CPS Release Change Reference, Release 20.2.0 (1)

First Published: 2020-08-27

Last Modified: 2021-04-07

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

CONTENTS

Preface

About This Guide

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

Note The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

Audience

This guide is best used by these readers:

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

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

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS.

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

SAVE THESE INSTRUCTIONS

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

Communications, Services, and Additional Information

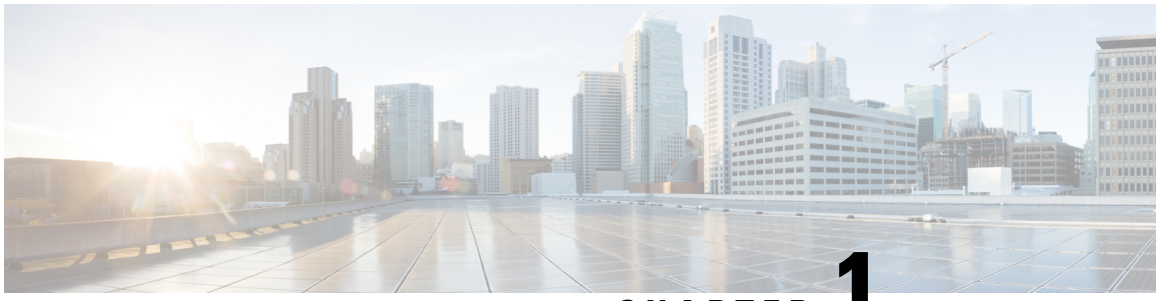
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class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

Cisco Bug Search Tool

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

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.



CHAPTER 1

20.2.0 Features and Changes

20.2.0 Features and Changes

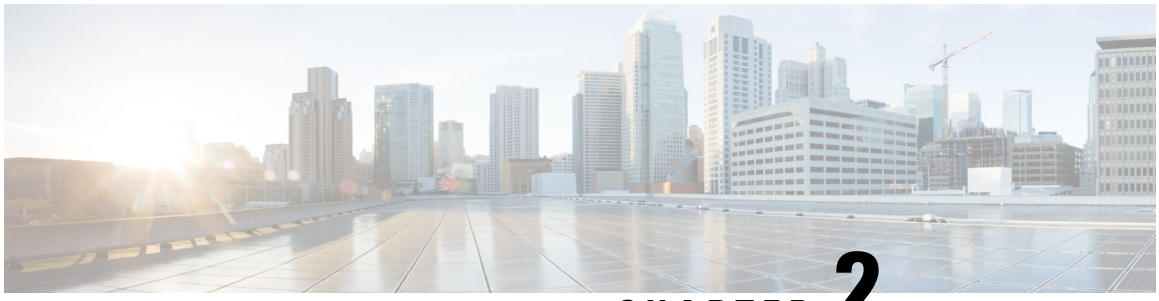
Table 1: 20.2.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
CentOS Security Enhancements/Kernel Upgrade, on page 55	CPS	20.2.0
Critical Resources Monitoring in CPS using KPIs, on page 37	CPS	20.2.0
Enabling In-Service MongoDB Authentication, on page 38	CPS	20.2.0
Enhanced Experimental CRD Visualization, on page 62	CPS	20.2.0
Enhanced BillCycle Recurrence Frequency Amount Configuration, on page 61	CPS	20.2.0
Enhancement on Logging and Logback , on page 23	CPS	20.2.0
Health Check to Prevent Primary Flapping, on page 47	CPS	20.2.0
Import All CRD Fallback Enhancements, on page 62	CPS	20.2.0
KPI Support to Monitor MongoDB Fragmentation and Generate an SNMP Alarm, on page 39	CPS	20.2.0
Optimized Secondary Binding Lookup, on page 40	CPS	20.2.0

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
PCRF Stale Message Handling Enhancements, on page 9	CPS	20.2.0
PSB Requirements for 20.2.0 Release, on page 57	CPS	20.2.0
PSB Requirements for UI and API Issues, on page 58	CPS	20.2.0
SNMP Alarm Additions or Changes, on page 24	CPS	20.2.0
Statistics/KPI Additions or Changes, on page 25	CPS	20.2.0
Support CPS on ESXi 6.7, on page 42	CPS	20.2.0
Support for Encoding Format, on page 10	CPS	20.2.0
Support for HAProxy Connection Balancing, on page 48	CPS	20.2.0
Support for JMS Queue Monitoring, on page 10	CPS	20.2.0
Support for Large Sessions, on page 12	CPS	20.2.0
Support for LDAP/IOMGR Overload Handling, on page 13	CPS	20.2.0
Support for Multiple User Login Privileges, on page 49	CPS	20.2.0
Support for Real Time Notification when Rollover Occurs, on page 14	CPS	20.2.0
Support for Secondary Keys Tag Padding, on page 17	CPS	20.2.0
Support for Separate Database Collections, on page 18	CPS	20.2.0
Support for Session ID Handling, on page 18	CPS	20.2.0
Support for SLA based Policy Director Queue Buffers, on page 19	CPS	20.2.0
Support for vCenter APIs, on page 50	CPS	20.2.0
Support to Align Rollover Quota Validity Period With Recurring Quota Billing Cycle, on page 20	CPS	20.2.0
Support to Check VM Power Status, on page 51	CPS	20.2.0
Support to Configure Database Fragmentation Threshold, on page 33	CPS	20.2.0

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Support to Configure Threshold Values for Gx and LDAP Alarms, on page 34	CPS	20.2.0
Upgrade CentOS to 8.1, on page 43	CPS	20.2.0
Upgrade MongoDB from 3.6.9 to 3.6.17, on page 45	CPS	20.2.0
CLI Support to Provide Shard Information, on page 65	vDRA	20.2.0
Configurable Relay Endpoints, on page 66	vDRA	20.2.0
Extend Peer Monitoring to Rebalance Diameter Connections, on page 67	vDRA	20.2.0
Mongod Consolidated Logs Utility, on page 68	vDRA	20.2.0
Platform Health Check and Operational Improvement, on page 69	vDRA	20.2.0
Support for Dynamic Database Rate Limiting, on page 70	vDRA	20.2.0
Support for Generating Alerts for Containers in Unhealthy State , on page 71	vDRA	20.2.0
Support for Health Check Files in RAM, on page 72	vDRA	20.2.0
Support for Storage Health Check Settings, on page 73	vDRA	20.2.0
Support for Zing C2 Compiler, on page 74	vDRA	20.2.0
Support to Generate Alerts for the Docker Engine Status, on page 74	vDRA	20.2.0
Upgrade Docker Version to 19.03, on page 75	vDRA	20.2.0

20.2.0 Features and Changes



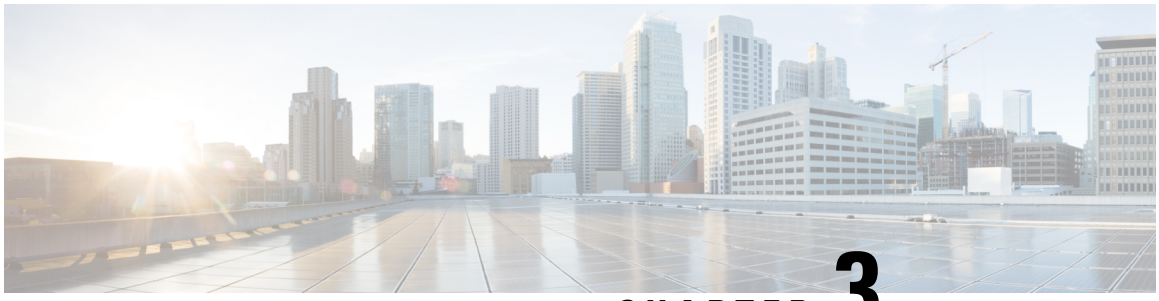
CHAPTER 2

ATS

ATS

No new features or changes were introduced in this release.

ATS



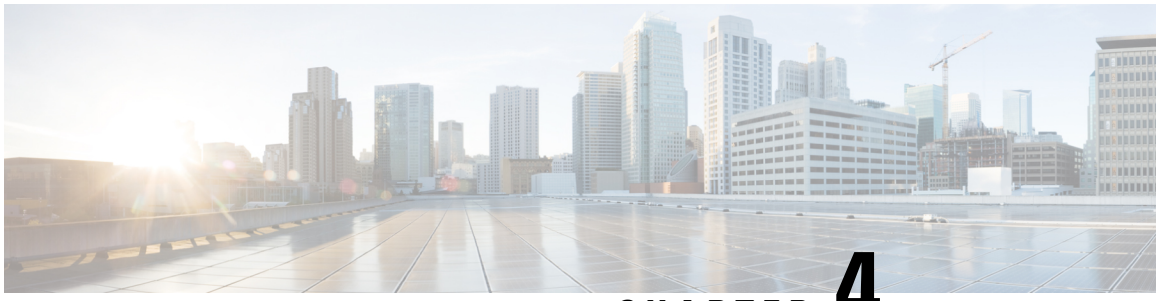
CHAPTER 3

Geographic Redundancy

Geographic Redundancy

No new features or changes were introduced in this release.

Geographic Redundancy



CHAPTER 4

Mobile

PCRF Stale Message Handling Enhancements

Feature Summary and Revision History

Table 2: 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 Mobile Configuration Guide

Table 3: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports enhancements to PCRF stale message handling. This feature enables CPS application to act according to the configuration when request processing crosses the given SLA time period for the incoming request. When the feature is enabled the request or responses which are crossing the configured SLA are dropped.

For more information, see *Stale Session Message Handling Configuration* section in the *CPS Mobile Configuration Guide*.

Support for Encoding Format

Feature Summary and Revision History

Table 4: 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 Mobile Configuration Guide

Table 5: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports encoding of the Monitoring key present in **ChargingPreconfiguredRule** based on the flag **`Encoding Format Source`** configured in **TableDrivenCharingRule** (or) **`Encoding Format`** flag configured in **PreConfiguredRule**.

For more information, see *PreConfiguredRule* and *TableDrivenChargingRule* sections in the *CPS Mobile Configuration Guide*.

