CONTENTS

Getting Started vii
Readers vii
Additional Support vii
Terms and Definitions viii

CHAPTER 1

Troubleshooting CPS 1-1

Troubleshooting 1-1
General Troubleshooting 1-1
Portal Troubleshooting 1-2
Domain Troubleshooting 1-4
RADIUS Troubleshooting 1-5
E2E Call Flow Troubleshooting 1-5

Troubleshooting Basics 1-5
Gathering Information 1-5
CPS Control Center Interface Guide 1-6
CPS Subscriber Services Admin User Interface Guide 1-6
Check Zabbix Information 1-7
Check NMS Information 1-7

Diameter Error Codes and Scenarios 1-7

Common Troubleshooting Scenarios 1-9
Scenario - No Response to Diameter Request 1-9
Using TCPDUMP 1-9
CPS Logs 1-9
TCPDUMP – User Id Filter 1-10
No Response – Using Policy Trace 1-11
Policy Trace – Match Response 1-11

Rare Troubleshooting Scenarios 1-12
Recovery using Remove/Add members Option 1-12
Remove Failed Members 1-13
Add Failed Members 1-14

Maintenance Window Procedures 1-16
Prior to Any Maintenance 1-16
Change Request Procedure 1-16
Software Upgrades 1-16
Application Restarts 1-17
VM Restarts 1-17
Hardware Restarts 1-17
Planned Outages 1-17

Non-maintenance Window Procedures 1-18

Common Troubleshooting Tasks 1-18
CPS Trace Monitoring 1-18
Kill All Cisco Processes From the Command Line as Root 1-18
Low or Out of Disk Space 1-20
df Command 1-20
du Command 1-20

Frequently Encountered Troubles 1-21
Subscriber not Mapped on SCE 1-21
CPS Server Will Not Start and Nothing is in the Log 1-22
Server returned HTTP Response Code: 401 for URL 1-23
com.broadhop.exception.BroadhopException: Unable to Find System Configuration for System 1-23
Log Files Display the Wrong Time but the Linux Time is Correct 1-23
JMX Management Beans are not Deployed 1-24
Unable to Access Binding Information 1-24
Error Processing Package, Reference Data Does Not Exist for NAS IP 1-24
REST Web Service Queries Returns an Empty XML Response for an Existing User 1-25
Error in Datastore: "err": "E11000 Duplicate Key Error Index 1-25
Error Processing Request: Unknown Action 1-26
Memcached Server is in Error 1-26
Firewall Error: Log shows Host Not Reachable, or Connection Refused 1-27
Unknown Error in Logging: License Manager 1-27
Ecore File is Not Generated: 1-27
Logging Does Not Appear to be Working 1-28
Cannot Connect to Server Using JMX: No Such Object in Table 1-29
File System Check (FSCK) Errors 1-29
CPS: 27717 Mongo Stuck in STARTUP2 after sessionMgr01/2 Reboot 1-32
SR: 628099455 System Failure Errors in Control Center 1-34
Zabbix is Using More Space in GR Setup on Site 1 and Site 2 1-37
MAC Address Change Fails the License Check 1-40
Multi-user Policy Builder Errors 1-40
Not able to do any edits after login 1-40
Error in login due to conflict 1-40
No configuration visible in Policy Builder after login 1-40
Exception Occurred During Login 1-41
Debug Details 1-42
Policy Reporting Configuration not getting updated post CPS Upgrade 1-42
CPS Memory Usage Increased 1-43
   Detect and Reclaim Cached Memory 1-43
spr_encryption_update 1-44
Enable/disable Debit Compression 1-45
SNMP Traps and Key Performance Indicators (KPIs) 1-46
   Full (HA) Setup 1-47
   All-in-one (AIO) Setup 1-48
   Add Multiple NMS Addresses to Configuration Files 1-49
Traps Generated by CPS 1-51
   Component Notifications 1-51
   Application Notifications 1-54
Components and KPI Values 1-59
   Component Values 1-59
   KPI Values 1-60
FAQs 1-62
Reference Document 1-62

CHAPTER 2
Check Subscriber Access 2-1
Checking Access 2-1
   Testing Subscriber Access with 00.testAccessRequest.sh 2-1
   Testing Subscriber Access with soapUI 2-2
   Testing for ISG Functionality and Connectivity with test aaa Scripts 2-6

CHAPTER 3
TCP Dumps 3-1
TCPDUMP Command 3-1
   Options 3-1
   To Specify Multiple Ports 3-1
   Verbose Mode 3-2
   Even more Verbose Mode 3-2
   Restrict to a Specific Interface, such as eth0 3-2
   Redirect Output of the Command to a File 3-2
   More options 3-2
Specific Traffic Types 3-2
   Capture RADIUS Traffic 3-2
   Capture SNMP Traffic 3-2
   Other Ports 3-3
Call Flows

A-1

One-click Call Flow  A-2
User/Password Login Call Flow  A-4
Data-limited Voucher Call Flow  A-6
Time-limited Voucher Call Flow  A-9
WISPr Call Flow  A-11
EAP-TTLS Call Flow  A-13
Service Selection Call Flow  A-15
MAC TAL Call Flow  A-17
Tiered Services Call Flow  A-20
SP WiFi-4.0 Call Flows  A-21
  Authentication Sequence in WLC Network Device Manager  A-22
  Authentication Sequence for EAP Requests  A-23
  Authentication Sequence in iWAG Network Device Manager  A-24
  MAG Coupled Web Based Authentication  A-25
Getting Started

Welcome to the Cisco Policy Suite 6.1 Troubleshooting Guide.
This document describes common methods and scenarios of correcting processing and production functions for the Cisco Policy Suite.
Read about these topics in these sections:

- Readers
- Additional Support
- Terms and Definitions

Readers

This guide is best used by the following readers.

- Deployment engineers
- System administrators
- Network administrators
- Network engineers
- Network operators
- Implementation engineers

This document assumes an intermediate level of understanding of network architecture, configuration, and operations. This document is most helpful if readers have completed Cisco training classes and have a firm introduction to the concepts and behavior of Cisco Policy Suite.

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 your other documents.
Terms and Definitions

This document uses certain terms and definitions specific to the CPS software application. Please refer to our common Glossary of Terms.
Troubleshooting CPS

Revised: April 28, 2015,
This chapter covers the following sections:

- Troubleshooting
- Troubleshooting Basics
- Diameter Error Codes and Scenarios
- Common Troubleshooting Scenarios
- Rare Troubleshooting Scenarios
- Maintenance Window Procedures
- Common Troubleshooting Tasks
- Frequently Encountered Troubles
- SNMP Traps and Key Performance Indicators (KPIs)

Troubleshooting

- Find out if your problem is related to CPS or another part of your network.
- Gather materials that facilitate the support call.

General Troubleshooting

- Are their specific SNMP traps being reported that can help you isolate the issue?
- Run `/opt/broadhop/installer/diagnostic.sh`

  [root@lab ~]# exec diagnostics.sh
  ?[H][2JQNS Diagnostics
  Validating hostnames...?[32mPASS?[0m
  Checking basic ports (80, 11211, 7070, 8080, 27017, 9091, 9092)...?[32mPASS?[0m
  Checking qns passwordless logins on all boxes...?[32mPASS?[0m
  Checking swap space...
  Checking swap memory usage on pcrcfclient01...?[33mWARN?[0m
  Swap usage is 977 MB. This may indicate that the system needs more memory allocated. Please monitor closely for swap usage increase.
If system memory usage is no longer high, you can reset swap with:

```
/opt/broadhop/installer/diag/support/swap2ram.sh
```

Checking disk usage... [PASS]
Checking QNS RADIUS (UDP) ports (1812, 1813)... Could not connect to port 1812 on qns01 (Radius access requests)... [FAIL]
Could not connect to port 1813 on qns01 (Radius accounting requests)... [FAIL]
Retrieving QNS diagnostics from qns01:9045... [WARN]

- **Run** `/opt/broadhop/control/statusall.sh`

```
[root@lab ~]# exec statusall.sh
Executing sudo /etc/init.d/qns status on all QNS Servers
lab
qns-1 (pid 21995) is running...
qns-2 (pid 22035) is running...
```

Connection to lab closed.

- **From pcrfclient01, run** `tail -f /var/log/broadhop/consolidated-qns.log`

Go to the bottom of the log file and search backwards for ‘ERROR’. For more details, see Cisco Policy Suite 6.1 Alarming and SNMP Guide.

- **Look for stack traces.**

```
2013-05-28 05:40:36 Error: [InternalErrorException]
Failed finding location.
```

```
#0 /var/www/portal/app/Controller/SubscribersController.php(1420):
Subscriber->getLocation()
#1 /var/www/portal/app/Controller/SubscribersController.php(45):
SubscribersController->_setLocationAndProfile()
#2 [internal function]:
SubscribersController->beforeFilter(Object(CakeEvent))
#3 /var/www/portal/lib/Cake/Event/CakeEventManager.php(246):
call_user_func(Array, Object(CakeEvent))
#4 /var/www/portal/lib/Cake/Controller/Controller.php(670):
CakeEventManager->dispatch(Object(CakeEvent))
```

```
#5 /var/www/portal/lib/Cake/Routing/Dispatcher.php(100):
Controller->startupProcess()
Dispatcher->_invoke(Object(SubscribersController),
Object(CakeRequest), Object(CakeResponse))
#7 /var/www/portal/app/webroot/index.php(153):
Dispatcher->dispatch(Object(CakeRequest),
Object(CakeResponse))
#8 {main}
```

**Portal Troubleshooting**

- Is the right portal page displaying?
- If not, review the consolidated log output to see what network mapping is being applied and what the location query response is back to the portal.
- Fix any network mapping problems through your portal administration GUI. In a web browser go to `<IP_address>users/login` and log in as administrator.
• Enable API debugging in the portal by modifying the script /var/www/portal/app/Config/broadhop.php

• Run tail -f /var/www/portal/app/tmp/logs/api_request.log

2013-05-28 05:40:36 Api_request: REQUEST:
Array

[method] => POST
    <soapenv:Header/>
    <soapenv:Body>
        <typ:ExecuteActionRequest>
            <typ:code>location-query</typ:code>
            <typ:arg>
                <typ:code>ip-address</typ:code>
                <typ:value><![CDATA[127.0.0.1]]></typ:value>
            </typ:arg>
            <typ:arg>
                <typ:code>port</typ:code>
                <typ:value><![CDATA[60147]]></typ:value>
            </typ:arg>
        </typ:ExecuteActionRequest></soapenv:Body></soapenv:Envelope>
[uri] => Array

[scheme] => http
[host] => 127.0.0.1
[port] => 8080
[path] => /ua/soap
)
[header] => Array

[Content-Type] => text/xml;charset=ISO-8859-1
[Cache-Control] => no-cache
Pragma] => no-cache
[SOAPAction] => ""
[Content-length] => 511
)

• For the older portal version run tail -f /var/www/portal/app/tmp/logs/qns_calls.log.

