CPS Release Change Reference, Release 22.2.0

First Published: 2022-08-25

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

CONTENTS

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 overrides the same document available in the 22.1.0. For other functionality refer to the 22.1.0 documentation at 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.

Audience

This guide is best used by these readers:

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

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

Additional Support

For further documentation and support:

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

Conventions (all documentation)

This document uses the following conventions.

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS.

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

SAVE THESE INSTRUCTIONS

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

Communications, Services, and Additional Information

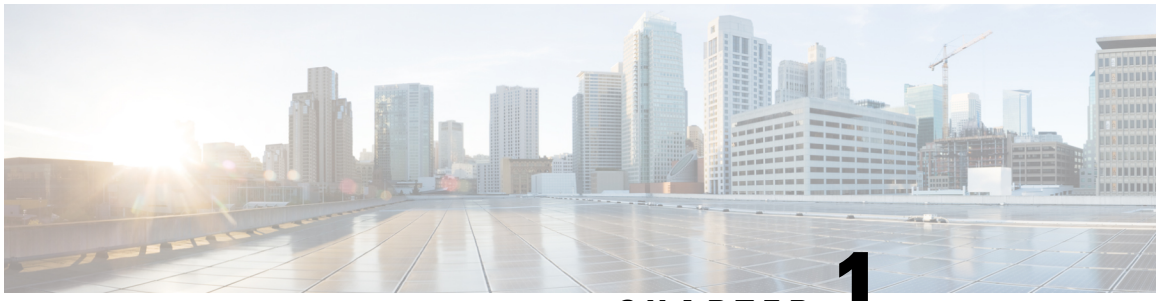
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class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

Cisco Bug Search Tool

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

Important Notes

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



CHAPTER 1

22.2.0 Features and Changes

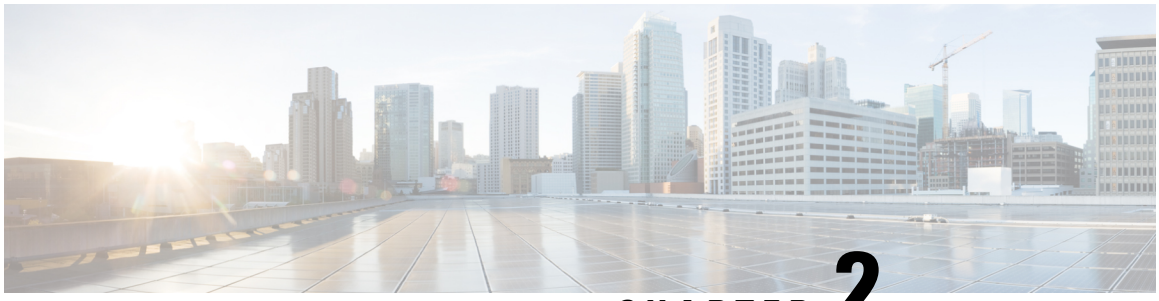
22.2.0 Features and Changes

Table 1: 22.2.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Add Per Diameter Peer Connection TCP Statistics, on page 17	vDRA	22.2.0
Benchmarking Zulu in DRA , on page 18	vDRA	22.2.0
Deploy all VMs using Hypervisor , on page 19	vDRA	22.2.0
Ensuring Equal Priority on Health Checks , on page 20	vDRA	22.2.0
Improving Visibility on Relay Traffic Timeouts or Failures, on page 24	vDRA	22.2.0
IPv6 Address Zone Range Validation, on page 25	vDRA	22.2.0
KPI Support to Account the Remote Peers Count , on page 25	vDRA	22.2.0
PSB Requirements for 22.2.0 Release, on page 11	CPS/vDRA	22.2.0
Preventing a Repository from Corruption and Publishing a Corrupted repository, on page 26	vDRA	22.2.0
Set Alarm Severity Based on Configurable Thresholds, on page 27	vDRA	22.2.0
Support for Python 3.9.6 Version, on page 9	CPS	22.2.0

22.2.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Support to Replace CentOS with Alma Linux on CPS, on page 5	CPS	22.2.0
Support for MongoDB 4.2 Version in vDRA, on page 8	vDRA	22.2.0
TLS Support for Diameter Encryption, on page 22	vDRA	22.2.0
User Audit Enhancements, on page 28	vDRA	22.2.0
Upgrade MongoDB Version 4.2, on page 6	CPS	22.2.0