Support for JMS Queue Monitoring

Feature Summary and Revision History

Table 6: Summary Data

Applicable Product(s) or Functional Area	CPS

Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 7: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports monitoring of JMS related statistics in Prometheus/Graphite databases for reporintg in Grafana. In addition to JMS statistics, JVM related statistics exported by Policy Director (LB)/Policy Server (QNS) nodes are also available for reporting.

The following JMS related statistics are added:

- node1.jms.PolicyEngineJmsSender.qns_jms_senders.MessagesSentCount
- node1.jms.PolicyEngineJmsReceiver-Cluster.qns_jms_receivers.MessagesReceived
- node1.jms.PolicyActionJmsSender.qns_jms_receivers.MessagesSentCount
- node1.jms.PolicyActionJmsReceiver-Global.qns_jms_receivers.MessagesReceived
- node1.jms.FlowControl.qns_jms_flowcontrols.NumberOfFlowControlledMessages
- node1.jms.FlowControl.qns_jms_flowcontrols.QueueSize
- node1.jms.FlowControl.qns_jms_flowcontrols.QueueSizeLimit

The following JVM related statistics are added:

- node[x].classes.gauge-loaded_classes
- node[x].classes.gauge-unloaded_classes
- node[x].thread.gauge-daemon_thread_count
- node[x].thread.gauge-live_thread_count
- node[x].thread.gauge-peak_live_thread_count
- node[x].thread.gauge-total_started_thread_count
- node[x].gc-ConcurrentMarkSweep.invocations
- node[x].gc-ConcurrentMarkSweep.total_time_in_ms-collection_time
- node[x].gc-ParNew.invocations
- node[x].gc-ParNew.total_time_in_ms-collection_time
- node[x].gc-PS_MarkSweep.invocations

- node[x].gc-PS_MarkSweep.total_time_in_ms-collection_time
- node[x].gc-PS_Scavenge.invocations
- node[x].gc-PS_Scavenge.total_time_in_ms-collection_time

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Support for Large Sessions

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	Not Applicable

Table 9: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

Previous Behavior: Currently, when CPS receives multiple application starts for one flow without the application stop, an AppInstanceId is also received by the CPS and is maintained in the list for each flow in the session object.

When the application start exceeds the maximum short value 32,767 for one flow, the list capacity is over-rolled and CPS system was unable to parse the subscriber session record from MongoDB object in the application resulted in the “Illegal Capacity -32768” exception and request failure.

New Behavior: In this release:

- For the existing subscriber sessions in MongoDB which are having AppInstanceIdList more than the capacity, CPS cannot deserialize and logs the ERROR message with sessionId information.
- For the existing subscriber session in MongoDB which are having AppInstanceIdList more than 10 and less than the capacity, CPS deserializes subscriber session successfully and considers only last pre-configured capacity AppInstanceId in the session loading.
- The AppInstanceIdList capacity is configurable. A new parameter `-DappInstanceIdListCapacity` is added in `qns.conf` file to decide the capacity of the AppInstanceIdList. The AppInstanceIdList contains the AppInstanceIds that are present in the subscriber session.

The following are the conditions:

- If the parameter value is configured <=0, then the list size is set to 10
- If the parameter value is configured > short.MAX_VALUE (32767), then the list size is set to 32766.
- If the parameter is not configured, the list size is set to the default value of 10.

- For new subscriber session records, the AppInstanceIdList will not grow beyond beyond the configured value for the AppInstanceIdList. CPS maintains only the latest AppInstanceIds in the list according to the list size capacity that is set in the configuration. Older entries are removed/ignored.

Upgrade/Migration/Backward Compatibility

By default, the feature is enabled and cannot be disabled. For the subscriber sessions having AppInstanceIdList size more than the configured capacity and less than the total capacity, only latest configured list size of the AppInstanceId entries are maintained and then forwarded.

Fresh Installation

During the fresh installation with the changes implemented, when there is a new subscriber session, the new appInstanceIds will be added to the AppInstanceIdList.

This AppInstanceIdList will store only 10 appInstanceIds which is a default size of the list.

If there are more than the configured value of the appInstanceIds as part of the session, the list will restore only the latest appInstanceIds entries which are allowed.

Support for LDAP/IOMGR Overload Handling

Feature Summary and Revision History

Table 10: 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	Contact your Cisco Account representative

Table 11: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports limiting the queue size and detect stale messages in the queue (SLA) for LDAP requests in IOMGR. Also, CPS now has the ability to apply default policy during IOMGR overload and fetch LDAP profile information when IOMGR overload stops.

To support this, you need to configure `ldap.request.queue.size` and `ldap.profile.overload.refreshtime.mins` parameters in `/etc/broadhop/qns.conf` file.

Queue size should have less value if there is very high latency in network but it is recommended to keep with default (10000) value.

For more information on `qns.conf` parameters, contact your Cisco Account representative.

Support for Real Time Notification when Rollover Occurs

Feature Summary and Revision History

Table 12: Summary Data

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

Table 13: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS supports sending Real-Time Notification when rollover occurs and the subscriber session is active. To support Real-Time notification, a new condition, *A MSBMRolloverQuota exists* is added.

Note The number of real time notifications depends on the number of RAR generated by the Policy Server (QNS) VM. If you need to increase the number of realtime notification, Max Timer T P S (under **Cluster** in Policy Builder) value has to be tuned accordingly. For more information, contact your Cisco Account representative.

Note An active Gy session should be present for balance transactions to be done on Gy. For balance transactions to be done on Gx, an active Gx session should be present.

The following attributes are present in the notification:

- IMSI
- Service ID
- Balance ID
- Quota ID
- Leftover amount that was rolled over
- Rollover Date

When rollover occurs for different rollover quotas (for same subscriber) at the same time, CPS sends a single notification with *Quota ID* as comma separated and consolidated roll-over amount. *Rollover Date* is the first start date among all rollovers happening at that time.

When multiple recurring quotas are mapped to different rollover quotas and rollover happens at different times (for example, different billcycle/expiration date), then notifications are sent individually.

CPS sends “rollover amount” in bytes.

For more information, see *A MSBMRolloverQuota exists* section in the *CPS Mobile Configuration Guide*.

The following new statistics are added:

- node[x].actions.ISendRealTimeNotificationRequest.qns_stat.avg
- node[x].actions.ISendRealTimeNotificationRequest.qns_stat.error
- node[x].actions.ISendRealTimeNotificationRequest.qns_stat.success
- node[x].actions.ISendRealTimeNotificationRequest.qns_stat.total_time_in_ms
- node[x].counters.r.n_<realtime_notification_template_name>_fail.qns_count
- node[x].counters.r.n.f_<realtime_notification_template_name>_fail.qns_count
- node[x].counters.r.n_<realtime_notification_template_name>_success.qns_count
- node[x].counters.r.n.f_<realtime_notification_template_name>_success.qns_count

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Configuration Considerations

Note All configurations mentioned below are applicable for 30 TPS per QNS. For more information, contact your Cisco Account representative.

- **Max Timer T P S:** Specifies the maximum number of internally generated transactions per second (TPS) the system produces. This parameter affects the RAR generated by CPS when they are triggered by an internal time event (change of time or quota refresh). The number of realtime notifications generated per second directly depends upon the RAR’s generated by the QNS per second. Tune this parameter as per the customer requirements.

  For more information, see *Cluster Parameters* table in the *CPS Mobile Configuration Guide*.

- **Recurring Refresh Max Delay (minutes):** The amount of time refreshing of recurring quotas are staggered across randomly, for sessions that are not actively using quota but are still established.

  This parameter is used in cases where subscribers always have a session, but is not using their quota actively. This allows staggering of recurring refreshes where you have set all their subscribers to refresh at the same time, say midnight. It avoids spiking the CPU.

  For more information, see *Balance Configuration Parameters* table in the *CPS Mobile Configuration Guide*.

- **Async Threading Configuration:** Adding specific configuration for realtime notification action prevents impact on other action threads.
  - **Action Name**: com.broadhop.notifications.actions.ISendRealTimeNotificationRequest"
  - **Action Threads:** Number of threads used to handle the notification messages in Policy Director (LB) VMs.
  - **Action Queue Size:** To hold the messages in the queue until other messages are sent.

  Note Generating realtime notification is done on the IOManager process running on Policy Director (LB). Notifications that are generated are submitted to the queue. Process pickups entry in the queue and sends it to the remote server. Since, it's an asynchronous operation, the TPS of realtime notification is not uniform (in Grafana).

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

- **`qns.conf` Parameters:**
  - `-Dbalance.recurring.refresh.broadcast=true`: Generates RAR messages on balance refresh and rollover events.
  - `-DrealtimeNotification.disableHttpPooling=true`: Increases the throughput of realtime notification messages that goes out.

  For more information on `qns.conf` parameters, contact your Cisco Account representative.

Limitations

CPS does not send notification in the following scenarios:

- If there is no active session and quota refresh time has crossed, then the quota refresh and rollover happens on the next CCR-I.
- When rollover quota is created manually through `CreateBalance API`, Real-Time notification is not triggered.
- When rollover occurs through `RolloverCredit API`, Real-Time notification is not triggered.

Support for Secondary Keys Tag Padding

Feature Summary and Revision History

Table 14: Summary Data

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

Table 15: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS is enhanced to provide the MongoDB subscriber session size to remain consistent through subscriber session life cycle.

The following are the new `qns.conf` file parameters added:

- max.tag.size
- tag.padding.char

For more information on `qns.conf` file parameter, contact your Cisco Account representative.

The following new checkbox is added under Cluster Configuration in Policy Builder.

- Session Tag Padding Configuration

For more information, see *Adding an HA Cluster* section in the *CPS Mobile Configuration Guide*.

The following new statistics are added:

- node1.counters.total_tags_added
- node1.counters.total_tags_removed
- node1.counters.session_count_exceeding_tag_size
- node1.counters.session_count_exceeding_predefined_number_of_tags
- node1.counters.total_session_with_padding
- node1.counters.total_session_without_padding

- indexSize
- storageSize
- fileSize

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Support for Separate Database Collections

Feature Summary and Revision History

Table 16: 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 Mobile Configuration Guide

Table 17: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now provides support for database collections to store the engine error logging and subscriber specific tracing data. The following parameter is added to cluster in Policy Builder.