• For the newer portal version run tail -f /var/www/portal/app/logs/api_response.log.

2013-05-28 05:40:36 Api_response: RESPONSE:
object(HttpResponse)#67 (7) {
"body"=> string(1274) "<html>
<head>
<meta http-equiv="Content-Type" content="text/html;charset=ISO-8859-1"/>
<title>Error 404 Not Found</title>
</head>
<body>
<h2>HTTP ERROR: 404</h2>
<p>Problem accessing /ua/soap. Reason: Not Found</p>
</body>
" ["headers"]=>
array(5) {
    "Cache-Control" => string(33) "must-revalidate,no-cache,no-store"
    "Content-Type" => string(28) "text/html;charset=ISO-8859-1"
    "Content-Length" => string(4) "1274"
    "Connection" => string(5) "close"
    "Server" => string(21) "Jetty(7.x.y-SNAPSHOT)"
}
"cookies" => bool(false)
"httpVersion" => string(8) "HTTP/1.1"
"code" => string(3) "404"
"reasonPhrase" => string(9) "Not Found"
"raw" => string(1466) "HTTP/1.1 404 Not Found
Cache-Control: must-revalidate,no-cache,no-store
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 1274
Connection: close
Server: Jetty(7.x.y-SNAPSHOT)
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;charset=ISO-8859-1"/>
<title>Error 404 Not Found</title>
</head>
<body>
<h2>HTTP ERROR: 404</h2>
<p>Problem accessing /ua/soap. Reason:
<pre>Not Found</pre></p>
<hr /><i><small>Powered by Jetty://</small></i>
</body>
</html>
}

Domain Troubleshooting

- Run `tail -f consolidated-qns.log` from the bottom to determine what domain is being calculated for your call flow.
- The domain calculation comes after the location query response to the portal.
- If the domain calculation is wrong, either the wrong portal has been determined or the wrong domain is associated with your desired portal page.
- You can fix your domain association through the portal administration page.
- If your domain is correct but the call flow is incorrect after that, access Policy Builder to review your domain configuration.
RADIUS Troubleshooting

- Test service definition requests from a PEP such as ISG to the CPS by running the following command:
  
  `test aaa group radius L4REDIRECT_SERVICE password legacy`
  
  - Repeat this command for PBHK_SERVICE and OPENGARDEN_SERVICE.
- Listen for RADIUS traffic from the PEP by logging into lb01 and lb02 and run the following command:
  
  `tcpdump –i any port 1812 –s 0 -vvv`

  Test general subscriber access with the procedures in Check Subscriber Access.

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 or RADIUS 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
  - Portallbs and Portals on ports 80

  Correct call flows are shown in Appendix A, “Call Flows”

Troubleshooting Basics

Troubleshooting CPS consists of these types of basic tasks:

- Gathering Information
- Collecting logs
- Running traces

This section also presents CPS-specific tasks:

- Common Troubleshooting Scenarios
- System Maintenance and Recovery
- System Maintenance
- Replacing Hardware

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?
• Is the issue affecting all subscribers?
• Is the issue affecting all subscribers on a specific service?
• Is there anything else common to the issue?
Initially, categorize the issue to determine the level of support needed.

CPS Control Center Interface Guide

The Control Center interface has screens that help you and your Cisco technical representative diagnose troubles.

1. Access the Control Center interface at http://<ipserver>:8090 on your server. Here, ipserver is lbvip01.
2. Enter your username and password to log in.
3. Click the Monitoring tab and open the tree on the left to examine:
   - System health
   - Current statistics for your system
   - Trends

For Control Center documentation, locate the Cisco Policy Suite Control Center Interface Guide.

CPS Subscriber Services Admin User Interface Guide

The CPS Subscriber Service Portal interface has screens that help you and your Cisco technical representative diagnose troubles with the portal and its interaction with Policy Builder.

1. Access the Subscriber Service Portal interface at http://<ipserver>/users/login on your server. Here ipserver is sslvip01.
2. Log in as an admin user.
3. Click Settings and use any of these screens underneath:
   - Configuration Check
   - Location Settings
   - Query Map
   - CPS Logs

For Subscriber Service Portal documentation, locate the Cisco Subscriber Service Portal Interface Guide.
Check Zabbix Information

- Is there any alarming in Zabbix that would indicate a component or connectivity failure?
- Do any of the KPIs indicate a change in the call flow or subscriber volume?

Check NMS Information

This is not as detailed as Zabbix KPIs or component views but provides a wider view of the entire system.

- Is there any alarming that would indicate a component or network failure?
- Are there any KPIs that indicate changes in the call flow or traffic volume?

Diameter Error Codes and Scenarios

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

<table>
<thead>
<tr>
<th>Error Code</th>
<th>CPS Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAMETER_ERROR_BEARER_NOT_AUTHORIZED</td>
<td>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.</td>
</tr>
<tr>
<td>DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED</td>
<td>Emergency service related- Used when the PCRF does not accept one or more of the traffic mapping filters.</td>
</tr>
<tr>
<td>DIAMETER_USER_UNKNOWN</td>
<td>Subscriber not found in SPR.</td>
</tr>
<tr>
<td>DIAMETER_AUTHORIZATION_REJECTED</td>
<td>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.</td>
</tr>
<tr>
<td>DIAMETER_UNABLE_TO_COMPLY</td>
<td>Message rejected as something else that went wrong and there’s no specific reason.</td>
</tr>
<tr>
<td>DIAMETER_SUCCESS</td>
<td>Everything went well and Request processed successfully.</td>
</tr>
<tr>
<td>Error Code</td>
<td>CPS Scenarios</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DIAMETER_TOO_BUSY</td>
<td>Message got discarded by the overload handling mechanism.</td>
</tr>
<tr>
<td>Note</td>
<td>CPS 6.1 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.</td>
</tr>
<tr>
<td>DIAMETER_UNABLE_TO_DELIVER</td>
<td>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.</td>
</tr>
<tr>
<td>DIAMETER_APPLICATION_UNSUPPORTED</td>
<td>A request was sent for an application that is not supported.</td>
</tr>
<tr>
<td>DIAMETERUNKNOWN_PEER</td>
<td>A CER was received from an unknown peer.</td>
</tr>
<tr>
<td>DIAMETER_UNKNOWN_SESSION_ID</td>
<td>The request contained an unknown Session-Id.</td>
</tr>
<tr>
<td>DIAMETER_NO_COMMON_APPLICATION</td>
<td>When a CER message is received, and there are no common applications supported between the peers.</td>
</tr>
<tr>
<td>DIAMETER_ERROR_TRIGGER_EVENT</td>
<td>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.</td>
</tr>
<tr>
<td>DIAMETER_PCC_RULE_EVENT</td>
<td>When for some reason the PCC rules cannot be installed/activated. The reason is provided in the Event Trigger AVP value.</td>
</tr>
<tr>
<td>DIAMETER_PCC_BEARER_EVENT</td>
<td>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.</td>
</tr>
<tr>
<td>DIAMETER_ERROR_UNKNOWN_POLICY_COUNTERS</td>
<td>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).</td>
</tr>
<tr>
<td>DIAMETER_ERROR_NO_AVAILABLE_POLICY_COUNTERS</td>
<td>Error used by the OCS to indicate to the PCRF that the OCS has no available policy counters for the subscriber.</td>
</tr>
</tbody>
</table>
Common Troubleshooting Scenarios

- Scenario - No Response to Diameter Request

Scenario - No Response to Diameter Request

Using TCPDUMP

- Collect tcpdump packet capture from the primary 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

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Request</th>
<th>Response</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>2</td>
<td>10:09:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>3</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>4</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>5</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>6</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>7</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
<tr>
<td>8</td>
<td>10:10:4.87</td>
<td>20.10.4.87</td>
<td>20.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>10.10.4.87</td>
<td>UMTS 1008</td>
</tr>
</tbody>
</table>

- Filter using Subscription-Id-Data (MSISDN) to retrieve the CCR initial request
- Start the policy trace for a subscriber using MSISDN as the search string. For example, in a deployment with qns01-04:
  ```java
  java -DsearchString=255654940574 -Dservers=qns01,qns02,qns03,qns04 -DtraceLogging=true -jar traceMonitor.jar &> /var/tmp/policy-trace.log &
  ```
- When a deployment with qns01-06
  ```java
  java -DsearchString=255654940574 -Dservers=qns01,qns02,qns03,qns04,qns05,qns06 -DtraceLogging=true -jar traceMonitor.jar &> /var/tmp/policy-trace.log &
  ```
- The Policy trace logs all policies executed for each message handled for the user.
- Verify the log to match requests and responses using CC-Request-Type attribute in the request/response.
Verify the log for any policy execution errors.

**No Response – Using Policy Trace**

Use the search string “Set Diameter Session Key” to identify incoming request

```
Policy executed "Set Diameter Session Key" [255654940573] Triggering Conditions [255654940573]
Object ID : 21, Class: com.broadhop.diameter.gx.allot.messages.DiameterCCRMessage [255654940573] {subIdType=1, calledStationID=tigoweb}
```
Use the search string “Send Allot Gx Answer Message” to identify matching response

```
age[255654940573]{subIdType=1, calledStationID=tigoweb,
requestId=bb487926-41c2-459f-aaf>d768cf5abe38#1026576,
msisdn=255654940573, originHost=allot-smp1-tz,
originRealm=tigo.co.tz, stackName=10.10.4.96:3868,
requestType=1, framedIpAddress=10.111.17.98,
bearerOperation=1, requestNumber=10660733,
usageVolume=-1,
sessionId=DPI.ALLOT.COM;702461250;485609944,
bearerIdentifier=1, eventTrigger=[],
chargingRuleReport=[], imsi=,
usageMonitoringControl=[]}
```

**Rare Troubleshooting Scenarios**

**Recovery using Remove/Add members Option**

When Arbiter blade and a sessionmgr blade goes down, there wont be any primary sessionmgr node to cater requests coming from CPS VMs (Classic HA setup-1 arbiter, 2 sessionmgrs). As a result, system becomes unstable.

