CPS Troubleshooting Guide, Release 18.1.0 (Restricted Release)

First Published: 2018-03-16

Last Modified: 2018-03-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 6

Preface

About this guide

This guide describes how to troubleshoot Cisco Policy Suite.

Audience

This guide is best used by these readers:

- Network administrators
- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.

- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Version Control Software

Cisco Policy Builder uses version control software to manage its various data repositories. The default installed version control software is Subversion, which is provided in your installation package.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

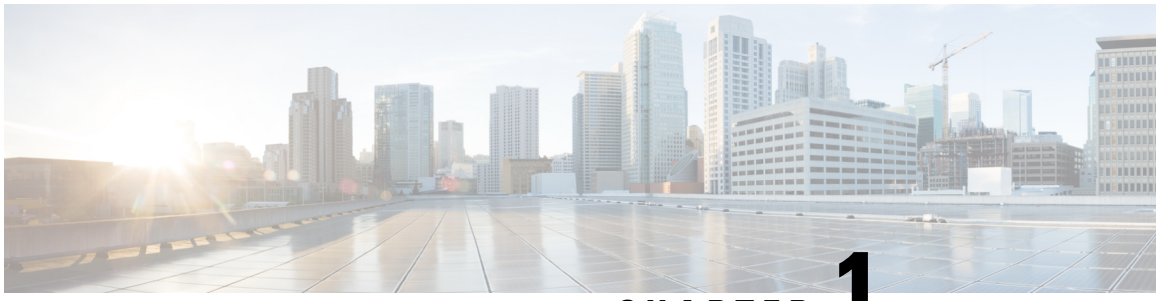
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

RESTRICTED RELEASE

Important This is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives for more information.

RESTRICTED RELEASE



CHAPTER 1

Troubleshooting CPS

General Troubleshooting

- Find out if your problem is related to CPS or another part of your network.
- Gather information that facilitate the support call.
- Are their specific SNMP traps being reported that can help you isolate the issue?

Gathering Information

Determine the Impact of the Issue

- Is the issue affecting subscriber experience?
- Is the issue affecting billing?
- Is the issue affecting all subscribers?
- Is the issue affecting all subscribers on a specific service?
- Is there anything else common to the issue?
- Have there been any changes performed on the CPS system or any other systems?
- Has there been an increase in subscribers?

- Initially, categorize the issue to determine the level of support needed.

Collecting MongoDB Information for Troubleshooting

This sections describes steps on how to collect information regarding mongo if a customer has issues with MongoDB:

Step 1 Collect the information from `/etc/broadhop/mongoConfig.cfg` file from pcrfclient01 VM.

Step 2 Collect `diagnostics.sh --get_replica_status` output.

Step 3 Collect the information from `/var/log/broadhop/mongodb-<dbportnum>.log` file from the sessionmgr VMs where database is hosted (primary/secondary/arbiter for all hosts in the configured replica set. If multiple replica sets experience issues collect from 1 replica set).

Step 4 Connect to the primary sessionmgr VM hosting the database and collect the data (for example, for 10 minutes) by executing the following commands:

```
/usr/bin/mongotop --port <dbportnum> | awk '{ print strftime("%Y-%m-%d %H:%M:%S"), $0; fflush(); }'
>

/var/tmp/mongotop-dbportnum.log &
```

where, <*dbportnum*> is the mongoDB port for the given database (session/SPR/balance/admin), such as 27717 for balance database.

```
vmstat 1 | awk '{ print strftime("%Y-%m-%d %H:%M:%S"), $0; fflush(); }' > /var/tmp/vmstat.log &
```

Note The above mentioned three commands must not be left running on the system, otherwise there will be performance degradation. After 10 min (or so), kill the above mentioned three processes using the 'kill -9' command on each of the three processes.

Step 5 Connect to the primary sessionmgr VM hosting the balance and collect all the database dumps by executing the following command:

```
mongodump --host <ipaddress> --port <dbport>
```

Note The mongo dump is a disk space intensive operation based on your database size, so run it from a VM which has enough disk space. It is also recommended to remove the collected dump/logs once diagnosis is complete.

Step 6 Use the following command to check mongoDB statistics on queries/inserts/updates/deletes for all CPS databases (and on all primary and secondary databases) and verify if there are any abnormalities (for example, high number of insert/update/delete considering TPS, large number of queries going to other site). Here considering the session database as an example:

```
mongostat --host <sessionmgr VM name> --port <dBportnumber>
```

For example,

```
mongostat --host sessionmgr01 --port 27717
```

High CPU Usage Issue

- Thread details and jstack output. It could be captured as:
  - From top output see if java process is taking high CPU.

- Capture output of the following command:

  ```
  ps -C java -L -o pcpu,cpu,nice,state,cputime,pid,tid | sort > tid.log
  ```

- Capture output of the following command where <process pid> is the pid of process causing high CPU (as per top output):

  If java process is running as a root user:

  ```
  jstack <process pid> > jstack.log
  ```

  If java process is running as policy server (qns) user :

  ```
  sudo -u qns "jstack <process pid>" > jstack.log
  ```

  If running above commands report error for process hung/not responding then use `-F` option after `jstack`.

  Capture another jstack output as above but with an additional `-l` option

JVM Crash

JVM generates a fatal error log file that contains the state of process at the time of the fatal error. By default, the name of file has format `hs_err_pid<pid>`.log and it is generated in the working directory from where the corresponding java processes were started (that is the working directory of the user when user started the policy server (qns) process). If the working directory is not known then one could search system for file with name `hs_err_pid*.log` and look into file which has timestamp same as time of error.

High Memory Usage/Out of Memory Error

- JVM could generate heap dump in case of out of memory error. By default, CPS is not configured to generate heap dump. For generating heap dump the following parameters need to be added to `/etc/broadhop/jvm.conf` file for different CPS instances present.

  ```
  -XX+HeapDumpOnOutOfMemoryError
  ```

  ```
  -XXHeapDumpPath=/tmp
  ```

  Note that the heap dump generation may fail if limit for core is not set correctly. Limit could be set in file `/etc/security/limits.conf` for root and policy server (qns) user.

- If no dump is generated but memory usage is high and is growing for sometime followed by reduction in usage (may be due to garbage collection) then the heap dump can be explicitly generated by running the following command:

  - If java process is running as user root:

    ```
    jmap -dumpformat=bfile=<filename> <process_id>
    ```

  - If java process is running as policy server (qns) user:

    ```
    jmap -J-d64 -dump:format=b,file=<filename> <process id>
    ```

    Example: `jmap -J-d64 -dump:format=b,file=/var/tmp/jmapheapdump_18643.map 13382`

Note

- Capture this during off-peak hour. In addition to that, nice utility could be used to reduce priority of the process so that it does not impact other running processes.
- Create archive of dump for transfer and make sure to delete dump/archive after transfer.

- Use the following procedure to log Garbage Collection:
  - Login to VM instance where GC (Garbage Collection) logging needs to be enabled.
  - Run the following commands:

```
cd /opt/broadhop/qns-1/bin/
chmod +x jmxterm.sh
./jmxterm.sh
> open <host>:<port>
> bean com.sun.management:type=HotSpotDiagnostic
> run setVMOption PrintGC true
> run setVMOption PrintGCDateStamps true
> run setVMOption PrintGCDetails true
> run setVMOption PrintGCDetails true
> exit
```

  - Revert the changes once the required GC logs are collected.

Issues with Output displayed on Grafana

In case of Grafana issue, whisper database output is required.

```
whisper-fetch --pretty /var/lib/carbon/whisper/cisco/quantum/qps/hosts/*
```

For example,

```
whisper-fetch --pretty
/var/lib/carbon/whisper/cisco/quantum/qps/dc1-pcrfclient02/load/midterm.wsp
```

Basic Troubleshooting

Capture the following details in most error cases:

Step 1 Output of the following commands:

```
diagnostics.sh
```

```
about.sh
```

Step 2 Collect all the logs:

- Archive created at `/var/log/broadhop` on pcrfclient01 and pcrfclient02 includes consolidated policy server (qns) logs. Make sure that consolidated logs cover logs of time when issue happened.
- SSH to all available policy server (qns) and load balancer (lb) VMs and capture the following logs:

```
/var/log/broadhop/qns-*.log
/var/log/broadhop/qns-*.log.gz
/var/log/broadhop/service-qns-*.log
/var/log/broadhop/service-qns-*.log.gz
```

- SSH to all the available sessionmgr VMs and capture the following mongoDB logs:

```
/var/log/mongodb-*.log
/var/log/mongodb-*.log.gz
```

- SSH to all available VMs and capture the following logs:

```
/var/log/messages*
```

Step 3 CPS configuration details present at `/etc/broadhop`.

Step 4 SVN repository

To export SVN repository, go to `/etc/broadhop/qns.conf` and copy the URL specified against com.broadhop.config.url.

For example,

```
-Dcom.broadhop.config.url=http://pcrfclient01/repos/run
```

Run the following command to export SVN repository:

```
svn export <url of run repo copied from qns.conf> <folder name where data is to be exported>
```

Step 5 Top command on all available VMs to display the top CPU processes on the system:

```
top -b -n 30
```

Step 6 Output of the following command from pcrfclient01 VM top_qps.sh with output period of 10-15 min and interval of 5 sec:

```
top_qps.sh 5
```

Step 7 Output of the following command on load balancer (lb) VMs having issue.

```
netstat -plan
```

Step 8 Output of the following command on all VMs.

```
service iptables status
```

Step 9 Details mentioned in Periodic Monitoring.

Trace Support Commands

This section covers the following two commands:

- trace.sh
- trace_id.sh

For more information on trace commands, refer to *Policy Tracing and Execution Analyzer* section in *CPS Operations Guide*.

trace.sh

`trace.sh` usage:

```
/var/qps/bin/control/trace.sh -i <specific id> -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace.sh -x <specific id> -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace.sh -a -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace.sh -e -d sessionmgr01:27719/policy_trace
```

This script starts a selective trace and outputs it to standard out.

- Specific Audit Id Tracing

  `/var/qps/bin/control/trace.sh -i <specific id>`

- Dump All Traces for Specific Audit Id

  `/var/qps/bin/control/trace.sh -x <specific id>`

- Trace All.

  `/var/qps/bin/control/trace.sh -a`

- Trace All Errors.

  `/var/qps/bin/control/trace.sh -e`

trace_id.sh

`trace_id.sh` usage:

```
/var/qps/bin/control/trace_ids.sh -i <specific id> -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace_ids.sh -r <specific id> -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace_ids.sh -x -d sessionmgr01:27719/policy_trace
/var/qps/bin/control/trace_ids.sh -l -d sessionmgr01:27719/policy_trace
```

This script starts a selective trace and outputs it to standard out.

- Add Specific Audit Id Tracing

  `/var/qps/bin/control/trace_ids.sh -i <specific id>`

- Remove Trace for Specific Audit Id

  `/var/qps/bin/control/trace_ids.sh -r <specific id>`

- Remove Trace for All Ids

  `/var/qps/bin/control/trace_ids.sh -x`

- List All Ids under Trace

  `/var/qps/bin/control/trace_ids.sh -l`

Periodic Monitoring

- Run the following command on pcrfclient01 and verify that all the processes are reported as Running.

For CPS 7.0.0 and higher releases:

```
/var/qps/bin/control/statusall.sh

Program 'cpu_load_trap'
  status                            Waiting
  monitoring status                 Waiting
Process 'collectd'
  status                            Running
  monitoring status                 Monitored
  uptime                            42d 17h 23m
Process 'auditrpms.sh'
  status                            Running
  monitoring status                 Monitored
  uptime                            28d 20h 26m
System 'qns01'
  status                            Running
  monitoring status                 Monitored
The Monit daemon 5.5 uptime: 21d 10h 26m
Process 'snmpd'
  status                            Running
  monitoring status                 Monitored
  uptime                            21d 10h 26m
Process 'qns-1'
  status                            Running
  monitoring status                 Monitored
  uptime                            6d 17h 9m
```

- Run `/var/qps/bin/diag/diagnostics.sh` command on pcrfclient01 and verify that no errors/failures are reported in output.

```
/var/qps/bin/diag/diagnostics.sh
CPS Diagnostics HA Multi-Node Environment
--------------------------
Ping check for all VMs...
Hosts that are not 'pingable' are added to the IGNORED_HOSTS variable...[PASS
                                                 ]
Checking basic ports for all VMs...[PASS]
Checking qns passwordless logins for all VMs...[PASS]
Checking disk space for all VMs...[PASS]
Checking swap space for all VMs...[PASS]
Checking for clock skew for all VMs...[PASS]
Checking CPS diagnostics...
  Retrieving diagnostics from qns01:9045...[PASS]
  Retrieving diagnostics from qns02:9045...[PASS]
  Retrieving diagnostics from qns03:9045...[PASS]
  Retrieving diagnostics from qns04:9045...[PASS]
  Retrieving diagnostics from pcrfclient01:9045...[PASS]
  Retrieving diagnostics from pcrfclient02:9045...[PASS]
Checking svn sync status between pcrfclient01 & 02...
svn is not sync between pcrfclient01 & pcrfclient02...[FAIL]
Corrective Action(s): Run ssh pcrfclient01 /var/qps/bin/support/recover_svn_sync.sh
Checking HAProxy statistics and ports...
```

- Perform the following actions to verify VMs status is reported as UP and healthy and no alarms are generated for any VMs.
  - Login to the VMware console
  - Verify the VM statistics, graphs and alarms through the console.
- Verify if any trap is generated by CPS.

```
cd /var/log/snmp
```

```
tailf trap
```

- Verify if any error is reported in CPS logs.

  ```
  cd /var/log/broadhop
  grep -i error consolidated-qns.log
  grep -i error consolidated-engine.log
  ```

- Monitor the following KPIs on Grafana for any abnormal behavior:
  - CPU usage of all instances on all the VMs
  - Memory usage of all instances on all VMs
  - Free disk space on all instances on all VMs
  - Diameter messages load: CCR-I, CCR-U, CCR-T, AAR, RAR, STR, ASR, SDR
  - Diameter messages response time: CCR-I, CCR-U, CCR-T, AAR, RAR, STR, ASR, SDA
- Errors for diameter messages.

  Run the following command on pcrfclient01:

  ```
  tailcons | grep diameter | grep -i error
  ```

- Response time for sessionmgr insert/update/delete/query.
  - Average read, write, and total time per sec:

    ```
    mongotop --host sessionmgr* --port port_number
    ```

  - For requests taking more than 100ms:

    SSH to sessionmgr VMs:

    ```
    tailf /var/log/mongodb-<portnumber>.log
    ```

Note Above commands will by default display requests taking more than 100 ms, until and unless the following parameter has been configured on mongod process --slows XYZms. XYZ represents the value in milliseconds desired by user.

- Garbage collection.

  Check the `service-qns-*.log` from all policy server (QNS), load balancer (lb) and PCRF VMs. In the logs look for “GC” or “FULL GC”.

- Session count.

  Run the following command on pcrfclient01:

  ```
  session_cache_ops.sh --count
  ```

- Run the following command on pcrfclient01 and verify that the response time is under expected value and there are no errors reported.

```
/opt/broadhop/qns-1/control/top_qps.sh
```

- Use the following command to check mongoDB statistics on queries/inserts/updates/deletes for all CPS databases (and on all primary and secondary databases) and verify if there are any abnormalities (for example, high number of insert/update/delete considering TPS, large number of queries going to other site).

  ```
  mongostat --host <sessionmgr VM name> --port <dBportnumber>
  ```

  For example,

  ```
  mongostat --host sessionmgr01 --port 27717
  ```

- Use the following command for all CPS databases and verify if there is any high usage reported in output. Here considering session database as an example:

  ```
  mongotop --host <sessionmgr VM name> --port <dBportnumber>
  ```

  For example,

  ```
  mongotop --host sessionmgr01 --port 27717
  ```

- Verify EDRs are getting generated by checking count of entries in CDR database.
- Verify EDRs are getting replicated by checking count of entries in the databases.
- Determine most recently inserted CDR record in MySQL database and compare the insert time with the time the CDR was generated. Time difference should be within 2 min or otherwise signifies lag in replication.
- Count of CCR-I/CCR-U/CCR-T/RAR messages from/to GW.
- Count of failed CCR-I/CCR-U/CCR-T/RAR messages from/to GW. If GW has capability, capture details at error code level.

  Run the following command on pcrfclient01:

  ```
  cd /var/broadhop/stats

  grep "Gx_CCR-" bulk-*.csv
  ```

- Response time of CCR-I/CCR-U/CCR-T messages at GW.
- Count of session in PCRF and count of session in GW. There could be some mismatch between the count due to time gap between determining session count from CPS and GW. If the count difference is high then it could indicate stale sessions on PCRF or GW.
- Count of AAR/RAR/STR/ASR messages from/to Application Function.
- Count of failed AAR/RAR/STR/ASR messages from/to Application Function. If Application Function has capability, capture details at error code level.

  Run the following command on pcrfclient01:

  ```
  cd /var/broadhop/stats

  grep "Gx_CCR-" bulk-*.csv
  ```

- Response time of AAR/RAR/STR/ASR messages at Application Function.

- Count of session in PCRF and count of session in Application Function. There could be some mismatch between the count due to time gap between determining session count from CPS and Application Function. If the count difference is high then it could indicate stale sessions on PCRF or Application Function.

  Count of session in PCRF:

  ```
  session_cache_ops.sh -count
  ```

E2E Call Flow Troubleshooting

- On an All-in-One deployment, run the following commands:

  ```
  tcpdump -i <any port 80 or 8080 or 1812 or 1700 or 1813 or 3868> -s 0 -vv
  ```

  - Append a `-w /tmp/callflow.pcap` to capture output to Wireshark file

- Open the file in WireShark and filter on HTTP to assist debugging the call flow.
- In a distributed model, you need to tcpdump on individual VMs:
  - Load balancers on port 1812, 1813, 1700, 8080 and 3868

Correct call flows are shown Call Flows.

Recovery using Remove/Add Members Option

When Arbiter blade and a sessionmgr blade goes down there is not any primary sessionmgr node to cater requests coming from CPS VMs (Classic HA setup-1 arbiter 2 sessionmgrs). As a result the system becomes unstable.

A safe way to recover from the issue is to bring UP the down blades to working state. If bringing blades back to working state is not possible then only way to keep setup working is removing failed members of replica-set from mongo-config. In doing so UP and running sessionmgr node becomes primary. It is must to add failed members back to replica-set once they come online.

The following sections describe how to remove failed members from mongo-replica set and how to add them back in replica-set once they are online.

Note The steps mentioned in the following sections should be executed properly.

Note The following steps are done only when only one sessionmgr is UP but is in secondary mode and cannot become primary on its own and bringing back down blades (holding arbiter and primary sessionmgr VMs) to operational mode is not possible.

Remove Failed Members

This option is usually used when member/s are not running and treated as failed member. The script removes all such failed members from replica-set.

Step 1 Login to pcrfclient01/02.

Step 2 Execute the diagnostics script to know which replica-set or respective component is failed and you want to remove.

```
diagnostics.sh --get_replica_status
```

Step 3 Execute `build_set.sh` with below options to remove failed member/s from replica set. This operation removes the all failed members across the site.

```
cd /var/qps/bin/support/mongo/
```

For session database:

```
./build_set.sh --session --remove-failed-members
```

For SPR database:

```
./build_set.sh --spr --remove-failed-members
```

For balance database:

```
./build_set.sh --balance --remove-failed-members
```

For report database:

```
./build_set.sh --report --remove-failed-members
```

Step 4 Execute the diagnostics script again to verify if that particular member is removed.

```
diagnostics.sh --get_replica_status
```

Note If status is not seen properly by above command, login to mongo port on sessionmgr and check replica status.

Figure 1: Replica Status

Add Failed Members

Step 1 Login to pcrfclient01/02.

Step 2 Once the failed members are back online, they can be added back in replica-set.

Step 3 Execute the diagnostics script to know which replica-set member is not in configuration or failed member.

```
diagnostics.sh --get_replica_status
```

If status is not seen properly by above command, login to mongo port on sessionmgr and check replica status.

Figure 2: Replica Status


```
cd /var/qps/bin/support/mongo
```

For session database:

```
./build_set.sh --session --add-members
```

For SPR database:

```
./build_set.sh --spr --add-members
```

For balance database:

```
./build_set.sh --balance --add-members
```

For report database:

```
./build_set.sh --report --add-members
```

Maintenance Window Procedures

The usual tasks for a maintenance window might include these:

Prior to Any Maintenance

Backup all relevant information to an offline resource. For more information on backup see Cisco Policy Suite Backup and Restore Guide.

- Data - Backup all database information. This includes Cisco MsBM Cisco Unified SuM.

Note Sessions can be backed up as well.

- Configurations - Backup all configuration information. This includes SVN (from PCRF Client) the `/etc/broadhop` directory from all PCRFs
- Logs - Backup all logs for comparison to the upgrade. This is not required but will be helpful if there are any issues.

Change Request Procedure

- Have proper sign off for any change request. Cisco and all customer teams must sign off.
- Make sure the proposed procedures are well defined.
- Make sure the rollback procedures are correct and available.

Software Upgrades

- Determine if the software upgrade will cause an outage and requires a maintenance window to perform the upgrade.
- Typically software upgrades can be done on one node a time and so minimize or eliminate any outage.
- Most of the time an upgrade requires a restart of the application. Most applications can be started in less than 1 minute.

VM Restarts

- LINUX must be shutdown normally for VM restarts.
- All VMs are Linux.
- The preferred methods are `init 0 or shutdown -h`
- Failure to use the Linux OS shutdown can result in VM corruption and problems restarting the VM and applications.
- VM restart is typically done to increase resources to the VM (disk memory CPU).

Hardware Restarts

- Hardware restarts should be rare.
- When a hardware restart is needed VMs must be shutdown first.
- When all VMs are stopped shutdown the hardware with either the ESXi console or as a power off.

Planned Outages

- Planned outages are similar to hardware restarts.
- VMs need to be shutdown hardware can then be stopped.
- When hardware is started the typical hardware starting order is:
  - Start the servers with PCRFClient01 LB01 and SessionMgr01 first.
  - Start all other servers in any order after that.

Non-maintenance Window Procedures

Tasks you can perform as non-maintenance that is at any time are these

- Data archiving or warehousing
- Log removal

Common Troubleshooting Tasks

This section describes frequently used troubleshooting tasks you might use before calling support or as directed by support.

Low or Out of Disk Space

To determine the disk space used use these Linux disk usage and disk free commands

- du
- df

df Command

df

For example:

```
home# df -h
[root@lab home]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/cciss/c0d0p5 56G 27G 26G 51% /
/dev/cciss/c0d0p1 99M 12M 83M 12% /boot
tmpfs 2.0G 0 2.0G 0% /dev/shm
none 2.0G 0 2.0G 0% /dev/shm
/dev/cciss/c0d0p2 5.8G 4.0G 1.6G 73% /home
```

As shown above the `/home` directory is using the most of it's allocated space (73%).

du Command

The /home directory is typically for /home/admin but in some cases there is also /home/qns or /home/remote. You can check both

du

For example:

```
home# du -hs
[root@lab home]# du -hs
160M .
[root@lab home]# du -hs *
1.3M   qns
158M   remote
36K    testuser
```

The **du** command shows where the space is being used. By default the du command by itself gives a summary of quota usage for the directory specified and all subdirectories below it.

Note By deleting any directories you remove the ability to roll back if for some reason an update is not working correctly. Only delete those updates to which you would probably never roll back perhaps those 6 months old and older.

LDAP Error Codes

The following table describes LDAP error codes:

Table 1: LDAP Error Codes

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
0	SUCCESS	The result code (0) that will be used to indicate a successful operation			Y		
1	OPERATIONS_ ERROR	The result code (1) that will be used to indicate that an operation was requested out of sequence.		Y		Y	
2	PROTOCOL_ERROR	The result code (2) that will be used to indicate that the client sent a malformed request.		Y		Y	

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
3	TIME_LIMIT_ EXCEEDED	The result code (3) that will be used to indicate that the server was unable to complete processing on the request in the allotted time limit.	Y	Y			
4	SIZE_LIMIT_ EXCEEDED	The result code (4) that will be used to indicate that the server found more matching entries than the configured request size limit.					Y
5	COMPARE_FALSE	The result code (5) that will be used if a requested compare assertion does not match the target entry.					Y
6	COMPARE_TRUE	The result code (6) that will be used if a requested compare assertion matched the target entry.					Y
7	AUTH_METHOD_ NOT_SUPPORTED	The result code (7) that will be used if the client requested a form of authentication that is not supported by the server.					Y
8	STRONG_AUTH_ REQUIRED	The result code (8) that will be used if the client requested an operation that requires a strong authentication mechanism.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
10	REFERRAL	The result code (10) that will be used if the server sends a referral to the client to refer to data in another location.					Y
11	ADMIN_LIMIT_ EXCEEDED	The result code (11) that will be used if a server administrative limit has been exceeded.					Y
12	UNAVAILABLE_ CRITICAL_ EXTENSION	The integer value (12) for the "UNAVAILABLE_ CRITICAL_ EXTENSION" result code.					Y
13	CONFIDENTIALITY_ REQUIRED	The result code (13) that will be used if the server requires a secure communication mechanism for the requested operation.					Y
14	SASL_BIND_IN_ PROGRESS	The result code (14) that will be returned from the server after SASL bind stages in which more processing is required.					Y
16	NO_SUCH_ ATTRIBUTE	The result code (16) that will be used if the client referenced an attribute that does not exist in the target entry.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
17	UNDEFINED_ ATTRIBUTE_TYPE	The result code (17) that will be used if the client referenced an attribute that is not defined in the server schema.					Y
18	INAPPROPRIATE_ MATCHING	The result code (18) that will be used if the client attempted to use an attribute in a search filter in a manner not supported by the matching rules associated with that attribute.					Y
19	CONSTRAINT_ VIOLATION	The result code (19) that will be used if the requested operation would violate some constraint defined in the server.					Y
20	ATTRIBUTE_OR_ VALUE_ EXISTS	The result code (20) that will be used if the client attempts to modify an entry in a way that would create a duplicate value, or create multiple values for a single-valued attribute.					Y
21	INVALID_ATTRIBUTE_ SYNTAX	The result code (21) that will be used if the client attempts to perform an operation that would create an attribute value that violates the syntax for that attribute.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
32	NO_SUCH_OBJECT	The result code (32) that will be used if the client targeted an entry that does not exist.					Y
33	ALIAS_PROBLEM	The result code (33) that will be used if the client targeted an entry that as an alias.					Y
34	INVALID_DN_SYNTAX	The result code (34) that will be used if the client provided an invalid DN.					Y
36	ALIAS_ DEREFERENCING_ PROBLEM	The result code (36) that will be used if a problem is encountered while the server is attempting to dereference an alias.					Y
48	INAPPROPRIATE_ AUTHENTICATION	The result code (48) that will be used if the client attempts to perform a type of authentication that is not supported for the target user.					Y
49	INVALID_ CREDENTIALS	The result code (49) that will be used if the client provided invalid credentials while trying to authenticate.					Y
50	INSUFFICIENT_ ACCESS_RIGHTS	The result code (50) that will be used if the client does not have permission to perform the requested operation.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
51	BUSY	The result code (51) that will be used if the server is too busy to process the requested operation.		Y		Y	
52	UNAVAILABLE	The result code (52) that will be used if the server is unavailable.		Y		Y	
53	UNWILLING_TO_PERFORM	The result code (53) that will be used if the server is not willing to perform the requested operation.		Y		Y	
54	LOOP-DETECT	The result code (54) that will be used if the server detects a chaining or alias loop.					Y
60	SORT_CONTROL_MISSING	The result code (60) that will be used if the client sends a virtual list view control without a server-side sort control.					Y
61	OFFSET_RANGE_ERROR	The result code (61) that will be used if the client provides a virtual list view control with a target offset that is out of range for the available data set.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
64	NAMING_ VIOLATION	The result code (64) that will be used if the client request violates a naming constraint (e.g., a name form or DIT structure rule) defined in the server.					Y
65	OBJECT_CLASS_ VIOLATION	The result code (65) that will be used if the client request violates an object class constraint (e.g., an undefined object class, a disallowed attribute, or a missing required attribute) defined in the server.					Y
66	NOT_ALLOWED_ ON_NONLEAF	The result code (66) that will be used if the requested operation is not allowed to be performed on non-leaf entries.					Y
67	NOT_ALLOWED_ ON_RDN	The result code (67) that will be used if the requested operation would alter the RDN of the entry but the operation was not a modify DN request.					Y
68	ENTRY_ALREADY_ EXISTS	The result code (68) that will be used if the requested operation would create a conflict with an entry that already exists in the server.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
69	OBJECT_ CLASS_MODS_ PROHIBITED	The result code (69) that will be used if the requested operation would alter the set of object classes defined in the entry in a disallowed manner.					Y
71	AFFECTS_ MULTIPLE_DSAS	The result code (71) that will be used if the requested operation would impact entries in multiple data sources.					Y
76	VIRTUAL_LIST_ VIEW_ERROR	The result code (76) that will be used if an error occurred while performing processing associated with the virtual list view control.					Y
80	OTHER	The result code (80) that will be used if none of the other result codes are appropriate.		Y		Y	
81	SERVER_DOWN	The client-side result code (81) that will be used if an established connection to the server is lost.		Y		Y	
82	LOCAL_ERROR	The client-side result code (82) that will be used if a generic client-side error occurs during processing.		Y		Y	

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
83	ENCODING_ ERROR	The client-side result code (83) that will be used if an error occurs while encoding a request.		Y		Y	
84	DECODING_ ERROR	The client-side result code (84) that will be used if an error occurs while decoding a response.		Y		Y	
85	TIMEOUT	The client-side result code (85) that will be used if a client timeout occurs while waiting for a response from the server.	Y	Y		Y	
86	AUTH_UNKNOWN	The client-side result code (86) that will be used if the client attempts to use an unknown authentication type.					Y
87	FILTER_ERROR	The client-side result code (87) that will be used if an error occurs while attempting to encode a search filter.			Y		
88	USER_CANCELED	The client-side result code (88) that will be used if the end user canceled the operation in progress.					Y
89	PARAM_ERROR	The client-side result code (89) that will be used if there is a problem with the parameters provided for a request.			Y		

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
90	NO_MEMORY	The client-side result code (90) that will be used if the client does not have sufficient memory to perform the requested operation.		Y		Y	
91	CONNECT_ ERROR	The client-side result code (91) that will be used if an error occurs while attempting to connect to a target server.		Y		Y	
92	NOT_SUPPORTED	The client-side result code (92) that will be used if the requested operation is not supported.					Y
93	CONTROL_NOT_ FOUND	The client-side result code (93) that will be used if the response from the server did not include an expected control.					Y
94	NO_RESULTS_ RETURNED	The client-side result code (94) that will be used if the server did not send any results.			Y		
95	MORE_RESULTS_ TO_RETURN	The client-side result code (95) that will be used if there are still more results to return.					Y
96	CLIENT_LOOP	The client-side result code (96) that will be used if the client detects a loop while attempting to follow referrals.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
97	REFERRAL_LIMIT_ EXCEEDED	The client-side result code (97) that will be used if the client encountered too many referrals in the course of processing an operation.					Y
118	CANCELED	The result code (118) that will be used if the operation was canceled					Y
119	NO_SUCH_ OPERATION	The result code (119) that will be used if the client attempts to cancel an operation that the client doesn't exist in the server.					Y
120	TOO_LATE	The result code (120) that will be used if the client attempts to cancel an operation too late in the processing for that operation.					Y
121	CANNOT_ CANCEL	The result code (121) that will be used if the client attempts to cancel an operation that cannot be canceled.					Y
122	ASSERTION_ FAILED	The result code (122) that will be used if the requested operation included the LDAP assertion control but the assertion did not match the target entry.					Y

	Name	Definition	Counts as Timeout	Triggers Retry	Sent To Policy Server	Terminate Connection	Not Applicable to Search
123	AUTHORIZATION_DENIED	The result code (123) that will be used if the client is denied the ability to use the proxied authorization control.					Y

Diameter Issues and Errors

Diameter Issues

The following details need to be captured for diameter issues:

- Details of service associated with subscribers in failure case.
- Pcaps capturing calls having issue.
- If the issue is with no response pcap should be captured both at CPS and the peer.
- Subscriber trace information can be captured using the following process
  - To add the subscriber that needs to be traced

    ```
    /var/qps/bin/control/trace_ids.sh -i <msisdn/imsi> -d sessionmgr01:<port no>/policy_trace
    ```

    ```
    cd /var/qps/bin/control
    ```

  - Run the following command to obtain subscriber information

    ```
    /var/qps/bin/control/trace.sh -i <msisdn/imsi> -d sessionmgr01<port no>/policy_trace
    ```

If CPS receives the request message for the same subscriber the trace result will be displayed.

Note Port no. can be found in “Trace DB Database” configuration in Cluster-1. If Trace Database is not configured then by default “Admin Db Configuration” will pick up the trace database.

Diameter Proxy Error in diagnostics.sh Output

When you execute `diagnostics.sh` script on pcrfclient01 VM and it shows the following errors related to diameter proxy

```
diameter_proxy-lb01_A DOWN L4CON
Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change (seconds): 2513094
diameter_proxy-lb01_B DOWN L4CON
Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change
```

```
(seconds): 2513093
diameter_proxy-lb01_C DOWN L4CON
Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change
(seconds): 2513092
diameter_proxy-BACKEND DOWN
Sessions (current,max,limit): 0,0,2000 Rate (sessions,max,limit): 0,0, Last Status change
(seconds): 2513092
```

The error L4CON message indicates that there is connection problem (e.g. “Connection refused” or “No route to host”) at layer 1-4. And the error message diameter_proxy-BACKEND DOWN signifies that all the service specified in diameter_proxy section in `haproxy.cfg` file are down.

1. Check whether HAProxy is running on load balancer VM. Specifically for this error message we should check in lb01.
2. Check the HAProxy configuration:

   ```
   vi /etc/haproxy/haproxy.cfg
   ```

   It should show similar entries as shown below. Try to telnet to corresponding load balancer VM with corresponding ports:

   ```
   diameter_proxy-lb01_A DOWN L4CON
   Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change
   (seconds): 2513094
   diameter_proxy-lb01_B DOWN L4CON
   Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change
   (seconds): 2513093
   diameter_proxy-lb01_C DOWN L4CON
   Sessions (current,max,limit): 0,0, Rate (sessions,max,limit): 0,0, Last Status change
   (seconds): 2513092
   diameter_proxy-BACKEND DOWN
   Sessions (current,max,limit): 0,0,2000 Rate (sessions,max,limit): 0,0, Last Status change
    (seconds): 2513092
   ```

Diameter Peer Connectivity is Down

If your Diameter Peer connectivity is down check the following:

1. Check the TCP connection on the diameter port (i.e.,) “netstat -pant | grep 3868". It should be in established state.
2. If the TCP connection is not getting established disable the firewall `service iptables stop` and check the port status `/opt/broadhop/installer/support/add_open_port.sh pcrf 3868`.
3. Open the Internet browser and go to your repository and check the published policies in runtime environment. You should notice the following configuration. If the following configuration is not there, then most probably it is a bad publish.

