UCC 5G RCM Release Notes, Release 2024.03.0

First Published: 2024-07-31

Redundancy Configuration Manager, Version 2024.03.0

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	31-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-2027

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.2024.03.0.SPA.tgz	2024.03.0
NED package	ncs-5.6.8-rcm-nc-2024.03.0 ncs-6.1-rcm-nc-2024.03.0
NSO	5.6.8 6.1

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.03.1.12

Products	Version
CDL	1.11.8.1
Ultra Cloud Core UPF	2024.03.0

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
RCM Core Dump Collection and Generation	RCM allows network operators to generate a full memory dump of the applications or pods for analysis and troubleshooting purposes. In addition to logs and statistics, the full core dump eases debugging and provides better serviceability. This feature applies to both SMI and VM-based RCM deployments. You can generate core dump for the Controller, BFDMgr, CheckpointMgr, and ConfigMgr pods. You can use this debug command **kubectl -n rcm exec -it** *pod_name* **-- kill -SIGUSR1 1** to generate a core dump for the required pod. The core dump must be generated upon request from your Cisco account representative only. Default Setting: Not Applicable
UCS C220 M7 Server Qualification	In this release, RCM is functionally qualified on the Cisco UCS C220 M7 server. The Cisco UCS C220 M7 Rack Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization and bare-metal applications.

Behavior Changes

This section covers a brief description of behavior changes introduced in this release.

Behavior Change	Description

ClusterIP Service for Internal Communication	RCM supports a clusterIP service for the Keepalived and BFDMgr host networking pods to listen on for internal requests.
	Previous Behavior: The Keepalived and BFDMgr pods listened on virtual IP address (VIP) for internal REST communication.
	New Behavior: The pods will now listen on the cluster IP address. You can configure custom ports in the RCM Ops Center to run multiple RCM instances in host and non-host networking modes.
	This release supports new CLI commands in Config mode to configure custom ports for the Keepalived and BFDMgr pods to listen on.
	• **k8 smf profile rcm-keepalived-ep custom-port-keepalived** *port_number*—Configure the Keepalived endpoint with the specified port number.
	• **k8 smf profile rcm-bfd-ep** *port_name port_number*—Configure the ports specific to the BFDMgr endpoint with the specified port number.
	Example:
	`[local] rcm# config`
	`[local] rcm(config)# k8 smf profile rcm-keepalived-ep custom-port-keepalived 8082`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep infraadmin-port 8890`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep infraprometheus-port 10091`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep ipc-ep-port 9014`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep metrics-port 8083`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep pprof-ep-port 8860`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep rest-port 9192`
	`[local] rcm(config)# k8 smf profile rcm-bfd-ep resthealth-port 8182`
	Note • If your deployment runs two RCM instances on the same AIO, each port must be different.
	• If your deployment runs only one RCM instance per VM or AIO, then you do not have to set the ports explicitly as the default values will be available already.
	• The **k8 smf profile rcm-bfd-ep setvar bfd-src-ip** *ip_address* CLI is deprecated with this release. This command is not required to display BFDMgr statistics.

Behavior Change	Description

Input Valid Range Values for VRRP Delay	**Previous Behavior:** In the RCM Ops Center configuration, the VRRP delay parameter accepted the old default value of "0" seconds.
	New Behavior: The VRRP delay parameter accepts any value in seconds, that ranges from 1 to 86400. The value "0" is invalid with this release.
	This parameter is configured to delay the start of VRRP instance.
	Example:
	`[local] rcm(config)# k8 smf profile rcm-keepalived-ep vrrp-config group s1`
	`[local] rcm(config-group-s1)# tuning-params vrrp-delay 1`
	`[local] rcm(config-group-s1)# end`
	Note If you must use startup delay for the Keepalived pod, the **k8 smf profile rcm-keepalived-ep init-container init-delay** CLI must be used instead of **tuning-params vrrp-delay**.
	Customer Impact: Prior to the RCM Ops Center upgrade, you must ensure that the **vrrp-delay** parameter has a value in the valid range. If "0" was used in the old configuration, use the **no tuning-params vrrp-delay** command to remove the configuration, and then perform Ops Center upgrade.

Behavior Change	Description
Reset Stale Connections on Standby RCM	**Previous Behavior:** This behavior was observed during RCM switchover: • When RCM starts and transitions to the MASTER state (due to system mode running, an RCM VM reboot, or a switch from MASTER > FAULT > BACKUP > MASTER), the CheckpointMgr pods are restarted even if RCM reports itself as MASTER. • In the BACKUP state, Keepalived restarts the ConfigMgr pod and all CheckpointMgr pods to clean up the state. Although RCM may transition from BACKUP to MASTER, the CheckpointMgr pods may not restart completely by the time the transition occurs. **New Behavior:** The ConfigMgr pod will not restart in BACKUP state. Instead, it will clean up its internal state when RCM enters the non-MASTER state. This release introduces the following behavior during RCM switchover: • RCM supports a new Ops-center CLI command to reset stale TCP connections from the backup CheckpointMgr to the standby UPF: **`k8 smf profile rcm-config-ep reset-stale-connection { true | false }`** Default value: **false** When the configuration is enabled (set to **true**), the CheckpointMgr pods will terminate TCP connections with all UPFs and perform other clean-up tasks when RCM enters the non-MASTER state. The CheckpointMgr pods will not be restarted in the BACKUP state. • When RCM transitions to the non-MASTER state, the RCM controller notifies the ConfigMgr and CheckpointMgr pods about this state change.

