This article describes how to troubleshoot vWAAS.

Guide Contents
Main Article
Understanding the WAAS Architecture and Traffic Flow
Preliminary WAAS Troubleshooting
Troubleshooting Optimization
Troubleshooting Application Acceleration
Troubleshooting the CIFS AO
Troubleshooting the HTTP AO
Troubleshooting the EPM AO
Troubleshooting the MAPI AO
Troubleshooting the NFS AO
Troubleshooting the SSL AO
Troubleshooting the Video AO
Troubleshooting the Generic AO
Troubleshooting Overload Conditions
Troubleshooting WCCP
Troubleshooting AppNav
Troubleshooting Disk and Hardware Problems
Troubleshooting Serial Inline Clusters
Troubleshooting vWAAS
Troubleshooting WAAS Express
Troubleshooting NAM Integration

Contents

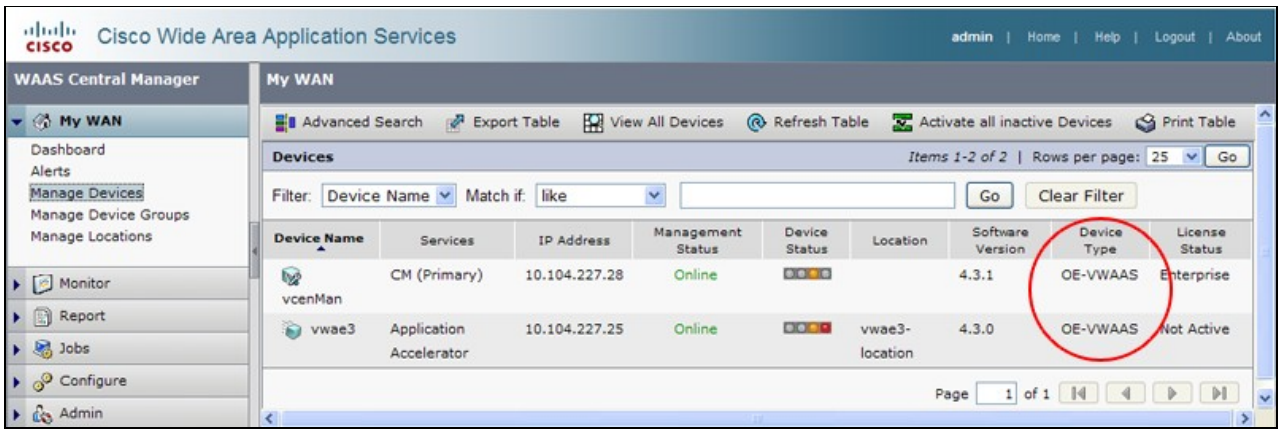
Virtual WAAS (vWAAS) implements a virtual WAAS appliance in VMware ESXi on a host server such as Cisco UCS.

NOTE: vWAAS was introduced in WAAS version 4.3.1. This section is not applicable to earlier WAAS versions.

