Clearing Procedures

Component Notifications

The following table provides the information related to clearing procedures for component notifications:

Table 1: Component Notifications - Clearing Procedures

Notification Name	Clearing Procedure
DiskFull	**1.** Login to VM on which the alarm has generated. **2.** Check the disk space for the file system on which alarm has generated. `df -k` **3.** Check what all files are using large disk space on file system and delete some unnecessary files to make free space on disk so that the alarm gets cleared. **4.** After removing some files if the size of disk is still more than the configured threshold value and you are not able to remove any more files then consider the option of adding more disk to the VM(s) or contact your Cisco technical representative to look into the issue.

Notification Name	Clearing Procedure

LowSwap	This alarm gets generated whenever available swap memory on the VM is lower than the configure threshold value.
	1. Login to VM for which alarms has generated.
	2. Check the threshold value configured for swap memory.
	`vi /etc/snmp/snmpd.conf`
	Search for the word “swap” in `snmpd.conf` file.
	3. You can check the available free swap memory on the VM by executing the following command:
	`free -m`
	If the available free swap memory is lower than the threshold value then check for the process which takes lots of swap memory by executing the following command:
	For file in `/proc/*/status`; do
	`awk '/VmSwap|Name/{printf $2 " " $3}END{ print ""}' $file; done | sort -k 2 -n -r | less`
	4. Get the output of above command and contact your Cisco technical representative to look into the issue.

HighLoad	This alarm gets generated for load average of 1, 5,15 minutes, whenever load average of the system is more than the configure threshold value the alarm gets generated.
	1. Login to VM for which the alarm has generated.
	2. Check the configure threshold value for the load average in `/etc/snmp/snmpd.conf` file.
	`vi /etc/snmp/snmpd.conf`
	Search for the word “load” in `snmpd.conf` file.
	3. Check the current load average on the system by executing top command.
	4. If the found load average is higher than the configured threshold value, then execute the following command to get the process list currently using CPU.
	`ps aux | sort -rk 3,3 | head -n 6`
	and contact your Cisco technical representative to look into the issue.

Notification Name	Clearing Procedure

LinkDown	This alarm gets generated for all physical interface attached to the system.
	1. Login to VM from where the trap has generated.
	2. Check the status of interface by executing `ifconfig` command.
	3. If the interface found is Down then bring it Up by executing the following command:
	`ifconfig <inf_name> up`
	`service network restart`
	4. If the interface is still not Up, check for IP address assigned to it and errors if thrown any.
	5. Get the solution for the error found in above steps and restart the network service.
	6. If the problem still persist contact your Cisco technical representative to look into the issue.

LowMemory	This alarm gets generated whenever allocated RAM on the VM is higher than the configure higher threshold value.
	1. Login to VM for which alarms has generated.
	2. Check the higher and lower threshold value configured for memory:
	`vi /etc/facter/facts.d/qps_facts.txt`
	Search for the following text:
	• free_mem_per_alert
	• free_mem_per_clear
	3. You can check the available free memory on the VM by executing the following command:
	`free -m`
	If the available free memory is lower than the clear threshold value then check for the process which takes lots of memory in top command output.
	4. Get the output of the following command:
	`ps -eo pmem,pcpu,vsize,pid,cmd | sort -k 1 -nr | head -5`
	and contact your Cisco technical representative to look into the issue.

Notification Name	Clearing Procedure

ProcessDown	This alarm is generated when the corosync process is stopped or fails.
	1. Login to the Policy Director (load balancer) VM from which the alarm has generated.
	2. Check the status of corosync process by executing the following command:
	`monit status corosync`
	3. If status is Down then start the process by executing the following command:
	`monit start corosync`

HIGH CPU USAGE Alert	This trap is generated whenever CPU usage on the VM is more than the higher threshold value.
	1. Login to VM for which the trap has generated.
	2. Check the higher and lower threshold value configured for CPU.
	`vi /etc/facter/facts.d/qps_facts.txt`
	Search for the following text:
	• cpu_usage_alert_threshold
	• cpu_usage_clear_threshold
	3. The CPU usage is calculated as a sum of 9th column value of top command output/no. of vCPU present on the VM.
	If the CPU usage is more than the clear threshold value then check for the process which takes lots of CPU cycle from the top command output.
	4. Get the output of the following command:
	`ps aux | sort -rk 3,3 | head -n 6`
	and contact your Cisco technical representative to look into the issue.

Critical File Operation Alert	This trap is generated when critical files configured in `CriticalFiles.csv` on VMware and `critFileMonConfig:` section in OpenStack gets modified. Event ID: 7400; Sub-event ID: 7403 This is a notification alarm so clearing procedure is not required.

Application Notifications

The following section provides the information related to clearing procedures for application notifications:

License

- LMGRD related:

- **License Usage Threshold Exceeded**: This alarm is generated when the current number of session usage exceeds the **License Usage Threshold Percentage** value configured in the Policy Builder under **Reference Data** > **Fault List**. CPS Alarm/Trap message contains the following key words:

  "InterfaceID=" this keyword indicates the threshold value.

  "severity=" this keyword indicates severity associated to the threshold. The severity value includes:

  - CRITICAL
  - ERROR
  - NOTICE
  - WARNING

  Alarm Code: 1111 - LICENSE_THRESHOLD

  Table 2: License Usage Threshold Exceeded

Possible Cause	Corrective Action
The current number of session usage exceeds the **License Usage Threshold Percentage** value.	Option 1: Purchase a license file having larger licensed session number. Option 2: Adjust **License Usage Threshold Percentage** value configured in Policy Builder.

- **LicenseSessionCreation**: This alarm is generated when CPS does not allow new CPS session to be created.

  Alarm Code: 1104 - ERROR_SESSION_CREATION

  Table 3: LicenseSessionCreation

Possible Cause	Corrective Action
CPS is running in Developer mode and the current number of session usage is > 100.	Clear 'DeveloperMode' flag to annotate the following to make sure the consistency: **1.** Remove the following line from the `/etc/broadhop/qns.conf` file: `-Dcom.broadhop.developer.mode=true.` **2.** Purchase and use a license file. **3.** Restart the Policy Server (QNS) process.