Safer way to recover from the issue is to bring UP down blades to working state. But 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.

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.

```bash
#diagnostics.sh --get_replica_status
```

**Step 3**
Execute build_set.sh with below option to remove failed member/s from replica set, this operation removes the all failed members across the site.

```bash
#cd /opt/broadhop/installer/support/mongo/

For session db

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

For spr db

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

For balance db

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

For report db

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

For portal db

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

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

```bash
#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.
Add Failed Members

Step 1  Login to pcrfclient01/02.

Step 2  Once 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
```

Step 4  If status is not seen properly by above command, login to mongo port on sessionmgr and check replica status.
# cd /opt/broadhop/installer/support/mongo

For session db

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

For spr db

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

For balance db

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

For report db
#./build_set.sh --report --add-members

For portal db

#./build_set.sh --portal --add-members

## Maintenance Window Procedures

The usual tasks for a maintenance window might include these:

- Prior to Any Maintenance
- Change Request Procedure
- Software Upgrades
- Application Restarts
- VM Restarts
- Hardware Restarts
- Planned Outages

### Prior to Any Maintenance

Backup all relevant information to an offline resource. For more information on backup, see the Cisco Policy Suite 6.1 Backup and Restore Guide.

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

**Note**  
Sessions can be backed up as well.

- Configurations - Backup all configuration information. This includes SVN (from PCRFClient), 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 at 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.

**Application Restarts**

Application restarts are component independent. These are the components:
- PCRF/PCRFClient
- Load Balancer/IO Manager
- sessionMgr

IO Manager, PCRF, PCRFClient
- IO Managers and PCRF give up their resources and allow the fail overs to take over. They can be stopped directly with `service qns restart`
- PCRFClient is a GUI application and can be restarted at any point. If SVN is restarted, the PCRF applications continue to run, but throw errors saying that they cannot check for new configurations. This will not impact the environment.
- sessionMgr is deployed as active - standby and is used by the policy server to maintain the subscriber session state information.
- Load Balancers distribute the load for RADIUS, Web Services, MySQL, LDAP, and SVN. Two load balancers are deployed for each Cisco Policy Suite in active/passive mode.

**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.
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.

CPS Trace Monitoring

In this policy trace example: the search string searches the incoming message and the network session.

```
java -DsearchString=255654940574
-Dservers=qns01,qns02,qns03,qns04,qns05,qns06,qns07,qns08,qns09
-DtraceLogging=true -jar traceMonitor.jar &> /var/tmp/policy-trace.log &
```

Kill All Cisco Processes From the Command Line as Root

Depending on the Linux version, one or both of these `ps` commands are applicable. Remove the portion 'lxargs kill -9' if you want to test out the command.

These commands do the following:

- print out all processes (ps), then
- search (grep) for all processes that do not contain the word grep or mysql, then
- use sed to remove all the remaining text except for the PID value, and then
- send that PID to kill -9.

PIDs must be 3 characters to 5 characters long.

```
[root@lab ~]# ps -A
PID TTY TIME CMD
1 ? 00:00:00 init
2 ? 00:00:01 migration/0
3 ? 00:00:00 ksoftirqd/0
4 ? 00:00:01 migration/1
5 ? 00:00:00 ksoftirqd/1
6 ? 00:18:49 events/0
7 ? 00:00:00 events/1
8 ? 00:00:00 khelper
49 ? 00:00:00 kthread
54 ? 00:00:00 kbhostd/0
55 ? 00:00:00 kbhostd/1
56 ? 00:00:00 kacpid
217 ? 00:00:00 cqueue/0
```
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**

Example is provided at

`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

An example of this command is found at:

home# du -hs * Linux Disk Usage command

This command produces this output:

[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.

---

**Frequently Encountered Troubles**

This section lists trouble issues already diagnosed and solved.

**Subscriber not Mapped on SCE**

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

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
tworkAccountingUtil No member in system for d162818
policy.log:2009-07-17  11:02:06,108 INFO
tworkAccountingUtil No member in system for D02625
policy.log.1:2009-07-17  09:25:29,036 INFO
tworkAccountingUtil No member in system for D162346
policy.log.1:2009-07-17  09:27:28,718 INFO
tworkAccountingUtil No member in system for d162365
policy.log.1:2009-07-17  09:27:37,193 INFO
tworkAccountingUtil No member in system for d162365
policy.log.1:2009-07-17  09:27:42,257 INFO
tworkAccountingUtil No member in system for d162365
```
Frequently Encountered Troubles

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

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 to give reasons it did not start, check the following list:

1. Check /var/log/broadhop/service-qns-1.log

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/control center 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) ~\[na:1.6.0_20\]

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 Policy Builder (and cluster name) must match the one specified in /etc/broadhop/qns.conf. Either add or change this via the 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.

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

```
ZONE="America/Denver"
UTC=false
ARC=false
```

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
JMX Management Beans are not Deployed

1. Restart the CPS Server. The JMX Beans sometimes are not deployed when features are installed or updated.
2. Run `ps -ef | grep java` and look for: `-javaagent:/opt/broadhop/qns/bin/jmxagent.jar`. If this is absent, you have an old build and need to update.
3. If you have an old build, see the Operations guide for instructions on updating.

Unable to Access Binding Information

Make sure the binding has been compiled. This error is typically caused by a bad build.

Attempt to upgrade to a newer build.

If you're on a released build, try restarting, there's been a strange bug which causes web service problems after update.

2010-10-19 12:05:00.194 [pool-4-thread-1] ERROR
c.b.d.impl.DiagnosticController - Diagnostic failed. A problem exists with the system --> Common Services: Feature com.broadhop.ws.service is unable to start. Error: Error creating bean with name 'org.springframework.web.servlet.mvc.annotation.DefaultAnnotationHandlerMapping#0' defined in URL [bundleentry://27.fwk15830670/META-INF/spring/bundle-ws-context.xml]: Initialization of bean failed; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'subscriberEndpoint' defined in URL [bundleentry://27.fwk15830670/META-INF/spring/bundle-ws-context.xml]: Cannot resolve reference to bean 'jibxMarshaller' while setting bean property 'marshaller'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'jibxMarshaller' defined in URL [bundleentry://27.fwk15830670/META-INF/spring/bundle-ws-context.xml]: Invocation of init method failed; nested exception is org.jibx.runtime.JiBXException: Unable to access binding information for class com.broadhop.ws.impl.messages.RemoveSubscriberProfileRequest

Error Processing Package, Reference Data Does Not Exist for NAS IP

Ensure that this NAS IP has been set up in Policy Builder under Reference Data->Policy Enforcement Points. If you use an ISG, add to the ISG Pools folder. Otherwise, add to the RADIUS Device Pools folder. The IP's that matter are in the 'Devices' table on the ISG Pool object itself.

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

This removes ALL 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.

1. ssh into sessionmgr01
2. Open SessionMgr CLI
   
   /usr/bin/mongo --port 27717
   
   Using /usr/bin/mongo indicates whether the mongo replica set is primary or secondary.
3. Enter following commands on the MongoDB CLI

```bash
use session_cache;
db.session.remove();
```

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

### Error Processing Request: Unknown Action

```java
```

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

```java
ERROR c.b.d.impl.DiagnosticController - Diagnostic failed.
A problem exists with the system --> Common Services:
 2:Memcached server is in error
```

1. Log on to the server where qns is running
2. `telnet` to the memcache server's IP and port 11211 (ex: `telnet lbvip01 11211`).

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

- If you can't `telnet` to the port, do this

Ensure memcache is running:

- Log on to server where memcache is running

run service memcached status

```
[root@sessionmgr01 ~]# service memcached status
memcached is stopped
```

- If the service is stopped, start it:

```
[root@sessionmgr01 ~]# service memcached start
Starting a new distributed memory caching
```
b. Ensure firewall configuration is OK:
To check if this is the problem, just 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 iptables /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(LicenseManager.java:311)

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 QPS 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/.

Ecore File is Not Generated:

    2010-12-12 18:39:34.075 [SpringOsgiExtenderThread-8] ERROR
A feature (RADIUS) has been installed in Policy Builder, but is not installed on the server. Or, a features file being accessed is not where features have been placed.

1. Check if the feature is installed in your server by running
   `/opt/broadhop/qns-1/bin/list_installed_features.sh`.

2. If the feature IS installed, you probably are pointing to (or publishing to) the wrong repository. Check where you’re publishing to in Policy Builder and check what URL you are pulling from in `/etc/broadhop/qns.conf`.

3. If the feature IS NOT installed, you may be pointing to a different features file than you expect. Do this:
   a. Login to CPS server and find the name of the qns server you are on
   b. Type: `hostname`
   c. Check `/etc/broadhop/servers` file

Whatever is listed next to the hostname you are using should also have a directory in the `/etc/broadhop` directory. It is in THAT directory you should change the features file. This defaults qns01 to ‘iomanager’. Change it to ‘pcrf’.

