Release Notes for the Ultra Cloud Core Redundancy Configuration Manager Version 2022.01.1

First Published: May 06, 2022
Last Updated: May 06, 2022

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	6-May-22
End of Life	EoL	6-May-22
End of Software Maintenance	EoSM	30-Nov-23
End of Vulnerability and Security Support	EoVSS	30-Nov-23
Last Date of Support	LDoS	29-Nov-24

These milestones and the intervals between them are defined in the Cisco Ultra Cloud Core (UCC) Software Release Lifecycle Product Bulletin available on cisco.com.

Release Package Version Information

Software Packages	Version
rcm.2022.01.1.SPA.tgz	2022.01.1

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2020.02.2.47
Ultra Cloud Core UPF	2022.01.1

Related Documentation

For a complete list of documentation available for this release, go to:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-user-plane-function/tsd-products-support-series-home.html

Installation and Upgrade Notes

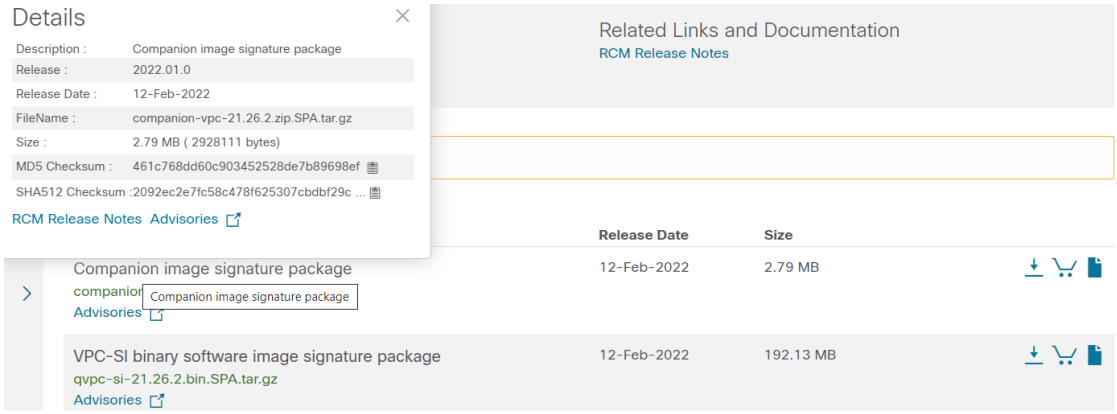
This Release Notes does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

NOTE: For CN deployments, RCM rolling upgrade to 2022.01.0.i6 fails as there is a change from previous versions in specification of checkpoint manager. In CN, cluster manager does cluster sync to do in-service upgrade of the RCM. In doing so, upgrade fails for rcm-checkpoint-manager. As a workaround remedy, execute "**system mode shutdown**" and then perform cluster sync.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details.** To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the table below.

Table 1 – Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command > certutil.exe -hashfile *<filename>.<extension>* SHA512

Operating System	SHA512 checksum calculation command examples
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 <filename>.<extension>

Linux	Open a terminal window and type the following command
	
	$ sha512sum <filename>.<extension>
	
	Or
	
	$ shasum -a 512 <filename>.<extension>

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

MD5 Checksum Details

Software Packages	MD5 Checksum
rcm.2022.01.1.SPA.tgz	b2b5a520b3a0204470b8b3b10a98520f

Certificate Validation

RCM software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

Open Bugs for this Release

None in this release.

Resolved Bugs for this Release

The following table lists the known bugs that are resolved in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

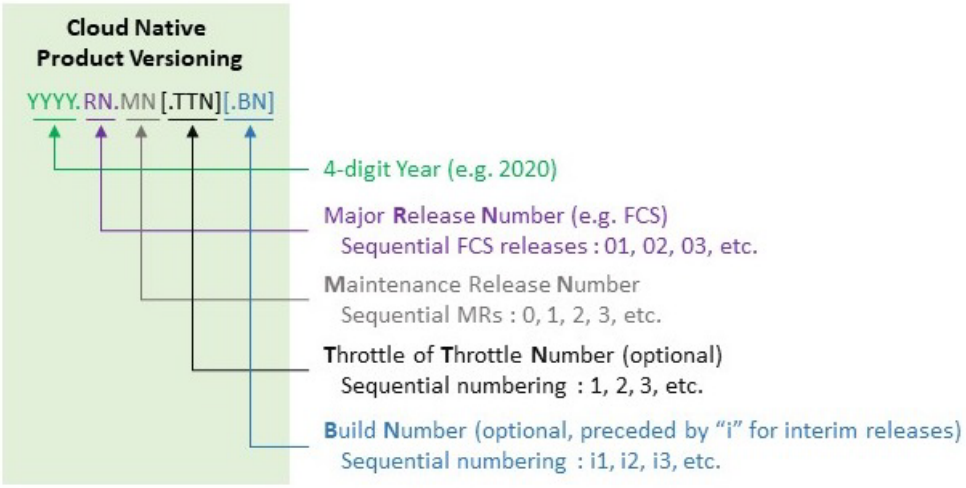
Bug ID	Headline	Product	Behavior Change
CSCwa21578	[soltest] Converged core Data UPF failover time with RCM is between 8 - 11 seconds	RCM	No

Bug ID	Headline	Product	Behavior Change
CSCwa53725	rcm checkpoint manager is not sending flush complete at s/o time after change in up sessmgr count	RCM	No
CSCwa57521	Remove etcd as event notification mechanism from bfdmgr to conctroller	RCM	No
CSCwa64779	RCM HA failing after controller restart	RCM	No
CSCwb12055	CLI to prevent multiple config push notifications towards NSO	RCM	Yes
CSCwb14755	RCM HA switchover is not working after first switchover in CNDP mode	RCM	No
CSCwb23196	RCM S/O via "rcm migrate primary" cli is failing on rcm.2022.01.1.i7	RCM	No
CSCwb24603	RCM HA S/O is triggered automatically on new masterr after keepalived pod is restarted on old mastr	RCM	No
CSCwb26274	RCM Ops-center pod needs restart in case of RCM HA s/o in CNDP Environmemt	RCM	No
CSCwb34749	[CNDP] rcm checkpoint manager crash(intermittent) seen in unplanned UP switchover	RCM	No
CSCwb36803	RCM checkpointmgr planned switchover issues	RCM	No
CSCwb38015	[PLT-RCM] Even after RCM getting into fault state, host reboot is not happening	RCM	No
CSCwb42558	Upgrade Spring Framework to version 5.2.20	RCM	No
CSCwb48335	RCM push corrupted config to UP after unplanned migration from UP	RCM	No
CSCwb60462	[UPF-RCM]Calls are incorrectly put in VOLTE Non active category and are not cleared as well.	RCM	No

Operator Notes

Cloud Native Product Version Numbering System

The **show helm list** command displays detailed information about the version of the cloud native product currently deployed.



The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 2 lists provides descriptions for the software packages that are available with this release.

Table 2 - Release Package Information

Software Packages	Description
rcm.<version>.SPA.tgz	The RCM release signature package. This package contains the deployment software for the RCM as well as the release signature, certificate, and verification information.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.