   ```
   DiameterConfiguration-_4davIF2KEeOXe-MDH-2FEQ.xmi

   DiameterStack-default-_A5cgQF2LEeOXe-MDH-2FEQ.xmi
   ```

4. If the problem is not in CPS and something is mis-configured in PCEF then you may notice the following messages in CPS

   ```
   tail -f /var/log/broadhop/service-qns-1.log

   Sending Alert Notification for host pcef realm lab.realm is down
   Sending Alert Notification for host pcef realm lab.realm is back up
   ```

```
Sending Alert Notification for host pcef realm lab.realm is down
Sending Alert Notification for host pcef realm lab.realm is back up
```

No Response to Diameter Request

Using TCPDUMP

- Collect tcpdump packet capture from the primary policy director (IOmanager).

  ```
  tcpdump –i any –port 3868 –s0 –w filename test.pcap
  ```

  In the collected trace file,

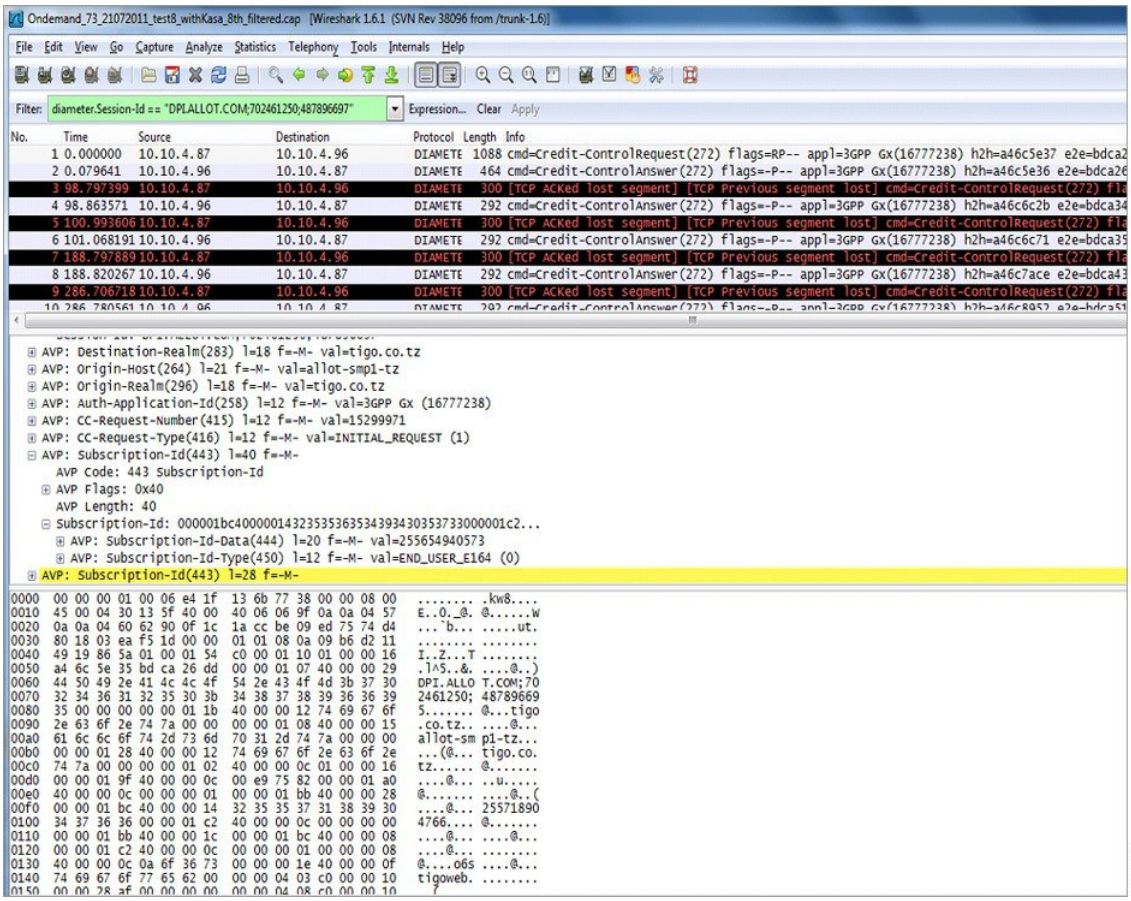
- Verify that the response message is sent back to PCEF.
- Use Session-Id as filter if the Session-Id of the user's session is available.
- If Session-Id for the user is not available use MSISDN as filter to retrieve the Session-Id. Then apply Session-Id filter to view all the messages for the session.
- Match the request to response for Credit Control Request CC-Request-Type attribute (Initial/Update/Terminate).

CPS Logs

- Verify the consolidated-qns.log on PCRFCLIENT01 for any exceptions with policy executions for example Null Pointer Exception.
- Filter using Session-Id

TCPDUMP – User Id Filter

Figure 3: TCPDUMP – User Id Filter



- Filter using Subscription-Id-Data (MSISDN) to retrieve the CCR initial request.

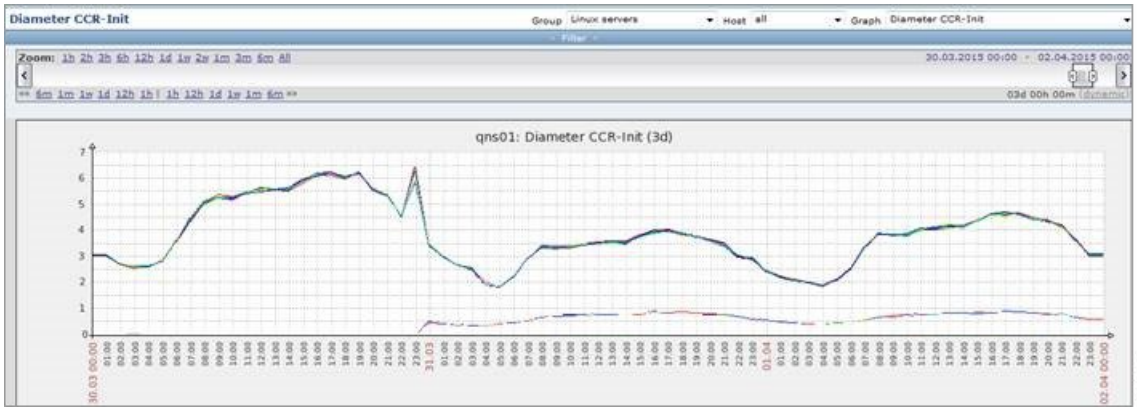
Diagnose Diameter No Response for Peer Message

Note The port numbers provided in this section are an example and can differ based on the network deployment. For more information on port numbers contact your Cisco Technical Representative.

Traffic Failover or Similar

In a Geo-Redundant deployment when there are issues in message processing on primary-site A policy director (LB) VMs then there is an increase in diameter traffic sent to secondary-site. This is an indication that there is a failure in responding to messages sent on primary-site A due to message response timeouts. For example, the following zabbix graphs shows diameter traffic failing over to secondary from 30th Mar 2300 onwards.

Figure 4: Zabbix Graph



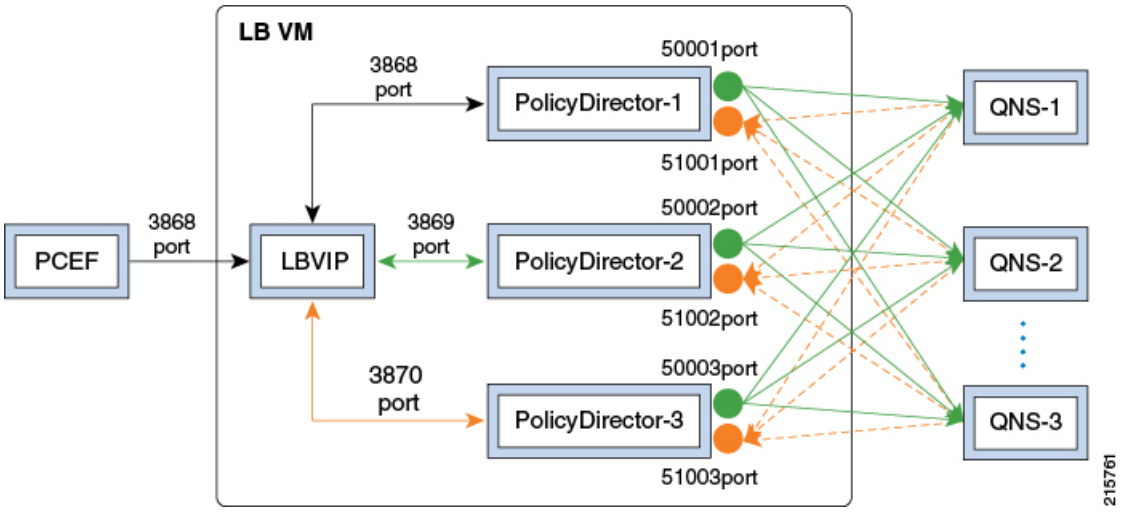
Note Here Zabbix graph is an example and similar graph in Grafana (6.x.x) or client traffic graphs reports CPS dropping response.

Policy Director (LB)<->Policy Server (QNS) Messaging

The following diagram describes processing of diameter messages sent from PCEF on EBW secondary policy director (lb).

Note The port numbers provided in this section are an example and can differ based on the network deployment. For more information on port numbers contact your Cisco Technical Representative.

Figure 5: Messaging between Policy Director (LB) and Policy Server (QNS)



As per the PCRF deployment PCEF sends diameter traffic on the 3868 port of the LBVIP running on the active policy director (LB) VM. These messages are distributed in a round-robin scheduling between three Policy Director (PD) instances based on the haproxy configuration. All the PDs are connected to all the policy

server (QNS) VMs instances using the ZMQ queues. Each PD uses a PUSH queue to send data to policy server (QNS) VM and PULL Queue to process a response from policy server (QNS) VM. The following table describes the various PUSH and PULL queue ports mapping

Table 2: Policy Director Ports Mapping

PD Instance	PUSH Queue Port	Pull Queue Port	HA Proxy Port
PD-1	50001	51001	3868
PD-2	50002	51002	3869
PD-3	50003	51003	3870

Port Details

1. HaProxy ports

```
monit status qnsXX
```

PD-1 port

```
netstat -anp | grep 31654 | grep 3868
tcp        0      0 ::ffff:10.192.131.3:3868    :::*                        LISTEN
 31654/java
tcp        0      0 ::ffff:10.192.131.3:3868    ::ffff:10.192.131.3:52762   ESTABLISHED
 31654/java
```

PD-2 port

```
netstat -anp | grep 31701 | grep 3869
tcp        0      0 ::ffff:10.192.131.3:3869    :::*                        LISTEN
 31701/java
tcp        0      0 ::ffff:10.192.131.3:3869    ::ffff:10.192.131.3:60936   ESTABLISHED
 31701/java
```

PD-3 port

```
netstat -anp | grep 31753 | grep 3870
tcp        0      0 ::ffff:10.192.131.3:3870    :::*                        LISTEN
 31753/java
tcp        0      0 ::ffff:10.192.131.3:3870    ::ffff:10.192.131.3:34338   ESTABLISHED
 31753/java
```

2. ZMQ PUSH queue ports for PD-1

```
netstat -anp | grep 31654 | grep 50001
tcp        0      0 ::ffff:10.192.131.3:50001   :::*                        LISTEN
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.17:53572  ESTABLISHED
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.15:60186  ESTABLISHED
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.23:52481  ESTABLISHED
 31654/java
...
...
```

All 10 policy server (QNS) VMs are connected on the ZMQ PUSH queue.

3. ZMQ PULL Queue ports for PD-2

```
netstat -anp | grep 31654 | grep 50001
tcp        0      0 ::ffff:10.192.131.3:50001   :::*                        LISTEN
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.17:53572  ESTABLISHED
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.15:60186  ESTABLISHED
 31654/java
tcp        0      0 ::ffff:10.192.131.3:50001   ::ffff:10.192.131.23:52481  ESTABLISHED
 31654/java
...
...
```

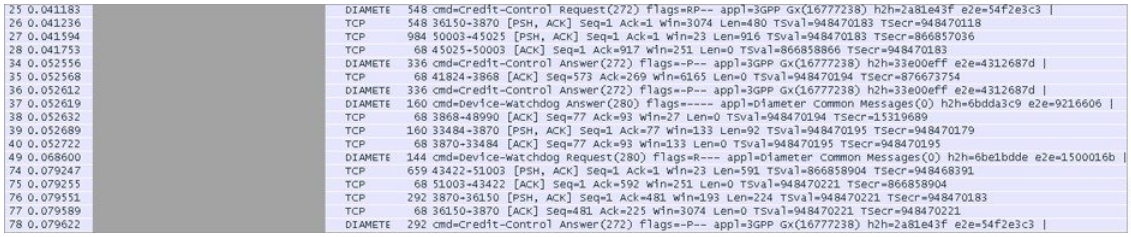
All 10 policy server (QNS) VMs are connected on the ZMQ PULL queue.

Similarly PD-2 and PD-3 will be connected to all the policy server (QNS) VMs on their respective PUSH and PULL queues port for internal IPC messaging.

Successful Message Handling

The following snapshot shows filtered packets for a successful CCR/CCA message handling done for PD-3. Packet capture was taken using tcpdump on all Ethernet interfaces of active policy director (LB).

Figure 6: Filtered Packet



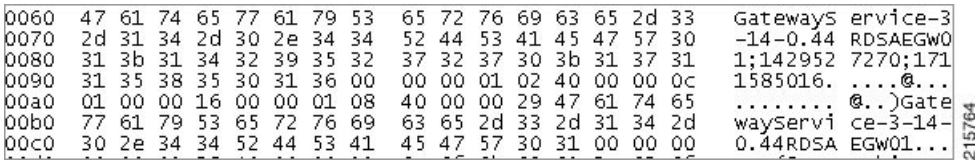
Packet Details

1. Packet#25 CCR message from PCEF to lbvip

   Figure 7: PCEF to lbvip CCR Message

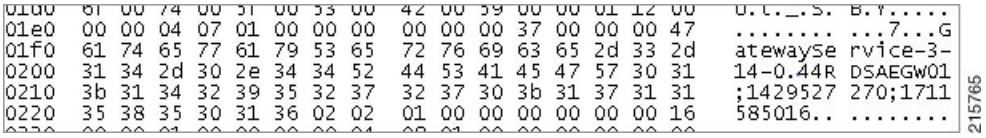
2. Packet#26 CCR message sent to HaProxy port 3870 of PD-3

   Figure 8: CCR Message to HaProxy



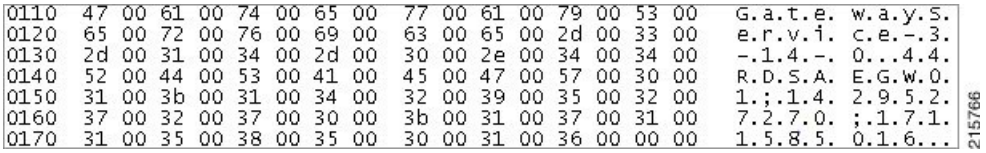
3. Packet#27 PD-3 sends message to policy server (QNS) VM by adding message to PUSH Queue port 50003

Figure 9: PD-3 Message



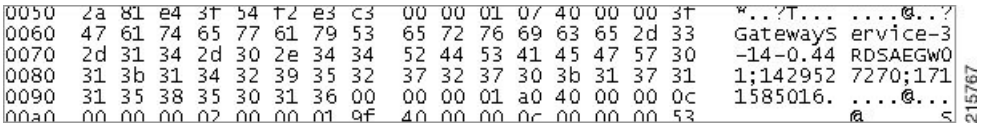
4. Packet#74 policy server (QNS) VM sends response back to PD-3 on PULL Queue port 51003

Figure 10: Policy Server (QNS) VM Response



5. Packet#76 PD-3 sends CCA message to HaProxy port 3870

Figure 11: PD-3 Message



6. Packet#78 CCA sent to PCEF

Figure 12: CCA Message

All the above packets are co-related based on the “Diameter Session-Id” found in the Wireshark hex/bytes “ascii character” details as shown above.

Wireshark Filters for capturing messages between PCEF, lbvip, Policy Director and Policy Server (QNS) when tcpdump taken on all Ethernet interfaces of active policy director (LB):

- Filter PD-1 ---> “tcp.srcport == 3868 || tcp.dstport == 3868 || tcp.srcport == 50001 || tcp.dstport == 50001 || tcp.dstport == 3868 || tcp.srcport == 3868 || tcp.srcport == 51001 || tcp.dstport == 51001"
- Filter PB-2 ---> “tcp.srcport == 3869 || tcp.dstport == 3869 || tcp.srcport == 50002 || tcp.dstport == 50002 || tcp.dstport == 3868 || tcp.srcport == 3868 || tcp.srcport == 51002 || tcp.dstport == 51002"
- Filter PD-3 ---> “tcp.srcport == 3870 || tcp.dstport == 3870 || tcp.srcport == 50003 || tcp.dstport == 50003 || tcp.dstport == 3868 || tcp.srcport == 3868 || tcp.srcport == 51003 || tcp.dstport == 51003"

Message Drops at Diameter Interface

Based on the zabbix graphs (an example) if there are messages failing over to secondary then tcpdump taken on primary site active policy director (LB) VM should show the diameter messages for which no response was sent to PCEF. On a sample tcpdump we can apply following filter to check the number of messages dropped and find the list of corresponding peers

Filter in Wireshark - “(!diameter.answer_in) && !(diameter.answer_to) && diameter”

Figure 13: Message Drops

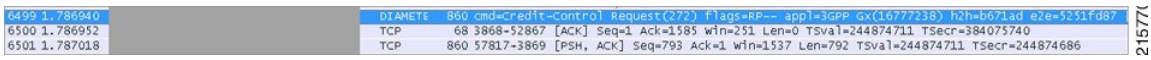
Now filtered packets can be checked to find the number of packets dropped for each peer connections. All the packets dropped should be for a given list of Peers which are currently not being processed at primary-site.

Message Dropped between Policy Director (LB)<->Policy Server (QNS)

The next step is to identify the PolicyDirector instance where these messages are being dropped.

1. top command output on active policy director (lb) should show that the PD instance not using any CPU as there are no messages being processed on the process-id, note the PD-instance.
2. Start a tcpdump on all Ethernet interfaces of the policy director VM which should contain all packets sent between lbvip, policy director instance and policy server (QNS) VMs. This tcpdump will also contain the requests which do not have any response from PCRF, so apply the filter "(!diameter.answer_in) && ! (diameter.answer_to) && diameter" in wireshark and note a single request which was not processed.
3. This packet should be then forwarded to PD-instance HaProxy port.

   Figure 14: Forwarded Packets



   Packet 6499 CCR-I request from PCEF was not answered and the message is forwarded to HaProxy port 3869 which is PD-2 instance in packet 6501 but no subsequent forwarding to policy server (QNS) VMs occurred. Hence PD-2 was not processing and forwarding any requests from PCEF to policy server (QNS) VMs. Similarly, this can be verified for other filtered packets as identified in Step 2 above.

   In such cases, your Cisco Technical Representative can be contacted to further diagnose the issue and find the cause for message drops at PD level. Similarly, above analysis can be applied to identify messages dropped at policy server (QNS) level if packets are forwarded from PD to policy server (QNS) on PUSH queue but no response from policy server (QNS) VM on PULL queue found.

Recovering Hung Peers

Based on the above diagnosis from tcpdump and top command messages were dropped at the PD-2 instance. This caused all traffic for peers connected to this PD-2 instance to failover to secondary-site LoadBalancers as shown in Zabbix graphs. In order to recover from this situation the LoadBalancer processes should be restarted as follows:

1. Login to the active policy director (lb) of primary-site and execute the following:

```
monit status qnsXX
service heartbeat status
service monit status
```

2. Stop the services.

```
service heartbeat stop
service monit stop
monit stop qnsXX
```

3. Start the policy server (QNS) service and check its status.

```
monit start qnsXX
monit status qnsXX
```

4. Start the monit and heartbeat service.

```
service monit start
service heartbeat start
```

5. Repeat Step 1 to Step 4 on newly active policy director (lb).
6. Verify from Zabbix graphs or similar graphs that traffic has stopped failing over to secondary-site.
7. Take a tcpdump on all Ethernet interfaces of active policy director (lb) and verify that all the three Policy Directors are sending/receiving messages from policy server (QNS) instances as explained in Successful Message Handling.

Diameter Result Codes and Scenarios

The following table describes some common diameter result codes and scenarios:

Table 3: Common Diameter Result Codes and Scenarios

Code	Name	CPS Scenarios
2001	DIAMETER_SUCCESS	Everything went well and Request processed successfully.
2002	DIAMETER_LIMITED_SUCCESS	The Request was successfully completed, but additional processing is required by the application in order to provide service to the user.
3001	DIAMETER_COMMAND_UNSUPPORTED	The Request contained a Command-Code that the receiver did not recognize or support. This MUST be used when a Diameter node receives an experimental command that it does not understand.
3002	DIAMETER_UNABLE_TO_DELIVER	Message cannot be delivered, either because no host within the realm supporting the required application was available to process the request or because Destination-Host AVP was given without the associated Destination-Realm AVP.
3003	DIAMETER_REALM_NOT_SERVED	The intended realm of the request is not recognized.

Code	Name	CPS Scenarios
3004	DIAMETER_TOO_BUSY	Message got discarded by the overload handling mechanism. Note: CPS 7.5 adds the option to silently discard instead of sending DIAMETER_TOO_BUSY as discarding is often a better way to have other node back off instead of immediately resending the request in an overload scenario.
3005	DIAMETER_LOOP_DETECTED	An agent detected a loop while trying to get the message to the intended recipient. The message MAY be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.
3006	DIAMETER_REDIRECT_INDICATION	A redirect agent has determined that the request could not be satisfied locally and the initiator of the request should direct the request directly to the server, whose contact information has been added to the response. When set, the Redirect-Host AVP MUST be present.
3007	DIAMETER_APPLICATION_UNSUPPORTED	A request was sent for an application that is not supported.
3008	DIAMETER_INVALID_HDR_BITS	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code's definition.
3009	DIAMETER_INVALID_AVP_BITS	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP's definition.
3010	DIAMETER_UNKNOWN_PEER	A CER was received from an unknown peer.
4001	DIAMETER_AUTHENTICATION_REJECTED	The authentication process for the user failed, most likely due to an invalid password used by the user. Further attempts MUST only be tried after prompting the user for a new password.
4002	DIAMETER_OUT_OF_SPACE	A Diameter node received the accounting request but was unable to commit it to stable storage due to a temporary lack of space.

Code	Name	CPS Scenarios
4003	ELECTION_LOST	The peer has determined that it has lost the election process and has therefore disconnected the transport connection.
4010	DIAMETER_END_USER_SERVICE_DENIED	The credit-control server denies the service request due to service restrictions. If the CCR contained used-service-units they are deducted, if possible.
4011	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE	The credit-control server determines that the service can be granted to the end user but no further credit-control is needed for the service (eg, service is free of charge).
4012	DIAMETER_CREDIT_LIMIT_REACHED	The credit-control server denies the service request since the end-user's account could not cover the requested service. If the CCR contained used-service-units they are deducted, if possible.
4141	DIAMETER_PCC_BEARER_EVENT	When for some reason a PCC rule cannot be enforced or modified successfully in a network initiated procedure. The reason is provided in the Event Trigger AVP value.
4241	DIAMETER_ERROR_NO_AVAILABLE_ POLICY_COUNTERS	Error used by the OCS to indicate to the PCRF that the OCS has no available policy counters for the subscriber.
5001	DIAMETER_AVP_UNSUPPORTED	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit. A Diameter message with this error MUST contain one or more Failed- AVP AVP containing the AVPs that caused the failure.
5002	DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.
5003	DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user could not be authorized. No session created due to various reasons. For example, this error could occur if the service requested is not permitted to the user.

Code	Name	CPS Scenarios
5004	DIAMETER_INVALID_AVP_VALUE	The request contained an AVP with an invalid value in its data portion. A Diameter message indicating this error MUST include the offending AVPs within a Failed-AVP AVP.
5005	DIAMETER_MISSING_AVP	The request did not contain an AVP that is required by the Command Code definition. If this value is sent in the Result-Code AVP, a Failed-AVP AVP SHOULD be included in the message. The Failed-AVP AVP MUST contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.
5006	DIAMETER_RESOURCES_EXCEEDED	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.
5007	DIAMETER_CONTRADICTING_AVPS	The Home Diameter server has detected AVPs in the request that contradicted each other, and is not willing to provide service to the user. One or more Failed-AVP AVPs MUST be present, containing the AVPs that contradicted each other.
5008	DIAMETER_AVP_NOT_ALLOWED	A message was received with an AVP that MUST NOT be present. The Failed-AVP AVP MUST be included and contain a copy of the offending AVP.
5009	DIAMETER_AVP_OCCURS_TOO_ MANY_TIMES	A message was received that included an AVP that appeared more often than permitted in the message definition. The Failed-AVP AVP MUST be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences
5010	DIAMETER_NO_COMMON_APPLICATION	When a CER message is received, and there are no common applications supported between the peers.

Code	Name	CPS Scenarios
5011	DIAMETER_UNSUPPORTED_VERSION	A request was received, whose version number is unsupported.
5012	DIAMETER_UNABLE_TO_COMPLY	Message rejected as something else that went wrong and there's no specific reason.
5013	DIAMETER_INVALID_BIT_IN_HEADER	An unrecognized bit in the Diameter header is set to one (1).
5014	DIAMETER_INVALID_AVP_LENGTH	The request contained an AVP with an invalid length. A Diameter message indicating this error MUST include the offending AVPs within a Failed-AVP AVP.
5015	DIAMETER_INVALID_MESSAGE_LENGTH	A request is received with an invalid message length.
5016	DIAMETER_INVALID_AVP_BIT_COMBO	The request contained an AVP with which is not allowed to have the given value in the AVP Flags field. A Diameter message indicating this error MUST include the offending AVPs within a Failed-AVP AVP.
5017	DIAMETER_NO_COMMON_SECURITY	A CER message is received, and there are no common security mechanisms supported between the peers. A Capabilities-Exchange-Answer (CEA) MUST be returned with the Result-Code AVP set to DIAMETER_NO_COMMON_SECURITY.
5030	DIAMETER_USER_UNKNOWN	The subscriber was not found in SPR.
5031	DIAMETER_RATING_FAILED	Informs the credit-control client that the credit-control server cannot rate the service request due to insufficient rating input, incorrect AVP combination or due to an AVP or an AVP value that is not recognized or supported in the rating.
5141	DIAMETER_ERROR_TRIGGER_EVENT	When the set of bearer/session information sent in a CCR originated due to a trigger event been met is incoherent with the previous set of bearer/session information for the same bearer/session.

Code	Name	CPS Scenarios
5142	DIAMETER_PCC_RULE_EVENT	When for some reason the PCC rules cannot be installed/activated. The reason is provided in the Event Trigger AVP value.
5143	DIAMETER_ERROR_BEARER_NOT_ AUTHORIZED	Emergency service related - Used when the PCRF cannot authorize an IP-CAN bearer upon the reception of an IP-CAN bearer authorization request coming from the PCEF.
5144	DIAMETER_ERROR_TRAFFIC_MAPPING_ INFO_REJECTED	Emergency service related - Used when the PCRF does not accept one or more of the traffic mapping filters.
5570	DIAMETER_ERROR_UNKNOWN_ POLICY_COUNTERS	Error used by the OCS to indicate to the PCRF that the OCS does not recognize one or more Policy Counters specified in the request, when the OCS is configured to reject the request provided with unknown policy counter identifier(s).

Diameter Experimental Result Codes

The following table describes some common Diameter experimental result codes and scenarios:

Table 4: Common Diameter Experimental Result Codes

Code	Name	CPS Scenarios
2001	DIAMETER_FIRST_REGISTRATION	The HSS informs the I-CSCF that: - The user is authorized to register this public identity; - A S-CSCF shall be assigned to the user.
2002	DIAMETER_SUBSEQUENT_REGISTRATION	The HSS informs the I-CSCF that: - The user is authorized to register this public identity; - A S-CSCF is already assigned and there is no need to select a new one.
2003	DIAMETER_UNREGISTERED_SERVICE	The HSS informs the I-CSCF that: - The public identity is not registered but has services related to unregistered state; - A S-CSCF shall be assigned to the user.
2004	DIAMETER_SUCCESS_SERVER_NAME_ NOT_STORED	The HSS informs to the S-CSCF that: - The de-registration is completed; - The S-CSCF name is not stored in the HSS.

Code	Name	CPS Scenarios
4100	DIAMETER_USER_DATA_NOT_AVAILABLE	The requested user data is not available at this time to satisfy the requested operation.
4101	DIAMETER_PRIOR_UPDATE_IN_PROGRESS	The request to update the repository data at the HSS could not be completed because the related repository data is currently being updated by another entity.
4143	DIAMETER_AN_GW_FAILED	The policy decisions (i.e. installation/modification of PCC rules or provisioning of policy decisions not related to a PCC rule) received within a RAR initiated by the PCRF cannot be enforced by the PCEF because the AN-Gateway has failed. If one or more PCC Rules are affected, these PCC Rules will be provided in the Charging-Rule-Report AVP including the Rule-Failure-Code AVP set to AN_GW_FAILED (17), and PCC-Rule-Status AVP set to INACTIVE as described in Clause 4.5.12. Applicable only to 3GPP-EPS.
4144	TGPP_DIAMETER_PENDING_TRANSACTION	A node that supports the PendingTransaction feature receives an incoming request on a session while it has an ongoing transaction on the same session and cannot handle the request as described in Clause 8.2 of 3GPP TS 29.213 [8].
4196	DIAMETER_REQUESTED_SESSION_NOT_FOUND	Returned by PCEF when it doesn't find the session info for the requested session in SDR.
4197	DIAMETER_SESSION_RECOVERY_REQUESTED	
4198	DIAMETER_PENDING_TRANSACTION	The PCRF expects a response to a pending request that it initiated. The PCRF can also retry the request message if needed.
5001	DIAMETER_ERROR_USER_UNKNOWN	Message was received for a user or a wildcarded identity that is unknown.

Code	Name	CPS Scenarios
5002	DIAMETER_ERROR_IDENTITIES_DONT_ MATCH	Message was received with a public identity and a private identity for a user, and server determines that the public identity does not correspond to the private identity.
5003	DIAMETER_ERROR_IDENTITY_NOT_ REGISTERED	A query for location information is received for a public identity that has not been registered before. The user to which this identity belongs cannot be given service in this situation.
5004	DIAMETER_ERROR_ROAMING_NOT_ ALLOWED	User is not allowed to roam in the visited network.
5005	DIAMETER_ERROR_IDENTITY_ALREADY_ REGISTERED	Identity has already a server assigned and the registration status does not allow that it is overwritten.
5006	DIAMETER_ERROR_AUTH_SCHEME_NOT_ SUPPORTED	Authentication scheme in an authentication request is not supported.
5007	DIAMETER_ERROR_IN_ASSIGNMENT_TYPE	Identity being registered has already the same server assigned and the registration status does not allow the server assignment type or the Public Identity type received in the request is not allowed for the indicated server-assignment-type.
5008	DIAMETER_ERROR_TOO_MUCH_DATA	Volume of the data pushed to the receiving entity exceeds its capacity.
5009	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	The S-CSCF informs HSS that the received subscription data contained information which was not recognised/supported
5011	DIAMETER_ERROR_FEATURE_UNSUPPORTED	A request application message was received indicating that the origin host requests that the command pair would be handled using a feature which is not supported by the destination host.
5012	DIAMETER_ERROR_SERVING_NODE_ FEATURE_UNSUPPORTED	The HSS supports the P-CSCF-Restoration-mechanism feature, but none of the user serving node(s) supports it.

Code	Name	CPS Scenarios
5061	INVALID_SERVICE_INFORMATION	PCRF rejects new or modified service information the service information provided by the AF is invalid /insufficient for the server to perform the requested action.
5062	FILTER_RESTRICTIONS	PCRF rejects new or modified service information because the Flow-Description AVPs cannot be handled by the server.
5063	REQUESTED_SERVICE_NOT_AUTHORIZED	PCRF rejects new or modified service information because the requested service is not consistent with the related subscription information /operator defined policy rules and/or the supported features in the IP-CAN network.
5064	DUPLICATED_AF_SESSION	PCRF rejects a new Rx session setup because the new Rx session relates to an AF session with another related active Rx session.
5065	IP_CAN_SESSION_NOT_AVAILABLE	PCRF rejects a new Rx session setup when it fails to associate the described service IP flows within the session information received from the AF to an existing IP-CAN session.
5066	UNAUTHORIZED_NON_EMERGENCY_SESSION	PCRF rejects new Rx session setup because the session binding function associated a non-Emergency IMS session to an IP-CAN session established to an Emergency APN.
5067	UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY	The PCRF rejects a new Rx session setup because the PCRF can’t authorize the sponsored data connectivity based on the sponsored data connectivity profile or the operator policy.
5068	TEMPORARY_NETWORK_FAILURE	
5100	DIAMETER_ERROR_USER_DATA_NOT_RECOGNIZED	The data received by the AS is not supported or recognized.
5101	DIAMETER_ERROR_OPERATION_NOT_ALLOWED	The requested operation is not allowed for the user.
5102	DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ	The requested user data is not allowed to be read.

Code	Name	CPS Scenarios
5103	DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED	The requested user data is not allowed to be modified.
5104	DIAMETER_ERROR_USER_DATA_CANNOT_BE_NOTIFIED	The requested user data is not allowed to be notified on changes
5105	DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC	The request to update the repository data at the HSS could not be completed because the requested update is based on an out-of-date version of the repository data. That is, the sequence number in the Sh-Update Request message, does not match with the immediate successor of the associated sequence number stored for that repository data at the HSS. It is also used where an AS tries to create a new set of repository data when the identified repository data already exists in the HSS.
5106	DIAMETER_ERROR_SUBS_DATA_ABSENT	The Application Server requested to subscribe to changes to Repository Data that is not present in the HSS.
5107	DIAMETER_ERROR_NO_SUBSCRIPTION_TO_DATA	The AS received a notification of changes of some information to which it is not subscribed
5108	DIAMETER_ERROR_DSAI_NOT_AVAILABLE	The Application Server addressed a DSAI not configured in the HSS.
5140	DIAMETER_ERROR_INITIAL_PARAMETERS	Used when the set of bearer or session or subscriber information needed by the PCRF for rule selection is incomplete/ erroneous/not available for the decision to be made.
5141	DIAMETER_ERROR_TRIGGER_EVENT	The set of bearer/session information sent in a CCR originated due to a trigger event been met is incoherent with the previous set of bearer/session information for the same bearer/session. (E.g. event trigger met was RAT changed, and the RAT notified is the same as before)

Code	Name	CPS Scenarios
5142	DIAMETER_PCC_RULE_EVENT	The PCC rules cannot be installed/activated. Affected PCC-Rules will be provided in the Charging-Rule-Report AVP including the reason and status as described in Clause 4.5.12. Absence of the Charging-Rule-Report means that all provided PCC rules for that specific bearer/session are affected.
5143	DIAMETER_ERROR_BEARER_NOT_AUTHORIZED	The PCRF cannot authorize an IP-CAN bearer (e.g. the authorized QoS would exceed the subscribed QoS) upon the reception of an IP-CAN bearer authorization request coming from the PCEF. The affected IP-CAN bearer is the one that triggered the corresponding CCR. The PCEF shall reject the attempt to initiate or modify the bearer indicated in the related CCR command.
5144	DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED	The PCRF does not accept one or more of the traffic mapping filters (e.g. TFT filters for GPRS) provided by the PCEF in a CC Request.
5147	DIAMETER_ERROR_CONFLICTING_REQUEST	The PCRF cannot accept the UE-initiated resource request as a network-initiated resource allocation is already in progress that has packet filters that cover the packet filters in the received UE-initiated resource request. The PCEF shall reject the attempt for UE-initiated resource request.
5148	DIAMETER_ADC_RULE_EVENT	The ADC rules cannot be installed/activated. Affected ADC Rules shall be provided in the ADC-Rule-Report AVP including the reason and status as described in Clause 5b.3.6. Absence of the ADC-Rule-Report means that all provided ADC rules for that IP-CAN session are affected.
5199	DIAMETER_NEWER_SESSION_DETECTED	Received in the authentication response message. This result code is introduced to detect stale message requests and support session uniqueness.

Frequently Encountered Scenarios

Subscriber not Mapped on SCE

This issue was causing the subscriber to get no mapping on the SCE.

