CPS Release Change Reference, Release 23.1.0

First Published: 2023-01-24

Last Modified: 2023-02-24

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.

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. 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 standards documentation, or language that is used by a referenced third-party product.

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

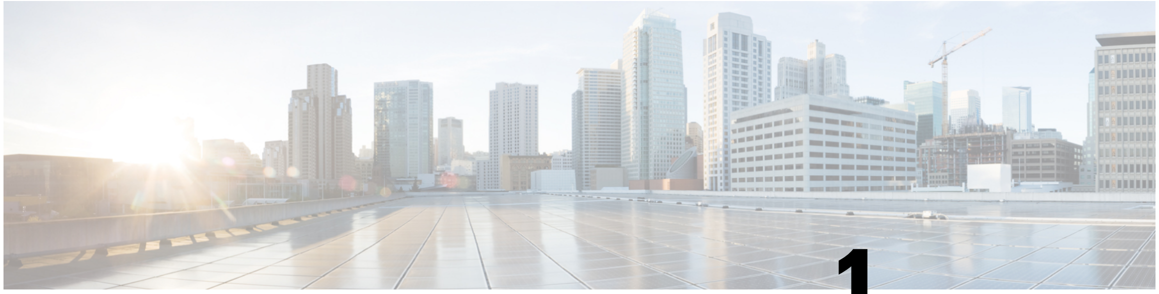
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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

23.1.0 Features and Changes

23.1.0 Features and Changes

Table 1: 23.1.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Prometheus Federated Counter Support to Expose Metrics Interface, on page 13	vDRA	23.1.0
Disable Auto Upgrade to the Next Level in Dynamic Peer Throttling, on page 14	vDRA	23.1.0
Ability to Configure Prometheus Sampling Interval, on page 15	vDRA	23.1.0
PSB Requirements for 23.1.0 Release, on page 9	CPS/vDRA	23.1.0
Source IP validation for Diameter connection ACL, on page 18	vDRA	23.1.0
Support for MongoDB 4.4 Version in vDRA, on page 6	vDRA	23.1.0
Support for TLS Certificate In-service Management and Expiry Alert, on page 16	vDRA	23.1.0
Upgrade Alma Linux to 8.6 , on page 5	PCRF	23.1.0
Upgrade MongoDB Version 4.4, on page 6	PCRF	23.1.0
Support for MongoDB 4.4 Version in vDRA, on page 6	vDRA	23.1.0

CHAPTER 2

Operations

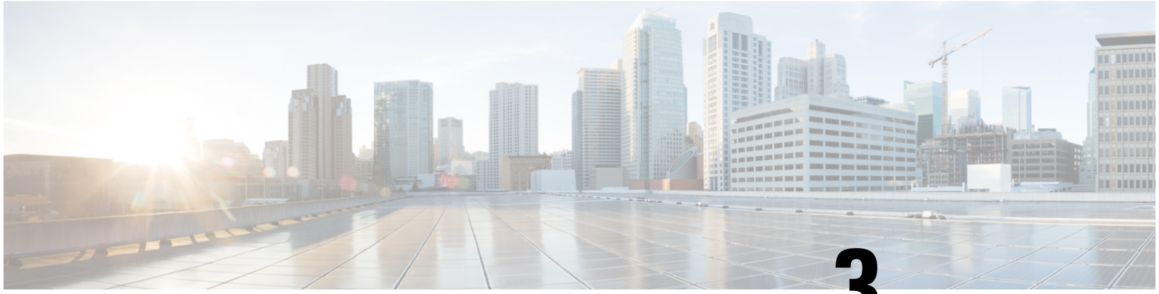
Statistics/KPI Additions or Changes

The following table provides information on new/modified statistics:

Table 2: Statistics Additions

Statistics Name	Description	Applicable Product(s)
CER_MESSAGE_REJECTED _UNKNOWN_PEER	Total number of CER messages from unknown Source-IP peers rejected by application. Following are the options: • remote_peer_host – Origin-Host of peer • remote_peer_realm – Origin-Realm of peer • source_ip – source IP of peer • local_peer – DRA Endpoint FQDN	vDRA
tls_cert_validity	Displays the value of the certificate expiry in days. The severity of the alert is triggered based on the days to expiration. For example, if the expiration in days is 14, then the severity is considered as Critical.	vDRA
ipc_message_drops	New parameter *message_class* is added as a second last parameter along with the existing parameters such as *system_id, instance_id, msg_destination, reason.*	vDRA
send_listener_drop	New parameter *message_class* is added as a second last parameter along with the existing parameters such as *system_id, app_id, remote_peer, type, exception_cause.*	vDRA

