CPS Release Change Reference, Release 24.1.0

First Published: 2024-03-21

Last Modified: 2024-10-09

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.

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

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface v

About This Guide v

Audience v

Additional Support vi

Conventions (all documentation) vi

Communications, Services, and Additional Information vii

Important Notes viii

CHAPTER 1

Platform 1

Support for MongoDB 5.0 Version in vDRA 1

Upgrade Alma Linux to 8.8 3

Upgrade MongoDB Version 5.0 4

MongoDB Recovery Script for Network Partition Resilience 5

VMware ESXi Hypervisor 7.0.3 Support 7

CHAPTER 2

Security Enhancements 9

Security Enhancements 9

PSB Requirements for 24.1.0 Release 9

CHAPTER 3

vDRA 11

Case Insensitivity for APN Names in CRD Table 11

Support Alerts for Monitoring NTP and SNMP Server Reachability 12

Preface

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

About This Guide

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

This document 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

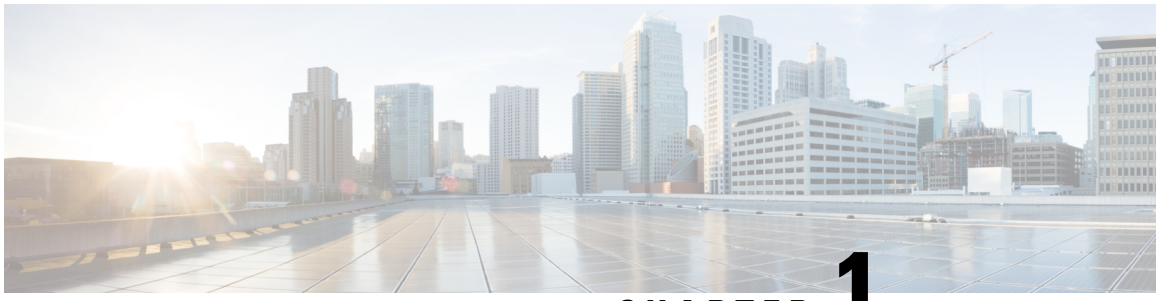
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class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

Platform

- Support for MongoDB 5.0 Version in vDRA, on page 1
- Upgrade Alma Linux to 8.8, on page 3
- Upgrade MongoDB Version 5.0, on page 4
- MongoDB Recovery Script for Network Partition Resilience, on page 5
- VMware ESXi Hypervisor 7.0.3 Support, on page 7

Support for MongoDB 5.0 Version in vDRA

Feature Summary and Revision History

Table 1: 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 2: Revision History

Revision Details	Release
First introduced	24.1.0

Feature Description

This release provides support for MongoDB version 5.0

Upgrade, Migrate, and Backward Compatibility Considerations

- **Supported DRA Releases for Upgrading to 5.0**: You can upgrade vDRA 23.1.0/23.2 (mongoDB version,4.4.18) to vDRA 24.1.0 (mongoDB version, 5.0).
- **Un Supported DRA Releases for Upgrading to 5.0**: Any DRA version prior to DRA 23.2.0/23.1.0 (Mongo 4.4) and previous versions of DRA, does not support direct upgrade to DRA 24.1 (mongoDB version, 5.0)

  Refer the link for upgrading the replica set to 5.0.

Note Upgrading to DRA 24.1 is supported only from DRA 23.1.0 and 23.2.0.

Mongo Java Driver: MongoDB version 4.4 and 5.0 requires Mongo Java Driver version 3.11 and above.

Prerequisite for upgrading to 24.1 from 23.1.0 and 23.2.0

The following are the common prerequisites for upgrade:

- Run the following CLI before upgrade:

  ```
  #database genericfcvcheck 4.4
  ```

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 24.1.0

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

Downgrade from 23.1.0 or 23.2.0

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

Upgrade Alma Linux to 8.8

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.	24.1.0

Feature Description

In CPS 24.1.0 release, Alma Linux version 8.7 is replaced with Alma Linux 8.8 along with upgrading to the latest rpm packages and their dependencies.

With Alma Linux 8.8 the kernel version is modified to:

```
# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-477.27.1.el8_8.x86_64

## cat /etc/redhat-release
AlmaLinux release 8.8 (Sapphire Caracal)

# uname -a
Linux localhost.localdomain 4.18.0-477.27.1.el8_8.x86_64 #1 SMP Thu Feb 8 13:51:50 EST 2024
 x86_64 x86_64 x86_64 GNU/Linux
```

Upgrade MongoDB Version 5.0

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	24.1.0

Feature Description

This release provides support for MongoDB version 5.0. Following are the supported and unsupported CPS releases:

- **Supported CPS Releases for upgrading to 5.0**:

You can upgrade CPS 23.1.0 or 23.2.0 (using mongoDB version 4.4.18) to CPS 24.1.0 (using mongoDB version, 5.0.20). Upgrade to MongoDB 5.0 is supported only from MongoDB 4.4. For example, if you are running a 4.2 series, you must first upgrade to 4.4 before you can upgrade to 5.0.