CHAPTER 2

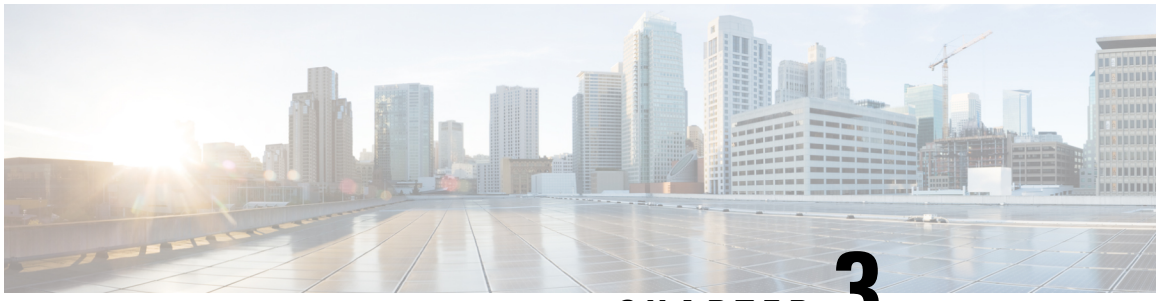
Operations

Statistics/KPI Additions or Changes

The following table provides information on new/modified statistics:

Table 2: Statistics Additions

Statistics Name	Description	Applicable Product(s)
diameter_request_total	New parameter **site_id** is added along with the existing parameters such as **app_id, result_code, message_type, sla and status**.	vDRA
diameter_request_timeout_total	New parameter **site_id** is added along with the existing parameters such as **app_id, message_type, status**.	vDRA
diameter_message_timeout_total	New parameter **site_id** is added along with the existing parameters. such as **app_id, message_class, message_type**	vDRA
active_peer_count	New parameters **system_id** and **app_id** are added to monitor peer traffic in Grafana.	vDRA



CHAPTER 3

Platform

Support to Replace CentOS with Alma Linux on CPS

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.	22.2.0

Feature Description

In CPS 22.2.0 release, Centos version 8.1 is replaced with Alma Linux 8.5 with latest rpm packages.

With Alma Linux 8.5, the kernel version is modified to:

```
# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-348.7.1.el8_5.x86_64
## cat /etc/redhat-release
```

```
AlmaLinux release 8.5 (Arctic Sphynx)
# uname -a
```

Along with the OS upgrade and Kernel upgrade many of the dependent third party packages are also upgraded.

Upgrade MongoDB Version 4.2

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	• *CPS Installation Guide for OpenStack* • *CPS Installation Guide for VMware*

Table 5: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

This release provides support for MongoDB version 4.2.20.

Upgrade, Migrate, and Backward Compatibility Considerations

You can upgrade CPS 22.1.0 (mongoDB version,4.0.27) to CPS 22.2.0 (mongoDB version,4.2.20).

Any CPS version prior to CPS 22.1 such as CPS 21.2 (mongo DB version,3.6.17) and previous versions of CPS, does not support direct upgrade to CPS 22.2 (mongoDB version, 4.2.20).

To upgrade the mongoDB version to the latest 4.2.20 then, you must upgrade the CPS version, which uses mongoDB 4.0.27 version.

Prerequisites for the ISSM Process

The following are the Prerequisites:

- Take a copy of the *mongoConfig.cfg* file in both old Cluster Managers.
- Update the following values in *mongoConfig.cfg* file:
  - WT_CACHESIZEGB=12
  - WT_CACHEARBSIZEGB=1

- Execute **import_deploy.sh** before performing ISSM procedure.
- Make sure that the system is running mongo 3.6 and Java driver patch is applied on the system.

Note CPS recommends configuring the above values in mongoConfig.cfg before performing fresh install or ISSM. For more information, visit mongoDB Package Components Upgrade. During deployment if you are using custom scripts for deploying the environment then change the scripts to modify the mongoConfig.cfg as needed.

After the prerequisites conditions are met, perform the ISSM process.

