Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2020.02.2.3.08

First Published: June 03, 2022
Last Updated: June 03, 2022

Introduction

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

Release Package Version Information

Software Packages	Version
smi-install-disk.20210416.iso.SPA.tgz	20210416
cee.2020.02.2.3.08.SPA.tgz	2020.02.2.3.08
cluster-deployer-2020.02.2.3.08.SPA.tgz	2020.02.2.3.08

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

Feature and Behavior Changes

Refer to the Release Change Reference for a complete list of feature and behavior changes associated with this software release.

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-subscriber-microservices-infrastructure/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.

Notes and Considerations

To upgrade the CEE release version, set it in system mode shutdown and then initiate its upgrade from Cluster Manager (CM). After the CEE Ops Center upgrade is complete, set the CEE back into running mode.

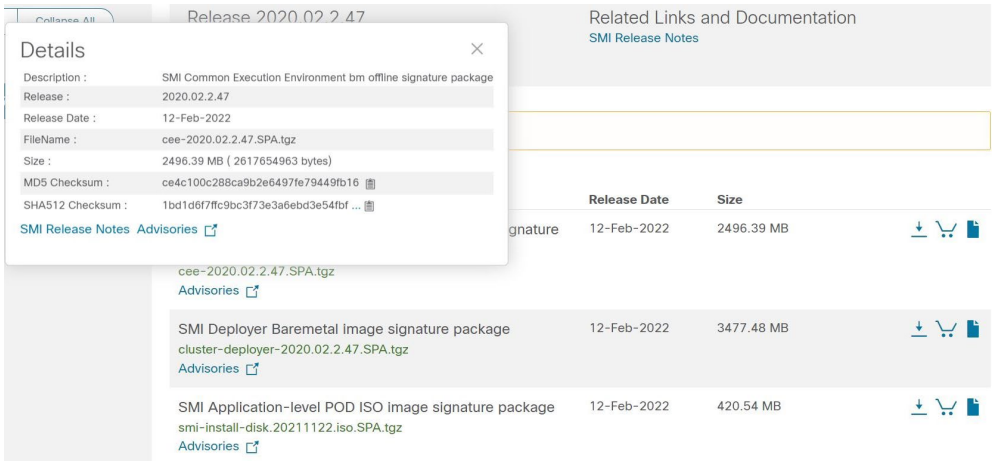
To rollback CEE to any previous version, follow the next steps:

1. Set CEE in system mode shutdown.
2. After the Postgres pods are removed, then remove the Postgres persistent data directories, /data/cee-namespace/data-postgres-* on all three master or oam nodes.
3. Initiate the CEE rollback from CM node.
4. After the CEE Ops Center is downgraded, set it back into running mode.

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 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

SMI 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

None for this 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.

Resolved Bugs for This Release

The table below highlights the known bugs that are resolved 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.

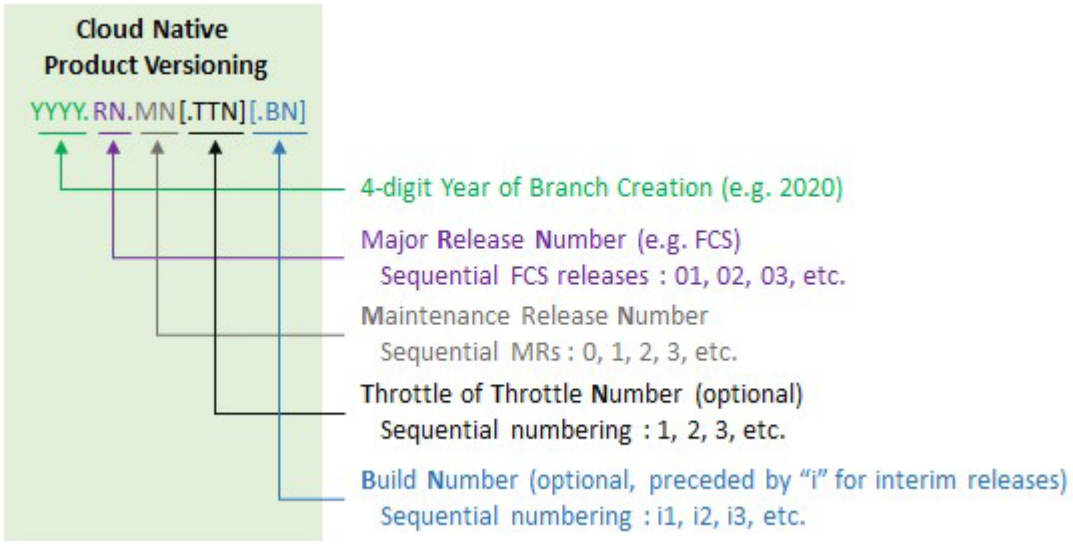
Bug ID	Headline	Behavior Change
CSCwb57923	CEE Monitoring Dashboard Not Showing Total CPU on CM nodes	No
CSCwc00016	Cluster Sync task "kubeadm-worker: Delete node if already joined" not able to load the exact node	No
CSCwc04302	CVE-2022-1292 - Upgrade CiscoSSL to 7.2.410 (1.1.1o)	No
CSCvz61826	Grafana access is lost for ~2 min when any of the mastr nodes are rebooted	No
CSCwb84661	Istio - primay node shut and observed session create timeout, grpccodedeadline exceeded	No
CSCwa19367	Log collection fails: Fluentbit fills up disk during high load	No
CSCwa97233	Log forwarding to fluent endpoint not working	No

Bug ID	Headline	Behavior Change
CSCwb72172	Postgres failing with Bus error (core dumped)	No
CSCvz62367	SIGSEGV causes fluentbit crash with coredump after node reboot	No
CSCwa59409	SMI High Memory Alert generates duplicates	No
CSCwb96044	[soltest] VIP movement during SMF upgrade is causing gARP broadcast with incorrect MAC	
CSCwa54238	Upgrade of Log4j 1.x to 2.16+ in smi and evaluation of CVE-2021-4104	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

Table 2 lists descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Software Packages	Description
base.<version>.iso.SPA.tgz	The application-level POD ISO image signature package for use with bare metal deployments. This package contains the base ISO image as well as the release signature, certificate, and verification information.

Software Packages	Description
cee.<version>SPA.tgz	The SMI Common Execution Environment (CEE) offline release signature package. This package contains the CEE deployment package as well as the release signature, certificate, and verification information.
cluster-deployer-<version>.SPA.tgz	The SMI Deployer image signature package for use with bare metal deployments. This package contains the Deployer v image 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.