Possible Cause	Corrective Action
CPS "CORE" license related error: • CPS "CORE" is NOT licensed: MOBILE_CORE, FIXED_CORE or SP_CORE license is NOT found. • CPS "CORE" is licensed but the licensed session count is not set. • CPS "CORE" license date already expired. • Current session count is >= CPS "CORE" licensed session count.	1. Add CPS "CORE" license to `/etc/broadhop/license/features.properties` file. 2. Purchase a license containing CPS "CORE". 3. Purchase a license containing CPS "CORE" and larger licensed session count. 4. Make sure that the `license.lic` file contains valid CPS "CORE" expiry date.

- **InvalidLicense**: This alarm is generated when CPS license has an error. The error could be any of the followings:

  1. Core license related: CPS "Core" license error.
  2. Feature license related: CPS "Feature" license error.

  CPS Alarm/Trap message format:

  "InterfaceID=" keyword indicates the license name.

  "license_state=" keywork indicates license state.

  CPS defined license sate includes:

  - UNVERIFIED
  - INVALID
  - EXPIRED
  - EXPIRE_WARN
  - RATE_LIMITED
  - RATE_LIMIT_WARN

  Alarm Code: 1110 - ERROR_LICENSE

Table 4: InvalidLicense

Possible Cause	Corrective Action
CPS "CORE" license related error: • license_state="INVALID": CPS "CORE" is NOT licensed: MOBILE_CORE, FIXED_CORE or SP_CORE license is NOT found. CPS "CORE" is licensed but the licensed session count is not set. • license_state="EXPIRED": CPS "CORE" license date already expired. • license_state="RATE_LIMITED": Current number of session usage is > CPS "CORE" licensed session count. • license_state="RATE_LIMIT_WARN": Current number of session usage is approaching the maximum allowed. The defined maximum ratio is 80% of the licensed count. • license_state="EXPIRE_WARN": CPS "CORE" license will expire at CPS EXPIRY DATE. The defined expire date warning interval is 30 days from the expiration date.	If the message contains "InterfaceID=core", this error is related to CPS "CORE". Take the corrective action based on the "license_state=" in the message: • license_state=INVALID": CPS "CORE" is NOT licensed: MOBILE_CORE, FIXED_CORE or SP_CORE license is NOT found. Corrective action: Make sure CPS "CORE" is specified in `features.properties` file and is licensed as contained in `.lic` file. CPS "CORE" is licensed but the licensed session count is not set. Corrective action: Make sure CPS "CORE" has valid licensed session count in `.lic` file. • license_state="RATE_LIMITED": Current number of session usage is > CPS "CORE" licensed session count. Corrective action: Purchase a larger licensed session count in `.lic` file. • license_state="EXPIRED": CPS "CORE" license date already expired. Corrective action: Make sure that CPS "CORE" expiry date has not expired in `.lic` file. • license_state="RATE_LIMIT_WARN": Current number of session usage is approaching the maximum allowed limit. Corrective action: Purchase a larger licensed session count in `.lic` file. • license_state="EXPIRE_WARN": CPS "CORE" license will expire at: CORE license expiry date. Corrective action: Make sure CPS "CORE" expiry date is not approaching the defined expiry interval - 30 days in `.lic` file.

Possible Cause	Corrective Action
CPS "feature" license related error: • license_state="INVALID": CPS FeatureLicenseManager does not provide a name Or CPS feature is not licensed. • license_state="EXPIRED": CPS feature license date already expired. • license_state="RATE_LIMITED": Feature current number of session usage is > CPS "CORE" licensed session count. • license_state="EXPIRE_WARN": CPS feature license will expire at: feature license expiry date. CPS defined expire date warning interval is 30 days from the expiration date.	The message "InterfaceID=" indicate which CPS "feature"has license related error: • license_state="INVALID": CPS FeatureLicenseManager does not provide a name OR CPS feature is not licensed. Corrective action: Make sure CPS "Feature" is specified in `features.properties` file and is licensed as contained in `.lic` file. • license_state="EXPIRED": CPS feature license date already expired. Corrective action: Make sure that CPS "Feature" expiry date has not expired in `.lic` file • license_state="RATE_LIMITED": Current number of session usage is > CPS "CORE" licensed session count. Corrective action: Create a larger CPS "CORE" licensed session count in `.lic` file. • license_state="EXPIRE_WARN": CPS feature license will expire at: feature license expiry date. CPS defined expiry date warning interval is 30 days from the expiration date. Corrective action: Make sure CPS "Feature" expiry date is not approaching the CPS defined expiry interval - 30 days in `.lic` file.

- **DeveloperMode**: This alarm is generated when CPS is running in DeveloperMode. CPS keeps reminding the user that system is running in Developer Mode and instructs on how to clear the Developer Mode. CPS is running in Deveoper Mode, number of concurrent session is limited to 100.

  Alarm/Trap message: Using Developer mode (100 session limit). To use a license file, remove `-Dcom.broadhop.developer.mode` from `/etc/broadhop/qns.conf` file.

  Alarm Code: 1105 - ERROR_DEVELOPER_MODE

Table 5: DeveloperMode

Possible Cause	Corrective Action
CPS is running in Developer mode and current number of session usage is <= 100.	Clear 'DeveloperMode' flag to annotate the following to make sure the consistency: 1. Remove the following line from the `/etc/broadhop/qns.conf` file: `-Dcom.broadhop.developer.mode=true.` 2. Purchase and use a license file. 3. Restart the Policy Server (QNS) process. 4. Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (load balancer).

- Smart Licensing related:
  - **License Usage Threshold Exceeded**: This alarm is generated when the current number of session usage exceeds the **License Usage Threshold Percentage** value configured in the Policy Builder under **Reference Data** > **Fault List**. CPS Alarm/Trap message contains the following key words:

    "InterfaceID=" this keyword indicates the threshold value.