Logging Does Not Appear to be Working

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
   ```
   2. Access that bean using JMX Term or JConsole to view the status of the Logback Appenders. To access JMX Term, follow these steps:
      - Execute below script: `/opt/broadhop/qns-1/bin/jmxterm.sh`
      - 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`
        - Again execute the script: `/opt/broadhop/qns-1/bin/jmxterm.sh`
        - Once command is executed, JMX terminal opens up.
        - Execute the below command to open connection:
          ```
          $>open qns01:9045
          ```
          - All beans can be seen using below command
            ```
            $>beans
            #domain = JMImplementation:
            JMImplementation:type=MBeanServerDelegate
            #domain = ch.qos.logback.classic:
            ch.qos.logback.classic:Name=default,Type=ch.qos.logback.classic.jmx.JMXConfigurator
            #domain = com.broadhop.action:
            com.broadhop.action:name=AddSubscriberService,type=hi
            ```
Frequently Encountered Troubles

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: iomgr01:9045. 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 1-1  FSCK Errors

<table>
<thead>
<tr>
<th>SNo.</th>
<th>FSCK Error</th>
<th>Description/Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BAD SUPER BLOCK: MAGIC NUMBER WRONG USE ALTERNATE SUPER-BLOCK TO SUPPLY NEEDED INFORMATION</td>
<td>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. Reference link to fix the issue - <a href="http://www.cyberciti.biz/faq/recover-bad-superblock-from-corrupted-partition/">http://www.cyberciti.biz/faq/recover-bad-superblock-from-corrupted-partition/</a></td>
</tr>
<tr>
<td>2</td>
<td>Block bitmap not in a group/inode bitmap not in a group</td>
<td>When this error occurs, data on the device need to be restored using dd or any other device specific command. Reference link to fix the issue - <a href="https://bbs.archlinux.org/viewtopic.php?id=128478">https://bbs.archlinux.org/viewtopic.php?id=128478</a> or <a href="http://serverfault.com/questions/131536/ext3-fs-block-bitmap-for-group-1-not-in-group-block-0-is-fs-dead">http://serverfault.com/questions/131536/ext3-fs-block-bitmap-for-group-1-not-in-group-block-0-is-fs-dead</a></td>
</tr>
<tr>
<td>3</td>
<td>Inode table not in a group</td>
<td>When this error occurs, data on the device need to be restored using dd or any other device specific command. Reference link to fix the issue - <a href="http://www.linuxquestions.org/questions/linux-hardware-18/missing-inode-table-646788/">http://www.linuxquestions.org/questions/linux-hardware-18/missing-inode-table-646788/</a></td>
</tr>
<tr>
<td>4</td>
<td>Primary superblock is corrupt</td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>Journal superblock has an unknown read-only feature flag set</td>
<td>Please refer to Error 1 to 4 to fix this issue.</td>
</tr>
<tr>
<td>6</td>
<td>Resize inode is invalid</td>
<td>This error occurs after file system is resized. Reference link to fix this issue - <a href="https://bugzilla.redhat.com/show_bug.cgi?id=156954">https://bugzilla.redhat.com/show_bug.cgi?id=156954</a></td>
</tr>
<tr>
<td>7</td>
<td>Last mount time is in the future</td>
<td>This error occurs after reboot system clock is not synchronized with UTC. Reference link to fix this issue - <a href="http://forums.debian.net/viewtopic.php?t=45797">http://forums.debian.net/viewtopic.php?t=45797</a></td>
</tr>
</tbody>
</table>
### Frequently Encountered Troubles

#### Reference to fix issues:
- [Causes of sudden massive filesystem damage: root inode is not a directory](http://serverfault.com/questions/204617/causes-of-sudden-massive-filesystem-damage-root-inode-is-not-a-directory)
- [Resolving Root inode is not a directory Clear Linux Error](http://www.programmersheaven.com/user/mariapeter12/blog/4320-Resolving-Root_inode_is_not_a_directory-Clear_Linux_Error/)

#### Table 1-1 FSCK Errors

<table>
<thead>
<tr>
<th>SNo.</th>
<th>FSCK Error</th>
<th>Description/Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Root directory is not an inode</td>
<td>If primary superblock is corrupt this error occurs, alternate superblock needs to be specified to fsck in this case. Reference link to fix this issue - <a href="http://serverfault.com/questions/204617/causes-of-sudden-massive-filesystem-damage-root-inode-is-not-a-directory">Causes of sudden massive filesystem damage: root inode is not a directory</a> <a href="http://www.programmersheaven.com/user/mariapeter12/blog/4320-Resolving-Root_inode_is_not_a_directory-Clear_Linux_Error/">Resolving Root inode is not a directory Clear Linux Error</a></td>
</tr>
<tr>
<td>9</td>
<td>Duplicate `..' entry</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 1-1  FSCK Errors

<table>
<thead>
<tr>
<th>SNo.</th>
<th>FSCK Error</th>
<th>Description/Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Error reading block &lt;block_no&gt; (Attempt to read from filesystem resulted in short read) while doing inode scan.</td>
<td>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.</td>
</tr>
<tr>
<td>11</td>
<td>Journal superblock has an unknown incompatible feature flag set</td>
<td>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 &quot;no&quot; and after this fix the superblock corruption. Reference link to fix the issue - <a href="http://forums.debian.net/viewtopic.php?f=5&amp;t=83716">http://forums.debian.net/viewtopic.php?f=5&amp;t=83716</a></td>
</tr>
</tbody>
</table>

- Following link gives list of all the errors which are automatically fixed by fsck as well as list of errors where user intervention is must - http://unix.stackexchange.com/questions/18526/what-does-fsck-p-preen-do-on-ext4
- Following link gives general idea about various phases in fsck - http://etutorials.org/Misc/solaris+exam+guide/Part+I+Solaris+9+Operating+Environment+Exam+I/Chapter+9+Introduction+to+File+Systems/Fixing+Problems+with+fsck/
- Following link describes all the errors in case of UFS file system - http://docs.oracle.com/cd/E19253-01/817-0403/tsfsck-26279/index.html
  This link can be used as a reference to fix the errors reported by fsck on CPS file system which is ext3.

**CPS: 27717 Mongo Stuck in STARTUP2 after sessionMgr01/2 Reboot**

There can be a situation where 27717 mongo process is stuck after sessionMgr01/02 is rebooted. In this situation follow the below mentioned steps to bring up 27717 all mongo process from STARTUP2 state to PRIMARY/SECONDARY state specific to session database only.

**Step 1** Stop CPS process.

**Step 2** Log onto pcrfclient01.

**Step 3** Execute the diagnostic 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 bad shape.
Currently, there is no support to create a specific replica set. For example, there is no support to create multiple session replica sets such as set01, set01a in configuration file.

**Step 4**
Take a backup of current configuration file and keep only the definition of replica set that needs to be rebuild.

```
#cd /etc/broadhop
#cp mongoConfig.cfg mongoConfig.cfg.bk
```

**Step 5**
Edit configuration file and keep only set01 definition (that is, failed replica set definition).

```
#vi mongoConfig.cfg
```

**Step 6**
Build session replica sets. Select 2 for session non-sharded sets.

```
#cd /opt/broadhop/installer/support/mongo/
./build_set.sh --session --create
```

Starting Replica-Set Creation

Please select your choice: replica sets sharded (1) or non-sharded (2):

```
2
```

**Step 7**
Ignore this step if the setup is HA environment, otherwise set priority 2 for primary site all replica set members. By default, 1 is used for secondary site members.

```
./set_priority.sh --p 2 --db session --sn pri
```

**Step 8**
Revert the backed-up configuration file.

```
#cd /etc/broadhop
#mv mongoConfig.cfg.bk mongoConfig.cfg
```

**Step 9**
Verify if priority is set correctly for newly created replica set.

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

**Step 10**
To recover other failed set, follow the recovery steps from Step 1 to Step 9.
Step 11  Restart CPS.

/opt/broadhop/control/restartall.sh

SR: 628099455 System Failure Errors in Control Center

Issue 1: The issue is that the Monitoring tab in control center is supposed to give system health status for the VM's that are hosted only within CPS. In this scenario, the Monitoring tab was reporting status for Gx-Origin and Gy-Origin host which are not the part of CPS setup but are added in /etc/hosts and we can't comment these Gx and Gy host name since this is used for diameter connectivity.

Issue 2: The customer is having only one QNS process running per CPS Virtual machine, but the control center reports that their second QNS process on all CPS VM is down. This second QNS process is not even configured in CPS virtual machine and the customer wants Control Center only to report for only one QNS process per CPS VM.
Step 1  Go to the path.
        cd /etc/collectd.d
Step 2  List the files.
        ls -lrth
Step 3  Take the backup of the below scripts before modifying them so that original data is preserved
        cp server_availability.sh old_serveravailability.sh
        cp database_availability.sh old_databaseavailability.sh
        cp types.db old_types.db
        cp qns_availability.sh old_qnsavailability.sh
Step 4  Enter the file using vi mode.
        vi server_availability.sh
Step 5  Change the line
        #SERVERLIST=$(egrep -v "(localhost|vip|corporate_nms_ip)"
        /etc/hosts | awk '{print $2}"
        to
        SERVERLIST=$(egrep -v -i
        "(localhost|vip|corporate_nms_ip|#|GX|GY|ext)" /etc/hosts | awk
        '{print $2}"
Step 6  Enter the file with vi mode.
        vi database_availability.sh
Step 7  Change the lines
        #PORTLIST="27717 27718 27719 27720 27730"
        #NAMELIST="session session quota report usum
        to
        PORTLIST="27717 27718 27719 27720
        NAMELIST="session quota report usum"
Step 8  Enter the file with vi mode.
        vi qns_availability.sh

This step is to be performed only when we have one QNS process per CPS VM.
If you see qns_availability.sh file, there are three ports 8080, 8081 and 9091. Identify the ports
which are not catering any process.
Steps to check a port that is not having QNS process: (from PCRF Client not in Vi Mode)

**a.** To list process:

```bash
netstat -an | grep 8080
netstat -an | grep 8081
netstat -an | grep 9091
```

**b.** Consider an example that 8081 is not carrying any QNS process. So to remove the same from `qns_availability.sh`, adjust the array size and also `qnsavailbility.sh` should look exactly same as below.

```bash
PORTLIST[0]="8080"
#PORTLIST[1]="8081"
PORTLIST[1]="9091"
CMDLIST[0]="GET /service/Subscribers/wsdlDefinition.wsdl HTTP/1.0\n\n'"
#CMDLIST[1]="GET /service/Subscribers/wsdlDefinition.wsdl HTTP/1.0\n\n'"
CMDLIST[1]="ss com.broadhop.model.policy"
RESLIST[0]="200 OK"
#RESLIST[1]="200 OK"
RESLIST[1]="ACTIVE"
```

**Step 9** Enter the file with vi mode.

```bash
vi types.db
```

**Step 10** Change the lines

```bash
#database_availability    session_a_db:GAUGE:0:1 session_b_db:GAUGE:0:1
quota_db:GAUGE:0:1 report_db:GAUGE:0:1 usum_db:GAUGE:0:1
```

to

```bash
database_availability    session_a_db:GAUGE:0:1 quota_db:GAUGE:0:1 report_db:GAUGE:0:1
usum_db:GAUGE:0:1
```

**Step 11** This step should be performed only if you have one QNS process per CPS VM i.e., in QPS-B and QPS-C we have only one QNS process per Virtual machine.

**Step 12** Change the line

```bash
#qns_availability       qns_a:GAUGE:0:1 qns_b:GAUGE:0:1 qns_admin:GAUGE:0:1
```

to

```bash
qns_availability       qns_a:GAUGE:0:1 qns_admin:GAUGE:0:1
```
Step 13 Enter the mongo DB and remove the qns availability records. This step should be performed only if you have one QNS process per CPS VM.

