Troubleshooting CPS vDRA

Overview

CPS vDRA is a functional element that ensures that all Diameter sessions established over Gx, Rx interfaces and for unsolicited application reporting, the Sd interface for a certain IP-CAN session reach the same PCRF or destined PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm.

General Troubleshooting

Run the following command in CLI to view the diagnostics status. Verify that the status of all the nodes is in passing state.

```
admin@orchestrator[master-0]# show system diagnostics status
```

Run the following command in CLI to view the docker engines status. Verify that all docker engines are in CONNECTED state.

```
admin@orchestrator[master-0]# show docker engine
```

Diameter Troubleshooting and Connections

For messages belonging to particular interface, CPS vDRA should be ready to make diameter connection on the configured application port. As CPS vDRA acts as a server, it should be listening on ports for different applications to accept any incoming diameter requests for the application.

If you are facing problems making diameter connections, check for the following configuration:

DRA Plug-in Configuration in DRA Policy Builder (PB)

Figure 1: DRA Endpoints

Dra Endpoints

*Vm Host Name	*Ip Address	*Base Port	*Realm	*Fqdn	*Enabled	*Application
lb01	80.80.80.10	3868	dra.cisco.com	dra	✓	Gx
lb01	80.80.80.10	4868	gx-dra2.cisco.com	gx-dra2	✓	Gx

Step 1 Check status of application base port on active policy director (lb). It should be listening to diameter connections externally on VIP and internally to Policy Servers (QNS).

```
[root@lb01 ~]# netstat -na | grep 3868
tcp        0      0 10.77.207.100:3868          0.0.0.0:*                   LISTEN
tcp        0      0 ::ffff:80.80.80.10:3868     :::*                        LISTEN
```

Step 2 Check `haproxy-diameter.cfg` file for proper entries:
For Step 1, on page 2 and Step 2, on page 2 configuration, the entries should be as follows:

```
[root@lb01 ~]# cat /etc/haproxy/haproxy-diameter.cfg
global
  daemon
  nbproc        1         # number of processing cores
  stats socket /tmp/haproxy-diameter
defaults
  timeout client    60000ms       # maximum inactivity time on the client side
  timeout server   180000ms       # maximum inactivity time on the server side
  timeout connect    5000ms       # maximum time to wait for a connection attempt to a server to
succeed
log             127.0.0.1       local1 err
listen diameter-int1
        bind 10.77.207.100:3868
        mode tcp
        option tcpka
        balance leastconn
        server lb01-A lb01:3868 check
        server lb01-B lb01:3869 check
        server lb01-C lb01:3870 check
listen diameter-int2
        bind 10.77.207.100:4868
        mode tcp
        option tcpka
        balance leastconn
        server lb01-A lb01:4868 check
        server lb01-B lb01:4869 check
        server lb01-C lb01:4870 check
listen stats_proxy_diameter lbvip01:5540
        mode http
        option httpclose
```

```
option abortonclose
# enable web-stats
stats enable
stats uri /haproxy-diam?stats
#stats auth        haproxy:cisco123
stats refresh     60s
stats hide-version
```

Step 3 Listen for diameter traffic by logging into lb01 and lb02 and execute the following command:

```
tcpdump -i any port 3868 -s 0 -vv
```

Troubleshooting Basics

Troubleshooting CPS vDRA consists of these types of basic tasks:

- Gathering Information
- Collecting Logs
- Running Traces

Diameter Error Codes and Scenarios

Table 1: Diameter Error Codes and Scenarios

Result-Code	Result-Code Value	Description
Informational		
DIAMETER_MULTI_ROUND_AUTH	1001	Subsequent messages triggered by client shall also used in Authentication and to get access of required resources. Generally used in Diameter NAS.
Success		
DIAMETER_SUCCESS	2001	Request processed Successfully.
DIAMETER_LIMITED_SUCCESS	2002	Request is processed but some more processing is required by Server to provide access to user.
Protocol Errors [E-bit set]		
DIAMETER_COMMAND _UNSUPPORTED	3001	Server returns it if Diameter Command-Code is un-recognized by server.