    "severity=" this keywod indicates severity associated to the threshold. The severity value includes:

    - CRITICAL
    - ERROR
    - NOTICE
    - WARNING

    Alarm Code: 1111 - LICENSE_THRESHOLD

    Table 6: License Usage Threshold Exceeded

Possible Cause	Corrective Action
The current number of session usage exceeds the **License Usage Threshold Percentage** value.	Option 1: Purchase more license session count. Option 2: Adjust **License Usage Threshold Percentage** value configured in Policy Builder.

  - **LicenseSessionCreation**: This alarm is generated when CPS does not allow new CPS session to be created.

    Alarm Code: 1104 - ERROR_SESSION_CREATION

Table 7: LicenseSessionCreation

Possible Cause	Corrective Action
• CPS "CORE" is not defined in `features.properties` file. • CPS license 90 days evaluation period timeout.	1. Add CPS "CORE" license to `/etc/broadhop/license_sl_conf/features.properties` file. 2. Purchase licenses as CPS evaluation 90 days period timeout already.

- **InvalidLicense**: This alarm is generated when CPS license status is not VALID. The error could be any of the followings:

  1. Core license related: CPS "Core" license error.
  2. Feature license related: CPS "Feature" license error.

  CPS Alarm/Trap message format:

  "InterfaceID=" keyword indicates the license name.

  "license_state=" keywork indicates license state.

  CPS defined license sate includes:

  - UNVERIFIED
  - INVALID
  - RATE_LIMITED (OutOfCompliance)
  - EVAL_EXPIRED

  Alarm Code: 1110 - ERROR_LICENSE

Table 8: InvalidLicense

Possible Cause	Corrective Action
CPS "CORE" license related error: • license_state="INVALID": CPS "CORE" is NOT licensed: MOBILE_CORE, FIXED_CORE or SP_CORE license is NOT found. CPS "CORE" is licensed but the licensed session count is not set. • OutOfCompliance - license_state="RATE_LIMITED": CPS current number of session usage is > CPS "CORE" licensed session count.	If the message contains "InterfaceID=core", this error is related to CPS "CORE". Take the corrective action based on the "license_state=" in the message: • license_state=INVALID": CPS "CORE" is NOT licensed: MOBILE_CORE, FIXED_CORE or SP_CORE license is NOT found. Corrective action: Make sure CPS "CORE" is specified in `features.properties` file and is licensed as contained in `.lic` file. CPS "CORE" is licensed but the licensed session count is not set. Corrective action: Make sure CPS "CORE" has valid licensed session count in `.lic` file. • OutOfCompliance - license_state="RATE_LIMITED": CPS current number of session usage is > CPS "CORE" licensed session count. Corrective action: Purchase a larger licensed session count in .lic file. • license_state="EVAL_EXPIRED": CPS 90 days evaluation period timeout already. Corrective action: Purchase licenses as 90 days evaluation period has finished.
CPS "feature" license related error: • license_state="INVALID": CPS FeatureLicenseManager does not provide a name or CPS feature is not licensed. • OutOfCompliance - license_state="RATE_LIMITED": CPS feature current number of session usage is > CPS "CORE" licensed session count.	The message "InterfaceID=" indicate which CPS "feature"has license related error: • license_state="INVALID": CPS FeatureLicenseManager does not provide a name or CPS feature is not licensed. Corrective action: Make sure CPS "Feature" is specified in `features.properties` file and is licensed as contained in `.lic` file. • OutOfCompliance - license_state="RATE_LIMITED": CPS feature current number of session usage is > CPS "CORE" licensed session count. Corrective action: Purchase more license to support the required sessions.

- **DeveloperMode**: This alarm is generated when CPS is running in DeveloperMode. CPS keeps reminding the user that system is running in Developer Mode and instructs on how to clear the Developer Mode. CPS is running in Deveoper Mode, number of concurrent session is limited to 100.

  Alarm/Trap message: Using Developer mode (100 session limit). To use a license file, remove `-Dcom.broadhop.developer.mode` from `/etc/broadhop/qns.conf` file.

  Alarm Code: 1105 - ERROR_DEVELOPER_MODE

  Table 9: DeveloperMode

Possible Cause	Corrective Action
CPS allows new session to be created. CPS is running in DeveloperMode and CPS current session usage is <= 100. **Message**: Using Developer mode (100 session limit). To use a license file, remove `-Dcom.broadhop.developer.mode` from `/etc/broadhop/qns.conf` file.	Clear 'DeveloperMode' flag to annotate the following to make sure the consistency: **1.** Remove the following line from the `/etc/broadhop/qns.conf` file: `-Dcom.broadhop.developer.mode=true.` **2.** Restart the Policy Server (QNS) process. **3.** Within 5 minutes of interval, verify the generated alarm on NMS server and `/var/log/snmp/trap` of active Policy Director (load balancer).

Other Alarms

- **PoliciesNotConfigured**: The alarm is generated when the policy engine cannot find any policies to apply while starting up. This may occur on a new system, but requires immediate resolution for any system services to operate.

  Alarm Code: 1001

  This alarm is generated when server is started or when Publish operation is performed. As indicated by the down status, policy configurations contains error - PB Configurations converted CPS Rules are failed. Message contains the error detail.

  Table 10: PoliciesNotConfigured - 1001

Possible Cause	Corrective Action
This event is raised when exception occurs while converting policies to policy rules. **Message**: 1001 Policies not configured. `Log file is logged with error message Exception stack trace is logged`	Corrective action needs to be taken as per the log message and corresponding configuration error needs to be corrected as mentioned in the logs.

  Alarm Code: 1002

This alarm is generated when `diagnostics.sh` runs which provides last success/failure policies message.

The corresponding notification appears when Policy Builder configurations converted CPS rules are failed during validation against "validation-rules".

Corrective action needs to be taken as per the log message and diagnostic result. Corresponding configuration error needs to be corrected as mentioned in the logs and diagnostic result.

Table 11: PoliciesNotConfigured - 1002

Possible Cause	Corrective Action
This event is raised when policy engine is not initialized. **Message**: Last policy configuration failed with the message: `Policy engine is not initialized` Log file is logged with the warning message: `Policy engine is not initialized`	Make sure that policy engine is initialized.
This event occurs when non policy root object exists. **Message**: Last policy configuration failed with the message: `Policy XMI file contains non policy root object` Log file is logged with the error message: `Policy XML file contains non policy root object`.	To add policy root object in Policies.
This event occurs when policy does not contain a root blueprint. **Message**: Last policy configuration failed with the message: `Policy Builder configurations does not have any Policies configured under Policies Tab`. Log file is logged with the error message: `Policy does not contain a root blueprint. Please add one under the policies tab`.	To add configures in Policies tab.