Step 1 Write an awk script to perform the following grep to create a text file of over 1000 instances of this message:

```
grep "No member in system" policy.log* >

no_member_found.txt
```

This grep resulted in a file with these lines:

```
policy.log:2009-07-17 11:00:21,201 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d162818
policy.log:2009-07-17 11:02:06,108 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for D02625
policy.log.1:2009-07-17 09:25:29,036 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for D162346
policy.log.1:2009-07-17 09:27:28,718 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d162365
policy.log.1:2009-07-17 09:27:37,193 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d162365
policy.log.1:2009-07-17 09:27:42,257 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d162365
policy.log.1:2009-07-17 09:38:09,010 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d02116
policy.log.1:2009-07-17 09:38:12,618 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for D163647
policy.log.1:2009-07-17 09:40:42,751 INFO
wikiimport:com.broadhop.sme.business.network.accounting.Ne
tworkAccountingUtil No member in system for d102096
```

Step 2 Then use the following awk script to generate a new file that only has the user name. The script says print the 10th field:

```
awk '{print $10}' no_member_found.txt >

no_member_found_usernames_with_dupes.txt
```

Step 3 Run the following command to remove duplicates:

```
sort no_member_found_usernames_with_dupes.txt | uniq >

uniq_sorted_no_member_found_usernames.txt
```

This resulted in a file with usernames only:

```
D00059

D00077
```

```
D001088

D00112

d001313

D00145

D001452

d00156

D00186

d00198

D00200

d00224
```

CPS Server Will Not Start and Nothing is in the Log

If the CPS server does not start (or starts and immediately crashes) and no errors appear in `/var/log/broadhop/qns.log` file to give reasons it did not start check the following list

1. Check `/var/log/broadhop/service-qns-1.log` file.
2. Check `/etc/broadhop/servers`.
   - There should be an entry in this file for the current host name (Type 'hostname' in the console window to find the local hostname)
   - There must be directory that corresponds to the hostname entry with config files. That is if the servers file has svn01=controlcenter there must be a `/etc/broadhop/controlcenter` directory.
3. Attempt to start the server directly from the command line and look for errors.
   - Type: `/opt/broadhop/qns/bin/qns.sh`
   - The server should start up successfully and the command line should not return. If the command prompt returns then the server did not start successfully.
   - Look for any errors displayed in the console output.
4. Look for OSGi errors.
   - Look in `/opt/broadhop/qns/configuration` for a log file. If any exist examine the log file for error messages.

Server returned HTTP Response Code: 401 for URL

A 401 type error means you're not logging in to SVN with proper credentials.

The server won't start and the following appears in the log:

```
2010-12-10 01:05:26,668 \[SpringOsgiExtenderThread-8\]
ERROR c.b.runtime.impl.RuntimeLoader - There was an error
initializing reference data\!
java.io.IOException: Server returned HTTP response code:
401 for URL: http://lbvip01/repos/run/config.properties
sun.net.www.protocol.http.HttpURLConnection.getInputStream
(HttpURLConnection.java:1313) \~\[na:1.6.0_20\]
org.springframework.core.io.UrlResource.getInputStream(Url
Resource.java:124) \~\[org.springframework.core_3.0.0.REL
```

To fix this error:

- Edit **/etc/broadhop/qns.conf**
- Ensure that the configuration URL and repository credentials hostnames match.

```
\-Dcom.broadhop.config.url=http://lbvip01/repos/run/

\-Dcom.broadhop.repository.credentials=broadhop/

broadhop@lbvip01
```

com.broadhop.exception.BroadhopException Unable to Find System Configuration for System

Symptoms server won't stay started and the log displays this:

```
com.broadhop.exception.BroadhopException: Unable to find system configuration for system:
The system that is set up in your Quantum Policy Builder (and cluster name) must match the
 one
specified in /etc/broadhop/qns.conf. Either add or change this via the Quantum Policy Builder

interface, and then publish or update the system/clustername in /etc/broadhop/qns.conf
\-Dcom.broadhop.run.systemId=poc-system
\-Dcom.broadhop.run.clusterId=cluster-1
```

Log Files Display the Wrong Time but the Linux Time is Correct

If log files or other dates are showing in the incorrect time zone despite the Linux time being set to the proper time zone, most likely the time zone that the JVM reads is incorrect.

Step 1 In **/etc/sysconfig**, run the command cat clock to see this output:

```
ZONE="America/Denver"

UTC=false

ARC=false
```

Step 2 Change the ZONE line to the time zone you desire, for instance you could change it to:

```
ZONE="Asia/Singapore"

UTC=false

ARC=false
```

to change the JVM time zone to Singapore time.

The value for ZONE is driven by the directories in **/usr/share/zoneinfo**

REST Web Service Queries Returns an Empty XML Response for an Existing User

For example:

```
<subscriberProfile><content/></subscriberProfile>
```

Because there are multiple ways needed to return web service data, the BroadHop Web Service Blueprint doesn't return any XML by default. To fix this issue, configure the 'Default Web Service Query Response' blueprint under the 'BroadHop Web Services' Blueprint.

Error in Datastore: "err" : "E11000 Duplicate Key Error Index

Here mongo database has been used an example. The same steps can be replicated for all the databases.

Note This removes all the sessions.

Typically, duplicate keys like this happen when initially configuring policies and switching primary keys. In a production scenario, you may not want to remove all sessions.

Step 1 **SSH** to sessionmgr01.

Step 2 Open sessionmgr CLI usin the following command:

```
/usr/bin/mongo --port 27717
```

Using `/usr/bin/mong` indicates whether the mongo replica set is primary or secondary.

Step 3 Enter following commands on the MongoDB CLI:

```
use session_cache;
```

```
db.session.remove({});
```

Step 4 If it gives you a 'not master' error, log into sessionmgr02 and perform the same steps.

Error Processing Request: Unknown Action

```
com.broadhop.policy.impl.RulesPolicyService - Error
processing policy request: Unknown action:
com.broadhop.pop3auth.actions.IPOP3AuthRequest and Remote
Actions are disabled.
```

If you see an error of the type above, it means that the implementation class it's looking for is not available on the server. This can be caused by:

- The component needed is not installed on the server.
- Ensure that the pop3auth service is installed in your server.
- Look for exceptions in the logs when starting up.
- Try restarting the service bundle (pop3auth service in this case) using the OSGi console and looking at the logs.

Memcached Server is in Error

```
ERROR c.b.d.impl.DiagnosticController - Diagnostic failed.

A problem exists with the system --> Common Services:

2:Memcached server is in error
```

Step 1 Log on to the server where policy server (qns) is running

Step 2 Telnet to the memcache server's IP and port 11211 (For example, `telnet lbvip01 11211`).

You can figure out which memcache server CPS is pointing to in Cisco Policy Builder. Look at:**Reference Data** > **Systems** > ***System Name*** > ***Cluster Name***.

a) If you cannot telnet to the port, do the following:

Make sure memcache is running:

- Log on to server where memcache is running.

```
run service memcached status

[root@sessionmgr01 ~]# monit status memcached

memcached is stopped
```

- If the service is stopped, start it:

```
[root@sessionmgr01 ~]# monit start memcached

Starting a new distributed memory caching

(memcached) process for 11211:
```

b) Make sure firewall configuration is OK.

To check if this is the problem, stop the firewall.

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

If it is the problem, add an exception in `/etc/sysconfig/iptables`. Look at other entries in the file for an example.

After adding an exception, restart the IP tables: `/etc/init.d/iptables restart`.

Firewall Error: Log shows Host Not Reachable, or Connection Refused

In HA environment if we see some connection refused errors stop the firewall and execute

```
service iptables stop
```

to see if the problem is related to the iptables firewall issue.

Unknown Error in Logging: License Manager

```
2010-12-12 18:51:32,258 [pool-4-thread-1] ERROR
c.b.licensing.impl.LicenseManager - Unknown error in
logging
java.lang.NullPointerException: null
at
com.broadhop.licensing.impl.LicenseManager.checkFeatures(L
icenseManager.java:311) ~[na:na]
```

This issue may occur if no license has been assigned yet.

Option 1: If this is for development or Proof Of Concept deployments you can turn on developer mode. This effectively gives you 100 users but is not for use in production.

1. Login to CPS.
2. Add the following to the **`/etc/broadhop/qns.conf`** file:

   ```
   -Dcom.broadhop.developer.mode=true
   ```

3. Restart CPS

Option 2: Generate a real license. Have your Cisco technical representative send you the Technical Article *Tool com.broadhop.licensing.service - Creating a CPS License*.

Option 3: If we have license error in the logs, check the MAC address of the VM and compare that with the MAC address in the license file in `/etc/broadhop/license/`.

Logging Does Not Appear to be Working

Step 1 Run the JMX Command:

```
/opt/broadhop/qns/bin/jmxcmd.sh

ch.qos.logback.classic:Name=default,Type=ch.qos.logback

.classic.jmx.JMXConfigurator Statuses
```

or

Step 2 Access that bean using JMX Term or JConsole to view the status of the Logback Appenders. To access JMX Term, follow these steps:

a) Execute the script: `/opt/broadhop/qns-1/bin/jmxterm.sh`
b) If user does not have permission to execute the command then change the permission using below command:

   ```
   chmod 777 opt/broadhop/qns-1/bin/jmxterm.sh
   ```

c) Again execute the script: `/opt/broadhop/qns-1/bin/jmxterm.sh`
d) Once command is executed, JMX terminal opens up.
e) Execute the following command to open connection:

   ```
   $>open qns01:9045
   ```

f) All beans can be seen using the following command:

```
$>beans
#domain = JMImplementation:
JMImplementation:type=MBeanServerDelegate
#domain = ch.qos.logback.classic:
ch.qos.logback.classic:Name=default,Type=ch.qos.logba
ck.classic.jmx.JMXConfigurator
#domain = com.broadhop.action:
com.broadhop.action:name=AddSubscriberService,type=hi
stogram
com.broadhop.action:name=AddSubscriberService,type=se
rvice
com.broadhop.action:name=GetSessionAction,type=histog
ram
com.broadhop.action:name=GetSessionAction,type=servic
e
com.broadhop.action:name=GetSubscriberActionImpl,type
=histogram
com.broadhop.action:name=GetSubscriberActionImpl,type
=service
com.broadhop.action:name=LockSessionAction,type=histo
gram
com.broadhop.action:name=LockSessionAction,type=servi
ce
com.broadhop.action:name=LogMessage,type=histogram
com.broadhop.action:name=LogMessage,type=service
com.broadhop.action:name=OCSLoadBalanceState,type=his
togram
com.broadhop.action:name=OCSLoadBalanceState,type=ser
vice
java.nio:name=mapped,type=BufferPool
#domain = java.util.logging:
java.util.logging:type=Logging
```

Cannot Connect to Server Using JMX: No Such Object in Table

This is likely caused because the server's name is not set up in the hosts file with its proper IP address.

In **/etc/hosts** the hostname (e.g. qns01) SHOULD NOT be aliased to 127.0.0.1 or localhost.

If improperly aliased JMX tells the server it's connecting to connect back with the IP of it's hostname. If it's aliased to localhost (127.0.0.1) the server attempts to open connections with itself which is unfortunate.

Example Error:

```
ERROR com.broadhop.management.JmxClient -

Unable to connect to JmxClient iomgr019045. Cause no

such object in table Will attempt to reconnect.
```

File System Check (FSCK) Errors

During machine boot **`fsck`** is run on file systems to check its consistency. This consistency check is done without user intervention and automatically fixes errors which it can. But sometimes if there is a hard reset to CPS VM/machine for example because of abrupt power failure then during **`fsck`** all the problems are not

automatically fixed and user intervention is must to fix the errors reported by fsck. The table below describes the common fsck errors along with their description and solution.

Table 5: File System Errors and Solutions

SNo.	FSCK Error	Description/Solution
1	BAD SUPER BLOCK MAGIC NUMBER WRONG USE ALTERNATE SUPER-BLOCK TO SUPPLY NEEDED INFORMATION	This error comes when file system is cleanly unmounted. Some superblock corruptions can be automatically repaired. But for some like BAD MAGIC number fsck aborts and alternate superblock must be specified to fsck command to continue file system check. Refer to the link to fix the issue.
2	Block bitmap not in a group/inode bitmap not in a group	When this error occurs data on the device need to be restored using dd or any other device specific command. Refer to the following links to fix the issue: Link 1, Link 2
3	Inode table not in a group	When this error occurs data on the device need to be restored using dd or any other device specific command. Refer to the link to fix the issue
4	Primary superblock is corrupt	Please refer to Error 1 apart from bad magic number if fsck detects corruption in any static parameters of primary superblock (file system size inode list size etc) it requests operator to specify location of alternate superblock.
5	Journal superblock has an unknown read-only feature flag set	Please refer to Error 1 to 4 to fix this issue.
6	Resize inode is invalid	This error occurs after file system is resized. Refer to the link to fix this issue.
7	Last mount time is in the future	This error occurs after reboot system clock is not synchronized with UTC. Refer to the link to fix the issue.
8	Root directory is not an inode	If primary superblock is corrupt this error occurs alternate superblock needs to be specified to fsck in this case. Refer to the following links to fix the issue: Link 1, Link 2

SNo.	FSCK Error	Description/Solution
9	Duplicate '..' entry	An indirect block is a pointer to a list of every block claimed by an inode. fsck checks every block number against a list of allocated blocks if two inodes claim the same block number that block number is added to a list of duplicate block numbers. The administrator may be asked to choose which inode is correct and usually time to verify files against backups. fsck additionally checks the integrity of the actual block numbers which can also become corrupt - it should always lie in the interval between the first data block and the last data block. If a bad block number is detected the inode is cleared. Similar to above example this issue is with file system synchronization with actual disk. If machine is powered OFF before fs synchronization to hardware disk on next reboot fsck will ask corrective questions to the user to take the action accordingly. For which manual intervention is needed as corrective actions will defer case to case. For example if one record is created by database operation and at the same time another record is deleted and same block number (of deleted record) is used for the newly created record duplicate block error might come.
10	Error reading block <block_no> (Attempt to read from filesystem resulted in short read) while doing inode scan.	This error stops the user from continuing with the fsck scan and correcting the problem. Disks that have physical hardware errors often report - being unable to read inodes error. To resolve this issue replace the disk rather than attempting any corrective action.
11	Journal superblock has an unknown incompatible feature flag set	Feature flag specifies what features a file system has. If this flag is corrupted fsck asks whether you want to abort the operation. You need to specify "no" and after this fix the superblock corruption. Refer to the link to fix the issue.

- The link gives list of all the errors which are automatically fixed by fsck as well as list of errors where user intervention is must -
- The link gives general idea about various phases in fsck.
- The link describes all the errors in case of UFS file system.

This link can be used as a reference to fix the errors reported by fsck on CPS file system which is ext3.

CPS: Session Cache mongoDB Stuck in STARTUP2 after sessionMgr01/2 Reboot

There can be a situation where session cache mongoDB process is stuck after sessionMgr01/02 is rebooted. In this situation follow the steps below to bring up session cache database mongo processes from STARTUP2 state to PRIMARY/SECONDARY state specific to session database only.

Note The steps mentioned in this section are applicable to GR deployments. For HA, the mongo processes are recovered automatically. In case they are not recovered automatically, then only the steps mentioned in this section should be used.

Step 1 Stop the CPS processes.

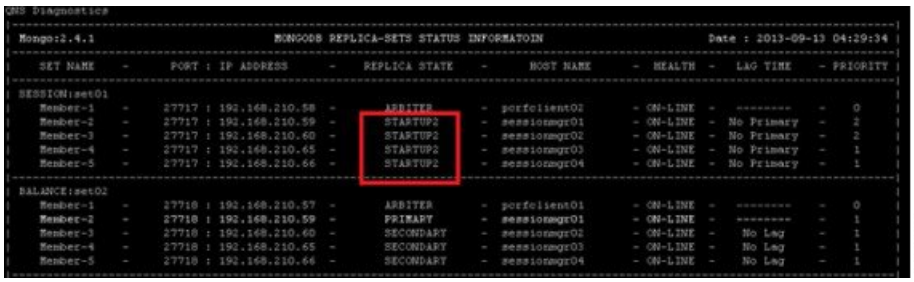
Step 2 Log onto pcrfclient01.

Step 3 Execute the diagnostic.sh script to know which replica set (all members) have failed.

```
diagnostics.sh --get_replica_status
```

The figure shows all replica set members of replica set set01 for session data are in STARTUP2 state.

Figure 15: Replica Set Members



Step 4 Build the session replica sets. Select 2 for session non-sharded sets.

```
./build_set.sh --create --setname <setname>
```

Step 5 Set the priority by executing the following command from Cluster Manager.

In case of GR: `set_priority.sh --db session --replSet <setname> --sitename <site1>`

In case of HA: `set_priority.sh --db session --replSet <setname>`

Step 6 Verify if priority is set correctly for newly created replica set.

```
diagnostics.sh --get_replica_status
```

Step 7 To recover other failed sets, follow the recovery Step 1, on page 56 to Step 6, on page 56.

Step 8 Restart CPS.

```
/var/qps/bin/control/restartall.sh
```

Caution Executing `restartall.sh` will cause messages to be dropped.

Multi-user Policy Builder Errors

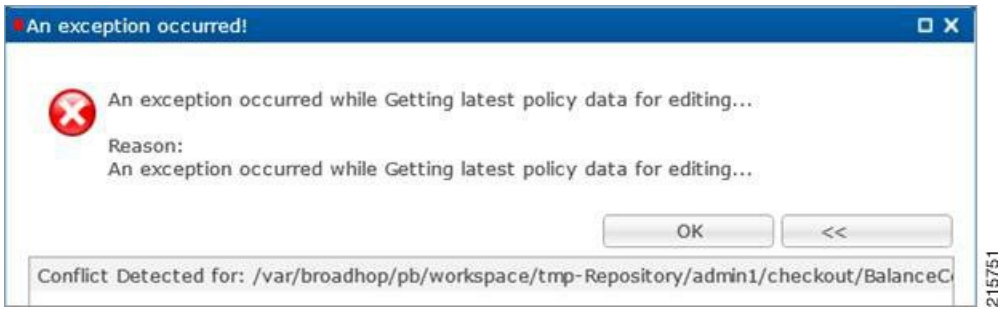
Not able to do any edits after login

Verify the newly created SVN user has write permission. User should be specified under admins in `/var/www/svn/users-access-file` file.

Error in login due to conflict

If error similar to below is seen during login, then revert the configuration and login again.

Figure 16: Login Error



No configuration visible in Policy Builder after login

1. Verify the directory `/var/broadhop/pb/workspace/<username>/checkout` is created on pcrfclient01 and it contains `.xmi` files.
2. If directory does not exist or does not have .xmi files then delete existing repository using Remove on login page and then add new repository using Add on login page.

Figure 17: Delete Existing Repository

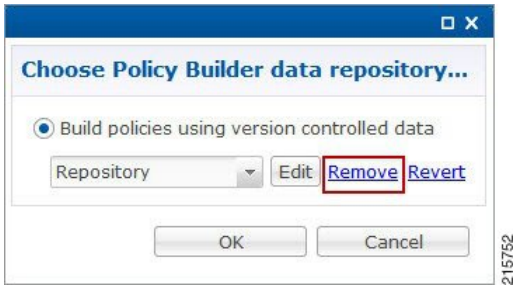
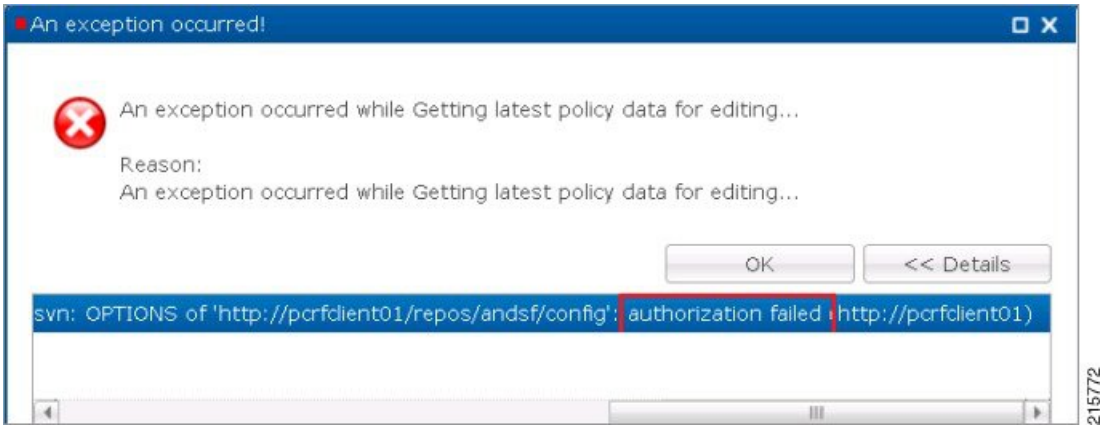


Figure 18: Add New Repository

Exception Occurred During Login

Figure 19: Exception Occurred



This indicates user does not exist in SVN server.

Debug: Verify user exist in `/var/www/svn/.htpasswd` file.

Debug Details

Log Files: `/var/log/broadhop/qns-pb.log`

Policy Reporting Configuration not getting updated post CPS Upgrade

During CPS upgrade from 5.5.1 to 7.0.1 it is observed that Policy Reporting configuration does not get updated as per configuration done in CPS 5.5.1.

All the configuration saved in Cisco Policy Builder are converted into XMI files which are added in the SVN repository. The XMI files based on the CPS 7.0.1 for Policy Reporting won't be fully compatible with the CPS 5.5 version.

To support backward compatibility a utility script migrateCdrXmi_5_5_to_7_0.sh can be implemented which upgrades the policy reporting configuration files (XMI files) to CPS 7.0.1.

Step 1 Obtain the installer archive from the update site corresponding to the build deployed on the system.

Step 2 Copy the archive into the **/tmp** directory of the CPS virtual machine pcrfclient01.

Step 3 Log in as root to the same CPS virtual machine and run these commands.

```
mkdir /opt/broadhop/installer/migrate/

tar -zxvf /tmp/<installer archive anme> -C /opt/broadhop/ installer/migrate/

chown -R qns:qns /opt/broadhop/installer/migrate

chmod +x /opt/broadhop/installer/migrate/*.sh
```

Step 4 Run these commands to execute the script:

```
cd /opt/broadhop/installer/migrate/

sh migrateCdrXmi_5_5_to_7_0.sh
```

The XMI files added or deleted from SVN configuration repository are displayed in the output.

Step 5 Open the Policy Builder page to verify the configuration changes and publish to runtime.

The utility upgrades the Policy reporting fields, the policy reporting records and the Policy CDR configuration in Policy Reporting section of the Cisco Policy builder.

If an older CPS configuration had any 'Reporting Server Configuration' (in Policy Reporting Plugin Configuration) that used any existing policy CDRs, you have to recreate those reporting configurations using the newly created policy CDRs.

CPS Memory Usage

CPS memory consumption can be monitored using appropriate KPIs in Grafana graphs or other monitoring tools. If memory consumption increases beyond the default threshold of 90% on any CPS VM CPS will generate a Low Memory alarm for that VM. This threshold is configurable in the CPS Deployment Template using the free_mem_per setting.

Detect and Reclaim Cached Memory

In some cases a Low Memory alarm may be a result of Linux memory management allocating objects in cache.

To evaluate how much memory a VM has cached and to trigger Linux to free some of the cached memory

1. Compare the amount of memory cached on two or more CPS VMs by running the free -m command on each VM.

   For example, on this qns01 VM 1893 MB of memory is cached.

```
[root@qns01 ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          7854       7719        135          0        311       1893
-/+ buffers/cache:       5514       2340
Swap:         4095         13       4082
```

215774

   However, on qns02 only 1273 MB of memory is cached..

```
[root@qns02 ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          7854       7175        678          0        321       1273
-/+ buffers/cache:       5580       2274
Swap:         4095         14       4081
[root@qns02 ~]#
```

215775

From this example qns01 is storing 620 MB more memory in cache than qns02.

2. To reclaim some of the inactive cached memory execute the following command:

```
free && sync && echo 3 > /proc/sys/vm/drop_caches && echo "" && free
```

Caution Running this command will discard cache objects which can cause a temporary increase in IO and CPU usage, **so it is recommend to run this command during off-peak hours/maintenance window**.

Note This is a non-destructive command and will only free memory that is not in use.

Errors while Installing HA Setup

Step 1 Modify file `/var/qps/config/deploy/csv/AdditionalHosts.csv` to correct `lbvip02` IP address and support sslvip01.

a) Correct lbvip02 IP address.
b) Add sslvip01 IP address.
c) Convert to json `/var/qps/install/current/scripts/import/import_deploy.sh`.
d) Synchronize host `/var/qps/bin/update/synchosts.sh`.
e) Restart all CPS process using the following commands:

```
/var/qps/bin/control/stopall.sh
```

```
/var/qps/bin/control/startall.sh
```

f) SSH to lbvip01 and update pcs resources.
g) Delete lbvip02 resource.

```
/usr/sbin/pcs resource delete lbvip02
```

h) Create `lbvip02` and `sslvip01` resources.

```
/var/broadhop/init_pacemaker_res.sh
```

i) Restart httpd to use correct lbvip02 IP.

Step 2 27717 replica set members are in startup state, recreate replica set.

a) Go to pcrfclient01, sessionmgr01 and sessionmgr02, and execute the following command:

```
/etc/init.d/sessionmgr-27717 stop
```

b) Delete current data directory.

```
\rm -fr /var/data/sessions.1/*
```

c) Go to pcrfclient01, sessionmgr01 and sessionmgr02, and execute the following command:

```
/etc/init.d/sessionmgr-27717 start

/var/broadhop/initialize_replicaset.sh --port 27717 --hosts sessionmgr01,sessionmgr02 --arbiter

pcrfclient01 --set set01
```

Step 3 Execute the following command to check errors:

```
/var/qps/install/7.0.1/scripts/bin/diag/diagnostics.sh (shows some memory and basic port unreachable errors)
```

Step 4 Install bc and nc, using the following commands:

```
yum install bc
yum install nc

Open port 6514 on pcrfclient01 and pcrfclient02, add highlighted bold mark line in
/etc/sysconfig/iptables and restart iptables.
-A INPUT -i eth0 -p udp -m multiport --ports 6514 -m comment --comment "100 allow logstash syslog
access" -j ACCEPT
-A INPUT -i eth0 -p tcp -m multiport --ports 6514 -m comment --comment "100 allow logstash syslog
access tcp" -j ACCEPT
/etc/init.d/iptables restart
```

Enable/disable Debit Compression

Debit compression can be used to identify what all the debits have happened for the subscriber. This data can also be used to cross check the debits with external entities.

- To disable compression add/edit the following flag in `/etc/broadhop/qns.conf` file.

  ```
  -DcompressDebits=false
  ```

- To enable compression add/edit the following flag in `/etc/broadhop/qns.conf` file.

  ```
  -DcompressDebits=true
  ```

We can also check directly in mongo how balance has been debited /credited for subscriber using the following queries

Command to find subscriber:

- SPR database:

  ```
  $use spr
  $db.subscriber.find({
              "credentials_key" : [
                   {
                           "network_id_key" : "111111201"
                  }]});
  ```

  Or

- db.subscriber.find({"network_id_key" : "886906007135"})db.subscriber.find({"network_id_key" : "111111201"})

Output:

```
{
        "_id" : ObjectId("001000009576290454afdc77"),
        "_id_key" : "001000009576290454afdc77",
        "name_key" : {

        },
        "end_date_key" : null,
        "realm_key" : null,
        "parent_id_key" : null,
        "billing_info_key" : {
                "rate_plan_code_key" : null,
                "charging_id_key" : null
        },
        "status_key" : "ACTIVE",
        "version_key" : 0,
        "start_date_key" : null,
        "credentials_key" : [
                {
                        "network_id_key" : "111",
                        "description_key" : null,
                        "password_key" : null,
                        "type_key" : null,
                        "expiration_date_key" : null
                }
        ],
        "role_key" : "READ_ALL",
        "external_id_key" : null,
        "_transId" : "d2a3f602-69bb-4047-af6f-c979ec36732f-1"
}
```

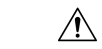
Use "_id_key" output from the above command as subscriber id:

Balance_mgmt

```
$use balance_mgmt

$db.account.find({"subscriberId" : "001000009576290454afdc77"}).pretty();
```

Not able to Publish the Policy in Policy Builder

- Check whether you are getting any errors in diagnostics.sh and try to fix the error.
- Make sure that you have the correct URL for the run time environment. For example http//pcrfclient01/repos/run
- Make sure that you have following configuration on `/etc/broadhop/pb/pb.conf` configuration file. If not then do the changes as shown below and run the `synconfig.sh` and `restartall.sh` for the changes to come into effect:



Caution Executing `restartall.sh` will cause messages to be dropped.

Sample Configuration:

```
SESSION_TIMEOUT="-Dsession.timeout=9000"
QNS_SESSION_DATABASE="-Dsession.db.primary=sessionmgr01
-Dsession.db.secondary=sessionmgr02 -Dsession.db.port=27717
-Dua.client.submit.audit=false"
```

```
HA System Sample Configuration:
SESSION_TIMEOUT="-Dsession.timeout=9000"
QNS_SESSION_DATABASE="-Dsession.db.primary=sessionmgr01
-Dsession.db.secondary=sessionmgr02 -Dsession.db.port=27717
-Dua.client.submit.audit=true
-Dua.client.server.url=http://:8080
```

Note The IP-address is usually LBVIP01 where the SOAP requests are sent to Unified API for our configuration.

- If you still face issue collect and analyze the following logs:
  - `/var/log/broadhop/qns-engine-pb.log`
  - `/var/log/broadhop/service-qns-pb.log`

    .

CPS not sending SNMP traps to External NMS server

- Check whether the "snmpd" process is running in respective VM with the command `monit status snmpd`. If it is stopped start the snmpd process with the command `monit start snmpd`.
- Check whether all the IP tables have been turned off and check the status of UDP port 162 provided you are using the same UDP port 162 at the NMS as well.
- Check the external NMS IP is defined in policy director (lb) VM under `/etc/hosts` and also in the `/etc/snmp/scripts/component_trap_convert` in place of `corporate_nms_ip`.
- Check the file cat `/etc/snmp/snmpd.conf` has the line "rocommunity Broadhop" because all the internal traps from various policy server (QNS) VM to active policy director (lb) VM is been sent over this default community name "Broadhop" as mentioned above.
- Check the trap community name is same both in policy director and as well as in external NMS system. For example, `cat /etc/snmp/scripts/snmp_communities trap_community=cisco` (customer external NMS system should also have this same "cisco" community name.
- Check whether the traps from respective policy server (QNS) VM is properly reaching active policy director (lb) VM this can be checked under `/var/log/snmp/trap`.
- Check for `/var/log/messages` on active policy director (lb) for further analysis.

Policy Builder Loses Repositories

When an hapoxy load balancer which forwards request to Policy Builder server on pcrfclient01 is not available then it forwards the request to backup server on pcrfclient02.

Consider pcrfclient01 is up and a new repository is added using Policy Builder. This repository is saved on pcrfclient01 (on file at `/etc/broadhop/pb/policyRepositories.xml` `/etc/broadhop/pb/publishRepositories.xml`).

If pcrfclient01 becomes inaccessible haproxy sends request to pcrfclient02 where it does not find the above mentioned two files (`publishRepositories.xml policyRepositories.xml`) and does not display any repository on PB GUI.

Fix

CPS does not currently support automatic synchronization of the two repository files
`/etc/broadhop/pb/policyRepositories.xml`
`/etc/broadhop/pb/publishRepositories.xml`

You must manually copy the two files from pcrfclient01 to pcrfclient02 or vice versa.

Not able to access IPv6 Gx port from PCEF/GGSN

Make sure the IPv6 firewall is disabled on lb01and lb02. If the firewall is not disabled then you can disable it by executing the command

```
service ip6tables stop
```

Bring up sessionmgr VM from RECOVERY state to PRIMARY or SECONDARY State

When any sessionmgr VM mongo instance is stuck at RECOVERY state for a long time, perform the following steps to bring up sessionmgr VM mongo instance to PRIMARY or SECONDARY state.

Note The recovery steps must be performed during maintenance window only.

Step 1 Execute the following command script to recover the member:

`high_tps_db_recovery.sh` <*replica_setname*>

For Example:

```
high_tps_db_recovery.sh SPR-SET1
```

Step 2 Execute `diagnostics.sh` command to check whether the RECOVERING member has recovered.

```
diagnostics.sh --get_replica_status
```

After the replica set member is recovered, the state will change to SECONDARY and all the process logs are stored in a log file at the location:
`/var/log/broadhop/scripts//high_tps_db_recovery_xxxxxxxxxx.log`.

ZeroMQ Connection Established between Policy Director and other site Policy Server

ZeroMQ connection established between Policy Director (lb) and other site Policy Server (qns).

How to check

Execute `netstat -apn | grep 2800`" on policy director (lb) and check if other site policy server (qns) are connected to this policy director (lb).

You may also see the following logs:

```
L2-CA-SEC-lb01  2015-05-10 18:58:04,943 [pool-2-thread-1] ERROR c.b.d.impl.server.StackManager
 - Stack
is Null and Realm is not found null:16777238 -  realmToStacks [ocs1.sy.server.cisco.com:7,

ocs3.sy.server.cisco.com:7, ocs4.sy.server.cisco.com:7, cscf3.cisco.com:16777236,
ocs2.sy.server.cisco.com:7, cscf6.cisco.com:16777236, ocs6.sy.server.cisco.com:7,
ocs5.sy.server.cisco.com:7]
L2-CA-SEC-lb01  2015-05-10 18:58:04,944 [pool-3-thread-1] WARN  c.b.d.impl.server.StackManager
 -
Dropping message Outbound: Cmd: 272/1/0 E2E: 1431976189, HBH: 2798797074, Session-ID:
ds4;333241;2883160674, Result-Code: 2001
L2-CA-SEC-lb01  2015-05-10 18:58:04,944 [pool-2-thread-1] ERROR c.b.d.impl.server.StackManager
 - Stack
is Null and Realm is not found null:16777238 -  realmToStacks [ocs1.sy.server.cisco.com:7,

ocs3.sy.server.cisco.com:7, ocs4.sy.server.cisco.com:7, cscf3.cisco.com:16777236,
ocs2.sy.server.cisco.com:7, cscf6.cisco.com:16777236, ocs6.sy.server.cisco.com:7,
ocs5.sy.server.cisco.com:7]
L2-CA-SEC-lb01  2015-05-10 18:58:04,944 [pool-3-thread-1] WARN  c.b.d.impl.server.StackManager
 -
Dropping message Outbound: Cmd: 272/2/1 E2E: 1431980725, HBH: 2798442695, Session-ID:
ds1;333241;2799910481, Result-Code: 2001
```

Fix

To fix the above mentioned problem, perform the following steps to clean the zmq endpoint registry.

1. Connect to admin database.

   ```
   mongo adminDbIpAddress:adminDbPort
   ```

2. Delete endpoint registry

   ```
   use queueing

   db.endpoints.remove({});
   ```

Caution This step impacts the local and remote site services (in case of GR deployment) as queueing database is common to both the sites.

3. Restart the application on local as well as remote site (in case of GR deployment) to create the ZMQ connections by executing the following command on both sites:

   ```
   /var/qps/bin/control/restartall.sh
   ```

Caution Executing `restartall.sh` impacts the service resulting in message drops. The command should be executed in Maintenance Window.

