



Mobile

- [Alarm Upon Detection of Missing/Corrupt Shards, on page 1](#)
- [MongoDB Health Monitoring for Write Operations, on page 2](#)
- [Prevention of Application from Using Missing/Corrupted Shards, on page 5](#)
- [RCS Feature Suppressing Gx, on page 6](#)
- [Session Manager NTP Synchronization Improvement, on page 10](#)
- [Support for WPS Service on PCRF, on page 10](#)

Alarm Upon Detection of Missing/Corrupt Shards

Feature Summary and Revision History

Table 1: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS SNMP, Alarms, and Clearing Procedures Guide CPS Troubleshooting Guide

Table 2: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description

CPS has been enhanced to generate alarms and let the service provider operators know:

- When the sharding database in the ADMIN replica-set is missing session shard entries in the HA/GR environment

- When a shard is created and an entry exists in the sharding database of the ADMIN replica-set, but Session Manager VM is not reachable
- When indexes are missing on collections existing on SPR/Session database

The following new alarms have been added:

- SESSION_SHARD_UNREACHABLE
- ADMIN_DB_MISSING_SHARD_ENTRIES
- MISSING_SESSION_INDEXES
- MISSING_SPR_INDEXES

A new `qns.conf` parameter `skipUnreachableShards` has been added. By default, the value is set to false. The value must be set to true so that the above mentioned alarms are generated. Contact your Cisco Account representative for information on `qns.conf` file parameters.

For more information, see the following sections:

- *Application Notifications* table in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Clearing Procedures* chapter in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Testing Traps Generated by CPS* in the *CPS Troubleshooting Guide*

MongoDB Health Monitoring for Write Operations

Feature Summary and Revision History

Table 3: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS SNMP, Alarms, and Clearing Procedures Guide CPS Troubleshooting Guide CPS Installation Guide for VMware CPS Installation Guide for OpenStack

Table 4: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description

CPS is enhanced to support MongoDB health monitor for write operations where application detects the false reporting of no PRIMARY connection available for the replica-sets and takes action accordingly.



Note The scope is limited to ADMIN, SESSION, SPR (excluding remote database), and Balance (excluding remote database) replica-sets.

The process of monitoring MongoDB write operations is divided into two sub-parts: Application side and Platform side.

- On the application side, MongoDB write operation and Reset MongoDB client connection threads are initialized to perform the write operations on replica-sets. This is done to verify the write operation failure threshold reached or not. If threshold has reached, MongoDB client connections are reset. Also, generates the counters for all the configured replica-sets.
- The platform scripts fetches the counters generated by the application and checks whether the failure counter for write operation is incrementing, and counter for reset MongoDB client connection fails after maximum retry of reset attempts. If parameter `autoheal_qns_enabled` value is set to **TRUE**, all the configured replica-sets sends an alarm and restarts the application (QNS process on QNS VMs) where the alarm is reported. If parameter value is set to **FALSE**, then the alarm is raised for all the configured replica-sets.

For more information on `autoheal_qns_enabled` configuration, see the following sections:

- *Installing Platform Scripts for MongoDB Health Monitoring - VMware in the CPS Installation Guide for VMware*
- *Installing Platform Scripts for MongoDB Health Monitoring - OpenStack in the CPS Installation Guide for OpenStack*

The following parameters should be configured in `qns.conf` file.

Table 5: qns.conf Parameters

Parameter	Description
<code>mongo.health.monitor.enabled</code>	This parameter is used to enable MongoDB health monitor for write operations. Default value is false.
<code>mongo.health.monitor.scheduler.period</code>	This parameter used to configure how frequently to execute the MongoDB write operation health monitor thread. Default value is 3000 milliseconds.
<code>mongo.reset.scheduler.period</code>	This parameter is used to configure how frequently to execute the thread for checking the reset MongoDB client connections in case of write operations are breached the failure threshold. Default value is 4000 milliseconds.

Parameter	Description
mongo.monitor.write.update.threshold	This parameter is used to configure number of MongoDB write operations to be performed on the database every time the thread executes. Default value is 50.
mongo.monitor.percentage.threshold	This parameter is used to calculate the success threshold percentage rate for MongoDB write operations. If success result is less than configured threshold, then only MongoDB client reset operation is triggered. Default value is 80.
wait.time.after.reset	This parameter is used to configure the time that thread for resetting MongoDB client connection should wait/sleep for after connection reset. Default value is 10000 milliseconds.
mongo.reset.retry.counter	This parameter is used to configure maximum retry attempts for resetting MongoDB client connections in case of previous reset failure. Default value is 2.