Possible Cause	Corrective Action
The event occurs when configured blueprint is missing. **Message**: Last policy configuration failed with the message: `There is a configured blueprint <configuredBlueprintId> for which the original blueprint is not found <originalBluePrintId>. You are missing software on your server that is installed in Policy Builder.` Log file is logged with the error message: `There is a configured blueprint <configuredBlueprintId> for which the original blueprint is not found <originalBluePrintId>. You are missing software on your server that is installed in Policy Builder.`	Make sure that the blueprints are installed.
This event occurs when error was detected while converting Policy Builder configuration to CPS Rrules when the server restarts or when Publish happens. **Message**: Last policy configuration failed with the message: `exception stack trace.` Log file is logged with the error message: `Exception stack trace is logged.`	Correct policy configuration based on the exception.

- **DiameterPeerDown**: Diameter peer is down.

  Alarm Code: 3001 - DIAMETER_PEER_DOWN

Table 12: DiameterPeerDown

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of the peer actually being down.	Check the status of the Diameter Peer, and if found down, troubleshoot the peer to return it to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of the Diameter Peer, and if found UP, check the network connectivity between CPS and the Diameter Peer. It should be reachable from both sides.

Possible Cause	Corrective Action
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the Diameter Peer for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the Diameter Peer being accidently not configured correctly.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to the Diameter Peer (port number, realm, and so on) for any incorrect data and errors. 3. Make sure that the application on Diameter Peer is listening on the port configured in PB.

- **DiameterAllPeersDown**: All diameter peer connections configured in a given realm are DOWN (connection lost). The alarm identifies which realm is down. The alarm is cleared when at least one of the peers in that realm is available.

  Alarm Code: 3002 - DIAMETER_ALL_PEERS_DOWN

Table 13: DiameterAllPeersDown

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of all the peer actually being down.	Check the status of each Diameter Peer, and if found down, troubleshoot each peer to return it to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of the each Diameter Peer, and if found up, check the network connectivity between CPS and each Diameter Peer. It should be reachable from each side.
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the Diameter Peers for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the Diameter Peers being incorrect.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to each peer (port number, realm, and so on) for any incorrect data and errors. 3. Make sure that the application on each Diameter Peer is listening on the port configured in PB.

- **DiameterStackNotStarted**: This alarm is generated when Diameter stack cannot start on a particular policy director (load balancer) due to some configuration issues.

  Alarm Code: 3004 - DIAMETER_STACK_NOT_STARTED

  Table 14: DiameterStackNotStarted

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, Diameter stack is not configured properly or some configuration is missing.	Check the Policy Builder configuration. Specifically check for local endpoints configuration under Diameter stack. 1. Verify localhost name defined is matching the actual hostname of the policy director (load balancer) VMs. 2. Verify instance number given matches with the policy director instance running on the policy director (load balancer) VM. 3. Verify all the policy director (load balancer) VMs are added in local endpoint configuration.
In case of an alarm raised after a recent PB configuration change, there may be a possibility that the PB configurations related to the Diameter Stack has been accidently misconfigured.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to the Diameter Stack (local hostname, advertise fqdn, and so on) for any incorrect data and errors. 3. Make sure that the application is listening on the port configured in PB in CPS.

- **SMSC server connection down**: SMSC Server is not reachable. This alarm gets generated when any one of the configured active SMSC server endpoints is not reachable and CPS will not be able to deliver a SMS via that SMSC server.

  Alarm Code: 5001 - SMSC_SERVER_CONNECTION_STATUS

  Table 15: SMSC server connection down

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of the SMSC Server actually being down.	Check the status of the SMSC Server, and if found down, troubleshoot the server to return it to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of the SMSC Server, and if found up, check the network connectivity between CPS and the Server. It should be reachable from both sides.

Possible Cause	Corrective Action
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the SMSC Server for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the SMSC Server being incorrect.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to SMSC Server (port number, realm, and so on) for any incorrect data and errors. 3. Make sure that the application on SMSC Server is listening on the port configured in PB.

- **All SMSC server connections are down**: None of the SMSC servers configured are reachable. This Critical Alarm gets generated when the SMSC Server endpoints are not available to submit SMS messages thereby blocking SMS from being sent from CPS.

  Alarm Code: 5002 - ALL_SMSC_SERVER_CONNECTION_STATUS

Table 16: All SMSC server connections are down

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of all the SMSC Servers actually being down.	Check the status of each SMSC Server, and if found down, troubleshoot the servers to return them to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of each SMSC Server, and if found up, check the network connectivity between CPS and each SMSC Server. It should be reachable from each side.
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the SMSC Servers for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the SMSC Servers being incorrect.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to SMSC Servers (port number, realm, and so on) for any incorrect data and errors. 3. Make sure that the application on each SMSC Server is listening on the respective port configured in PB.

- **Email Server not reachable**: Email server is not reachable. This alarm gets generated when any of the configured Email Server Endpoints are not reachable. CPS will not be able to use the server to send emails.

  Alarm Code: 5003 - EMAIL_SERVER_STATUS

  Table 17: Email server is not reachable

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of the Email Server actually being down.	Check the status of the Email Server, and if found down, troubleshoot the server to return it to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of Email Server, and if found up, check the network connectivity between CPS and the Email Server. It should be reachable from both sides.
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the Email Server for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the Email Server being incorrect.	**1.** Verify the changes recently made in PB by taking the SVN diff. **2.** Review all PB configurations related to Email Server (port number, realm, and so on) for any incorrect data and errors. **3.** Make sure that the application on Email Server is listening on the port configured in PB.

- **All Email servers not reachable**: No email server is reachable. This alarm (Critical) gets generated when all configured Email Server Endpoints are not reachable, blocking emails from being sent from CPS.

