Release Notes for the Ultra Cloud Core Session Management Function Version 2020.02.3

First Published: July 10, 2020
Last Updated: July 10, 2020

Introduction

This Release Notes identifies changes and issues related to this software release. This release is the next release after 2020.02.2.

Release Package Version Information

Software Packages	Version
smf.2020.02.3.SPA.tgz	2020.02.3

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

Verified Compatibility

Products	Version
Ultra Cloud Core PCF	2020.02.1.65
Ultra Cloud Core SMI	2020.02.1
Ultra Cloud Core UPF	2020.02.3

Enhancements and Behavior Changes

Authorized QoS Handling for Default Bearer

The SMF allows modification of the authorized default Quality of Service (QoS) of a session rule whenever the user's quota exhausts. The QoS can be QoS Class Identifier (QCI) or 5G QoS Indicator (5QI), session Aggregate Maximum Bit Rate (AMBR), or both QCI/5QI and session AMBR.

When the user replenishes the quota, the PCF reverts to the previous authorized QoS for the default bearer.

Configuration Support for TFT Packet Filters

The SMF provides a new CLI command “max-supported-pkt-filter” to allow the configuration of maximum Traffic Flow Template (TFT) packet filters supported per 4G/5G call.

Previous Behavior: In previous releases, the maximum TFT packet filter value for a 4G or 5G call (including the TFTs for all the bearers or flows) was limited to 16.

The SMF used to assign the TFT packet ID sequentially whenever the PCC rules are sent from PCF irrespective of the bearers/flows.

New Behavior: In this release, the maximum TFT filter value is 16 per bearer/flow, and 256 per 4G/5G call. The maximum TFT packet filter is now configurable with the **max-supported-pkt-filter** CLI command. If this CLI command is not configured, a maximum of 16 TFT filters are allowed per 4G or 5G call.

NOTE: The maximum TFT filter configurable limit is applicable for 5G sessions only if there is no maximum TFT packet filter limit sent from the UE.

If the UE sends the maximum packet filter value in a 5G call, then the configured value is overridden. The UE sent value for maximum packet filter is applicable for both the 4G and 5G sessions.

Now, the SMF assigns the TFT packet filters on per bearer/flow basis. That is, the SMF increments the TFT packet ID based on the last count of ID in that bearer.

Use the following configuration to enable the configuration for maximum TFT packet filters.

```
configure
  policy network-capability policy_name
    max-supported-pkt-filter max_filter_value
    end
```

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

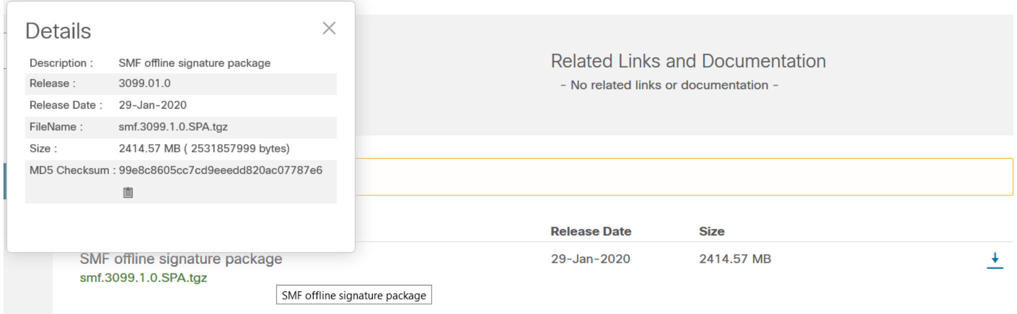
Installation and Upgrade Notes

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.



Details

Description : SMF offline signature package
Release : 3099.01.0
Release Date : 29-Jan-2020
FileName : smf.3099.1.0.SPA.tgz
Size : 2414.57 MB (2531857999 bytes)
MD5 Checksum : 99e8c8605cc7cd9eeedd820ac07787e6

Related Links and Documentation
- No related links or documentation -

	Release Date	Size
SMF offline signature package smf.3099.1.0.SPA.tgz	29-Jan-2020	2414.57 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 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.