Installation and Upgrade Notes

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

RCM Ops Center Logging Levels

It is recommended to use the following logging levels for RCM Ops Center to ensure that logs do not overflow.

```
logging level application debug
logging level transaction debug
logging level tracing off

logging name infra.dpd.core level application off
logging name infra.dpd.core level transaction off
logging name infra.dpd.core level tracing off
logging name infra.application.core level application off
logging name infra.application.core level transaction off
logging name infra.application.core level tracing off

logging name infra.etcd_client.core level application warn
logging name infra.etcd_client.core level transaction warn
logging name infra.etcd_client.core level tracing off
logging name infra.virtual_msg_queue.core level application warn
logging name infra.virtual_msg_queue.core level transaction warn
logging name infra.virtual_msg_queue.core level tracing off
logging name infra.edr.core level application warn
logging name infra.edr.core level transaction warn
logging name infra.edr.core level tracing off
logging name infra.ipcstream.core level application warn
logging name infra.ipcstream.core level transaction warn
logging name infra.ipcstream.core level tracing off
logging name infra.memory_cache.core level application warn
logging name infra.memory_cache.core level transaction warn
logging name infra.memory_cache.core level tracing off
logging name infra.topology_lease.core level application warn
logging name infra.topology_lease.core level transaction warn
logging name infra.topology_lease.core level tracing off
logging name infra.ipc_action.core level application warn
logging name infra.ipc_action.core level transaction warn
logging name infra.ipc_action.core level tracing off
logging name infra.vrf_etcd_update.core level application warn
logging name infra.vrf_etcd_update.core level transaction warn
logging name infra.vrf_etcd_update.core level tracing off
logging name infra.config.core level application warn
logging name infra.config.core level transaction warn
logging name infra.config.core level tracing off
logging name infra.heap_dump.core level application warn
logging name infra.heap_dump.core level transaction warn
logging name infra.heap_dump.core level tracing off
logging name infra.resource_monitor.core level application warn
logging name infra.resource_monitor.core level transaction warn
logging name infra.resource_monitor.core level tracing off
logging name infra.topology.core level application warn
logging name infra.topology.core level transaction warn
logging name infra.topology.core level tracing off
logging name infra.transaction.core level application warn
logging name infra.transaction.core level transaction warn
logging name infra.transaction.core level tracing off
logging name infra.diagnostics.core level application warn
logging name infra.diagnostics.core level transaction warn
logging name infra.diagnostics.core level tracing off
```

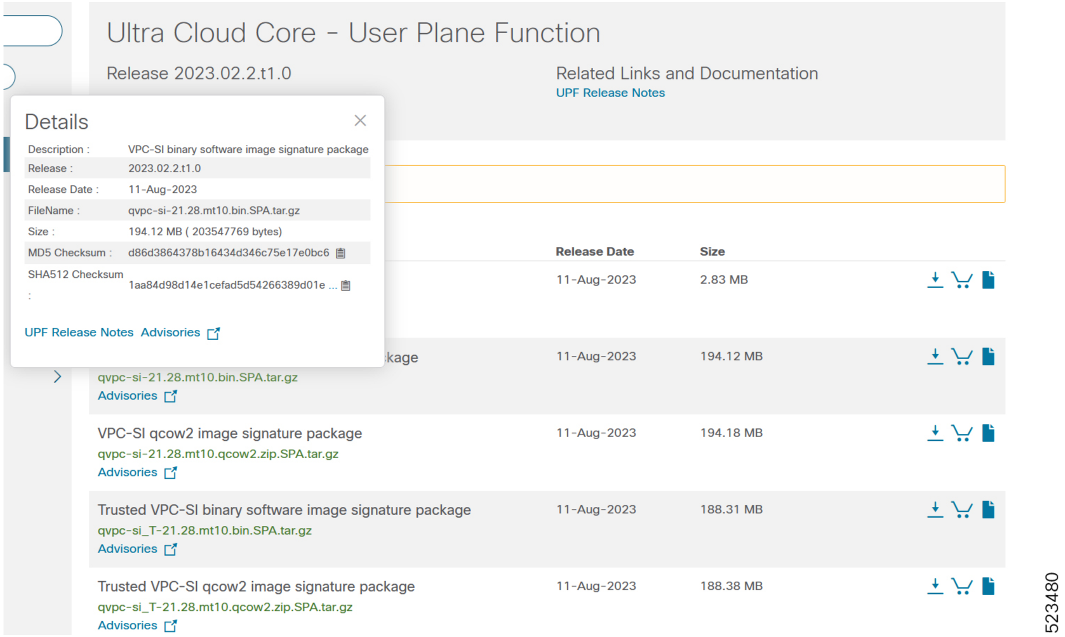
Software Integrity Verification

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.