Statistics Name	Description	Applicable Product(s)
zone_range_config_status	New parameter is added to track zone range config modifications in IPv6 zone aware configuration.	vDRA
monitor_subscriber_key	A new parameter subscription_id_value is added to track the number of subscribers in Monitor Activity.	vDRA
peer_message_total	The parameter is extended with the DSCP label to display the number of messages per DSCP.	vDRA
peer_connection_status	The parameter is extended with the DSCP label to display the number of connections per DSCP.	vDRA
relay_message_total	The parameter is extended with the DSCP to display the number of relay messages per DSCP.	vDRA
relay_peer_status	The parameter is extended with the DSCP to display the number of relay connections per DSCP.	vDRA



CHAPTER 3

Platform

Upgrade Alma Linux to 8.6

Feature Summary and Revision History

Table 3: 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.	23.1.0

Feature Description

In CPS 23.1.0 release, Alma Linux version 8.5 is replaced with Alma Linux 8.6 along with upgrading to the latest rpm packages and their dependencies.

With Alma Linux 8.6, the kernel version is modified to:

```
[root@localhost ~]# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-372.32.1.el8_6.x86_64
[root@localhost ~]# cat /etc/redhat-release
AlmaLinux release 8.6 (Sky Tiger)
```

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 4.18.0-372.32.1.el8_6.x86_64 #1 SMP Tue Oct 25 05:53:57 EDT
2022 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost ~]#
```

Upgrade MongoDB Version 4.4

Feature Summary and Revision History

Table 4: 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 5: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

This release provides support for MongoDB version 4.4.0.

You can upgrade CPS 22.2.0 (using mongoDB version,4.2.20) to CPS 23.1.0 (using mongoDB version,4.4.18).

Un-Supported CPS Releases for Ugrading to Mongo 4.4

Any CPS version prior to CPS 22.2.0 such as CPS 22.1.1 (using mongoDB version 4.0.27) and previous versions of CPS (using mongoDB version 3.x) does not support direct upgrade to CPS 23.1.0 (using mongoDB version 4.4.18).

To upgrade the mongoDB version to 4.4, you must upgrade to CPS version 22.2.0, which uses the mongoDB 4.2.20 version. For example, if you are running mongoDB 3.6 series in your CPS release, it is required to first upgrade to 4.0 and then to 4.2 before planning for any upgrade to 4.4.

Support for MongoDB 4.4 Version in vDRA

Feature Summary and Revision History

Table 6: 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 7: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

This release provides support for MongoDB version 4.4.18

Upgrade, Migrate, and Backward Compatibility Considerations

- **Supported DRA Releases for Upgrading to 4.4**: You can upgrade vDRA 22.2.0 (mongoDB version,4.2.20) to vDRA 23.1.0 (mongoDB version,4.4.18).
- **Un Supported DRA Releases for Upgrading to 4.4**: Any DRA version prior to CPS 22.2.0 such as DRA 22.1 (mongo 4.0.27 MMAP storage engine), 21.2 (mongo 3.6.9) or DRA 19.4/18.2 (mongo 3.4.5) and previous versions of DRA, does not support direct upgrade to DRA 23.1 (mongoDB version, 4.4.18)

Note Upgrading to DRA 23.1 is supported only from DRA 22.2.0.

Mongo Java Driver: MongoDB version 4.4 requires Mongo Java Driver version 3.12.9.

Prerequisite for upgrading to 23.1 from 22.2.0 and rollback from 23.1 to 22.2.0

The following are the common prerequisites for upgrade and roll back:

- Run the following CLI before upgrade:

  ```
  #database genericfcvcheck 4.2
  ```

Note Make sure to run the above CLI before upgrade and / or downgrade on all sites.

- Specify any one of the CLI options:
  - **Set**: This option checks and sets FCV only on primary.

Note

We recommend to use **Set** option first and then **Check** to make sure that FCV is replicated on secondary members. Upgrade/downgrade should not be triggered if any error is found in above CLI or FCV is not replicated on secondary members. Make sure to resolve the CLI error, rerun the CLI, and then only proceed for upgrade or downgrade.

- **Check**: This option only checks FCV on all members (primary, secondary, and arbiter).

Upgrade to 23.1.0

1. Run the prerequisite steps.
2. Follow the standard documented procedure for upgrade.

Downgrade from 23.1.0

1. Run the steps mentioned in the prerequisite section.
2. Follow the standard documented procedure for downgrade.

CHAPTER 4

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 23.1.0 Release

Feature Summary and Revision History

Table 8: 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 9: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

CPS PCRF meets the Cisco security guidelines and is aligned with the security features for 23.1.0 release. CPS now supports the following PSB requirements:

Table 10: CPS PSB Requirements

PSB Item	Description
CT2226: SEC-HRD-BUILDENV-FR1-v2	Register and link your build environment to your offer.
CT2239: SEC-SW-APPDTCT-FR8-v1	Protect Signature Verification Elements (was SEC-SW-INSCHK-FR7.
CT2277: SEC-UPS-REGI-FR1-v4	Register Third Party Software.
CT2278: SEC-UPS-REGI-FR2-v4	Update TPS Registrations Regularly.
CT2232: SEC-SW-APPDTCT-FR1-v1	Check all signatures before installing code (was SEC-SW-INSCHK-FR1, SEC-SW-INSCHK-FR2 and SEC-SW-INSCHK-FR.
CT2233: SEC-SW-APPDTCT-FR2-v1	Check all subsidiary module signatures on installation (was SEC-SW-INSCHK-FR11).
CT2234: SEC-SW-APPDTCT-FR3-v1	Reject code with unexpected signatures on installation (was SEC-SW-INSCHK-FR3).
CT2223: SEC-DAT-KNOWWHAT-2	Know what data your product or service processes and assess the privacy risk.
CT2227: SEC-HRD-BUILDENV-FR2-v2	Perform the Build Environment Security (BES) risk assessment of your build environment.
CT2235: SEC-SW-APPDTCT-FR4-v1	Closed code must use Cisco installers (was SEC-SW-INSCHK-FR8).
CT2211: SEC-ASU-TRAIN-3	Train developers, testers, etc.
CT2231: SEC-PRV-USERAUTH-3	Control user and system access to personal information.

CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 23.1.0 release. vDRA now supports the following PSB requirements:

Table 11: vDRA PSB Requirements

PSB Item	Description
CT2226: SEC-HRD-BUILDENV-FR1-v2	Register and link your build environment to your offer.
CT2239: SEC-SW-APPDTCT-FR8-v1	Protect Signature Verification Elements (was SEC-SW-INSCHK-FR7.
CT2277: SEC-UPS-REGI-FR1-v4	Register Third Party Software.

PSB Item	Description
CT2278: SEC-UPS-REGI-FR2-v4	Update TPS Registrations Regularly.
CT2232: SEC-SW-APPDTCT-FR1-v1	Check all signatures before installing code (was SEC-SW-INSCHK-FR1, SEC-SW-INSCHK-FR2 and SEC-SW-INSCHK-FR.
CT2233: SEC-SW-APPDTCT-FR2-v1	Check all subsidiary module signatures on installation (was SEC-SW-INSCHK-FR11).
CT2234: SEC-SW-APPDTCT-FR3-v1	Reject code with unexpected signatures on installation (was SEC-SW-INSCHK-FR3).
CT2223: SEC-DAT-KNOWWHAT-2	Know what data your product or service processes and assess the privacy risk.
CT2227: SEC-HRD-BUILDENV-FR2-v2	Perform the Build Environment Security (BES) risk assessment of your build environment.
CT2235: SEC-SW-APPDTCT-FR4-v1	Closed code must use Cisco installers (was SEC-SW-INSCHK-FR8).
CT2211: SEC-ASU-TRAIN-3	Train developers, testers, etc.
CT2231: SEC-PRV-USERAUTH-3	Control user and system access to personal information.

CHAPTER 5

vDRA

Prometheus Federated Counter Support to Expose Metrics Interface

Feature Summary and Revision History

Table 12: 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 13: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS vDRA 23.1.0 the Prometheus Federated Counter support is introduced to expose the KPI metrics to the external nodes.

You can configure the Prometheus Federate Server to get the Prometheus API metrics from Prometheus clusters. You can achieve scalable Prometheus monitoring setups or pull related metrics from one service of Prometheus into another.

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

Configuration and Restrictions

Following are configuration and restrictions:

- To federate metrics from one server to another, configure the destination Prometheus server.
- To enable the honor_labels scrape option and passing in the desired match parameters, scrape from the federate endpoint of a source server.

> **Note** All the federation configuration works on the external server.

- Minimum scrape interval to be configured is >=30 secs.
- Supported for only hi-res interface

Disable Auto Upgrade to the Next Level in Dynamic Peer Throttling

Feature Summary and Revision History

Table 14: 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 Configuration Guide*

Table 15: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS 23.1.0 release, vDRA allows to apply the next level throttling (dynamic peer rate limit throttling) only if there is increase / change in the current DB VM CPU utilization. Use the **Auto Apply Next Level Throttle** check box in the **DRA Configuration** to enable the auto update of the next level CPU.

