



## **CPS Release Change Reference, Release 21.2.0 (2)**

**First Published:** 2021-08-27

**Last Modified:** 2022-01-25

### **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2022 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## PREFACE

<b>Preface</b>	<b>v</b>
About This Guide	v
Audience	vi
Additional Support	vi
Conventions (all documentation)	vi
Communications, Services, and Additional Information	vii
Important Notes	viii

---

## CHAPTER 1

<b>21.2.0 Features and Changes</b>	<b>1</b>
21.2.0 Features and Changes	1

---

## CHAPTER 2

<b>Geographic Redundancy</b>	<b>3</b>
Geographic Redundancy	3

---

## CHAPTER 3

<b>Mobile</b>	<b>5</b>
Mobile	5

---

## CHAPTER 4

<b>Operations</b>	<b>7</b>
API Additions or Changes	7
MIB Additions or Changes	7
SNMP Alarm Additions or Changes	7
Statistics/KPI Additions or Changes	8

---

## CHAPTER 5

<b>Performance Improvement</b>	<b>11</b>
Performance Improvement	11

---

**CHAPTER 6 Platform 13**

- Remove Zing from Default Deployment and Distribution Process 13
- Support for MongoDB Replication Health Monitoring 14
- VMware vSphere 7.0 Support 15

---

**CHAPTER 7 Policy Reporting 17**

- Policy Reporting 17

---

**CHAPTER 8 Product Security 19**

- Support to Restrict Application Service Ports 19

---

**CHAPTER 9 Security Enhancements 21**

- Security Enhancements 21
- PSB Requirements for 21.2.0 Release 21

---

**CHAPTER 10 UI Enhancements 23**

- UI Enhancements 23

---

**CHAPTER 11 vDRA 25**

- Archiving Journalctl Logs in DRA 25
- CLI Support for Automatic Recovery of Database Shards 27
- CLI Support for Mongo Query Function 28
- Deterministic Start with Equal Weight Priority for Director/Distributor VIP 29
- DRA Application Health Checks to Handle Traffic 30
- DRA Distributor Connection Rebalancing Support 32
- GUI to Display Policy Builder Configuration Change Summary 33
- Monitor Single Subscriber Utility (Logs) 34
- Support for Dynamic Peer Rate Limit based on DB VM CPU Usage 35
- Support PCRF Session Query for WPS messages over WPS Rest API Endpoints 37
- Support to Trigger Alarm when Logging is Stopped 38
- Trace Single Subscriber Utility (PCAP) 39



## Preface

---

- [About This Guide](#), on page v
- [Audience](#), on page vi
- [Additional Support](#), on page vi
- [Conventions \(all documentation\)](#), on page vi
- [Communications, Services, and Additional Information](#), on page vii
- [Important Notes](#), on page viii

## About This Guide



---

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

---

This document overrides the same document available in the 22.1.0. For other functionality refer to the 22.1.0 documentation at [Cisco.com](https://www.cisco.com).

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](https://www.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](mailto: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
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold</b> font.
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> 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.

Conventions	Indication
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

## 21.2.0 Features and Changes

- [21.2.0 Features and Changes](#), on page 1

## 21.2.0 Features and Changes

*Table 1: 21.2.0 Features and Changes*

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
<a href="#">Archiving Journalctl Logs in DRA</a> , on page 25	vDRA	21.2.0
<a href="#">CLI Support for Automatic Recovery of Database Shards</a> , on page 27	vDRA	21.2.0
<a href="#">CLI Support for Mongo Query Function</a> , on page 28	vDRA	21.2.0
<a href="#">Deterministic Start with Equal Weight Priority for Director/Distributor VIP</a> , on page 29	vDRA	21.2.0
<a href="#">DRA Application Health Checks to Handle Traffic</a> , on page 30	vDRA	21.2.0
<a href="#">DRA Distributor Connection Rebalancing Support</a> , on page 32	vDRA	21.2.0
<a href="#">GUI to Display Policy Builder Configuration Change Summary</a> , on page 33	vDRA	21.2.0
<a href="#">Monitor Single Subscriber Utility (Logs)</a> , on page 34	vDRA	21.2.0
<a href="#">PSB Requirements for 21.2.0 Release</a> , on page 21	CPS/vDRA	21.2.0
<a href="#">Remove Zing from Default Deployment and Distribution Process</a> , on page 13	CPS	21.2.0