The following new statistics are added:

- `mongodb_heartbeat_update_success_<replicaSetName>`
- `mongodb_heartbeat_update_error_<replicaSetName>`
- `mongo_client_reset_<replicaSetName>`
- `mongo_client_reset_fail_<replicasetSetName>`

For more information on statistics, see [Statistics/KPI Additions or Changes](#).

Also, a new alarm, `Database Operations` is added.

For more information, see the following sections:

- *Application Notifications* table in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Clearing Procedures* chapter in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Testing Traps Generated by CPS* in the *CPS Troubleshooting Guide*
- *Installing Platform Scripts for MongoDB Health Monitoring - VMware* in the *CPS Installation Guide for VMware*
- *Installing Platform Scripts for MongoDB Health Monitoring - OpenStack* in the *CPS Installation Guide for OpenStack*

Performance Impact

- When the MongoDB health monitoring is enabled, application initiates two thread for each Session, ADMIN, Balance (excluding remote database replica-sets), SPR (excluding remote database replica-sets) replica sets. The number of threads depends on the number of replica-sets.
- In the scaled setups, as there are more number of replica-sets, you will observe that there is an increase in CPU utilization by 4 - 5%. The increase in the CPU utilization varies if the environment has large number of replica-sets.

Prevention of Application from Using Missing/Corrupted Shards

Feature Summary and Revision History

Table 6: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 7: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description

CPS can now detect missing or unrecognizable secondary session shards and direct the applications not to use them for its CRUD (create, read, update and delete) operations.

This excludes arbiter members and hot standby/backup members as arbiter nodes do not store any data as well as participate in application related CRUD operations. The hot standby/backup VMs are not used in normal traffic operations unless there is a failover/election in progress.

The following scenarios describe when a session shard of a secondary member becomes unreachable:

- When the sessionmgr VM is shutdown. All mongo process running on that VM including the one hosting session information is down, which means all the shards are not reachable.
- The sessionmgr VM is up, but the mongo process is shutdown gracefully:
 - Using `monit stop aido_client` followed by `/etc/init.d/sessionmgr-portno. stop` (for instance)
 - The mongo process is killed abruptly after `monit stop aido_client`

In this case, all the session shards are not reachable on that secondary member.

- Another variant could be that the shards were created but later dropped from the mongo CLI using:

```
session_cache_*, db.dropDatabase() command on the secondary members
```

New `qns.conf` parameters, `skipUnreachableShards` and `skipDbOperOnUnreachableShards` are added. Both the parameters must be set to `true` to skip database operations on unreachable shards.

- `skipUnreachableShards`: By default, the value is set to false. The value must be set to true to generate or clear the alarms.
- `skipDbOperOnUnreachableShards`: By default, the value is set to false. The value must be set to true to enable the feature.

Contact your Cisco Account representative for information on `qns.conf` file parameters.



Restriction

The scope of the feature is restricted to prevent an application from using secondary member session shards when they are unreachable. This feature is not meant to eliminate CRUD operations on other databases such as, SPR, Balance, `sk_cache` and so on.

All session shards unreachable checks happen on secondary MongoDB members in a replica-set. The existing logic to detect unreachable primaries remain unaltered, which when not available writes to the hot standby database for a brief period. Then they are reconciled to newly elected primaries and flushed from hot standby database. No changes were done to the existing behavior related to primary members when unreachable.

RCS Feature Suppressing Gx

Feature Summary and Revision History

Table 8: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS Mobile Configuration Guide

Table 9: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description

Previous Behavior: In previous releases, PCRF created dedicated bearers during the RCS service. Creating dedicated bearers for each RCS service sometimes exceeded dedicated bearer limit in PGW and hence there was a degradation and interference with VoLTE calls.

New Behavior: In current release, CPS skips dedication bearer creation during AAR for RCS media type 'MESSAGE' and takes no action over the Gx interface for rule-installation.

For the first Rx transaction, there is no existing pre-configured rule. CRD lookup happens on table `rx_dedicated_bearer_create`. If result is **true**, then dedicated bearer is created. Otherwise, rule installation is skipped. For this feature, CRD must be configured to return false for media-type=6 so that the rule installation is skipped. There is no RAR on Gx interface for rule activation, but any other trigger (for example, new event-trigger added to Gx session based on specific-actions AVP on Rx_AAR) can trigger Gx RAR.

For the second or any upcoming transaction, CRD lookup is done based on existing service object **EvaluateRxDedicatedBearer** for each media sub-components and result is used in evaluating the existing pre-configured rule.