Storage Engine Support

To upgrade to MongoDB 4.2 from MongoDB 4.0 deployment that uses MMAPv1, you must upgrade to **WiredTiger**.

Note Starting in version 4.2, mongoDB deprecates the MMAPv1 storage Engine and in version 4.2, MongoDB removes the deprecated MMAPv1 storage engine.

MongoDB with WiredTiger supports either XFS or EXT4 filesystems. To avoid performance issues, it is recommended to use XFS file systems for data bearing nodes with the WiredTiger storage engine.

Upgrading Procedure

- Ensure to change the storage engine from MMapV1 to WiredTiger in MongoDB 4.0. For more information see the
- Perform ISSM from 22.1.0 to 22.2.0.
- To migrate to CPS 22.1 release , ISSM from CPS 21.1/21.2 releases is recommended, post following a pre-requisite of applying Mongo Driver Patch.

The prerequisites for upgrading to 22.1.x release are:

- Set the 4.0 replica set to CompatibilityVersion 4.0. To ensure that all members of the replica set have featureCompatibilityVersion set to 4.0, connect to each replica set member and check the featureCompatibilityVersion:

  ```
  db.adminCommand( { getParameter: 1, featureCompatibilityVersion: 1 } )
  ```

  All members return a result that includes "featureCompatibilityVersion" : { "version" : "3.6" }.
- To set or update featureCompatibilityVersion, run the following command on the primary. Most of the data-bearing members must be available:

  ```
  db.adminCommand( { setFeatureCompatibilityVersion: "4.0" } )
  ```

Note Ensure that no Replica set member is in Rollback or recovering state.

For more information, see the *Configuration Parameters - HA System* table in the *CPS Installation Guide for OpenStack* and *Modification of Storage Engine before Upgrade*.

Memory and Performance Impact

Wired Tiger Storage engine change in MongoDB Server 4.0 requires additional CPU resources of ~15% and additional memory (RAM) resources of ~40% in the Session Manager VMs. Up to ~40% more memory being consumed more by wiredtiger from total memory(RAM) than MMapV1.

For example, if the session manager VM(150GB) with MMapV1 utilizes 60GB then, wiredtiger requires 120GB(MMapV1 usage 60GB + 40% of total memory 150GB).

For more information, see the *Configuration Parameters - HA System* table in the *CPS Installation Guide for OpenStack* and *Modification of Storage Engine before Upgrade*.

Roll back Procedure

Before performing a rollback, restore the copied *mongoConfig.cfg* file in older Cluster Managers.

Execute the **import_deploy.sh** before performing ISSM rollback procedure.

Support for MongoDB 4.2 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	22.2.0

Feature Description

This release provides support for MongoDB version 4.2.20.

Upgrade, Migrate, and Backward Compatibility Considerations

- **Supported DRA Releases for upgrading to 4.2**: You can upgrade vDRA 22.1.1 (mongoDB version,4.0.27 WT storage engine) to vDRA 22.2.0 (mongoDB version,4.2.20 WT storage engine).
- **Un Supported DRA Releases for upgrading to 4.2**: Any DRA version prior to CPS 22.1.1 such as DRA 22.1 (mongo 4.0.27 MMAP storage engine), 21.2 (mongo 3.6.9 MMAP storage engine) or DRA 19.4/18.2 (mongo 3.4.5 MMAP storage engine), and previous versions of DRA, does not support direct upgrade to DRA 22.2 (mongoDB version, 4.2.20)

Note Upgrading to DRA 22.2 is supported only from DRA 22.1.1 MR.

Prerequisite for upgrading to 22.2 from 22.1.1 MR and rollback from 22.2 to 22.1.1 MR

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

- Run the following CLI before upgrade:

```
#database fcvcheck4
```

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 22.2.0

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

Downgrade from 22.2.0

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

Support for Python 3.9.6 Version

Feature Summary and Revision History

Table 8: Summary Data

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

Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS Migration and Upgrade Guide*