```
[root@pcrfclient01 collectd.d]# mongo --port 27017
MongoDB shell version: 2.4.6
connecting to: 127.0.0.1:27017/test
> use collectd
switched to db collectd
> db.exec.remove({"type" : "qns_availability"})
> exit
```

Step 14 Restart collectd process.

```
/etc/init.d/collectd restart
```

Step 15 Go to Control center and check for system health under Monitoring tab wait for 60 seconds (1 minute) and click Refresh.

The result of above steps is:

1. To monitor CPS that is having only one QNS process per CPS VM.
2. Make sure that Control center sends the health check only for the Virtual Machine hosted in CPS setup and not for all the hosts present under /etc/hosts.

Zabbix is Using More Space in GR Setup on Site 1 and Site 2

Call model:

- 8k Make break TPS across 4 GGSN across both GR sites
- 30M subscribers in SPR.
- 3.4M static active PDP across Both GR sites

Details of issue:

With the above call model running overnight, `/var/lib/mysql` dir going in GB's on pcrfclient01 of both GR Site 1 and Site 2.

Site 1 pcrfclient01

```
=================
Disk usage on pcrfclient01...[WARN]
```

Disk usage is above warning threshold (90%) on pcrfclient01.

Results of: `ssh qns@pcrfclient01 -x 'df -hP'`

```
-----------------------------------------------
Frequently Encountered Troubles

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00 28G 4.5G 22G 18% /
/dev/mapper/VolGroup00-LogVol02 18G 15G 1.5G 92% /var
/dev/sda1 99M 59M 36M 62% /boot
tmpfs 7.8G 0 7.8G 0% /dev/shm

[root@pcrfclient01 lib]# du -sH * | grep sql
du: WARNING: use --si, not -H; the meaning of the -H option will soon change to be the same as that of --dereference-args (-D)
6.5G mysql

Site 2 pcrfclient01

Disk usage on pcrfclient01...

Disk usage is above warning threshold (90%) on pcrfclient01.

Results of: ssh qns@pcrfclient01 -x 'df -hP'

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00 29G 4.3G 23G 16% /
/dev/mapper/VolGroup00-LogVol02 18G 16G 1.1G 94% /var
/dev/sda1 99M 59M 36M 62% /boot
tmpfs 7.8G 0 7.8G 0% /dev/shm

[root@pcrfclient01 lib]# du -sH * | grep sql
du: WARNING: use --si, not -H; the meaning of the -H option will soon change to be the same as that of --dereference-args (-D)
6.7G mysql

[root@pcrfclient01 lib]#
Attached debug info logs for both sites

Setup Details:

Site 1 Pcrfclient01 IP:X.X.X.X
Site 2 Pcrfclient01 IP:X.X.X.X

Solution:
Create the partition of the zabbix DB for all history related tables. These partitions are automatically deleted if they are older than 3 days and new partition are created. The script which initializes Zabbix DB to create partition of history tables is executed manually. Before execution of the script:

Step 1  Take a backup of the current DB using:
         
         mysql -u root -p --opt --all-databases > /var/tmp/backup_name.sql

Step 2  Stop mysql service.
         service mysql stop
         mv ibdata1 /var/tmp/
         rm zabbix ib_logfile*

Step 3  Add below lines in /etc/my.cnf file. If the file does not exist, then create it and add below entry to it.
         [mysqld]
         innodb_file_per_table

Step 4  Start mysql service.
         service mysql start

Step 5  Login to mysql using your credentials.
         For example,
         mysql -u<username> -p<password>

Step 6  Restore DB from backup.
         \./var/tmp/backup_name.sql

Step 7  Exit from mysql shell.

Step 8  Goto /etc/zabbix/script/partition_db/.

Step 9  ./zabbix_initialize_partition.sh /* command takes long time to complete (depending on size of backup data)*/.

Step 10 To verify whether partition is created or not:
         b. List all history tables with partitions. There should be around 7 partitions for every table.
ls -lrt | grep history

MAC Address Change Fails the License Check

Issue:
After the pcrcfclient01 and pcrcfclient02 Virtual Machines are recreated. If the MAC address is changed, the license file they previously created will not be valid. CPS will not be able to function.

Solution:
Reassign the old MAC address to the new virtual machines. Use the MAC addresses from the previous license file generated from the old VM's MAC address.
The process of reassigning the old MAC address to VM varies for different virtualization technologies. Please refer to corresponding documentation for the process.

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.

![An exception occurred!](image)

No configuration visible in Policy Builder after login

Step 1 Verify the directory /var/broadhop/pb/workspace/<username>/checkout is created and it contains .xmi files.
Step 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.
Chapter 1      Troubleshooting CPS

Frequently Encountered Troubles

Exception Occured During Login

An exception occurred while Getting latest policy data for editing...

Reason:
An exception occurred while Getting latest policy data for editing...

svn: OPTIONS of 'http://pcrfclient01/repos/andsf/config': authorization failed (http://pcrfclient01)
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 6.1, 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 Policy Builder are converted into XMI files, which are added in the SVN repository. The XMI files based on the CPS 6.1 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_6_0.sh` can be implemented, which upgrades the policy reporting configuration files (XMI files) to CPS 6.1.

---

**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_6_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 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 Increased**

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:

Step 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
```

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
```

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

**Step 2**

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

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

**Note**

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.

The `sync` command can also be used before running the above command to reduce the number of objects on the system. This can enable even more cached memory to be freed.

For more information about Linux memory management, refer to [http://www.linuxatemyram.com](http://www.linuxatemyram.com) and [http://linux-mm.org/Drop_Caches](http://linux-mm.org/Drop_Caches).

### spr_encryption_update

**Symptom**

When mongo db subscribers are migrated from CPS 5.5.3 to CPS 6.0 or higher version, then `diagnostic.sh` script shows errors on subscriber. In CPS 6.0 and higher version, encryption on password field for subscriber have been incorporated.

**Recommendation**

To overcome issue of `diagnostic.sh` due to encryption of password field, we need to run `spr_encryption_update.sh` script. This script is present on pcrfclient01 at the location `/opt/broadhop/installer/update`.

To run the script, we need to pass two parameter: IP address of primary SPR db and port number.

Primary SPR IP address can be identified by running the following command:

```
$diagnostics.sh --get_replica_status
```
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 db
- `$use spr`
- `$db.subscriber.find({
  
  “credentials_key” : [
  
  {
  
  “network_id_key” : “111111201”
  
  }])`});

Or

- `$db.subscriber.find({“network_id_key” : “886906007135”})`$db.subscriber.find({“network_id_key” : “111111201”})`}

```bash
$cd /opt/broadhop/installer/update

$.spr_encryption_update.sh <ip-address> <port number>
```
SNMP Traps and Key Performance Indicators (KPIs)

This section covers the following topics:

- Full (HA) Setup
- All-in-one (AIO) Setup
- Add Multiple NMS Addresses to Configuration Files
- Traps Generated by CPS
- Components and KPI Values
- FAQs
- Reference Document
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:

```
 service snmpd start
```

**Step 2** Check whether `snmptrapd` is running on LB VMs. If the service is not running then start it by executing the command:

```
 service snmptrapd start
```

**Step 3** On pcrfclient01:

a. 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:

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

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

b. Execute the command `syncconfig.sh` so that the change done in Step a gets synchronized to all VMs.

c. Execute the command `restartall.sh` to restart all qns processes.

Perform the following steps on all pcrfclient VMs:

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 pcrfclient VMs then you need to get the monit rpm and install it in on all 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 pcrfclient VMs and update it on all pcrfclient VMs setup.

f. Restart monit service.
service monit start

Step 4  On 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 is not installed on LB VMs then you need to get the monit rpm and install it on all 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 LB VMs and update it on all 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:

    service snmpd start

    service snmptrapd start

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:

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

Note  server_name details can be found from /etc/broadhop/server file.
Chapter 1    Troubleshooting CPS

SNMP Traps and Key Performance Indicators (KPIs)

Step 3 Execute `restartall.sh` command to restart all qns processes.

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
```

Note If `monit` is not installed on LB VMs then you need to get the `monit` rpm and install it on all LB VMs.

Step 6 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 AIO VM and update it on all AIO VM.

Step 7 Restart monit service.

```
  service monit start
```

Add Multiple NMS Addresses to Configuration Files

Step 1 Login to LB01 VM.

Step 2 Open `/etc/hosts` file.

Step 3 Add new NMS entries as below.

```
<NMS_IP_ADDRESS> <HOST_NAME>
```

For example,

```
10.10.0.1 corporate_nms_ip1
10.10.0.2 corporate_nms_ip2
```

Step 4 Open `/etc/snmp/snmptrapd.conf` file.

Step 5 Add below entries in `snmptrapd.conf` file.

