UCC 5G RCM Release Notes, Release 2024.01.1

First Published: 2024-03-26

Redundancy Configuration Manager, Version 2024.01.1

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	30-Apr-24
End of Life	EoL	30-Apr-24
End of Software Maintenance	EoSM	29-Oct-25
End of Vulnerability and Security Support	EoVSS	31-Oct-25
Last Date of Support	LDoS	31-Oct-26

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.2024.01.1.SPA.tgz	2024.01.1
NED package	ncs-6.1-rcm-nc-2024.01.1
NSO	6.1

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.01.1
CDL	1.11.6
Ultra Cloud Core UPF	2024.01.1

What's New in this Release

New in Documentation

This version of Release Notes includes a new section titled **What’s New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all the 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.01, the RCR document will be deprecated.

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
Liveliness Check between UPF and RCM using Heartbeat Communication	The application-level heartbeat mechanism between UPF and RCM allows you to monitor the liveliness of the TCP connection. This feature will resolve the half-closed TCP connections between RCM checkpoint managers and UP session managers. RCM sends a heartbeat message every 3 seconds. It checks if it has received the heartbeat message from UPF in the last 60 seconds. RCM will close the TCP connection if it has not received the message. This behavior is applicable for both Active UP to RCM and RCM to Standby UP communication. UPF also behaves similarly where it sends a heartbeat message every 3 seconds. UPF checks if it has received the message from RCM in the last 60 seconds. If UPF has not received the message, then it will close the TCP connection. The heartbeat functionality is configurable on RCM and UPF using the following commands: • RCM—**k8 smf profile rcm-config-ep enable-up-heartbeat { true | false }** in Config mode • UPF—**up-sm-heartbeat { enable | disable }** in Redundancy Configuration Module mode The following show commands on RCM and UPF display the total number of heartbeat messages received and sent: • RCM—**rcm show-statistics checkpointmgr-endpointstats** • UPF—**show rcm checkpoint statistics sessmgr all** **Default Setting**: Disabled – Configuration required to enable

Behavior Changes

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

Behavior Change	Description
IP Pool Audit Timer Behavior	UPF and RCM support a configurable timer to initiate IP pool audit periodically. **Previous Behavior**: When the **send-ip-pool-audit** CLI in Exec mode was configured, UPF sent the IP pool audit messages to RCM only. **New Behavior**: If you configure the **send-ip-pool-audit** command in Exec mode, UPF will also stop and restart any running audit timer in addition to sending the audit message to RCM. This behavior maintains the periodical audit of configured IP pool chunks.
Sending IP Pool Audit Message Periodically	**Previous Behavior**: RCM did not support the timer to initiate IP pool audit periodically. **New Behavior**: RCM supports the functionality to trigger the IP pool audit message manually using the **send-ip-pool-audit** CLI in Exec mode and to audit the IP pool information periodically with a timer using the **ip-pool-audit interval** *audit_timer* CLI in RCM Service Configuration mode. **Note** This functionality was introduced in release 2024.01.0. • Using the **send-ip-pool-audit** CLI command in Exec mode, RCM sends the IP pool audit message. • Using the **[no] ip-pool-audit interval** *audit_timer* CLI command in the RCM Service Configuration mode, UPF sets a time interval towards RCM controller between successive audits. *audit_timer* is the timer value ranging from 900 to 43200 seconds. The default value of the timer is 1 hour. The **no ip-pool-audit interval** command disables the timer.
Socket Write Timeout Configuration from RCM Controller to UPF	**Previous Behavior:** RCM did not support the I/O timeout configuration for TCP connection between RCM Controller and UPF. **New Behavior:** RCM supports a configurable I/O timeout for TCP socket from RCM controller to UPF. The following CLI command is introduced in the Configuration mode to configure write timeout: **`k8 smf profile rcm-config-ep upf-write-timeout`** *`write_timeout_value`* *write_timeout_value* must be an integer ranging from 300 to 60000 milliseconds. The default value is 1000 milliseconds. **Customer Impact:** The TCP socket from RCM controller towards UPF could get blocked. This CLI can determine the timeout if the TCP socket gets blocked. If an error such as I/O timeout is seen in the controller logs, you can try increasing the timeout value. You can configure the write timeout value based on your tolerance requirements.