Table 9: Revision History

Revision Details	Release
First introduced	22.2.0

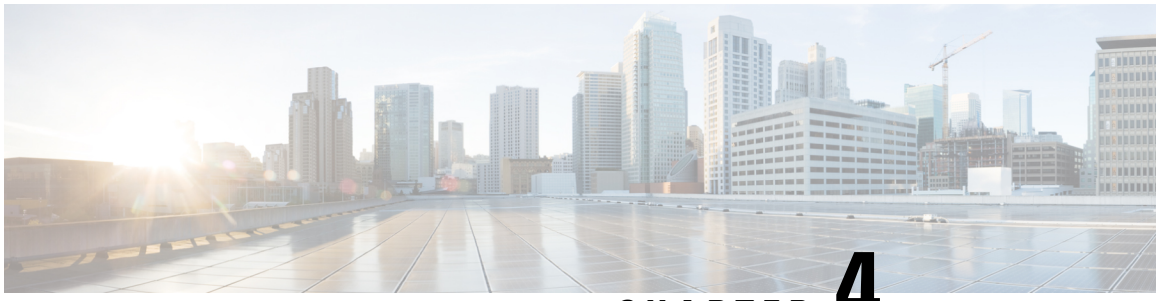
Feature Description

In CPS 22.2.0 and later releases, the python is upgraded to the latest 3.9.6 stable version.

Configuration and Restrictions

To perform ISSM, ensure to follow the steps to perfom Cluster Manager backup:

- Mount the existing ISO of your current CPS and run the backup cluman step specified in the *Migrate the Cluster Manager VM* section in the *CPS Migration and Upgrade Guide*. For example, if you are migrating to 22.2.0 from 22.1.0 then, mount the 22.1 ISO for taking Cluster Manager backup operations.
- During the ISSM rollback, at the time of migration from x.iso to y.iso and and at the time of mounting y.iso for rollback procedure, ensure to use Python2 (22.1) ISO.



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 22.2.0 Release

Feature Summary and Revision History

Table 10: 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 11: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

CPS PCRF meets the Cisco security guidelines and is aligned with the security features for 22.2.0 release. CPS now supports the following PSB requirements:

Table 12: CPS PSB Requirements

PSB Item	Description
CT2001: SEC-RUN-ASLR-FR1-v3	Randomize memory segments.
CT2115: SEC-SW-SIG-FR3-v5	Wrapping signatures.
CT1995: SEC-ASU-TMOD-FR4-v3	Review and update threat models as needed.
CT1982: SEC-ASU-TMOD-FR1-v3	Create and review a System-Level threat model.
CT2093: SEC-CRY-STDCODE-FR4-v3	Cisco Cryptographic specialists.
CT2088: SEC-RUN-ASLR-FR2-v3	Randomization Entropy.
CT2087: SEC-CRY-PRIM-FR1-v7	Algorithms and primitives.
CT2131: SEC-ASU-TMOD-FR6-v3	Threat models for offers that use Machine Learning or Artificial Intelligence.
CT2116: SEC-SW-SIG-FR4-v5	Protected data.
CT2114: SEC-SW-SIG-FR2-v5	Native signature formats.
CT2113: SEC-SW-SIG-FR1-v5	Sign all code.
CT2086: SEC-TLS-CURR-FR3-v6	SSL 2.0 and SSL 3.0
CT2060: SEC-CRY-STDCODE-FR3-v3	Third-party libraries.
CT2059: SEC-ASU-TMOD-FR2-v3	Assess and mitigate Threats against high value assets.
CT2048: SEC-CRY-PRIM-FR2-v7	Random number generation.
CT2037: SEC-CRY-STDCODE-FR2-v3	Adaptation layers and C3M.
CT2034: SEC-UPS-REGI-FR1-v3	Register third-party software.
CT2118: SEC-SW-SIG-FR6-v5	Cisco controlled packaging systems.
CT2117: SEC-SW-SIG-FR5-v5	Code-signing keys.

