Release Notes for the Ultra Cloud Core Session Management Function Version 2020.02.2

First Published: May 29, 2020
Last Updated: May 29, 2020

Introduction

This Release Notes identifies changes and issues related to this software release. This release is the next release after 2020.02.1.

Release Package Version Information

Software Packages	Version
smf.2020.02.2.SPA.tgz	2020.02.2

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	2020.02.1
Ultra Cloud Core PCF	2020.02.1.65
Ultra Cloud Core UPF	2020.02.2

Enhancements and Behavior Changes

PDU Session Cache Conflict Handling Support

The smf-service pods support handling of affinity failure and redirects the request messages to the appropriate pod for the corresponding session. A new metrics is introduced to identify the number of redirects with labels, Message Type, and Sync/Aysnc.

Prioritization of RA Procedure over PDU Session Modification in Case of a Collision

In previous releases, the SMF queued the Router Advertisement (RA) and Router Solicitation (RS) messages when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request.

In the current release, the SMF sends the RA message and also responds to the RS message when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request. That is, the SMF prioritizes the processing of RA and RS messages over the PCF-initiated PDU Modification Request.

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-session-management-function/tsd-products-support-series-home.html

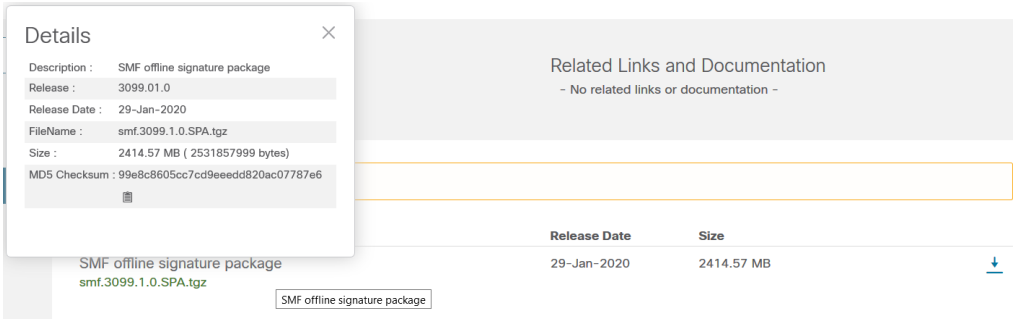
Installation and Upgrade Notes

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.



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
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

SMF 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

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
CSCvu14928	[SVI-SMF] After multiple call-model iterations, entries under sessions affinity not cleared
CSCvu17321	[SMF-SVI] PDU Session Release - SMF initiated ProcStatusComplete takes more than 5secs to process
CSCvu23582	[SMF-SVI] Drain Node (Protocol VM [which has UDP-Proxy - Standby]) - - > Sx Path Reset
CSCvu38791	[SMF-IVT] WIFI to NR HO - Modified QOS values from PCF during HO not taking effect

Resolved Bugs for this Release

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

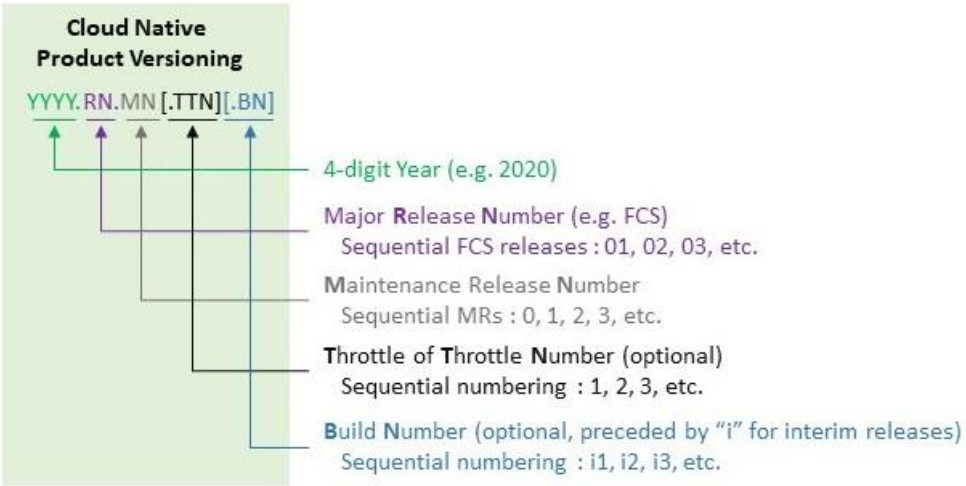
NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCvq16989	[SMF-SVI] NRF Heart-beat procedure is not handled as expected
CSCvt95054	[SVI-SMF] Wifi-5G-EPSFB PDU UnTrusted WiFi to 5G to EPS Fallback stats support
CSCvt97943	[SVI SMF] small num of 404 not found errors on n2ho with partial fail for PDU session mod complete
CSCvu00921	[SMF-IOT] SMF is not handling AN-release procedure when received after Handover during EPSFB
CSCvu00941	[SMF-IVT] DL FARs are not removed in N4 during 5G to 4G HO for failed bearers in MBReq
CSCvu13936	PGW-C is using TEID as 000 in PFCP delete session request.
CSCvu15973	ControlPlane inactivity timer support
CSCvu19134	[SMF-IOT] SMF has to prioritise RA procedure over PDU session modification when there is a collision

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 packages that are available with this release.

Table 2 – Release Package Information

Software Packages	Description
smf.<version>.SPA.tgz	The SMF offline release signature package. This package contains the SMF 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.