  Alarm Code: 5004 - ALL_EMAIL_SERVER_STATUS

  Table 18: All Email servers not reachable

Possible Cause	Corrective Action
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of all the Email Servers actually being down.	Check the status of each Email Server, and if found down, troubleshoot the server to return it to service.
In case of a down alarm being generated but no clear alarm being generated, there could be a possibility of a network connectivity issue.	Check the status of the each Email Server, and if found up, check the network connectivity between CPS and each Email Server. It should be reachable from each side.

Possible Cause	Corrective Action
In case of a down alarm getting generated intermittently followed by a clear alarm, there could be a possibility of an intermittent network connectivity issue.	Check the network connectivity between CPS and the Email Servers for intermittent issues and troubleshoot the network connection.
In case of an alarm raised after any recent PB configuration change, there may be a possibility of the PB configurations related to the Email Servers being incorrect.	1. Verify the changes recently made in PB by taking the SVN diff. 2. Review all PB configurations related to Email Servers (port number, realm, and so on) for any incorrect data and errors. 3. Make sure that the application on each Email Server is listening on the respective port configured in Policy Builder.

- **MemcachedConnectError**: This alarm is generated if attempting to connect to or write to the memcached server causes an exception.

  Alarm Code: 1102 - MEMCACHED_CONNECT_ERROR

Table 19: MemcachedConnectError

Possible Cause	Corrective Action
The memcached process is down on lbvip02.	Check the memcached process on lbvip02. If the process is stopped, start the process using the command `monit start memcached` assuming the monit service is already started.
The Policy Server VMs fail to reach/connect to lbvip02 or lbvip02:11211.	Check for connectivity issues from Policy Server (QNS) to lbvip02 using `ping`/`telnet` command. If the network connectivity issue is found, fix the connectivity.
The test operation to check memcached server timed out. This can happen if the memcached server is slow to respond/network delays OR if the application pauses due to GC. If the error is due to application pause due to GC, it will mostly get resolved when the next diagnostics is run.	1. Check the parameter `-DmemcacheClientTimeout` in `qns.conf` file. If the parameter is not present, the default timeout is 50 ms. So if the application pause is >= 50 ms, this issue can be seen. The pause can be monitored in `service-qns-x.log` file. The error should subside in the next diagnostics run if it was due to application GC pause. 2. Check for network delays for RTT from Policy Server to lbvip02.

Possible Cause	Corrective Action
The test operation to check memcached server health failed with exception.	Check the exception message and if an exception is caused, during that time only, the diagnostics for memcached should pass in the next run. Check if the memcached process is up on lbvip02. Also check for network connectivity issues.

- **ZeroMQConnectionError**: Internal services cannot connect to a required Java ZeroMQ queue. Although retry logic and recovery is available, and core system functions should continue, investigate and remedy the root cause.

  Alarm Code: 3501 - ZEROMQ_CONNECTION_ERROR

  Table 20: ZeroMQConnectionError

Possible Cause	Corrective Action

Internal services cannot connect to a required Java ZeroMQ queue. Although retry logic and recovery is available, and core system functions should continue, investigate and remedy the root cause.	1. Login to the IP mentioned in the alarm and check if the Policy Server (QNS) process is up on that VM. If it is not up, start the process.
	2. Login to the IP mentioned in the alarm and check if the port mentioned in the alarm is listening using the `netstat` command).
	`netstat -apn | grep <port>`
	If not, check the Policy Server logs for any errors.
	3. Check if the VM which raised the alarm is able to connect to the mentioned socket using the `telnet` command.
	`telnet <ip> <port>`
	If it is a network issue, fix it.

- **LdapAllPeersDown**: All LDAP peers are down.

  Alarm Code: 1201 - LDAP_ALL_PEERS_DOWN

  Table 21: LdapAllPeersDown

Possible Cause	Corrective Action
All LDAP servers are down.	Check if the external LDAP servers are up and if the LDAP server processes are up. If not, bring the servers and the respective server processes up.
Connectivity issues from the LB to LDAP servers.	Check the connectivity from Policy Director (LB) to LDAP server. Check (using ping/telnet) if LDAP server is reachable from Policy Director (LB) VM. If not, fix the connectivity issues.

- **LdapPeerDown**: LDAP peer identified by the IP address is down.

  Alarm Code: 1202 - LDAP_PEER_DOWN

  Table 22: LdapPeerDown

Possible Cause	Corrective Action
The mentioned LDAP server in the alarm message is down.	Check if the mentioned external LDAP server is up and if the LDAP server process is up on that server. If not, bring the server and the server processes up.
Connectivity issues from the Policy Director (LB) to the mentioned LDAP server address in the alarm.	Check the connectivity from Policy Director (LB) to mentioned LDAP server. Check (using ping/telnet) if LDAP server is reachable from Policy Director (LB) VM. If not, fix the connectivity issues.

- **ApplicationStartError**: This alarm is generated if an installed feature cannot start.

  Alarm Code: 1103

  Table 23: ApplicationStartError

Possible Cause	Corrective Action
This alarm is generated if installed feature cannot start.	**1.** Check which images are installed on which CPS hosts by reading `/var/qps/images/image-map`. **2.** Check which features are part of which images by reading `/etc/broadhop/<image-name>/features` file. **Note** A feature which cannot start must be in at least one of images. **3.** Check if feature which cannot start has its jar in compressed image archive of all images found in above steps. **4.** If jar is missing contact Cisco support for required feature. If jar is present, collect logs from `/var/log/broadhop` on VM where feature cannot start for further analysis.

- **VirtualInterface Down**: This alarm is generated when the internal Policy Director (LB) VIP virtual interface does not respond to a ping.

  Alarm Code: 7405

Table 24: VirtualInterface Down

Possible Cause	Corrective Action
This alarm is generated when the internal Policy Director (LB) VIP virtual interface does not respond to a ping. Corosync detects this and moves the VIP interface to another Policy Director (LB). The alarm then clears when the other node takes over and a ViritualInterface Up trap is sent.	No action is required since the alarm is cleared automatically as long as a working Policy Director (LB) node gets the VIP address.
This alarm is generated when the internal Policy Director (LB) VIP virtual interface does not respond to a ping and selection of a new VIP hosts fails.	**1.** Run `diagnostics.sh` on Cluster Manager as root user to check for any failures on the Policy Director (LB) nodes.. **2.** Make sure that both policy director nodes are running. If problems are noted, refer to *CPS Troubleshooting Guide* for further steps required to restore policy director node function problem. **3.** After all the policy directors are up, if the trap still does not clear, restart corosync on all policy directors using the `monit restart corosync` command.

