CPS Release Change Reference, Release 23.2.0

First Published: 2023-08-24

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 NONINFRINGEMENT 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.

CONTENTS

PREFACE

Preface

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 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.

Conventions	Indication
[ ]	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

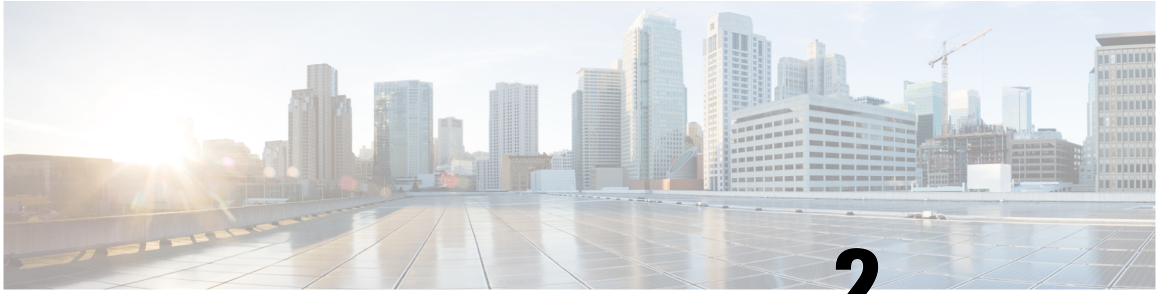
23.2.0 Features and Changes

23.2.0 Features and Changes

Table 1: 23.2.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Apply Filter for Specific Column in CRD Table, on page 15	vDRA	23.2.0
Create and Manage API Dedicated User, on page 16	vDRA	23.2.0
Debug Log Collection Statistics Support, on page 17	vDRA	23.2.0
Display Last Published Repository in Policy Builder, on page 18	vDRA	23.2.0
Error Code Classification per Peer/End Node in Grafana, on page 18	vDRA	23.2.0
Limit Permissions to Subset of CRD Tables, on page 19	vDRA	23.2.0
Support Alerts for Monitoring Primary DB, on page 20	vDRA	23.2.0
Support TLS for Gy and Sy, and MTLS Support for Diameter Application, on page 21	vDRA	23.2.0
PSB Requirements for 23.2.0 Release, on page 13	CPS/vDRA	23.2.0
Upgrade Alma Linux to 8.7, on page 9	PCRF	23.2.0

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Congestion Handling during OCS Failure, on page 3	PCRF	23.2.0
Support for VoLTE-IR, on page 4	PCRF	23.2.0



CHAPTER 2

Mobile

Congestion Handling during OCS Failure

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	Not Applicable

Table 3: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

CPS supports the congestion handling by introducing a **Re-initiation Queue** during OCS failure in PCRF.

When the OCS is unresponsive, all the messages towards that OCS have failure result code. These messages are re-initiated and put into the **Re-initiation Queue**. This leaves an open space in the existing queue and used for processing the messages towards other OCS. By default, the feature is disabled.

The following configuration in the `/etc/broadhop/qns.conf` file enables or disables the feature:

```
-Denable.udc.sy.reinit.queue=true/false
```

For more information, see the *CPS UDC Administration Guide* and *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Generating Valid MAC Address to Boot the VM

Behavior Change Summary and Revision History

Table 4: Summary Data

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

Table 5: Revision History

Revision Details	Release
First Introduced.	23.2.0

Behavior Change

Run the genmac.py script to assign the MAC address to the VMs. If the VMs are not rebooting, it is because of the invalid MAC address. Updating the fourth octet range from 7F to 3F generates a valid MAC address for VMs.

Previous Behavior:

The starting range of fourth octet in the MAC address was 7F.

```
Old Range : 00:50:56:00:00:00 - 00:50:56:7F:FF:FF
```

New Behavior:

The starting range of fourth octet in the MAC address is 3F.

```
New Range : 00:50:56:00:00:00 - 00:50:56:3F:FF:FF
```

Customer Impact:

The VMs will not boot when you use the old genmac.py script. Use the correct range to generate the valid MAC address.

Support for VoLTE-IR

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 6: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

CPS supports the VoLTE for international roaming (IR) by sending the 3GPP-SGSN-MCC-MNC AVP in the Rx AAA message to P-CSCF and subscribe the **PLMN_CHANGE** event trigger.