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Support for Dynamic Peer Rate Limit based on DB VM CPU Usage, on page 35	vDRA	21.2.0
Support for MongoDB Replication Health Monitoring, on page 14	CPS	21.2.0
Support PCRF Session Query for WPS messages over WPS Rest API Endpoints, on page 37	vDRA	21.2.0
Support to Restrict Application Service Ports, on page 19	CPS	21.2.0
Support to Trigger Alarm when Logging is Stopped, on page 38	vDRA	21.2.0
Trace Single Subscriber Utility (PCAP), on page 39	vDRA	21.2.0
VMware vSphere 7.0 Support, on page 15	CPS/vDRA	21.2.0



## CHAPTER 2

# Geographic Redundancy

---

- [Geographic Redundancy, on page 3](#)

## Geographic Redundancy

No new features or changes were introduced in this release.





## CHAPTER 3

# Mobile

---

- [Mobile, on page 5](#)

## Mobile

No new features or changes were introduced in this release.





## CHAPTER 4

# Operations

- [API Additions or Changes, on page 7](#)
- [MIB Additions or Changes, on page 7](#)
- [SNMP Alarm Additions or Changes, on page 7](#)
- [Statistics/KPI Additions or Changes, on page 8](#)

## API Additions or Changes

No changes were introduced in this release.

## MIB Additions or Changes

No changes were introduced in this release.

## SNMP Alarm Additions or Changes



**Note** The alarms mentioned in [Table 2: Alarm Additions, on page 7](#) have not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

The following table provides information on new alarms added in the 21.2.0 release:

**Table 2: Alarm Additions**

New Alarms	Release	Applicable Product(s)
APP_SERVICE_HEALTH_STATUS_CRD	2120	vDRA
APP_SERVICE_HEALTH_STATUS_METADATA_DB	2120	vDRA

New Alarms	Release	Applicable Product(s)
VIP_NOT_ACTIVE_ ON_PREFERRED	2120	vDRA
PEER_DYNAMIC_RATE_ LIMIT_THROTTLING	2120	vDRA
NO_DB_CPU_ THRESHOLD_STATUS	2120	vDRA
QNS_LOGGING_ STOPPED	2120	vDRA

For more information, see the following sections:

- *Application Notifications* table in the *CPS vDRA SNMP and Alarms Guide*
- *Sample Alert Rules* table in the *CPS vDRA SNMP and Alarms Guide*

## Statistics/KPI Additions or Changes

The following tables provide information on new/modified statistics:

**Table 3: Statistics Additions**

Statistics Name	Description	Applicable Product(s)
app_service_health_status	Displays health status of the Application service. <b>Label:</b> service = CRD/METADATA_DB	vDRA
metadata_db_status	Displays health status of the Metadata DB. <b>Label:</b> metadata_db = drasessionsShardDB/ipv6ShardDB/ipv4ShardDB/ imsiApnShardDB/msisdnApnShardDB status = success/error Debug to be enabled: dra.stats.db	vDRA
topology_update_ msg_sent_total	The total number of messages sent for topology updates. <b>Label:</b> endpoint_revoked	vDRA



