Release Notes for the Ultra Cloud Core Access and Mobility Management Function Version 2021.04.1

First Published: February 7, 2022
Last Updated: February 7, 2022

Introduction

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

Release Package Version Information

Software Packages	Version
amf.2021.04.1.SPA.tgz	2021.04.1
cdl-1.5.2-amf-2021.04.1.SPA.tgz	1.5.2

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

Verified Compatibility

Products	Version
Ultra Cloud Core SMI	2020.02.2.i41
Ultra Cloud CDL	1.5.2

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

Related Documentation

For the complete list of documentation available for this release, go to: https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-access-mobility-management-function/products-installation-and-configuration-guides-list.html

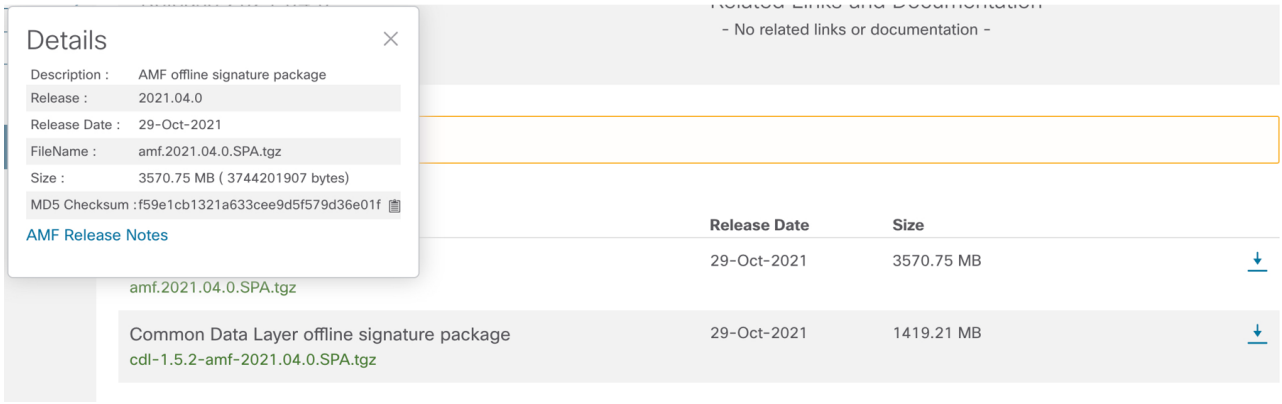
Installation and Upgrade Notes

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

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 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
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.

Certificate Validation

The software images are signed via x509 certificates. For information and instructions on how to validate the certificates, refer to the .README file packaged with the software.

Open Bugs for this Release

The following table lists the known bugs that were found in this software release, and which remain open.

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	Product
CSCvu94428	N26: Mon sub support for GTPC messages is missing	AMF
CSCvz71315	Reg's getting rejected as implicit detach	AMF
CSCvz82099	Periodic registration rejected, but UE context at AMF is not deleted.	AMF
CSCvz86590	Reg's failing in 2/7 AMF apps, takes higher execution times	AMF
CSCvz87609	Unsupported query-param for nrf discovery should be removed from cli	AMF
CSCvz97651	SVI Paging call model not working after x, looks like uectxt release taking more time	AMF
CSCvz99540	AMF: IN EAP-AKA After ERROR CODE 404 we are not able to get Authentication Reject	AMF
CSCwa06705	AMF-sequence number value is not updating properly on MDF2_AMF_REGISTRATION, DEREGISTRATION etc.	AMF
CSCwa36938	5Gaas: AMF Sending Registration Request to UDM even for GUTI Identity	AMF
CSCwa61789	"Id Deallocation failed" errors leading to "ID_not_allocated" in node manger	AMF
CSCwa68516	AMF is not updating the SMF about the PDN for roaming scenario in context transfer	AMF
CSCwa70670	MobilityRestriction IEs not sent in Service Accept after Paging	AMF
CSCwa76453	Mobility Registration post N2 or N26 HO triggers UDM registration for emergency UE	AMF
CSCwa78338	Registration getting rejected in case of N2Ho target AMF as DUT emg with cli w/o override	AMF
CSCwa81105	AMF isnt sendig PDUSession Rel to vSMF after 5g to 4G N26HO resulting a stale session on vSMF	AMF
CSCwa82033	RPC error OnN1N2TransferFailureUcnnmRequest observed after master reboot	AMF
CSCwa82748	Affinity issue in N26 HO (5G-4G) with UDM Rsp	AMF
CSCwa83240	AMF does not trigger deRegistration for restriction config change after Service request	AMF

