CPS Release Change Reference, Release 25.1.0

First Published: 2025-04-30

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

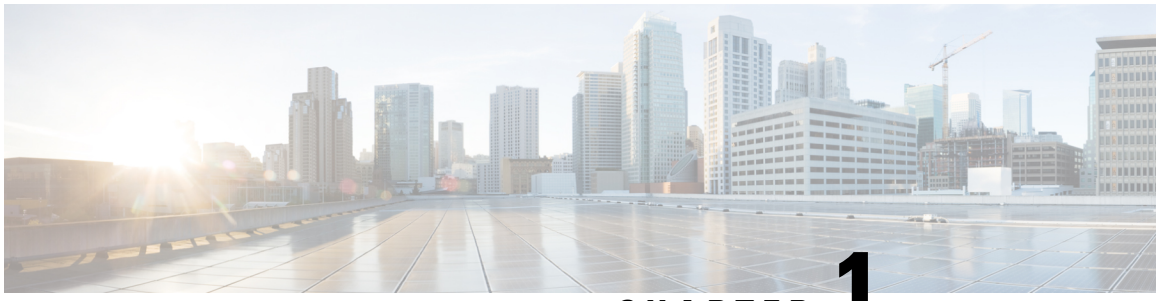
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class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

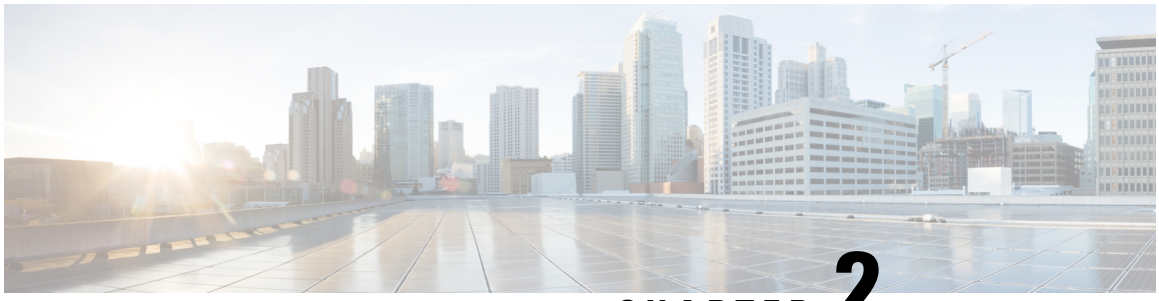
25.1.0 Features and Changes

25.1.0 Features and Changes

Table 1: 25.1.0 Features and Changes

Features/Behavior Changes	Applicable Product(s)/ Functional Area	Release Introduced/ Modified
Additional Directors to Handle Gy/Sy Traffic in vDRA, on page 11	vDRA	25.1.0
PSB Requirements for 25.1.0, on page 9	PCRF/vDRA	25.1.0
Support for MongoDB 7.0 Version in vDRA, on page 4	vDRA	25.1.0
Upgrade Alma Linux to 8.10, on page 3	PCRF	25.1.0
Upgrade MongoDB Version 7.0 in PCRF, on page 6	CPS/vDRA	25.1.0
Support for VMware OVF Tool 4.6.3 , on page 7	PCRF	25.1.0
Support for VMware ESXi Hypervisor 8.0.3 , on page 8	PCRF	25.1.0
Weave Replacement with Docker Overlay Network Driver in vDRA, on page 13	vDRA	25.1.0

25.1.0 Features and Changes



CHAPTER 2

Platform

Upgrade Alma Linux to 8.10

Feature Summary and Revision History

Table 2: 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.	25.1.0

Feature Description

In CPS 25.1.0 release, Alma Linux version 8.9 is replaced with Alma Linux 8.10 along with upgrading to the latest rpm packages and their dependencies.