Statistics Name	Description	Applicable Product(s)
peer_dynamic_rate_limit_throttling	<p>Indicates that the dynamic throttling is applied to a peer.</p> <p><b>Label:</b> peer</p> <p><b>Value:</b> Current Throttle Percentage</p> <p><b>Type:</b> Gauge</p> <p><b>Note</b> This KPI doesn't display the entire throttling percentage. This KPI displays only the percentage of throttling applied on existing message rate limit configuration.</p> <p>For example, if current Message Rate Limit is configured to 1000 and peer_dynamic_throttling KPI value is 55, then New Message Rate limit configuration value is 450.</p>	vDRA
dra_db_cpu_message_published_total	<p>The number of DB CPU control messages published.</p> <p><b>Label:</b>system, instance, endpoint</p> <p>type=THRESHOLD_BREACH/NORMAL</p> <p><b>Type:</b> Counter</p>	vDRA
db_cpu_control_message_fail	<p>The number of DB CPU control messages publish failures.</p> <p><b>Label:</b>system, instance, endpoint</p> <p>type=THRESHOLD_BREACH/NORMAL</p> <p><b>Type:</b> Counter</p>	vDRA
processed_db_cpu_control_message_total	<p>The number of DB CPU control messages processed by Director.</p> <p><b>Label:</b>system, instance, endpoint</p> <p>type=THRESHOLD_BREACH/NORMAL</p> <p><b>Type:</b> Counter</p>	vDRA

Table 4: Statistics Modification/Changes

Statistics Name	Description	Applicable Product(s)
pcrf_binding_query_total	The total number of diameter messages that triggered PCRF session queries <sup>1</sup> .	vDRA
pcrf_api_request_duration_ms	The response time in milliseconds (ms) for REST APIs that are sent to PCRF for session queries <sup>2</sup> .	vDRA
pcrf_api_request_send_total	The total number of REST API requests sent to PCRF for session queries <sup>3</sup> .	vDRA

<sup>1</sup> New label *message\_class* is added to monitor PCRF session query for WPS messages.

<sup>2</sup> New label *message\_class* is added to monitor PCRF session query for WPS messages.

<sup>3</sup> New label *message\_class* is added to monitor PCRF session query for WPS messages.



## CHAPTER 5

# Performance Improvement

---

- [Performance Improvement, on page 11](#)

## Performance Improvement

No new features or changes were introduced in this release.





## CHAPTER 6

# Platform

- [Remove Zing from Default Deployment and Distribution Process, on page 13](#)
- [Support for MongoDB Replication Health Monitoring, on page 14](#)
- [VMware vSphere 7.0 Support, on page 15](#)

## Remove Zing from Default Deployment and Distribution Process

### Feature Summary and Revision History

*Table 5: 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 CPS Installation Guide for OpenStack

*Table 6: Revision History*

Revision Details	Release
First introduced	21.2.0

### Feature Description

In the CPS 21.2.0 release and later releases, by default, the `perf_mod` in VMware deployment and `performanceMode` in OpenStack deployment is set to 1. The Policy Builder (LB) and UDC VM's does not support Zing package installed on VMware and OpenStack. By default, QNS process is controlled by Zulu.

For more information, see the *General Configuration* table in the *CPS Installation Guide for VMware* and *Configuration Parameters- HA System* table in the *CPS Installation Guide for OpenStack*.

## Support for MongoDB Replication Health Monitoring

### Feature Summary and Revision History

**Table 7: 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 8: Revision History**

Revision Details	Release
First introduced	21.2.0

### Feature Description

CPS now supports monitoring secondary members of the replica sets and if any of them lags behind the primary member it recovers automatically. To support this functionality, a new script `auto_recovery_replica.sh` is added. The following four parameters can be configured:

- Mandatory parameter: `auto_replica_monitor`
- Optional parameters: `max_replica_lag_time`, `auto_replica_cron_hour`, `auto_replica_cron_minute`

For more information, see the *General Configuration Parameters* section in the *CPS Installation Guide for VMware* and *Configuration Parameters - HA System* section in the *CPS Installation Guide for OpenStack*.