- **Un Supported CPS Releases for upgrading to 5.0**:

  Any CPS version before CPS 23.1.0 or 23.2.0 such as CPS 22.2.0 (using mongoDB version 4.2.20) or CPS 22.1.1 (using mongodb version 4.0.27) or previous versions of CPS (using mongoDB version 3.x) does not support direct upgrade to CPS 24.1.0.

  To upgrade the mongoDB version to 5.0, you must upgrade to CPS version 23.2.0 or 23.1.0, which uses the mongoDB 4.4 version. For example, if you are running a mongoDB 3.6 series in your CPS release, it is required to first upgrade to 4.0, then to 4.2, and then to 4.4 before planning for any upgrade to 5.0.

  To upgrade the Replica set to 5.0, go to https://www.mongodb.com/docs/manual/release-notes/5.0-upgrade-replica-set/

The compatible Java driver for 5.0 is 3.12.9.

Note Execute the following steps after successfully moving to 24.1.0 (either through fresh install or ISSM):

- Verify whether the DefaultRWConcern configuration for MongoDB is set to 1.
- If the value is not set to 1, run the following script from Cluman to update it to 1.

```
source /var/qps/install/current/scripts/bin/support/mongo/dbcmds.sh

replica_sets=$(perl -wlne 'print if /SETNAME=/../MEMBER1=/;' /etc/broadhop/mongoConfig.cfg
   |awk -F=
/MEMBER1/'{print $2}')
  for set in ${replica_sets[*]}; do
    echo $set;
    x="$MONGO_ADMIN  ${set}   --eval 'db.adminCommand(  {    setDefaultRWConcern : 1,

 \"defaultWriteConcern\": { \"w\" : 1 ,\"wtimeout\" : 0  } })'";
    xx=$(eval $x);
    echo $xx
done
```

MongoDB Recovery Script for Network Partition Resilience

Feature Summary and Revision History

Table 6: Summary Data

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

Related Documentation	CPS Installation Guide for Vmware

Table 7: Revision History

Revision Details	Release
First introduced	24.1.0

Feature Description

Starting with the release of MongoDB 5.0, when a majority of replica set members are unavailable, the MongoDB storage undergoes exponential growth, potentially resulting in a complete database crash and the creation of a black hole in CPS.

MongoDB recovery Script for Network Partition Resilience is designed to handle the scenarios during failover, so that majority of the replica set members are available.

The following `Configuration.csv` parameters are introduced as part of this feature:

- enable_mongodb_majority_failover_monit - Set the value as true or false to enable or disable the feature respectively. **Default Value**: False
- majority_failover_monit_cycles - Set the time interval value in seconds to periodically run the MongoDB recovery Script. **Default Value**: 180 Seconds
- majority_failover_action - Choose any of the following actions on the member which is down:
  - REDUCE_PRIORITY - Reduce the priority and vote the member to 0. (Default, Recommended)
  - REMOVE_MEMBER - Remove the member from the replica set.
- majority_failover_iteration_threshold - Number of iterations the MongoDB recovery Script can wait before taking `majority_failover_action` on a member that is is down. **Default Value**: 3

Following is the sample configuration:

```
enable_mongodb_majority_failover_monit,true,
majority_failover_monit_cycles,180,
majority_failover_action,REDUCE_PRIORITY,
majority_failover_iteration_threshold,5,
```

Note The above MongoDB configuration.csv parameter values change from deployment to deployment, depending on factors such as disk usage and the number of SM VMs per site. We recommend you use appropriate values, as default values might not be suitable for all deployments.

VMware ESXi Hypervisor 7.0.3 Support

Feature Summary and Revision History

Table 8: Summary Data

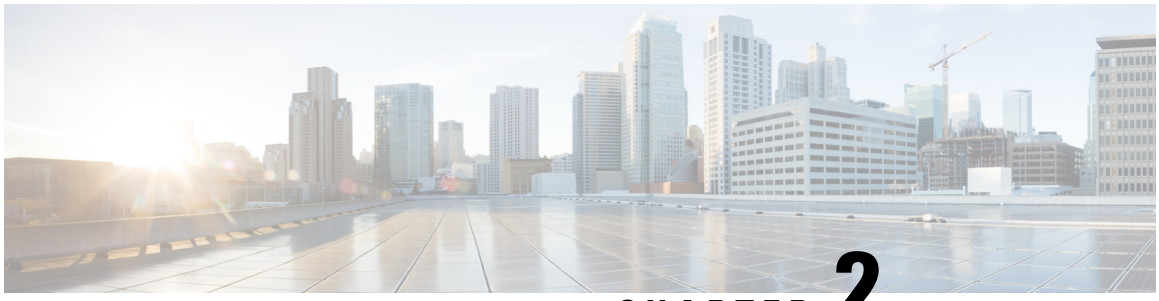
Applicable Product(s) or Functional Area	CPS
Applicable Platform(s)	Not Applicable
Default Setting	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	CPS Installation Guide for VMware CPS Migration and Upgrade Guide

Table 9: Revision History

Revision Details	Release
First introduced **Important** This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	24.1.0

Feature Description

This release provides support for VMware ESXi™ Hypervisor 7.0.3 version. For details about deploying CPS on ESXi 7.0.3, refer to the *CPS Installation Guide for VMware* and *CPS Migration and Upgrade Guide* respectively.