For more information, see the *Enable DRA Dynamic Peer Rate Limiter* section in the *CPS vDRA Configuration Guide*.

Ability to Configure Prometheus Sampling Interval

Feature Summary and Revision History

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 Operations Guide*

Table 17: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

Scrape interval configuration is important because it determines the number of data points per minute (DPM) scraped in your active series. In CPS vDRA 23.1.0 and later releases, vDRA allows maximum scrape interval timings configuration using CLI commands. This method helps in taking fewer samples but keeps the data for longer interval.

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

Configuration and Restrictions

Prometheus recommends not to configure scrape interval for more than 2 minutess. Due to the default staleness period of 5 minutes, the scrape interval of 2 minutes allows for one failed scrape. Hence, the metrics will no longer be stale.

Support for TLS Certificate In-service Management and Expiry Alert

Feature Summary and Revision History

Table 18: 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 19: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS 23.1.0 and later release, vDRA supports the following function:

- Installation of a new certificate on the Directors before expiration of a TLS certificate

Note After installation the same certificate must be installed on the client.

- After replacing a new certificate, the client should re-initiate the connection to make use of new certificate.
- Monitoring of certificate validity will be every hour from the time of application restart.
- Alert notification prior to the certificate expiration date based on the following alert notification metrics.

Table 20: Alert Notification

Expiration in Days	Alert Level
60 days	Minor
40 days	Major
14 days	Critical

Inservice Certificate Management

The vDRA facilitates installation of a new TLS certificate on the Director before the TLS certificate expiration. Ensure to follow the procedure:

- Place the new certificate in the following path `/data/orchestrator/pemKey/`.
- After placing a new updated certificate on the Master VM, use the same CLI command to replace the existing certificate.

  The existing connection from the older certificate remains connected and there should not be a call failure.
- To get the new certificate in place, terminate the existing connection and the new connection must be negotiated by the client.

Configuration and Restrictions

- Ensure to install CA certificates through a CLI before initiating the Stack from the Diameter PB configuration.
- Until the existing connection is terminated, its considered as valid and the replacement of certificate file in the container will not impact the existing connection.
- CLI command is used to place the java key store file to the desired location.

Note Threshold alert configuration does not work for decreasing threshold.

For more information, see the *Creating a new TLS Certificate* section in the *CPS VDRA Configuration Guide*, *Applications Notifications* table and *Enabling Alerts for TLS Certificate Expiration* section in the *CPS vDRA SNMP and Alarms Guide*, and *CLI Commands* section in the *CPS vDRA Operations Guide*.

Apply Dynamic DB Throttling only for IPv6 and Session Cluster

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	23.1.0

Feature Description

In CPS 23.1.0 and later release, you can dynamically apply throttling to DB VMs based on the configuration. CPU throttling is enabled to only VMs, which has IPv6 session, IMSI, or IPv4 DBs based on the CLI configuration.

If two or more DB types are configured, then all the VMs that have shared types are monitored.

Use the binding monitor-db-vms CLIto monitor only a particular type of DBs based on the cluster name in DB VNF.Also, every 10 seconds CPU gets monitored from the metrics DB from the Worker node.

Configuration and Restrictions

- Monitoring DB VMs starts only after configuration in DB VNF.
- If any one of VMs in which shards of cluster type is breached, then throttling is applied.
- Throttling is applied based on the VM CPU.

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

Source IP validation for Diameter connection ACL

Feature Summary and Revision History

Table 23: 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	*vDRA Configuration Guide*

Table 24: Revision History

Revision Details	**Release**
First introduced	23.1.0

Feature Description

In vDRA, you can allow or deny a peer based on the Source-IP validation. The Source-IP validation is an optional check, which an administrator can decide to configure Source-IP with peer FQDN/Realm or not. Source-IP uses Custom Reference Data (CRD) to persist the configuration. Hence the configuration is limited to a site.

You can monitor disconnects and rejections for unknown Source-IP peers in the existing CER_MESSAGE_REJECTED_UNKNOWN_PEER KPI used for the Peer Rejection case.

Configuration and Restrictions

- Source-IP Validation is performed only for a new connection and is not applied on existing connection.
- After an ISO upgrade or patching for this feature, if the CRD contains any existing details, then export the existing details, populate a default value (*) to the **Source-IP** field, and then import back. Otherwise, it restricts to add new entries to the CRD as the existing data doesn't have valid Source-IP value.

  The allowed IPv4/IPv6 subnet formats:

  ```
  (Starting Address of IPv4/IPv6)/(Prefix Length)
  Ex.1: 172.10.216.176/28
  Ex.2: 2001:420:27c1:906:250:56ff:feae:88c0/124
  Ex.3: 2001:420:27c1:906::/64
  Ex.4: 2001:420:27c1:906::
  ```

Note Input IP should be the starting address of that particular subnet range.

- To block a peer from connecting to multiple sites, ensure to disable peer on each site.

For more information, see the *Peer Control Access List* section in the *vDRA Configuration Guide* and *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Monitor Single Subscriber for Non Gx or Rx Protocol

Feature Summary and Revision History

Table 25: 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 Administration Guide*

Table 26: Revision History

Revision Details	Release
CPS vDRA supports monitoring of single subscriber activity for Non-Gx / Rx protocols.	23.1.0

Feature Description

In CPS 23.1.0 and later releases, vDRA supports the monitoring of single subscriber activity for Non-Gx / Rx protocols such as Sy/Sd/Gy messages along with Gx/Rx protocols. A new KPI is added in the monitor activity:

- In CPS DRA, click the Subscriber Monitoring tab.
- In the DRA Subscriber Monitor area, click any one of the IMSI/MSISDN/IPv6 options to monitor for a single subscriber.
- Enter the required Subscriber identity values for IMSI/MSISDN/IPv6.

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

Enhance Clearzoneinfo Script to Add or Modify the Existing Zone Configuration

Feature Summary and Revision History

Table 27: 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 28: Revision History

Revision Details	**Release**
In CPS vDRA, the clearZoneInfo script supports the deletion of single zone range configuration.	23.1.0

Feature Description

In previous releases, after performing the initial ipv6 database configuration, vDRA allows you to modify the zones and ranges. Use the clearZoneInfo script to clear the old configuration and to apply the new configuration. The script deletes all zone range configuration which is stored in the Mongo db. This script does not support the deletion of a single zone range configuration.

From CPS vDRA 23.1.0 and later releases, you can delete a single zone range configuration using CLI commands. A new KPI is introduced to track zone range configuration modifications in the ipv6 zone aware configuration.

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

IPv4 DB Support in Orchestrator Mongo Query

Feature Summary and Revision History

Table 29: 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 30: Revision History

Revision Details	Release
In CPS vDRA, the CLI command for a Mongo query function supports. It also supports the existing IMSI, IPv6, MSISDN, and SESSION databases.	23.1.0

Feature Description

The CPS vDRA uses an orchestrator CLI for App sharding queries.

Earlier, the CLI allowed IMSI, IPv6, MSISDN, and SESSION databases. In CPS 23.1.0 and later releases, it allows the IPv4 database with same keys such as staleBindingExpiryTime, srk, session id, and uuid.

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

Enhance IPC Queue Processing to Fix Single Point of Failure (SPOF)

Feature Summary and Revision History

Table 31: 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* • *CPS vDRA Advanced Tuning Guide*

Table 32: Revision History

Revision Details	Release
The CPS vDRA: • Introduces a new IPC thread pool to process priority messages • Adds an IPC Queue Send Thread priority configuration to handle the slow network peers.	23.1.0

Feature Description

In vDRA, the IPC thread pool is common for both priority and non-priority messages. The slow processing in the nonpriority message affects the priority messages. In CPS vDRA 23.1.0 and later releases, instead of a common pool, two IPC thread pools, one for priority messages and another for non-priority messages are configured through:

- The CLI command *dra ipc-send-thread priority* configuration
- *Policy Builder - qprocessor.priority* threading configuration to process the priority messages.
