Release Notes for Cisco Prime Collaboration Deployment, Release 14SU4

First Published: 2024-05-30

Introduction

About Cisco Prime Collaboration Deployment

These release notes describe new features, requirements, restrictions, and caveats for Cisco Prime Collaboration Deployment. These release notes are updated for every maintenance release.

Cisco Prime Collaboration Deployment is an application designed to assist in the management of Unified Communications applications. It allows the user to perform tasks such as migration of older software versions of clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

Cisco Prime Collaboration Deployment has four primary, high-level functions:

- Migrate an existing cluster of Unified Communications servers to 11.5 or higher from 10.x and above (this would be Virtual to Virtual)
- Perform operations on existing clusters (11.5 or higher). Examples of these operations include:
  - Upgrade the cluster to a new version (11.5 or higher) of software
  - Switch version
  - Restart the cluster
- Changing IP addresses or hostnames in the cluster on existing Release 10.x or higher clusters.
- Fresh install a new Release 11.5 or higher Unified Communications cluster.

Note Cisco Prime Collaboration Deployment does not support internationalization or languages other than English.

Upgrading to Cisco Prime Collaboration Deployment 14SU3 from Pre-14 source release need COP file *ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn* to be installed to list the Cisco Prime Collaboration Deployment 14SU3 ISO file as valid.

Related Documentation

You can view documentation that is associated with supported applications.

Application	Documentation Link
Cisco Unified Communications Manager	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Contact Center Express	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html
Cisco Unity Connection	http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/tsd-products-support-series-home.html

New and Changed Information

There are no new features added for this release.

Caveats

Bug Search Tool

The system grades known problems (bugs) per severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://bst.cloudapps.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field and click **Go**.

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

Open Caveats

Identifier	Headline
CSCwj78212	Prime Collaboration Deployment Root Shell Access via VMware Tools
CSCwi85229	Vulnerabilities in linux-kernel - multiple versions CVE-2023-51042 a...

Resolved Caveats

Identifier	Headline
CSCwj39514	Install and Migration Task is getting failed after an hour of installation
CSCwi38877	Upgrade task using PCD didn't start after dependent tasks completed
CSCwf63341	Vulnerabilities in linux-kernel - multiple versions CVE-2022-42896
CSCwh23858	Vulnerabilities in openjdk - multiple versions CVE-2023-21968
CSCwi17414	tomcat_threads diagnose test CLI is not working on PCD
CSCwh04518	Critical CVE in component rpcbind. Upgrade to latest version.
CSCwe91124	PCD not adding sftp server with hostname or IP when ESXI has swapped config.
CSCwf42277	Vulnerabilities in libxml2 2.9.1 CVE-2016-4658
CSCwf98603	Vulnerabilities in json-c - multiple versions CVE-2013-6371 and others
CSCwf98668	Vulnerabilities in patch - multiple versions CVE-2018-20969
CSCwh12075	Vulnerabilities in perl - multiple versions CVE-2020-10878 and others
CSCwh18363	Vulnerabilities in libx11 - multiple versions CVE-2021-31535

Identifier	Headline
CSCwh18721	Vulnerabilities in screen - multiple versions CVE-2021-26937
CSCwh18911	Vulnerabilities in rsync - multiple versions CVE-2022-29154
CSCwi09888	PCD: Vulnerabilities in tomcat 9.0.56 CVE-2023-44487 and others
CSCwi53398	Vulnerabilities in jackson-databind 2.13.2.2 CVE-2023-35116