Identifying a vWAAS Device

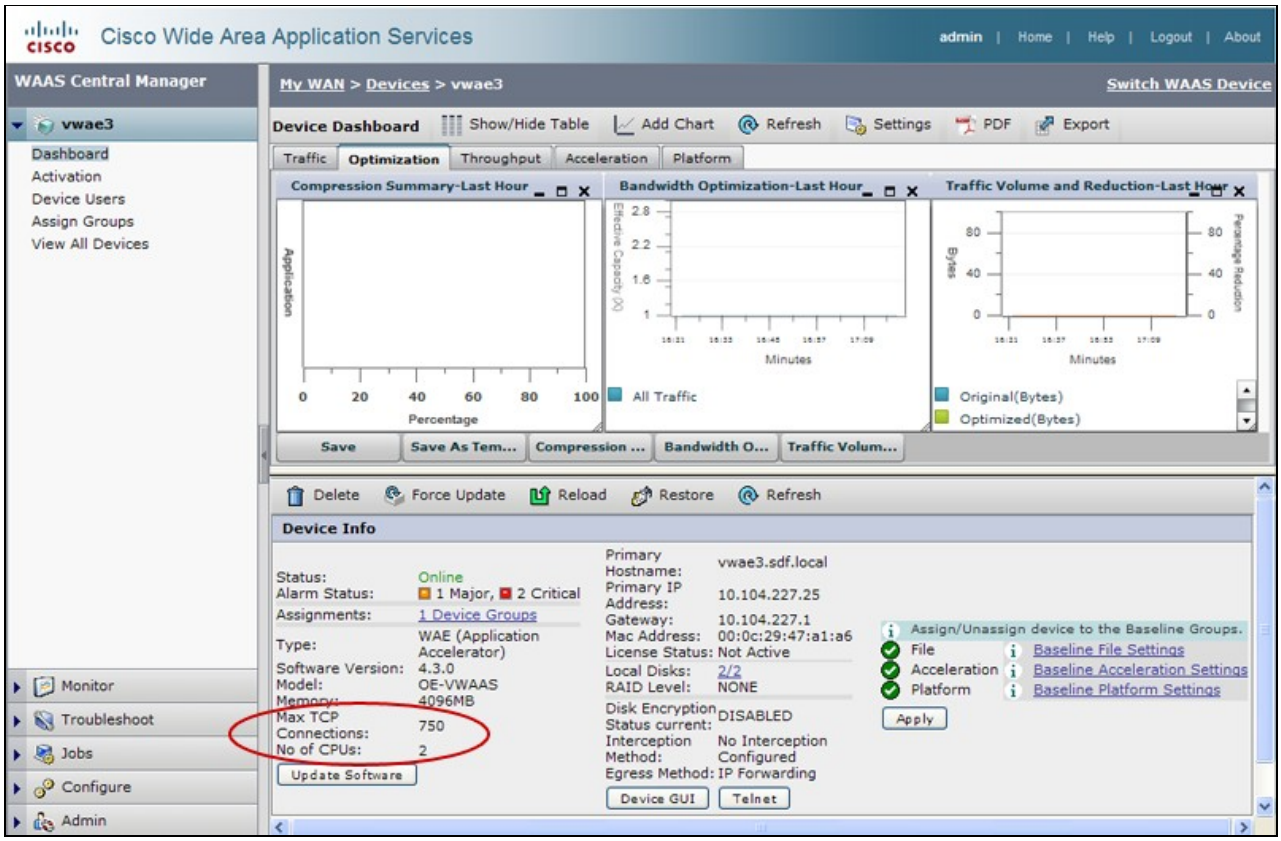
You can identify a vWAAS device from the Manage Devices page of the WAAS Central Manager. The device type appears as OE-VWAAS for all types of vWAAS devices. The **show version** and **show hardware** CLI commands also show the device Version as OE-VWAAS.

Figure 1. vWAAS Device Type



The model of the vWAAS device is determined from the number of CPUs and Maximum TCP Connections shown in the Device Dashboard window when you select the device from the Manage Devices page. These two fields are displayed only for vWAAS devices.

Figure 2. vWAAS Capabilities



The models are as follows:

- vWAAS-750: 2 CPUs, 750 maximum TCP connections
- vWAAS-6000: 4 CPUs, 6000 maximum TCP connections
- vWAAS-12000: 4 CPUs, 12000 maximum TCP connections
- vCM-100N: 2 CPUs, 100 maximum nodes
- vCM-2000N: 4 CPUs, 2000 maximum nodes

For vCM devices, you can use the **show hardware** command to determine the number of CPUs, which tells

you which model of vCM is installed.

Note: The vWAAS device shows 2 disks installed. The first, disk00, is 4 GB and emulates the flash storage in a physical WAAS device. The second, disk 01, emulates the hard disk in a physical WAAS device and varies in size depending on the vWAAS model.

The **show tfo detail** command also displays the maximum TCP connection limit:

```
vWAAS# show tfo detail
  Policy Engine Config Item            Value
  -------------------------            -----
  State                                Registered
  Default Action                       Use Policy
  Connection Limit                     750                <------ Max TCP connection limit
  Effective Limit                      750
  Keepalive timeout                    3.0 seconds
```

Troubleshooting vWAAS Device Registration

You must register each vWAAS device with the WAAS Central Manager for normal operation. If a vWAAS device is not registered with the Central Manager, it shows the Not registered alarm:

```
vWAAS# show alarms

Critical  Alarms:
-----------------
None

Major  Alarms:
--------------
        Alarm ID                 Module/Submodule              Instance
   ---------------             --------------------          ---------------
   1  notregistered             vwaas/model                                    <------Not
.  . .
```