With Alma Linux 8.10 the kernel version is modified to:

```
# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-553.45.1.el8_10.x86_64
```

```
# cat /etc/redhat-release
AlmaLinux release 8.10 (Cerulean Leopard)

# uname -a
Linux localhost.localdomain 4.18.0-553.45.1.el8_10.x86_64 #1 SMP Wed Mar 19 09:44:46 EDT
2025 x86_64 x86_64 x86_64 GNU/Linux
```

Support for MongoDB 7.0 Version in vDRA

Feature Summary and Revision History

Table 3: 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 4: Revision History

Revision Details	Release
First introduced	25.1.0

Feature Description

This release provides support for MongoDB version 7.0

Upgrade, Migrate, and Backward Compatibility Considerations

- **Supported DRA Releases for Upgrading to 7.0**: You can upgrade vDRA 24.2.0 (mongoDB version,6.0) to vDRA 25.1.0 (mongoDB version, 7.0).
- **Un Supported DRA Releases for Upgrading to 7.0**: Any DRA version prior to DRA 24.2(mongo 6.0) like DRA 24.1 (mongo 5.0), DRA 23.1/23.2(mongo 4.4), 22.2 (mongo 4.2) and previous versions of DRA doesn't support direct upgrade to DRA 25.1 (mongo version 7.0)

  Refer the link for upgrading the replica set to 6.0.

Note Upgrading to DRA 25.1 is supported only from DRA 24.2.

Mongo Java Driver: Current DRA Version 25.1.0 supports mongo java driver 3.12.9.

Prerequisite for upgrading to 25.1.0 from 24.2.0

The following are the common prerequisites for both upgrade and downgrade:

- Run the following CLI before upgrade:

```
#database genericfcvcheck 6.0
```

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 using the **Set** option first and then **Check** to make sure that FCV is replicated on primary members. Upgrade/downgrade should not be triggered if any error is found in the 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).

- Run the following CLI before upgrade:

```
#database dwccheck
```

Note CLI automatically takes care of the defaultWriteConcern version on all databases.

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

Note We recommend using the **Set** option first and then **Check** to make sure that DWC is replicated on primary members. Upgrade/downgrade should not be triggered if any error is found in the above CLI or DWC 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 dwc on all members.
  - **(set/check) << set**
    - **Set**: This option checks and sets defaultWriteConcern.
    - **Check**: This option only checks defaultWriteConcern on all members(primary/secondary).

Upgrade to 25.1..0

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

Downgrade from 25.1.0

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

Upgrade MongoDB Version 7.0 in PCRF

Feature Summary and Revision History

Table 5: 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 6: Revision History

Revision Details	Release
First introduced	25.1.0.

Feature Description

This release provides support for MongoDB version 7.0.

Following are the supported and unsupported CPS releases:

- **Supported CPS Releases for upgrading to 7.0**:

  You can upgrade CPS 24.2.0 (using mongoDB version 6.0.14) to CPS 25.1.0 (using mongoDB version 7.0.14). Upgrade to MongoDB 7.0 is supported only from MongoDB 6.0.

  For example, if you are running a 5.0 series (CPS 24.1.0), you must first upgrade to MongoDB 6.0 (CPS 24.2.0) before you can upgrade to MongoDB 7.0 (CPS 25.1.0).

Important Upgrading to CPS 25.1.0 is supported only from CPS 24.2.0.

- **Un Supported CPS Releases for upgrading to 7.0**:

  Any CPS versions prior to CPS 24.2.0 (using MongoDB version 6.0.14) such as CPS 24.1.0 (using MongoDB version 5.0.20), 23.1.0 or 23.2.0 (using MongoDB version 4.4.18), CPS 22.2.0 (using MongoDB version 4.2.20), or CPS 22.1.1 (using MongoDB version 4.0.27), and previous versions of CPS does not support direct upgrade to CPS 25.1.0 (using MongoDB version 7.0.14).

  To upgrade the Replica set to 7.0, go to https://www.mongodb.com/docs/manual/release-notes/7.0-upgrade-replica-set/

The compatible Java driver for 7.0 is 3.12.9.