PSB Item	Description
CT2026: SEC-TLS-CURR-FR1-v6	TLS 1.2 and TLS 1.3.
CT2025: SEC-ASU-TMOD-FR3-v3	Create additional threat models for new features.
CT2015: SEC-CRY-STDCODE-FR1-v3	Cisco common Cryptography Modules (C3M).
CT2004: SEC-UPS-REGI-FR2-v3	Update TPS registrations regularly.
CT2140: SEC-PWD-STORE-2	Hash and salt non-recoverable stored credentials. Store recoverable credentials using a password manager.
CT1997: SEC-TLS-CURR-FR2-v6	TLS 1.0 and TLS 1.1.
CT2135: SEC-HRD-BUILDENV-FR1-v1	Register and link your build environment to your offer.
CT2138: SEC-HRD-MANDACC	Mandatory Access Controls (MAC) must be enabled and constraining all network services.
CT2080: SEC-ASU-TMOD-FR5-v3	Store threat models.
CT2050: SEC-RUN-ASLR-FR3-v3	ASLR canot be disabled.
CT2021: SEC-RUN-ASLR-FR4-v3	Do not leak addresses.

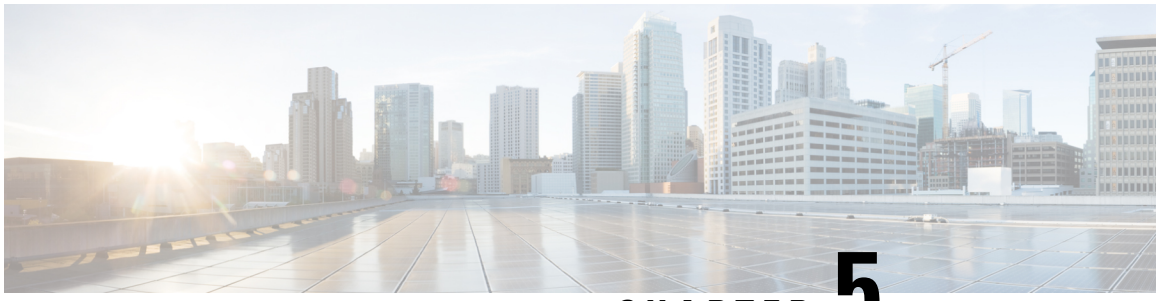
CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 22.2.0 release. vDRA now supports the following PSB requirements:

Table 13: vDRA PSB Requirements

PSB Item	Description
CT1723: SEC-HRD-OS	Harden production components.
CT2001: SEC-RUN-ASLR-FR1-v3	Randomize memory segments.
CT2115: SEC-SW-SIG-FR3-v5	Wrapping signatures.
CT1995: SEC-ASU-TMOD-FR4-v3	Review and update threat models as needed.
CT1982: SEC-ASU-TMOD-FR1-v3	Create and review a System-Level threat model.

PSB Item	Description
CT2093: SEC-CRY-STDCODE-FR4-v3	Cisco Cryptographic specialists.
CT2088: SEC-RUN-ASLR-FR2-v3	Randomization Entropy.
CT2087: SEC-CRY-PRIM-FR1-v7	Algorithms and primitives.
CT2131: SEC-ASU-TMOD-FR6-v3	Threat models for offers that use Machine Learning or Artificial Intelligence.
CT2116: SEC-SW-SIG-FR4-v5	Protected data.
CT2114: SEC-SW-SIG-FR2-v5	Native signature formats.
CT2113: SEC-SW-SIG-FR1-v5	Sign all code.
CT2086: SEC-TLS-CURR-FR3-v6	SSL 2.0 and SSL 3.0
CT2060: SEC-CRY-STDCODE-FR3-v3	Third-party libraries.
CT2059: SEC-ASU-TMOD-FR2-v3	Assess and mitigate Threats against high value assets.
CT2048: SEC-CRY-PRIM-FR2-v7	Random number generation.
CT2037: SEC-CRY-STDCODE-FR2-v3	Adaptation layers and C3M.
CT2034: SEC-UPS-REGI-FR1-v3	Register third-party software.
CT2118: SEC-SW-SIG-FR6-v5	Cisco controlled packaging systems.
CT2117: SEC-SW-SIG-FR5-v5	Code-signing keys.
CT2026: SEC-TLS-CURR-FR1-v6	TLS 1.2 and TLS 1.3.
CT2025: SEC-ASU-TMOD-FR3-v3	Create additional threat models for new features.
CT2015: SEC-CRY-STDCODE-FR1-v3	Cisco common Cryptography Modules (C3M).
CT2004: SEC-UPS-REGI-FR2-v3	Update TPS registrations regularly.