## VMware vSphere 7.0 Support

### Feature Summary and Revision History

**Table 9: Summary Data**

Applicable Product(s) or Functional Area	CPS/vDRA
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 vDRA Installation Guide for VMware

**Table 10: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

This release provides support for VMware vSphere® 7.0 (version until 7.0.2), and the ESXi™ Hypervisor 7.0 (version until 7.0.2). For details about deploying CPS/vDRA on ESXi 7.0 (version until 7.0.2), refer to the *CPS Installation Guide for VMware* and *CPS vDRA Installation Guide for VMware* respectively.

For more details about VMware vSphere 7.0, refer to <https://docs.vmware.com/en/VMware-vSphere/index.html>.







## CHAPTER 7

# Policy Reporting

---

- [Policy Reporting](#), on page 17

## Policy Reporting

No new features or changes were introduced in this release.





## CHAPTER 8

# Product Security

- [Support to Restrict Application Service Ports](#), on page 19

## Support to Restrict Application Service Ports

### Feature Summary and Revision History

**Table 11: 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 12: Revision History**

Revision Details	Release
First introduced	21.1.0

### Feature Description

**Previous Behavior:** In CPS 21.1.0 and earlier releases,

- Policy Director (LB) VMs accepted Rsyslog requests on both internal and external interface (port 5544 and 6514).

- Whisper server default port 9213 and Zookeeper port 2181 listened on all the interfaces that exposed the system to vulnerable attacks for service.

**New Behavior:** In CPS 21.2.0 and later releases, CPS restricts application service ports to only internal network.

- Product Security access is restricted through external interfaces for Rsyslog requests.
- Whisper service is bound to internal interface thus restricting external access.
- Rsyslog, Whisper, and Zookeeper allows only one bind address. Either IPv4 or IPv6 is supported as IP address.

You can now find that the Rsyslog and Whisper are now deployed using the internal interfaces. The ports connectivity will now work only using the internal IP address and the same can be verified using the `telnet` command.

```
telnet <internalIP> 5544 - rsyslog
telnet <internalIP> 6514 - rsyslog
telnet <internalIP> 9213 - whisper
telnet <internalIP> 2181 - zookeeper
```



## CHAPTER 9

# Security Enhancements

- [Security Enhancements](#), on page 21

## 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 21.2.0 Release

### Feature Summary and Revision History

**Table 13: Summary Data**

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

**Table 14: Revision History**

Revision Details	Release
First introduced	21.2.0

### Feature Description

CPS PCRf meets the Cisco security guidelines and is aligned with the security features for 21.2.0 release. CPS now supports the following PSB requirements:

**Table 15: CPS PSB Requirements**

PSB Item	Description
CT1885: SEC-SW-SIG-4:	Digitally sign software and control the keys.
CT1975: SEC-CRY-PRIM-6	Use approved cryptographic primitives and parameters.
CT1900: SEC-SW-INSCHK	Check software signatures at installation time.
CT1977: SEC-SUP-PATCH-2	Propagate upstream security patches.
CT1973: SEC-AUT-AUTH-6	Authenticate and authorize remote agents seeking access.
CT1965: SEC-CRY-SNMP	Support SNMPv3 with cryptographic encryption and authentication.

### Feature Description

CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 21.2.0 release. vDRA now supports the following PSB requirements:

**Table 16: CPS vDRA Requirements**

PSB Item	Description
CT1977: SEC-SUP-PATCH-2	Propagate upstream security patches.
CT1975: SEC-CRY-PRIM-6	Use approved cryptographic primitives and parameters.
CT1900: SEC-SW-INSCHK	Check software signatures at installation time.
CT1885: SEC-SW-SIG-4	Digitally sign software and control the keys.
CT1973: SEC-AUT-AUTH-6	Authenticate and authorize remote agents seeking access.
CT1972: SEC-AUT-API-3	Use authentication and authorization to protect the API service offerings.
CT1965: SEC-CRY-SNMP	Support SNMPv3 with cryptographic encryption and authentication.
CT667: SEC-LOG-INDC-2	Indicates the status at login.
CT479:SEC-SW-SIGCUST	Allow customers to sign software.