Support for VMware OVF Tool 4.6.3

Feature Summary and Revision History

Table 7: Summary Data

Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS Installation Guide for VMware* • *CPS Migration and Upgrade Guide*

Table 8: Revision History

Revision Details	Release
First introduced **Note** This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	25.1.0

Feature Description

Previously, VMware OVF Tool 4.3.0 was used up to the CPS 24.2 release, but it was susceptible to several security vulnerabilities. These vulnerabilities have been addressed in the latest VMware OVFTool 4.6.3 version. For detailed instructions on installing VMware OVFTool 4.6.3, refer to the *CPS Installation Guide for VMware* and the *CPS Migration and Upgrade* Guides.

Support for VMware ESXi Hypervisor 8.0.3

Feature Summary and Revision History

Table 9: Summary Data

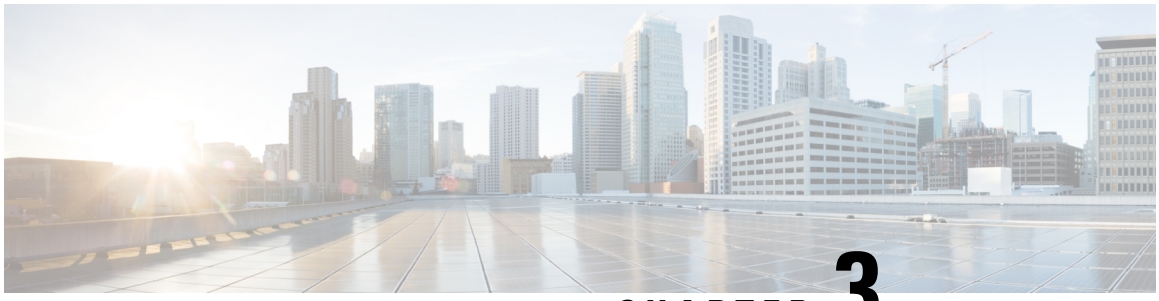
Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS Installation Guide for VMware* • *CPS Migration and Upgrade Guide*

Table 10: Revision History

Revision Details	Release
First introduced **Note** This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	25.1.0

Feature Description

This release provides support for VMware ESXi™ Hypervisor 8.0.3 version. For details about deploying CPS on ESXi 8.0.3, refer to the *CPS Installation Guide for VMware* and the *CPS Migration and Upgrade* Guides.



CHAPTER 3

Security Enhancements

PSB Requirements for 25.1.0

Feature Summary and Revision History

Table 11: 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 12: Revision History

Revision Details	Release
First Introduced.	25.1.0

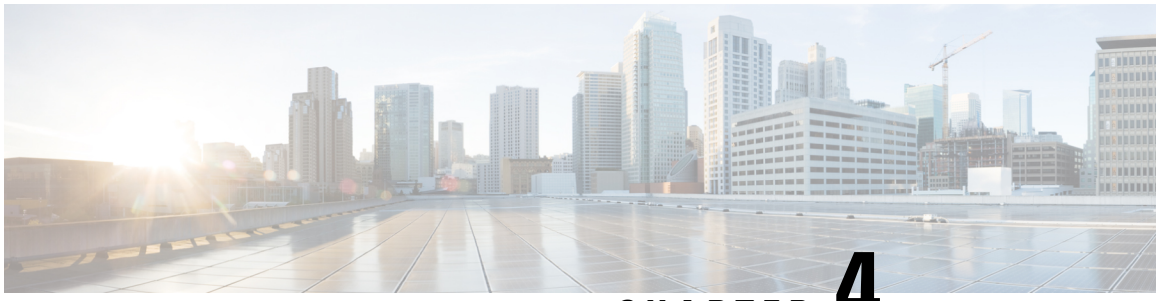
Feature Description

CPS PCRF and vDRA meets the Cisco security guidelines and is aligned with the security features for 25.1.0 release. CPS now supports the following PSB requirements:

Table 13: vDRA PSB Requirements

PSB Item	Description
CT2309: SEC-UPS-TPSQUAL-2	Do not use third-party software with known high risk.
CT2312: SEC-SUP-PATCH-4	Propagate upstream security patches.