PSB Item	Description
CT2140: SEC-PWD-STORE-2	Hash and salt non-recoverable stored credentials. Store recoverable credentials using a password manager.
CT1997: SEC-TLS-CURR-FR2-v6	TLS 1.0 and TLS 1.1.
CT2135: SEC-HRD-BUILDENV-FR1-v1	Register and link your build environment to your offer.
CT2080: SEC-ASU-TMOD-FR5-v3	Store threat models.
CT2050: SEC-RUN-ASLR-FR3-v3	ASLR cannot be disabled.
CT2021: SEC-RUN-ASLR-FR4-v3	Do not leak addresses.



CHAPTER 5

vDRA

Add Per Diameter Peer Connection TCP Statistics

Table 14: 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 15: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In CPS vDRA, you can monitor statistics for each physical interface using *link_state* KPI to figure out which interface is up or down at each Virtual Machine (VM). However, this does not provide more information about latency or any other errors on the network.

In CPS 22.2.0 and later releases, vDRA provides more information about the statistics of these network interfaces, which allows you to narrow down errors in peer connections on a particular interface.

Enabling the TCP statistics per diameter interface allows you to::

- Fetch the required network interface statistics during issues or troubleshooting.
- Receive information about dropped packets within any specific interfaces and determine if any peer connections went bad due to issues in physical interfaces.
- Monitor the network latency at regular intervals for the same purpose.
- Get get the information of these network interfaces by querying the Prometheus data stores.
- Get the same information over a time in Grafana for all the Prometheus data stores.
- Collect the SAR reports to check the network bandwidth over a time for the specific interfaces.

Benchmarking Zulu in DRA

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	Not Applicable

Table 17: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the CPS 22.2.0 release, DRA supports both Zing and Zulu JVM software. Zing is the default software used in 22.2.0 release:

- **Enabling Zing and Zulu in DRA –** DRA supports both Zing and Zulu JVMs. While Zing is existing supported JVM, Zulu is added newly from 22.2.0 with limited qualification [Only FPAS]. User can chose

to enable either Zing or Zulu.. When Zulu is enabled, the following Zing related containers get terminated from DRA Worker and Director VMs:

- Haproxy-zvision
- Zvision

To enable Zulu/Zing through CLI, use the following commands:

- **dra jvm zulu enable** – Enables Zulu as default JVM.
- **dra jvm zing enable** – Enables Zing as default JVM.
- **show dra jvm** – Displays the default JVM service.

Note Zulu is qualified only in fPAS environment with SLA lock timeout disabled. For vPAS, it is not qualified and hence not recommended to enable in vPAS.

Deploy all VMs using Hypervisor

Feature Summary and Revision History

Table 18: Summary Data

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

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

During ESXI upgrades, when VMs deployed in a single hypervisor are down, you can install all VMs from a particular blade using a single command **--hypervisor** flag with the hypervisor name.

CPS commands on vDRA can perform the following functionalities:

- Recognize a **--hypervisor** tag to fetch VM's that are tagged with the ESXIHOST value in their *vm.esxi.env* file.

- Recognize a **--addartifact** tag to perform operations on more than one artifact file. You can also use the **--hypervisor** tag on top of it to filter VMs.

Health Checks

Using the **--hypervisor** option that you can perform health check of docker engine and consul status of other VMs before making changes on the requested VM.

Configuration and Restrictions

Perform the health check only if the master VM is active. If there are no master VMs, then a prompt message appears indicating you to skip the health check and proceed to the next step because of master unavailability. You can choose Yes or No.

It is always recommended that you perform a manual check and consul status of docker engine, and other similar states of alternate VMs before proceeding with the deployments using *--hypervisor* option. Copy *cps.pem* keys that can be used for performing SSH to master VMs to `/data/deployer/envs` folder

For more information, see the *Deploy all VMs with or without a Hypervisor flag* section in the *CPS vDRA Installation Guide for VMware*.

Ensuring Equal Priority on Health Checks

Feature Summary and Revision History

Table 19: Summary Data

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

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

vDRA ensures that health checks for critical processes have equal priority to the monitored entity process using the **system-config get-cpu-priority** and **system-config set-cpu-priority** CLI commands.