```
# Forward system event (DISMAN) traps to NMS
#
# NOTE: Change IP address at end of lines to match your end NMS trap receiver
```

Note

- Make sure the below entries contain the `HOSTNAME` defined above. For example, below entries contain name as `corporate_nms_ip1`. If hostname defined inside `/etc/hosts` is something different than `corporate_nms_ip1`, then change hostname for all entries and copy the configuration to `snmptrapd.conf` file.

- Add the below configuration entries multiple times if there are multiple NMS addresses defined in `/etc/hosts` file (After changing hostname for each copy).
Chapter 1  Troubleshooting CPS

SNMP Traps and Key Performance Indicators (KPIs)

# traphandle DISMAN-EVENT-MIB::mteTriggerFired
/etc/snmp/scripts/component_trap_convert corporate_nms_ip1
traphandle DISMAN-EVENT-MIB::mteTriggerRising
/etc/snmp/scripts/component_trap_convert corporate_nms_ip1
traphandle DISMAN-EVENT-MIB::mteTriggerFalling
/etc/snmp/scripts/component_trap_convert corporate_nms_ip1
traphandle IF-MIB::linkDown /etc/snmp/scripts/component_trap_convert
corporate_nms_ip1
traphandle IF-MIB::linkUp /etc/snmp/scripts/component_trap_convert
corporate_nms_ip1
#
# Forward (new) BROADHOP traps to NMS
#
# NOTE: Change IP address at end of lines to match your end NMS trap
# receiver
#
forward BROADHOP-NOTIFICATION-MIB::broadhopQNSComponentNotification
corporate_nms_ip1
forward BROADHOP-NOTIFICATION-MIB::broadhopQNSApplicationNotification
corporate_nms_ip1
#
# Forward (old) BROADHOP traps to NMS
#
# NOTE: Change IP address at end of lines to match your end NMS trap
# receiver
#
traphandle BROADHOP-MIB::broadhopNormalAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1
traphandle BROADHOP-MIB::broadhopIndeterminateAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1
traphandle BROADHOP-MIB::broadhopWarningAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1
traphandle BROADHOP-MIB::broadhopMinorAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1
traphandle BROADHOP-MIB::broadhopMajorAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1
traphandle BROADHOP-MIB::broadhopCriticalAlarm
/etc/snmp/scripts/application_trapv1_convert corporate_nms_ip1

Step 6  Execute the following commands:

    service snmptrapd restart
scp /etc/hosts lb02:/etc/hosts
scp /etc/snmp/snmptrapd.conf lb02:/etc/snmp/snmptrapd.conf
ssh lb02 “service snmptrapd restart”

**Note**
If there are more than two LB VMs present on the setup, then execute Step 6 for remaining LBs also.

### Traps Generated by CPS

The following tables describes the various traps generated by CPS and different procedures associated with individual traps to test the traps. For example, when a trap is generated, it is thrown to LBVIP02 (can be on port 162. On LB, process snmptrapd is listening on port 162. When snmptrap sees trap on 162, it logs it in the file `/var/log/snmpd/trap` and re-throws it on corporate_nms_ip on port 162.

This section covers the following topics:

- Component Notifications
- Application Notifications

#### Component Notifications

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Procedure to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Full: This alarm gets generated for following file system: 1. / 2. /var 3. /home 4. /boot 5. /opt</td>
<td><strong>Step 1</strong> In <code>/etc/snmp/snmpd.conf</code>, set “disk / 90%”. (So when disk remaining is 90% ie. Disk occupied is 10%, alarm is generated.)  <strong>Step 2</strong> service snmpd restart  <strong>Step 3</strong> Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.  <strong>Step 4</strong> trap have messages like :dskErrorMsg.1 = STRING: /: less than 90% free (= 100%)</td>
</tr>
<tr>
<td>Disk Full Clear: This alarm gets generated for following file system: 1. / 2. /var 3. /home 4. /boot 5. /opt</td>
<td><strong>Step 1</strong> In <code>/etc/snmp/snmpd.conf</code>, set &quot;disk / X%&quot;. (X should just less than actual remaining space. For example, if drive / is 25% full, put 74% as value of X).  <strong>Step 2</strong> service snmpd restart  <strong>Step 3</strong> Now dump a big file which consumes at least 2-3% space on drive /. This generates diskful alarm first.  <strong>Step 4</strong> Then delete this file. This generates clear alarm.  <strong>Step 5</strong> Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Procedure to Test</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Load Average of local system       | **Step 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.)  
|                                    | **Step 2** service snmpd restart                                                                                                                      |
|                                    | **Step 3** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active lb.                                                            |
|                                    | **Step 4** trap have message like 1 min Load Average too high (≈ 1.41)                                                                                 |
| Load Average Clear of local system | **Step 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.)  
|                                    | **Step 2** service snmpd restart                                                                                                                      |
|                                    | **Step 3** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active lb.                                                            |
|                                    | **Step 4** trap have message like 1 min Load Average too high (≈ 1.41)                                                                                 |
|                                    | **Step 5** Now wait till load comes below 1 % OR write a script which runs in infinite loop and create some load on CPU. Killing this script reduces the load and generates clear trap. |
| Low Swap memory alarm              | **Step 1** `swapoff -a /*` - This command makes the swap off. You can see swap as 0 in `top` command output. The trap should get generated if swap is 0 in output of `top`/*.  
|                                    | **Step 2** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active lb.                                                            |
|                                    | **Step 3** trap have message mentioning swap.                                                                                                         |
| Low Swap memory clear              | **Step 1** `swapon -a /*` - This will make swap to on. The `top` command output will show the swap memory size. The clear trap gets generated if swap alarms gets generated earlier/*.  
|                                    | **Step 2** Verify the generated alarm on NMS server and `/var/log/snmp/trap` of active lb.                                                            |
|                                    | **Step 3** trap have message mentioning swap.                                                                                                         |
### Link Down Alarm
This alarm gets generated for all physical interface attached to the system.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>ifconfig &lt;interface_name&gt; down</code> (For example, <code>ifconfig eth2 down</code>)</td>
</tr>
<tr>
<td>2</td>
<td>within 1 minute interval interface down trap gets generated</td>
</tr>
<tr>
<td>3</td>
<td>Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.</td>
</tr>
</tbody>
</table>

### Link Up Alarm
This alarm gets generated for all physical interface attached to the system.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>ifconfig &lt;interface_name&gt; up</code> (For example, <code>ifconfig eth2 up</code>)</td>
</tr>
<tr>
<td>2</td>
<td>within 1 minute interval interface up trap gets generated</td>
</tr>
<tr>
<td>3</td>
<td>Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.</td>
</tr>
</tbody>
</table>

### Low Memory Alert Alarm

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In output of <code>top</code> command find out the current free RAM memory value.</td>
</tr>
<tr>
<td>2</td>
<td>Update <code>snmpd.conf</code> file monitor entry for Low Memory Alert to have value just less than the current free RAM memory value.</td>
</tr>
<tr>
<td>3</td>
<td><code>service snmpd restart</code></td>
</tr>
<tr>
<td>4</td>
<td>Do some activity on VM such as running some command or starting some process so that free RAM value goes below the configured value.</td>
</tr>
<tr>
<td>5</td>
<td>The low memory alert alarm gets generated within a minute interval.</td>
</tr>
<tr>
<td>6</td>
<td>Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.</td>
</tr>
</tbody>
</table>

### Low Memory Clear Alarm

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In output of <code>top</code> command find out the current free RAM memory value.</td>
</tr>
<tr>
<td>2</td>
<td>Update <code>snmpd.conf</code> file monitor entry for Low Memory Clear to have value just more than the current free RAM memory value.</td>
</tr>
<tr>
<td>3</td>
<td><code>service snmpd restart</code></td>
</tr>
<tr>
<td>4</td>
<td>Kill some processes on VM so that free RAM memory value is more than the configured value.</td>
</tr>
<tr>
<td>5</td>
<td>The low memory clear alarm gets generated within a minute interval.</td>
</tr>
<tr>
<td>6</td>
<td>Verify the generated alarm on NMS server and <code>/var/log/snmp/trap</code> of active lb.</td>
</tr>
</tbody>
</table>
### Application Notifications

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Procedure to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Usage Threshold Exceeded</td>
<td><strong>Step 1</strong> Create the license having small no. of Usage Threshold limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Install the above created license on setup.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> restart all qns processes</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Send multiple request so that it crosses the threshold limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 5</strong> The License Usage Threshold Exceeded alarm gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 6</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Memcached ConnectError</td>
<td><strong>Step 1</strong> Kill the memcached process running on active LB.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Within 5 minutes of interval Memcached Connect Error trap gets generated from QNS VMs.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>ApplicationStartError</td>
<td><strong>Step 1</strong> Rename any of the dependent jar files from /opt/broadhop/qns-1/plugins dir e.g. rename com.broadhop.spr.dao jar file.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> restart qns process</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Within 5 minute of interval ApplicationStartError Trap gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>LicensedSessionCreation</td>
<td><strong>Step 1</strong> Create the license having small no. of Session Usage Threshold limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Install the above created license on setup.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> restart all qns processes</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Send multiple request so that it crosses session threshold limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 5</strong> For the next request after the limit over LicenseSessionCreation alarm gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 6</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Procedure to Test</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| InvalidLicense          | **Step 1** Copy the license of pcrfclient02 on pcrfclient01 or create a license for pcrfclient02 and install it on pcrfclient01.  
|                         | **Step 2** restart lmgrd service                                                  |
|                         | **Step 3** restart qns process                                                    |
|                         | **Step 4** Within 5 minutes of interval the License invalid trap gets generated.  |
|                         | **Step 5** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| PolicyConfiguration     | **Step 1** Configure some wrong policy in PB Policies tab.                        |
|                         | **Step 2** Publish the configuration.                                              |
|                         | **Step 3** restartall.sh                                                          |
|                         | **Step 4** Last policy configuration failed with the following message:xxx trap gets generated. |
|                         | **Step 5** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| SessionManagerUnavailable| **Step 1** Make any sessionmgr down using command such as etc/init.d/sessionmgr-27017. |
|                         | **Step 2** Within 5 minute of interval the SessionManagerUnavailable trap gets generated. |
|                         | **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| PoliciesNotConfigured   | **Step 1** Create the invalid blueprint (java code having syntax error) in PB under Policies tab. |
|                         | **Step 2** Assign the created blueprint to some policies.                         |
|                         | **Step 3** Publish the configuration.                                              |
|                         | **Step 4** restart all qns process                                                 |
|                         | **Step 5** PoliciesNotConfigured trap gets generated.                             |
|                         | **Step 6** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| DiameterPeerDown        | **Step 1** Make a seagull diameter call.                                           |
|                         | **Step 2** After seagull script terminate it generates the diameter peer down trap. |
|                         | **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
## Alarm Name | Procedure to Test
---|---
**HA_Failover**<br>Step 1: Cat /etc/broadhop/mongoConfig.cfg.<br>Step 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.<br>Step 3: Shutdown the primary instance of sessionmgr.<br>Step 4: Within 1 minute of interval HA Failover trap gets generated.<br>Step 5: Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.<

**Geo_Failover**<br>Step 1: Cat /etc/broadhop/mongoConfig.cfg.<br>Step 2: There should be primary and secondary member set for each replica set. Found the current active sessionmgr instance of a replica set using rs.isMaster().primary.<br>Step 3: Shutdown all sessionmgr instances of active sessionmgr instance set.<br>Step 4: Within 1 minute of interval Geo Failover trap gets generated.<br>Step 5: Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.<

**All_replica_of_DB_down**<br>Step 1: Get all members of replica set from /etc/broadhop/mongoconfig.cfg.<br>Step 2: Go to each sessionMgr of a replica set and stop the sessionmgr service or shutdown the sessionmgr VM.<br>Step 3: Within 5 minutes of interval All replicas of DB Down trap gets generated.<br>Step 4: Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.<

**No_Primary_member_found**<br>Step 1: run diagnostics.sg -get_replica_status.<br>Step 2: Choose any set which has arbiter and primary and secondary db member.<br>Step 3: Shutdown Arbiter VM.<br>Step 4: Shutdown Primary Sessionmgr VM.<br>Step 5: Within 5 minute of interval No primary Member found trap gets generated.<br>Step 6: Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.
<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Procedure to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary DB Down</td>
<td><strong>Step 1</strong> Cat /etc/broadhop/mongoConfig.cfg.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Shutdown any of the sessionmgr VM listed in the configuration as db member of replica set.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Within 5 minute of interval Secondary DB down trap gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Arbiter Down</td>
<td><strong>Step 1</strong> Cat /etc/broadhop/mongoConfig.cfg.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Shutdown any of the arbiter VM listed in the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Within 5 minute of interval Arbiter down trap gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Config Server is Down</td>
<td><strong>Step 1</strong> Cat /etc/broadhop/mongoConfig.cfg.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Shutdown any of the config server VM listed in the configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Within 5 minute of interval config server down trap gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Site Down</td>
<td>Assumption: Configured the same NMS address on both sites.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 1</strong> Make lbvip01 and lbsvip01 down of one site using command ifconfig eth1:0 down on active lb and ifconfig eth1:0 down on standby lb of same site.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Within 5 minutes of interval Site Down trap gets generated from other site.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> On configured NMS server the trap gets received and tail -f /var/log/snmp/trap on active LB of other site will log the site down generated trap.</td>
</tr>
<tr>
<td>VM Down</td>
<td><strong>Step 1</strong> cat /etc/hosts file on lb VM.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Make any one of the VM down listed under /etc/hosts.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> Within 5 minutes of interval VM down trap gets generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Procedure to Test</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| QPS Process Down       | **Step 1** Make qns process down using command service qns stop.  
                       | **Step 2** Within 5 minutes of interval qps process down trap gets generated.  
                       | **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| Admin Logged In        | **Step 1** Create a new telnet session for any VM and login with root user on it.  
                       | **Step 2** Within 1 minute interval Admin User logged in trap gets generated.  
                       | **Step 3** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| VirtualInterfaceError  | **Step 1** Login to active lb VM.  
                       | **Step 2** Run command ifconfig eth1:0 down  
                       | **Step 3** VirtualInterfaceError trap with the interface name gets generated.  
                       | **Step 4** You can see this trap on NMS server. |
| Developer Mode License traps | **Step 1** Use developer mode in qns.conf file.  
                          | **Step 2** restart qns process  
                          | **Step 3** Within 5 minutes interval the Developer Mode License gets generated.  
                          | **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
| Can't create sessions due to errors. | **Step 1** Install invalid license on the setup.  
                          | **Step 2** Send session creation request such as diameter/radius call request.  
                          | **Step 3** Session creation not allowed, trap gets generated.  
                          | **Step 4** Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb. |
### Components and KPI Values

The following table describes component and KPI values and procedures to get them.

This section covers the following topics:

- Component Values
- KPI Values

#### Component Values

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Procedure to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZeroMQConnectionError</td>
<td><strong>Step 1</strong> Start QNS.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Start Messaging Load (CCR-I, CCR-U, CCR-T) scenario at high TPS.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> The trap will be seen if message sending over socket between LB and QNS fails (Due to socket send errors). For subsequent failures there is no further trap raised.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
<tr>
<td>ZeroMQConnectionError(clear)</td>
<td><strong>Step 1</strong> This trap will be sent when message send on socket succeeds after the prior failure.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong> Verify the generated alarm on NMS server and /var/log/snmp/trap of active lb.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component Values</th>
<th>Procedure to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>LB01 snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB &lt;lbvip01&gt; BROADHOP-QNS-MIB::broadhopProductsQNSComponents53LB01</td>
<td>List all(14)component scalar parameter values of LB01</td>
</tr>
<tr>
<td>LB02 snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB &lt;lbvip01&gt; BROADHOP-QNS-MIB::broadhopProductsQNSComponents53LB02</td>
<td>List all(14)component scalar parameter values of LB02</td>
</tr>
</tbody>
</table>
KPI Values

<table>
<thead>
<tr>
<th>KPI Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>LB01/LB02</td>
</tr>
</tbody>
</table>