# CHAPTER 10

## UI Enhancements

---

- [UI Enhancements, on page 23](#)

## UI Enhancements

No new features or changes were introduced in this release.







# CHAPTER 11

## vDRA

- Archiving Journalctl Logs in DRA, on page 25
- CLI Support for Automatic Recovery of Database Shards, on page 27
- CLI Support for Mongo Query Function, on page 28
- Deterministic Start with Equal Weight Priority for Director/Distributor VIP, on page 29
- DRA Application Health Checks to Handle Traffic, on page 30
- DRA Distributor Connection Rebalancing Support, on page 32
- GUI to Display Policy Builder Configuration Change Summary, on page 33
- Monitor Single Subscriber Utility (Logs), on page 34
- Support for Dynamic Peer Rate Limit based on DB VM CPU Usage, on page 35
- Support PCRF Session Query for WPS messages over WPS Rest API Endpoints, on page 37
- Support to Trigger Alarm when Logging is Stopped, on page 38
- Trace Single Subscriber Utility (PCAP), on page 39

## Archiving Journalctl Logs in DRA

### Feature Summary and Revision History

**Table 17: 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	CPS vDRA Operations Guide

Table 18: Revision History

Revision Details	Release
<p>First introduced</p> <p><b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.</p>	21.2.0

### Feature Description

In vDRA, Docker engine is configured with [journalld](#) logging driver on every VM. The journalld logging driver sends container's logs to journal daemon.

Use the **journalctl** command, through journal API, or use the **docker logs** command to systemd journal to retrieve the log entries.

As part of the logging enhancements, vDRA supports retaining of journalctl logs for longer duration around 10 days on all VMs. This helps in debugging any issues even though journal logs gets rolled over early.

All the logs are captured through automated cron job at daily basis on nonpeak time and cronjob timings are configurable through cron job file. The collected logs are stored under `/data/journal-logs` directory on each VM and also stored at remote server. You can configure the size of the logs folder and days of retention in the configuration file.

On every VM, log collection happens based on disk size of the `/data/journal-logs` folder, Default `/data/journal-logs` directory size is 10GB. If the `/data/journal-logs` directory size is less than 10GB it will collect the logs and it will copy to the Control VM and remote server, If the `/data/journal-logs` directory size exceeds to 10 GB , `journal.sh` script deletes files beyond 2 days to free up the disk space on the VM. This parameter is also configurable from `cps-journal.conf` file.

You can configure the retention days and size of log storage folder on `/etc/cps/cps-journal.conf` file. And copying journal logs to Control VM works with static and Virtual VIP IP.

While copying the journal logs to a control VM, `journal.sh` script checks the / disk usage on control VM. If the disk size is less than 60 % it copies files to the control VM, otherwise it won't copy and these log files are stored on same VM based on the retention period. This disk usage value for Control VM is configuration through `cps-journal.conf` file.

For the CPU usage optimization, this script is limited to execute with only 50 % of the system CPU.

For more information, see *Retaining journalctl Logs in DRA* section in the *CPS vDRA Operations Guide*.

# CLI Support for Automatic Recovery of Database Shards

## Feature Summary and Revision History

**Table 19: 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 CPS vDRA Troubleshooting Guide

**Table 20: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

## Feature Description

In 21.2.0 and later releases, support is added to recover single/multiple/all shards and metadata database using CLI.

The following new CLI commands are added to recover shards:

- `database repair <clustername> <shardname>`
- `database repair <clustername> <shardname1> <shardname2> <shardname3>`
- `database repair <clustername> All`
- `database repair <clustername> sharddb`

For more information, see the following sections:

- *database repair* in the *CPS vDRA Operations Guide*
- *Recovery Using database repair Command* in the *CPS vDRA Troubleshooting Guide*

## CLI Support for Mongo Query Function

### Feature Summary and Revision History

**Table 21: 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 22: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

In CPS Diameter Routing Agent (DRA), you can query the database in Mongo Sharding with the help of Mongo router VM. In case, the VM is removed as a part of App sharding, the capability to query all shards for specific conditions is lost. To overcome this situation, DRA supports new orchestrator CLI for App sharding queries..

