过程中，并且集群尚未同步流。

“稳定视图”(Stable View)字段（上图）列出此ANC设备在集群的最后一个融合视图中看到的ANC和WN的IP地址。这是用于分配操作的视图。“当前视图”字段列出此ANC在其心跳消息中通告的设备。

在ANC上，可**以使用show service-insertion appnav-controller-group命令查看ANC组中每个ANC的状态：**

```
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
```

有关可能的ANC状态和加入状态的列表，请参阅《思科广域应用服务**命令参考》中的**show service-insertion*命令*。

在ANC上，可**以使用show service-insertion service-node**命令查看集群中特定WN的状态：

```
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
```

在ANC上，可以使用show service-insertion service-node-group命令查看集群中特定WNG的状态：

```
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
```

上例中的第一个WN的状态为Excluded，这意味着ANC可以看到WN，但它被从集群中排除，因为一个或多个其他ANC无法看到它。

每个AO的SNG可用性表显示每个AO是否能够为新连接提供服务。如果WNG中的至少一个WN具有AO的绿色状态，则AO可用。

您可以在WN上使用show service-insertion service-node命令查看WN的状态：

```
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
```

加速器的监控状态是其实际状态，但报告的状态可能不同，因为它是系统状态或加速器状态的较低值。

有关WN上的故障排除优化的详细信息，请参阅故障排除优化和排除应用加速故障文章。

用于监控流分布统计信息的AppNav CLI命令

几个CLI命令对ANC上的策略和流分布进行故障排除非常有用：

- **show policy-map type appnav** *policymap-name* **— 显示策略映射中每个类的策略规则和命中计数。**
- **show class-map type appnav class-name** — *显示类映射中每个匹配条件的匹配条件和命中计数。*
- **show policy-sub-class type appnav** *level1-class-name level2-class-name — 显示嵌套AppNav策略映射中类映射中每个匹配条件的匹配条件和命中计数。*
- **show statistics class-map type appnav class-name** — 显示类映射的流量拦截和分布统计信息。
- **show statistics policy-sub-class type appnav** *level1-class-name level2-class-name* — 显示嵌套AppNav策略映射中类映射的流量拦截和分发统计信息。
- **show statistics pass-through type appnav** — 显示每个直通原因的AppNav流量统计信息。
- **show appnav-controller flow-distribution** — 显示如何根据定义的策略和动态负载条件由ANC对特定假设流进行分类和分配。此命令可用于验证ANC上如何处理特定流及其所属的类。

在WN上使用以下命令排除流量分配故障：

- **show statistics service-insertion service-node** *ip-address* — 显示分发到WN的加速器和流量的统计信息。
- **show statistics service-insertion service-node-group name** *group-name* — 显示分发到WNG的加速器和流量的统计信息。

可以在ANC**上使用show statistics class-map type appnav** *class-name*命令来排除流量分布故障，例如确定特定类的流量可能变慢的原因。这可能是应用类映射（如HTTP），或者，如果流向分支的所有流量看起来都很慢，则可能是分支关联类映射。以下是HTTP类的示例：

```
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
  ...
```

仅当在WN上配置了直通分流时，“由SN指示”部分中的WN直通原因才会增加。否则，ANC不知道WN正在通过连接，并且不计算它。

如果连接：被ANC计数器截获的数据没有增加，存在截获问题。您可以使用WAAS

TcpTraceroute实用程序排除ANC在网络中的放置故障，查找非对称路径并确定应用于连接的策略。有关详细信息，请参阅“连接跟踪”部分。

用于调试连接的AppNav CLI命令

要调试ANC上的单个连接或连接集，可以使用**show statistics appnav-controller connection**命令显示活动连接列表。

```
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
```

您可以通过指定客户端或服务器IP地址和/或端口选项来过滤列表，也可以通过指定detail关键字来显示有关连接的详细**统计**信息。

```
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
...
```

您可以指定摘要选项以显示活动分布式和直通连接的数量。

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

连接跟踪

要帮助排除AppNav流的故障，可以在中央管理器中使用连接跟踪工具。此工具显示特定连接的以下信息：

- 如果连接通过或分发到WNG
- 传递原因（如果适用）
- 连接分发到的WNG和WN
- 为连接监控的加速器
- 已应用类映射

要使用“连接跟踪”工具，请执行以下步骤：

1.从“中央管理器”菜单中，选择**AppNav Clusters >** *cluster-name，然*后选择监**控器>工具>连接跟踪**。

2.选择ANC、对等WAAS设备，并指定连接匹配条件。

3.单击“跟**踪”**以显示匹配的连接。

WAAS TCP Traceroute是另一种不特定于AppNav的工具，可帮助您排除网络和连接问题（包括非对称路径）。您可以使用它查找客户端和服务器之间的WAAS节点列表，以及连接的已配置和已应用的优化策略。从Central Manager中，您可以选择WAAS网络中运行traceroute的任何设备。要使用WAAS Central Manager TCP Traceroute工具，请执行以下步骤：