4. Verify by executing `netstat` command:

```
netstat -plan | grep 2800
tcp        0      0 ::ffff:172.20.7.18:28001    :::*                        LISTEN
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28002    :::*                        LISTEN
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28003    :::*                        LISTEN
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.26:35308    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.30:60045    ESTABLISHED
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.34:46369    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.24:38216    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.32:55328    ESTABLISHED
 32294/java
tcp        0   1130 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.28:58586    ESTABLISHED
 32352/java
tcp        0   1123 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.30:49349    ESTABLISHED
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.34:40201    ESTABLISHED
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.34:40447    ESTABLISHED
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.30:52127    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.24:34238    ESTABLISHED
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.36:52364    ESTABLISHED
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.28:38456    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.36:50427    ESTABLISHED
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.22:44375    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.32:60651    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.22:45991    ESTABLISHED
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28003    ::ffff:172.20.7.36:38120    ESTABLISHED
 32235/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.26:46593    ESTABLISHED
 32352/java
tcp        0   1130 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.28:56499    ESTABLISHED
 32294/java
tcp        0   1130 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.24:57277    ESTABLISHED
 32294/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.32:48030    ESTABLISHED
 32352/java
tcp        0      0 ::ffff:172.20.7.18:28001    ::ffff:172.20.7.22:36000    ESTABLISHED
 32352/java
tcp        0   1130 ::ffff:172.20.7.18:28002    ::ffff:172.20.7.26:53322    ESTABLISHED
 32294/java
```

Incorrect Version after Upgrade from 7.0.0 System

If **Upgrade from Existing 7.0 System** does not show latest version then perform the following steps to show the latest version:

1. Reinitialize your environment by executing the following command from Cluster Manager:

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

2. To restart all the policy server (qns) services execute the following command from Cluster Manager:

```
/var/qps/install/current/scripts/bin/control/restartall.sh
```

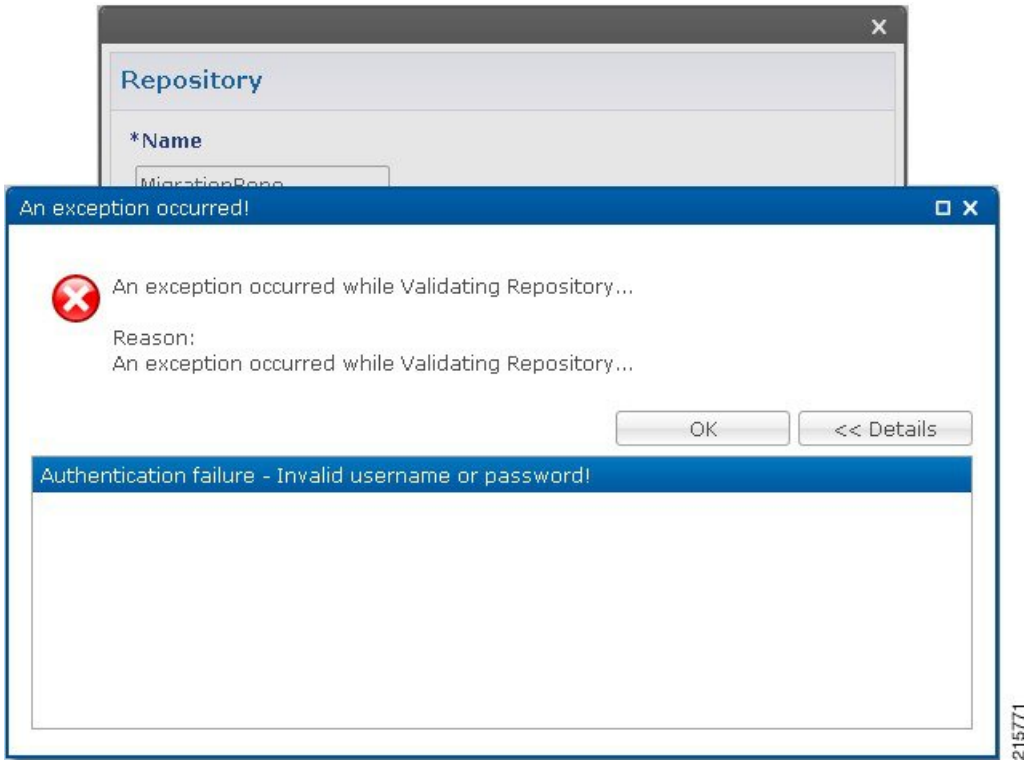
Caution Executing `restartall.sh` will cause messages to be dropped.

3. Verify CPS Status by running `diagnostics.sh` and `about.sh` scripts from Cluster Manager.

Not able to access Policy Builder

Scenario 1: When the svn-repos password expires the Policy Builder opens only in Read-only mode.

Scenario 2: Invalid username or password.



To resolve the errors described in Scenarios 1 and 2 above perform the following steps:

1. Login to Cluster Manager VM as the root user. The default credentials are root/cisco123.
2. Execute `change -l <username>` to check the status of repository password.

   For example,

```
[root@lab ~]# chage -l qns
Last password change : Jun 17, 2015
Password expires : Aug 16, 2015
Password inactive : never
Account expires : never
```

```
Minimum number of days between password change : 7
Maximum number of days between password change : 60
Number of days of warning before password expires : 7
```

3. If the password has expired, execute `change_passwd.sh` to change the password.

   ```
   /var/qps/bin/support/change_passwd.sh
   ```

4. When prompted, enter qns.

   ```
   Enter username whose password needs to be changed: qns
   ```

5. When prompted, enter and reconfirm the desired password for the policy server (qns) user.

   ```
   Enter new password:

   Re-enter new password:
   ```

   The script changes the policy server (qns) user password on all the CPS VMs in the cluster.

   ```
   Changing password on $host...

   Connection to $host closed.

   Password for qns changed successfully on $host
   ```

6. You can use the above steps to set or change the passwords for root and qns-svn users.

Note For more information about this and other CPS administrative commands, refer to the *CPS Operations Guide*.

Graphs in Grafana are lost when time on VMs are changed

Case: Graphs in Grafana are lost when system time on VMs are changed.

Solution: Change the system timing on all VMs. Also change the browser time according to graphite server time and restart the **`collectd`** service on each VM.

The graphite server time and browser time should match then only we will be able to see graphs.

Systems is not enabled for Plugin Configuration

Case: Systems configuration is not displayed for Plugin Configuration in Reference Data tab.

Possible Cause: This issue could occur if Systems plugin configuration is configured using system.json file.

Solution: Check whether your system.json file is valid or not using any json validator.

Publishing is not Enabled

Case: Publishing is not available

Possible Cause: SVN configuration is manually exported and imported from one setup to another. While performing import user missed to import .broadhopFileRepository or deleted it unknowingly.

Solution: Check whether `.broadhopFileRepository` is present in pcrfclient01. If it not present import the file.

Added Check to Switch to Unknown Service if Subscriber is deleted Mid Session

Problem: There is an impact on 7.5.0 and higher releases with a new feature "**check to switch to unknown service if subscriber is deleted mid session**" due to the custom policies defined in some customer locations.

Solution: For the customers who are on pre-7.5.0 release and don't want the new feature a work around has been suggested with an addition of custom policy that will bypass this feature.

The custom policy has to be added in the call flow based on the conditions. This custom policy will add a "IgnoreSPR" AVP to policy state. If this AVP is present internally the code will skip the feature.

Below are screenshots of the policy where the customer wants to skip the feature in some specific conditions of flow like when "**Authenticating a subscriber on AAA server**" since we don't store subscriber information in SPR.

Without this custom polices we will see session switching from known to unknown service during SPR update/Accounting. This will be visible in information logs in engine and policy server (qns) with "**Session has switched from known to unknown as subscriber could not be found**".

Conditions

Figure 20: Conditions - 1

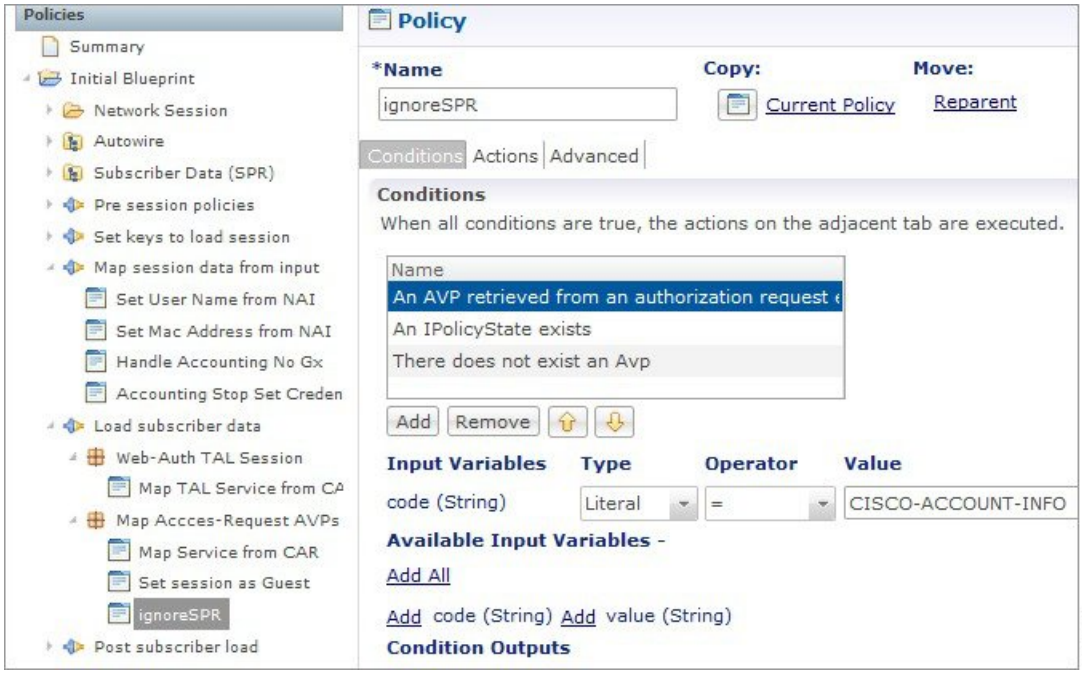


Figure 21: Conditions - 2

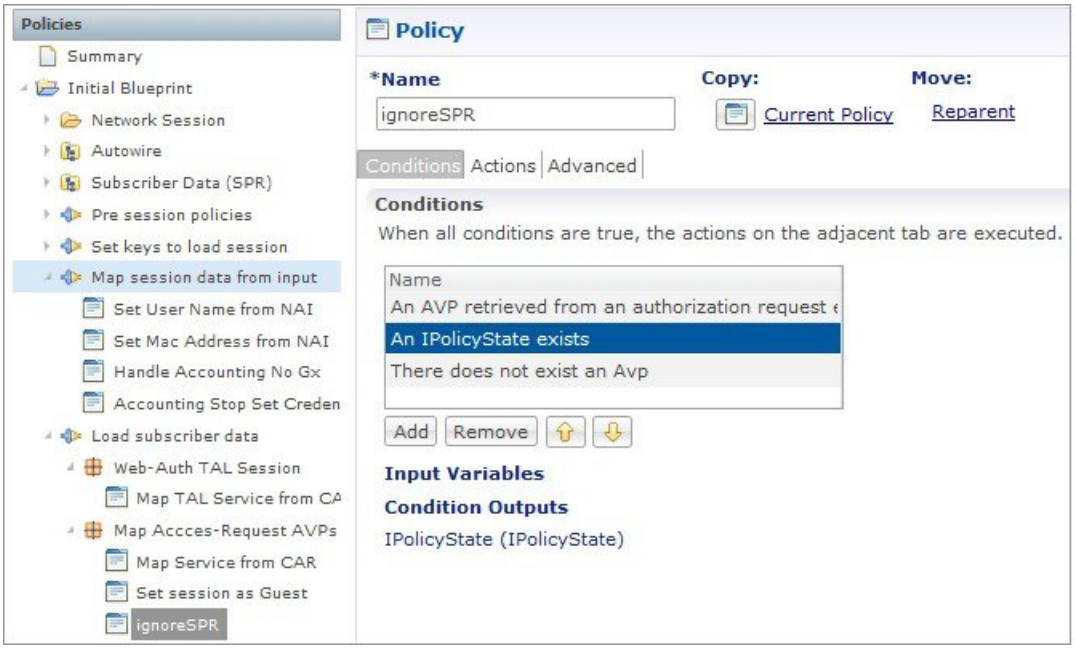
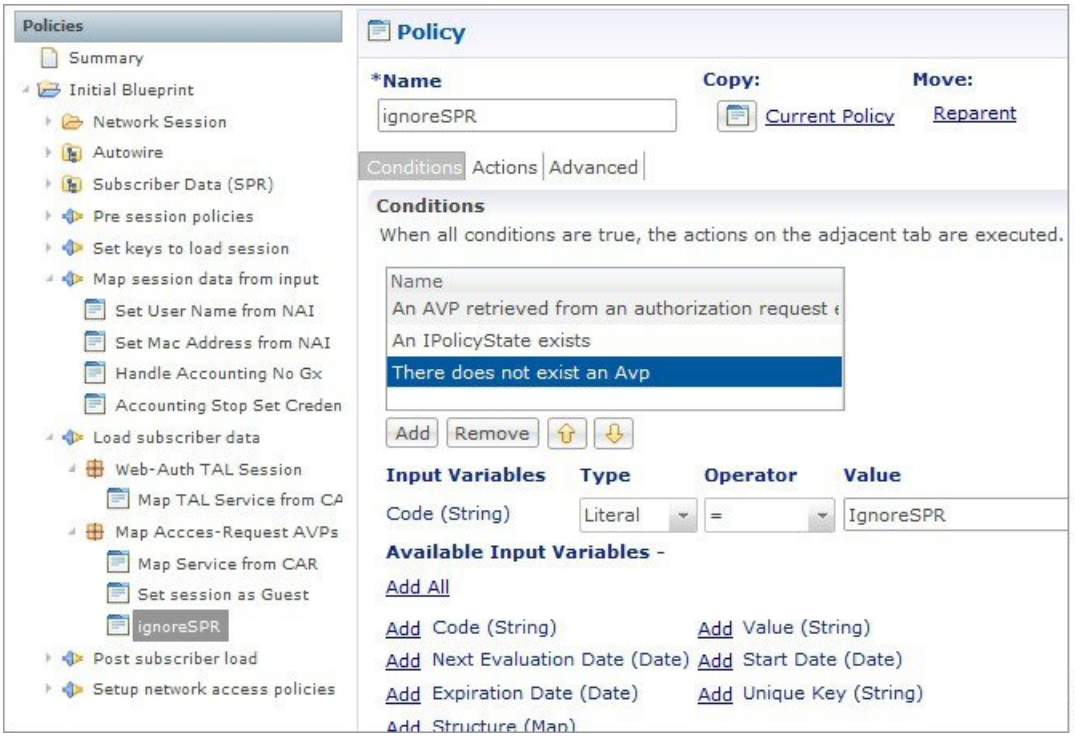


Figure 22: Conditions - 3



Actions

Figure 23: Actions - 1

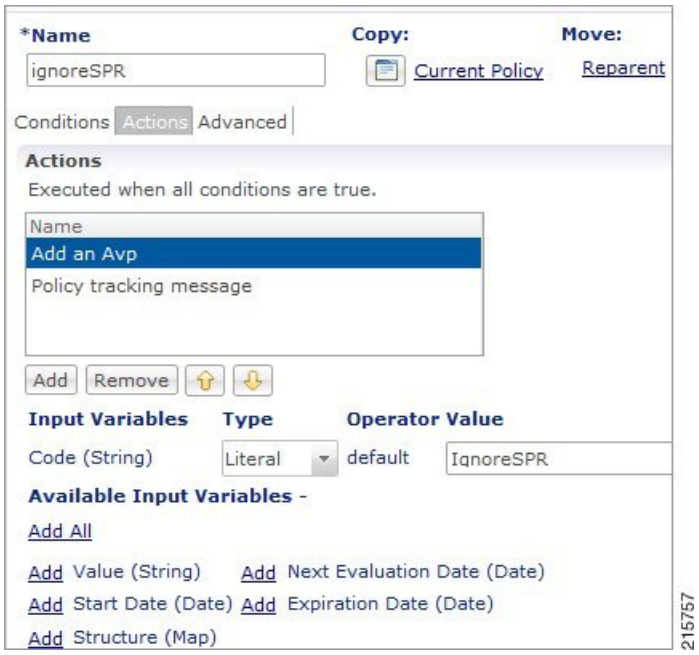
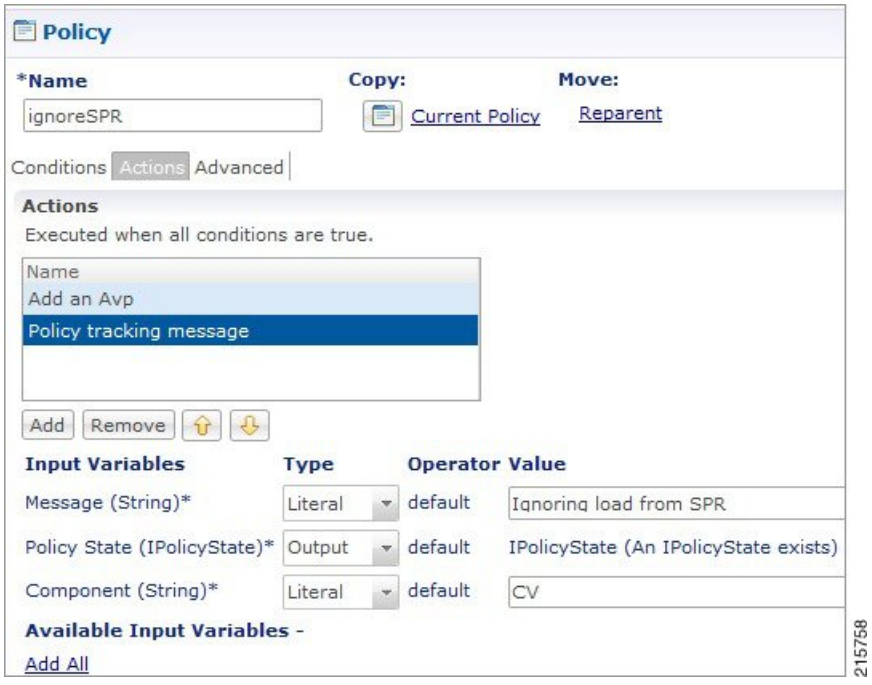


Figure 24: Actions - 2



Could not Build Indexes for Table

Issue: Policy Builder is not able to build indexes for table (Custom Reference Table).

Case: While publishing Policy Builder CPS logs below exception in policy server (qns) log.

For example,

```
ERROR c.b.custrefdata.impl.dao.GenericDao - Could not build indexes for table

QoS-Reference-Mapping

com.mongodb.CommandFailureException
```

Possible Cause: This could happen when CRD table key columns are changed from back-end (xmi) in Policy. Due to this underlying composite index on CRD table does not reflect new/changed key columns.

Solution: Drop the index on CRD table in MongoDB and publish the Policy Builder.

1. Drop index manually.

   ```
   db.<crdtablename>.dropIndexes()
   ```
2. Make sure xmi (backend) and Policy Builder data of CRD table whose index you want to drop are in sync.

   If both are not in sync, CPS displays `There are uncommitted changes to the '<PBrepositoryname>' repository. Do you wish to discard those changes?` while logging to the Policy Builder.

   For example, if CRD table data gets modified via backend (xmi) then when you login, CPS shows uncommitted message. Choosing **Retain** will sync up the xmi and Policy Builder.
3. Publish Policy Builder.
4. Check the rebuilt index.

   ```
   db.<crdtablename>.getindexes()
   ```

Error Submitting Message to Policy Director (lb) during Longevity

Case: Messages timed out intermittently. CPS logs reports following exceptions

```
2015-10-11 145054918 [pool-2-thread-1] ERROR c.b.d.p.event.DiameterMessageDealer.? - Error

submitting message to lb

2015-10-11 145054918 [pool-2-thread-1] ERROR c.b.d.p.event.DiameterMessageDealer.? - Error

submitting message to lb
```

Possible Cause: Message timed out intermittently problem happens when a GC pause greater than 10 seconds is occurring on policy server (qns) and policy director (lb). Due to this pause queue gets overloaded and there are message drops and timeouts. This pause happens when the service-qns logs are getting rotated with size 100 M.

Solution: The following changes need to be done on cluster manager

- Change Daily > hourly, size 100M > 25M and rotate 5 > 20

  ```
  cat /etc/logrotate.d/qps
  /var/log/broadhop/determine_cluster_state.log
  /var/log/broadhop/service-qns-*.log
  /var/log/elasticsearch/*.log
  ```

```
{
     daily
     nodateext
     copytruncate
     size 25M
     rotate 20
     missingok
     compress
}
```

- Copy the changes to all the VMs using `copytoall` command.

Mismatch between Statistics Count and Session Count

Case: There are no sessions on CPS but the statistics count still showing statistics.

```
#session_cache_ops.sh --count
Session cache operation script
Fri Nov 13 01:26:08 EST 2015
-------------------------------------------------------
Session Replica-set SESSION-SET1
-------------------------------------------------------
Session Database          : Session Count
-------------------------------------------------------
 session_cache            : 0
 session_cache_2          : 0
 session_cache_3          : 0
 session_cache_4          : 0
-------------------------------------------------------
 No of Sessions in SET1   : 0
-------------------------------------------------------

Total Number of Sessions  : 0

#session_cache_ops.sh --statistics-count
Session cache operation script
Fri Nov 13 01:26:31 EST 2015
-------------------------------------------------------
 Sessions statistic counter on Genaral
-------------------------------------------------------
  Session Type         : Session Count
-------------------------------------------------------
ADMIN-SET1
  RX_TGPP              : 364
  GX_TGPP              : 983269
  SY_PRIME             : 974457
-------------------------------------------------------
#
```

Possible Cause: CPS monitors the session count and updates the aggregation of message type into counters collection in the admin database. This query is performed on secondary databases. If due to some reason all secondary members are not in healthy state or are in recovering state, then we can incur that the discrepancy is in session count.

```
mongo rtpclabqps5g-sm01a:47721
MongoDB shell version: 2.6.3
set05:PRIMARY> use sharding
set05:PRIMARY> db.counters.find()
{ "_id" : 8, "db" : "session_cache_3", "session_type" : [ ] }
{ "_id" : 9, "db" : "session_cache_4", "session_type" : [ ] }
{ "_id" : 10, "db" : "session_cache", "session_type" : [ { "type" : "SY_PRIME", "count" :
246563 },
```

```
{ "type" : "GX_TGPP", "count" : 248921 }, { "type" : "RX_TGPP", "count" : 93 } ] }
{ "_id" : 11, "db" : "session_cache_2", "session_type" : [ { "type" : "SY_PRIME", "count"
: 247330 },
{ "type" : "GX_TGPP", "count" : 249614 }, { "type" : "RX_TGPP", "count" : 94 } ] }
{ "_id" : 12, "db" : "session_cache_3", "session_type" : [ { "type" : "SY_PRIME", "count"
: 227624 },
{ "type" : "GX_TGPP", "count" : 229542 }, { "type" : "RX_TGPP", "count" : 90 } ] }
{ "_id" : 13, "db" : "session_cache_4", "session_type" : [ { "type" : "SY_PRIME", "count"
: 252940 },
{ "type" : "GX_TGPP", "count" : 255192 }, { "type" : "RX_TGPP", "count" : 87 } ] }
{ "_id" : 18, "db" : "session_cache_2", "session_type" : [ ] }
```


Diagnostic showing all secondary members are in bad shape:

Figure 25: Secondary Members

Consolidated CPS log throws below exception


```
rtpclabqps5g-qns09b  rtpclabqps5g-qns09b 2015-11-13 03:06:45,603 [pool-2-thread-1] WARN
c.b.c.m.dao.impl.ShardInterface - Unable to get direct connection for DB shard { "_id" :
10 ,
"seed_1" : "sessionmgr21" , "seed_2" : "sessionmgr22" , "port" : 27737 , "db" :
"session_cache" ,
"online" : true , "count" : 0 , "backup_db" : false , "lockTime" : { "$date" :
"2015-11-13T08:06:25.997Z"} , "isLocked" : false , "lockedBy" :  null } - bypassing type
counts
rtpclabqps5g-qns09b  rtpclabqps5g-qns09b 2015-11-13 03:06:45,605 [pool-2-thread-1] WARN
c.b.c.m.dao.impl.ShardInterface - Unable to get direct connection for DB shard { "_id" :
11 ,
"seed_1" : "sessionmgr21" , "seed_2" : "sessionmgr22" , "port" : 27737 , "db" :
"session_cache_2" ,
"online" : true , "count" : 0 , "backup_db" : false
```


Solution: Recovers all the secondary database members.

Disk Statistics not Populated in Grafana after CPS Upgrade

Case: After CPS upgrade disk statistics are not populated in Grafana.

Possible Cause: Configurations are not refreshed after collectd package is upgraded.

Solution: Restart collectd service on respective VM/VMs.

Re-create Session Shards

All sessions require to be cleared/removed from CPS.

Note Steps are NOT recommended to be performed in Production environment.

To delete all shards and then re-create shards, perform the following steps:

Step 1 Take the backup of admin database.

a) Run diagnostics command on pcrfclient01 and find admin database primary member and port

```
diagnostics.sh --get_replica_status
```

Table 6: Admin Database and Port Information

SET NAME	PORT	IP ADDRESS	REPLICA STATE	HOST NAME	HEALTH	LAST SYNC	PRIORITY
ADMIN:set06							
Member-1	27721	192.167.82.35	ARBITER	pcrfclient01	ON-LINE	-------	0
Member-2	27721	192.167.82.29	PRIMARY	sessionmgr01	ON-LINE	-------	1
Member-3	27721	192.167.82.30	SECONDARY	sessionmgr02	ON-LINE	0	1

b) Execute `mongo dump` command with primary member, and port to backup admin database:

```
mongodump --host sessionmgr01 --port 27721
```

This command creates the mongo dump files in the file system.

Step 2 Clear all sessions from all the shards (execute command from pcrfclient01)

```
session_cache_ops.sh --remove
```

When prompted for input, input **`yes`**

Step 3 To recreate the shards you have two options:

a) Option-1: Delete or drop the “sharding” database and recreate the shards.

1. Stop all QNS process using `stopall.sh` script.

```
PRIMARY> use sharding
PRIMARY> Db.dropDatabase()
```

2. Start all QNS process using `startall.sh` script.
3. Once diagnostics shows green, you can start OSGi command to create the shards.

b) Option-2: Delete the collection entries in the “sharding” database.

1. Login to the ADMIN replica-set primary member by executing `mongo --sessionmgr01 --port 27721` and drop the “sharding” database.

```
PRIMARY> use sharding
PRIMARY> db.shards.remove({});
PRIMARY> db.buckets.remove({});
PRIMARY> db.config.remove({});
PRIMARY> db.instances.remove({});
```

2. Start and execute OSGi command to create the shards.

Step 4 (Optional) Change default shards (skip this step if default shard does not need to be changed).

By default, one shard gets created. Default shard is sessionmgr01/sessionmgr02 27717.

In case user wants to change default shards, add/modify following parameter in `/etc/broadhop/qns.conf` file on cluster manager.

-Dsession.db.init.1=sessionmgr01

-Dsession.db.init.2=sessionmgr02

-Dsession.db.init.port=27717

Copy this file to all nodes (run script from Cluster Manager)

```
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf
```

Step 5 Restart policy server (QNS) services (execute script from cluster manager).

```
restartall.sh
```

Caution Executing `restartall.sh` will cause messages to be dropped.

Step 6 Once policy servers (QNS) are UP, verify default shard is created in shard collection.

a. Login to admin database.

mongo - sessionmgr01 -port 27721

Check for default shard.

set01:PRIMARY> use sharding

set01:PRIMARY> db.shards.count();

{

"_id" : 1,

"seed_1" : "sessionmgr01",

"seed_2" : "sessionmgr02",

"port" : 27717,

"db" : "session_cache",

"online" : true,

"count" : NumberLong(0),

"lockTime" : ISODate("2016-02-04T11:41:47.259Z"),

"isLocked" : false,

"lockedBy" : null

}

Step 7 To add shard, refer to section Create Session Shards in *CPS Installation Guide for VMware*.

Session Switches from Known to Unknown in CCR-U Request

Case: On running a load with Total TPS of 1200 for a CPS having four policy servers (qns) and for 500000 subscribers it was seen that for some of the CCR-U request the CPS sends "Session has switched from known to unknown as subscriber could not be found" causing the CCA-U to give a result code of 5012.

The call model that is used here is a simple Gx call model involving several CCR-U for Charging-Rule-Report were the subscribers are provisioned in a Auto-provisioning manner.

Possible Cause: The call model being run was auto provisioning call model with 200 TPS CCR-I 800 CCR-U and 200 CCR-T. On every CCR-I we had a subscriber being automatically provisioned and the balance provisioned automatically with the Automatic Balance Provisioning service.

We saw lot of locking errors for balance being the cause as there was a version mismatch being seen while updating balance.

```
qns02 qns02 2016-02-11 06:11:21,231 [pool-1315-thread-1] ERROR
c.b.b.i.d.i.MongoBalanceRepository -
Cache data is out of date for object 0057170054ce8d1a56bc6c59
qns03 qns03 2016-02-11 06:11:22,041 [pool-1308-thread-1] WARN
c.b.b.i.a.AutowireBalanceManagerBlueprint - Couldn't find a current Account Balance Status
 for
template: daily
qns02 qns02 2016-02-11 06:11:21,232 [pool-1315-thread-1] WARN
c.b.d.p.g.t.DiameterGxTGPPDeviceMgr -
Issue getting reservation status for external reservation id: 1234ds1;338812;2613626736,
Balance
Code 1234, Subscriber Id: 0057170054ce8d1a56bc6c59
com.broadhop.exception.CachedDataIsOutOfDate: Optimistic Locking Error - the version number
 does
not match the database version for subscriber: 0057170054ce8d1a56bc6c59
```

Solution: Thus with balance auto provisioning enabled and high TPS of balance provisioning (high CCR-I TPS which causes balance to be provisioned) it is suggested to keep the **Db Read Preference** as **Primary** or **PrimaryPreferred** under **Balance Configuration** plug-in in Policy Builder. This will avoid the balance locking errors.

Intermittent BSON Object Size Error in createsub with Mongo v3.2.1

Case: While retrieving/searching subscriber profile using CPS Control Center/Unified API or using mongo client, the query results into BSONObj Size error. Due to this error, the subscriber is not displayed and an error is recorded in MongoDB.

Example:

```
set27:PRIMARY> db.subscriber.findOne({"credentials_key.network_id_key" : "910010100034"})
2016-02-17T02:42:18.263-0500 E QUERY [thread1] Error: error: {
"ok" : 0,
"errmsg" : "BSONObj size: 117440514 (0x7000002) is invalid. Size must be between 0 and
16793600(16MB) First element: id: ?type=95",
"code" : 10334
} :
```

Possible Cause: Data corruption can have many causes.

Solution: Repair all databases:

Step 1 Repair all secondary databases.

```
mongo <hostname>:<port>/spr --eval "db.repairDatabase();"
```

Step 2 Repair primary database.

```
/etc/init.d/sessionmgr-<port#> repair
```

Step 3 After stopping check another secondary has become primary or not.

```
/etc/init.d/sessionmgr-<port#> repair
```

```
ps -ef | grep <port#>
```

Step 4 After repairing, mongod process will be stopped. Make sure it is not running.

```
/etc/init.d/sessionmgr-<port#> start
```

Note Repairing database takes more time when database size is more (approx 30 sec for 1 GB database), so this activity should be performed in maintenance window (in non-peak hour).

No Traps Generated When Number of Sessions Exceeds the Limit

Case: No traps are generated for license threshold when number of sessions exceeds the assigned limit.

Possible Cause: Parameter not added in qns.conf file.

Solution:

Step 1 To generate license usage threshold trap, we need to configure the following parameter in `/etc/broadhop/qns.conf` file.

```
-Dcom.cisco.enforcementfree.mode=false
```

Step 2 After adding the above entry in qns.conf file, execute `copytoall.sh` to synchronize the configuration changes to all VMs in the CPS cluster:

```
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf
```

Step 3 After modifying the configuration file, to make the changes permanent for future use (when any VM is redeployed or restarted...etc.), user needs to rebuild etc.tar.gz.

```
/var/qps/install/current/scripts/build/build_etc.sh
```

Step 4 Restart the CPS service.

```
/var/qps/bin/control/restartall.sh
```

Caution Executing `restartall.sh` will cause messages to be dropped.

RAR Message Not Received

Case: Sometimes the RAR message is not sent out from policy director (lb) even though CPS records in engine logs that the message (RAR, ASR and so on) has been sent. It is an intermittent behavior.

The following logs can be seen on the occurrence of this issue:

```
qns02  qns02 2016-02-22 18:07:31,634 [pool-2-thread-1] DEBUG c.b.d.p.registry.EndpointRegistry
 - No
endpoint available and current endpoint is down lb01-4:diameter-lb site null
qns02  qns02 2016-02-22 18:07:31,634 [pool-2-thread-1] DEBUG c.b.d.p.registry.EndpointRegistry
 -
Unable to get alternate endpoint for realm site-rx-client.com, host site-host-rx. Setting
destination to null.
```

Possible Cause: This issue may occur if the correct value of the parameter `-Ddiameter.peer.reload.interval` is not configured in `/etc/broadhop/qns.conf` file.

CPS reloads the peer endpoints after every 30 seconds. It also reloads endpoints whenever there is an occurrence of peer flapping or new peer tries to connect.

To avoid unnecessary reloading of endpoints CPS checks that if endpoint reload request comes within the 3 second interval after 30 seconds regular reload. If the reload request does not come within the stipulated time CPS does not allow to reload.

Sometimes if request comes within this 3 second interval then the request is not processed and endpoints are not loaded due to which the message in question at that time will not be sent out from policy director (lb) though it is visible in engine logs that the message has been sent out.

Solution: This 3 second interval can be tweaked using `-Ddiameter.peer.reload.interval` parameter in `/etc/broadhop/qns.conf` file.

If it is kept to default value (0 millisecond) then there is a very less probability of collision so a 0 millisecond or very small value is advisable.

Admin Database shows Problem in Connecting to the Server

Case: Admin database shows problem in connecting to the server in diagnostics. It throws the following error message while checking replica set status.

```
diagnostics.sh --get_replica_status

Current setup have problem while connecting to the server on port 27721
```

Possible Cause: The oplog collection is a circular capped collection. It is possible that the corruption occurred due to abrupt failure of VM and exception comes when the collection wrapped around to the corrupted region.

- Check which specific replica-set member is corrupted. It can be verified using rs.status() command.

  For example,

  ```
  mongo sessionmgr01:27721
  >rs.status()
  "_id" : 3,
  "name" : "L3-CA-SEC-sessionmgr01:27721",
  "health" : 1,
  "state" : 2,
  "stateStr" : "SECONDARY",
  "lastHeartbeatMessage" : "syncThread: 17322 write to oplog failed: InternalError no
  space in capped collection",
  "syncingTo" : "L3-CA-SEC-sessionmgr02:27721"
  ```

- Also verify if mongo logs shows the following related errors:

  ```
  2016-03-09T14:33:24.101+0530 [rsHealthPoll] replSet member L3-CA-SEC-sessionmgr01:27721
   is up
  2016-03-09T14:33:24.101+0530 [rsHealthPoll] replSet member L3-CA-SEC-sessionmgr01:27721
  ```

```
 is now in state SECONDARY
2016-03-09T14:33:29.801+0530 [rsSync] couldn't make room for new record (len: 172) in
capped ns local.oplog.rs
2016-03-09T14:33:29.801+0530 [rsSync]   Extent 0
2016-03-09T14:33:29.801+0530 [rsSync]  (capExtent)
2016-03-09T14:33:29.801+0530 [rsSync]
2016-03-09T14:33:29.801+0530 [rsSync]     magic: 41424344 extent->ns: local.oplog.rs
2016-03-09T14:33:29.801+0530 [rsSync]    fr: null lr: 1:1b8dedd4 extent->len: 1073741824
2016-03-09T14:33:29.801+0530 [rsSync] local.oplog.rs Assertion failure len * 5 >
_lastExtentSize
src/mongo/db/structure/catalog/namespace_details.cpp 366
```

Solution: Make sure there is at least one surviving member that is primary database member using `rs.status()` command.

1. Stop mongo process.

   ```
   /etc/init.d/sessionmgr-27721 stop
   ```

2. Go to the data directory.

   For example,

   ```
   cd /var/data/sessions.3
   ```

3. Take backup of local file at a temporary location.

   ```
   ls -l local*

   -rw------- 1 root root 67108864 Jan 7 2253 local.0

   -rw------- 1 root root 2146435072 Jan 27 0251 local.1

   -rw------- 1 root root 16777216 Jan 27 0251 local.ns
   ```

4. Remove the local files.

   ```
   rm -rf local.*
   ```

5. Start the mongo process.

   ```
   /etc/init.d/sessionmgr-27719 start
   ```

6. Check whether the local files have been re-created again.

   ```
   ls -l local*

   -rw------- 1 root root 67108864 Jan 7 2253 local.0

   -rw------- 1 root root 2146435072 Jan 27 0251 local.1

   -rw------- 1 root root 16777216 Jan 27 0251 local.ns
   ```

7. Repeat Step 1 to Step 6 for other corrupted member.

Corosync Process Taking lot of Time to Unload and is Stuck

Issue: The corosync process is taking a lot of time to unload and is stuck.