The following statistics verify the **PLMN_CHANGE** in Gx and Rx interfaces:

- **Gx CCR-I with 3GPP-SGSN-MCC-MNC value**
- **Rx AAR with PLMN_CHANGE**
- **Rx AAA with 3GPP-SGSN-MCC-MNC value**
- **Gx RAR with PLMN_CHANGE subscribe to event trigger**
- **Gx CCR-U with updated 3GPP-SGSN-MCC-MNC value**
- **Rx RAR with updated 3GPP-SGSN-MCC-MNC value**

For more information, see *Rx Services* chapter in *CPS Mobile Configuration Guide*.

CHAPTER 3

Operations

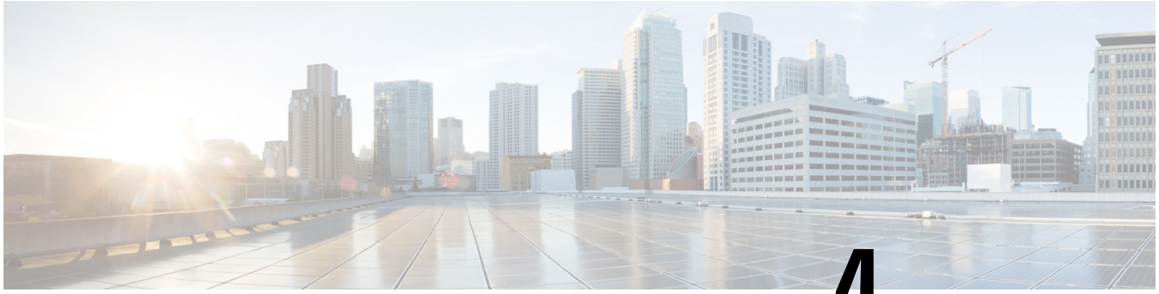
Statistics/KPI Additions or Changes

The following table provides information on new/modified statistics:

Table 7: Statistics Additions

Statistics Name	Description	Applicable Product(s)
mongo_primary_reachable	The parameter is extended with preferredprimary, and seed labels to track the seed server values.	vDRA
peer_message_total	The parameter is extended with the destination_host, destination_realm, and peer_group labels to display the specific errors of peer traffic respectively.	vDRA
node[x].actions.send.reinit.diameter_Sy_SLR.qns_stat.error	Erred actions count, for reinitiated SLR messages.	UDC

Statistics Name	Description	Applicable Product(s)
node[x].actions.send.reinit.diameter_Sy_SLR.qns_stat.success	Success actions count, for reinitiated SLR messages.	UDC
node[x].actions.send.reinit.diameter_Sy_SLR.qns_stat.total_time_in_ms	Total milliseconds of successful actions, for reinitiated SLR messages.	UDC
node[x].actions.send.reinit.diameter_Sy_SLR.qns_stat.avg	Rolling five minutes average of successful executed actions, for reinitiated SLR messages.	UDC
node[x].counters.Sy_Action_Reinitiate.qns_count	When congestion handling feature is enabled, the counter can also be considered as messages submitted to Re-initiation queue.	UDC



CHAPTER 4

Platform

Upgrade Alma Linux to 8.7

Feature Summary and Revision History

Table 8: Summary Data

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

Revision History

Revision Details	Release
First introduced.	23.2.0

Feature Description

In CPS 23.2.0 release, Alma Linux version 8.6 is replaced with Alma Linux 8.7 along with upgrading to the latest rpm packages and their dependencies.

With Alma Linux 8.7, the kernel version is modified to:

```
root@localhost ~]# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-425.19.2.el8_7.x86_64
[root@localhost ~]#

[root@localhost ~]# cat /etc/redhat-release
AlmaLinux release 8.7 (Stone Smilodon)
```

```
[root@localhost ~]#

[root@localhost ~]# uname -a
Linux localhost.localdomain 4.18.0-425.19.2.el8_7.x86_64 #1 SMP Tue Apr 4 05:30:47 EDT 2023
 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost ~]#
```

Support for Ubuntu 20.04 LTS Version

Table 9: 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 10: Revision History

Revision Details	Release
First Introduced	23.2.0

Feature Description

In CPS vDRA, Ubuntu is upgraded to the latest 20.04 stable version. The following package versions are also upgraded:

Table 11: Package Versions

Package Name	20.04 Version
Openssl	1.1.1f
Python	3.8.10
Weave	2.8.1
Haproxy	2.0.31-0ubuntu0.1
Docker	20.10.24
collectd	5.12.0
Zing	23.02.101

Use the following latest release and Kernel version in Base VM’s:

```
## cat /etc/lsb-release
```

```
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.6 LTS"
# uname -a
Linux vpas-A-dra-master-0 5.4.0-152-generic #169-Ubuntu SMP Tue Jun 6 22:23:09 UTC 2023
x86_64 x86_64 x86_64 GNU/Linux
```

Prerequisite

Upgrade the ESXI Hosts to minimum of 7.0 version.

Upgrade, Migration, Backward Compatibility Considerations

- Verify ISSM procedure with rollback changes.
- Backward compatible with Ubuntu-18 for CPS 22.2.0 and 23.1.0 releases.

Troubleshooting

For service-related issues, use the journactl to get the systemctl logs.

CHAPTER 5

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 23.2.0 Release

Feature Summary and Revision History

Table 12: 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 13: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

CPS PCRF meets the Cisco security guidelines and is aligned with the security features for 23.2.0 release. CPS now supports the following PSB requirements:

Table 14: CPS PSB Requirements

PSB Item	Description
CT2281: SEC-HRD-BUILDENV-3	Register and link your build environment to your offer.

CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 23.2.0 release. vDRA now supports the following PSB requirements:

Table 15: vDRA PSB Requirements

PSB Item	Description
CT2281: SEC-HRD-BUILDENV-3	Register and link your build environment to your offer.
CT2282: SEC-UPS-TPSQUAL	Register Third Party Software.

CHAPTER 6

vDRA

Apply Filter for Specific Column in CRD Table

Table 16: 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 17: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the CRD table supports filter option to select a specfic column and search the required data in the selected column

Note By default, the CRD table is set with the **All Visible Columns** option. It selects and searches the keyword against all the columns of that table.

Configuration and Restrictions

- The **All Visible Columns** option displays all the table data if any of the column data matches with the search string.
- If you select any particular column, the filter option of the table displays all the table data of the selected column data that matches with the search string.

For more information, see the *Custom Reference Data Configuration* chapter in the *CPS vDRA Configuration Guide*.

Create and Manage API Dedicated User

Table 18: 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 19: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, by default the local users have access to API, CLI and read-only access for central and Grafana and the external users can access VM, API, CLI, central and Grafana.

From this release, you can create and manage users only with the API and restrict other accesses.

The **api-user add** and **api-user remove** CLI commands allow to create and remove API users either with the user-name or gid value.

The following CLI commands help to manage the API dedicated users and to map the external users:

- **api-user add/remove group-details gid <GID> auth-type local/external write-enable true/false**
- **api-user add/remove user-details name <USER_NAME> auth-type local/external write-enable true/false**

- **external-aaa pam username-mapping <USER-NAME> <ROLE>**

Configuration and Restrictions

- In previous releases, the user part of Grafana-admin and Grafana-editor have admin or editor access and the user part of remaining groups have viewer access. From this release, if the user is not a part of any Grafana groups (grafana-admin/editor/viewer), they cannot access the Grafana.
- To convert the read-only and read-write API user roles, remove the access from API user CLI and add a flag with the required write-enable flag.
- Configure the below nacm rule in the configuration mode for CLI restriction.

  ```
  config
  nacm rule-list restricting-CLI-access group [ rest-api-ro rest-api-rw ] cmdrule
  restrict-CLI-acccess command * access-operations create,read,update,delete,exec context
   cli action deny
  ```

- The pem file should be in the `/data/keystore` path of the orchestrator.
- If the Halo-E is enabled, the API user is still able to access Grafana in viewer mode using the Halo-E login as the user is getting assigned with default viewer role.

For more information, see the *CLI Commands* topic in the *CPS vDRA Operations Guide*.

Debug Log Collection Statistics Support

Feature Summary and Revision History

Table 20: 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 21: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the log collection CLIs collect the logs to support the troubleshooting based on timestamps.

In CPS 23.2.0 and later releases, you can track the log collection status through the **log_collection_stats** KPI.

For more information, see *Managing CPS Interfaces and APIs* chapter in the *CPS vDRA Operations Guide* and the *Statistics/KPI Additions or Changes* section in the *CPS Release Change Reference Guide*.