- Suppress Error Audit Traces To Trace DB

For more information, see *Adding HA Cluster* section in the *CPS Mobile Configuration Guide*.

Support for Session ID Handling

Feature Summary and Revision History

Table 18: 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 Mobile Configuration Guide

Table 19: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now provides support to parse part of the Diameter session-Id attributes and store them in session AVP. Session Id Handling Configuration option is introduced under **Diameter Configuration** in **Policy Builder**.

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

Support for SLA based Policy Director Queue Buffers

Feature Summary and Revision History

Table 20: 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	Contact your Cisco Account representative

Table 21: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS can now handle the surge of traffic without overloading JVM memory when multiple simultaneous connections from diameter exists.

CPS now:

- Supports SLA based queue which expires and discards messages exceeding configured threshold value. If the rate of messages discarded exceeds configured threshold, then CPS generates `Disconnect Peer Request` to indicate some downstream bottleneck in handling burst of messages.

- Can apply queue threshold independently to inbound and outbound peers individually.
- Has the option to disable and fallback to legacy diameter per peer processing.

The following is the list of new `qns.conf` file parameters added:

- enable.send.receive.queue.ttl
- receive.peer.queue.ttl.ms
- send.peer.queue.ttl.ms
- max.discard.tps

For more information on `qns.conf` file parameters, contact Cisco Account representative.

The following new statistics has been added:

- rcv_ttl_drop_<*fqdn*>
- send_ttl_drop_<*fqdn*>

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Memory and Performance Impact

SLA based diameter LB queue provides better management of JVM memory and avoids OOM conditions. However, tracking of messages for SLA requires more CPU compared to legacy ThreadPoolExecutor based diameter LB queue.

Limitations

The feature should not be enabled in either of the following deployments:

- Deployment connecting to CPS over DRA which consolidates multiple diameter peers thus reducing number of peers which are connected to Policy Director (LB).
- ZING based Policy Director (LB) deployments which use sufficiently large JVM memory.

Support to Align Rollover Quota Validity Period With Recurring Quota Billing Cycle

Table 22: 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 Mobile Configuration Guide

Table 23: Revision History

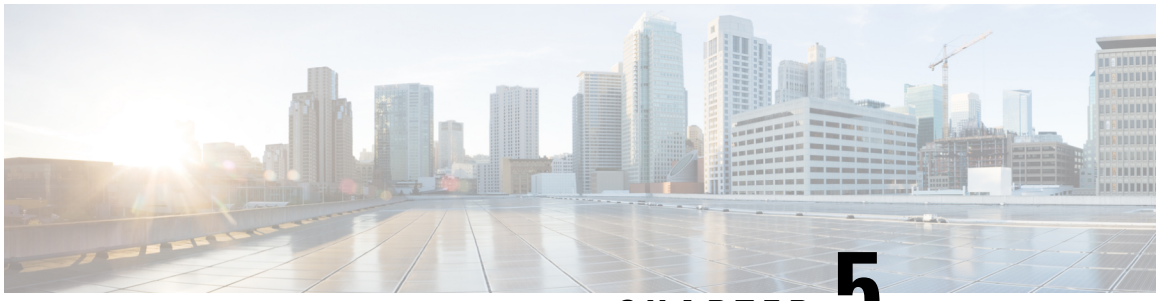
Revision Details	Release
First introduced	20.2.0

Feature Description

CPS is enhanced to support aligning Rollover Quota validity period with the Recurring Quota bill cycle. The following checkbox is provided in Policy Builder under **Recurring Quota Template**:

- Align ROQ Validity Period With RQ BillCycle

For more information, see *Recurring Quota Templates Parameters* table in the *CPS Mobile Configuration Guide*.



CHAPTER 5

Operations

API Additions or Changes

No changes were introduced in this release.

Log Additions or Changes

Enhancement on Logging and Logback

Feature Summary and Revision History

Table 24: Summary Data

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

Table 25: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports enhancements to logback xml file.

A new script `logCollector.sh` is introduced which performs the following operations:

- Provides options to enable and disable the log levels for specific components, class, and interfaces
- Collects the enabled debug logs from all VMs or Specific VMs and store provided log path.
- Displays proper error message when the user does not provide valid inputs.
- Enables alias functionality for each function which helps user to provide only the operation name which is needed to execute the script.
- Adds the timer function to ensure the collection of required logs in the amount of time passed to the script.

Logging system provides more information with exception in a user-friendly and readable format. This feature is applicable for logging messages in both Core and CustRefData modules to print the clear context of the source such as process, subsystem, and exception when occurs.

MIB Additions or Changes

No changes were introduced in this release.

SNMP Alarm Additions or Changes

The following table provides information on new/modified alarms:

Table 26: Alarm Additions or Changes

New/Modified Alarms	Release Introduced/ Modified	Applicable Product(s)/
MongoPrimaryDB fragmentation exceeded the threshold value	20.2.0	CPS
PrimaryDB fragmentation percent conforms to threshold	20.2.0	CPS
SVNnotinsync	20.2.0	CPS
SVNinsync	20.2.0	CPS
DOCKER_ENGINE_DOWN	20.2.0	vDRA

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*

Configuration for SNMP Gets and Walks

As CPS 20.2.0 is built on CentOS 8.1, `snmpwalk` command has limitations and hence cannot perform a direct snmpwalk on the OID such as .1.3.6.1.4.1.26878.200.3.2.70. Instead of snmpwalk, you need to use `snmpget` command along with the complete OID such as .1.3.6.1.4.1.26878.200.3.2.70.1.1. The list of OIDs for the individual machines are available in `/etc/snmp/snmpd.conf` file. The OIDs are part of the line containing the word proxy.

Here is an example:

```
proxy -e 0x0102030405060708 -v 3 -u cisco_snmpv3 -a SHA -m
0x71d8d544a7447e377fa5fc355d8f08f81f1a901c -x AES -m 0x71d8d544a7447e377fa5fc355d8f08f8
-l authPriv localhost .1.3.6.1.4.1.26878.200.3.2.70.1.1.0  .1.3.6.1.4.1.2021.11.9.0
```

Here .1.3.6.1.4.1.26878.200.3.2.70.1.1.0 is the OID and hence the `snmpget` must be triggered as follows:

```
snmpget -e 0x0102030405060708 -v 3 -u cisco_snmpv3 -a SHA -A cisco_12345
-x AES -l authNoPriv -m +/etc/snmp/mibs/BROADHOP-MIB.txt:/etc/snmp/mibs/CISCO-QNS-MIB.txt
lb01 ".1.3.6.1.4.1.26878.200.3.3.70.11.2.0"
CISCO-QNS-MIB::kpiLBPCRFProxyInternalCurrentSessions.0 = STRING: 0
```

For more information, see *Configuration for SNMP Gets and Walks* section in the *CPS SNMP, Alarms, and Clearing Procedures Guide*.

Statistics/KPI Additions or Changes

The following table provides information on new/modified statistics:

Table 27: Statistics Additions or Changes

Statistics Name	Description	Applicable Product(s)
node1.counters. total_tags_added	The total number of new tags added in overall sessions. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.counters. total_tags_removed	The total number of tags removed in overall sessions. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
node1.counters.session_ count_exceeding_tag_size	The total number tags exceeding the predefined size. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.counters. session_count_exceeding_ predefined_number_of_tags	The total number of sessions containing the number of tags in TagsList more than predefined size. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.counters.total_ session_with_padding	The total number of sessions created with padding. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.counters.total_ session_without_padding	The total number of sessions created without padding. The source of the statistics is Policy Server (QNS) VM.	CPS
indexSize	Indicates the total size of all indexes created on a database. The source of the statistics is Policy Server (QNS) VM.	CPS
storageSize	The total amount of space allocated to collections in database for document storage. The source of the statistics is Policy Server (QNS) VM.	CPS
fileSize	The total size (in bytes) of the data files that hold the database. This value includes pre-allocated space and the padding factor. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.jms.PolicyEngineJmsSender. qns_jms_senders. MessagesSentCount	Number of async messages sent. The source of the statistics is Policy Server (QNS).	CPS
node1.jms.PolicyEngineJmsReceiver-Cluster.qns_jms_receivers. MessagesReceived	Number of messages received. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
node1.jms.PolicyActionJmsSender. qns_jms_receivers. MessagesSentCount	Number of PolicyAction messages sent. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.jms.PolicyActionJmsReceiver- Global.qns_jms_receivers. MessagesReceived	Number of PolicyAction messages received. The source of the statistics is Policy Director (LB) VM.	CPS
node1.jms.FlowControl. qns_jms_flowcontrols. NumberOfFlowControlledMessages	Number of messages that were flow controlled. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.jms.FlowControl. qns_jms_flowcontrols.QueueSize	Flow control queue size. The source of the statistics is Policy Server (QNS) VM.	CPS
node1.jms.FlowControl. qns_jms_flowcontrols.QueueSizeLimit	Flow control queue size limit. The source of the statistics is Policy Server (QNS) VM.	CPS
rcv_ttl_drop_<*fqdn*>	Number of messages discarded due to exceeding SLA in inbound direction. The source of the statistics is Policy Director (LB) VM.	CPS
send_ttl_drop_<*fqdn*>	Number of messages discarded due to exceeding SLA in outbound direction. The source of the statistics is Policy Director (LB) VM.	CPS
node1.cdr.<CDRName>.write	Number of CDRs written to the database for the CDR name The source of the statistics is Policy Server (QNS) VM.	CPS
node1.cdr.<CDRName>.drop	Number of CDRs dropped without writing to database for the CDR name. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
node1.cdr.<CDRName>. replTaskOverrun	Number of times the replication task could not be run as the previous task was still running for the CDR name. The source of the statistics is Policy Server (QNS)/Policy Director (LB) VM.	CPS
node1.cdr.<CDRName>. replSkipNearCurrentTime	Number of times the replication task was skipped as the replication time is near current time for the CDR name. The source of the statistics is Policy Server (QNS)/Policy Director (LB) VM.	CPS
node[x].classes.gauge- loaded_classes	Number of loaded classes in the JVM. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].classes.gauge- unloaded_classes	Number of unloaded classes in JVM. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].thread.gauge- daemon_thread_count	Total number of daemon threads in the JVM. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].thread.gauge- live_thread_count	Total number of live threads in the JVM. The source of the statistics is Policy Server (QNS), Policy Director (LB) VMs.	CPS
node[x].thread.gauge-peak_ live_thread_count	Peak count of the live thread in the JVM. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].thread.gauge-total_ started_thread_count	Total number of threads started by the JVM. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].gc-ConcurrentMark Sweep.invocations	Total number of times ConcurrentMarkSweep GC occurred. The source of the statistics is Policy Server (QNS) VM.	CPS
node[x].gc-ConcurrentMarkSweep.total_ time_in_ms-collection_time	Time taken in millisecods for the ConcurrentMarkSweep GC. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
node[x].gc-ParNew. invocations	Total number of times ParNew GC occurred. The source of the statistics is Policy Server (QNS) VM.	CPS
node[x].gc-ParNew.total_ time_in_ms-collection_time	Time taken in millisecods for the ConcurrentMarkSweep GC. The source of the statistics is Policy Server (QNS) VM.	CPS
node[x].gc-PS_MarkSweep. invocations	Total number of times PS MarkSweep GC occurred. The source of the statistics is Policy Director (LB) VM.	CPS
node[x].gc-PS_MarkSweep.total_ time_in_ms-collection_time	Time taken in millisecods for the PS MarkSweep GC. The source of the statistics is Policy Director (LB) VM.	CPS
node[x].gc-PS_Scavenge. invocations	Total number of times PS Scavenge GC occurred. The source of the statistics is Policy Director (LB) VM.	CPS
node[x].gc-PS_Scavenge.total_ time_in_ms-collection_time	Time taken in milliseconds for the PS Scavenge GC. The source of the statistics is Policy Director (LB) VM.	CPS
skdb_cache_get_total. qns_stat.success	The total number of success queries on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_ total.qns_stat.error	The total number of error/fail queries on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_total. qns_stat.total_time_in_ms	The total time in millisecond to query on all SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
skdb_cache_get_ total.qns_stat.avg	The average time taken by the queries on all SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get. qns_stat.success	The number of success queries on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_ get.qns_stat.error	The number of error/fail query on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get.qns_ stat.total_time_in_ms	The total time in millisecond to query on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get. qns_stat.avg	The average number of queries on SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_remote. qns_stat.success	The total number of success queries on remote SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_ remote.qns_stat.error	The total number of error/fail query on remote SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_remote.qns_ stat.total_time_in_ms	The time in millisecond to query on remote SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_ pri.qns_stat.avg	The average number of queries on primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
skdb_cache_get_ pri.qns_stat.success	The total number of success queries on primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_ pri.qns_stat.error	The total number of error/fail query on primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri.qns_ stat.total_time_in_ms	The time in millisecond to query on primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri. qns_stat.avg	The average number of queries on primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri_ remote.qns_stat.success	The number of success queries on remote site for primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri_ remote.qns_stat.error	The number of error/fail query on remote site for primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri_remote. qns_stat.total_time_in_ms	The total time in millisecond to query on remote site for primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
skdb_cache_get_pri_ remote.qns_stat.avg	The average number of queries on remote site for primary SK database cache. The source of the statistics is Policy Server (QNS) VM.	CPS
parallel_query_ skdb_fail	Parallel query to get secondary key record from the local site secondary member if SK database fails. The source of the statistics is Policy Server (QNS) VM.	CPS

Statistics Name	Description	Applicable Product(s)
svn_status.records,1.0	This statistics shows that SVN is in sync on the pcrfclient VM's. **Note** New SVN KPI stats are added in `/var/broadhop/stats/bulk-pcrfclient-*.csv`.	CPS
svn_status.records,0.0	This statistics shows that SVN is not in sync on the pcrfclient VM's. **Note** New SVN KPI stats are added in `/var/broadhop/stats/bulk-pcrfclient-*.csv`.	CPS
node[x].actions. ISendRealTimeNotificationRequest. qns_stat.avg	Rolling 5 minute average of sending of outbound real time notifications. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].actions. ISendRealTimeNotificationRequest. qns_stat.error	Count of errors sent in outbound real time notifications. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].actions. ISendRealTimeNotificationRequest. qns_stat.success	Count of real time notifications sent out successfully. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].actions. ISendRealTimeNotificationRequest. qns_stat.total_time_in_ms	Total time in milliseconds required to sent out successful outbound realtime notifications. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].counters.r.n_ <realtime_notification_template_name> _fail.qns_count	Number of failed *<realtime_notification_template_name>* notifications sent to primary URL. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].counters.r.n.f_ <realtime_notification_template_name> _fail.qns_count	Number of failed *<realtime_notification_template_name>* notifications sent to fallback URL. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS

Statistics Name	Description	Applicable Product(s)
node[x].counters.r.n_ <realtime_notification_template_name> _success.qns_count	Number of successful <*realtime_notification_template_name*> notifications sent to primary URL. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
node[x].counters.r.n.f_ <realtime_notification_template_name> _success.qns_count	Number of successful <*realtime_notification_template_name*> notifications sent to fallback URL. The source of the statistics are Policy Server (QNS) and Policy Director (LB) VMs.	CPS
db_cpu_threshold_ breach_total	This statistics displays the total number of requests rejected/forwarded due to database CPU usage threshold breach. CCR-I requests are rejected in case of database CPU threshold breach and bindings are not marked as best effort bindings. Requests are forwarded in case of database CPU threshold breach and bindings are marked as best effort bindings. For CCR-I, bindings are not stored. For CCR-T/ Gx RAR, bindings are not deleted. Field in statistics: status = discard/forward operation = create/read/update/delete	vDRA
dra_api_binding_ sharddetails_count	Total number of shard details requests that are successful or failures. Details of field in statistics. • binding_type = session/ipv6/ipv4/imsi/msisdn • status = error_500/error_404/success	vDRA

Support to Configure Database Fragmentation Threshold

Feature Summary and Revision History

Table 28: Summary Data

Applicable Product(s) or Functional Area	CPS

Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required Default value - 40 %
Related Changes in This Release	Not Applicable
Related Documentation	CPS Operations Guide

Table 29: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports configuring custom database fragmentation threshold percentage for the list of databases present in `/etc/collectd.d/dbMonitorList.cfg` file on sessionmgr VMs. By default, the threshold is set to 40 % for all the databases in `/etc/collectd.d/dbMonitorList.cfg` file.

For more information, see *Configure Custom Database Fragmentation Threshold Percentage* section in the *CPS Operations Guide*.

Support to Configure Threshold Values for Gx and LDAP Alarms

Feature Summary and Revision History

Table 30: 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 Installation Guide for VMware CPS Installation Guide for OpenStack

Table 31: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

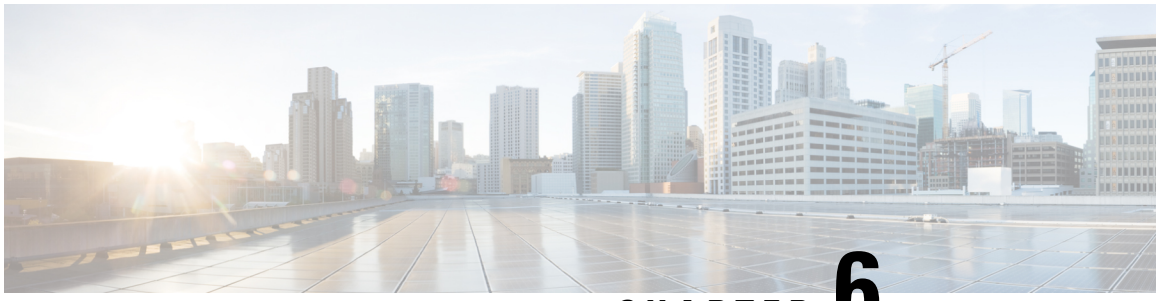
CPS now supports:

- To configure different threshold values for CCR-I/U/T response time exceeded alarms.
- To configure LDAP retry, request and result alarm threshold values using `Configuration.csv` in VMware environment and YAML file in OpenStack environment.

To support the threshold values, following parameters are added:

- Under *Configuration Parameters - HA System* section in the *CPS Installation Guide for OpenStack*:
  - gxAlarmCcrIAvgThreshold
  - gxAlarmCcrUAvgThreshold
  - gxAlarmCcrTAvgThreshold
  - ldapAlarmRetryThreshold
  - ldapAlarmCcrIReqThreshold
  - ldapAlarmResultThreshold
  - ldapAlarmRequestThreshold
- Under *General Configuration* section in the *CPS Installation Guide for VMware*:
  - gx_alarm_ccr_i_avg_threshold
  - gx_alarm_ccr_t_avg_threshold
  - gx_alarm_ccr_u_avg_threshold
  - ldap_alarm_ccr_i_req_threshold
  - ldap_alarm_request_threshold
  - ldap_alarm_result_threshold
  - ldap_alarm_retry_threshold

For more information, refer to the concerned sections in *CPS Installation Guide for OpenStack* and *CPS Installation Guide for VMware*.



CHAPTER 6

Performance Improvement

Critical Resources Monitoring in CPS using KPIs

Feature Summary and Revision History

Table 32: 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	CPS SNMP, Alarms, and Clearing Procedures Guide CPS Troubleshooting Guide

Table 33: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now provides support to monitor whether SVN on pcrfclient VMs are in sync to ensure stable operations.

A new alarm is generated as alert when SVN is not in sync and a corresponding clear alarm is triggered when SVN is in sync.

You can use the following commands to get the SVN repos and revision number details:

```
/usr/bin/svn info http://pcrfclient01/repos
/usr/bin/svn info http://pcrfclient02/repos
```

The SVN KPI is captured using whisper `.wsp` in `/var/lib/carbon/whisper/cisco/quantum/qps/pcrfclient01` location and Whisper provides details of CPU, memory, and other plugins which are defined in the `collectd.conf` file.