Solution: If user finds corosync process is stuck, while doing `monit restart corosync` or `monit stop corosync`, perform the following steps:

Step 1 Exit from the process by pressing `Ctrl+c`.

Step 2 Note down corosync process *pid* by executing the following command:

```
cat /var/run/corosync.pid
```

Step 3 Stop coroysnc and its child processes by executing the following command:

```
kill -2 <coroysnc process pid>
```

Step 4 Check whether all the corosync and all the child processes are stopped by executing the following command:

```
ps -ef | grep "corosync\|pacemaker"
```

Step 5 If you are still seeing that the processes are UP then kill all the processes (corosync and pacemaker), which are shown in Step 4, on page 81 by executing the following commands:

```
kill -9 <all pid of processes, space seprated>
```

Old VIP is not deleted After Modifying VIP Name

If VIP name is modified then user has to manually delete old VIP from active policy director (lb)/OAM (pcrfclient) using the following below command:

```
pcs resource delete <old-vip-name>
```

where, <*old-vip-name*> is the old VIP name.

lbvip not moving to Secondary Policy Director (lb) VM

Issue: lbvip does not move cleanly to the secondary policy director (lb) VM when the network on primary policy director (lb) VM is stopped.

Scenario: For example, consider lbvip is on lb01 VM.

To stop the network on lb01 VM, execute the following command:

```
service network stop
```

lbvip moves to lb02 VM immediately but it is not pingable from anywhere which stops the traffic and grafana.

After performing `service network restart` on lb02 VM, the traffic restored partially with lot of errors (and lbvip is pingable from everwhere).

After stopping the network on lb01 VM, lbvip was seen on both the lb VMs (even after doing network restrat on lb02 VM).

Solution:

Before executing `service network stop`, stop corosyn from the node using `monit stop corosync` command.

Note This is needed since corosync has the functionality to bring up an interface if they are down. So after `service network stop` is executed all interfaces are down and corosync brings up the interfaces (like, eth0:0, eth1:0, and so on).

Running Puppet on Cluster Manager in HA Setup

Issue: After applying patch or updating kernel in HA setup, when you run `puppet apply` command `/etc/httpd/conf/httpd.conf` file was modified, not all VMs are configured with the modified `httpd.conf` file:

Solution: After applying a patch or updating kernel in HA setup, run the following command from Cluster Manager:

```
puppet apply --logdest=/var/log/cluman/puppet-custom-run.log --
modulepath=/opt/cluman/puppet/modules --config=/opt/cluman/puppet/ puppet.conf
/opt/cluman/puppet/nodes/node_repo.pp
```

Note Manually enter `puppet apply` command in your system.

After applying the `puppet apply` command, run the following command from Cluster Manager to update the `/etc/httpd/conf/httpd.conf` file on all VMs:

```
/var/qps/install/current/scripts/modules/update_httpd_conf.py
```

SNMP Traps and Key Performance Indicators (KPIs)

Full (HA) Setup

Step 1 Check whether `snmpd` service is running on all VMs. If the service is not running then start it by executing the command:

```
monit start snmpd
```

Step 2 Check whether `snmptrapd` is running on policy director (lb) VMs. If the service is not running then start it by executing the command:

```
monit start snmptrapd
```

Step 3 On pcrfclient01:

a) Verify whether `/etc/broadhop/<server_name>/snmp/manager.xml` file has the following content. If the content is not present, add the following content to the file:

Note server_name details can be found from `/etc/broadhop/server` file.

```
<manager-list>
  <manager>
    <address>localhost</address>
    <port>162</port>
    <version>1</version>
  </manager>
</manager-list>
```

b) Execute the command `syncconfig.sh` so that the change done in Step 3.a, on page 82 gets synchronized to all VMs.

c) Execute the command `restartall.sh` to restart all policy server (qns) processes.

Caution Executing `restartall.sh` will cause messages to be dropped.

d) Verify whether service monit is running or not. If the service is not running then start it by executing the command:

```
service monit start
```

Note If monit in not installed on OAM (pcrfclient) VMs, then you need to get the monit rpm and install it in on all OAM (pcrfclient) VMs.

e) Verify whether `monit.conf` file has entries of check_program executing different traps generating script. If the entries are not present, then get the latest `monit.conf` file for OAM (pcrfclient) VMs and update it on all OAM (pcrfclient) VMs setup.

f) Restart monit service.

```
service monit start
```

Step 4 On policy director (lb) VMs:

a) Verify whether `/etc/hosts` file has the entry as `corporate_nms_ip <ip_address>`.

Note <*ip_address*> is the NMS address.

b) Verify whether service monit is running or not, If the service is not running then start it by executing the command:

```
service monit start
```

Note If monit in not installed on policy director (lb) VMs then you need to get the monit rpm and install it on all policy director (lb) VMs.

c) Verify whether `monit.conf` file has entries of check_program executing different traps generating script. If the entries are not present then get the latest `monit.conf` file for policy director (lb) VMs and update it on all policy director (lb) VMs,

d) Restart monit service.

```
service monit start
```

All-in-one (AIO) Setup

Step 1 Verify whether snmpd and snmptrapd services are running. If the services are not running, then start them by executing the following commands:

```
monit start snmpd

monit start snmptrapd
```

Step 2 Verify whether `/etc/broadhop/<server_name>/snmp/manager.xml` file has below content. If the content is not present, add the following content to the file:

Note server_name details can be found from `/etc/broadhop/server` file.

```
<manager-list>
<manager>
<address>localhost</address>
<port>162</port>
<version>1</version>
</manager>
</manager-list>
```

Step 3 Execute `restartall.sh` command to restart all Policy Server (qns) processes.

Caution Executing `restartall.sh` will cause messages to be dropped.

Step 4 Verify whether `/etc/hosts` has entry as `corporate_nms_ip <ip_address>`.

Note <*ip_address*> is the NMS address.

Step 5 Verify whether service monit is running or not. If the service is not running then start it by executing the command:

```
service monit start
```

Testing Traps Generated by CPS

The following tables describe the SNMP notifications (traps) generated by CPS as well as the procedures that can be used to test their operation.

For a complete list of CPS traps, including detailed descriptions, refer to the *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases.

Component Notifications

Table 7: Component Notifications

Alarm Name	Procedure to Test
DiskFull	**1.** In `/etc/snmp/snmpd.conf`, set "disk / 90%". (So when disk remaining is 90% i.e. Disk occupied is 10%, alarm is generated.) **2.** Restart the snmpd process. **monit restart snmpd** **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (lb). **4.** Trap have messages like :dskErrorMsg.1 = STRING: /: less than 90% free (= 100%)

Alarm Name	Procedure to Test
DiskFull	**1.** In `/etc/snmp/snmpd.conf`, set "disk / X%". (X should just less than actual remaining space. For example, if drive / is 25% full, put 74% as value of X). **2.** Restart the snmpd process. **monit restart snmpd** **3.** Now dump a big file which consumes at least 2-3 % space on drive /. This generates diskful alarm first. **4.** Delete this file. This generates clear alarm. **5.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (lb).
HighLoadAlert	**1.** In `/etc/snmp/snmpd.conf`, set "load 1 1 1". (first digit corresponds to average 1 min load. Second digit is for 5 minutes average load. Third is for 15 mins. When it crosses 1 %, alarm is generated.) **2.** Restart the snmpd process. **monit restart snmpd** **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (lb). **4.** Trap have message like 1 min Load Average too high (= 1.41)
HighLoadClear	**1.** In `/etc/snmp/snmpd.conf`, set "load 1 1 1". (first digit corresponds to average 1 min load. Second digit is for 5 minutes average load. Third is for 15 mins. When load is below value (as mentioned 1 %), clear alarm is generated.) **2.** Restart the snmpd process. **monit restart snmpd** **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (lb).
LowSwapAlert	**1.** **swapoff -a** This command disables all swap areas. Use the top command to see that the swap has been disabled: "**Swap: 0k total**". **2.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (lb): "QNS component notification Running out of swap space".

Alarm Name	Procedure to Test
LowSwapClear	**1.** **swapon -a** This command enables all swap areas again. The top command output shows the correct swap memory size (not 0k total). The clear trap gets generated if swap alarms was generated earlier. **2.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb): “QNS component notification Swap space recovered”.
Link Down	**1.** ifconfig <*interface_name*> down (For example, ifconfig eth2 down) **2.** Within 1 minute interval interface down trap gets generated. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Link Up	**1.** ifconfig <*interface_name*> up (For example, ifconfig eth2 up) **2.** Within 1 minute interval interface up trap gets generated **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
LowMemoryAlert	**1.** In output of top command find out the current free RAM memory value. **2.** Update `snmpd.conf` file monitor entry for Low Memory Alert to have value just less than the current free RAM memory value. **3.** Restart the snmpd process. **monit restart snmpd** **4.** Do some activity on VM such as running some command or starting some process so that free RAM value goes below the configured value. **5.** The low memory alert alarm gets generated within a minute interval. **6.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
LowMemoryClear	**1.** In output of top command find out the current free RAM memory value. **2.** Update **snmpd.conf** file monitor entry for Low Memory Clear to have value just more than the current free RAM memory value. **3.** Restart the snmpd process. **monit restart snmpd** **4.** Kill some processes on VM so that free RAM memory value is more than the configured value. **5.** The low memory clear alarm gets generated within a minute interval. **6.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
ProcessDown	**1.** On the Load Balancer VMs, issue the following command to stop the corosync process: **monit stop corosync** **2.** Within 5 minutes of interval process down trap is generated. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb): “QNS component notification corosync process is down”.
ProcessUp	**1.** Issue the following command to restart the **corosync** process: **monit start corosync** **2.** Within 5 minutes of interval process up trap is generated. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb):“QNS component notification corosync process is up”.
HIGH CPU USAGE Alert	**1.** Change the threshold value for the CPU usage alert (cpu_usage_alert_threshold) to a lower value. The default value is 80 percent. Refer to the *CPS SNMP, Alarms and Clearing Procedures Guide* for steps to configure this threshold. **2.** The system generates an Alert trap whenever the CPU usage of the VM goes above be higher than this value. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
HIGH CPU USAGE Clear	**1.** Change the clear threshold value for CPU usage (cpu_usage_clear_threshold) to a higher value. The default value is 40 percent. Refer to the *CPS SNMP, Alarms and Clearing Procedures Guide* for steps to configure this threshold. **2.** The system generates a Clear trap whenever the CPU usage of the VM drops below this threshold value. It is generated only when a High CPU Usage Alert was generated earlier. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Application Notifications

Table 8: Application Notifications

Alarm Name	Procedure to Test
MemcachedConnectError	**1.** Kill the memcached process running on active policy director (lb). **2.** Within 5 minutes of interval memcached Connect Error trap gets generated from policy server (QNS) VMs. **3.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
ApplicationStartError	**Note** Take the configuration backup before applying the procedure. **1.** Remove the balance configuration from Policy Builder and publish the changes. **2.** Restart the policy server (QNS) process. **3.** Within 5 minute of interval ApplicationStartError trap gets generated on active policy director (lb). **4.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
License Usage Threshold Exceeded	**1.** Create the license having small number of Usage Threshold limit. **2.** Install the above created license on setup. **3.** Restart all policy server (QNS) processes. **4.** Send multiple request so that it crosses the threshold limit. **5.** The License Usage Threshold Exceeded alarm gets generated. **6.** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
LicensedSessionCreation	1. Create the license having small number of Session Usage Threshold limit. 2. Install the above created license on setup. 3. Restart all policy server (QNS) processes. 4. Send multiple request so that it crosses session threshold limit. 5. For the next request after the limit over LicenseSessionCreation alarm gets generated. 6. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
InvalidLicense	1. Copy the license of pcrfclient02 on pcrfclient01 or create a license for pcrfclient02 and install it on pcrfclient01. 2. Restart **lmgrd** service. 3. Restart the policy server (QNS) process. 4. Within 5 minutes of interval the License invalid trap gets generated. 5. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
PolicyConfiguration	1. Configure some wrong policy in Policy Builder under the Policies tab. 2. Publish the configuration. 3. **restartall.sh**. 4. Last policy configuration failed with the following message:xxx trap gets generated. 5. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
PoliciesNotConfigured	1. Create the invalid blueprint (java code having syntax error) in Policy Builder under the Policies tab. 2. Assign the created blueprint to some policies. 3. Publish the configuration. 4. Restart all policy server (QNS) processes. 5. PoliciesNotConfigured trap gets generated. 6. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
DiameterPeerDown	1. Make a seagull diameter call. 2. After seagull script terminate it generates the diameter peer down trap. 3. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
DiameterAllPeersDown	1. Integrate CPS with two Seagull/SITE Instances. 2. Make a seagull diameter call. 3. Simultaneously make a diameter call from another Seagull/SITE Instance. 4. After two Seagull/SITE scripts terminate it generates the DiameterAllPeersDown trap. 5. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
HA_Failover	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. If there are two or more sessionmgr ports configured as replica set then find out the one acting as a primary member using rs.isMaster().primary. 3. Shutdown the primary instance of sessionmgr. 4. Within 1 minute of interval HA Failover trap gets generated. 5. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
GR_Failover	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. There should be primary and secondary member set for each replica set. Find the current active sessionmgr instance of a replica set using rs.isMaster().primary. 3. Shutdown all sessionmgr instances of active sessionmgr instance set. 4. Within 1 minute of interval Geo Failover trap gets generated. 5. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
All DB Member of replica Down	1. Get all members of replica set from `/etc/broadhop/mongoconfig.cfg`. 2. Go to each sessionMgr of a replica set and stop the sessionmgr service or shutdown the sessionmgr VM. 3. Within 5 minutes of interval All replicas of DB Down trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
All DB Member of replica Up	1. Perform the steps above to generate the All DB Member of replica Down trap. 2. Once that trap is generated, start the session manager service or bring up the sessionmanager VM. 3. Within 5 minutes of interval All DB Member of replica Up trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
No Primary DB Member Found	1. Run **diagnostics.sh -get_replica_status**. 2. Choose any set which has arbiter and primary and secondary database member. 3. Shutdown Arbiter VM. 4. Shutdown Primary Session Manager VM. 5. Within 5 minutes of interval No primary Member found trap gets generated. 6. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Primary DB Member Found	1. Run **diagnostics.sg -get_replica_status**. 2. Choose any set which has arbiter and primary and secondary database member. 3. Shutdown Arbiter VM. 4. Shutdown Primary Session Manager VM or stop the corresponding mongo set process. 5. After 5 minutes, power on the Primary Session Manager VM. 6. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
DB Member Down	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. Shutdown any of the sessionmgr VM listed in the configuration as database member of replica set. 3. Within 5 minutes of interval database down trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
DB Member Up	1. Perform the steps above to generate the DB Member Down trap. 2. After 5 minutes, power on the sessionmgr VM (the secondary database) that was shutdown earlier. 3. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Arbiter Down	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. Shutdown any of the Arbiter VMs listed in the configuration. 3. Within 5 minutes of interval Arbiter down trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Arbiter Up	1. Perform the steps above to generate the Arbiter Down trap. 2. After 5 minutes, power on the Arbiter VM that was shutdown earlier. 3. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
DB resync is needed	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. Shutdown any of the sessionmgr VM (the secondary database) listed in the configuration as database member of replica set. 3. From Primary member find out oplog holding seconds, using below command: **mongo --host <primary host name> --port <DB port number> --eval 'rs.printReplicationInfo()' | grep 'log length start to end'** 4. Wait till oplog holding seconds and check shutdown database member is in the RECOVRING state, using below command: **diagnostics.sh --get_replica_status** 5. When this database member goes to 'RECOVERING' state. After 5 minutes of interval 'DB resync is needed' trap gets generated. 6. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
DB resync is not needed	1. Power on the sessionmgr VM (the secondary database) that was shutdown early. 2. Stop the sessionmgr mongod process, using below command (XXXXX change to database port number). **/etc/init.d/sessionmgr-XXXXX stop** 3. Clear data directory of that sessionmgr (specify correct data directory path). **\rm -fr <data directory path of that mongod>** 4. Start the sessionmgr mongod process, using below command (XXXXX change to database port number). **/etc/init.d/sessionmgr-XXXXX start** 5. When this database member goes to 'SECONDARY' state. After 5 minutes of interval 'DB resync is not needed' trap gets generated, using below command: **diagnostics.sh --get_replica_status** 6. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
Config Server Down	1. Cat `/etc/broadhop/mongoConfig.cfg`. 2. Shutdown any of the Config Server VMs listed in the configuration. 3. Within 5 minutes of interval, Config Server Down trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Config Server Up	1. Perform the steps above to generate the Config Server Down trap. 2. After 5 minutes, power on the Config Server VM that was shutdown earlier. 3. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
VM Down	1. Cat `/etc/hosts` file on policy director (lb) VM. 2. Shutdown and power off any of the VMs listed under /etc/hosts. 3. Within 5 minutes of interval VM down trap gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
VM Up	1. Perform the steps above to generate the VM Down trap. 2. After 5 minutes, power on the VM that was shutdown earlier. 3. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
QNS Process Down	1. Stop the policy server (QNS) process using the command: **monit stop qnsXX**. 2. Within 5 minutes of interval CPS process down trap gets generated. 3. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
QNS Process Up	1. Perform the steps above to generate the CPS Process Down trap. 2. After 5 minutes, start the process again using the command: **monit start qnsXX**. 3. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
Admin Logged In	1. Create a new telnet session for any VM and login with root user on it. 2. Within 1 minute interval Admin User logged in trap gets generated. 3. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Developer Mode	1. Use developer mode by adding the following in `qns.conf` file: `-Dcom.broadhop.developer.mode`. 2. Restart the policy server (QNS) process. 3. Within 5 minutes interval the Developer Mode License gets generated. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
Developer Mode Clear	1. Perform the steps above to generate the Developer Mode License trap. 2. Now remove the following line from the `qns.conf` file: `-Dcom.broadhop.developer.mode`. 3. Restart the policy server (QNS) process. 4. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
ZeroMQConnectionError	1. Start policy server (QNS). 2. Start Messaging Load (CCR-I,CCR-U,CCR-T) scenario at high TPS. 3. The trap will be seen if message sending over socket between policy director (lb) and policy server (QNS) fails (Due to socket send errors). For subsequent failures there is no further trap raised. 4. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).
ZeroMQConnectionError Clear	1. This trap will be sent when message send on socket succeeds after the prior failure. 2. Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
VirtualInterfaceDown	**1.** Login to active policy director (lb) VM. **2.** Run command **ifconfig eth1:0 down**. **3.** VirtualInterface Down trap with the interface name gets generated. **4.** You can see this trap on NMS server.
VirtualInterfaceUp	**1.** Login to active policy director (lb) VM. **2.** Run command **ifconfig eth1:0 up**. **3.** VirtualInterface Up trap with the interface name gets generated. **4.** You can see this trap on NMS server.
LdapAllPeersDown	**1.** Configure LDAP in CPS and verify the connection between CPS and LDAP. **netstat -an | grep 389** Let us say you configure 2 LDAP servers. **2.** Bring down the LDAP server: Kill the LDAP process on LDAP server or break the connectivity between LDAP and CPS (for example, block the port through firewall). **3.** Verify the LdapAllPeersDown alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb). This alarm will be generated only when all the LDAP servers configured in the CPS are down.
LdapAllPeersDown Clear	**1.** Perform the steps above to generate the LdapAllPeersDown trap. **2.** Bring up any one or both the LDAP servers. **3.** Verify the LdapAllPeersDown Clear alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
LdapPeerDown	1. Configure LDAP in CPS and verify the connection between CPS and LDAP. **netstat -an | grep 389** Let us say you configure 2 LDAP servers. 2. Bring down any one LDAP server: Kill the LDAP process on LDAP server or break the connectivity between LDAP and CPS (for example, block the port through firewall). 3. Verify the LdapPeersDown alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb). Verify that the IP address of the LDAP server is correct in the alarm. So, this alarm is generated per LDAP server.
LdapPeerDown Clear	1. Perform the steps above to generate the LdapPeerDown trap. 2. Bring up the LDAP server. 3. Verify the LdapPeerDown Clear alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb). Verify that the IP address of the LDAP server is correct in the alarm.
Percentage of LDAP retry threshold Exceeded	1. CPS HA is deployed as per guidelines provided in the *CPS Installation Guide for VMware* (this alarm is not applicable for AIO deployments). 2. Run Gx diameter calls and LDAP (configure multiple LDAP servers). 3. Verify Call Model is stable using **top_qps.sh** command. 4. Check for latest log: `/var/log/broadhop/scripts/gen-ldap-trap.log`. 5. If system (all policy server (QNS) VMs) is processing Gx and LDAP messages normal, then normal text message will be logged into the log file. 6. Abruptly shutdown LDAP server. 7. Within 30 seconds of interval, trap (dropped alarm) is generated. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
Percentage of LDAP retry threshold Normal	1. After dropped trap alarm is generated, restart LDAP server. 2. Within 30 seconds of interval, trap (clear indicator) is generated 3. Verify the clear indicator was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
LDAP Requests as percentage of CCR-I Dropped	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
LDAP Requests as percentage of CCR-I Normal	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
LDAP Request Dropped	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
LDAP Requests Normal	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
LDAP Query Result Dropped	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
LDAP Query Result Normal	Refer to steps for "Percentage of LDAP retry threshold Normal" alarm.
Gx Message processing Dropped	**1.** CPS HA is deployed as per guidelines provided in the Cisco Policy Suite Installation Guide (this alarm is not applicable for AIO deployments). **2.** Configure Message Handling Rules in Policy Builder. **3.** Run Gx diameter calls (CCR-I, U or T). **4.** Verify Call Model is stable using top_qps.sh command. **5.** Check for latest log: `/var/log/broadhop/scripts/gen-gx-drop-trap.log`. **6.** If system (all policy server (QNS) VMs) is processing Gx messages normally, then normal text messages will be logged into the log file. **7.** Increase the Gx message load beyond system capacity, such that threshold configured in Policy Builder should be breached. **8.** Within 30 seconds of interval, trap (dropped alarm) is generated. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
Gx Message processing Normal	**1.** After Gx Message Dropped trap alarm is generated, reduce traffic within system capacity. **2.** Within 30 seconds of interval, trap (clear indicator) is generated **3.** Verify the Gx Message processing Normal alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
Average Gx Message processing Dropped	1. CPS HA is deployed as per guidelines provided in the Cisco Policy Suite Installation Guide (this alarm is not applicable for AIO deployments). 2. Configure Message Handling Rules in Policy Builder. 3. Run Gx diameter calls (CCR-I, U or T). 4. Verify Call Model is stable using **top_qps.sh** command. 5. Check for latest log: `/var/log/broadhop/scripts/gen-gx-drop-trap.log`. 6. If system (all policy server (QNS) VMs) is processing Gx messages normally, then normal text messages will be logged into the log file. 7. Increase the Gx message load beyond system capacity, such that threshold configured in Policy Builder should be breached. 8. Within 30 seconds of interval, trap (dropped alarm) is generated. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
Average Gx Message processing Normal	1. After Average Gx Message processing Dropped alarm is generated, reduce traffic within system capacity. 2. Within 30 seconds of interval, trap (clear indicator) is generated 3. Verify the Gx Message processing Normal alarm was generated on NMS server and `/var/log/snmp/trap` of active policy director (lb).
AllSMSCNotification ServerDown	1. Stop all the Active SMSC servers. 2. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
AtLeastOneSMSC NotificationServerUp	1. Start any of the configured SMSC servers. 2. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
SMSCNotification ServerDown	1. Stop one of the active SMSC servers. 2. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
SMSCNotification ServerUp	1. Start one of the down and configured SMSC servers. 2. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).

Alarm Name	Procedure to Test
AllEmailNotification ServerDown	1. Close all SMTP servers defined. 2. In Wireshark trace, Major alarm will be triggered along with Critical alarm as 'Email server not reachable' and 'All Email servers not reachable'.
AtLeastOneEmail NotificationServerUp	1. Perform the steps above to generate the Email server not reachable and All Email servers not reachable traps. 2. Since all the servers are down, try bringing up only one SMTP server. 3. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
EmailNotification ServerDown	1. Consider multiple SMTP servers are defined in CPS under 'Multiple Email Server Configuration' with different ports. 2. Close any one of the SMTP servers (this will make the SMTP server not reachable), and keep the Wireshark trace ON. 3. Filter out the Wireshark trace with SNMP. 4. Verify receipt of the alarm on NMS and `/var/log/snmp/trap` of active policy director (lb).
EmailNotification ServerUp	1. Perform the steps above to generate the Email server not reachable trap. 2. Now bring up the SMTP server that was powered OFF. 3. In Wireshark trace another alarm (Clear Alarm) will be triggered as 'Email server reachable'.

SNMP System and Application KPI Values

SNMP System KPIs

In this table, the system KPI information is provided:

Table 9: SNMP System KPIs

Component	Information
lb01/lb02 pcrfclient01/pcrfcient02 sessionMgr01/sessionMgr02 QNS01/QNS02/QNS03/QNS04...	CpuUser CpuSystem CpuIdle CpuIdle LoadAverage1 LoadAverage5 LoadAverage15 MemoryTotal MemoryAvailable SwapTotal SwapAvailable

Application KPI Values

Table 10: Application KPI Values

KPI Values	
lb01/lb02	**snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB <lb01> <OIDvalue>** For example, **snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB lb01 .1.3.6.1.4.1.26878.200.3.3.70.11** List all KPIs value of load balancer (lb), if all values are 0 then For ExternalCurrentSession: **1.** Open another terminal. **2.** Enter the following command: **telnet <lbvip01> 8443** **3.** On previous terminal run the above **snmpwalk** command again. **4.** This time it will display the externalCurrentSession KPIs value to be 1. **5.** Repeat the process with more telnet session open on lbvip01 8080 port For InternalCurrentSession: **1.** Open another terminal. **2.** Enter the following command: **telnet <lbvip02> 8080** **3.** On previous terminal run the above **snmpwalk** command again. **4.** This time it will display the internalCurrentSession KPIs value to be 1. **5.** Repeat the process with more telnet sessions open on lbvip01 8080 port.

KPI Values	
qns01/qns02/qns03/qns04...	**snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB <qns01/02/03/04...> <OIDvalue>** For example, **snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB qns01 .1.3.6.1.4.1.26878.200.3.3.70.15** List all KPIs value of load balancer (lb), if all values are 0 then For ExternalCurrentSession: **1.** Open another terminal. **2.** Enter the following command: **telnet <lbvip01> 8443** **3.** On previous terminal run the above **snmpwalk** command again. **4.** This time it will display the externalCurrentSession KPIs value to be 1. **5.** Repeat the process with more telnet sessions open on lbvip01 8080 port For InternalCurrentSession: **1.** Open another terminal. **2.** Enter the following command: **telnet <lbvip02> 8080** **3.** On previous terminal run the above **snmpwalk** command again. **4.** This time it will display the internalCurrentSession KPIs value to be 1. **5.** Repeat the process with more telnet session open on lbvip01 8080 port.

KPI Values	
qns01/qns02/qns03/qns04...	**snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB <qns01/02/03/04...> <OIDvalue>** For example, **snmpwalk -v 2c -c broadhop -M +BROADHOP-MIB:CISCO-QNS-MIB qns01 .1.3.6.1.4.1.26878.200.3.3.70.15** List all KPIs value of policy server (QNS) VM. For example, the output will be displayed as below: SNMPv2-SMI::enterprises.26878.200.3.3.70.15.20 = STRING: “11” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.20.0 = STRING: “11” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.21 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.21.0 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.22 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.22.0 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.23 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.23.0 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.24 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.24.0 = STRING: “0” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.25 = STRING: “3204764880” SNMPv2-SMI::enterprises.26878.200.3.3.70.15.25.0 = STRING: “3204764880”

FAQs

Q. Where to check if traps are getting generated or not?

A. On active policy director (lb) VMs tail the below log file `/var/log/snmp/trap` to get the generated trap.

Q. Traps are getting generated from different VMs such as OAM (pcrfclient) or policy server (QNS) VMs but not getting logged to `/var/log/snmp/trap` and not appear on NMS receiver?

A. Check on active policy director (lb) VM if `/etc/snmp/scripts/application_trapv1_convert` and `component_trap_convert` files are present or not. If the files are present but traps are not getting generated then try to execute the following commands and test it again.

```
dos2unix /etc/snmp/scripts/application_trapv1_convert
dos2unix /etc/snmp/scripts/component_trap_convert
```

Q. The traps are getting logged in `/var/log/snmp/trap` but not receive on NMS?

A.
1. Check the setup configuration is correct or not as per the instruction given above.
2. Perform the steps given in the previous question.

3. Check if NMS IP is accessible from policy director (lb) VMs. Using command such as **ping <nms_ip>**.

Q. Database related traps not getting generated?

A. 1. Check the setup is configured and running as per instruction given above.

2. On `pcrfclient/lb` VMs all the scripts generating the traps are logging the details inside `/var/log/broadhop/script/<script_name><date>.log` file. Open log file to check if there is any error in the script or is it generating the traps successfully or not. If not generated by script then contact system administrator team to resolve the issue.

Q. What is the difference between pcrfclient01 and pcrfclient02 virtual machines?

A.
- pcrfclient01 --Master / Standby
- pcrfclient02 ---Slave / Standby
- pcrfclient02 support high availability of policy related services but it may not replicate all the services which were present in pcrfclient01.

Q. What is the ideal threshold limit for processor load in particular VM?

A. **A.** Ideally the threshold limit should be equal to number of vCPU that are present in the VM.

You can check the vCPU on a particular VM using the following command: `grep ^processor /proc/cpuinfo | wc -l`.

So if we have 12 vCPU, threshold limit for processor load is 12.

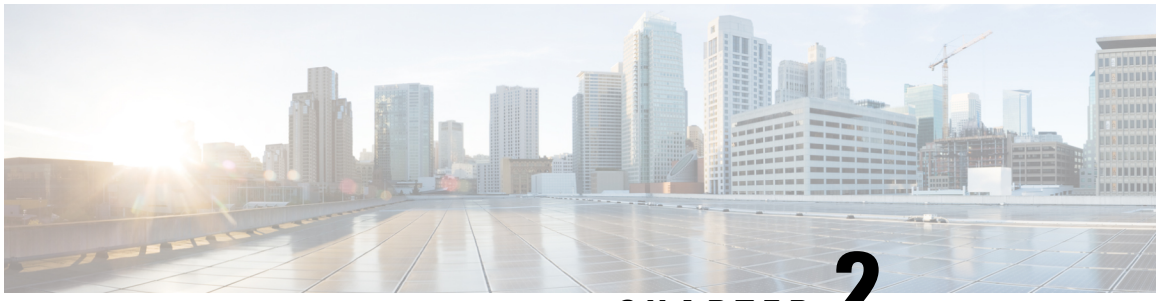
Q. I have multiple release trains (software releases) in my repository file (`cat /etc/broadhop/repositories`). Which one will take high precedence?

A. The highest version number is always selected and it is all merged. The versions are classified as follows and each type of versions will have version number and highest version takes high precedence:

1. Major
2. Minor
3. Patch
4. Build

Reference Document

For more information on SNMP traps and KPIs, refer to *CPS SNMP, Alarms and Clearing Procedures Guide*.



CHAPTER 2

Troubleshooting ANDSF

Policy Builder Scenarios

Not Able to See DM Configuration Tab in Policy Builder after Installation

Figure 26: DM Configuration Tab

Step 1 Execute **list_installed_features.sh** script from Cluster Manager to verify whether the ANDSF feature (**com.broadhop.client.feature.andsf**) is enabled or not.

```
list_installed_features.sh
```

Step 2 In case the above feature (**com.broadhop.client.feature.andsf**) is missing, edit the `/etc/broadhop/pb/features` file from Cluster Manager VM and add the following lines:

com.broadhop.client.feature.andsf

com.broadhop.andsf.service.feature

Step 3 After modifying the feature files, execute the following commands from Cluster Manager:

/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh

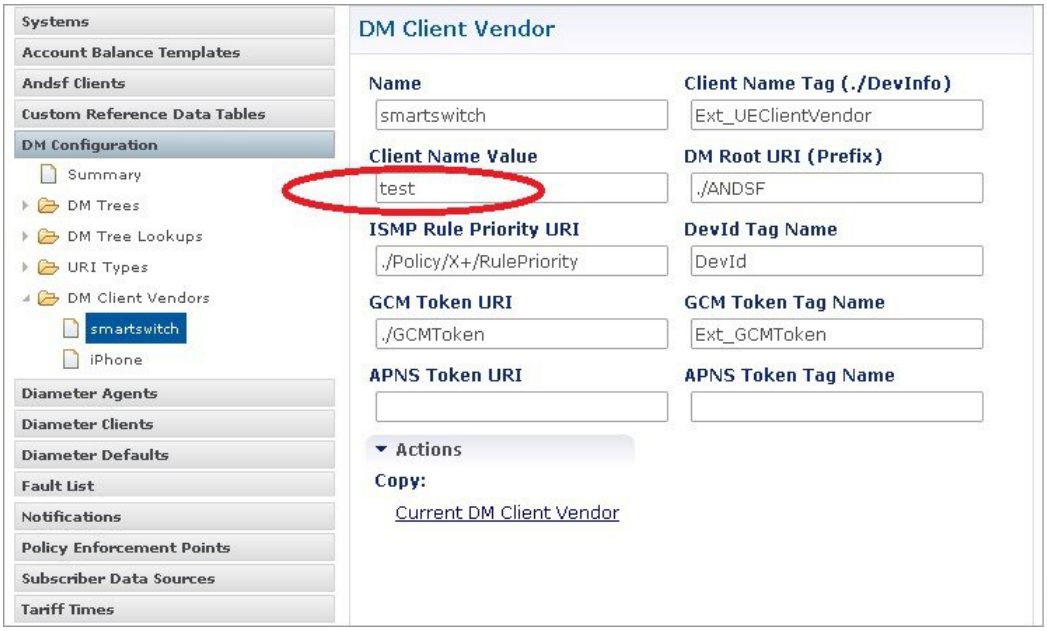
Note If the DM configuration does not show up then do a **restartall.sh** at the end.

Caution Executing `restartall.sh` will cause messages to be dropped.