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

Fluentbit Log Forwarding without Authentication

Feature Summary and Revision History

Table 20: Summary Data

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

Table 21: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In CPS 22.2 release, vDRA supports log forwarding to the external server in either of the 2 ways / or in both ways:

- **External fluentbit instance without authentication**: vDRA supports log forwarding to the external server without authentication through a CLI command. The **log-forward fluentbit external-forward** CLI can send the logs to another external server where fluentbit or fluentd is configured. This external server in turn forward logs to elasticsearch based on configuration provided by user at the external server.

Note The **log-forward fluentbit external-forward** CLI takes threshold input as IP and Port of the external server.

- **Elasticsearch with authentication**: Enables or disables log forwarding to elasticsearch.

Note Recommendation is to use any one of the above external forwarding only at a time and not to use both.

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

TLS Support for Diameter Encryption

Feature Summary and Revision History

Table 22: 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

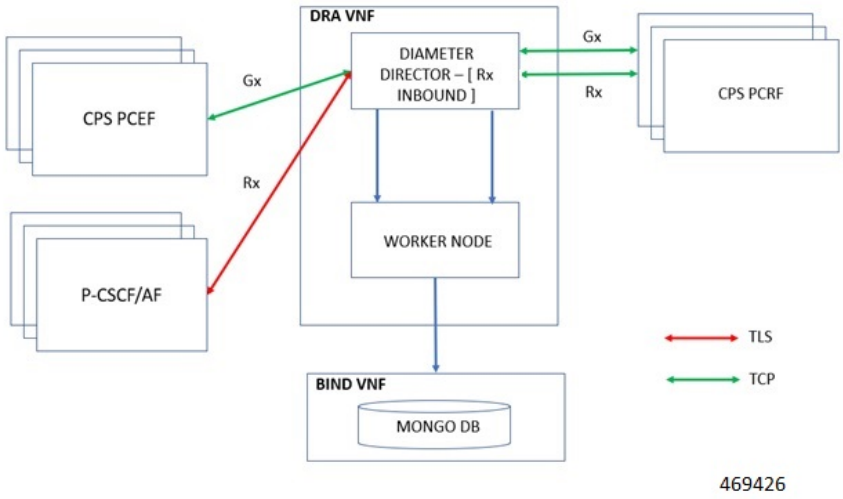
Table 23: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

The vDRA supports a Transport Layer Security (TLS) secure channel for diameter peer connection. The following architecture describes TLS in DRA.

Figure 1: TLS in DRA



Following standards/functionalities are supported:

- Only compliant to RFC 6733 [Establishment of TLS connection before exchanging CER/CEA messages]
- Only Inbound configuration is supported for TLS.
- Only Rx protocol is supported with TLS.
- Certificate authentication is supported with the current feature:
  - Client CA certificate authentication is performed only using issuer-based authentication approach.
  - Supports certificate import option on server and user can generate their certificate.
  - Import certificate using CLI command is supported.
  - Third party certificates are required.

Following standards/functionalities are not supported:

- Other type of authentication to be treated as separate requirement.
- Backward compatibility support RFC 3588.
- Default certificate are not provided or packed in the ISO image.
- No other protocols other than Rx is supported for TLS.
- Outbound configurations for TLS.
- MTLS is not supported.
- Validation of TLS for vPAS.
- Inservice Certificate management.
- Certificate Expiry notification.

Before you Begin

- Ensure to input CA certificate to install and initiate the secured TLS connection in the Diameter application.
- Single CA certificate should be used for all TLS connection per site.

vDRA allows you to enable a connection as TLS in the Policy Builder and supports import of certificate through **dra-tls cert import <certificate file> <private file>** CLI command. For more information, see the *Enable TLS Option in the Policy Builder* and *Import Certificate through CLI* sections in the *CPS vDRA Configuration Guide*.

Configuration and Restrictions

Following are the configuration and restrictions:

- Install CA certificates through CLI before initiating the Stack from the Diameter PB configuration.
- Use the CLI command to place the java key store file to the desired location.
- Due to .pem files for certificate and private key support, place files in `/data/orchestrator/pemKey/` master VM.

- After completion of the certificate import, the new keystore file is placed in the `/etc/tls/certs/` folder in the diameter container.