If the database record count is less than or equal to 5, then the record is displayed as CLI output, otherwise it is saved to a file. For the required number of records provide maximum value and find corresponding records in `/data/config/Query.log`. All database queries runs on Secondary DB instances to avoid major performance impact.

For more information, see *database query* section in the *CLI Commands* chapter in *CPS vDRA Operations Guide*.

## Deterministic Start with Equal Weight Priority for Director/Distributor VIP

### Feature Summary and Revision History

**Table 23: 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	CPS vDRA SNMP and Alarms Guide CPS vDRA Operations Guide

**Table 24: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

The Deterministic Start with Equal Weight Priority for VIP feature prevents the automatic second failover when the preferred or high priority director or distributor is back online. This feature provides `vip-failover` CLI command to do VIP failover which ensures that the high priority director or distributor owns the VIP.

This feature provides the option to configure VIPs with different weight or priorities with a **nopreempt** option set to true.

The deterministic start is decided based on the host priority in VIP configurations. Higher priority host is preferred to own the VIP initially. If the VIP is not present in the preferred director or distributor, an SNMP alarm is triggered. `vip-failover` CLI command is used to move the VIP to the preferred director or distributor.

For more information, see *vip-failover* section in the *CPS vDRA Operations Guide*.

The following new alarm is added:

- VIP\_NOT\_ACTIVE\_ON\_PREFERRED

For more information, see the following tables in the *CPS vDRA SNMP and Alarms Guide*.

- *Application Notifications*
- *Sample Alert Rules*

## DRA Application Health Checks to Handle Traffic

### Feature Summary and Revision History

**Table 25: 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 Administration Guide CPS vDRA SNMP and Alarms Guide

Table 26: Revision History

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

CRD, Metadata DB connectivity, and Consul failures lead to improper processing of the Diameter messages in the Worker node. To enhance product resiliency in the Worker CRD failure, Worker Metadata DB, and Worker consul readiness scenarios, vDRA supports health checks to ensure that all prerequisites are met before Diameter messages are processed by that node.

The following validations are done during Binding/Diameter application initialization.

- CRD validation for Diameter and binding initiation
- Metadata DB access check from binding node
- Consul health check during Binding/Diameter application initialization

For more information, see *DRA Health Checks* section in the *CPS vDRA Administration Guide*.

The following new statistics are added to track the DRA health checks:

- app\_service\_health\_status
- metadata\_db\_status
- topology\_update\_msg\_sent\_total

For more information on statistics, see [Statistics/KPI Additions or Changes, on page 8](#).

The following new alarms are added to track the DRA health checks:

- APP\_SERVICE\_HEALTH\_STATUS\_CRD
- APP\_SERVICE\_HEALTH\_STATUS\_METADATA\_DB

For more information, see the following tables in the *CPS vDRA SNMP and Alarms Guide*.

- *Application Notifications*
- *Sample Alert Rules*

# DRA Distributor Connection Rebalancing Support

## Feature Summary and Revision History

**Table 27: 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 Administration Guide CPS vDRA Operations Guide

**Table 28: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

## Feature Description

DRA distributor rebalances the existing active connections across all available directors through CLI commands. The rebalancing allows:

- Equal distribution of connections on all available directors
- Recommendation of number of peers that are disconnected from each director where there are more active connections.
- Ensures graceful disconnect of peers on directors with more connections and on reconnect, same peers gets distributed to other directors that has less number of connections.