PSB Item	Description
CT2315: SEC-UPS-NOBACK-3	Protect against Supplier backdoors, malware, or known vulnerabilities.



CHAPTER 4

vDRA

Additional Directors to Handle Gy/Sy Traffic in vDRA

Feature Summary and Revision History

Table 14: Summary Data

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

Table 15: Revision History

Revision Details	Release
First introduced	25.1.0

Feature Description

In the current deployment, various Virtual IPs (VIPs) manage different types of interface traffic, including Gx, Rx, Sd, Gy, and Sy.

To address the challenges associated with managing Gy/Sy traffic, the deployment is enhanced by adding two additional directors dedicated explicitly to handling Gy/Sy interface traffic.

Implementation Details:

- The two new directors are configured to exclusively manage Gy/Sy interface traffic.

- Existing directors will continue to handle Gx, Rx, Sd, and other traffic types, ensuring balanced and efficient traffic management.
- The separation of IPC channels for Gy/Sy traffic will prevent bottlenecks and enhance the ability of the system to manage incoming traffic more effectively.

Steps to Add New Directors

Use the following steps to add new directors:

1. **Install New Virtual Machines:**
   - Update the setup artifacts with the information for the additional directors.
   - Install the two new virtual machines to accommodate these directors.
2. **Configure VIPs for New Directors:**

   This can be achived in two ways.

   - **Existing VIP configuration:** Update the existing configuration only if a dedicated VIP configuration is present for Gy and Sy by replacing the old director IPs with the new IPs. Use the following CLI command to configure the VIP:

     ```
     network dra-distributor <NAME>
     service <EXISTING-SERVICE-NAME> virtual-router-id <ID>
     interface <INTERFACE-NAME> service-ip <VIRTUAL-IP>
     service-port <PORT> host <DISTRIBUTOR-IP>
     priority <PRIORITY>
     real-server <DIRECTOR-IP>
     ```

     Here is the sample configuration:

     ```
     admin@orchestrator[WPS-DRA-master](config)# network dra-distributor client service
     GySy virtual-router-id 10 interface ens160 service-ip 172.XX.XX.102 service-port
     3868 host 172.XX.XX.104 priority 20
     admin@orchestrator[WPS-DRA-master](config-host- 172.XX.XX.104)# exit
     admin@orchestrator[WPS-DRA-master](config-service-GySy)# host 172.XX.XX.109 priority
      10
     admin@orchestrator[WPS-DRA-master](config-host- 172.XX.XX.109)# exit
     admin@orchestrator[WPS-DRA-master](config-service-GySy)# real-server 172.XX.XX.103
     admin@orchestrator[WPS-DRA-master](config-real-server-172.XX.XX.103)# exit
     admin@orchestrator[WPS-DRA-master](config-service-GySy)# real-server 172.XX.XX.108
     admin@orchestrator[WPS-DRA-master](config-real-server-172.XX.XX.108)# commit
     Commit complete.
     ```

   - **New VIP Configuration:** Add a new VIP configuration with the following CLI command:

     ```
     network dra-distributor <NAME>
     service <NEW-SERVICE-NAME> virtual-router-id <ID>
     interface <INTERFACE-NAME> service-ip <VIRTUAL-IP>
     service-port <PORT> host <DISTRIBUTOR-IP>
     priority <PRIORITY>
     real-server <DIRECTOR-IP>
     ```

     Here is the sample configuration:

     ```
     admin@orchestrator[WPS-DRA-master](config)# network dra-distributor client service
     GySy virtual-router-id 10 interface ens160 service-ip 172.XX.XX.102 service-port
     3868 host 172.XX.XX.104 priority 20
     ```

```
admin@orchestrator[WPS-DRA-master](config-host- 172.XX.XX.104)# exit
admin@orchestrator[WPS-DRA-master](config-service-GySy)# host 172.XX.XX.109 priority
 10
admin@orchestrator[WPS-DRA-master](config-host- 172.XX.XX.109)# exit
admin@orchestrator[WPS-DRA-master](config-service-GySy)# real-server 172.XX.XX.103
admin@orchestrator[WPS-DRA-master](config-real-server-172.XX.XX.103)# exit
admin@orchestrator[WPS-DRA-master](config-service-GySy)# real-server 172.XX.XX.108
admin@orchestrator[WPS-DRA-master](config-real-server-172.XX.XX.108)# commit
Commit complete.
```

Update PB configuration: Add the configuration for the new VIP to the Policy Builder (PB) page.

3. **Include in VMDK Upgrade Sets:** Ensure the new directors are included in the Virtual Machine Disk (VMDK) upgrade sets for consistency and future upgrades.

For more information on the configuration, see the DRA Distributor Configuration Chapter in *CPS vDRA Configuration Guide*.

Weave Replacement with Docker Overlay Network Driver in vDRA

Feature Summary and Revision History

Table 16: Summary Data

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

Table 17: Revision History

Revision Details	Release
First introduced	25.1.0.

Feature Description

This feature outlines the transition from Weave, a third-party software, to a new Container Network Interface (CNI) solution for vDRA. This transition is necessitated by the shutdown of Weaveworks, the provider of Weave software, which was essential for enabling communication between containers across Virtual Machines (VMs) in the vDRA solution.

Prerequiste

Before you migrate from Weave software to Docker Overlay,

- Verify that the system and all container services are fully operational and healthy.
- Ensure the cps.pem file is present in both `/home/cps/` and orchestrator container `/data/keystore/`.
- Execute the network refresh-overlay-config CLI command before starting the network migration to back up the existing overlay-scripts folder and re-create the latest files.

Both the Weave and Docker Overlay networks cannot co-exist in the same site for communication among containers across VMs. The VM /containers running with Docker Overlay network cannot reach other containers in Weave network. Hence, the default network while upgrading to 25.1.0 version will be Weave. Migrating from Weave to Docker Overlay can be initiated once the site is completely upgraded to 25.1.0 version.

Upgrading to 25.1.0:

- Weave is the default network when the site is upgraded to 25.1.0.
- Migration from Weave to Overlay network can be done only after upgrading the site to 25.1.0.
- Initiate the migration from Weave to Overlay at each site sequentially.

Downgrading from 25.1.0:

- Initiate the migration from Overlay to Weave network at each site sequentially.
- Verify if all the VMs are running with Weave network and the system is 100% up.
- Initiate the downgrade to 24.2.0

Configure Docker Overlay Using CLI Command

The feature allows the migration of different VNFs between Weave and Docker Overlay without service disruption through these CLI commands for enabling and disabling network options:

- *network migrate-to-overlay true* - To enable the Docker Overlay network.
- *network migrate-to-weave true* - To enable the Weave network
- *network detach-weave true* - To detach the Weave network after migrating to Overlay network.
- *network detach-overlay true* - To detach the Docker Overlay network after migrating to Weave network.
- *network migration-status* - To verify the current migration status.
- *network refresh-overlay-config* - To refresh the latest Overlay script configuration file update.

Note

- During migration, the trafffic must be switched to other SITE.
- By default, the weave network is enabled.
- When you execute the CLI command, the current network will be disabled.
- The Weave software will not be completely disabled. It is still operational for particular scripts or commands such as **weave status connections**.
- During CNI migration, the running container will need to be re-created when enabling or disabling the network.

For more information, refer the following guides:

- *Configure Docker Overlay Network Driver in vDRA* topic in *CPS vDRA Configuration Guide* for configuring Docker Overlay network.
- *CLI Commands* chapter in *CPS vDRA Operations Guide* for CLI command details.
- *Redeploy VMs during the ISSM Operation with Overlay Network* section in *CPS vDRA Installation Guide* for ISSM configuration with Overlay network.