Behavior Change	Description
Socket Write Timeout Configuration from RCM CheckpointMgr to UPF	**Previous Behavior:** RCM did not support the I/O timeout configuration for TCP connection between RCM CheckpointMgr and standby UPF SessMgr. **New Behavior:** RCM supports a configurable I/O timeout for TCP socket from RCM CheckpointMgr to UPF. The default value of the write timeout between RCM CheckpointMgr and standby UP SessMgr is 10 seconds. The following CLI command is introduced in the Configuration mode to configure the write deadline timeout during switchover: **`k8 smf profile rcm-config-ep write-timeout`** *`write_timeout_value`* The default value is 10000 milliseconds. **Customer Impact:** The TCP socket from RCM CheckpointMgr towards UPF SessMgr could get blocked. This CLI can determine the timeout if the TCP socket gets blocked. If an error such as I/O timeout is seen in the CheckpointMgr logs, you can try increasing the timeout value. You can configure the write timeout value based on your tolerance requirements.

Behavior Change	Description
TCP Connectivity between Backup RCM and UPF	The RCM CheckpointMgr and ConfigMgr pods will be restarted in the following scenarios: • When RCM is brought up with system mode running • When RCM keepalived pod restarts due to configuration or operation change • When one MASTER RCM moves to BACKUP if dual MASTER resolution is done by VRRP • In CNDP deployment, the pods will be restarted twice in the new BACKUP RCM after RCM HA migration—in the FAULT state first and then in BACKUP state • In VM deployment, the pods will be restarted after booting the RCM VM **Note** It is normal to observe pods restarting even during MASTER state because the pod restart was initiated in the previous BACKUP state and RCM went from BACKUP to MASTER state quickly. **Previous Behavior**: When RCM moved to the BACKUP state directly from the MASTER state, the CheckpointMgrs were not notified and not restarted. Using the **k8 smf profile rcm-keepalived-ep vrrp-config group** CLI, RCM supported default values for the following commands: • **tuning-params script-interval**—30 • **tuning-params fall**—5 **New Behavior**: When the Keepalived pod moves to the BACKUP state from any state or no state (such as RCM startup), it will restart the ConfigMgr pod and all CheckpointMgr pods. Using the **k8 smf profile rcm-keepalived-ep vrrp-config group** CLI, RCM supports new default values for the following commands: • **tuning-params script-interval**—40 • **tuning-params fall**—20 **Customer Impact:** To prevent stray TCP connections between backup RCM and UPFs, some backup RCM pods are restarted when RCM Keepalived moves to the Backup state.

Installation and Upgrade Notes

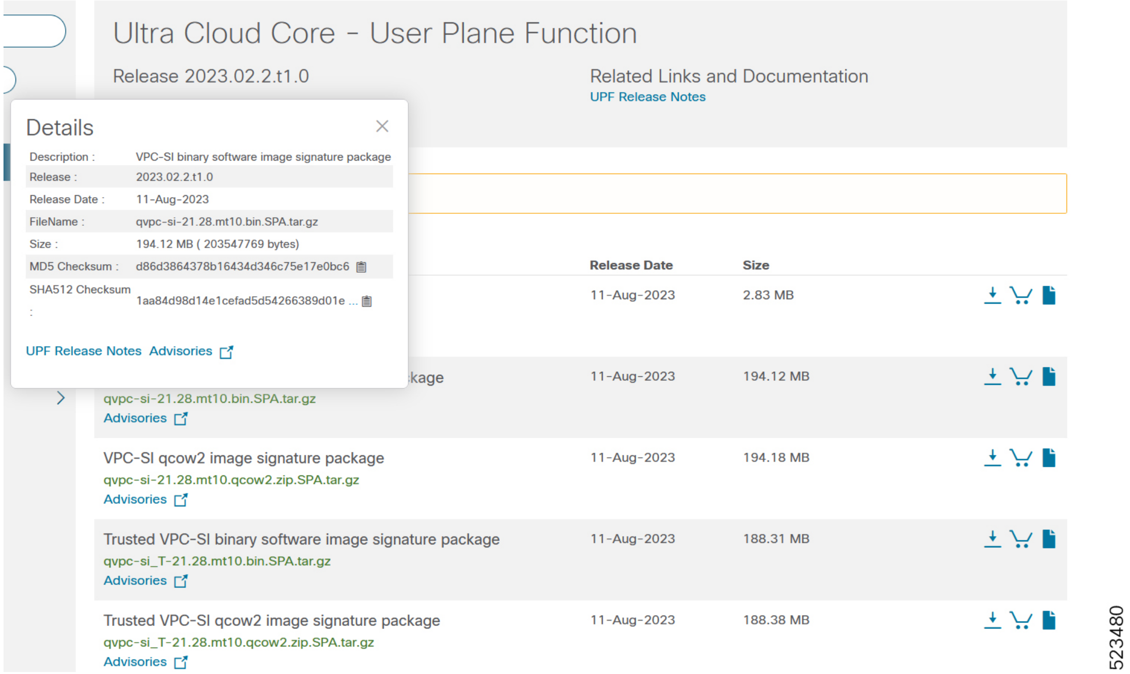
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

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.