The following new alarms has been added:

- SVNnotinsync
- SVNinsync

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*

The following new statistics has been added:

- svn_status.records,1.0
- svn_status.records,0.0

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Enabling In-Service MongoDB Authentication

Table 34: 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 Installation Guide for OpenStack CPS Installation Guide for VMware

Table 35: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS supports enabling in-service MongoDB authentication. In case of GR/multi-cluster setups, add:

- *remote_site_ip* in the `Configuration.csv` file for VMware setups. This parameter needs to be added in both clusters.
- *remoteSiteIp* in the `YAML` file for OpenStack setups. This parameter needs to be added in both clusters.

For more information, see the following sections:

- *General Configuration* and *MongoDB Authentication Process* sections in the *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System* and *MongoDB Authentication Process* sections in the *CPS Installation Guide for OpenStack*.

Logs are available over the console and in the files:

- */var/log/broadhop/scripts/mongo_auth_upgrade.log*
- `/var/log/sessionmgr-XXXX.log` in the respective VM

Configuration and Restrictions

- Configurations need to be done in the `Configuration.csv` file.
- Encrypted password only needs to be updated.

Troubleshooting

If MongoDB processes on arbitervip are not coming up when enabling/disabling the MongoDB authentication, see *MongoDB Processes not Coming Up on Arbitervip* section in the *CPS Troubleshooting Guide*.

KPI Support to Monitor MongoDB Fragmentation and Generate an SNMP Alarm

Feature Summary and Revision History

Table 36: Summary Data

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

Related Documentation	CPS Troubleshooting Guide CPS SNMP, Alarms, and Cleaning Guide CPS Operation Guide

Table 37: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS supports new KPIs to monitor MongoDB level fragmentation in bulkstats via Grafana and to generate an SNMP alarm when MongoDB fragment percentage exceeds a specified value.

The following new alarms are added:

- MongoPrimaryDB fragmentation exceeded the threshold value
- PrimaryDB fragmentation percent conforms to threshold

For more information on alarms, see the following guides:

- *Application Notifications* table and *Clearing Procedures* chapter in the *CPS SNMP, Alarms, and Cleaning Guide*
- *Testing Traps Generated by CPS* in the *CPS Troubleshooting Guide*
- *DB Fragmentation Monitoring KPIs* and *Resync Member of a Replica Set* sections in the *CPS Operation Guide*

Optimized Secondary Binding Lookup

Feature Summary and Revision History

Table 38: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Contact your Cisco Account representative

Table 39: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS is enhanced to provide support to query on available secondary member of the local site replica-set and remote site replica-set available in local site simultaneously to get the secondary key record from SK DB.

Note

- This feature provides improvement for secondary key lookups happening on secondary sessions initiate requests in the current site and their primary sessions present in the remote site.
- In case there is any latency between the primary and secondary sites, the latency time is reduced while finding the secondary key records for secondary session initiate call processing.
- There are two parts of this feature. Both of them are optimized to reduce the processing time to match the latency between the sites.

  The current feature implementation covers the following to reduce the processing time to match the latency between the sites:

  - Optimization in existing serial or sequential query for secondary key lookup.
  - Introduction of parallel query for secondary key lookup.

The following is the list of new `qns.conf` file parameters added:

- `enable.primary.parallel.queries`
- `mongo.skdb.query.pool.size`
- `mongo.skdb.query.thread.pool.queue.size`

For more information on `qns.conf` file parameters, contact your Cisco Account representative.

The following new statistics are added:

- skdb_cache_get_total.qns_stat.success
- skdb_cache_get_total.qns_stat.error
- skdb_cache_get_total.qns_stat.total_time_in_ms
- skdb_cache_get_total.qns_stat.avg
- skdb_cache_get.qns_stat.success
- skdb_cache_get.qns_stat.error
- skdb_cache_get.qns_stat.total_time_in_ms
- skdb_cache_get.qns_stat.avg
- skdb_cache_get_remote.qns_stat.success

- skdb_cache_get_remote.qns_stat.error
- skdb_cache_get_remote.qns_stat.total_time_in_ms
- skdb_cache_get_pri.qns_stat.avg
- skdb_cache_get_pri.qns_stat.success
- skdb_cache_get_pri.qns_stat.error
- skdb_cache_get_pri.qns_stat.total_time_in_ms
- skdb_cache_get_pri.qns_stat.avg
- skdb_cache_get_pri_remote.qns_stat.success
- skdb_cache_get_pri_remote.qns_stat.error
- skdb_cache_get_pri_remote.qns_stat.total_time_in_ms
- skdb_cache_get_pri_remote.qns_stat.avg
- parallel_query_skdb_fail

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Memory and Performance Impact

When the feature is enabled, additional threads are invoked to process the parallel operation to fetch the Secondary Key records from SK DB which increases the CPU consumption by 3-4 %.

Support CPS on ESXi 6.7

Feature Summary and Revision History

Table 40: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	CPS Installation Guide for VMware

Table 41: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS is now supported on ESXi 6.7. To support CPS on ESXi 6.7, you need to install OVF tool 4.3.0 version.

Version 4.3.0 for VMware 6.5/6.7: `VMware-ovftool-4.3.0-13981069-lin.x86_64.bundle`

You can download the OVF tool from https://code.vmware.com/web/tool/4.3.0/ovf.

Upgrade CentOS to 8.1

Feature Summary and Revision History

Table 42: Summary Data

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

Table 43: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

In CPS 20.2.0 release, CentOS is upgraded to 8.1 version. With CentOS 8.1, kernel is upgraded to 4.18.0-147.5.1.el8_1.x86_64. Also, all the packages are upgraded to be compatible with CentOS 8.1.

- Network Time Protocol (NTP) is implemented using Chronyd daemon in Centos 8.1. Chronyd daemon replaces NTPD daemon. To check if the system time is synchronized, use the following commands:
  - `chronyc sources`: Displays information about the current time sources that chronyd is accessing.
  - `chronyc tracking`: Provides information about time sync status.
  - `chronyc sourcestats`: Displays information about the drift rate and offset estimation process for each of the sources currently being examined by chronyd.

For more information on Chrony, see Red Hat documentation.

Note In this release, automatic installation and configuration of NTP is added for Cluster Manager.

- Corosync package has been upgraded. Current corosync version isn't compatible with previous release corosync version. Due to corosync version incompatibility, during in-service migration (ISSM) Set1 and Set 2 VMs won't be able to form the cluster. This leads to split brain scenario during ISSM. This is transient and system recovers automatically once both Set 1 and Set 2 VMs are upgraded to new corosync version. In-service migration has been designed to migrate customer system with minimal disruption of traffic.

  Transport protocol is changed for Corosync from **udpu** to **knit**
- Puppet is upgraded from 3.6.2-3 to 5.5.19 version. Puppet code has been modified to adapt to this change. Customers are also required to test and adapt custom puppet code before applying same to CPS.
- Grafana package is upgraded from 6.2.2-1 to 6.7.1-1.
- MongoDB is upgraded to 3.6.17.
- Memcache is upgraded to 1.5.9-2.

Memory and Performance Impact

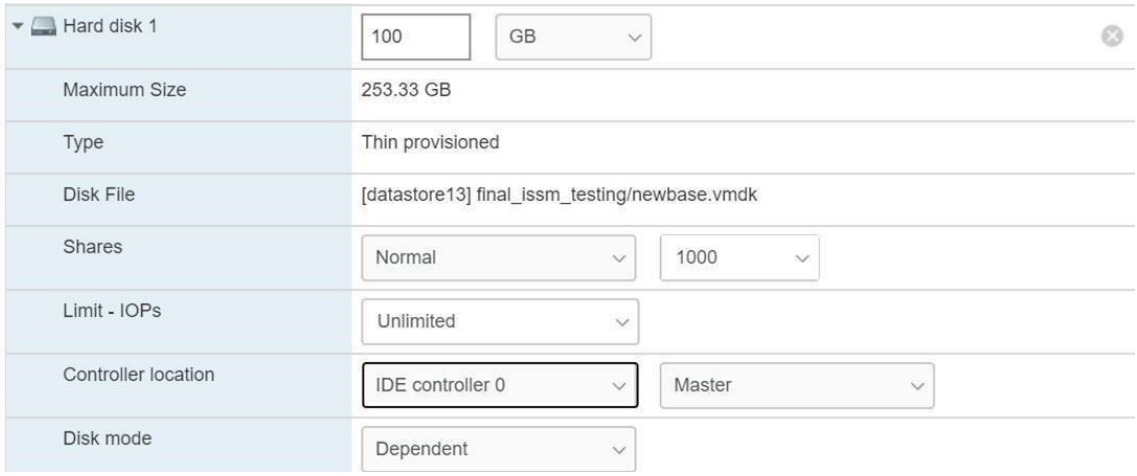
The boot time for VM has marginally increased. Also, there's a moderate increase in puppet run time during fresh installation and ISSM. For subsequent puppet runs there's no change in execution time.

Deployment Considerations

It's required to have ESXi Hosts upgraded to minimum 6.5. Controller location should be set to IDE or SCSI. For SCSI, select the SCSI Controller to VMware Paravirtual.

Note It is recommended to use SCSI controller.

The following is a sample configuration:



Upgrade/Migration/Backward Compatibility Considerations

CPS 20.2.0 is built on a newer version of CentOS. Previous versions of the CPS platform used CentOS 7; however CPS 20.2.0 uses CentOS 8.1. Because of this change, an in-service software upgrade (ISSU) is not

possible. If customers want to move to CPS 20.2.0, they must perform an in-service migration which has been designed to migrate their system with minimal disruption of traffic.

In CPS 20.2.0, puppet is upgraded from 3.6.2-3 to 5.5.19 version. Puppet code has been modified to adapt to this change. Previous release puppet code is not compatible with the current puppet version (5.5.19). Customer specific puppet code must be adapted to current release puppet version (5.5.19) before applying it to CPS 20.2.0.

VMware ESXI server must be updated to 6.5 or more.

Backup/Restore Considerations

`config_br.py` script isn't supported for backup and restoring users.

Geo-Redundancy/HA Consideration

As Corosync version is incompatible with previous release, there is traffic loss during ISSM.