Result-Code	Result-Code Value	Description
DIAMETER_UNABLE _TO_DELIVER	3002	Message cannot be delivered because there is no Host with Diameter URI present in Destination-Host AVP in associated Realm.
DIAMETER_REALM_NOT _SERVED	3003	Intended Realm is not recognized.
DIAMETER_TOO_BUSY	3004	Shall return by server only when server unable to provide requested service, where all the pre-requisites are also met. Client should also send the request to alternate peer.
DIAMETER_LOOP_DETECTED	3005	-
DIAMETER_REDIRECT _INDICATION	3006	In Response from Redirect Agent.
DIAMETER_APPLICATION _UNSUPPORTED	3007	-
DIAMETER_INVALID_HDR_BITS	3008	It is sent when a request is received with invalid bits combination for considered command-code in DIAMETER Header structure. For example, Marking Proxy-Bit in CER message.
DIAMETER_INVALID_AVP_BITS	3009	It is sent when a request is received with invalid flag bits in an AVP.
DIAMETER_UNKNOWN_PEER	3010	A DIAMETER server can be configured whether it shall accept DIAMETER connection from all nodes or only from specific nodes. If it is configured to accept connection from specific nodes and receives CER from message from any node other than specified.
Transient Failures [Could not satisfy request at this moment]		
DIAMETER_AUTHENTICATION _REJECTED	4001	Returned by Server, most likely because of invalid password.
DIAMETER_OUT_OF_SPACE	4002	Returned by node, when it receives accounting information but unable to store it because of lack of memory.

Result-Code	Result-Code Value	Description
ELECTION_LOST	4003	Peer determines that it has lost election by comparing Origin-Host value received in CER with its own DIAMETER IDENTITY and found that received DIAMETER IDENTITY is higher.
Permanent Failures [To inform peer, request is failed, should not be attempted again]		
DIAMETER_AVP _UNSUPPORTED	5001	AVP marked with Mandatory Bit, but peer does not support it.
DIAMETER_UNKNOWN _SESSION_ID	5002	-
DIAMETER_AUTHORIZATION _REJECTED	5003	User can not be authorized. For example, Comes in AIA on s6a interface.
DIAMETER_INVALID_AVP_VALUE	5004	-
DIAMETER_MISSING_AVP	5005	Mandatory AVP in request message is missing.
DIAMETER_RESOURCES _EXCEEDED	5006	A request was received that cannot be authorized because the user has already expended allowed resources. An example of this error condition is a user that is restricted to one dial-up PPP port, attempts to establish a second PPP connection.
DIAMETER_CONTRADICTING _AVPS	5007	Server has identified that AVPs are present that are contradictory to each other.
DIAMETER_AVP_NOT_ALLOWED	5008	Message is received by node (Server) that contain AVP must not be present.
DIAMETER_AVP_OCCURS _TOO_MANY_TIMES	5009	If message contains the a AVP number of times that exceeds permitted occurrence of AVP in message definition.
DIAMETER_NO_COMMON _APPLICATION	5010	In response of CER if no common application supported between the peers.
DIAMETER_UNSUPPORTED _VERSION	5011	Self explanatory.

Result-Code	Result-Code Value	Description
DIAMETER_UNABLE _TO_COMPLY	5012	Message rejected because of unspecified reasons.
DIAMETER_INVALID_BIT _IN_HEADER	5013	When an unrecognized bit in the Diameter header is set to one.
DIAMETER_INVALID _AVP_LENGTH	5014	Self explanatory.
DIAMETER_INVALID _MESSAGE_LENGTH	5015	Self explanatory.
DIAMETER_INVALID_AVP _BIT_COMBO	5016	For example, marking AVP to Mandatory while message definition doesn't say so.
DIAMETER_NO_COMMON _SECURITY	5017	In response of CER if no common security mechanism supported between the peers.

Policy DRA Error Codes

Non-compliant Diameter requests are checked for errors in routing AVP and P-bits. The following table describes the error codes and the reasons for errors in Diameter requests:

Table 2: Policy DRA Error Codes

Policy DRA Error String	Error Code	Sub-code	Description
No application route found	3002	001	Route List Availability Status is “Unavailable”
Timeout triggered	3002	002	Timeout triggered
No peer group	3002	003	No peer group
Session DB Error	3002	004	Session DB Error
Binding DB Error	3002	005	Binding DB Error
No key for binding lookup	3002	006	No key for binding lookup
Binding not found	3002	007	Binding not found
Message loop detected	3002	008	Message loop detected