CHAPTER 2

Security Enhancements

- Security Enhancements, on page 9

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 24.1.0 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.	24.1.0

Feature Description

CPS PCRF meets the Cisco security guidelines and is aligned with the security features for 24.1.0 release. CPS now supports the following PSB requirements:

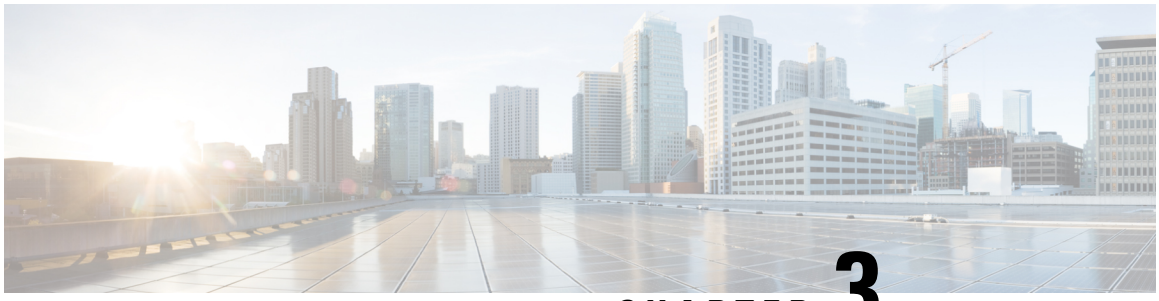
Table 12: CPS PSB Requirements

PSB Item	Description
CT2285: SEC-ASU-STATIC-3	Perform static analysis.
CT2286: SEC-CRY-PRIM-8.	Use approved cryptographic primitives and parameters.
CT2287: SEC-CRY-RANDOM-4	Use approved and well seeded random number generation.

CPS vDRA meets the Cisco security guidelines and is aligned with the security features for 24.1.0 release. vDRA now supports the following PSB requirements:

Table 13: vDRA PSB Requirements

PSB Item	Description
CT2287: SEC-CRY-RANDOM-4	Use approved and well seeded random number generation.
CT2286: SEC-CRY-PRIM-8	Use approved cryptographic primitives and parameters.
CT2285: SEC-ASU-STATIC-3	Perform static analysis.



CHAPTER 3

vDRA

- Case Insensitivity for APN Names in CRD Table, on page 11
- Support Alerts for Monitoring NTP and SNMP Server Reachability, on page 12

Case Insensitivity for APN Names in CRD Table

Feature Summary and Revision History

Table 14: 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 15: Revision History

Revision Details	Release
First introduced	24.1.0

Feature Description

In vDRA, the CRD table supports case insensitivity for APN names in the following tables:

- APN Mapping
- Binding Key Profile Creation Map
- Best Effort Binding

The Called-Station-Id is an unique key value. If the Called-Station-Id input is in upper case, the feature converts it to a lower case value and check for duplicate entries.

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

Support Alerts for Monitoring NTP and SNMP Server Reachability

Feature Summary and Revision History

Table 16: Summary Data

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

Table 17: Revision History

Revision Details	Release
First introduced	24.1.0

Feature Description

vDRA supports the following alerts and KPI extensions for monitoring the NTP and SNMP server reachability and NTP clock skew value:

Alerts

- NTP_SERVER_NOT_REACHABLE - When any of the configured NTP servers are not reachable.
- SNMP_SERVER_NOT_REACHABLE - When any of the SNMP server is not reachable.
- HIGH_CLOCK_SKEW_FOR_NTP_CLIENT - When the NTP clock skew is more than the threshold.

KPI/Statistics

- ntp_server_status - To monitor NTP server reachability status. KPI value is the count of unreachable servers configured.
- snmp_server_status - To monitor SNMP server reachability status. KPI value is the count of unreachable servers configured.
- ntp_client_clock_skew - To monitor ntp server clock skew with the `server_ip` label. KPI value is the NTP client clock skew value.

CLI Commands

The following CLI commands display the server reachability of NTP and SNMP servers:

- `show ntp-server-status` - To display the NTP server reachability.
- `show snmp-server-status` - To display the SNMP server reachability.

For more information, see the *Notification and Alerts* chapter in the *CPS vDRA SNMP and Alarm Guide* and *CLI Commands* chapter in the *CPS vDRA Operations Guide*.