- **VM Down**: This alarm is generated when the administrator is not able to ping the VM.

  Alarm Code: 7401

Table 25: VM Down

Possible Cause	Corrective Action
This alarm is generated when a VM listed in the `/etc/hosts` does not respond to a ping.	**1.** Run `diagnostics.sh` on Cluster Manager as root user to check for any failures. **2.** For all VMs with FAIL, refer to *CPS Troubleshooting Guide* for further steps required to restore the VM function.

- **No Primary DB Member Found**: This alarm is generated when the system is unable to find primary member for the replica-set.

  Alarm Code: 7101

Table 26: No Primary DB Member Found

Possible Cause	Corrective Action
This alarm is generated during mongo failover or when majority of replica-set members are not available.	**1.** Login to pcrfclient01/02 VM and verify the replica-set status `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. **2.** If the member is not running start the mongo process on each sessionmgr/arbiter VM For example, `/usr/bin/systemctl start sessionmgr-`*`port`* **Note** Change the port number (*port*) according to your deployment. **3.** Verify the mongo process, if the process does not come UP then verify the mongo logs for further debugging log. For example, `/var/log/mongodb-`*`port`*`.log` **Note** Change the port number (*port*) according to your deployment.

- **Arbiter Down**: This alarm is generated when the arbiter member of the replica-set is not reachable.

  Alarm Code: 7103

Table 27: Arbiter Down

Possible Cause	Corrective Action
This alarm is generate in the event of abrupt failure of arbiter VM and does not come up due to some unspecified reason (In HA - arbiter VM is pcrfclient01/02 and for GR - third site or based on deployment model).	**1.** Login to pcrfclient01/02 VM and verify the replica-set status `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. **2.** Login to arbiter VM for which the alarm has generated. **3.** Check the status of mongo port for which alarm has generated. For example, `ps -ef | grep 27720` **4.** If the member is not running, start the mongo process. For example, `/usr/bin/systemctl start sessionmgr-27720` **5.** Verify the mongo process, if the process does not come UP then verify the mongo logs for further debugging log. For example, `/var/log/mongodb-`*`port`*`.log` **Note** Change the port number (*port*) according to your deployment.

- **Config Server Down**: This alarm is generated when the configuration server for the replica-set is unreachable. This alarm is not valid for non-sharded replica-sets.

  Alarm Code: 7104

Table 28: Config Server Down

Possible Cause	Corrective Action
This alarm is generated in the event of abrupt failure of configServer VM (when mongo sharding is enabled) and does not come up due to some unspecified reasons.	**1.** Login to pcrfclient01/02 VM and verify the shard health status `diagnostics.sh --get_shard_health <dbname>` **2.** Check the status of mongo port for which alarm has generated. For example, `ps -ef | grep 27720` **3.** If the member is not running, start the mongo process. For example, `/usr/bin/systemctl start sessionmgr-27720` **4.** Verify the mongo process, if the process does not come UP then verify the mongo logs for further debugging log. For example, `/var/log/mongodb-port.log` **Note** Change the port number (*port*) according to your deployment.

- **All DB Member of replica set Down**: This alarm is generated when the system is not able to connect to any member of the replica-set.

  Alarm Code: 7105

Table 29: All DB Member of replica set Down

Possible Cause	Corrective Action
This alarm is generated in the event of abrupt failure of all sessionmgr VMs and does not come up due to some unspecified reason or all members are down.	**1.** Login to pcrfclient01/02 VM and verify the replica-set status `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. **2.** If the member is not running start the mongo process on each sessionmgr/arbiter VM For example, `/usr/bin/systemctl start sessionmgr-`*`port`* **Note** Change the port number (*port*) according to your deployment. **3.** Verify the mongo process, if the process does not come UP then verify the mongo logs for further debugging log. For example, `/var/log/mongodb-`*`port`*`.log` **Note** Change the port number (*port*) according to your deployment.

- **DB resync is needed**: This alarm is generated whenever a manual resynchronization of a database is required to recover from a failure.

  Alarm Code: 7106

Table 30: DB resync is needed

Possible Cause	Corrective Action
This alarm is generated whenever a secondary member of replica-set of mongo database does not recover automatically after failure. For example, if sessionmgr VM is down for longer time and after recovery the secondary member does not recover.	1. Login to pcrfclient01/02 VM and verify the replica-set status `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. 2. Check which member is in recovering/fatal or startup2 state. 3. Login to that sessionmgr VM and check for mongo logs. Refer to *CPS Troubleshooting Guide* for recover procedure.

- **QNS Process Down**: This alarm is generated when Policy Server (QNS) java process is down.

  Alarm Code: 7301

Table 31: QNS Process Down

Possible Cause	Corrective Action
This alarm is generated if Policy Server (QNS) process on one of the CPS VMs is down.	1. Run `diagnostics.sh` on Cluster Manager as root user to check for any failures.. 2. On VM where qns is down, run `monit summary` to check if "monit" is monitoring policy server (QNS) process. 3. Analyze logs in `/var/log/broadhop` directory for exceptions and errors.

- **Gx Message processing Dropped**: This alarm is generated for Gx Message CCR-I, CCR-U andCCR-T when processing of messages drops below 95% on qnsXX VM.

  Alarm Code: 7302

Table 32: Gx Message processing Dropped

Possible Cause	Corrective Action
1. Gx traffic to the CPS system is beyond system capacity. 2. CPU utilization is very high on qnsXX VM. 3. Mongo database performance is not optimal.	1. Login via Grafana dashboard and check for any Gx message processing trend. 2. Check CPU utilization on all the Policy Server (QNS) VMs via grafana dashboard. 3. Login to pcrfclient01/02 VM and check the mongo database health. `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. 4. Check for any unusual exceptions in consolidated policy server (qns) and mongo logs.