```
snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB <lbvip01>
BROADHOP-QNS-MIB::broadhopProductsQNSKPI53LB(01/02)
```

List all KPIs value of LB, if all values are 0 then

**ExternalCurrentSession**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open another terminal.</td>
</tr>
<tr>
<td>Step 2</td>
<td>telent lbvip01 8080</td>
</tr>
<tr>
<td>Step 3</td>
<td>On previous terminal run the above snmpwalk command again.</td>
</tr>
<tr>
<td>Step 4</td>
<td>This time it will display the externalCurrentSession KPIs value to be 1.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat the process with more telnet session open on lbvip01 8080 port</td>
</tr>
</tbody>
</table>

**InternalCurrentSession**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open another terminal.</td>
</tr>
<tr>
<td>Step 2</td>
<td>telent lbvip02 8080</td>
</tr>
<tr>
<td>Step 3</td>
<td>On previous terminal run the above snmpwalk command again.</td>
</tr>
<tr>
<td>Step 4</td>
<td>This time it will display the internalCurrentSession KPIs value to be 1.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat the process with more telnet session open on lbvip01 8080 port</td>
</tr>
</tbody>
</table>
### KPI Values

<table>
<thead>
<tr>
<th>PortalLB01/PortalLB02</th>
<th>snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB &lt;lbvip01&gt; BROADHOP-QNS-MIB::broadhopProductsQNSKPI53PortalLB(01/02)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>List all KPIs value of PortalLB, if all values are 0 then</td>
</tr>
<tr>
<td></td>
<td><strong>ExternalCurrentSession</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>Open another terminal.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>telent sslvip01 80</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>On previous terminal run the above snmpwalk command again.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>This time it will display the externalCurrentSession KPIs value to be 1.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Repeat the process with more telnet session open on sslvip01 80 port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QNS01/QNS02/QNS03/QNS04</th>
<th>snmpwalk -v 2c -c broadhop -m +BROADHOP-MIB:BROADHOP-QNS-MIB &lt;lbvip01&gt; BROADHOP-QNS-MIB::broadhopProductsQNSKPI53QNS(01/02/03/04)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>List all KPIs value of QNS VM</td>
</tr>
<tr>
<td></td>
<td>For example, the output will be displayed as below:</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04PolicyCount = STRING: 1</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04PolicyCount.0 = STRING: 1</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04QueueSize = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04QueueSize.0 = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04FailedEnqueueCount = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04FailedEnqueueCount.0 = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04ErrorCount = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04ErrorCount.0 = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04SessionCount = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04SessionCount.0 = STRING: 0</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04FreeMemory = STRING: 3943912704</td>
</tr>
<tr>
<td></td>
<td>BROADHOP-QNS-MIB::kpi53QNS04FreeMemory.0 = STRING: 3943912704</td>
</tr>
</tbody>
</table>
FAQs

Q. Where to check if traps are getting generated or not?
A. On active 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 pcrfclient or QNS VMs but not getting logged to /var/log/snmp/trap and not appear on NMS receiver?
A. Check on Active 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 Question.
   3. Check if NMS IP is accessible from LB VMs. Using command such as ping <nms_ip>

Q. DB 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.

Reference Document

For more information on SNMP traps and KPIs, refer to CPS 6.1 Alarming and SNMP Guide.
Check Subscriber Access

This chapter covers the following sections:

- Checking 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 the 00.testAccessRequest.sh in /opt/broadhop/installer/isg/troubleshooting directory on the CPS server.

To configure the subscriber used, edit /opt/broadhop/installer/isg/troubleshooting/config.ini

---

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 displays:
Testing Subscriber Access with soapUI

This procedure tests end subscriber access to your system.

---

**Step 1**
Download soapUI from here: [http://www.soapui.org/](http://www.soapui.org/)
You only need the freeware version (not soapUI Pro).

**Step 2**
Launch soapUI.

**Step 3**
Right click on projects, select New soapUI Project from the drop-down menu.

**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:
Step 5  In the tree click Demo > SubscriberBinding > GetSubscriber > Request 1, as shown in the figure on the right.
**Step 6**  Edit the End Point by selecting from the drop down: [edit current...]. Enter the appropriate IP.

**Step 7**  In the XML file:
Check Subscriber Access

1. Replace the ? in `<typ:networkId>?</typ:networkId>` with the appropriate credential or network Id.

**Step 8**  Click on the green arrow (underneath "Request 1")

**Step 9**  Check the resulting XML output. Pay special attention to the relevant subscriber information:
Chapter 2      Check Subscriber Access

Checking Access

Testing for ISG Functionality and Connectivity with test aaa Scripts

The four scripts described here test ISG functionality and connectivity.

Step 1       Connect to the ISG with username and password.
Step 2       Type the 'en' command.
Step 3       Enter 'cisco' as the password to the en command.

From here use the four "test aaa" scripts to verify correct ISG functionality and connectivity. No IP addresses or any other arguments are needed.

test aaa group QNS_AAA PBHK_SERVICE servicecisco legacy
test aaa group QNS_AAA L4REDIRECT_SERVICE servicecisco legacy
test aaa group QNS_AAA OPENGARDEN_SERVICE servicecisco legacy
test aaa group QNS_AAA BroadHop BroadHop legacy
If functioning correctly, each script returns this message:

```plaintext
Attempting authentication test to server-group QNS_AAA using radius
User was successfully authenticated.
```
TCP Dumps

Revised: April 28, 2015,
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.

This chapter covers the following sections:
- TCPDUMP Command
- Specific Traffic Types

TCPDUMP Command