To support this feature, following new configurations have been added in Policy Builder:

- EvaluateRxDedicatedBearerCreate under **rx** service configuration objects
 - EvaluateRxDedicatedBearerCreate service object is introduced which should be added under service configuration object. While configuring the service option, new STG table should be linked to this object.
- `rx_dedicated_bearer_create` search table for CRD lookup
- `rx_bearer_evaluation_create` search table to evaluate rule for the first transaction



Note As CRD lookup happens for AAR-I, there can be an increase in Rx response time.

For more information, see *EvaluateRxDedicatedBearerCreate* section in the *CPS Mobile Configuration Guide*.

Configuration

Service object **EvaluateRxDedicatedBearerCreate** has been added which must be binded to new STG. In New CRD/STG table, one must set output column to 'false' for media-type:6 so that dedicated bearer is not created.

Sample Policy Builder and CRD changes are mentioned below (table name, column names can be changed).

1. Policy Builder - Search Table Groups

Adding new STG: `rx_dedicated_bearer_create`. Evaluation order for this STG must be new (evaluation order configured can be different for new CRD version).

Custom Reference Data Table Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

***Name** rx_bearer_evaluation_create **Display Name** rx_bearer_evaluation_create Cache Results

Activation Condition Svn Crd Data Best Match

***Evaluation Order** 0

*Name	Display Name	*Use In Conditio	*Type	Key	Required
APPLICATION_ID	APPLICATION ID	<input type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
COMMAND_CODE	COMMAND CODE	<input type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
REQUEST	REQUEST	<input type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media-Type	Media-Type	<input type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EVALUATE	EVALUATE	<input type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

2. Policy Builder - Service Configuration

1. Use case template:

Add newly created service object EvaluateRxDedicatedBearerCreate in the existing use case template:

Use Case Template

Name: Evaluate_Rx_Bearer

Use Case Initiators | **Actions** | Documentation

Service Configurations

- name
- EvaluateRxDedicatedBearer
- EvaluateRxDedicatedBearerCreate

EvaluateRxDedicatedBearerCreate Parameters

*Display Name	Value	Bind Field	Allow Override
Priority	0		<input checked="" type="checkbox"/>
Diameter Client			<input checked="" type="checkbox"/>
Stg Name			<input checked="" type="checkbox"/>
List Of Input Column Avp Pairs (List)			<input checked="" type="checkbox"/>
List Of Output Column Avp Pairs			<input checked="" type="checkbox"/>

2. Service option:

Existing:

Service Option

Name Evaluate_Rx_Bearer **Use Case Template:** Evaluate_Rx_Bearer

Service Configurations

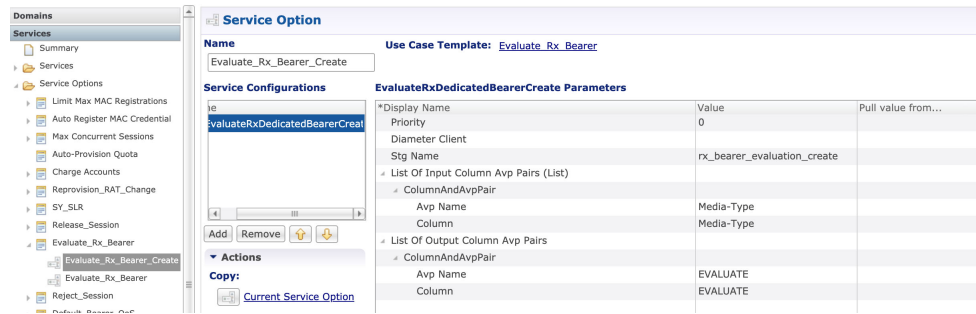
- name
- EvaluateRxDedicatedBearer

Actions

EvaluateRxDedicatedBearer Parameters

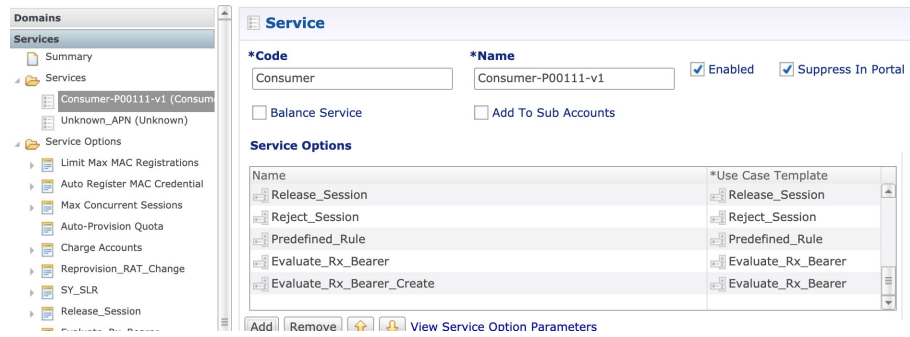
*Display Name	Value	Pull value from...
Priority	0	
Diameter Client		
Stg Name	rx_bearer_evaluation	
List Of Input Column Avp Pairs (List)		
ColumnAndAvpPair		
Avp Name	Media-Type	
Column	Media-Type	
List Of Output Column Avp Pairs		
ColumnAndAvpPair		
Avp Name	EVALUATE	
Column	EVALUATE	

Add new service object and bind it to new STG. Also bind the input and output column to new CRD table (Media-Type, Evaluate of rx_bearer_evaluation_create).



3. Service binding:

New service option must be added to service.



3. CRD Data: rx_bearer_evaluation table data

Existing design contains “Evaluate” as output column which is used only during update (can be CCR-U/2nd AAR/Sy messages)

1. Existing CRD table:

The configuration shown below is set Evaluation to false when CPS receive a Sy SSNR or SLA.

One more entry must be added for media-type: 6 and output should be set to false so that bearer evaluation is skipped (however, bearer is not created).

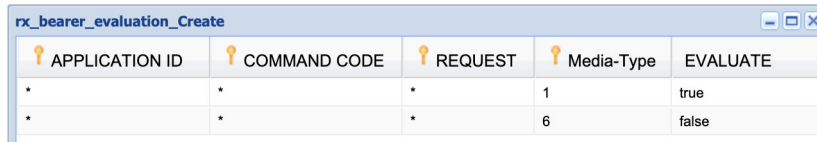
APPLICATION ID	COMMAND CODE	REQUEST	Media-Type	EVALUATE	imp
16777302	8388636	true	1	false	
16777302	8388635	true	1	false	
16777236	265	true	1	true	
16777238	272	true	1	true	
*	*	*	1	false	
*	*	*	6	false	

2. New CRD table:

The **rx_bearer_evaluation_create** search table is created to evaluate rule for the first transaction and decide if dedicated bearer must be created.

Output must be set to false for media-type: 6 (MESSAGE) so that rule is not created.

For all other media-type, it should be true. If there are no entries for specific media-type, the value is set to true (by default) and rule is created for each media sub-component if present.



APPLICATION ID	COMMAND CODE	REQUEST	Media-Type	EVALUATE
*	*	*	1	true
*	*	*	6	false

Session Manager NTP Synchronization Improvement

Feature Summary and Revision History

Table 10: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 11: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description

Previous Behavior: In previous releases, clock synchronization did not happen between Session Managers and Policy Director (LB01) for fresh installations. Also, NTP was not in sync and TIME_WAIT increased after sessionmgr VM was restarted or suspended.

New Behavior: In current release, the issue has been fixed and NTP time synchronization happens between Session Managers and Policy Director (LB) VM of HA/GR/Dual cluster during deployment/reboot/powered-on scenarios.

As a part of fix, MongoDB on Session Manager does not start till loop for syncing NTP is completed.

Support for WPS Service on PCRF

Feature Summary and Revision History

Table 12: Summary Data

Applicable Product(s) or Functional Area	UDC
Applicable Platform(s)	Not Applicable

Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS UDC Administration Guide

Table 13: Revision History

Revision Details	Release
First introduced	19.4.0

Feature Description



Important

This feature is not fully qualified in this release, and is available only for testing purposes. It is planned to be qualified in the subsequent release. For more information, contact your Cisco Account representative.

CPS now provides support for WPS service on PCRF using LWR. The following new UDC service object is introduced to configure the Rx message AVPs which can be used to generate a LDAP attribute:

- BindUDCAtributeForRx

LWR replicated LDAP attribute generated using service BindUDCAtributeForRx can become stale during certain error scenarios. In such scenarios, a Guard Time can be specified to ignore the AVP if it is older than the configured time. While processing any event, QNS evaluates the staleness of the configured attribute and does not use it for policy evaluations.

CPS also supports modification of QoS in WPS usecase if the UE sessions for different APNs are created on different CPS datacenters.



Note

This feature can only be supported when LWR replication is configured for cross-site replication.

For more information, see *Configuring WPS Service on PCRF* section in the *CPS UDC Administration Guide*.