- **Gx Average Message processing Dropped**: This alarm is generated for Gx Message CCR-I, CCR-U and CCR-T when average message processing is above 20ms on qnsXX VM.

  Alarm Code: 7303

Table 33: Average Gx Message processing Dropped

Possible Cause	Corrective Action
1. Gx traffic to the CPS system is beyond system capacity. 2. CPU utilization is very high on qnsXX VM. 3. Mongo database performance is not optimal.	1. Login via Grafana dashboard and check for any Gx message processing trend. 2. Check CPU utilization on all the Policy Server (QNS) VMs via grafana dashboard. 3. Login to pcrfclient01/02 VM and check the mongo database health. `diagnostics.sh --get_replica_status` **Note** If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, mostly an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status. 4. Check for any unusual exceptions in consolidated policy server (qns) and mongo logs.

- **Percentage of LDAP retry threshold Exceeded**: This alarm is generated for LDAP search queries when LDAP retries compared to total LDAP queries exceeds 10% on qnsXX VM.

  Alarm Code: 7304

Table 34: Percentage of LDAP retry threshold Exceeded

Possible Cause	Corrective Action
Multiple LDAP servers are configured and LDAP servers are down.	1. Check connectivity between CPS and all LDAP servers configured in Policy Builder. 2. Check latency between CPS to all LDAP servers and LDAP server response time should be normal. 3. Restore connectivity if any LDAP server is down.

- **LDAP Requests as percentage of CCR-I Dropped**: This alarm is generated for LDAP operations when LDAP requests as percentage of CCR-I (Gx messages) drops below 25% on qnsXX VM.

  Alarm Code: 7305

Table 35: LDAP Requests as percentage of CCR-I Dropped

Possible Cause	Corrective Action
1. Gx traffic to the CPS system is beyond system capacity. 2. CPU utilization is very high on qnsXX VM. 3. Mongo database performance is not optimal.	1. Check connectivity between CPS and all LDAP servers configured in Policy Builder. 2. Check latency between CPS to all LDAP servers and LDAP server response time should be normal. 3. Check policy server (qns) logs on policy director (lb) VM for which alarm has been generated.

- **LDAP Query Result Dropped**: This alarm is generated when LDAP Query Result goes to 0 on qnsXX VM.

  Alarm Code: 7306

Table 36: LDAP Query Result Dropped

Possible Cause	Corrective Action
Multiple LDAP servers are configured and LDAP servers are down.	1. Check connectivity between CPS and all LDAP servers configured in Policy Builder. 2. Check latency between CPS to all LDAP servers and LDAP server response time should be normal. 3. Restore connectivity if any LDAP server is down.

- **LDAP Request Dropped**: This alarm is generated for LDAP operations when LDAP requests drop below 0 on lbXX VM.

  Alarm Code: 7307

Table 37: LDAP Request Dropped

Possible Cause	Corrective Action
Gx traffic to the CPS system is increased beyond system capacity.	1. Check connectivity between CPS and all LDAP servers configured in Policy Builder. 2. Check latency between CPS to all LDAP servers and LDAP server response time should be normal. 3. Check policy server (qns) logs on policy director (lb) VM for which alarm has been generated.

- **Binding Not Available at Policy DRA**: This alarm is generated when IPv6 binding for sessions is not found at Policy DRA. Only one notification is sent out whenever this condition is detected.

  Alarm Code: 6001

  Table 38: Binding Not Available at Policy DRA

Possible Cause	Corrective Action
Binding Not Available at Policy DRA	This alarm is generated whenever binding database at Policy DRA is down. This alarm gets cleared automatically after the time configured in Policy Builder (**Diameter Configuration** > **PolicyDRA Health Check** > **Alarm Config** > **Alarm Clearance Interval** is reached.

- **SPR_DB_ALARM**: This alarm indicates there is an issue in establishing connection to the Remote SPR Databases configured under **USuM Configuration** > **Remote Database Configuration** during CPS policy server (qns) process initialization.

  Alarm Code: 6101

  Table 39: SPR_DB_ALARM

Possible Cause	Corrective Action
A network issue/latency in establishing connection to the remote SPR databases.	Check the network connection/latency and adjust the qns.conf parameter `-DserverSelectionTimeout.remoteSpr` in consultation with Cisco Technical Representative.

- **DiameterQnsWarmupError**: The alarm is generated when the warmup feature is enabled and there is an exception in retrieving Policy Server (qns) node number, site ID, parsing the warmup dictionaries or scenario file.

  Alarm Code: 3005

  Table 40: DiameterQnsWarmupError

Possible Cause	Corrective Action
qns.node.warmup.hostname.substring parameter is not configured in qns.conf file. GeoSiteName is not configured if it is a GR setup	• If alarm contains ‘didn’t start node num/SITE_ID not parsed’, make sure that `qns.node.warmup.hostname.substring` and GeoSiteName (if it is GR setup) is configured in `qns.conf` file. Policy Server (QNS) VMs hostname must only contain number after substring parameter is configured. • If alarm contains ‘didn't start due to exception’, please consult with Cisco Technical Representative.

- **SPRNodeNotAvailable:** This alarm is generated when all the members of the SPR replica set are not available and a master node is available for that given replica-set.

  Alarm Code: 6102

Table 41: SPRNodeNotAvailable

Possible Cause	Corrective Action
SPR node is not available	When the member(s) of the replica-set are manually recovered and a master node is available for the SPR replica-set, the alarm automatically clears.

- **GC State:** This alarm is generated when Garbage collection on Policy Server (qns) java process occurs three or more (configurable) times within 10 (configurable) mins of interval.

  Alarm Code: 7311

Table 42: GC State

Possible Cause	Corrective Action
GC State	Restart the Policy Server (qns) application for which alarm was reported. After gc_alarm_trigger_interval is reached, if there is no GC triggered, the alarm gets cleared.

- **OldGen State:** This alarm is generated if Oldgen% is more than configured threshold (OLD_GEN_ALARM_TRIGGER_THR) for more than 2 (OLD_GEN_ALARM_TRIGGER_CONT_GC_COUNT) GC.