Bug ID	Headline	Product
CSCwa83342	AMF adds MobilityRestriction IEs in Registration except for emergency registration	AMF
CSCwa83674	AMF sends PUT request for the endpoint SBI VIP offline	AMF
CSCwa83884	slice selection:2nd registration of ICSR we are getting 1st registration NSSAI values buffer overflow	AMF
CSCwa84737	T-AMF is sending PDU resource setup request to GNB even when no PDU activation is involved.	AMF
CSCwa85066	DeReg req with NGAP ID=0 after ServiceReq in idle mode - restriction config change	AMF
CSCwa85208	AMF: in Data change notification response if SUPI is changed then instead of 404 we are getting 500	AMF
CSCwa85301	Mobility reg after idle mode not getting rejected after rat restriction NR applied by cli	AMF
CSCwa86289	S-AMF is not deleting PCF association while reg again and deregistration scenario.	AMF
CSCwa86311	S-AMF is sending wrong reject error code on receiving unknown GUTI in Transfer Update Req	AMF

Resolved Bugs for this Release

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

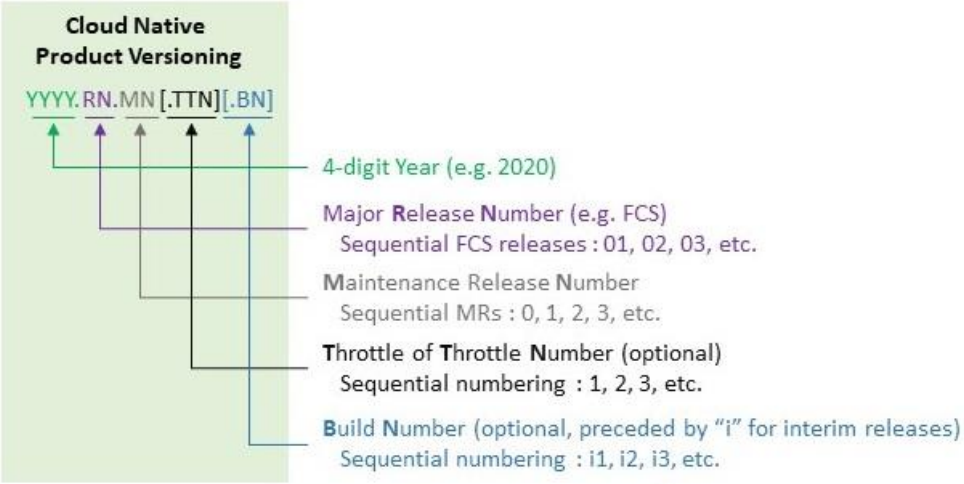
NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Product	Behavior Change
CSCvy91266	F106535_retry-and-continue, continue not working as expected with PCF interface_i41 build	AMF	No
CSCvz38359	AMF is not sending HO Preparation failure when there is no response for fwd relocation req	AMF	No
CSCvz69348	[AMF-Timers]: HO supervisory timer not getting triggered in case of AMF to EPC HO over N26	AMF	No
CSCvz89052	UE Security Capability in HO Req (4G to 5G HO) N26 HO	AMF	No
CSCvz91937	Inter AMF registration at New AMF fails due to affinity issues.	AMF	No
CSCvz94736	OAM POD crash when doing show sub SUPI imsi-xxxx	AMF	No
CSCwa06936	5G to 4G Idle HO is failing with Context Not Found(64)	AMF	No
CSCwa35193	N26 Handover Failure due to incorrect affinity selection at GTPC-ep.	AMF	No
CSCwa36287	AMF is performing NGAP release before sending registration accept on that NGAP connection.	AMF	No
CSCwa45512	MDF message MDF2_AMF_UNSUCCESSFULPROCEDURE Proc_Type IEs is printing wrong value on build I181	AMF	No
CSCwa47060	Service pods crashed during Resiliency Events	AMF	No

Bug ID	Headline	Product	Behavior Change
CSCwa51774	Evaluation for Log4j RCE (Log4Shell) Vulnerability - AMF	AMF	No
CSCwa52662	AMF crash when monitor the AMF-OPS	AMF	No
CSCwa54615	Evaluation of SMF for Log4j 2.x DoS vulnerability fixed in 2.17	AMF	No
CSCwa58567	The 5GC will send extra code in PDU session with i95 and i144 AMF	AMF	No

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 provide 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 deployment software 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.