None in this release.

Resolved Bugs for this Release

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

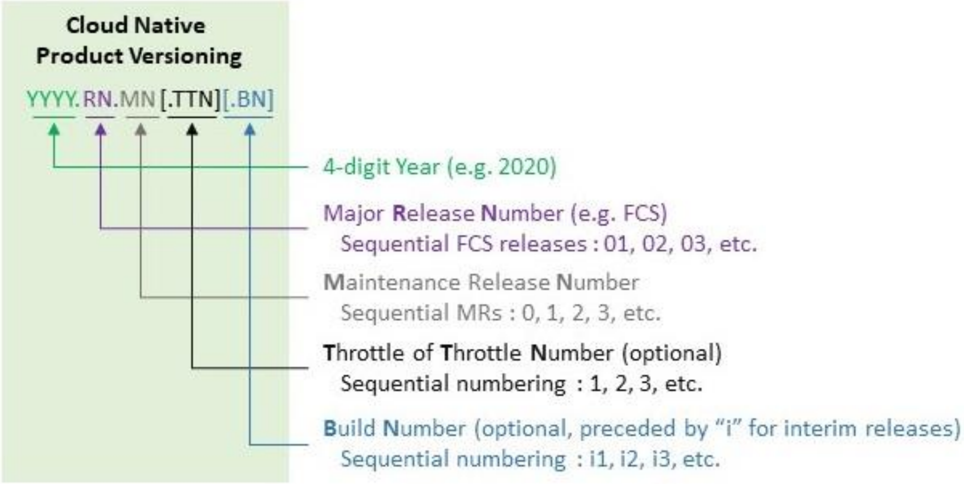
NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCvu34436	[SMF]: SMF sends 2nd CBR with different Precedence when Dedicated bearer proc is aborted due to MBR.
CSCvu38791	[SMF-IVT] WIFI to NR HO - Modified QOS values from PCF during HO not taking effect
CSCvu41546	[SMF]: SMF update duplicate entry for ipv6 prefix in CDL
CSCvu43268	[SMF]: SMF Installing voice flow in 4g to 5g idle mode MRU
CSCvu45463	[SMF]: SMF sends N1N2 PDU REL CMD and Notification status for 5g create over create.
CSCvu46533	[SMF-IOT] TFT issues in UpdateBearerRequest during multi party scenario
CSCvu49408	[SMF] Only NR Capable UE support on SMF + PGW-C node
CSCvu57487	[SMF] SMF not copying the seq no from Del Br Cmd to Del Br Request
CSCvu74715	[SMF] SMF using non standard cause (\"Update Failure\") while returning status 500
CSCvu79719	[SMF] SMF to handle collision between PDU Mod Fail and idle to connected mode
CSCvu87465	[SMF]During 4G to 5G Idle mode mobility, SMF is sending additional PDU_RES_SETUP_REQ msg to AMF
CSCvu89792	Rolling update from i95 to i96 is causing rest-ep and upd-proxy pods to restart
CSCvu93200	[SMF] : SMF retransmit N1 when N2 fails during PCF init Modification.
CSCvu94607	[SMF] : SMF sends optional Tunnel information during PCF init modification for non GBR flow

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.


Cloud Native
Product Versioning
YYYY.RN.MN[.TTN][.BN]
4-digit Year (e.g. 2020)
Major Release Number (e.g. FCS)
Sequential FCS releases : 01, 02, 03, etc.
Maintenance Release Number
Sequential MRs : 0, 1, 2, 3, etc.
Throttle of Throttle Number (optional)
Sequential numbering : 1, 2, 3, etc.
Build Number (optional, preceded by "i" for interim releases)
Sequential numbering : i1, i2, i3, etc.

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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.