  Alarm Code: 7312

Table 43: OldGen State

Possible Cause	Corrective Action
OldGen State	Restart the Policy Server (qns) application for which alarm was reported. On restart, if oldGen value is less than configured oldgen_clear_ trigger_thr_per value, the alarm gets cleared.

- **SessionLimitOverloadProtectionNotSet:** This alarm is generated when **Session Limit Overload Protection** is configured to 0 (default). With value as 0, CPS can handle infinite number of sessions and this can affect the database and can lead to application crash.

  Alarm Code: 1112

Table 44: SessionLimitOverloadProtectionNotSet

Possible Cause	Corrective Action
SessionLimitOverload ProtectionNotSet	Go to **System** configuration in Policy Builder and set the value for **Session limit Overload Protection** to recommended value and publish it. This will clear the alarm within 30 seconds.

- **SessionLimitOverloadProtectionExceeded:** The alarm is generated when the current session count of the system exceeds the value configured for Session Limit Overload protection.

  Alarm Code: 1113

Table 45: SessionLimitOverloadProtectionExceeded

Possible Cause	Corrective Action
SessionLimitOverload ProtectionExceeded	Increase the database capacity after consulting with Cisco representative or clear the sessions in the session database so that 'n' becomes less than 'm' (n<m). This should clear the alarm within 30 seconds.

- **SESSION_SHARD_UNREACHABLE:** This alarm is generated when a session manager VM other than primary member is unreachable.

  Alarm Code: 6501

Table 46: SESSION_SHARD_UNREACHABLE

Possible Cause	Corrective Action
SESSION_SHARD_ UNREACHABLE	Bring up the VM. The alarm should get cleared when seen in `diagnostics -get_active_alarms`.

- **ADMIN_DB_MISSING_SHARD_ENTRIES:** This alarm is generated when there are no shards present in the ADMIN replica-skip set > sharding database > shards/sk_shards.

  Alarm Code: 6502

Table 47: ADMIN_DB_MISSING_SHARD_ENTRIES

Possible Cause	Corrective Action
ADMIN_DB_MISSING_ SHARD_ENTRIES	Either create shards in GR/HA for this error to go away. In case of HA, if you had removed the default shard entry, restart Policy Server (qns) services for default shard to be created.

- **MISSING_SESSION_INDEXES:** This alarm is generated when the session database/session collection does not have the required indexes for the normal functioning of the application.

  Alarm Code: 6503

Table 48: MISSING_SESSION_INDEXES

Possible Cause	Corrective Action
MISSING_SESSION_ INDEXES	Recreate the dropped index using mongo CLI for the session collection or restart Policy Server (qns) service on one of the QNS nodes to clear the alarm.

- **MISSING_SPR_INDEXES:** This alarm is generated when the SPR database/subscriber collections does not have the required indexes for the normal functioning of the application.

  Alarm Code: 6504

Table 49: MISSING_SPR_INDEXES

Possible Cause	Corrective Action
MISSING_SPR_ INDEXES	Recreate the dropped index using mongo CLI for the SPR collection or restart Policy Server (qns) service on one of the QNS nodes to clear the alarm.

- **Database Operation** This alarm is generated when the Policy Server (QNS) VM is not able to connect to primary MongoDB replica-set member.

  Alarm Code: 7400, Sub-event ID: 7406

Table 50: Database Operation

Possible Cause	Corrective Action
Database Operation	To clear the alarm, restart the QNS process on the Policy Server (QNS) VMs from where the alarm was generated. Post process restart the alarm clearing will be handled automatically by the system.

- **SVNnotinsync:** This alarm is generated when SVN is not in sync between pcrfclient VMs.

  Alarm Code: 7300, Sub-event ID: 7309

Table 51: SVNnotinsync

Possible Cause	Corrective Action
SVNnotinsync	To clear the alarm, restart the service on the corresponding pcrfclient VM from where the alarm was generated. This brings back the SVN on the pcrfclient VM and the corresponding clear event (SVNinsync) is triggered.

- **MongoPrimaryDB fragmentation exceeded the threshold value:** The alarm is generated if the fragmentation percent breaches default value if threshold value is not configured.

  Alarm Code: 7107

Table 52: MongoPrimaryDB fragmentation exceeded the threshold value

Possible Cause	Corrective Action
This alarm is generated when the fragmentation percentage of primary member for the replica-set exceeds the configured threshold fragmentation value. The configured threshold value is present on sessionmgr VM's `/etc/collectd.d/dbMonitorList.cfg` file.	To reduce the fragmentation percentage, shrink the database when an alarm is generated. Refer to *Steps to Resync a Member of a Replica Set* section in *CPS Operations Guide* to reduce the fragmentation of member. Once the database is shrunk (fragmentation percentage decreases), a clear alarm is sent.

- **Realtime Notification Server not reachable:** This alarm is generated when the configured realtime notification server is not reachable blocking realtime notifications to be sent from CPS.

  Alarm Code: 5005 - REALTIME_NOTIFICATION_SERVER_STATUS

  Table 53: Realtime Notification server is not reachable

Possible Cause	Corrective Action
When the down alarm is generated and the alarm is not cleared, Realtime Notification Server can be actually being down.	Check the status of the Realtime Notification Server. If the server is down, troubleshoot the server to return it to service.
When the down alarm is generated and the alarm is not cleared, there can be a network connectivity issue.	Check the status of Realtime Notification Server. If the server is UP, check the network connectivity between CPS and the Realtime Notification Server. It should be reachable from both sides.
When the down alarm is generated intermittently followed by a clear alarm, there can be intermittent network connectivity issue.	Check the network connectivity between CPS and the Realtime Notification Server for intermittent issues and troubleshoot the network connection.
When an alarm is generated after PB configuration change, there can be issue with the PB configurations related to the Realtime Notification Server.	**1.** Verify the changes recently made in PB by taking the SVN diff. **2.** Review all the PB configurations related to Realtime Notification Server (port number, realm, and so on) for any incorrect data and errors. **3.** Ensure that the application on Realtime Notification Server is listening on the port configured in PB.