```
tcpdump -i any -s 0 port XXXX
```

where XXXX is the port number you are interested in, RADIUS ports are used for Default examples unless otherwise specified.

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 Policy Builder. One must modify these examples to use the appropriate ports that have been specified in Policy Builder if the default/typical values have been changed.

**Capture RADIUS Traffic**

tcpdump -i any -s 0 port 1812 or 1813

Port 1812 is the default for Authorization traffic.
Port 1813 is the default for Accounting traffic.

**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 "Portal vip management"
lbvipXX 80 "Subversion vip external"
lbvipXX 8080 "QNS/Unified API VIP"
lbvipXX 11211 "Memcache vip internal"
lbvipXX 7070 "Policy Builder VIP"
lbvipXX 8082 "Portal Admin VIP"
qnsXX 9091 "QNS admin port"
Call Flows

Revised: April 28, 2015,

The following call flow diagrams are given to help you troubleshoot and understand CPS deployment.

- One-click Call Flow
- User/Password Login Call Flow
- Data-limited Voucher Call Flow
- Time-limited Voucher Call Flow
- WISPr Call Flow
- EAP-TTLS Call Flow
- Service Selection Call Flow
- MAC TAL Call Flow
- Tiered Services Call Flow
- SP WiFi-4.0 Call Flows
One-click Call Flow

OneClick Call Flow

Subscriber → ISG → I Portal → QPS

http://google.com

L4 redirect to portal on port 80

Portal queries

Portal must have access to the original (non nat) IP address and remote port on the user session's Port Bundle Host Key

Completed on port 6000

CoA Get Completeld on port 1700

CoA ACK

Returned IP/MAC/Location

User agent filtering

Portal prompts user for credentials

One Click User/Password login request on port 80

Setup Subscriber Profile API on port 9999

CoA Account Login on port 1700

ISG_IP = remote address
ISG_PORT = remote port plus username and password
(continued)

Contains the service assigned 512K-DOWN

Contains the ACLs and the Accounting List

User Access Request on port 1812

Access Accept

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

302 to original URL

Service Accounting Start on port 1813

Accounting Response

Username, password, acct session id, nas ip, framed ip all needed

Username, service name, acct session id, nas ip, framed ip all needed

Service name as UserName, password, nas ip all needed

Username, serv name, acct session id, parser acct session id, nas ip, framed ip all needed
User/Password Login Call Flow

1. Subscriber
2. ISG
3. Portal
4. QPS

--->

http://google.com

L4 redirect to portal on port 80

Portal must have the original (non nat) IP address and remote port on the Port Bundle Host Key

Portal queries completed on port 8080

Uses Remote IP and Remote Port

CoA Get Completed on port 1700

CoA ACK

Returned IP/MAC/Location

User prompts user for credentials

User/Password login request on port 80

Setup Subscriber Profile API on port 8080

CoA Account Login on port 1700

User Access Request on port 1812

Contains the service assigned
512K-DOWN

Access Accept

ISG_IP = remote address
ISG_PORT = remote port plus username and password
Username, password, acct session id, nas framed ip all needed
User/Password Login Call Flow

Contains the service assigned 512K-DOWN

Contains the Traffic Class ACLs and the Accounting List

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

Username, service name, acct session id, nas ip, framed ip all needed

Service Accounting Start on port 1813

Accounting Response

302 to original URL

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Data-limited Voucher Call Flow

Subscriber

http://google.com

L4 redirect to portal on port 80

Portal must have access to the original (non nat) IP address and remote port on the user session's Port Bundle Host Key

Portal queries Completesd on port 8080

Uses Remote IP and Remote Port

CoA Get Completesd on port 1700

CoA ACK

Returned IP/MAC/Location

User agent filtering

Portal prompts user for credentials

Voucher/Pin login request on port 80

Setup Subscriber Profile API on port 8080

CoA Account Login on port 1700

User Access Request on port 1812

Contains the service assigned VOUCHER_SERVICE

Access Accept

ISG_IP = remote address
ISG_PORT = remote port plus username and password
Username, password, acct session id, nas ip, framed ip all needed
Appendix A  Call Flows

Data-limited Voucher Call Flow

(continued)

Contains the Traffic Class ACLs and the Prepaid Config

Contains the QV attribute

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

Prepaid Access Request on port 1814

Access Accept

Service Accounting Start on port 1815

Accounting Response

Username, service name, acct session id, nas ip, framed ip all needed

Service name as UserName, password, nas ip all needed

User name, Service name, password, acct session id, nas ip framed ip all needed

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed

Volume is used.
(continued)

Contains the QV attribute

User name, Service name, password, acct session id, nas ip framed ip all needed

All Volume Balance is used.

User name, Service name, password, acct session id, nas ip framed ip all needed

Prepaid Access Request on port 1814

Access Accept

Prepaid Access Request on port 1814

Access Reject

Service Accounting Stop on port 1815

Accounting Response

The call flow starts over with the portal redirection.

http://google.com
L4 redirect to portal on port 80

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Time-limited Voucher Call Flow

1. **Subscriber**
   - http://google.com

2. **ISG**
   - L4 redirect to portal on port 80
   - Portal queries
     - Completed on port 8080
     - Portal must have access to the original (non nat) IP address and remote port on the user session's Port Bundle Host Key

3. **Portal**
   - Portal queries
     - Completed on port 8080
   - CoA Get Completed on port 1700
   - CoA ACK
   - Returned IP/MA/CJ Location
   - User agent filtering
   - Portal prompts user for credentials
   - One Click User/Password login request on port 80
   - Setup Subscriber Profile API on port 8080
   - CoA Account Login on port 1700
   - User Access Request on port 1812

4. **QPS**
   - Access Accept
   - Uses Remote IP and Remote Port

Additional Notes:
- ISG_IP = remote address
- ISG_PORT = remote port plus username and password
- Username, password, acct session id, nas ip, framed ip all needed

Contains the service assigned 512K-DOWN and Session Timeout of the duration
(continued)

Contains the Traffic Class ACLs and the Accounting List

302 to original URL

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

Username, service name, acct session id, nas ip, framed ip all needed

Service name as UserName, password, nas ip all needed

After session timeout.

Service Accounting Start on port 1813

Accounting Response

Service Accounting Stop on port 1813

Accounting Response

Session Accounting Stop on port 1813

Accounting Response

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed

Username, service name, acct session id, nas ip, framed ip all needed
WISPr Call Flow

Subscriber

WISPr Client tries www site (e.g. www.myprovider.com)

L4 redirect to portal on port 80

Portal must have access to the original (non nat) IP address and remote port on the user session's Port Bundle Host Key

Portal queries
Completed on port 8080

CoA Get Completed on port 1700

CoA ACK

Returned IP/MAC/Location

User agent filtering

HTTP Response with WISPr XML embedded

User/Password login request on over HTTPS on port 8443

Setup Subscriber Profile API on port 8080

CoA Account Login on port 1700

ISG_IP = remote address
ISG_PORT = remote port plus username and password

QPS

Uses Remote IP and Remote Port

Portal

WISPr Call Flow
(continued)

Contains the service assigned 512K-DOWN

User Access Request on port 1812

Access Accept

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

200 Response to WISPr client

Service Accounting Start on port 1813

Accounting Response

Username, password, acct session id, nas ip, framed ip all needed

Username, service name, acct session id, nas ip, framed ip all needed

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
EAP-TTLS Call Flow

- Subscriber
  - Associate
  - EAP Request Identity
  - EAP Response Identity
  - EAP Request TLS Exchange
  - EAP Response TLS Exchange
  - EAP Response Identity (inner)
- W-CAP
- ISG
- Portal
- QPS

- EAP Response Identity on port 1812
- EAP Request TLS Exchange
- EAP Response TLS Exchange on port 1812
- EAP Request Identity (inner)
- Access-Request on port 1812
- Access-Accept
(continued)

http://google.com on port 80

Contains the service assigned 512K-DOWN

MAC Access Request on port 1812

Access Accept

MAC as Username, password, acct session id, nas ip framed ip all needed
Service Selection Call Flow

Subscriber navigates to the Portal directly. Portal must have access to the original (non nat) IP address and remote port on the user session’s Port Bundle Host Key

http://bhportal.operator.com

Subscriber

ISG

Portal

QPS

Execute Action API on port 8080

CoA Get Completed on port 1700

CoA ACK

Returned Location/Subscriber/Session

Displays service options

Change Service request on port 80

CoA Start/Stop service on port 1700

Session Accounting Start on port 1813

Accounting Response

Uses Remote IP and Remote Port, Action

ISG_IP = remote address
ISG_PORT = remote port plus action and service

Username, NEW service name, acct session id, nas ip, framed ip all needed
Service Selection Call Flow (continued)

- Session Accounting Stop on port 1813
- Accounting Response
- CoA ACK
- Display New Service
- Username, OLD service name, acct session id, nas ip, framed ip all needed
- API Success
MAC TAL Call Flow

Subscriber

ISG

Portal

QPS

http://google.com

MAC Access Request on port 1812

Access Reject

Portal must have access to the original (non-nat) IP address and remote port on the user session's Port Bundle Host Key.

Portal queries Completed on port 8080

CoA Get Completed on port 1700

CoA ACK

Returned IP/MAC Location

User prompts user for credentials

User/Password login request on port 80

Setup Subscriber Profile API on port 8080

CoA Account Login on port 1700

MAC as Username, password, acct session id, nas ip, framed ip all needed

Uses Remote IP and Remote Port

ISG_IP = remote address
ISG_PORT = remote port plus username and password
MAC TAL Call Flow (continued)

Contains the service assigned 512K-DOWN

User Access Request on port 1812

Access Accept

QNS stores MAC as credential in Quantum USuM.

Session Accounting Start on port 1813

Accounting Response

CoA ACK (or NACK)

Service Definition Access Request on port 1812

Access Accept

API Success

302 to original URL

Service Accounting Start on port 1813

Accounting Response

ISG CLI to clear the session

Username, password, acct session id, nas ip, framed ip all needed

Username, service name, acct session id, nas ip, framed ip all needed

Service name as UserName, password, nas ip all needed

Username, service name, acct session id, parent acct session id, nas ip, framed ip all needed
Tiered Services Call Flow

Subscriber

http://google.com

L4 redirect to portal on port 80

Portal

Portal must have access to the original (non nat) IP address and remote port on the user session’s Port Bundle Host Key

Portal queries

Completed on port 8000

Uses Remote IP and Remote Port

CoA Get Completed on port 1700

CoA ACK

Returned IP/MAC/Location

User agent filtering

Portal prompts user for credentials

User/Password login request on port 80

Setup Subscriber Profile API on port rAAA

Contains the service assigned 2M-UP-DOWN

CoA Account Login on port 1700

User Access Request on port 1812

Access Accept

ISG_IP = remote address
ISG_PORT = remote port plus username and password
Username, password, acct session id, nas ip, framed ip all needed
SP WiFi-4.0 Call Flows

Following are the call flows within the CPS system based on the requests received from the network device and the presence of the subscriber information in SPR profile.
Authentication Sequence in WLC Network Device Manager
Authentication Sequence for EAP Requests
Authentication Sequence in iWAG Network Device Manager
MAG Coupled Web Based Authentication

MAG coupled Web based authentication entails that the unauthenticated client will be assigned a temporary IP address. This temporary IP address is used as the source address by the UE while accessing the web portal. After successful authentication, the client is forced to reassociate and that will cause the client to go through the IP address assignment phase again. At this stage since the client is already authenticated, the LMA will assign the IP address for the client.