Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2023.03.1.31

First Published: July 21, 2023

Introduction

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

Release Package Version Information

Software Packages	Version
smi-install-disk.20.04.0-20230704.iso.SPA.tgz	20.04.0-20230704
cee.2023.03.1.31.SPA.tgz	2023.03.1.31
cluster-deployer-2023.03.1.31.SPA.tgz	2023.03.1.31

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

Verified Compatibility

Products	CIMC Firmware Version
Cisco UCS C220 M5	4.1(3f) or later
Cisco UCS C220 M6	4.2(2a) or later

Supported Kubernetes Version

In this release, the supported Kubernetes version is 1.25.

Updated Versions for Third Party Software

The following software versions are upgraded in this release.

Software Package	Component(s)	Previous Version	Current Version
containerd	Inception server Base image Cluster deployer	1.6.4	1.7.2

Software Package	Component(s)	Previous Version	Current Version
Prometheus	Metrics	2.37.2	2.44.0
Docker	--	23.0.1	24.0.2

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

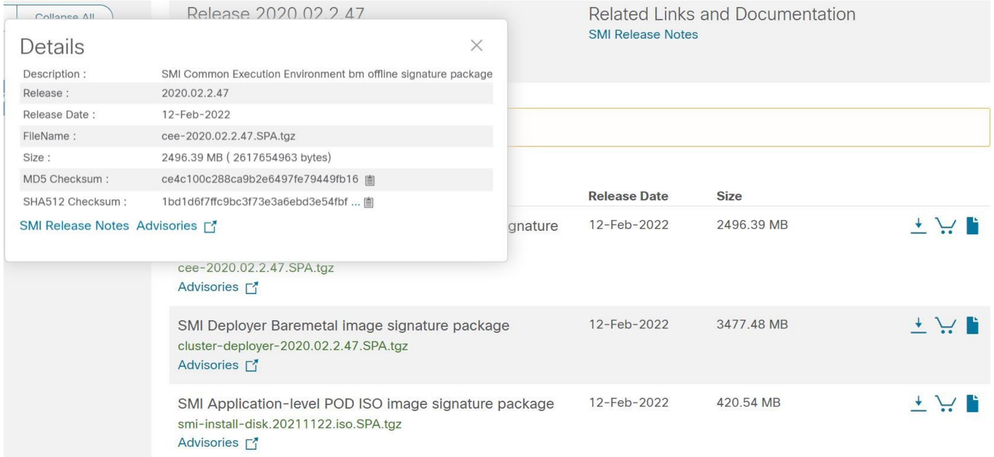
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Note: In this release, you must install a patch to use all the functionalities in SMI. For more information, contact your Cisco Account representative.

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 :	SMI Common Execution Environment bm offline signature package
Release :	2020.02.2.47
Release Date :	12-Feb-2022
FileName :	cee-2020.02.2.47.SPA.tgz
Size :	2496.39 MB (2617654963 bytes)
MD5 Checksum :	ce4c100c288ca9b2e6497fe79449fb16
SHA512 Checksum :	1bd1d6f7ffc9bc3f73e3a6ebd3e54fbf ...

	Release Date	Size
...gnature cee-2020.02.2.47.SPA.tgz Advisories	12-Feb-2022	2496.39 MB
SMI Deployer Baremetal image signature package cluster-deployer-2020.02.2.47.SPA.tgz Advisories	12-Feb-2022	3477.48 MB
SMI Application-level POD ISO image signature package smi-install-disk.20211122.iso.SPA.tgz Advisories	12-Feb-2022	420.54 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 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

There are no open bugs in this software release.

Resolved Bugs for This Release

The table below highlights the known bugs that are resolved in this specific software release.

NOTE: Additional information for all resolved bugs in this release are available in the Cisco Bug Search Tool.

Issue	Impact	Summary	Fix Details	Reproduction Steps
CSCwf14850	Exited containers are not cleaned up. Node can become not ready because of the PLEG unhealthy	PLEG not healthy log is seen. Too many exited containers	Prune exited containers during the cluster sync	Cluster sync

Features for This Release

The table below highlights the new features introduced in this specific software release.

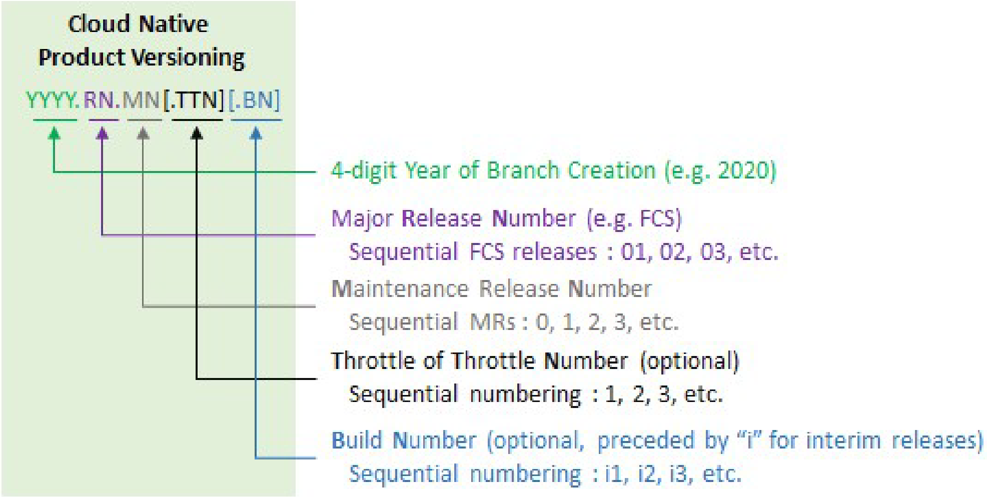
Issue	Impact	Summary	Change Details	Reproduction Steps
UCS certificate renew	Not a defect	Renew the CIMC certificate during the cluster sync Need to enable it explicitly	An option to enable CIMC certificate renew	NA
Upgrade Kubernetes to 1.25	Not a defect	Kubernetes is 1.25	Container runtime is containerd 1.7.2	NA
July 2022 to July 2023 Upgrade Support	Not a defect	Upgrade SMI July 2022 to July 2023 release with upgrade strategy concurrent	Docker to containerd migration	NA
Install cilium as k8s add-ons	Not a defect	Install the cilium plugin on top of Calico SMI CLI is added. Full support is planned in next release	Option to enable Cilium add-ons	NA
Tune kubelet sensitivity to failures to harden the system reliability	Not a defect	Tuning kubelet node monitor period and pod not-ready-toleration-seconds To harden Kubernetes control plane stability Too short period can falsely change the node status for temporary issues like DIMM or battery learning	Node-monitor-grace-period 20s to 40s Default pod toleration 30s to 300s Aggressive eviction leads to resource crunch in working node when it is trying recover the calls from faulty node. Critical pods can override this value.	N/A

Issue	**Impact**	**Summary**	**Change Details**	**Reproduction Steps**
K8s VIP change to avoid VIP switchovers between K8s masters	Not a defect	Keepalived is configured nopreempt to prevent flip flopping of VIPs.		

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 of Branch Creation (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 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.
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.

Software Packages	Description
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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANYKIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITHTHE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSEOR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright ©1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.