Distributor connection balancing uses the following CLIs:

- **dra-distributor balance connection** *cluster-name service-name*
- **dra-distributor balance connection** *cluster-name service-name audit*

For more information, see the following:

- *Balancing Distributor Connections* section in the *CPS vDRA Administration Guide*
- *dra-distributor balance connection* and *dra-distributor balance traffic* sections in the *CPS vDRA Operations Guide*

## GUI to Display Policy Builder Configuration Change Summary

### Feature Summary and Revision History

**Table 29: 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	CPS vDRA Configuration Guide

**Table 30: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

The DRA currently supports collection of SVN log commit messages with summary of Policy Builder (PB) publish changes, differences between revisions by executing the commands directly on the container.



**Note** In CPS 21.1.0 and earlier releases, SVN logs were verified in the SVN container using `svnlog http://svn/repos/<repo-name>-v` command.

For example:

```
root@svn:/# svn log http://svn/repos/<repo> -v
```

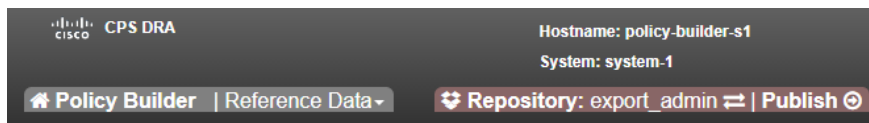
```
-----
r468 | admin | 2021-05-05 04:18:50 +0000 (Wed, 05 May 2021) | 1 line
Changed paths:
```

```
  M /peer_mismatch/.broadhopFileRepository
```

```
  M /peer_mismatch/DRAConfiguration-_XqSCsFInEeW_YtnMevZ4Fg.xmi
```

This feature enhances the Policy Builder UI which allows the user to view and save the history of the repository changes such as, revision number, timestamp, username, commit messages, files impacted and the differences between the two adjacent revisions.

**Figure 1: SVN Repository Changes**



## DRA Policy Builder Overview

### Reference Data

Data referenced from services or used for system wide configuration

- Environment specific data
  - Systems for initial setup of environment.
- Custom Reference Data Schemas
  - Search Table Groups allow setting custom reference data for installation
  - Custom Reference Data Tables are basic tables without search functionality
- Diameter Application specific data
  - Diameter Applications
- Routing AVP
  - Routing AVP Definitions
- SVN repository changes
  - History of configuration changes

For more information, see *SVN Repository Changes* section in the *CPS vDRA Configuration Guide*.

# Monitor Single Subscriber Utility (Logs)

## Feature Summary and Revision History

**Table 31: 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 Administration Guide

Table 32: Revision History

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

CPS vDRA traces the flow of a message from a single subscriber, including Policy Builder STG lookup, CRD tables and route rules used, VM/containers, systems traversed, DB lookups performed with results, and so on to show the successful (or failed) transmissions. In the CPS 21.2.0 release, vDRA monitors live logs for single subscriber activities based on IMSI/MSISDN/IPv6.

For more information, refer to the *Monitoring Single Subscriber Activity* section in the *CPS vDRA Administration Guide*.

## Support for Dynamic Peer Rate Limit based on DB VM CPU Usage

### Feature Summary and Revision History

Table 33: 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 Configuration Guide CPS vDRA SNMP and Alarms Guide

Table 34: Revision History

Revision Details	Release
First introduced	21.2.0
<b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	

### Feature Description

Overload conditions on binding databases occurs when CCR-I or CCR-T bursts over one or more peer connections, thereby destabilizing the system. vDRA supports the following mechanisms to protect the system from such an overload condition:

- Dynamically vary peer message rate limits (CCR-I/T) based on DB CPU load to enable better utilization of available DB capacity.
- Selectively throttle peer connections with traffic burst and continue processing of messages for peers with BAU traffic.

Configure Message Rate Limit profile to throttle messages on the Director and rate limits for each message type in the profile. Dynamic rate limiting allows you to:

- Determine the available DB capacity and dynamically derive the rate limits.
- Configure preferred rate limits and apply dynamic throttling on configured values.

