UCC AMF Release Notes, Release 2024.03.0

First Published: 2024-07-31

Ultra Cloud Core Access and Mobility Management Function

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
amf.2024.03.0.SPA.tgz	2024.03.0
cdl-1.11.8.1-amf-2024.03.0.SPA.tgz	1.11.8.1
NED package	ncs-6.1-amf-nc-2024.03.0
NSO	6.1.11

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 6 section.

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2024.03.1.12

Products	Version
Ultra Cloud CDL	1.11.8.1

For information on the Ultra Cloud Core SMI release, refer to the SMI documents available at:

https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/series.html

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
AMF Deployment on Four Servers	AMF now supports deploying a single AMF instance across a four-server configuration using M5 servers. This setup includes three master servers and one worker server. This deployment provides an enhanced scalability and reliability with the AMF instance distributed across the available M5 servers.
Equipment Identity Register (EIR)	This feature allows the AMF to interact with EIR to validate the UE identity during the UE registration procedure. EIR check enhances the network management by tracking and managing the status of the devices. Command introduced: **eir-check { enabled | emergency-registration | deny-greylisted | initial-registration }** Default Setting: Disabled – Configuration Required
Event Data Record (EDR) Support	AMF supports the storage of the EDR files in the EDR monitor pods. You can use the EDR files for debugging and troubleshooting. Command introduced: **edr reporting { enable [all subscribers | file [transaction | transaction-collision]] | disable file [transaction | transaction-collision] }** Default Setting: Disabled – Configuration Required

Feature	Description
Rolling Upgrade Optimization	AMF provides the following support for rolling upgrade optimization: • Retry mechanism at service and protocol pods during upgrades • Configuration-based rolling upgrade enhancements This optimization helps in reduced session and call events per second (CEPS) loss during the upgrade procedure. The configurable rolling upgrade enhancements enable smooth rollout of the changes. **Note** It is recommended that you enable the merged mode in the GTPC endpoint configuration to optimize the performance. Command introduced: • **supported-features [app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra]** in AMF service configuration mode. • **interface n26 { vip-ip** *vip_ip_address* **}** in GTP endpoint configuration mode. Default Setting: Disabled – Configuration Required

Behavior Changes

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

Behavior Change	Description
Generate Pod Logs in JSON Format	**Previous Behavior**: AMF did not have functionality to generate pod logs in JSON format. However, this functionality was present in the CDL application. **New Behavior**: AMF can now generate pod logs in JSON format using the **logging json-logging [application | monitor-subscriber | transaction]** CLI command. Once this feature is activated, all AMF-related application pods begin generating logs in JSON for the selected log types.

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.

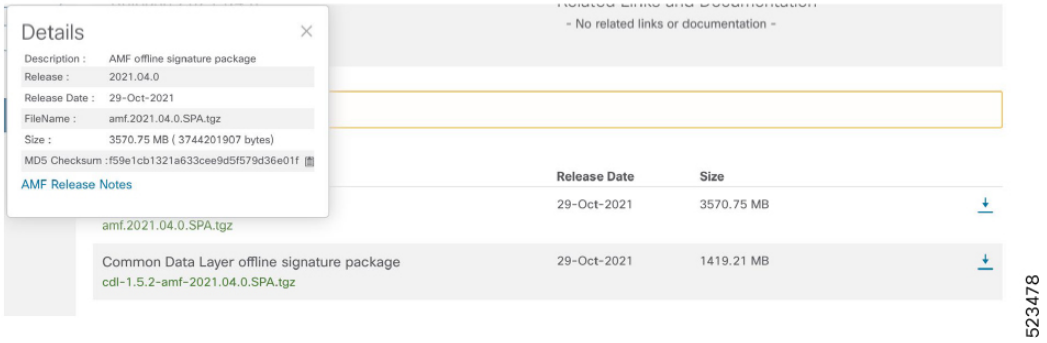
Certificate Validation

AMF 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.

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 will find the SHA512 checksum. If you do not see the whole checksum, you can expand it by pressing "..." 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 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**
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
Note 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.

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 is available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwk45189	Rest ep pod crash at infra.(*RestRouter).populateHttpResponse
CSCwk63875	AMF does NRF discovery of SMF instead of using the same SMF as before N2HO handover
CSCwk72821	Rest ep pod crash at nrfnfdproto.(*PlmnId).MarshalToSizedBufferVT
CSCwk88929	Error"ID allocation failed" in node manager due to high go routine seen during AMF performance run

Resolved Bugs for this Release

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

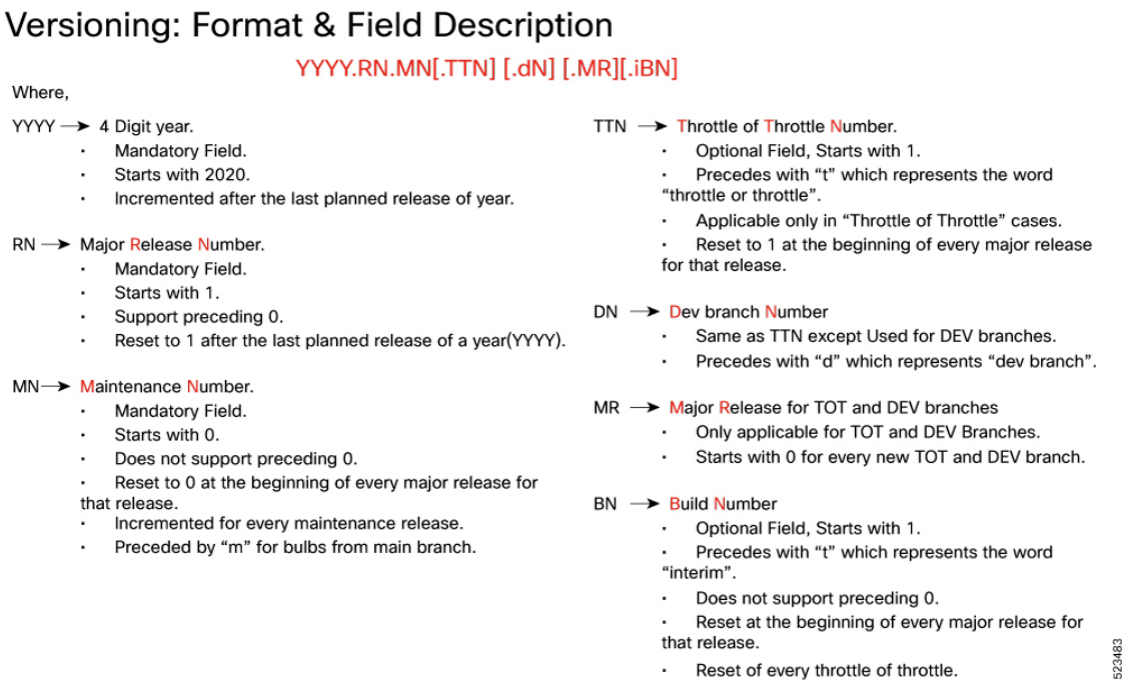
Note This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Behavior Change
CSCwi71509	Memory consumption of Stand-by Protocol-ep pod is high during performance run	No
CSCwk27765	Invalid Entry for peer is seen in show peer CLI output	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

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

Table 2: Release Package Information

Software Packages	Description
amf.<version>.SPA.tgz	The offline release signature package. This package contains the AMF deployment software, NED package, as well as the release signature, certificate, and verification information.
ncs-<nso_version>-amf-<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 the 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.