  The keystore credentials will be encrypted and placed as part of application property file and it will be decrypted and used in the application

Improving Visibility on Relay Traffic Timeouts or Failures

Feature Summary and Revision History

Table 24: Summary Data

Applicable Product(s) or Functional Area	vDRA
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.	22.2.0

Feature Description

vDRA allows you to differentiate failed requests and identify whether the failed calls are locally routed or relayed.

With this release, **site_id** parameter is added to the existing KPI parameters in Grafana.

- diameter_request_total
- diameter_request_timeout_total
- diameter_message_timeout_total

For more information, see the *Statistics/KPI Additions or Changes*.

IPv6 Address Zone Range Validation

Feature Summary and Revision History

Table 25: Summary Data

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

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

In CPS vDRA 22.2.0 and later releases, vDRA supports the IPv6 address validation in the IPv6 Range System ID Mapping CRD table and while configuring IPv6 zone ranges in the CLI.

Note During multi_table update, if any row gets failed due to conflict then entire Custom Reference Data (CRD) table is not updated. Displays a warning message after updating CRD successfully.

For more information see, the *CLI Commands* section in the *CPS vDRA Operations Guide* and *Regular Expression* parameter description in the *CPS vDRA Administration Guide.*

KPI Support to Account the Remote Peers Count

Feature Summary and Revision History

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 SNMP and Alarms Guide*

Table 27: Revision History

Revision Details	Release
First introduced	22.2.0

Feature description

In the CPS 22.2.0 and later releases, vDRA allows you to track a count of active peers (local and active according to the remote peer policy) that are known to a local site.

In Grafana, you can identify the *active_peer_count* KPI with *app_id* and *system_id* parameters in the Peer traffic monitor dashboard.

Configurations and Restrictions

You can configure Grafana and bulk statistics with the *active_peer_count* KPI.

Configure the *PEER_LIMIT_FOR_SITE_EXCEEDED* Alert with this KPI along with *peer_connection_status* to alert when total peers crossed the supported number per site.

For more information on alarms, see the *Sample Alert Rules Table* in the *CPS vDRA SNMP and Alarms Guide*.

Note While deriving a threshold, you can consider the remote policy.

Preventing a Repository from Corruption and Publishing a Corrupted repository

Table 28: 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* *CPS vDRA Operations Guide*

Table 29: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the Policy Builder, during the import and publish process, if there is any invalid or incomplete data being imported it overwrites the current configuration in the SVN. During publishing there is a possibility that the imported data can corrupt the application cache. This can affect the traffic until the data is recovered.

To overcomme this issue, the CPS vDRA provides additional validation facility on the imported data before publishing. vDRA returns appropriate error messages if the import or publish is not successful due to any validation failure.

For more information , see the *Publish Configuration Changes* section in the *CPS vDRA Administration Guide* and the *dra policy-builder-must-plugins plugins-name* CLI section in the *CPS vDRA Operations Guide*.

Set Alarm Severity Based on Configurable Thresholds

Feature Summary and Revision History

Table 30: Summary Data

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

Revision History

Revision Details	Release
First introduced.	22.2.0

Feature Description

In CPS 22.2.0 and later releases, vDRA allows you to:

- Configure thresholds parameter with threshold input as comma separated fields at the time of Alarm severity setup.

Note The **threshold** parameter is optional. This is because not all alerts will have different thresholds.

- Configure the following two type of alerts expression:
  - ascending threshold [HIGH_CPU_USAGE]
  - descending threshold [LOW_MEMORY]

For more information, the *Component Notifications* table and *Configure Different Thresholds* sections in the *CPS vDRA SNMP and Alarms Guide*.

User Audit Enhancements

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	Not Applicable

Table 32: Revision History

Revision Details	Release
First introduced	22.2.0

Feature Description

In the CPS 22.2.0 and later releases, in vDRA, User Audit feature supports the following functionalities:

- Tracks events that are related to user login or logout details in JSON format at the external server.
- Allows you to obtain information that is related to a login or logout for the user.
- Verifies if the action is triggered by the system or kernel or user.
- Allows you to forward them to the external server or Elasticsearch and filter information of these details with specific keywords, which can feed the data to the external tool in JSON format.
- Tracks events that are related to peer connections and tracks peer disconnects /admin disable details.