- *message_class* parameter with the existing parameters in KPI

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

DSCP Confirmation for Relay and Diameter Peer Connection

Feature Summary and Revision History

Table 33: 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* • *CPS vDRA Administration Guide* • *CPS vDRA SNMP and Alarm Guide*

Table 34: Revision History

Revision Details	Release
vDRA updates KPI with configured DSCP value for relay and diameter peer connections.	23.1.0

Feature Description

With this configuration of DSCP values for Relay and Diameter peer connections feature, the following activities are automated to reduce the overall time taken during upgrade:

Confirm the configured DSCP values for Relay and Peer through:

- KPIs that are updated with the DSCP parameter.
  1. peer_message_total
  2. peer_connection_status
  3. relay_message_total
  4. relay_peer_status
- Relay and Peer APIs with DSCP value
  1. /dra/api/activePeerEndpoints
  2. /dra/api/localActiveRelayEndpoints
- Monitoring GUIs with DSCP value
  1. Peer Monitoring GUI
  2. Relay Connections GUI

This **$ cps redeploy dra-vnf --healthcheck yes --sysenv dra** command performs redeployment along with healthchecks on the VMs mentioned in `/data/deployer/env/upgradelit.txt` files and order to be maintained. For more information, see the *CPS vDRA Installation Guide for VMware*.

Configuration and Restrictions

PCRF session query API support to display DSCP value is not supported.

For more information, see *DSCP Mapping for DRA Endpoints section* in the *CPS vDRA Configuration Guide*, *Peer Monitoring section and Monitoring Relay Connections section* in the *CPS vDRA Administration Guide* and *Sample Alert Rules section* in the *CPS vDRA SNMP and Alarm Guide.*

vDRA ISSM Automation Improvements

Feature Summary and Revision History

Table 35: 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 Installation Guide*

Table 36: Revision History

Revision Details	**Release**
First introduced	23.1.0

Feature Description

Currently in consumer DRA, the new version upgrade takes more time and it could take up to 4 maintenance windows for migrating to a higher version.

With vDRA ISSM Automation Improvements feature, the following activities are automated to reduce the overall time taken during upgrade:

- Complete diagnostics report of DRA and DB VNF VMs.
- Automatic redeployment of VMs with required health check performed.

vDRA also supports in upgrading the VMs by performing diagnostics and redeployment health checks to reduce time constraints.Below arguments are added to the CPS commands.

- diagnostics
- --healthcheck
- –sysenv

Following commands are introduced to perform health check and redeployment of VMs:

$ cps diagnostics dra-vnf

The **$ cps diagnostics dra-vnf** command connects to the existing master vm of the corresponding artifact files placed on the system and runs a sequence of health checks and prompts a clear output to the user.

$ cps redeploy dra-vnf --healthcheck yes --sysenv dra

The **$ cps redeploy dra-vnf --healthcheck yes --sysenv dra** command performs redeployment along with healthchecks on the VMs mentioned in `/data/deployer/env/upgradelist.txt` files and order to be maintained as specified in the installation guide.

For more information, see the *Upgrading VMs Using Diagnostics and Redeployment Health Check* section in the *CPS vDRA Installation Guide*.

Support the Integration of CPS Web Interfaces to the External Server (Halo.E)

Feature Summary and Revision History

Table 37: 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 Installation Guide*

Table 38: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS vDRA, the current authentication works using GTAC LDAP, which is not multifactor aware. For a multifactor user authentication process, DRA Central UI and Grafana use OpenID Connect (OIDC) to integrate to Halo.E and Global Logon.

For more information, see the *Integrating CPS vDRA and Grafana to Halo-E for User Authentication* chapter in the *CPS ATT-specific Features Guide*.