Diagnostic.sh throws Errors after Restart

Check Client Name Value is not blank as shown in the following figure:

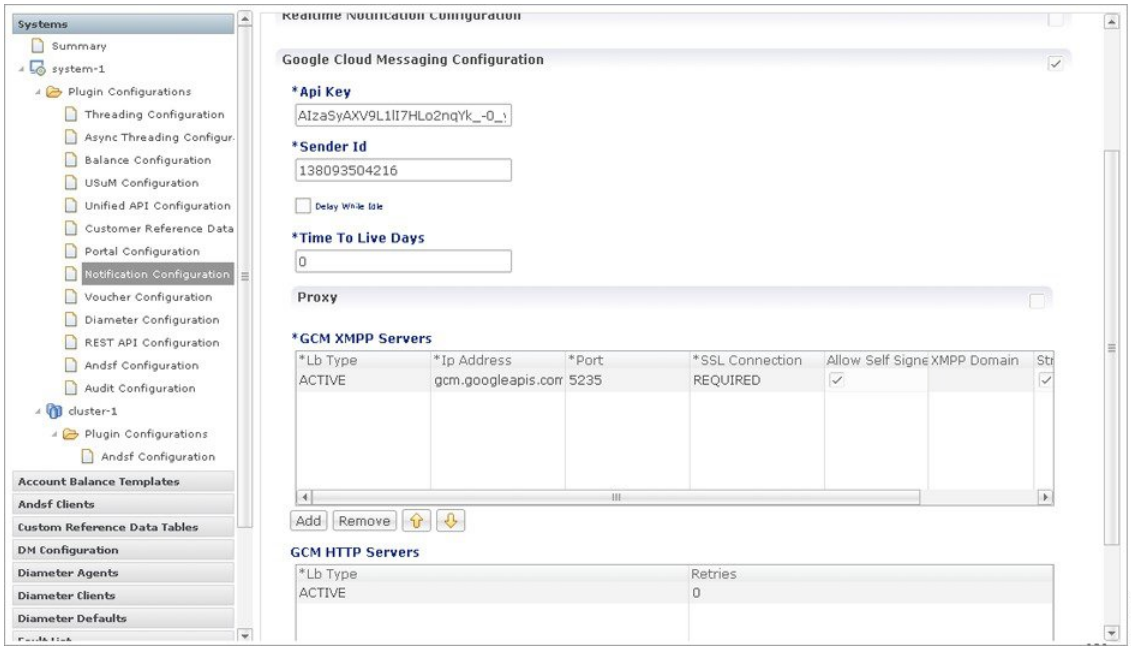
Figure 27: DM Client Vendor



Not Getting GCM Notifications in Logs

Verify the GCM tokens are configured in Policy Builder as shown in the following figure:

Figure 28: Notification Configuration



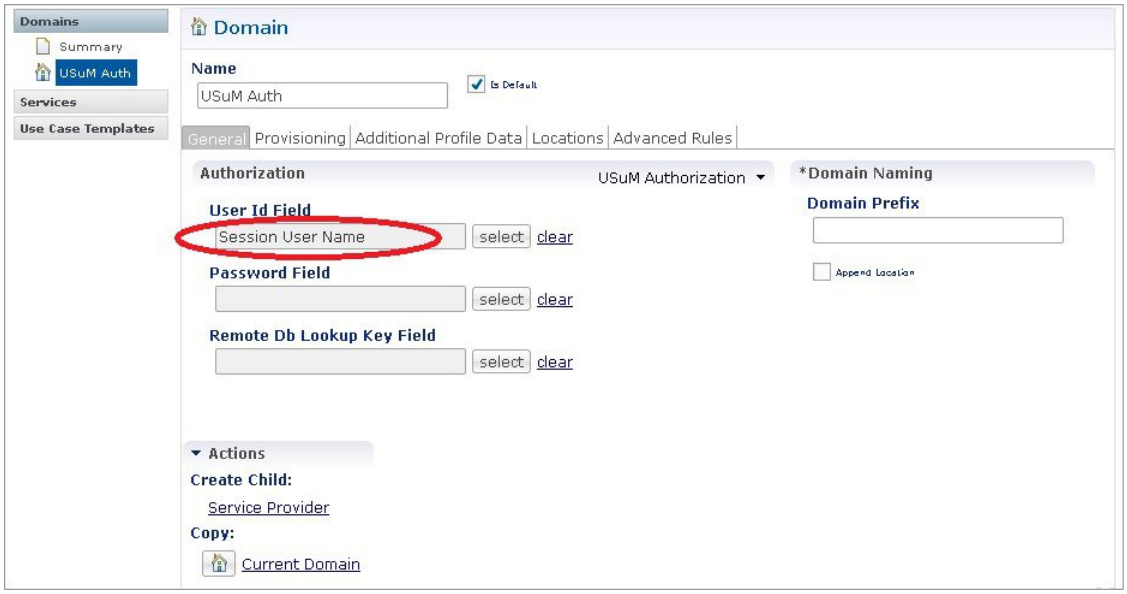
Session is not created for iPhone and Android Users

Step 1 Go to **Services** > **Domains** in Policy Builder.

Step 2 Under **Domains**, select **USum Auth**.

Step 3 On right hand side, in the **General** tab, under **Authorization** tab, check that the **User Id Field** value is set to **Session User Name** for both Android and Apple clients.

Figure 29: USum Auth



Check for service Use Case Templates for GCM, APNS, General, and default Services

Step 1 Go to **Services** tab in Policy Builder and click on **Use Case Templates**.

Step 2 Check that the use case template is there for the service being attached to a particular subscriber.

There should be two use case templates for a general ANDSF service and one more use case template for GCM/APNS notification if you have attached notification service to the subscriber.

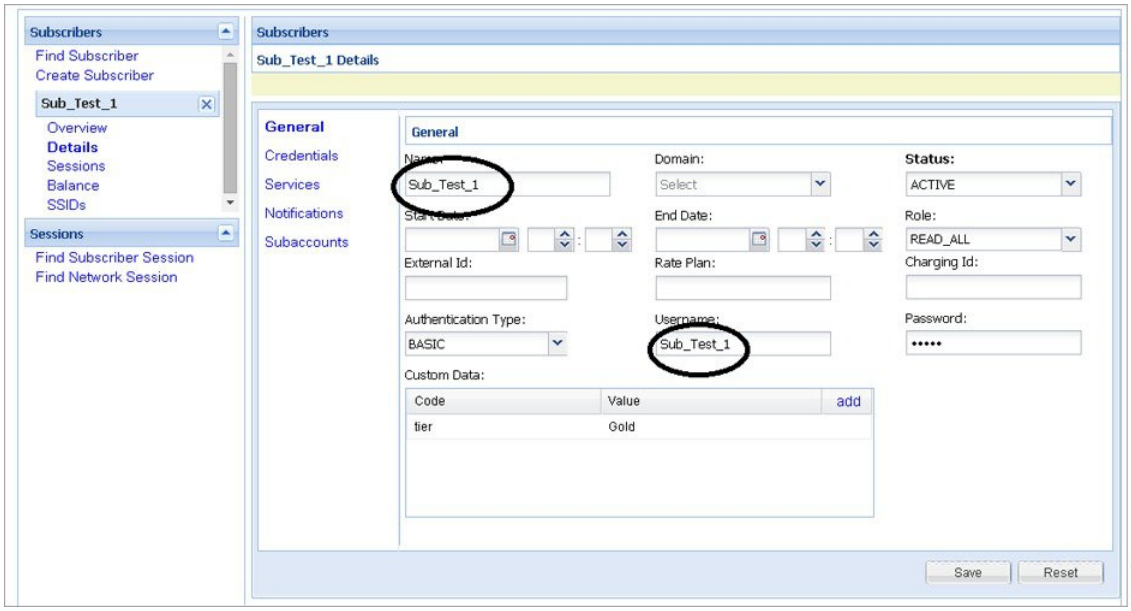
Step 3 If the templates are not there, see the *CPS ANDSF Configuration Guide* to create Use case Templates for the above services.

Control Center Scenarios

Subscriber Session not getting Created and Getting Exception Error (401)

- Make sure username and name should be same and unique.
- In case of Android, username will be IMSI.
- In case of iPhone, username will be MSISDN.

Figure 30: Subscribers



SSID Credentials are Wrongly Passed in Policy

Step 1 Go to Subscriber section in Control Center.

Step 2 Click on **SSID** section.

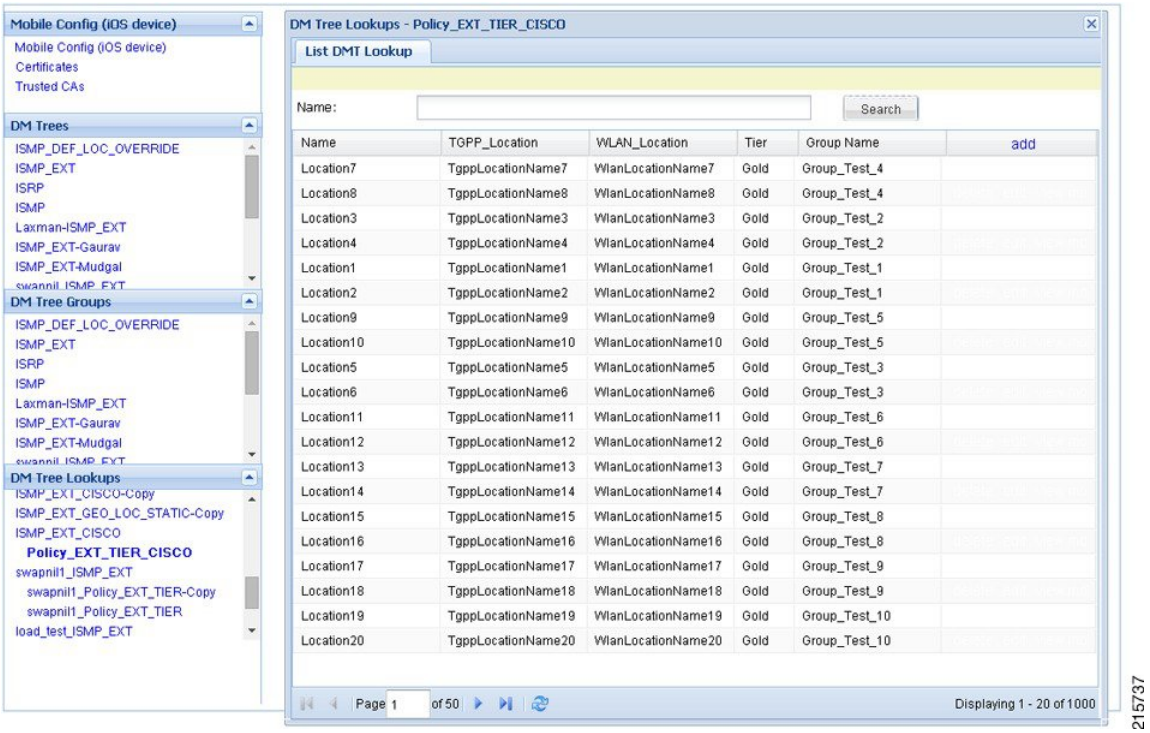
Step 3 Check the subscriber credentials are populated for specific SSIDs.

Step 4 Verify all the above three steps for all the subscribers.

DM Tree Lookups Fail and Exception in consolidated-qns.log

Step 1 Make sure CRD mapping is done properly in DM lookup.

Figure 31: DM Tree Lookups



Step 2 Check the CRD entries in DM tree lookup table.

Step 3 Check whether the CRD tables (for example, check in configuration section) exists and have entries defined in the lookup table.

Data Populated in MongoDB ANDSF Collection, but values are not shown in Control Center

Step 1 Go to all the policy server (QNS) nodes.

Step 2 Edit the following `qns.conf` file at `/etc/broadhop/`.

Step 3 Add the following parameter in the `qns.conf` file.

```
-Dandsf.mongo.thread.maxWaitTime=10000
```

Step 4 Execute `restart.sh` from Cluster Manager VM.

Not able to see the Mobile Configuration Certificate sub screen in Control Center

Step 1 Check if the screen is hidden behind the mobile configuration main screen.

Step 2 Close all the screens and re-open the mobile configuration screen.

If the certificate screen is not visible, you may need to close the Control Center and Mobile Configuration screens and reopen them again to make it visible.

Control Center session timeout frequently and not able to login from another browser

Step 1 Increase the number of sessions limit which will allow to create more sessions.

Step 2 Edit the `qns.conf` file and add the following parameter:

```
-Dcc.user.session.limit=5000
```

Geo-location is not read Properly in Control Center

Step 1 Go to **Configuration** tab in Control Center.

Step 2 Click on the **Geo-location** table and verify the format.

Latitude and Longitude value should be in degrees.

For example:

Longitude: 36.0044

Latitude: -68.9956

Radius: 100

ANDSF Server Scenarios

API Error Codes

The following table provides the information related to API Error Codes:

Table 11: API Error Codes

Error Code	Scenario
400 Bad request	The requested command could not be performed because of malformed syntax in the command. The malformed command may also be returned in the item Element type in the Status. Check SyncML syntax. For more information, refer to *CPS ANDSF Configuration Guide*.
401 Invalid credentials	The requested command failed because of improper authentication or authorization. If the property type of authentication was presented in the original request, then the response code indicates that the requested command has been refused for those credentials. Check **cred data** and **Authentication** type in syncml. For more information, refer to *CPS ANDSF Configuration Guide*.
500 Command failed	The recipient encountered an unexpected condition which prevented it from fulfilling the request. Verify **ssids** are attached to the subscriber and check **qns consolidated** logs in OAM (pcrfclient).
503 Service unavailable	The recipient is currently unable to handle the request due to a temporary overloading or maintenance of the recipient. The implication is that this is a temporary condition, which will be alleviated after some delay Check **qns consolidated** logs in OAM (pcrfclient).

General Errors

Problem Accessing ua/soap Getting Jetty Related Error

This problem occurs when Unified API service is not functioning.

Step 1 Execute **list_installed_features** command to check whether the following features are installed:

PCRF

- `com.broadhop.unifiedapi.interface.feature`
- `com.broadhop.unifiedapi.ws.service.feature`

Policy Builder

- `com.broadhop.client.feature.andsf`
- `com.broadhop.client.feature.unifiedapi`

Step 2 Add the missing features in Policy Builder and PCRF feature file (`/etc/broadhop/pb/features`, `/etc/broadhop/pcrf/features`).

Step 3 Execute the following commands from Cluster Manager.

/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh

Check if Blank Policy is Retrieved in SyncML Response

This problem occurs whenever a respective policy for the UE request is not found.

Step 1 Make sure lookups defined in Control Center and Policy Builder are properly configured.

Step 2 Map DM configuration templates in Policy Builder with the actual DM configuration in Control Center and also look into subscriber mapped service configuration.

Step 3 Make sure no error object is being created for a non-matching option in Service Configuration. Check if options in Use Case Templates match corresponding Service Options and Service Configuration. They will be marked with a (X) if there is an error.

Step 4 Publish the corrections.

Step 5 After restarting policy server (QNS), run the use case again.

Policy Engine not Returning a Management Response

This problem occurs when a certain process during policy retrieval is failing due to an Exception in some process.

Step 1 Go to Policy Builder.

Step 2 Check that all the configurations are correct as per *CPS ANDSF Configuration Guide*.

Step 3 Check that the Control Center Lookup and associations are properly configured.

Step 4 Check `consolidated-qns.log` in pcrfclient01 VM to debug any relevant exceptions.

Notification Errors

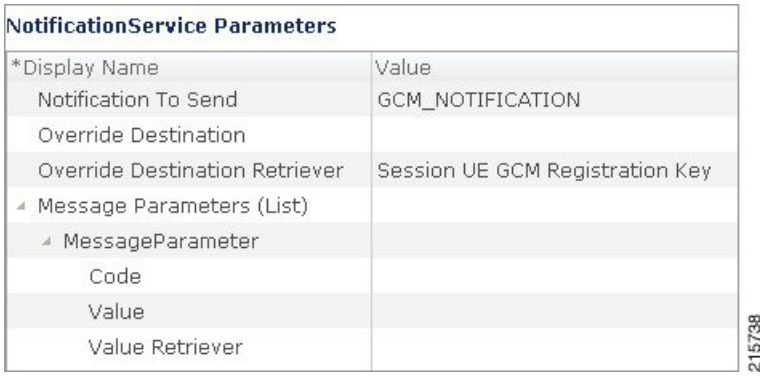
GCM Notification

No GCM Token Found

This generally happens when either UE is not sending the token in Device Info or Server is unable to retrieve this token for notification. Server can only retrieve token and store in the Device session if notification service is properly configured (if not using default configurations).

- Andsf_ISMP_Google_Notification

Figure 32: NotificationService Parameters



In the **Override Destination Retriever**, specify this field which will pick Token from Device Info field, having the following two tags: <GCMToken> for google devices. Make sure these are set in DM Client Vendor Page.

Figure 33: DM Client Vendor

Whenever notification is not received by client, following common error scenarios can occur:

- Couldn't Connect To GCM Server Exception

  This generally happens when Notification Configuration is not configured properly. Ensure load balancer is able to listen on the ports specified by GCM. The feature `com.broadhop.notifications.service.feature` is enabled on Policy Director (lb). Similarly `com.broadhop.notifications.local.feature` should be enabled on Policy Server (qns).

- Policy Builder Configuration
  - Under Notification Configuration check the configuration for GCM Configuration.

- The configuration should not be in error. The correct API key and Sender Id should be present.

- Server Configuration
  - Check there is an active connection established on the port 5235. The firewall is opened for the port.

    ```
    service iptables stop
    ```

    ```
    netstat -apn | grep 5235
    ```
    (Connection should be in established state)
  - Telnet connection is established for the port.

    Ping to **gcm.googleapis.com** should be successful.

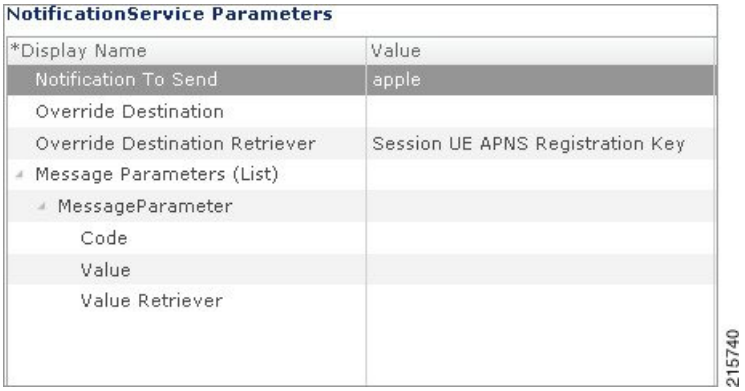
    Ping to **android.googleapis.com** should be successful.
  - A valid xmpp or http connection is established. The same should be visible in policy server (qns) logs on the active policy director (lb). Check Notification is being sent from policy server (qns) and the same is being relayed correctly by the policy director (lb) to the GCM Server.

APNS Notification

- No APNS Token Found

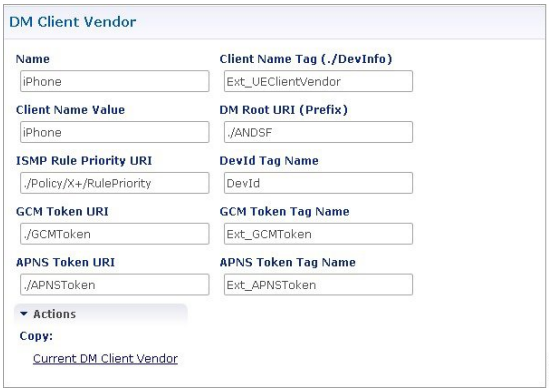
  This generally happens when either UE is not sending the token in Device Info or Server is unable to retrieve this token for notification. Server can only retrieve token and store in the Device session if notification service is properly configured (if not using default configurations)
  - Andsf_ISMP_Apple_Notification

    Figure 34: NotificationService Parameters

    In the **Override Destination Retriever**, specify this field which will pick Token from Device Info field, having the following two tags: <APNSToken> for apple devices. Make sure these are set in DM Client Vendor Page.

Figure 35: DM Client Vendor



Whenever notification is not received by client, following common error scenarios can occur:

- Couldn't Connect To APNS Server Exception

  This generally happens when Notification Configuration is not configured properly. Ensure load balancer is able to listen on the ports specified by APNS. The feature `com.broadhop.notifications.service.feature` is enabled on policy director (lb). Similarly, `com.broadhop.notifications.local.feature` should be enabled on policy server (qns).

- Policy Builder Configuration
  - Check the correct APNS Server is provided with the correct Server Port. The APNS token being sent is valid.
  - A valid Certificate and password is provided.
  - Correct Geo Fence value is configured under the ANDSF Configuration.

- Server Configuration
  - Check there is an active connection established on the port 2195. The firewall is opened for the port.

    ```
    service iptables stop
    ```

    ```
    netstat -apn | grep 2195
    ```
    (Connection should be in established state)
  - Telnet connection is established for the port.
  - Check if the APNS token is updated with the correct value in the Session Data. This should be a valid APNS Token.
  - Check Notification is being sent from policy server (qns) and the same is being relayed correctly by the policy director (lb) to the APNS Server

Basic Troubleshooting Using ANDSF Logs

Debugging Common Errors using Logging Techniques of ANDSF

The following procedure describes how to enable logs in `logback.xml`.

Step 1 Edit `/etc/broadhop/logback.xml`.

Step 2 Search for the following:

```
<!-- APS Loggers -->
```

Step 3 Change `<logger name="com.broadhop" level="warn"/>` to `<logger name="com.broadhop" level="debug"/>`.

Step 4 (Optional) To enable module specific logging, set the debugging level to debug for the specific module.

For example, `<logger name="com.broadhop.notifications" level="debug"/>` will set the debug level log for notifications module only.

Step 5 Copy this `logback.xml` file to all other policy server (qns) VMs using the following command:

```
copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml
```

Step 6 Capture the trace. Now run the call flow so that the trace is captured in the logs.
Logs will be captured in `/var/log/broadhop`.

Step 7 After you have captured and debugged the logs, roll back the `logback.xml` file.

Debugging Common Call Flow Scenarios for ANDSF using Logging Patterns

Generic Call Flow For Android

Step 1 Enable the logging for broadhop module at debug level as described in Debugging Common Errors using Logging Techniques of ANDSF, on page 119.

Step 2 On pcrfclient01, navigate to /var/log/broadhop.

Step 3 Use the tail command to view the consolidated-engine.log

Step 4 Send Package #1 for the subscriber. Look for the following values:

a) Correct Message and User Info is picked:

```
Message Id: 1

Source: IMEI:User_UseCase_Tier

User Name: User_UseCase_Tier
```

The Correct IMEI and User Name value should be displayed as specified in Control Center.

b) Check if USUSM Authorization was successful. If not, check that the User Name is the same as in Control Center and that Correct Authorization is given in Policy Builder.

```
INFO : (auth) Success USUM_AUTHORIZATION
```

c) Check if DevInfo gets Processed.

```
INFO : (ANSDF) DevInfo processed : vendor SmartSwitch
```

d) If a GCM token is supplied, see if it is read and updated.

```
INFO : (ANSDF) Updating GCM registration key !Vendor: SmartSwitch
```

e) Check the correct Use Case is picked and a valid response is sent to the same Subscriber.

```
INFO : (ANSDF) Sending response for session
imei:User_UseCase_Tier;Session_User_UseCase_Tier

INFO : (use-cases) Use case 'Andsf_ISMP_LOC', status: true, Condition: No Condition Set
```

Step 5 Send Package #3 for the subscriber. The correct policy should to be sent to the user on the basis of the lookups defined in DM Configuration in Control Center.

a) Correct Message and User Info is picked:

```
Message Id: 2

Source: IMEI:User_UseCase_Tier

User Name: User_UseCase_Tier
```

The Correct IMEI and User Name value should be displayed as specified in Control Center.

b) Check that the correct session is picked, as was given in Package #1:

```
Session ID: imei:User_UseCase_Tier;Session_User_UseCase_Tier
```

c) Check that correct TGPP and WLAN Location Values are picked as defined in Control Center under the DM Configuration Tab:

```
INFO : (ANSDF) Processing result cmd: 14

INFO : (ANSDF) Processed URI ./UE_Location/TGPP_Location value: [UseCase_Tier_TGPP]

INFO : (ANSDF) Processed URI ./UE_Location/WLAN_Location value: [UseCase_Tier_WLAN]
```

UseCase_Tier_TGPP is configured in TGPP_Location Table.

UseCase_Tier_WLAN is configured in WLAN_Location Table.

d) Check that the correct lookup is picked as defined in the DM Configuration and correct lookup filters are processed.

```
INFO : (ANSDF) checking state: LOOKUP {90}

INFO : (ANSDF) Processing lookup Policy_EXT_TIER

INFO : (ANSDF) Lookup using ./UE_Location/TGPP_Location value: [UseCase_Tier_TGPP]

INFO : (ANSDF) Lookup using ./UE_Location/WLAN_Location value: [UseCase_Tier_WLAN]

INFO : (ANSDF) Lookup using TIER value: [Gold]
```

e) Correct DM Treee is picked:

```
INFO : (ANSDF) Found subscriber specific node [SSIDTypeWLAN_Location2] in DMT
[UseCase_SSID_Tier]
```

UseCase_SSID_Tier is the Tree that is configured for the Lookups defined above in Control Center DM Configuration.

f) A valid response command is sent to the client:

```
INFO : (ANDSF) Adding Replace [response=2,7] for
imei:User_UseCase_Tier;Session_User_UseCase_Tier, msg=2
```

g) A valid Syncml response is sent:

```
INFO : (ANSDF) Sending response for session
imei:User_UseCase_Tier;Session_User_UseCase_Tier
```

Generic Call Flow For Apple

Step 1 Enable the logging for broadhop module at debug level as described in Debugging Common Errors using Logging Techniques of ANDSF, on page 119.

Step 2 On pcrfclient01, navigate to `/var/log/broadhop`.

Step 3 Use the **tail** command to view the consolidated-engine.log.

Step 4 Send Package #1 for the subscriber. Look for the following values:

a) Correct Message and User Info is picked:

```
Source: UUID:User_UseCase_IOS_1

User Name: User_UseCase_IOS

UUID: User_UseCase_IOS_1
```

The Correct UUID and User Name value should be displayed as specified in Control Center.

b) Correct Services are attached to the subscriber:

```
SERVICES: Andsf_ISMP_Apple_Notification Andsf_ISMP_GEO_LOC_STATIC
```

c) Check if USUSM Authorization was successful. If not, check that the User Name is the same as in Control Center and that Correct Authorization is given in Policy Builder.

```
INFO : (auth) Success USUM_AUTHORIZATION
```

d) Check the correct Use Case is picked and a valid response is sent to the same Subscriber.

```
INFO : (use-cases) Use case 'Andsf_ISMP_Apple_Notification', status: false, Condition:
("DM Device MO"=false)

INFO : (use-cases) Use case 'Andsf_ISMP_GEO_LOC_STATIC', status: true, Condition: No
Condition Set
```

Step 5 Send Package #3 for the subscriber. The correct policy should to be sent to the user on the basis of the lookups defined in DM Configuration in Control Center.

a) Correct Message and User Info is picked:

```
Message Id: 2

Source: UUID:User_UseCase_IOS_1

User Name: User_UseCase_IOS

UUID: User_UseCase_IOS_1
```

Correct UUID and User Name value should be displayed as specified in Control Center.

b) Correct Session is picked as was given in Package #1:

```
Session ID: uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1
```

c) Check the DevInfo gets Processed:

```
INFO : (ANSDF) Pre-fetch URI ./DevInfo cmd: 4

INFO : (ANSDF) DevInfo processed : vendor iPhone DevId: 12345 DevType: NA
```

d) If an APNS token is supplied, see if it is read and updated.

```
INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: iPhone, Client: NA, DevId: 12345,
GCMToken: null
```

e) Check that correct Geo Location Values are picked as defined in Control Center under the DM Configuration Tab:

```
INFO : (ANSDF) Processed URI ./UE_Location/Geo_Location value: [geo_1]
```

geo_1 is configured in Geo_Location Table.

f) Check that the correct lookup is picked as defined in the DM Configuration and correct lookup filters are processed:

```
INFO : (ANSDF) checking state: LOOKUP {90}

INFO : (ANSDF) Processing lookup Policy_EXT_GEO_LOC_STATIC

INFO : (ANSDF) Lookup using ./UE_Location/Geo_Location value: [geo_1]
```

g) A valid response command is sent to the client:

```
INFO : (ANDSF) Adding Replace [response=2,6] for
uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1, msg=2
```

h) A valid Syncml response is sent:

```
INFO : (ANSDF) Sending response for session
uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1
```

GCM Notification

Step 1 Check that the GCM Token is defined and updated in the Logs for the subscriber:

```
UUID: Sub_Test_1

User Name: User_UseCase_GCM_1

INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: SmartSwitch, Client: NA, DevId:
User_UseCase_Tier, GCMToken:
APA91bGbvmHGxpePBt_HkV3Rqw7SW01GyaiqoYdvJv1SPPtQDrO62RGEK-tbk5-bQ5VOCgj4fHM98LzEQPLw6uR4
XlSqu-FW7lqwApCTf-ssjIo1_1oFmyd-VDpcyvN0PIkkGeW0wDNilcjyLmX92bfpusD6RUuIx_1m88maJJzSQPiM
fdq3rTA

INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 2 On Subscriber Version Update, check that the Notification is being sent:

```
POLICY RESULT SUCCESS:

session action = None
```

```
domainId = ANDSF

subscriberId = 00300000e4b0fb825589222c

SERVICES: NOTIF_GCM Andsf_ISMP_Tier

TRIGGER: com.broadhop.spr.impl.messages.RefreshSPRProfile Key:
pk:userId:User_UseCase_GCM_1

DEBUG MSGS:

  INFO : (core) Lock obtained on key: pk:userId:User_UseCase_GCM_1

  INFO : (core) Successful load by key: pk:userId:User_UseCase_GCM_1

  INFO : (ANSDF) Sending PUSH on subscriber-version update

  INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:44 IST 2015
```

Step 3 On the Load Balancer, check qns-1.log:

```
Received GCM Notification request : Request:

template name: GCM_NOTIFICATION

collapse key: COLL_KEY_1

time to live: 1


DEBUG c.b.n.gcm.GcmMessageManager.? - Standard parameters used for sending GCM notification
: timeToLive(days) : 5, delayWhileIdle : false, collapseKey : COLL_K****,
apiKeyAIzaSyAXV9L1lI7HLo2n********************, senderId1380935*****

DEBUG c.b.n.gcm.GcmMessageManager.? - GCM message to be sent : Test Message

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Listener Received: <message><gcm xmlns="goog

DEBUG c.b.notifications.gcm.GcmXmppServer.? - XMPP packate recieved : {"registration_id":

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Collector Received: <message><gcm
xmlns="google:mobile:data"

DEBUG c.b.notifications.gcm.GcmXmppServer.? - CCS ACK received !!

DEBUG c.b.n.i.a.SendGcmNotificationRequest.? - GCM Notification request processing got
completed !!
```

APNS Notification

Step 1 Check that the APNS Token is defined and updated in the Logs for the subscriber:

```
UUID: Sub_Test_1

User Name: User_UseCase_IOS_8

INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: SmartSwitch, Client: NA, DevId: 12345

INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 2 On Subscriber Version Update, check that the Notification is being sent:

```
POLICY RESULT SUCCESS:

session action = None

domainId = ANDSF

subscriberId = 00500000e4b0fb8255892f94

SERVICES: ISMP_Apple_Notification

TRIGGER: com.broadhop.spr.impl.messages.RefreshSPRProfile Key:
pk:userId:User_UseCase_IOS_08

DEBUG MSGS:

  INFO : (core) Lock obtained on key: pk:userId:User_UseCase_IOS_08

  INFO : (core) Successful load by key: pk:userId:User_UseCase_IOS_08

  INFO : (ANSDF) Sending PUSH on subscriber-version update

  INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 3 On the Load Balancer, check qns-1.log:

```
DEBUG c.b.n.impl.NotificationsManager.? - sendApplePushNotification: Device Token being
pushed to is: 67349132e3631b7a5642d2dae5991359042120c9ca0c30236bcc0bcaed1741c7.

DEBUG c.n.apns.internal.ApnsConnectionImpl.? - Made a new connection to APNS

DEBUG c.n.apns.internal.ApnsConnectionImpl.? - Message
"com.notnoop.apns.ApnsNotification@ecdaaeef"
```

Notification for Revalidation Timer

Step 1 Check that the value for revalidation timer (as defined in Policy Builder) is set in the logs:

```
INFO : (ANSDF) Setting next evaluation time Tue Jun 23 13:05:09 IST 2015
```

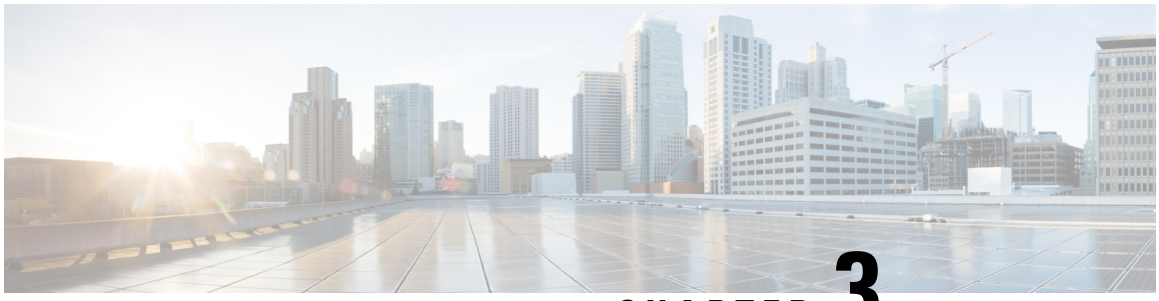
Step 2 Check that a revalidation Timer Push Notification is sent after the timer has expired. Check that correct Use Case and Trigger are used:

```
qns02 [2015-06-23 13:03:05,317] ================================================

  POLICY RESULT SUCCESS:

    session action = None

    domainId = ANDSF

    subscriberId = 00153c00e4b0c35e558901c0

    SERVICES: Andsf_ISMP_Tier

    TRIGGER: com.broadhop.cache.TimerExpired request:

  key: null:userId:User_UseCase_Tier
```

```
  DEBUG MSGS:

    INFO : (ANSDF) Sending PUSH for re-validation timer expiry

    INFO : (ANSDF) Setting next evaluation time Tue Jun 23 13:13:05 IST 2015

    INFO : (use-cases) Use case 'Andsf_ISMP_LOC', status: true, Condition: No Condition Set

==============================================================================
```

Step 3 On the Load Balancer, check qns-1.log:

```
Received GCM Notification request : Request:

template name: GCM_NOTIFICATION

collapse key: COLL_KEY_1

time to live: 1


DEBUG c.b.n.gcm.GcmMessageManager.? - Standard parameters used for sending GCM notification
: timeToLive(days) : 5, delayWhileIdle : false, collapseKey : COLL_K****,
apiKeyAIzaSyAXV9L1lI7HLo2n******************, senderId1380935*****

DEBUG c.b.n.gcm.GcmMessageManager.? - GCM message to be sent : Test Message

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Listener Received: <message><gcm xmlns="goog

DEBUG c.b.notifications.gcm.GcmXmppServer.? - XMPP packate recieved : {"registration_id":

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Collector Received: <message><gcm
xmlns="google:mobile:data"

DEBUG c.b.notifications.gcm.GcmXmppServer.? - CCS ACK received !!