For more information, see *Dynamic Peer Rate Limit based on DB VM CPU Usage* section in the *CPS vDRA Configuration Guide*

The following new statistics are added:

- peer\_dynamic\_rate\_limit\_throttling
- dra\_db\_cpu\_message\_published\_total
- db\_cpu\_control\_message\_fail

- processed\_db\_cpu\_control\_message\_total

For more information on statistics, see [Statistics/KPI Additions or Changes](#), on page 8.

The following new alarms are added:

- PEER\_DYNAMIC\_RATE\_LIMIT\_THROTTLING
- NO\_DB\_CPU\_THRESHOLD\_STATUS

For more information, see the following tables in the *CPS vDRA SNMP and Alarms Guide*.

- *Application Notifications*
- *Sample Alert Rules*

## Support PCRF Session Query for WPS messages over WPS Rest API Endpoints

### Feature Summary and Revision History

**Table 35: 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 Configuration Guide

**Table 36: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

vDRA is enhanced to send WPS/non-WPS IPv6 binding queries to PCRF with different DSCP value and receive SRK information to route the Rx AAR messages.

vDRA allows the following functionalities:

- Separate REST API endpoint configurations to support WPS IPv6 binding queries.
- WPS REST API endpoints selection to query IPv6 binding for all WPS messages and non-WPS messages.
- PCRF session query for WPS Rx AAR messages is set with configured DSCP value as 47.
- PCRF session query for non-WPS RX AAR messages is set with configured DSCP value as 32.
- Attribute class:wps set up to the payload for all WPS PCRF session queries.
- Fallback to non-WPS PCRF REST API endpoints. This is to get session route key information for WPS Rx AAR messages when there is any issue in sending query with WPS PCRF REST API endpoints or WPS PCRF REST API endpoints not configured.

For more information, see *PCRF Session Query for WPS Messages* section in the *CPS vDRA Configuration Guide*.

The following statistics are modified:

- pcrf\_binding\_query\_total
- pcrf\_api\_request\_duration\_ms
- pcrf\_api\_request\_send\_total

For more information on statistics, see [Statistics/KPI Additions or Changes, on page 8](#).

## Support to Trigger Alarm when Logging is Stopped

### Feature Summary and Revision History

**Table 37: 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 SNMP and Alarms Guide
-----------------------	--------------------------------------

**Table 38: Revision History**

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

**Feature Description**

In 21.2.0 and later releases, support is added to trigger an alarm to notify the user when application has stopped logging consolidated-qns logs unexpectedly.

The following new alarm is added:

- QNS\_LOGGING\_STOPPED




---

**Note** If there is no activity on the system, and an alarm is raised, it is expected and is resolved automatically when application activity starts.

---

For more information, see the following tables in the *CPS vDRA SNMP and Alarms Guide*.

- *Application Notifications*
- *Sample Alert Rules*

## Trace Single Subscriber Utility (PCAP)

**Feature Summary and Revision History****Table 39: 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 Administration Guide

Table 40: Revision History

Revision Details	Release
First introduced  <b>Important</b> This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.2.0

### Feature Description

CPS vDRA stores audit logs based on modules. If you enable the debug or trace logging function, CPS vDRA stores detailed logs for all the subscribers and modules which fills the logs and rotates it quickly. In order to avoid this filling of logs, vDRA is enhanced to support tracing function of incoming and outgoing messages for a single subscriber.

The main functions are:

- vDRA captures diameter request and response messages across all vDRA sites for a single subscriber and stores all messages in configured DB in PCAP format.
- Captures Request and Answer messages as received from the peer and as sent to the peer on ingress and egress director, respectively.
- Starts or stops the trace by getting the subscriber identity, which is IMSI/MSISDN/IPv6.
- Retrieves the PCAP based on the subscriber identity. By default, vDRA stores the PCAP in admin-db.
- vDRA allows you to configure any other MongoDB URI to store the PCAP.

For more information, refer to the *Tracing and Monitoring Single Subscriber Activities* section in the *CPS vDRA Administration Guide*.