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`

Operating System	SHA512 checksum calculation command examples
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.

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.dispatcher.core level application warn
logging name infra.dispatcher.core level transaction warn
logging name infra.dispatcher.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
```

Open Bugs for this Release

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

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

Bug ID	Headline
CSCwj31708	checkpointmgr restart @redmgrtcplocal.go:733

Resolved Bugs for this Release

The following table lists the resolved bugs 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.

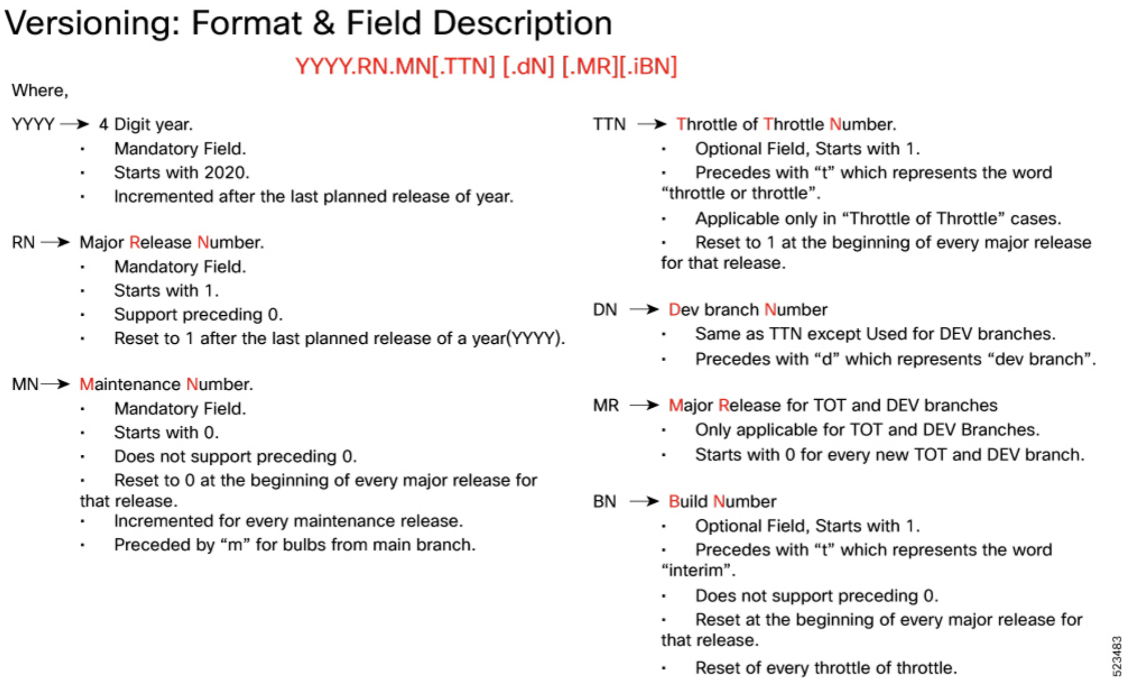
Bug ID	Headline	Behavior Change
CSCwe23786	CLI controlled rcm vpnmgr message to clear the contextpoolinfo in rcm controller	Yes

Bug ID	Headline	Behavior Change
CSCwi68538	RCM-Checkpointmgr crash due to fatal error concurrent map read and map write	No
CSCwi70133	Switchover message should add hostID if its is not present in configmgr	No
CSCwi74961	TCP hardening - Timeout observed during socket write during switchover	Yes
CSCwi79878	IP Pool flush enhancements for planned RCM UPF SWO	Yes
CSCwi87259	StandbySessmgrDisconnected trap is not generated when upf reload due to planned switchover fails	No
CSCwi91381	RCM checkpointmgr to standby UPF smgr connection framework modifications	No
CSCwi94808	Operator configurable IP Pool Chunks push i/o timeout	Yes
CSCwj19662	post sessmgr restart the fullcheckpoint doesnt consider pre-existing recovered calls	No
CSCwj24899	Few sessmgrs having TCP connect issues on Checkpointmgr	Yes

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.