Policy DRA Error String	Error Code	Sub-code	Description
Parsing exception with message	3002	009	Parsing exception with message
CRD DB Error	3002	010	CRD DB Error
Retries exceeded	3002	011	Retries exceeded
No peer route	3002	012	No peer routing rule found for a Realm-only or non-peer Destination-Host
P-bit not set	3002	013	P-bit in the Request message is set to “0”
Missing Origin-Host AVP	5005	014	Mandatory Origin-Host AVP missing
Missing Origin-Realm AVP	5005	015	Mandatory Origin-Realm AVP missing
Missing Destination-Realm AVP	5005	016	Mandatory Destination-Realm AVP missing
No avp found in request for SLF lookup type	3002	101	No avp found in request for SLF lookup type
SLF DB Error	3002	102	SLF DB Error
SLF credential not found in DB	3002	103	SLF credential not found in DB
SLF Destination type not found in DB	3002	104	SLF Destination type not found in DB
Destination not found in SLF Mapping Table	3002	105	Destination not found in SLF Mapping Table

Common Troubleshooting Steps

Using TCPDUMP

Step 1 Run the following command to capture the packets on specific IP address:

```
admin@orchestrator[master-0]# debug packet-capture start
ip-address 192.169.22.158 port 9100 timer-seconds 230
```

Step 2 Run the following command to capture the packets on the host (executes tcpdump from host):

```
admin@orchestrator[master-0]# debug tcpdump
an-dra-director-0 gen1.pcap 200s -i any port 3868
```

Step 3 Run the following command to gather all the packet captures that were started:

```
admin@orchestrator[an-master]# debug packet-capture gather
directory test1
```

You can view all the gathered packet captures at the following URL:
https://<Master-IP>/orchestrator/downloads/debug/

CPS vDRA Logs

Step 1 Use the following command in CLI to view the consolidated application logs.

```
admin@orchestrator[master-0]# show log application
```

Step 2 Use the following command in CLI to view the consolidated engine logs.

```
admin@orchestrator[master-0]# show log engine
```

Counters and Statistics

Check for statistics generated at pcrfclient01/02 in `/var/broadhop/stats` and counters in beans at jmx terminal.

Frequently Encountered Troubles in CPS vDRA

Redis Not Working

Step 1 Check redis status by executing the following command:

```
[root@lb01 ~]# service redis status
redis-server (pid  22511) is running...
```

Step 2 Try starting redis process by executing the following command:

```
[root@lb01 ~]# service redis start
```

Step 3 Check the following entries in /etc/broadhop/draTopology.ini file at policy directors (lb) and Policy Servers (QNS) for redis connecting on ports 6379, 6380, 6381, 6382:

```
[root@lb02 ~]# cat /etc/broadhop/draTopology.ini
dra.redis.qserver.1=lb02:6379
dra.redis.qserver.2=lb02:6380
dra.redis.qserver.3=lb02:6381
dra.redis.qserver.4=lb02:6382
dra.redis.qserver.4=lb02:6383
dra.local-control-plane.redis.1=lb02:6379
dra.mongodb.binding.db.ipv6.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.ipv4.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.imsiapn.uri=mongodb://sessionmgr01:27718
dra.mongodb.pcap.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.session.uri=mongodb://sessionmgr01:27718
[root@lb02 ~]# cat /etc/broadhop/redisTopology.ini
dra.redis.qserver.1=lb02:6379
dra.redis.qserver.2=lb02:6380
dra.redis.qserver.3=lb02:6381
dra.redis.qserver.4=lb02:6382
dra.local-control-plane.redis.1=lb02:6379
```

Step 4 Redis process on active policy director (lb) should be established with all Policy Servers (QNS) as shown below:

```
[root@lb01 ~]# netstat -na | grep 6379
tcp        0      0 0.0.0.0:6379                0.0.0.0:*                   LISTEN
tcp        0      0 80.80.80.10:6379            80.80.80.10:37400           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38020           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38034           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37390           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38207           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.16:50597           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.14:35703           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.14:35711           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38188           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37375           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38174           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38229           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38211           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.14:35709           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.16:50590           ESTABLISHED
```

```
tcp        0      0 80.80.80.10:6379            80.80.80.10:38032           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38172           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.16:50605           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38204           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38213           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38223           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38044           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38187           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38205           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38211           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37672           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.14:35710           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.17:59833           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37388           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37389           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37662           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.17:59824           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.16:50596           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38210           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.15:49162           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38231           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38230           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.15:49159           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38152           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37659           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38208           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.17:59832           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.15:49161           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38206           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38212           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:38033           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37650           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.15:49160           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38155           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.10:37660           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.17:59831           ESTABLISHED
tcp        0      0 80.80.80.10:6379            80.80.80.11:38186           ESTABLISHED
tcp        0      0 :::6379                     :::*                        LISTEN
tcp        0      0 ::ffff:80.80.80.10:37660    ::ffff:80.80.80.10:6379     ESTABLISHED
```

Gx Bindings not happening on Mongo

Step 1 Check if the binding's exceptions are coming in `consolidated-qns.log` file.