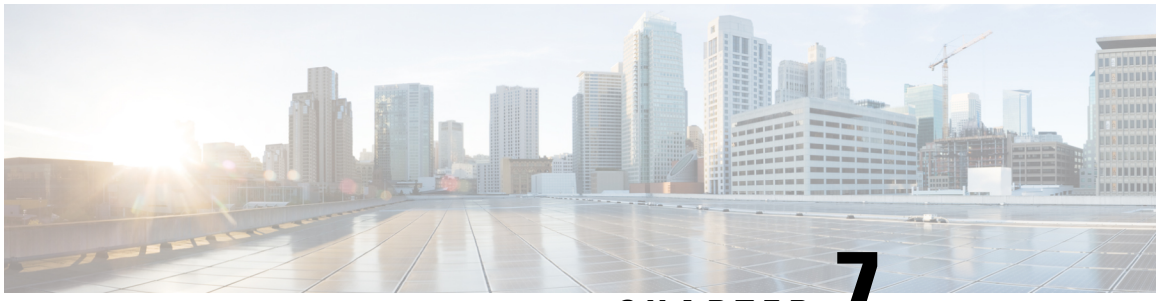
guestNic value must be configured for standalone arbiter. For more information, refer to the *CPS Geographic Redundancy Guide*.

Upgrade MongoDB from 3.6.9 to 3.6.17

In CPS 20.2.0, MongoDB has been upgraded from 3.6.9 to 3.6.17. To verify mongod is running the latest RPMs, execute the command:

```
runonall.sh 'grep "db version" /var/log/mongo* | tail -1' 2>&1 | grep 'CONTROL'
```

```
[pcrfclient02] out: /var/log/mongodb-27727.log:2018-04-09T06:28:28.207+0000 I CONTROL
[initandlisten] db version v3.6.17
[sessionmgr01] out: /var/log/mongodb-27727.log:2018-04-09T06:30:57.810+0000 I CONTROL
[initandlisten] db version v3.6.17
[sessionmgr02] out: /var/log/mongodb-27727.log:2018-04-09T06:31:43.853+0000 I CONTROL
[initandlisten] db version v3.6.17
```



CHAPTER 7

Platform

Health Check to Prevent Primary Flapping

Feature Summary and Revision History

Table 44: 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 Installation Guide for VMware CPS Installation Guide for OpenStack

Table 45: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

In GR setup, when the primary of a replica-set keeps on flapping between the sites (Site1 and Site2) because of continuous reboot scenario in Session Manager VMs, the application fails to detect the appropriate primary member for write operation which brings QNS process down.

CPS now supports health check to prevent primary flapping from impacting the remote sites.

To enable this feature in VMware environment, the flag `prevent_primary_flapping_enabled` is set to **true** in `Configuration.csv` file

To enable this feature in OpenStack environment, the flag `preventPrimaryFlappingEnabled` is set to **true** in YAML file.

Restriction

- When the local site is handling traffic, during local site reboot scenario, if the latency is more between the local and remote sites, then there may be some timeout or high response time from remote site since the PRIMARY is shifted to remote site.
- If the member state is not stable within the stipulated 300 seconds time, then the priority level is retained as 1 for those members until it becomes stable for minimum 300 seconds.
- If `mon_db*` is enabled, make sure not to enable the `prevent_primary_flapping_enabled`/`preventPrimaryFlappingEnabledflag` flag. If both the parameters are enabled in a setup, it creates conflicts in MongoDB operations.

For more information, see the following sections:

- *General Configuration Parameters* table in the *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System*, *Enable Health Check to Prevent Flapping*, and *Disable Health Check to Prevent Flapping* sections in the *CPS Installation Guide for OpenStack*

Support for HAProxy Connection Balancing

Feature Summary and Revision History

Table 46: 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 Installation Guide for VMware CPS Installation Guide for OpenStack

Table 47: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports connection transfer between the Policy Director (LB) servers in order to prevent high CPU utilization issues.

To support this, the code has been implemented to check for total number of available HAProxy servers and the total number of connections to calculate the average connection for each Policy Director (LB) HAProxy servers. Any servers handling connections more than its average threshold are evaluated and existing connections that exceed the threshold are gracefully terminated. Once the terminated connections reconnect, the HAProxy adds those connections to the next available Policy Director (LB) HAProxy server based on leastconn algorithm. However, the script also ensures that the new connections added in runtime does not exceed its average threshold value. The script has been added as a part of Monit which constantly checks HAProxy servers and initiates the script if balancing is required.

The HAProxy diameter servers diagnostic report and their total number of connections can be displayed using `diagnostics.sh` script.

On Cluster Manager, run `diagnostics.sh --ha_proxy` to fetch details of the diameter servers and the active connections.

To enable this feature in VMware environment, add `auto_haproxy_balancing_list` with the dimeter endpoints that are required for Policy Director (LB) HAProxy diameter in `Configuration.csv` file.

To enable this feature in OpenStack environment, add `autoHaproxyBalancingList` with diameter endpoint details in YAML file.

For more information, see the following sections:

- *General Configuration Parameters* table in the *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System* table in the *CPS Installation Guide for OpenStack*

Support for Multiple User Login Privileges

Feature Summary and Revision History

Table 48: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	CPS Installation Guide for OpenStack

Table 49: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports multiple user login credentials with different privileges for all non-cluman VMs in OpenStack environment. To support this, **allowUserForCluman** parameter has been added in YAML file.

Note Multiple user login credentials with different privileges for all non-cluman VMs is already supported for VMware environment.

For more information on **allowUserForCluman** parameter, refer to *Configuration Parameters - HA System* section in the *CPS Installation Guide for OpenStack*

Support for vCenter APIs

Feature Summary and Revision History

Table 50: 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 Migration and Upgrade Guide

Table 51: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now provides support to disable ESXi host SSH access for VM management and use the vCenter API calls with IT service domain authentication for vCenter users.

vCenter manages all ESXi hosts by using the vpxa and vpxd services. vCenter REST APIs are used to stop and start the services to enable the CPS deployment on the ESXi hosts managed by the vCenter.

You need to append **--nossh** to the `deploy_all.py` command to deploy VMs using VMware Rest API.

make the feature effective.

Example: `python deploy_all.py --nossh`

Note vCenter Rest API support is available from vCenter 6.5 onwards only.

Upgrade/Migration/Backward Compatibility Considerations

- **Upgrade CPS (ISSU)**: As the upgrade is initiated from Cluster Manager, the current ISSU deployment approach works after implementing the vCenter REST API deployment approach.
- **Migrate CPS (ISSM)**: Migrate procedure/steps are same as in current implementation.

For more information, see the following sections:

- *Migrate CPS Set 1 VMs* and *Migrate CPS Set 2 VMs* in the *CPS Migration and Upgrade Guide*
- `deploy_all.py` command in the *CPS Operations Guide*

Support to Check VM Power Status

Feature Summary and Revision History

Table 52: 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	CPS Operations Guide

Table 53: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports displaying the VM power state.

You need to append **--vmPowerstate** to the `python vm_utilities.py` command to check the VM power state.

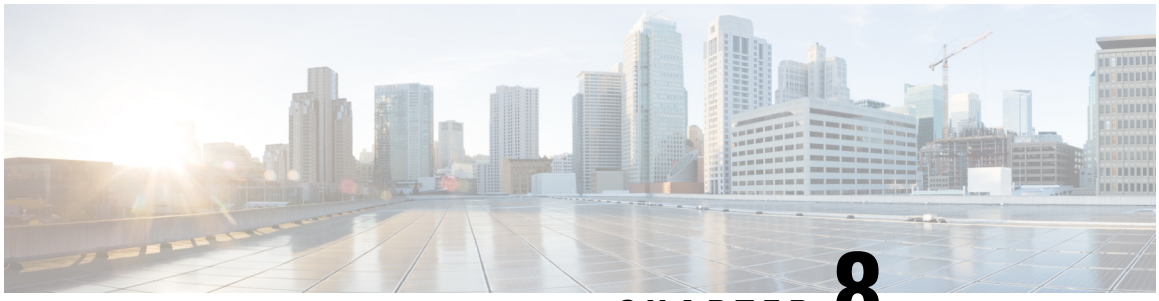
Example:

Note `python vm_utilities.py --vmPowerstate` works only with vCenter 6.5 or 6.7.

```
[root@localhost support]# python vm_utilities.py --vmPowerstate
esxi-host-1.cisco.com is reachable
esxi-host-2.cisco.com is reachable
Found a valid certificate file [/var/tmp/combined.crt] to establish a secure communication
Validated the hostname/username/password of the vCenter
```

```
Host                      Vmname                     Status
qns01                   ssh-qns01                POWERED_ON
sessionmgr02            ssh-sessionmgr02         POWERED_ON
qns02                   ssh-qns02                POWERED_ON
sessionmgr01            ssh-sessionmgr01         POWERED_ON
lb02                    ssh-lb02                 POWERED_ON
lb01                    ssh-lb01                 POWERED_ON
pcrfclient02            ssh-pcrfclient02         POWERED_ON
pcrfclient01            ssh-pcrfclient01         POWERED_ON
```

For more information, see the *vmutilities.py* section in the *CPS Operations Guide*.



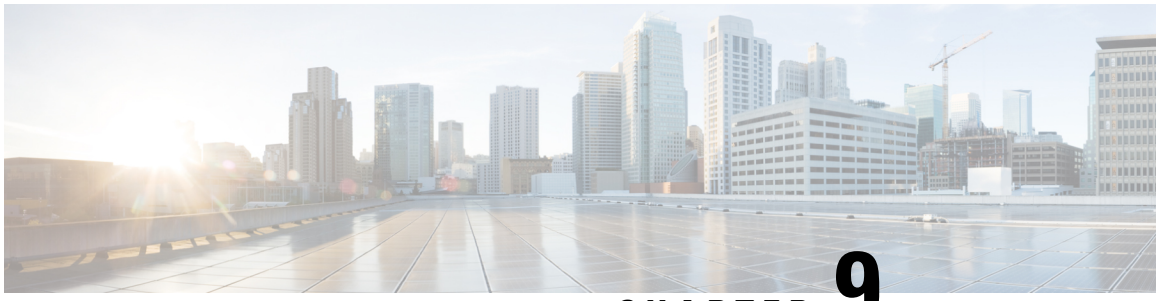
CHAPTER 8

Policy Reporting

Policy Reporting

No new features or changes were introduced in this release.