1.从WAAS Central Manager菜单中，选择Monitor > Troubleshoot > WAAS Tcptraceroute。或者，您可以先选择设备，然后选择此菜单项从该设备运行traceroute。

2.从WAAS Node下拉列表中，选择要从中运行traceroute的WAAS设备。（如果您在设备上下文中，则不显示此项目。）

3.在“目标IP”和“目标端口”字段中，输入要运行traceroute的目标的IP地址和端口

4.单击“运**行TCPTraceroute”**以显示结果。

跟踪路径中的WAAS节点显示在字段下方的表中。您还可以使用waas-tcptrace命令从CLI运**行此实用**程序。

AppNav调试日志记录

以下日志文件可用于排除AppNav群集管理器问题：

- 调试日志文件：/local1/errorlog/cmm-errorlog.current（和cmm-errorlog.*）

要设置并启用AppNav集群管理器的调试日志记录，请使用以下命令。

NOTE:调试日志记录占用大量CPU资源，并且可以生成大量输出。在生产环境中谨慎、谨慎地使用它。

您可以启用对磁盘的详细日志记录：

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

集群管理器调试（在5.0.1及更高版本上）的选项如下：

```
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
```

您可以为集群管理器启用调试日志记录，然后显示调试错误日志的结束，如下所示：

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

您还可以使用以下命令为流分配管理器(FDM)或流分配代理(FDA)启用调试日志记录：

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

FDM根据WN的策略和动态负载条件确定分发流的位置。FDA收集WN负载信息。以下日志文件可用于排除FDM和FDA问题：

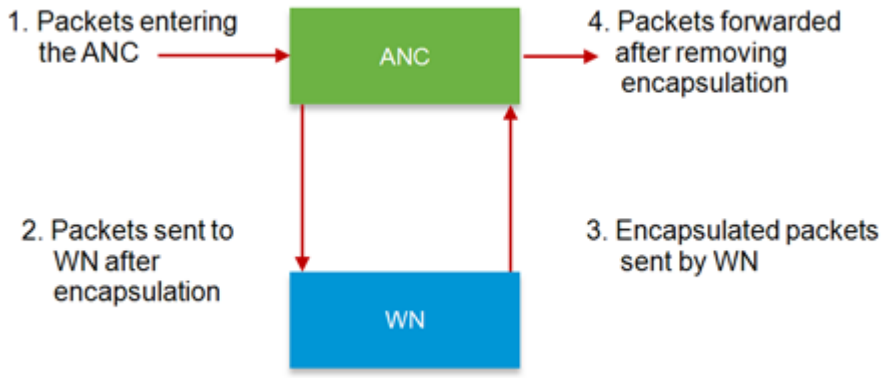
- 调试日志文件：/local1/errorlog/fdm-errorlog.current（和fdm-errorlog.*）
- 调试日志文件：/local1/errorlog/fda-errorlog.current（和fda-errorlog.*）

AppNav数据包捕获

引入了新的**packet-capture**命令，以允许捕获Cisco AppNav控制器接口模块接口上的数据包。此命令还可以捕获其他接口上的数据包，并可以解码数据包捕获文件。**packet-capture**命令优先于**弃用的命令tcpdump**和**tethereal**，后者无法在Cisco AppNav控制器接口模块上捕获数据包。有关命令*语法的详细信息，请参阅《思科广域应*用服务命令参考》。

注意：数据包捕获或调试捕获都可以处于活动状态，但不能同时同时进行。

ANC和WN之间发送的数据包将进行封装，如下图所示。



如果在图中的第1点或第4点捕获数据包，则它们将解封。如果在第2点或第3点捕获数据包，则会封装这些数据包。

以下是封装数据包捕获的输出示例：

```
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)
```

以下是未封装数据包捕获的输出示例：

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

数据包捕获指南：

- 数据包捕获ACL始终应用于WCCP-GRE和SIA封装数据包的内部IP数据包。
- 如果未提供用于数据包捕获的ANC接口，则在所有ANC接口上完成数据包捕获。

以下是WN接口上数据包捕获的输出示例：

```
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 ...
```

以下是解码数据包捕获文件的示例：

```
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
```

可以指定src-ip/dst-ip/src-port/dst-port以过滤数据包：

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
```