The following screenshot is an example of a UPF release posted in the Software Download page.

Figure 1:



Ultra Cloud Core - User Plane Function

Release 2023.02.2.t1.0

Related Links and Documentation

UPF Release Notes

Details

Description :	VPC-SI binary software image signature package
Release :	2023.02.2.t1.0
Release Date :	11-Aug-2023
FileName :	qvpc-si-21.28.mt10.bin.SPA.tar.gz
Size :	194.12 MB (203547769 bytes)
MD5 Checksum :	d86d3864378b16434d346c75e17e0bc6
SHA512 Checksum :	1aa84d98d14e1cefad5d54266389d01e ...

UPF Release Notes Advisories

	Release Date	Size
	11-Aug-2023	2.83 MB
…kage qvpc-si-21.28.mt10.bin.SPA.tar.gz Advisories	11-Aug-2023	194.12 MB
VPC-SI qcow2 image signature package qvpc-si-21.28.mt10.qcow2.zip.SPA.tar.gz Advisories	11-Aug-2023	194.18 MB
Trusted VPC-SI binary software image signature package qvpc-si_T-21.28.mt10.bin.SPA.tar.gz Advisories	11-Aug-2023	188.31 MB
Trusted VPC-SI qcow2 image signature package qvpc-si_T-21.28.mt10.qcow2.zip.SPA.tar.gz Advisories	11-Aug-2023	188.38 MB

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, refer to the following table.

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**
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 (for example, .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.

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

There are no open bugs in this specific software release.

Resolved Bugs for this Release

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

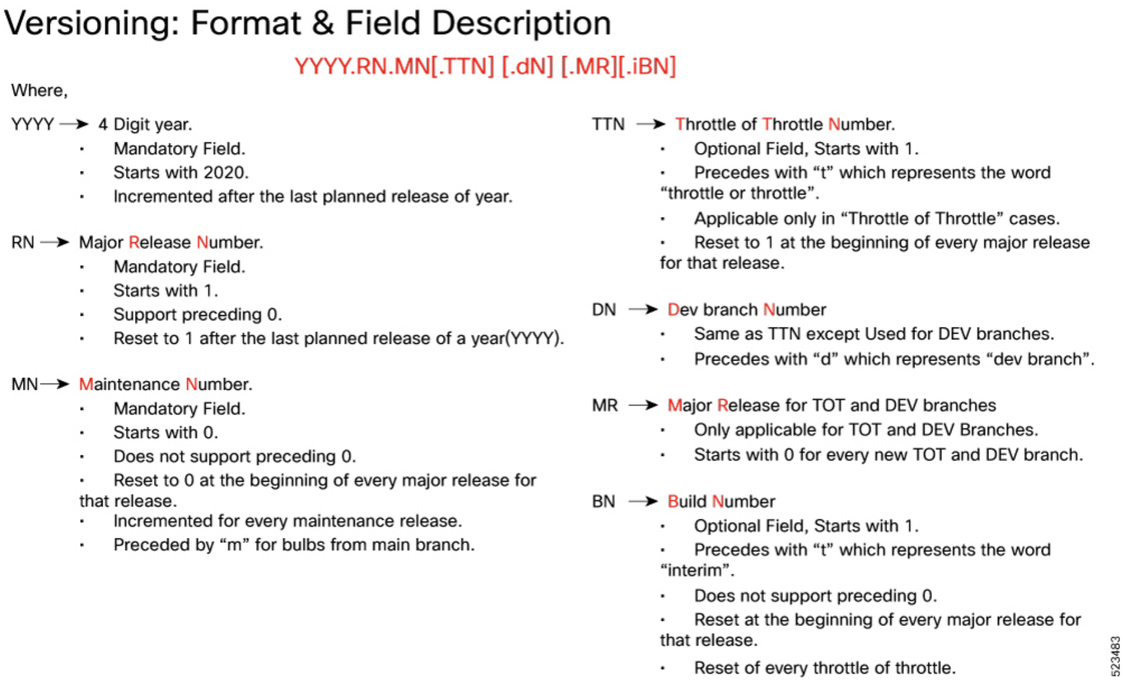
Note This software release may contain resolved bugs first identified in other releases. Additional information for all bugs specific to this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwc34602	ClusterIP service for BfdMgr and keepalived to listen on for internal requests	Yes
CSCwj80455	Resetting Stale Connections from Standby RCM Checkpointmgr to UPFs via new IPC	Yes
CSCwk07581	Ops-center crash due to vrrp-delay=0 in ops-center config	Yes
CSCwk23832	Checkpointmgr--1500 instance# is wrong in checkpoint stats o/p when"IsConnected":false for stdby UPF	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.



Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.

- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.

- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN→ Maintenance Number.

- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number

- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches

- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

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

The following table provides descriptions for the packages that are available with this release.

Software Packages	Description
rcm.<version>.SPA.tgz	The RCM offline release signature package. This package contains the RCM deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-rcm-nc-<version>.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration. Note that NSO is used for NED file creation.

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.