Policy Reporting



CHAPTER 9

Product Security

CentOS Security Enhancements/Kernel Upgrade

Feature Summary and Revision History

Table 54: 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 55: Revision History

Revision Details	Release
CentOS upgraded to 8.1 Kernel upgraded to 4.18.0-147.5.1.el8_1 Grafana upgraded to 6.7.1-1	20.2.0
Kernel upgraded to 3.10.0-957.12.2.el7 Grafana upgraded to 6.2.2-1	19.4.0
CentOS upgraded to 7.6 (1810) Kernel upgraded to 3.10.0-957.10.1.el7	19.3.0
Kernel upgraded to 3.10.0-957.5.1.el7	19.2.0
Kernel upgraded to 3.10.0-957.e17	19.1.0

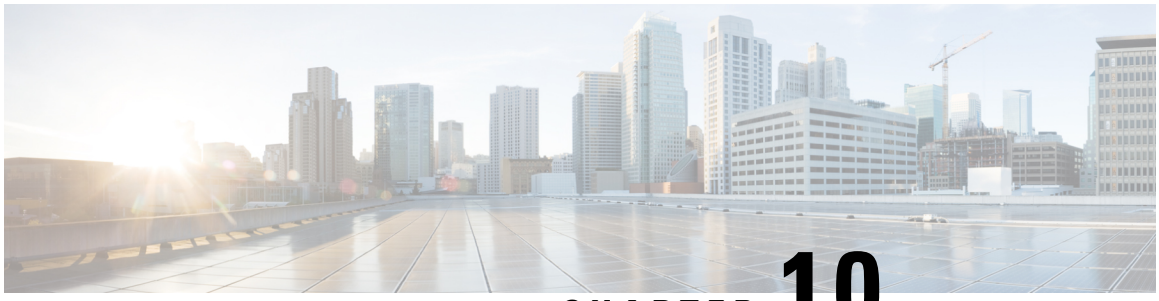
Revision Details	Release
First introduced: kernel upgraded to 3.10.0-862.14.4.el7.x86_64	18.5.0

Feature Description

In this release, the following upgrades have been done to fix the vulnerabilities:

- CentOS upgraded from 7.6 to 8.1
- Kernel upgraded from 3.10.0-957.12.2.el7 to 4.18.0-147.5.1.el8_1
- Grafana upgraded from 6.2.2-1 to 6.7.1-1

For service-related issues, you can use `journactl` to get systemctl logs.



CHAPTER 10

Security Enhancements

Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html

PSB Requirements for 20.2.0 Release

Feature Summary and Revision History

Table 56: Summary Data

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

Table 57: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports the following PSB requirements:

- Generating SHA-512 algorithm-based hash and salt credentials using OpenSSL.

- Verifying support for current TLS and SSL versions using CAVE tool.
- Verifying harden production software and infrastructure components using cloud9 audit tool.
- Making sure you allow the use of credentials specified in accordance with the credentials CPS offers.
- Deleting unnecessary information (PII).
- Utilizing prepared statements or validating user input to construct XPath queries.
- Disabling entity expansion or validating text content after expansion to prevent XML External Entity (XXE) Injection.

As a part of PSB requirements, the following is added:

- SSH timeout parameter is added. You can define `clientAliveInterval` for OpenStack setup and `client_Alive_Interval` for VMware setup to configure SSH idle timeout. By default, the value is 0 (zero).
- `-f` or `--force` option to the `change_passwd.sh` script to reset the forgotten password only from the root user.
- `generate_encrypt_password.sh` script used to generate encrypted passwords. This method can be used for fresh install and new user. Existing users and passwords will work without any problem. You need to update your old CSV/YAML files with new encrypted passwords.

  When ISSM is performed from an older release to this release, use `generate_encrypted_password.sh` script to generate the encrypted password.

  For more information, see *System Password Encryption* section in the *CPS Installation Guide for VMware*.

PSB Requirements for UI and API Issues

Feature Summary and Revision History

Table 58: Summary Data

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

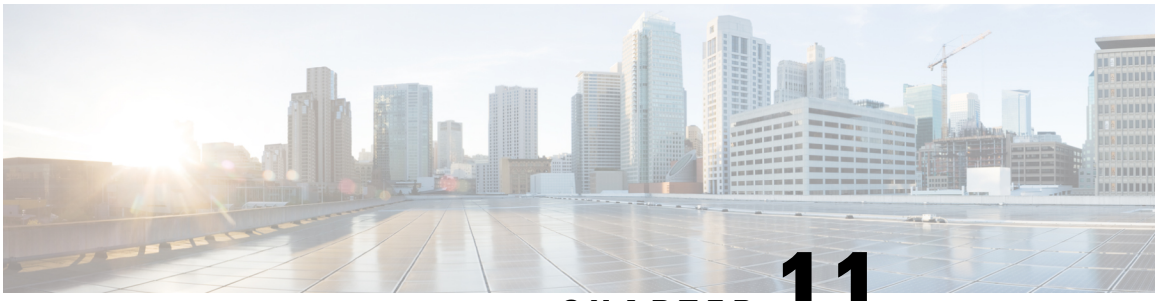
Table 59: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports the following PSB requirements:

- CPS UIs are protected against possible server path disclosure risk.
- CPS UIs are protected against Query Pattern in SSL request attack.
- Protects command processors from injecting vulnerabilities by preventing the execution of arbitrary commands or code.
- CPS UIs are protected against SQL injection.
- Policy Builder and Control Center complies with the requirement that the request headers must not contain any sensitive information.



CHAPTER 11

UI Enhancements

Enhanced BillCycle Recurrence Frequency Amount Configuration

Table 60: 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 Mobile Configuration Guide

Table 61: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports Recurrence Frequency Amount configuration while calculating Recurring Quota (RQ) next refresh date for the following conditions:

- When **Recurrence Frequency** is set as **Bill Cycle**.
- When **BillCycle Per Quota** check box is enabled.

The **Recurrence Frequency** option is changed from **Bill Cycle (RFAmt Ignored)** to **Bill Cycle**.

For more information, see *Recurring Quota Templates Parameters* table in the *CPS Mobile Configuration Guide*.

Enhanced Experimental CRD Visualization

Feature Summary and Revision History

Table 62: Summary Data

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

Table 63: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

Experimental CRD visualization tool in CPS Central user interface is modified and new enhancements are added in the current CRD to improve usability.

For more information, see *View Details of STG Element* section in the *CPS Central Administration Guide*.

Import All CRD Fallback Enhancements

Feature Summary and Revision History

Table 64: 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 Operations Guide CPS Central Administration Guide

Table 65: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports backing up of the existing CRD data and push it to SVN location(s). This backup can be used to restore cust_ref_data in case of error scenario(s) after import all.

If there is any kind of error during import all, then CPS stops the process, sets the system in BAD state and blocks CRD APIs execution. CPS also sends error response to the client stating that the system is in BAD state. If system is in BAD state and user restarts QNS/UDC server then CRD cache is built by using golden-crd data. If system BAD state is FALSE, then CRD cache is built using MongoDB.

This enhancement alerts the user about the system state and if the system state is in BAD state, then user has to restore cust_ref_data with old and working CRD by using import all API.

Default repository location for golden-crd is: `http://<IP | Hostname>/repos/golden-crd`.

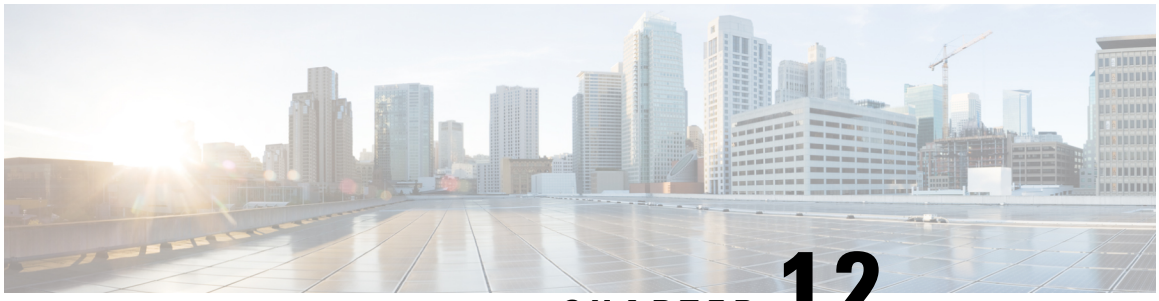
where, <*IP* | *Hostname*> is the IP addresses or hostnames for all the SVN destinations while executing export all proxy API to push existing and working CRD data into SVN.

To know the CRD version from golden-crd's metadata, execute the following command:

```
$ svn cat http://<IP | hostname>/repos/golden-crd/.metadata
```

For more information, see the following sections:

- *Export Golden CRD API* section in the *CPS Operations Guide*
- *Export Custom Reference Data* section in the *CPS Central Administration Guide*



CHAPTER 12

vDRA

CLI Support to Provide Shard Information

Feature Summary and Revision History

Table 66: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Contact your Cisco Account representative

Table 67: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

A new REST API is introduced to query shard information of given session or binding.

- API details: `https://{DRA_MASTER_IP}/dra/api/binding/shardDetails/{dbName}/{searchKey:.+}`

  where,

  DRA_MASTER_IP - DRA VNF IP

  dbName - Any one of the following values:

  - session
  - ipv4
  - ipv6
  - imsi
  - msisdn

  searchKey:.+ - Session or binding value

The following new statistics is added:

- dra_api_binding_sharddetails_count

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Configurable Relay Endpoints

Feature Summary and Revision History

Table 68: 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 vDRA Configuration Guide

Table 69: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now supports configuring realm in **Policy Builder** relay endpoints.

A new column with name **Realm** is added to support configurable relay endpoint realm name.

For more information, see *Policy DRA Relay Configuration* section in the *CPS vDRA Configuration Guide*.