To register the vWAAS device with the Central Manager, use the **cms enable** global configuration command on the vWAAS device:

```
vWAAS# config
vWAAS(config)#  cms enable
Registering  WAAS Application Engine...
Sending  device registration request to  Central Manager with address 2.75.16.100
Please wait,  initializing CMS tables
Successfully initialized CMS tables
. . .
management  services enabled
```

You can verify the registration with the **show cms info** command:

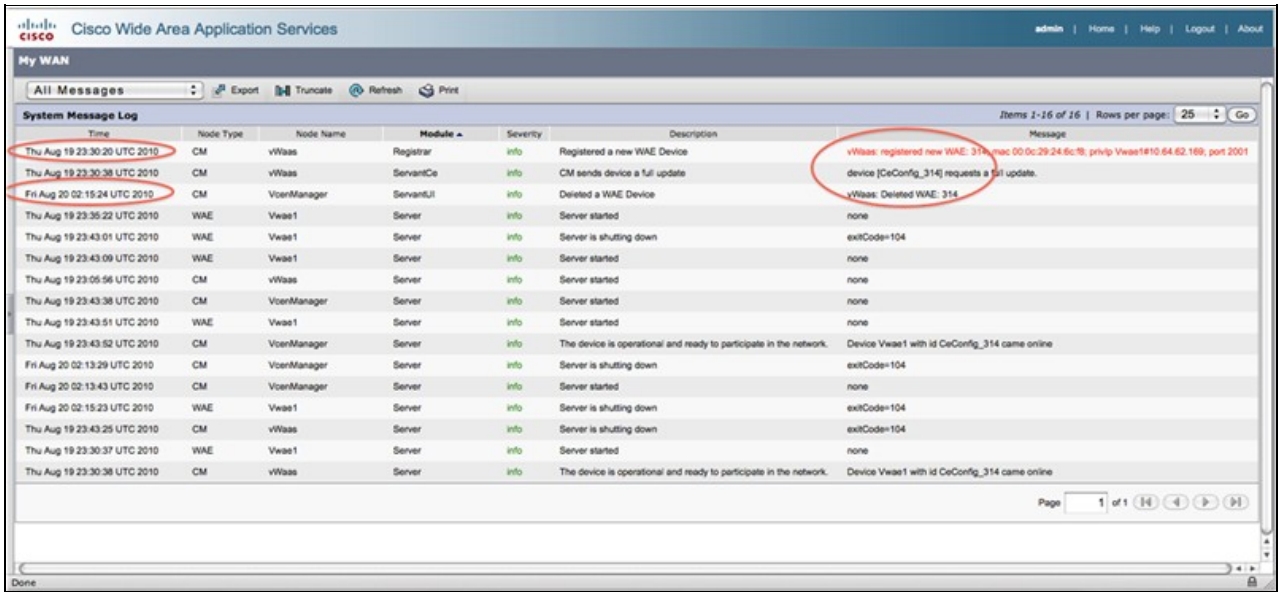
```
vWAAS# show cms info
Device  registration information :
Device Id                          =  1730
Device  registered as               = WAAS Application Engine
Current WAAS  Central Manager       = 2.75.16.100
Registered  with WAAS Central Manager = 2.75.16.100
Status                              = Online                        <----- Successful  registrat
Time of last config-sync            = Thu Aug 19 18:38:13 2010

CMS services  information :
```

```
Service cms_ce is running                                    <----- CMS service is runnir
```

vWAAS device registration and deregistration is logged in the system message log with a line that begins with "vWAAS:". You can view the system message log in the Central Manager by choosing **Admin > Logs > System Messages**.

Figure 3. vWAAS Registration Syslog Message



Verifying vWAAS Virtual Interfaces

Two virtual interfaces are available on vWAAS devices.

In the Central Manager *device* **> Configure > Network > Network Interfaces** page, the vWAAS interface type appears as Virtual (Port Channel, Standby, Inline, and GigabitEthernet are not applicable), which is similar to the GigabitEthernet . Some of the GigabitEthernet interface options, such as Port Channel, autosense, speed, mode, and standby, do not apply to virtual interfaces.

You can also see the virtual interfaces with the **show running-config** command:

```
VWAAS# show running-config interface
primary-interface Virtual 1/0
!
!
!
interface Virtual 1/0
 ip address 10.104.227.25 255.255.255.128
 exit
interface Virtual 2/0
 shutdown
 exit
```

Additional details are available with the **show interface virtual 1/0** or **show interface virtual 2/0** commands.