Display Last Published Repository in Policy Builder

Table 22: 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 23: Revision History

Revision Details	Release
Display the last published and commit repository details in the last commit order in the history page of DRA Policy builder.	23.2.0

Feature Description

In CPS 23.2.0 and later releases, the policy builder displays the last published and commit repository details using the newly added API from the SVN commands. It displays the following details:

- Last committed repository and published repository in the history page.
- List of repositories sorted based on the last commit order in DRA central.

Limitation

DRA Central GUI retrieves the SVN last publish and SVN commit repositories by using an underlying SVN containers. If SVN container is down then GUI will have issues.

For more information, see *SVN Repository Changes* topic in *Policy Builder Configuration* chapter from the *CPS vDRA Configuration Guide*.

Error Code Classification per Peer/End Node in Grafana

Table 24: 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 25: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In CPS vDRA, the Grafana monitors the per peer message failures as 3XXX or 5XXX error codes. From CPS vDRA 23.2.0 and later releases, the peer traffic monitor in Grafana includes the following monitoring panels as a part of the **peer_message_total** KPI enhancement:

- destination_host
- destination_realm
- peer_group

The Grafana updates the KPI based on the error code type. It does not consider the DRA rejection messages and the 4XXX error codes in the KPI.

For more information, see the *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Limit Permissions to Subset of CRD Tables

Table 26: 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 27: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the Custom Reference Data (CRD) REST API supports the query for selection, creation, deletion, and update of CRD table data with the read-only and read-write access. From this release, the CRD REST API allows the following CRD groups to limit the read or write access to a subset of the CRD Table:

- `crd-table-restrict-read-write` - read and write access to the configured subset of CRD tables
- `crd-table-restrict-read-only` - read only access to the configured subset of CRD tables
- `crd-table-restrict-write-only` - read only access to all the CRD tables and write access to the configured subset of CRD tables

Configuration and Restrictions

Use the CLI commands to:

- manage the CRD table group
- manage the mapping of local and external users to the CRD table group

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

Support Alerts for Monitoring Primary DB

Table 28: 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 Alarm Guide*

Table 29: Revision History

Revision Details	Release
Enhanced the NO_PRIMARY_DB alert and added a new alert to monitor the status of primary DB in vDRA.	23.2.0

Feature Description

vDRA supports the following alerts and KPI extensions:

- **PREFERRED_PRIMARY_NOT_RUNNING** - Use the alert to know if the the primary DB is not running on the server seed.

- **NO_PRIMARY_DB** - Enhancement to this alert provides information on the DB name and replica set name.
- The **mongo_primary_reachable** KPI includes the following labels added along with the existing labels:
  - preferredprimary
  - seed

Configuration and Restrictions

- In database configuration, the server seed should be the highest priority member.
- If the low priority member is configured as server seed and when the server-seed is down, it triggers the **PREFERRED_PRIMARY_NOT_RUNNING** alert.
- If there are two highest priority members configured and the server seed goes down, another highest priority becomes a primary member. This raises the **PREFERRED_PRIMARY_NOT_RUNNING** alert even if the server seed rolls back. There is no automatic switchover of primary to server seed because of the same priority
- If the seed member is restoring from site 2 to site 1 (inter site primary transition), the alert status may flap for a few seconds before becoming stable.

For more information, see the *Notification and Alerts* section in the *CPS vDRA SNMP and Alarm Guide* and *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Support TLS for Gy and Sy, and MTLS Support for Diameter Application

Table 30: 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 31: Revision History

Revision Details	Release
The feature supports both TLS and MTLS in the policy builder page of vDRA.	23.2.0

Feature Description

In CPS 23.2.0 and later releases, the vDRA supports both TLS and MTLS encryption by enabling them from the PB GUI.

The following DRA applications support TLS and MTLS encryption.

- Gx interface
- Rx interface
- Gy interface
- Sy interface

Configuration and Restrictions

- The open stack supports either TLS or MTLS for data encryption.
- The connecting peer must be inline with the DRA peers.
  - If the DRA peer is TLS enabled, then the connecting peer should be TLS enabled
  - If the DRA peer is MTLS enabled, then the connecting peer should be MTLS enabled

For more information, see the *Policy Builder Configuration* chapter in the *CPS vDRA Configuration Guide*.