Extend Peer Monitoring to Rebalance Diameter Connections

Feature Summary and Revision History

Table 70: Summary Data

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

Table 71: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

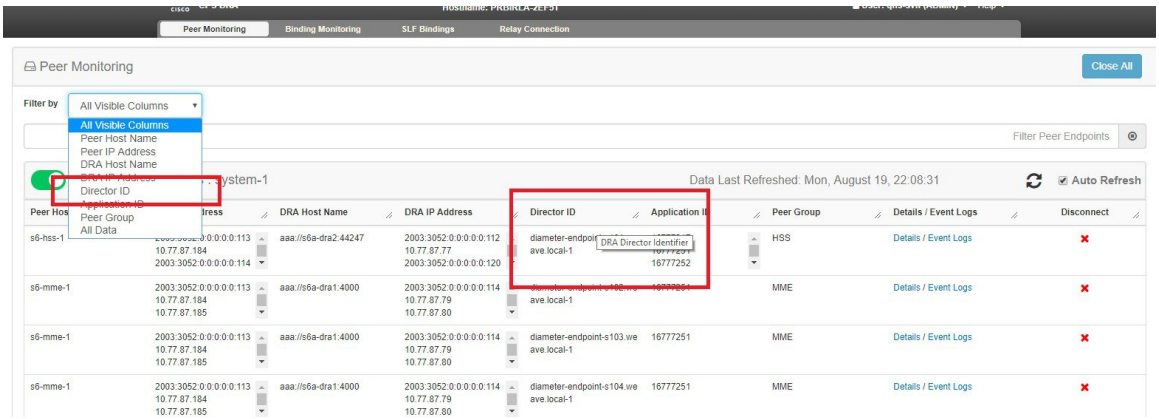
vDRA supports rebalancing the connections across the DRA Directors to make sure that if a signaling spike occurs there is CPU available to process the messages.

In order to manually rebalance DRA, you must know which connections are on which DRA Directors. This helps to figure out which connections should be disconnected to allow them to reconnect on the DRA Director with the lower number of connections.

Currently, you need to configure the Director ID manually.

Here is a sample configuration:

Figure 1: Director ID



To support extended peer monitoring, existing REST APIs are enhanced to return the peers connected to each Director instance.

- Existing “activePeerEndpoints” REST API is enhanced with additional field “instanceId”.
  - API details: `https://{DRA_MASTER_IP}/dra/api/activePeerEndpoints`
- Existing “localActivePeerEndpoints/disconnect/key/{searchKey:.+}” REST API is used to gracefully disconnect a peer connection.
  - API details:
    `https://{DRA_MASTER_IP}/dra/api/localActivePeerEndpoints/disconnect/key/{searchKey:.+}`

    Value to be provided in {*searchKey*:.+} is the key value which is returned in API call “activePeerEndpoints”.

Mongod Consolidated Logs Utility

Feature Summary and Revision History

Table 72: Summary Data

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

Table 73: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now supports collecting all the mongod log files from different VMs and create a single consolidated MongoDB log file based on the start and end timestamps which can be provided as inputs.

This feature also provides flexibility to get the consolidated view of all the MongoDB logs into a single file or collect as a single`tar.gz` file for offline analysis.

For more information, see the following sections in the *CPS vDRA Operations Guide*.

- debug collect-db-logs-advanced collect
- debug collect-db-logs-advanced scan

Limitations

- This utility can fetch logs only for the mongod instances which are running on respective sites where commands are executed.
- The log collection is limited to 15 days. If you need logs beyond 15, you must login to VM directly to pull the logs.
- Before executing `debug collect-db-logs-advanced scan` command, you need to execute `collect` command which pulls all the logs from different VMs into `tar.gz`.
- `debug collect-db-logs-advanced scan` command allows you to input timestamps in maximum of 6 hours time interval. Currently, this command expects `tar.gz` file to be present in the respective storage location and creates consolidated-log-output in same place.

Platform Health Check and Operational Improvement

Feature Summary and Revision History

Table 74: Summary Data

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

Table 75: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now:

- Supports displaying the MongoDB members status of the replica-set which runs on the orchestrator containers.
- Supports executing specific command on specific or all the containers.
- Supports dynamic deletion of bindings for a given IPv6 address range and all associated bindings. Scripts are added to delete the stale database records which are left out on the databases after applying the new configurations.

For more information, see the following commands in the *CPS vDRA Operations Guide*.

- show orchestrator-database-status
- docker exec
- database delete all-bindings-sessions zone
- database delete ipv6bindings zone

Support for Dynamic Database Rate Limiting

Feature Summary and Revision History

Table 76: Summary Data

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

Table 77: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now has the ability to throttle incoming request based on database VM CPU usage. If database VM CPU crosses threshold value, calls are rejected.

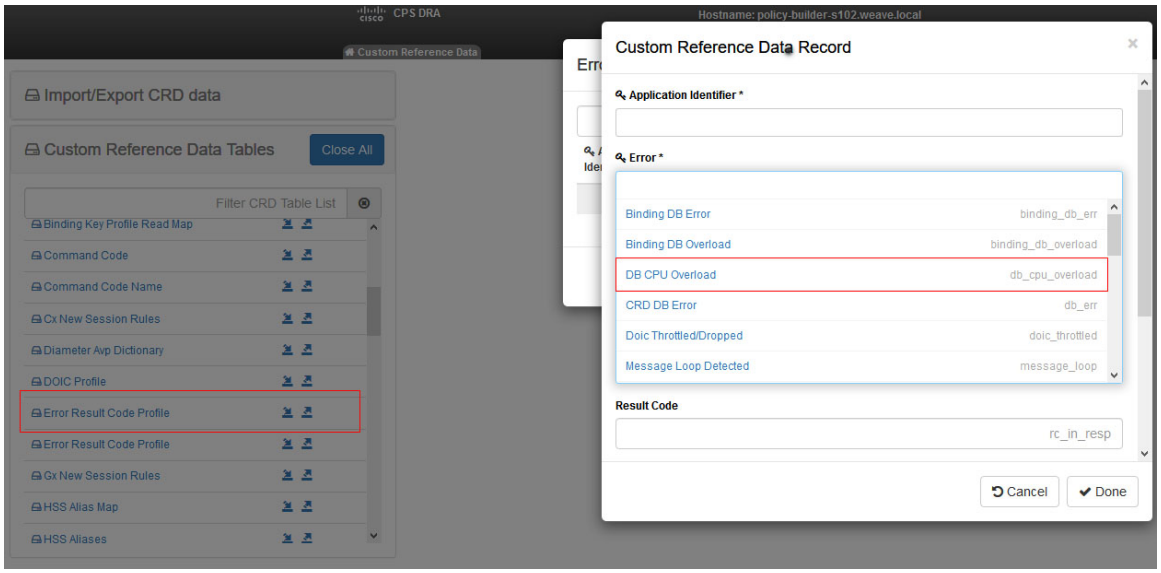
You can define CPU threshold for read database operations for write DB operations. For CLI command, see *binding throttle-db-operation* section in the *CPS vDRA Operations Guide*.

If bindings are best effort then calls are processed without performing any DB operation if CPU usage threshold is breached.

To support the feature, in **Error Result Code Profile** CRD under **Error** field, new error code **DB CPU Overload** is added.

Error profile can be configured with this value and result code that needs to be sent in response to PCEF for messages which are rejected due to DB VM CPU overload.

Figure 2: DB CPU Overload



The following new statistics has been added:

- db_cpu_threshold_breach_total.

For more information on statistics, see Statistics/KPI Additions or Changes, on page 25.

Support for Generating Alerts for Containers in Unhealthy State

Feature Summary and Revision History

Table 78: Summary Data

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

Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Contact your Cisco Account representative

Table 79: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

DRA provides support to generate alerts when the docker container state is un-healthy. The alert is resolved immediately after the container state changes to healthy.

Support for Health Check Files in RAM

Feature Summary and Revision History

Table 80: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 81: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now uses memory-based volume (“tmpfs”) in health monitoring services (keepalived, keepalived-monitor, docker-host-info, etc.) to store/track the health status information of the monitored services.

It also support migration to “tmpfs” volume upon software upgrade and fresh installation. Downgrade reverts the system back to using disk-based volumes.

Memory and Performance Impact

As tmpfs volumes are created in memory, there is an increase in the memory usage by monitoring services.

Upgrade/Migration/Backward Compatibility Considerations

Note The upgrade from non-tmpfs version to tmpfs version would disrupt the service. It is recommended that the traffic is directed to an alternate site when performing upgrade. For more information, contact you Cisco Account representative.

The feature is enabled when the system is upgraded through normal upgrade procedure.

When upgrading DRA VNF, it migrates the required health monitoring services to use tmpfs volume for health status configuration and status information.

vDRA supports migrating the required health monitoring services to use tmpfs volume for health status configuration and status information. Downgrade reverts the system back to using disk-based volumes.

Support for Storage Health Check Settings

Feature Summary and Revision History

Table 82: Summary Data

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

Table 83: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now supports the following new DRA VNF commands to to configure and control the new health check service.

- `show storage-health-check service`
- `storage-health-check service <enable | disable | restart>`
- `storage-health-check set interval <value in seconds>`
- `storage-health-check set failover-hold-time <value in seconds>`
- `Storage-health-check clear interval`

- `storage-health-check clear failover-hold-time`
- `storage-health-check service restart`
- `storage-health-check service enable`

Note Storage health check feature is supported only on director nodes and triggers VIP failover for director VIPs. Storage health check-based failover is not supported for distributor VIPs.

For more information, see the *CPS vDRA Operations Guide*.

Support for Zing C2 Compiler

Feature Summary and Revision History

Table 84: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Table 85: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now uses Azul C2 compiler JVM for director and worker nodes.

Support to Generate Alerts for the Docker Engine Status

Feature Summary and Revision History

Table 86: Summary Data

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

Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS vDRA SNMP and Alarms Guide

Table 87: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

CPS now provides support to generate alarm based on Docker Engine state when VM goes down.

The following new alarm is added:

- DOCKER_ENGINE_DOWN

For more information, see *Component Notifications* and *Sample Alert Rule Configuration* sections in the *CPS vDRA SNMP and Alarms Guide*.

Upgrade Docker Version to 19.03

Feature Summary and Revision History

Table 88: Summary Data

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

Table 89: Revision History

Revision Details	Release
First introduced	20.2.0

Feature Description

vDRA now uses latest stable docker engine version 19.03. The latest version includes fixes for open issues, security patches and some improvements.

You can check the docker by using the `docker --version` command from VM shell.

For more information, see https://docs.docker.com/engine/release-notes/.