To make interface configuration changes, you can use the Central Manager Network Interfaces page or the **interface**, **ip**, and **primary-interface** configuration commands, as follows:

```
vWAAS# config
vWAAS(config)# interface virtual 1/0
vWAAS(config-if)# ip addr 10.10.10.15 255.255.255.0
vWAAS(config-if)# end
vWAAS# config
vWAAS(config)# ip default-gateway 10.10.10.1
vWAAS(config)# primary-interface virtual 1/0
vWAAS(config)# end
```

Troubleshooting vWAAS Networking

If you see no connections on the vWAAS device, check the vWAAS networking configuration in the vSphere Client. Is the vWAAS device connected to the correct vSwitch?

Using the vSphere Client, you can trace vWAAS network connectivity from the device page. Identify which network label the network adapter is connected to, determine the virtual switch that this network is connected to, and determine the physical NIC that is a member of this virtual switch. Verify that the configuration is correct.

Also make sure the virtual switch VLAN settings are correctly configured to reach the network.

Verify the configured IP address, netmask, default gateway, and primary interface on the vWAAS device. For details, see the previous section, "Verifying vWAAS Virtual Interfaces".

From the vWAAS device, ping the default gateway and Central Manager to make sure they are reachable.

Troubleshooting VPATH Interception

A vWAAS device can use VPATH or WCCP interception methods, but not both. To check if VPATH interception is enabled from the Central Manager, choose the vWAAS device, then choose **Configure > Interception > VPATH**. If the Enable VPATH box is checked, then it is enabled. WCCP must be disabled before VPATH can be enabled.

You can use the **vn-service vpath** global configuration command to enable or disable VPATH interception.

From the vWAAS device CLI, you can view VPATH status and statistics with the **show statistics vn-service vpath** command:

```
vWAAS# show statistics vn-service vpath
VPATH Statistics
****************
Packet Statistics
-----------------
                                    VPATH Enabled = YES             <-----Should be YES
                              VPATH Packet received = 4783472       <-----Should be incrementing
             Optimized TCP Packets VPATH returned = 918762          <-----Should be incrementing
             WAAS Bypassed VPATH packets returned = 15537
VPATH encapsulated IP pkts(excluding TCP) returned = 0
        VPATH encapsulated Non-IP packets returned = 26
                           VPATH Fragments received = 0
                           VPATH Fragments returned = 0
  VPATH Packets returned when VPATH not configured = 0
                        Non-VPATH Packets received = 810022
Error Statistics
-----------------
                 VPATH intercepted packets dropped = 0
                          VPATH Packet CRC failures = 0
```

```
            VPATH packets with unsupported Version = 0
             VPATH packets with wrong request type = 0
```

To determine if VPATH is sending ARP requests, use the **tcpdump arp** command.

To display VPATH MAC address information for TCP flows, use the **show statistics connection egress-methods** command:

```
vWAAS# show statistics connection egress-methods
------------------------------------------------------------------------
|                        |         TUPLE         |          MATE       |
------------------------------------------------------------------------
Local-IP:Port               10.104.227.25:443       10.104.227.28:36052
Remote-IP:Port              10.104.227.28:36052     10.104.227.25:443
Directed Mode             No                      No
Egress method             IP Forwarding           IP Forwarding
VPATH mode                Yes                     Yes                      <-----VPATH connecti
WCCP Service|Bucket
Tuple Flags               NON-WCCP|L2|            NON-WCCP|L2|
Intercepting Device (ID):
  ID IP address
  ID MAC address
  ID IP address updates   0                       0
  ID MAC address updates  0                       0
  Egress Tunnel Dst
  VPATH MAC Address       00:02:3D:83:B5:03       00:02:3D:83:B5:03        <-----VPATH MAC addr
Memory address            0xffff8101078b1b80      0xffff8101078b1b80
. . .
```

Troubleshooting Undersized Alarm

If the proper memory and hard disk resources are not allocated to the vWAAS device, the following alarm is shown:

```
vWAAS# show alarms

Critical Alarms:
----------------
None

Major Alarms:
-------------
        Alarm ID                Module/Submodule             Instance
   ---------------            --------------------         ---------------
   1 undersized                 vwaas/model                   memory            <-----Undersize
. . .
```

You should never see this alarm if you are using valid OVA files to deploy vWAAS. If you see this alarm, delete the vWAAS VM and redeploy it using a valid OVA file.