DEBUG c.b.n.i.a.SendGcmNotificationRequest.? - GCM Notification request processing got
completed !!
```



CHAPTER 3

Check Subscriber Access

Checking Access

When you are confident that the installation and configuration tasks are complete and processing properly, try running a small amount of test traffic, following it through the system. Here are three ways to ascertain correct process of access from a subscriber perspective.

Testing Subscriber Access with 00.testAccessRequest.sh

00.testAccessRequest.sh is a test script used to test subscriber access to the ISG and CPS system.

You can find **00.testAccessRequest.sh** in `/opt/broadhop/installer/isg/troubleshooting` directory on the CPS server.

To configure the subscriber used, edit the `/opt/broadhop/installer/isg/troubleshooting/config.ini` file.

Step 1 In the `config.ini` file, change the **User-Name** and **Password** fields.

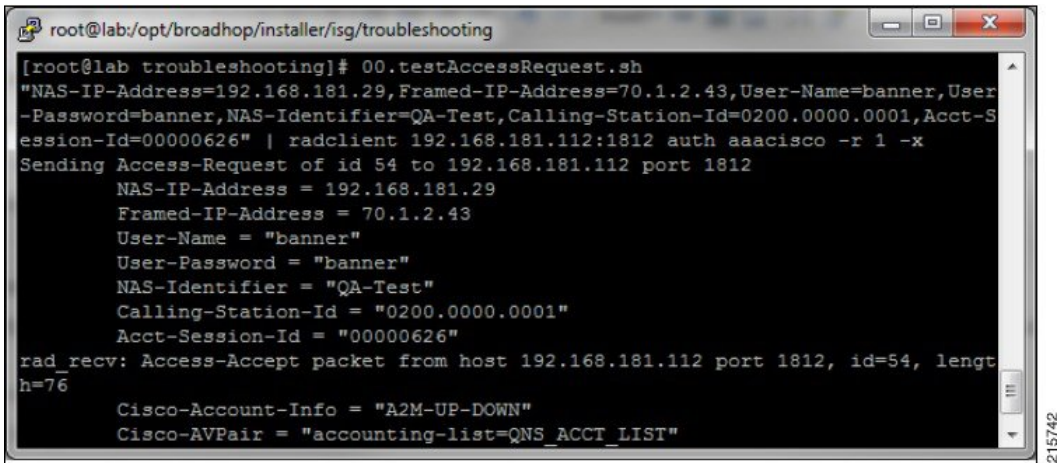
Note You may need to change some of the other parameters in order to match your configuration. The other main attributes to change will be the NAS-IP-Address and Framed-IP-Address.

Step 2 Run the script from a command line. No arguments are necessary:

00.testAccessRequest.sh

Upon success, this output is displayed as follows:

Figure 36: 00.testAccessRequest.sh Output



Testing Subscriber Access with soapUI

This procedure tests end subscriber access to your system.

Step 1 Download soapUI from here: http://www.soapui.org/

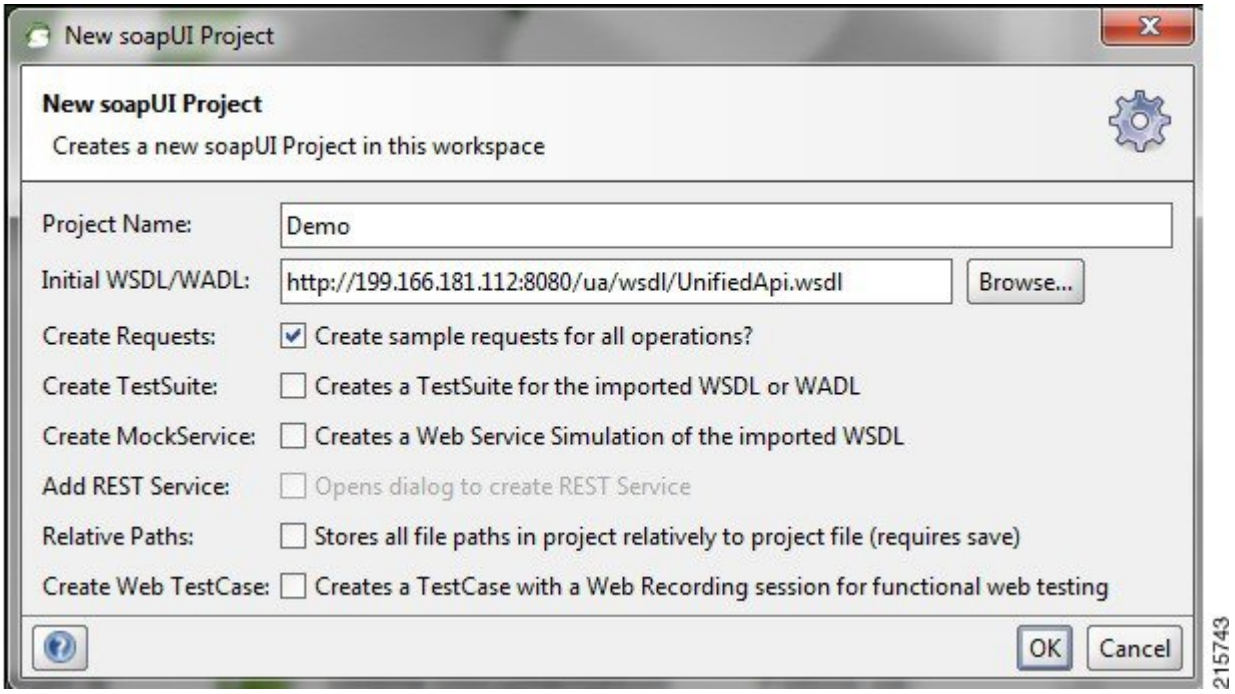
You only need the freeware version (not the soapUI Pro).

Step 2 Launch soapUI.

Step 3 Right click on **Projects** and select **New soapUIProject** from the drop-down list.

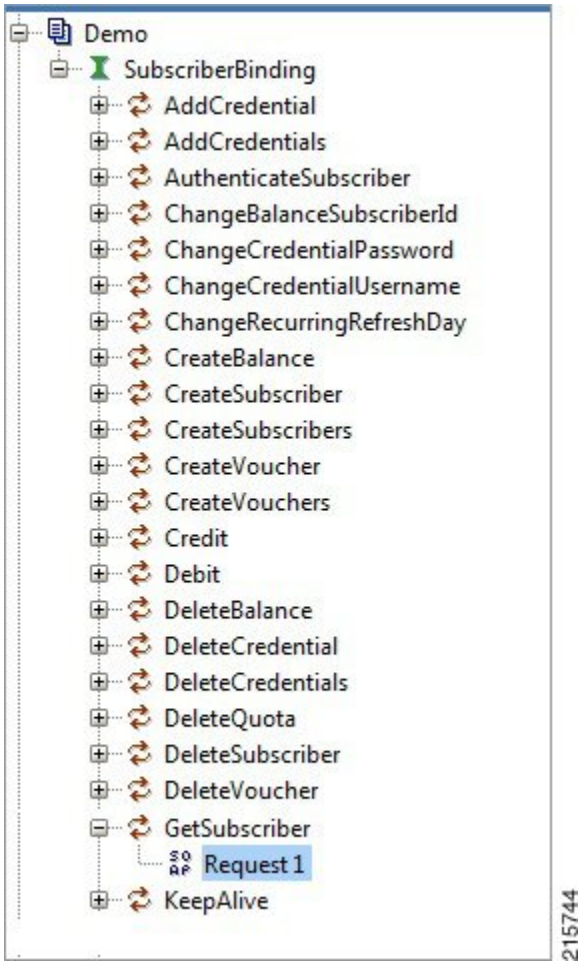
Step 4 Name your project and enter into **Initial WSDL/WADL** the appropriate WSDL URL (you may have to replace the IP in display with your own IP) and select **OK**.

Figure 37: New soapUIProject



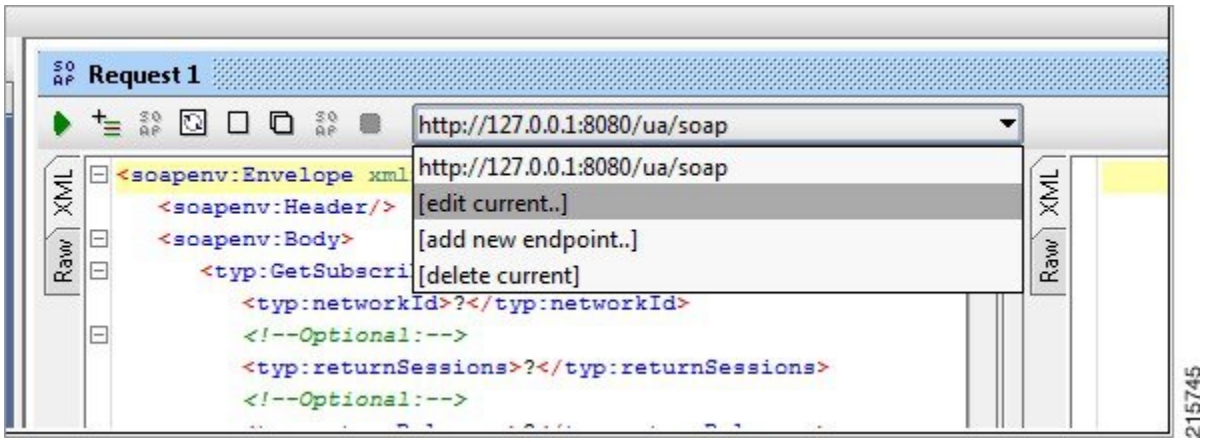
Step 5 In the tree, select **Demo** > **SubscriberBinding** > **GetSubscriber** > **Request 1** as shown in the following figure:

Figure 38: Request 1 Node



Step 6 Select **edit current..** to edit the end point. Enter the appropriate IP.

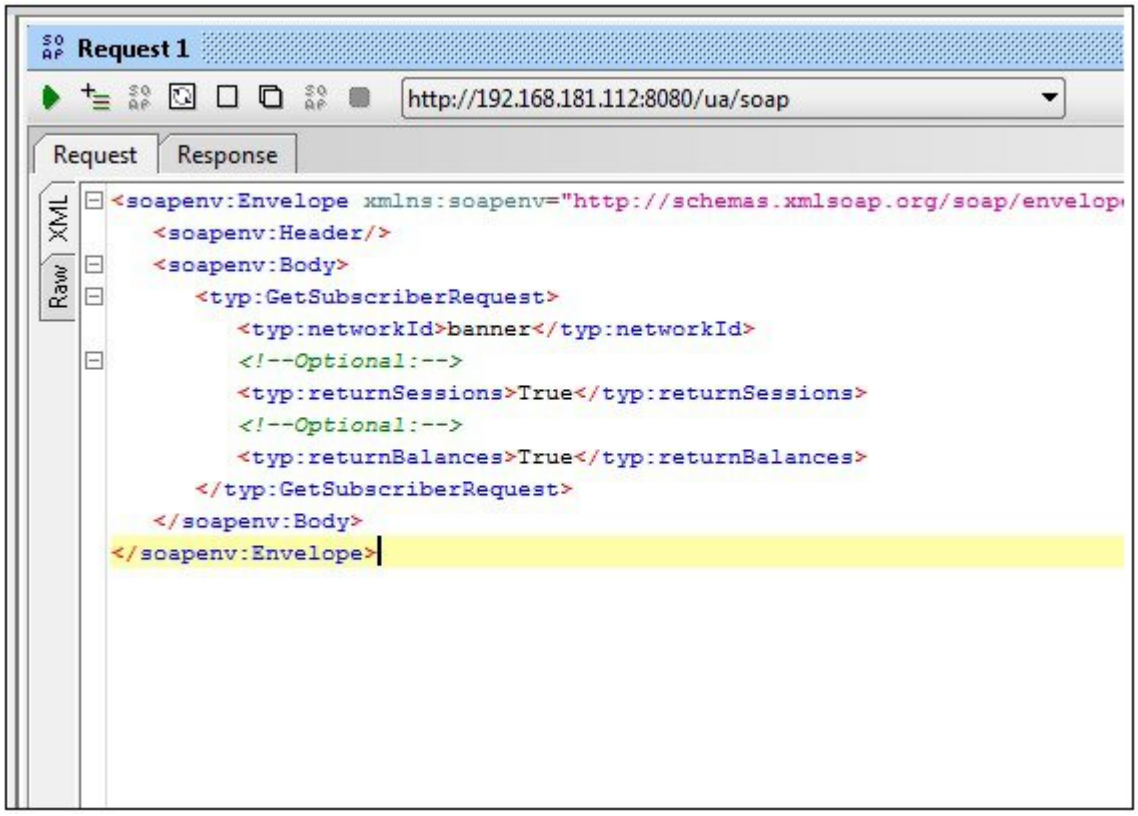
Figure 39: Request 1 XML File



Step 7 In the XML file:

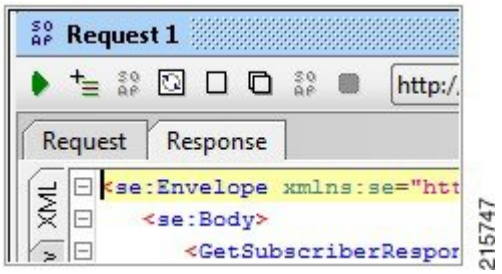
- Replace `?` in `<typ:networkId>?</typ:networkId>` with the appropriate credential or network ID.
- Replace `?` in `<typ:returnSessions>?</typ:returnSessions>` with `True`.
- Replace `?` in `<typ:returnBalance>?</typ:returnBalance>` with `True`.

Figure 40: Request 1 XML File



Step 8 Click the green arrow (underneath **Request 1**).

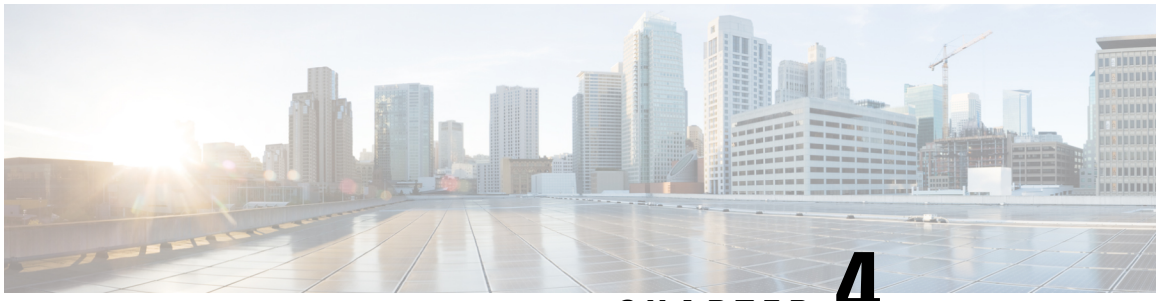
Figure 41: Request 1 XML File



Step 9 Check the resulting XML output. Pay special attention to the relevant subscriber information.

Figure 42: XML Output


```
<se:Envelope xmlns:se="http://schemas.xmlsoap.org/soap/envelope/">
   <se:Body>
      <GetSubscriberResponse xmlns="http://broadhop.com/unifiedapi/soap/types">
         <errorCode>0</errorCode>
         <errorMessage>Request completed successfully</errorMessage>
         <subscriber>
            <id>4fb54d03e4b01e8478d309c2</id>
            <name>
               <fullName>Bruce Banner</fullName>
            </name>
            <credential>
               <networkId>banner</networkId>
               <password>banner</password>
            </credential>
            <credential>
               <networkId>0200.0000.0001</networkId>
               <expirationDate>2012-05-17T13:17:07.020-06:00</expirationDate>
            </credential>
            <service>
               <code>SERVICE_A</code>
               <enabled>true</enabled>
            </service>
            <session>
               <sessionKey>
                  <code>UserIdKey</code>
                  <primary>false</primary>
                  <keyField>
                     <code>userId</code>
                     <value>banner</value>
                  </keyField>
               </sessionKey>
               <sessionObject>
                  <entry>
                     <string>tags</string>
                     <list>
```



CHAPTER 4

TCP Dumps

About TCP Dumps

CPS administrators can use the **tcpdump** Linux command in the command line to intercept and display TCP/IP packets, as well as others, as they are being transmitted or received.

With the **tcpdump** command, you can analyze network behavior, performance, and applications that generate or receive network traffic.

While not specific to CPS, the following examples of **tcpdump** are frequently helpful for troubleshooting CPS network packets.

Note Starting the heapdump on policy director (LB) will have an impact on performance.

TCPDUMP Command

```
tcpdump -i any -s 0 port XXXX
```

where, XXXX is the port number you are interested in.

Options

To Specify Multiple Ports

To capture more than one port:

```
tcpdump -i any -s 0 port 1812 or 1813
```

To capture a port range:

```
tcpdump -i any -s 0 portrange 1812-1817
```

Combining both techniques:

```
tcpdump -i any -s 0 portrange 1812-1817 or port 1700
```

Verbose Mode

```
tcpdump -i any -s 0 -v port XXXX
```

Even more Verbose Mode

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

Restrict to a Specific Interface, such as eth0

```
tcpdump -i eth0 -s 0 port XXXX
```

Redirect Output of the Command to a File

```
tcpdump -i any -s 0 port 1812 -w output.pcap
```

The resulting `output.pcap` file can be opened and utilized using such tools as WireShark.

More options

From a UNIX/Linux prompt, type **man tcpdump**.

Specific Traffic Types

Note These examples assume that the default ports have not been changed or have been specified in Cisco Policy Builder. One must modify these examples to use the appropriate ports that have been specified in Cisco Policy Builder if the default/typical values have been changed.

Capture SNMP Traffic

```
tcpdump -i any -s 0 port 1161 or 1162 or 161 or 162
```

Note This command works for both the sending and receiving machine; the port just needs to match the source or destination port.

Other Ports

The following information is the information format:

Host/VM name Port "Service/traffic type"

where XX is the numeric value of the given host, i.e. pcrfclient01.

pcrfclientXX 80 "Subversion"

pcrfclientXX 7070 "Policy Builder"

sessionmgrXX 27717 "Session Database"

sessionmgrXX 27718 "Quota/Balance Database"

sessionmgrXX 27719 "Reporting Database"

sessionmgrXX 27720 "USuM Database"

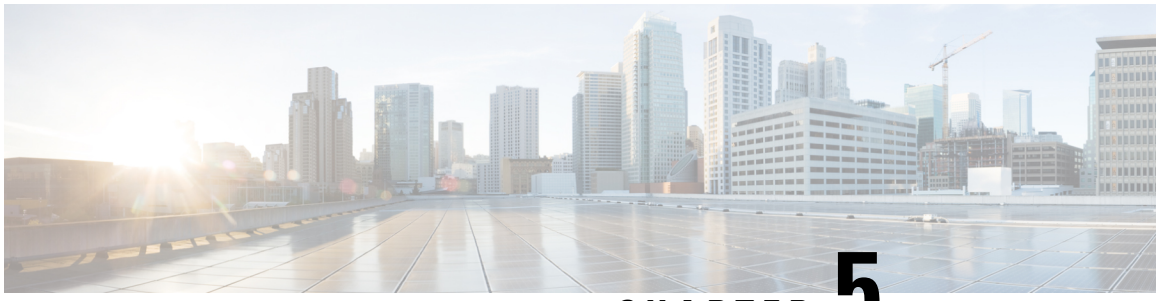
lbvipXX 80 "Subversion vip external"

lbvipXX 8080 "QNS/Unified API VIP"

lbvipXX 11211 "Memcache vip internal"

lbvipXX 7070 "Policy Builder VIP"

qnsXX 9091 "QNS admin port"



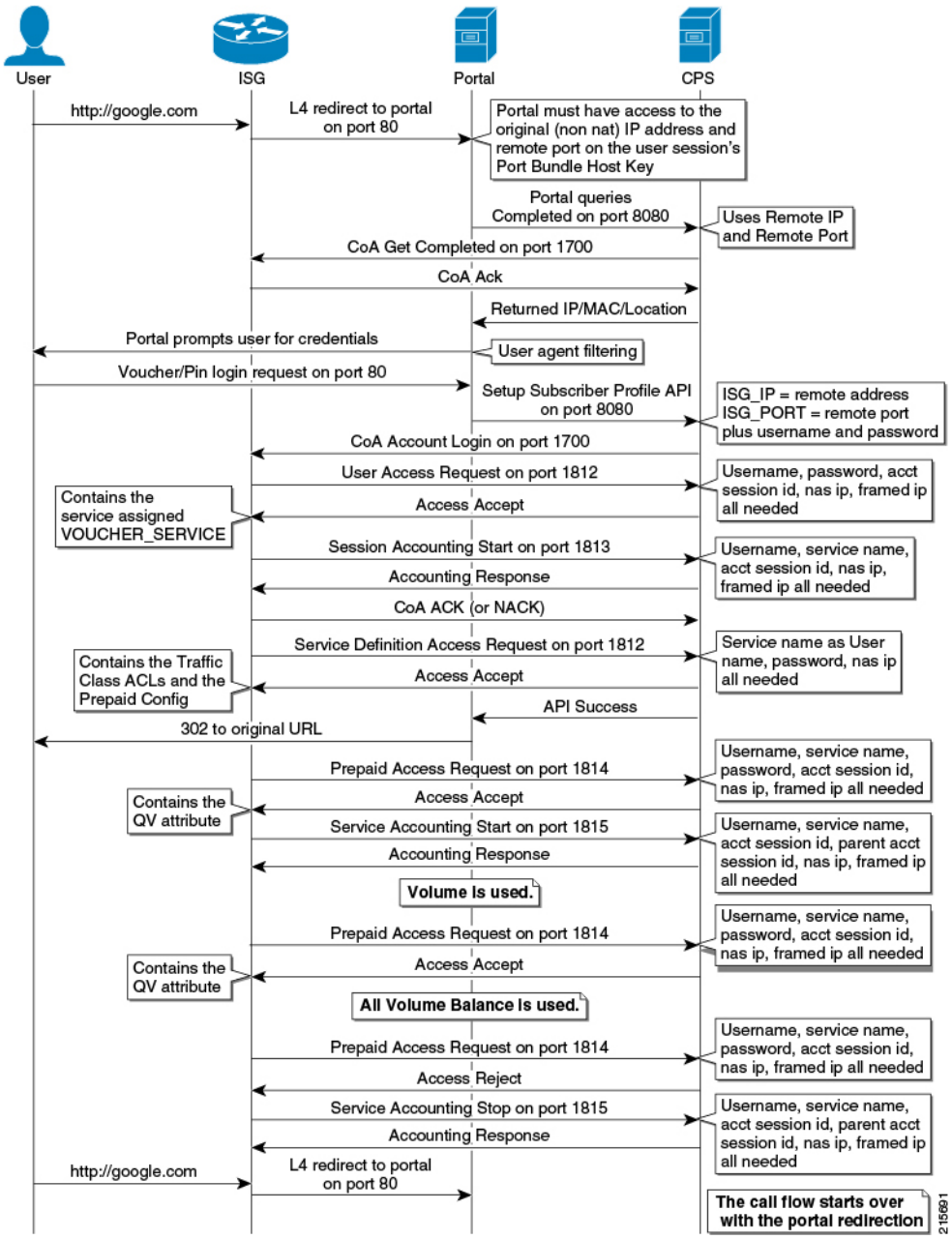
CHAPTER 5

Call Flows

The following call flow diagrams are given to help you troubleshoot and understand CPS deployment.

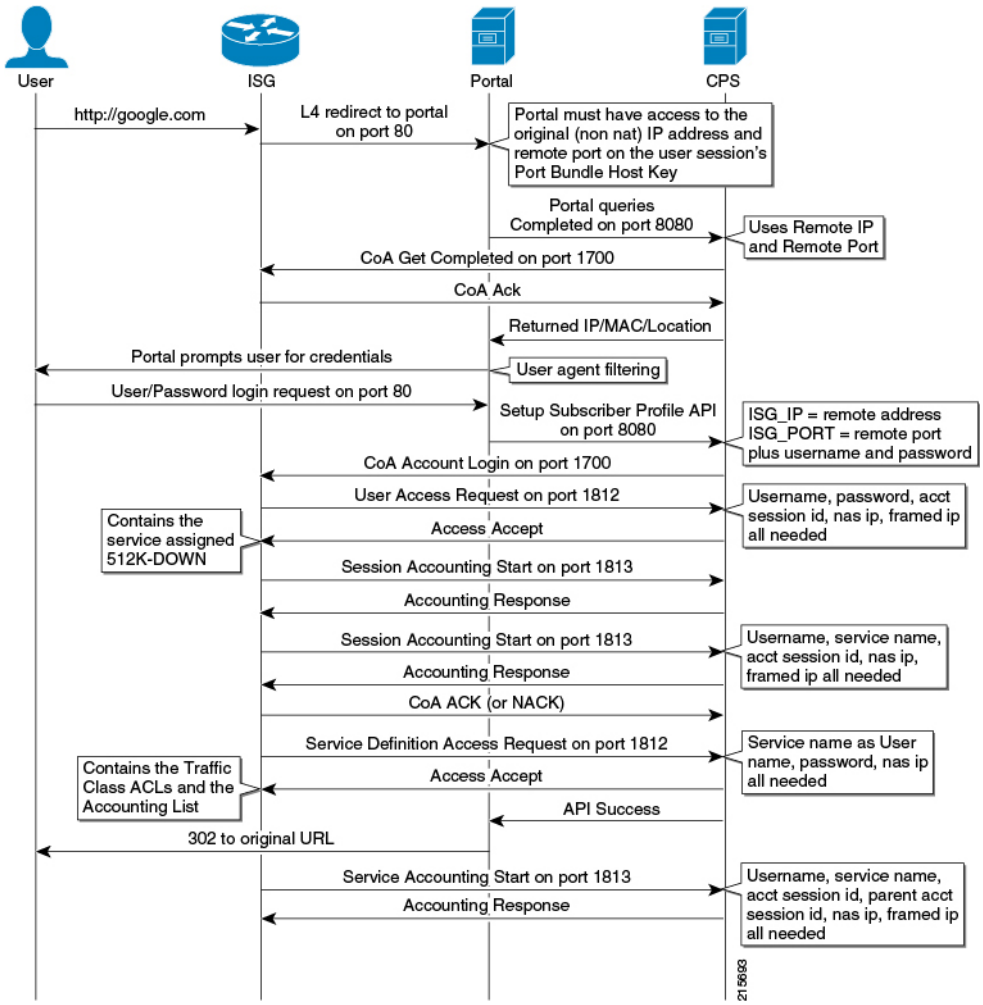
One-Click Call Flow

Figure 43: One-Click Call Flow



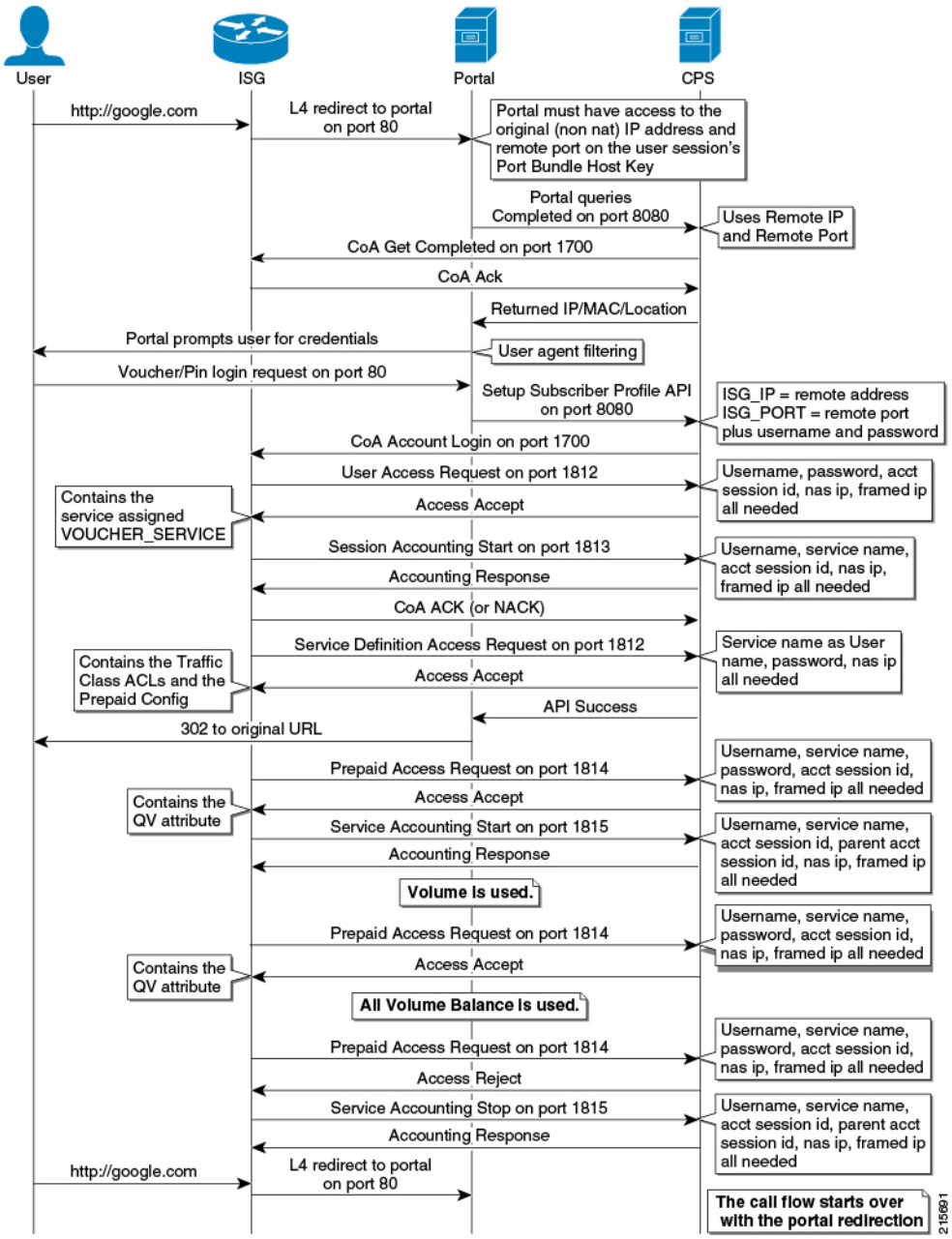
User/Password Login Call Flow

Figure 44: User/Password Login Call Flow



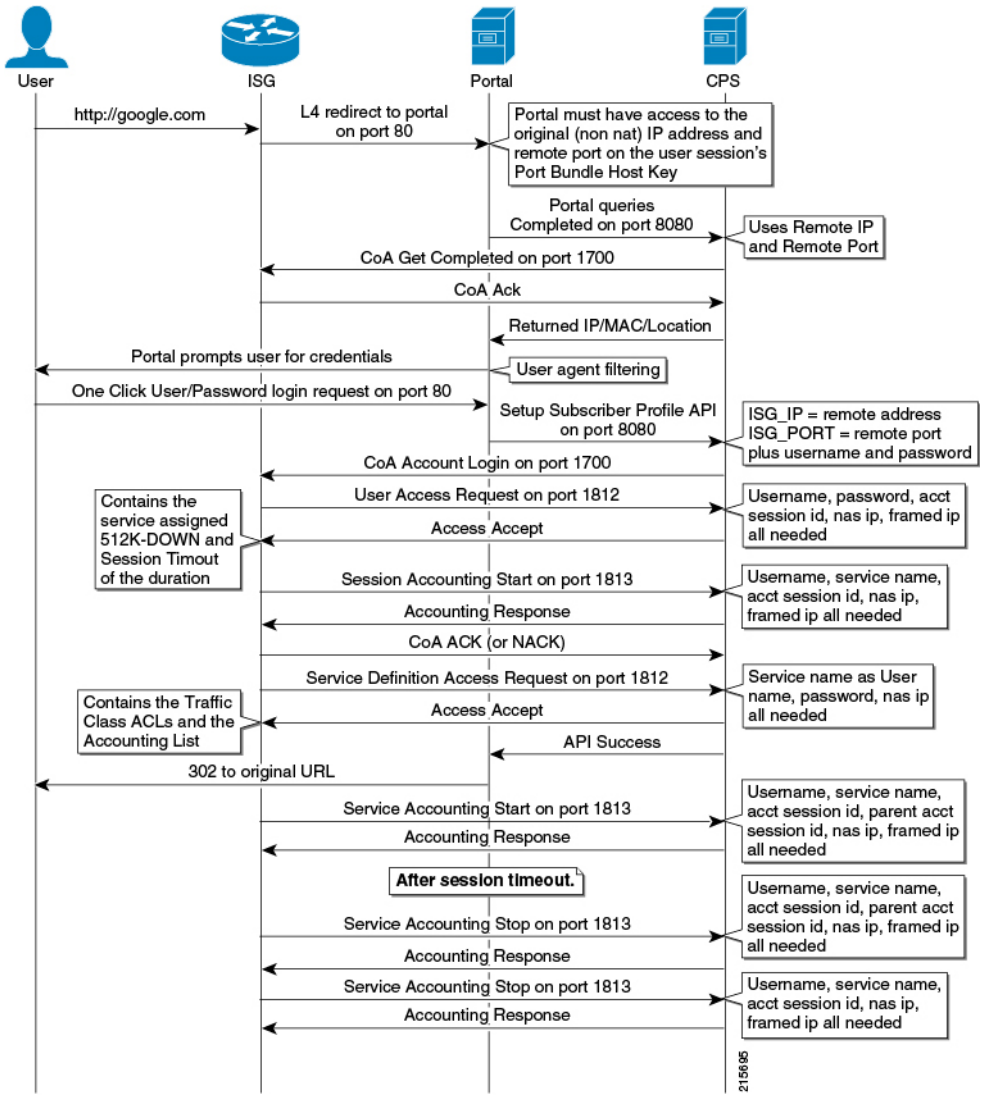
Data-limited Voucher Call Flow

Figure 45: Data-limited Voucher Call Flow



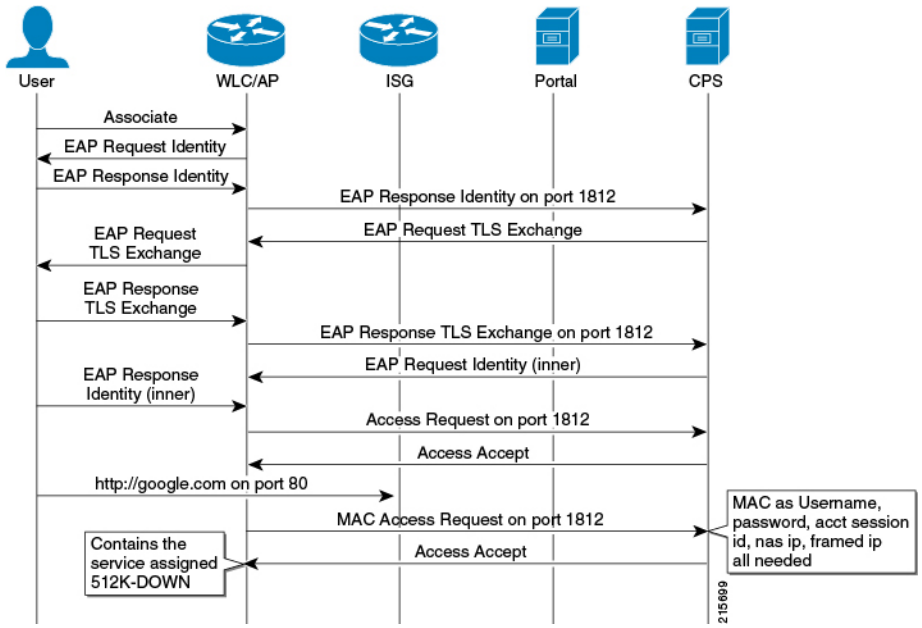
Time-limited Voucher Call Flow

Figure 46: Time-limited Voucher Call Flow



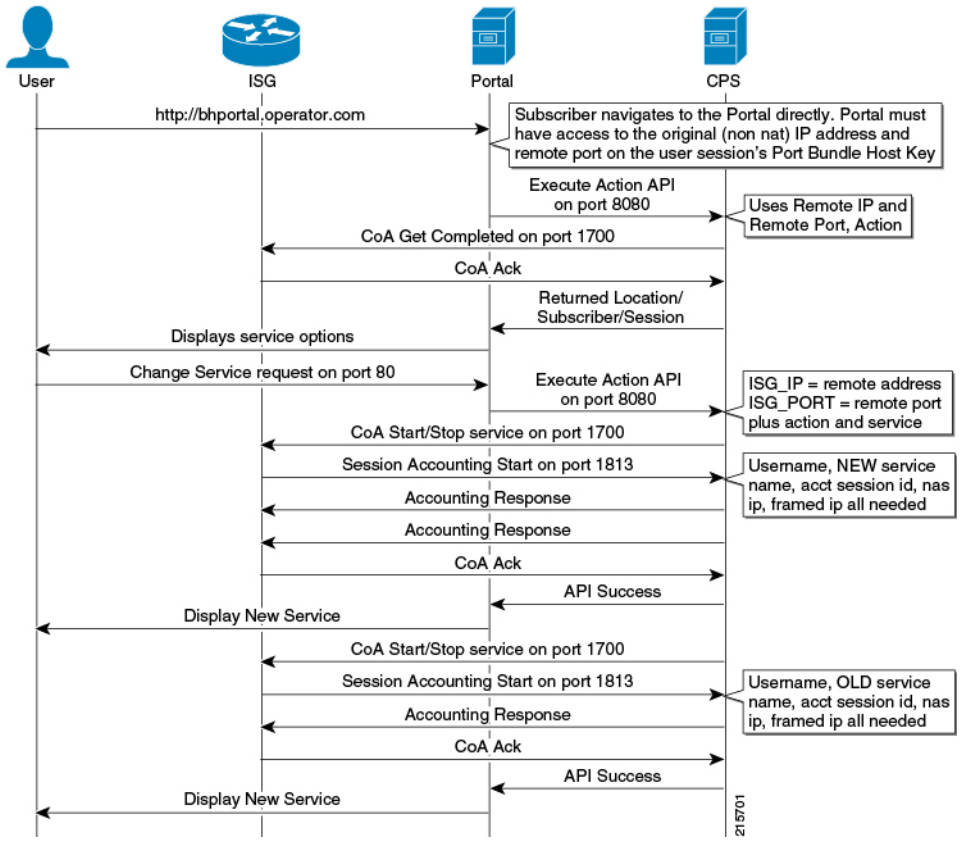
EAP-TTLS Call Flow

Figure 47: EAP-TTLS Call Flow



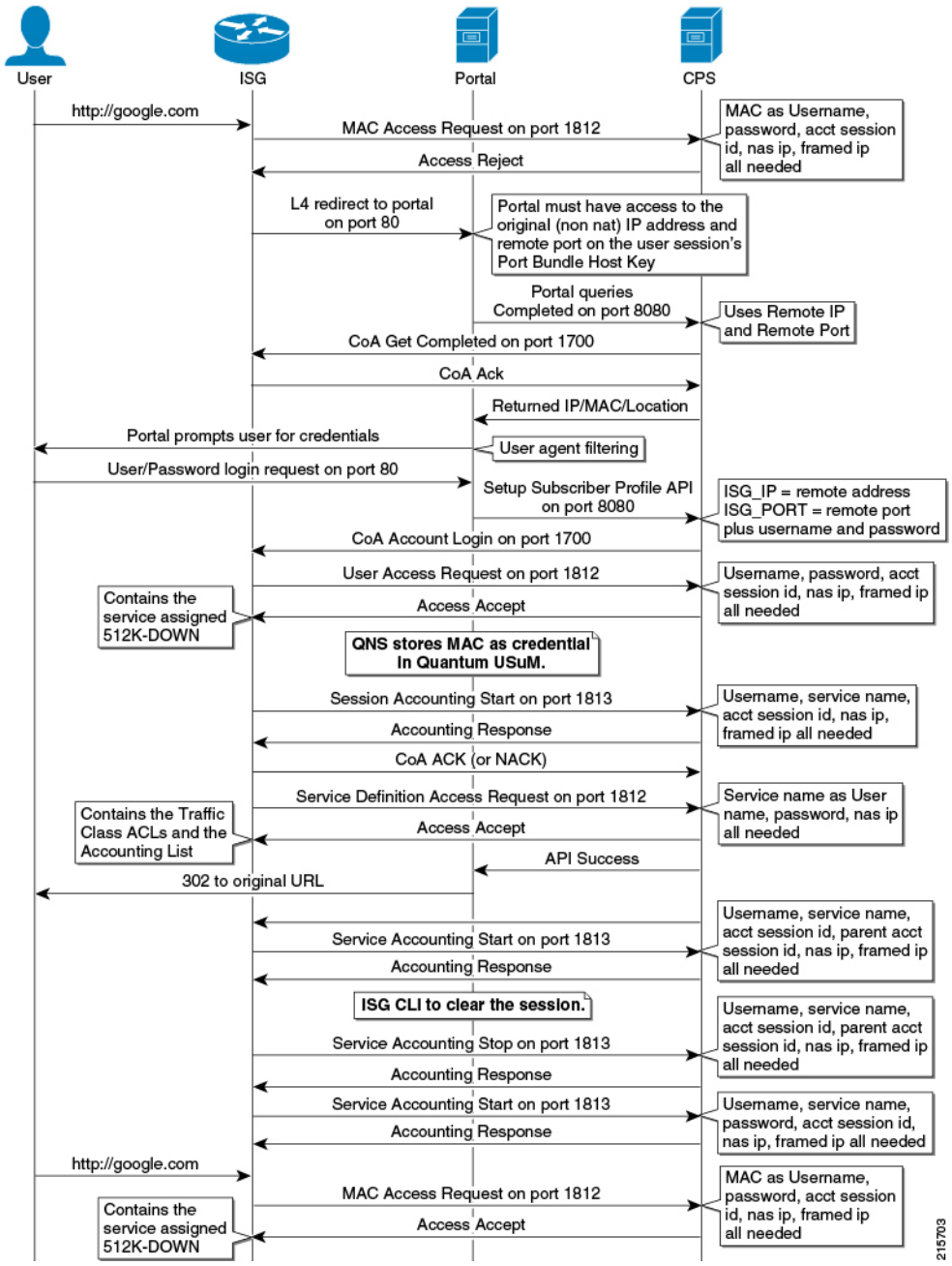
Service Selection Call Flow

Figure 48: Service Selection Call Flow



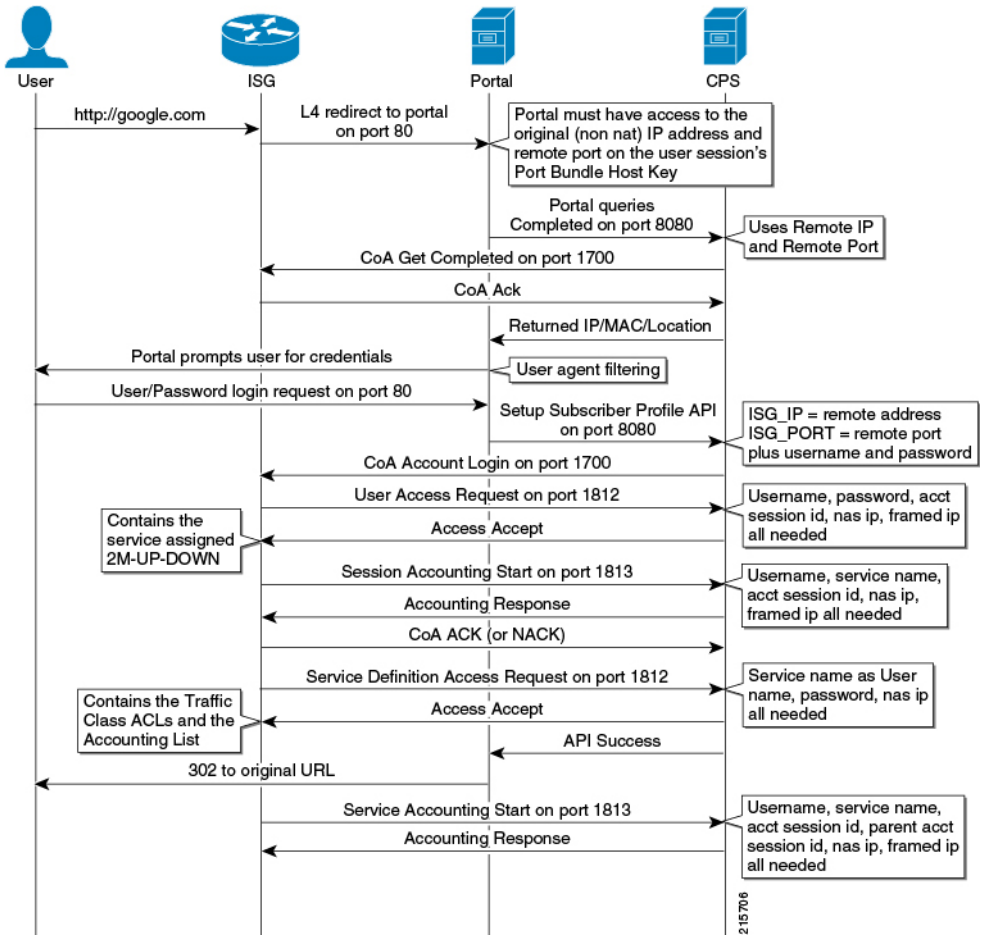
MAC TAL Call Flow

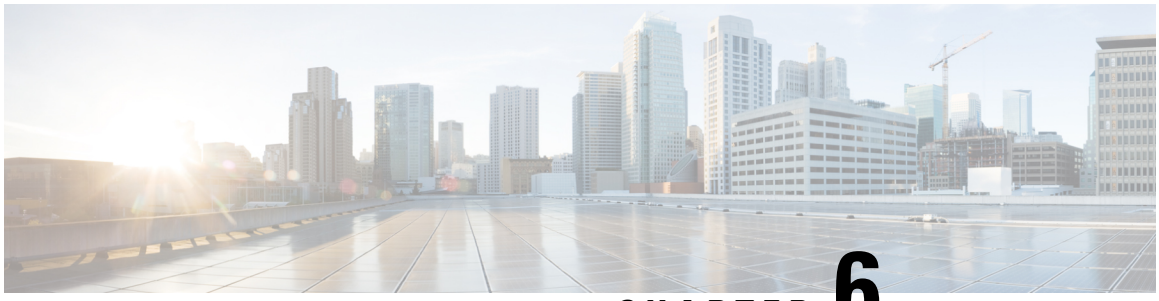
Figure 49: MAC TAL Call Flow



Tiered Services Call Flow

Figure 50: Tiered Services Call Flow





CHAPTER 6

Logging

Overview

CPS logs can be divided into two types:

- Application Logs – generated by CPS applications
- VM Logs – generated by the underlying virtual machine operating system

The normal logs on the individual policy server/policy director/OAM (pcrfclient) VMs are:

Table 12: Normal Logs

File	Contains	Useful for
`/var/log/broadhop/qns-1.log`	main detailed policy server (qns) application logs.	finding initialization errors and application level errors.
`/var/log/broadhop/qns-engine-1.log`	detailed event logs.	finding which services a subscriber has, the state of a session, and other detailed information.
`/var/log/broadhop/service-qns-1.log`	the startup logs. If `logback.xml` is incorrectly formatted, all other log statements will go into this log.	startup errors.

Policy Server (QNS) writes policy director (iomgr) and policy server (qns) logs to consolidated logs on pcrfclient01 including:

Table 13: policy director (iomgr) and policy server (qns) logs

File	Contains	Useful for
/var/log/broadhop/consolidated-qns.log	the consolidation of all policy server (qns) logs with the IP of the instance as part of the log event.	finding initialization errors and application level errors.
/var/log/broadhop/consolidated-engine.log	the consolidation of all policy server (qns) engine logs with the IP of the instance as part of the log event.	finding which services a subscriber has, the state of a session, and other detailed information.

Each VM stores their log files locally before they are consolidated on pcrfclient01. The local logs are:

```
/var/log/broadhop/qns-<#>.log
/var/log/broadhop/service-qns-<#>.log
```

Enable Debug Logs

By default, Cisco recommends to keep log level as WARN or ERROR. Sometimes for analysis the user may need more detailed logging. For this, the user needs the log level based on Cisco recommendation on case-to-case basis.

The following are the various top-level loggers for which the user may need to change log level on case-to-case basis. These loggers must be defined in `/etc/broadhop/logback.xml` file.

To make sure that all changes are controlled from one VM, synchronize all changes made in the Cluster Manager to all the other VMs.

```
SSHUSER_PREFERROOT=true copytoall.sh <path of file where changes have been made> <path of file in other VMs where changes are to be reflected>
```

For example,

```
SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml
```

- For Diameter issues: com.broadhop.diameter2
- For CDR/EDR issues: com.broadhop.policyintel
- For Custom Reference Data issues: com.broadhop.custrefdata
- For Notifications issues: com.broadhop.notifications
- For Session Manager Cache issues: com.broadhop.policy.mdb.cache
- For Control Center issues: com.broadhop.controlcenter
- For Fault Management issues: com.broadhop.faultmanagement
- For LDAP issues: com.broadhop.ldap
- For SPR issues: com.broadhop.spr
- For Unified API issues: com.broadhop.unifiedapi

- For audit issues: com.broadhop.audit
- For policy related issues: com.broadhop.policy
- For any CPS logs issues for which the log level is not overridden by other loggers: com.broadhop
- For CER/CEA DWR/DWA stack level message debugging: jdiameter logs with org.jdiameter

Note For consolidated logs make sure that the configuration specified in Control Center is correct to forward logs to OAM (pcrfclient) VMs.

CPS Logs

The pcrfclient01 VM also contains the consolidated logs from all of the policy director (LB), policy server (QNS) and OAM (PCRFCLIENT) VMs.

The CPS logs can be divided based on Application/Script that produces the logs:

Application/Script Produces Logs: Deploy Logs

- **Log:** deploy log
  - **Description:** Log messages generated during CPS deployment.
  - **Log file name, format, path:**

    HA/GR: cluman: `/var/log/install_console_YYYYMMDD_HHMMSS.log`
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: policy server

- **Log:** policy server (qns) log
  - **Description:** Main and most detailed logging. Contains initialization errors and application level errors.
  - **Log file name, format, path:**

    HA/GR: VM: `/var/log/broadhop/qns-<instance no.log`
  - **Log config File:** `/etc/broadhop/logback.xml`
  - **Log Rollover:** No
- **Log:** policy server (qns) service logs
  - **Description:** Contains start up logs. If `/etc/broadhop/logback.xml` is incorrectly formatted, all logging statements go into this log.

  - **Log file name, format, path:**

    HA/GR: qns0*: `/var/log/broadhop/service-qns-<instance no>.log`

  - **Log config File:** `/etc/broadhop/logback.xml`
  - **Log Rollover:** No

- **Log:** consolidated policy server (qns) logs
  - **Description:** Contains the consolidation of all policy server (qns) logs with the IP of the instance as part of the log event.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/broadhop/consolidated-qns.log`

  - **Log config File:** `/etc/broadhop/controlcenter/logback.xml`
  - **Log Rollover:** No

- **Log:** consolidated engine logs
  - **Description:** Contains the consolidation of all policy server (qns) engine logs with the IP of the instance as part of the log event.
  - **Log file name, format, path:**

    HA/GR: `/var/log/broadhop/consolidated-engine.log`

  - **Log config File:** `/etc/broadhop/controlcenter/logback.xml`
  - **Log Rollover:** No

- **Log:** consolidated diagnostics logs
  - **Description:** Contains logs about errors occurred during diagnostics of CPS.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/broadhop/consolidated-diag.log`

  - **Log config File:** `/etc/broadhop/controlcenter/logback.xml`
  - **Log Rollover:** No

Application/Script Produces Logs: policy server pb

- **Log:** policy server (qns) pb logs
  - **Description:** Policy Builder startup, initialization, warnings, and errors get logged into this log file.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/broadhop/qns-pb.log`

  - **Log config File:** `/etc/broadhop/logback.xml`
  - **Log Rollover:** No

- **Log:** service policy server (qns) pb logs
  - **Description:** Policy Builder service logs.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/broadhop/service-qns-pb.log`
  - **Log config File:** `/etc/broadhop/logback.xml`
  - **Log Rollover:** No

Application/Script Produces Logs: mongo

- **Log:** MongoDB logs
  - **Description:** Contains useful information about the MongoDB operations including queries, errors, warnings, and users' behavior.
  - **Log file name, format, path:**

    HA/GR: sessionmgr01: `/var/log/mongodb-<port>.log`
  - **Log config File:** `/etc/init.d/sessionmgr-*` (the log options are hard coded into these startup scripts)
  - **Log Rollover:** No

Application/Script Produces Logs: httpd

- **Log:** httpd access logs
  - **Description:** Apache server records all incoming requests and all requests processed to a log file.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/httpd/qns-default_access.log`
  - **Log config File:** `/etc/httpd/conf/httpd.conf`
  - **Log Rollover:** Yes
- **Log:** httpd error logs
  - **Description:** All apache errors/diagnostic information about other errors found during serving requests are logged to this file. This apache log file often contain details of what went wrong and how to fix it.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/httpd/error_log`
  - **Log config File:** `/etc/httpd/conf/httpd.conf`
  - **Log Rollover:** Yes

Application/Script Produces Logs: license manager

- **Log:** lmgrd logs
  - **Description:** Contains license file related errors.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/broadhop/lmgrd.log`
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: svn

- **Log:** SVN log
  - **Description:** Displays commit log messages. For more information refer: `/usr/bin/svn log -help`. For example:

    ```
    ./usr/bin/svn log http://lbvip02/repos/run
    ```
  - **Log file name, format, path:**

    HA/GR: NA
  - **Log config File:** NA
  - **Log Rollover:** No

Application/Script Produces Logs: auditd

- **Log:** audit logs
  - **Description:** Contains cron job logs and logs of all SSH sessions established to a CPS VM.
  - **Log file name, format, path:**

    HA/GR: VM: `/var/log/audit/audit.log`
  - **Log config File:** NA
  - **Log Rollover:** Yes

Application/Script Produces Logs: graphite

- **Log:** carbon client logs
  - **Description:** Contains client connection logs.
  - **Log file name, format, path:**

    AIO: `/var/log/carbon/clients.log`

HA/GR: pcrfclient0*: `/var/log/carbon/clients.log`

- **Log config File:** `/etc/carbon/carbon.conf`
- **Log Rollover:** No

- **Log:** carbon console logs
  - **Description:** Contains process startup and initialization logs.
  - **Log file name, format, path:**

    AIO: `/var/log/carbon/console.log`

    HA/GR: pcrfclient0*: `/var/log/carbon/console.log`
  - **Log config File:** `/etc/carbon/carbon.conf`
  - **Log Rollover:** No

- **Log:** carbon query logs
  - **Description:** Contains log queries which are performed on the application.
  - **Log file name, format, path:**

    AIO: `/var/log/carbon/query.log`

    HA/GR: pcrfclient0*: `/var/log/carbon/query.log`
  - **Log config File:** `/etc/carbon/carbon.conf`
  - **Log Rollover:** No

- **Log:** carbon creates logs
  - **Description:** This log tells you what.wsp (whisper) database files are being created.
  - **Log file name, format, path:**

    AIO: `/var/log/carbon/creates.log`

    HA/GR: pcrfclient0*: `/var/log/carbon/creates.log`
  - **Log config File:** `/etc/carbon/carbon.conf`
  - **Log Rollover:** Yes

- **Log:** carbon listener logs
  - **Description:** Contains connection related logs.
  - **Log file name, format, path:**

    AIO: `/var/log/carbon/listener.log`

    HA/GR: pcrfclient0*: `/var/log/carbon/listener.log`
  - **Log config File:** `/etc/carbon/carbon.conf`
  - **Log Rollover:** Yes

Application/Script Produces Logs: kernel

- **Log:** haproxy
  - **Description:** Contains information about HAProxy and VIP failovers.
  - **Log file name, format, path:**

    HA/GR: pcrfclient0*: `/var/log/messages`
  - **Log config File:** NA
  - **Log Rollover:** Yes

Basic Troubleshooting Using CPS Logs

- Review the policy server (qns) engine logs on pcrfclient01/02:

  HA/GR: `/var/log/broadhop/consolidated-engine.log`

  These logs display issues or problems in the subscriber or services. If the event is not found in the engine logs, check the policy server (qns) logs to look for anomalies.
- Determine when the call was supposed to occur in order to narrow down the issue.
- grep usernames, MAC addresses, IP addresses, or other relevant data to find required information.

Logging Level and Effective Logging Level

Logging level and the actual effective logging level can be two different levels because of the following logback logging rules:

- When a logging level is set, if the logging level of the parent process is higher than the logging level of the child process, then the effective logging level of the child process is that of the parent process. That is, even though the logging level of the child process is set, it cannot be below the logging level of the parent process and is automatically overridden to the higher logging level of the parent process.
- There is a global “root” logging level that each process can inherit as an effective default logging level.
  - HA deployments default all logging to ‘warn’ level.
- Each logging level prints the output of the lower logging levels.

  The following table displays the logging level and the message types printed.

Table 14: Logging Level and Effective Logging Level

Level	Message Types Printed
All	Equivalent to Trace and some more messages.
Trace	Trace, Debug, Info, Warn, & Error
Debug	Debug, Info, Warn, & Error

Level	Message Types Printed
Info	Info, Warn, & Error
Warn	Warn & Error
Error	Error
Off	-

The following table describes the different logging levels and what they should be used for:

Table 15: Logging Levels

Logging Level	Description	Valid Use Case	Invalid Use Case
Error	Error conditions that break a system feature. The error logging level should not be used for call flow errors.	Database is not available.	Subscriber not found.
Warn	Helps to understand the early signs that will prevent the system from functioning in the near future OR are triggered by unexpected preconditions in a method.	Retrieved more then one Gx QoS profile.	Warnings should not be used for individual call flows. No service found for session.
Info	Helps to understand the life cycle of components and subsystems, such as plug-ins and databases.	Troubleshooting low-level application issues.	Info should not be used for individual call flows.
Debug	Helps to understand the flow of the code execution at Class/Method level. i.e. in _createIsgDeviceSession({log...)	Troubleshooting low-level application issues.	NA
Trace	Helps to understand the values of the statement and branch of logics within the method for troubleshooting.	Troubleshooting low-level application issues.	NA

You can configure target and log rotation for consolidated logs in the control center's log configuration file `/etc/broadhop/controlcenter/logback.xml`.

The following parameters can be configured for target VM and port.

```
<appender name="SOCKET-BASE" class="ch.qos.logback.classic.net.SocketAppender>"
    <RemoteHost>${logging.controlcenter.host:-lbvip02}</RemoteHost>
    <Port>${logging.controlcenter.port:-5644}</Port>
    <ReconnectionDelay>10000</ReconnectionDelay>
    <IncludeCallerData>false</IncludeCallerData>
</appender>
```

The configuration above is used to redirect consolidated logs to lbvip02 VM on port 5644 with reconnection delay.

Consolidated log rotation is configured using the following configuration in `/etc/broadhop/controlcenter/logback.xml`.

```
<rollingPolicy
    class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
    <fileNamePattern>
${com.broadhop.log.dir:-/var/log/broadhop}/consolidated-diag.%i.log.gz
    </fileNamePattern>
    <minIndex>1</minIndex>
    <maxIndex>5</maxIndex>
  </rollingPolicy>
<triggeringPolicy
    class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
    <maxFileSize>100MB</maxFileSize>
  </triggeringPolicy>
```

Using the above configuration, 100 MB log files are generated and after that, log files rotate from index 1 to 5. This configuration will require 500 MB total available disk space.

Note Do not set `maxFileSize` greater than 100MB as this impacts performance in order to compress the log files.

Do not set `maxIndex` greater than 13, which is the limitation on the logging framework used by CPS.

When the 100 MB log file trigger condition is met, the order in which CPS system performs the file operations is:

- log.5.gz > deleted
- log.4.gz > log.5.gz
- log.2.gz > log.3.gz
- log.1.gz > log.2.gz
- Current > log.1.gz

Similar configurations can be applied for policy server (qns) logs in `/etc/broadhop/logback.xml`.

Consolidated Application Logging

Consolidated logging is a function of all of the CPS VMs, and sends CPS application logs to a central server (either pcrfclient01 or pcrfclient02) to aid the debugging process. The following procedure describes how to configure the consolidated logging function.

Step 1 Edit the `logback.xml` file that is present in the `/etc/broadhop` directory and the `logback.xml` file that is present in the `/etc/broadhop/controlcenter` directory.

Start by viewing the `/etc/broadhop/logback.xml` file. It must have a section that looks similar to this:

```
<!-- Configure Loggers -->
<!-- Hide 'Could not load class...' noise. -->
<logger
name="org.springframework.osgi.extensions.annotation.ServiceRefe
renceDependencyBeanFactoryPostProcessor" level="error" />
<logger name="org.springframework" level="warn" />
<logger name="com.broadhop.resource.impl" level="warn" />
<logger name="com.danga" level="warn" />
```

```
<logger name="httpclient.wire" level="warn" />
<logger name="org.apache.commons.httpclient" level="warn" />
<logger name="sun.rmi.tranrsport.tcp" level="warn" />
<logger name="org.apache.activemq.transport.InactivityMonitor" level="warn" />
<!-- Configure default Loggers -->
<root level="warn">
<appender-ref ref="FILE" />
<appender-ref ref="SOCKET" />
</root>
```

The level can be configured to error, warn, info, or debug in the order of least logging to most logging. When debugging an issue or during initial installation. We recommend that you set the logging level to debug. To change the logging level, change one of the levels or add additional categories, for which you must contact a Cisco support representative.

View the `/etc/broadhop/controlcenter/logback.xml` file. It must have a section that looks similar to this:

```
<!-- Configure Remote Logger -->
<logger name="remote" level="info" additivity="false">
<appender-ref ref="CONSOLIDATED-FILE" />
<appender-ref ref="CONSOLIDATED-JMX" />
</logger>
```

Step 2 If you do not want to have a default effective logging level, then set the root level to off, as shown:

```
<!-- Configure default Loggers -->
<root level="off">
<appender-ref ref="FILE" />
<appender-ref ref="SOCKET" />
</root>
```

Enable Debug Logs

By default, Cisco recommends to keep log level as WARN or ERROR. Sometimes for analysis the user may need more detailed logging. For this, the user needs the log level based on Cisco recommendation on case-to-case basis.

The following are the various top-level loggers for which the user may need to change log level on case-to-case basis. These loggers must be defined in `/etc/broadhop/logback.xml` file.

To make sure that all changes are controlled from one VM, synchronize all changes made in the Cluster Manager to all the other VMs.

```
SSHUSER_PREFERROOT=true copytoall.sh <path of file where changes have been made> <path of file in other VMs where changes are to be reflected>
```

For example,

```
SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml
```

- For Diameter issues: com.broadhop.diameter2
- For CDR/EDR issues: com.broadhop.policyintel
- For Custom Reference Data issues: com.broadhop.custrefdata
- For Notifications issues: com.broadhop.notifications
- For Session Manager Cache issues: com.broadhop.policy.mdb.cache
- For Control Center issues: com.broadhop.controlcenter

- For Fault Management issues: com.broadhop.faultmanagement
- For LDAP issues: com.broadhop.ldap
- For SPR issues: com.broadhop.spr
- For Unified API issues: com.broadhop.unifiedapi
- For audit issues: com.broadhop.audit
- For policy related issues: com.broadhop.policy
- For any CPS logs issues for which the log level is not overridden by other loggers: com.broadhop
- For CER/CEA DWR/DWA stack level message debugging: jdiameter logs with org.jdiameter

Note For consolidated logs make sure that the configuration specified in Control Center is correct to forward logs to OAM (pcrfclient) VMs.

Note Do not set the root log level to anything higher than 'warn' in a production system. If needed, adjust the individual loggers listed in `logback.xml`.

The levels debug or info usually have logs rollover very quickly. After the log rolls over, the information is lost. For this reason, warn or error generates a substantially smaller amount of logging, and gives you the ability to look for issues in the system over a longer period of time.

Step 1 On the CPS node where you require debug logs, edit the `/etc/broadhop/logback.xml` file.

The default root logger level would be currently set to WARN. It must be changed to debug, as shown.

```
<!-- Configure default Loggers -->
<root level="debug">
<appender-ref ref="FILE" />
<appender-ref ref="SOCKET" />
</root>
```

Step 2 The specific component for which you require the debug log should be set to "debug" in the appropriate line. For example:

For Control Center:

On pcrfclient01, update the logback.xml on `/etc/broadhop/controlcenter/`.

```
<logger name="com.broadhop.controlcenter" level="debug"/>
And
<root level="debug">
    <appender-ref ref="FILE" />
  </root>
```

For Audit:

```
<logger name="com.broadhop.audit" level="debug"/>
```

For Balance:

```
<logger name="com.broadhop.balance" level="debug"/>
```

For SPR:

```
<logger name="com.broadhop.spr" level="debug"/>
```

For Congestion Reference Data:

```
<logger name="com.broadhop.CongestionRefData" level="debug"/>
```

For LDAP:

```
<logger name="com.broadhop.ldap" level="debug"/>
```

For DRA:

```
<logger name="com.broadhop.dra" level="debug"/>
```

For POP-3 Authentication:

```
<logger name="com.broadhop.pop3auth" level="debug"/>
```

For Scheduled Events:

```
<logger name="com.broadhop.scheduledevents" level="debug"/>
```

For Diameter:

```
<logger name="com.broadhop.diameter2" level="debug"/>
```

For CDR/EDR:

```
<logger name="com.broadhop.policyintel" level="debug"/>
```

For Custom Reference Data:

```
<logger name="com.broadhop.custrefdata" level="debug"/>
```

For Notification:

```
<logger name="com.broadhop.notifications" level="debug"/>
```

Session Manager Cache:

```
<logger name="com.broadhop.policy.mdb.cache" level="debug"/>
```

Step 3 Save and exit.

Step 4 Run the following command to synchronize changes to all CPS VMs:

```
/var/qps/bin/update/syncconfig.sh
```

Enable Unified API Request and Response Logging

The following procedure describes how to enable logging to debug Unified API requests and responses. This level of logging is usually sufficient for the majority of debugging.

Step 1 On the Cluster Manager VM, add the following entry to `/etc/broadhop/logback.xml`:

```
<logger name="com.broadhop.unifiedapi.soap.servlet" level="debug"/>
```

Step 2 Copy the updated `/etc/broadhop/logback.xml` file to all other CPS VMs:

```
/var/qps/install/current/scripts/bin/control/copytoall.sh /etc/broadhop/logback.xml
```

Step 3 Search the logs for the following phrases to locate valid API requests/responses:

```
request to server:
response from server:
```

The logs will include a string containing the XML sent on the request and response for Unified API calls. This XML will NOT contain the SOAP wrapper information, such as the namespace info and envelope, header, and body tags. It will only include the inner XML that policy server (QNS) actually processes.

The SOAP wrapper tags would need to be added to paste this into SoapUI and submit it. However, this is easily done by using SoapUI to create a sample request after reading the WSDL and then just pasting in the piece from the log in the appropriate place in the XML in SoapUI.

Note Set the following parameter in the `qns.conf` file to output the Unified API logs in formatted XML instead of a continuous string. You must restart the policy server (qns) processes after modifying `qns.conf` file.

```
-Dpretty.print.responses=true
```

Rsyslog Log Processing

Rsyslog Overview

Rsyslog logs Operating System (OS) data locally on each VM (`/var/log/messages`) using the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*conf` configuration files.

On all nodes, Rsyslog forwards the OS system log data to lbvip02 via UDP over the port defined in the logback_syslog_daemon_port variable as set in the CPS deployment template (Excel spreadsheet). To download the most current CPS Deployment Template (`/var/qps/install/current/scripts/deployer/templates/QPS_deployment_config_template.xlsm`), refer to the *CPS Installation Guide for VMware* or *CPS Release Notes* for this release.

Refer to http://www.rsyslog.com/doc/ for more details and Rsyslog documentation.

Rsyslog-proxy

A second instance of Rsyslog called Rsyslog-proxy is installed only on Policy Director (LB) nodes. Rsyslog-proxy is only installed if the syslog_managers_list variable is set in the CPS Deployment Template.

Rsyslog-proxy is the main log forwarding process and is configured in `/etc/rsyslog-proxy.conf` on LB01/LB02 VMs.

- It receives OS system log data from all the nodes via UDP over the PORT defined in the logback_syslog_daemon_port variable. The default port number is 6514.
- The `/etc/broadhop/controlcenter/logback.xml` file on OAM (pcrfclients) is configured to send logs to rsyslog-proxy via UDP using the logback SyslogAppender. See Configuration of Logback.xml, on page 163 for more information.

- Rsyslog-proxy forwards the OS system log data and CPS log data to logstash via TCP on PORT 6513 with a UDP backup.
- By default, Rsyslog-proxy does not log any syslog data to local files on the OAM (PCRFClient) VMs. To configure the system to output consolidated log files for syslog data on the OAM (PCRFclients), see Enable Consolidated Syslog Output to Files on OAM VMs, on page 162.
- It receives CPS JSON formatted log data via TCP on PORT 5544. Rsyslog-proxy forwards that to logstash via TCP on PORT 5543 with a UDP backup.
- It receives SNMP events via TCP on PORT 7546. rsyslog-proxy forwards that to logstash via TCP on PORT 7545 with a UDP backup.
- Rsyslog-proxy sends all OS system log data and CPS log data to any number of remote servers via UDP or TCP in case the encryption is enabled. (The remote servers must be configured to receive traffic but that is not a part of the scope of this document.)

Configuration for HA Environments

Configuration of Rsyslog for High Availability CPS environments is performed using the CPS Deployment Template.

Refer to the following information available in the template tabs.

Configuration Variables

The following variables can now be set in the CPS Deployment Template:

- syslog_managers_list — space separated list of remote logging servers (tuple protocol:hostname:port). Only UDP is currently supported.
- syslog_managers_ports — comma separated list of the remote logging server ports (must match the ports in the syslog_managers_list).
- logback_syslog_daemon_addr — hostname of the internal UDP server that rsyslog-proxy runs to receive incoming logs from CPS and OS (defaults to lbvip02).
- logback_syslog_daemon_port — incoming port for rsyslog-proxy (defaults to 6514).

Note If the syslog_managers_list variable is empty, the rsyslog-proxy instance is not installed or configured.

Additional Hosts Tab

The following parameter can be configured in the Additional Hosts tab of the CPS Deployment Template file:

Table 16: Parameters in Additional Hosts Tab

corporate_syslog_ip	syslog_manager	<IP ADDR>

Configuration Tab

The following parameters can be configured in the Configuration tab of the CPS Deployment Template file:

syslog_managers_list	udp:corporate_syslog_ip:<PORT>
syslog_managers_ports	<PORT>
logback_syslog_daemon_addr	lbvip02
logback_syslog_daemon_port	6514

- lbvip02 is the default address for logback to send data.
- 6514 is the default port for logback to send data.

Configuration for AIO

The Rsyslog-proxy configuration for AIO environment uses a custom “facts” file:

`/etc/facter/facts.d/rsyslog.txt`

The same variables are used as in the CPS Deployment Template.

For example:

- syslog_managers_list=udp:corporate_syslog_ip:514
- syslog_managers_ports=514
- logback_syslog_daemon_addr=lbvip02
- logback_syslog_daemon_port=6514

On AIOs, you must add aliases to `/etc/hosts` for the remote servers as defined in the syslog_managers_list.

Enable Consolidated Syslog Output to Files on OAM VMs

By default, consolidated syslog logs from all VMs are not written to local files on the OAM (PCRFClient) VMs. The following procedure describes how to configure the system to output consolidated log files for syslog data on the OAM (PCRFclients).

Step 1 On the Cluster Manager VM, edit the following file:

`/etc/puppet/modules/qps/templates/logstash/logstash.conf`

Step 2 Add the following section highlighted below:

```
output {
  if [type] == "snmp-event-log" or [type] == "qps" {
    udp {
      host => "127.0.0.1"
       port => 2121
    }
  }
  if [type] == "syslog" {
```

```
    file {
      message_format => "%{[message_remainder]}"
      codec => "plain"
      path => "/var/log/broadhop/syslog/consolidated-messages.log"
    }
  }
}
```

Step 3 The directory in the 'path' above must exist on pcrfclient01/pcrfclient02 VMs and the directory must be owned by 'logstash:logstash'. If needed, SSH to each OAM (pcrfclient) to create the directory. Use the following command to change ownership of this directory:

```
chown -R logstash:logstash <dir>
```

Step 4 Once the configuration is in place on the Cluster Manager VM, run the following command to prepare the VMs using this new configuration:

```
/var/qps/install/current/scripts/build/build_puppet.sh
```

Step 5 Run the following command to propogate the changes to all VMs:

```
pupdate
```

Step 6 To control how often these log files are overwritten, edit the file `/etc/logrotate.d/logstash` on pcrfclient01/02 VMs with the following content.

Note The path and filename specified below should match the 'path' value in `/etc/puppet/modules/qps/templates/logstash/logstash.conf`.

```
/var/log/broadhop/syslog/*.log
/var/log/logstash/*.log
{
        daily
        rotate 7
        copytruncate
        compress
        delaycompress
        missingok
        notifempty
}
```

Configuration of Logback.xml

The `/etc/broadhop/controlcenter/logback.xml` file on OAM (pcrfclients) is configured to send logs to rsyslog-proxy via UDP using the logback SyslogAppender.

Refer to http://logback.qos.ch/manual/appenders.html#SyslogAppender for the Syslog Appender documentation.

The following appender forwards all CPS logs to a remote server.

```
<appender name='SYSLOG' class='ch.qos.logback.classic.net.SyslogAppender'>
  <syslogHost>lbvip02</syslogHost><!--#SAP#-->
  <port>6514</port><!--#SAP#-->
  <suffixPattern>[qps] [%d{yyyy-mm-dd'T'HH:mm:ss.SSSZ}] %msg</suffixPattern>
  <facility>LOCAL0</facility>
</appender>
```