Step 2 Check for the entry `-DdraBindingTier=true` in `qns.conf` file on all Policy Servers (QNS).

Step 3 Check for the entries in `/etc/broadhop/draTopology.ini` file.

```
dra.redis.qserver.1=lb02:6379
dra.redis.qserver.2=lb02:6380
```

```
dra.redis.qserver.3=lb02:6381
dra.redis.qserver.4=lb02:6382
dra.redis.qserver.4=lb02:6383
dra.local-control-plane.redis.1=lb02:6379
dra.mongodb.binding.db.ipv6.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.ipv4.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.imsiapn.uri=mongodb://sessionmgr01:27718
dra.mongodb.pcap.uri=mongodb://sessionmgr01:27718
dra.mongodb.binding.db.session.uri=mongodb://sessionmgr01:27718
```

For example, make sure if the primary binding server is 27718 only as per above example.

Step 4 Check for the Binding Keys entries in binding key type profile and the application attached to the profile.

Rx Call Failing at CPS vDRA

Step 1 Check for the Binding key Retriever for Rx Profile.

Step 2 Check if the Gx Binding is available for that Binding key.

Step 3 Check the `consolidated-qns.log` file if CPS vDRA is able to retrieve SRK from the bindings.

Step 4 Check for any exception in `consolidated-qns.log` file during binding retrieval.

Step 5 If Rx peer is available for the same SRK at CPS vDRA, CPS vDRA should forward the Rx message to that peer.

Step 6 Check the connection for that peer and proper entries in Peer Group, Peer Routing, Peer Group Peer and Rx_Routing for Rx New session rules.

CPS vDRA Forwarding Message to Wrong Peer

Step 1 Check the Control Center configuration in Gx_Routing for new session rules. Gx routing should have the AVP defined on the basis of which, one wants to route the traffic.

Step 2 Check whether the Control Center configuration for the Peer is bonded to correct Peer Group.

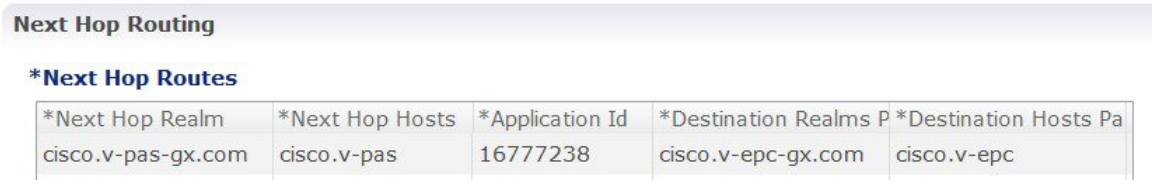
Step 3 Check whether the Peer Group is assigned to correct Peer Route and Dynamic AVPs are properly aligned with Peer Route in Gx New Session Rules.

Step 4 Diameter Connection with the desired Destination Peer should be established with CPS vDRA.

PCRF Generated Messages not Reaching CPS vDRA

Step 1 Make sure PCRF has the correct entry of CPS vDRA as next hop.

Figure 2: Next Hop Routes



Next Hop definition is mandatory in PCRF to forward the messages to CPS vDRA generated by PCRF itself.

For example, Gx-RAR, Sd-TSR

Step 2 Wild Card Entry not supported in Next Hop Routing configuration.

Issues in Reaching Ports and Setup IPs

Step 1 Check firewall is running or not.

Step 2 Make sure the firewall configuration is OK.

a) To check if this is the problem, then stop the firewall.

```
/etc/init.d/iptables stop
```

PB and CRD Inaccessible

Policy Builder and CRD are inaccessible when there are multiple route entries on the master node.

This issue occurs only on OpenStack setups.

OpenStack Neutron configures multiple default routes, if the gateway is also present in the interfaces static configuration.

For example, when configuring multiple interfaces on any VM, set "gateway" for only one interface, preferably public interface.

```
# public network
auto ens160
iface ens160 inet static
address x.x.x.60
```

```
netmask 255.255.255.0
gateway x.x.x.1

# private network
auto ens192
iface ens192 inet static
address y.y.y.155
netmask 255.255.255.0
```

Workaround

Run the following command to delete the default route to the internal network.

```
sudo route del default gw <internal network gateway IP>
```
For example: `sudo route del default gw y.y.y.1`

If the default route is not present for public network, run the following command:

```
ip route add default via <public network gateway IP>
```
For example: `ip route add default via x.x.x.1`