Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2020.02.1.32

First Published: January 29, 2021
Last Updated: January 29, 2021

Introduction

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

Release Package Version Information

Software Packages	Version
smi-install-disk.20210107.iso.SPA.tgz	20210107
cee-2020.02.1.32.SPA.tgz	2020.02.1.32
cluster-deployer-2020.02.1.32.SPA.tgz	2020.02.1.32
NOTE: In the event bugs need to be opened against this product, please reference the Package Component Version information in this table.	

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

Enhancements

K8s Version Upgrade to 1.19.5 (NIC Bond Failure)

After an NIC bond failure, the kubelet terminates connections to the Apiserver and is unable to establish these connections unless it is manually restarted. In this release, the K8s version 1.19.5 enables the kubelet to reconnect to the Apiserver after an NIC failure.

Pods in NodeAffinity State after Reboot (CEE)

After a K8s cluster is restarted using the CIMC interface, the pods remain in NodeAffinity state.

To override this issue, either delete the pods with NodeAffinity status or restart the kubelet and run the failed cluster-sync.

Postgres Improvements

Postgres supports SQL database with redundancy to store alerts and Grafana dashboards. In this release, the Common Execution Environment (CEE) is updated to include improvements in Postgres.

Note: You must run the following custom out-of-service upgrade procedure to apply updates to Postgres DB.

Impact

There is no service or customer impact during the upgrade procedure. However, the CEE downtime during the upgrade impacts monitoring tasks due to the unavailability of Grafana or KPIs. The estimated time required to finish the upgrade is 30 minutes.

Upgrade

To upgrade the CEE, use the following steps:

1. Before you start the upgrade, put the config in shutdown mode from CEE confd: **system mode shutdown**. Wait for the shutdown to complete.
2. Update the deployer config with new CEE release and run sync. Wait for ops-center helm chart and pods to upgrade to new release.
3. Connect to CEE and set the config in running mode: **system mode running**. Wait for all pods to become available. All three postgres pods must start.
4. Check the Postgres DB health status. Refer the *Postgres DB Health Status* section for more information.

Rollback

To perform a rollback for the CEE upgrade, use the following steps:

1. Before you start the CEE rollback, put the config in shutdown mode from CEE confd: **system mode shutdown**. Wait for the shutdown to complete.
2. Remove all three /data/<cee namespace>/data-postgres-* directories from the nodes where the postgres pods run. 2020 arch: master nodes; 2019 arch: oam nodes.
3. Update the deployer config with old CEE release and run sync. Wait for ops-center helm chart and pods to roll back to previous release.
4. Connect to CEE and set the config in running mode: **system mode running**. Wait for all pods to become available. All three postgres pods must start.
5. Check the Postgres DB health status. Refer to the *Postgres DB Health Status* section for more information.

Postgres DB Health Status

To check the health of Postgres DB, run the following two CLI commands as a one liner. A sample output is shown below.

```
cloud-user@cndp-spr12-k8-master-1:~$ echo "0--------------------------------
";kubectl exec -it postgres-0 -n $(kubectl get pods -A | grep postgres | awk '{print
$1}' | head -1) -- /usr/local/bin/cluster/healthcheck/is_major_master.sh;echo "1----
```

```
------------------------------";kubectl exec -it postgres-1 -n $(kubectl get pods -A
| grep postgres | awk '{print $1}' | head -1) --
/usr/local/bin/cluster/healthcheck/is_major_master.sh;echo "2----------------------
----------"; kubectl exec -it postgres-2 -n $(kubectl get pods -A | grep postgres |
awk '{print $1}' | head -1) --
/usr/local/bin/cluster/healthcheck/is_major_master.sh;

0--------------------------------

[bin][h][imm] >>> [2021-01-08 21:46:02] My name is pg-postgres-0

[bin][h][imm] >>> My state is good.

[bin][h][imm] >>> I think I'm master. Will ask my neighbors if they agree.

[bin][h][imm] >>> Will ask nodes from PARTNER_NODES list

[bin][h][imm] >>> Checking node pg-postgres-0

[bin][h][imm] >>> Checking node pg-postgres-1

[bin][h][imm] >>>>>>>>> Count of references to potential master pg-postgres-0 is 1
now

[bin][h][imm] >>> Checking node pg-postgres-2

[bin][h][imm] >>>>>>>>> Count of references to potential master pg-postgres-0 is 2
now

[bin][h][imm] >>> Potential masters got references:

[bin][h][imm] >>>>>> Node: pg-postgres-0, references: 2

[bin][h][imm] >>> I have 2 incoming reference[s]!

[bin][h][imm] >>>> 2/2 Does anyone have more?

[bin][h][imm] >>> Yahoo! I'm real master...so I think!

1--------------------------------

[bin][h][imm] >>> [2021-01-08 21:46:04] My name is pg-postgres-1

[bin][h][imm] >>> My state is good.

[bin][h][imm] >>> I'm not a master, nothing else to do!

2--------------------------------

[bin][h][imm] >>> [2021-01-08 21:46:05] My name is pg-postgres-2

[bin][h][imm] >>> My state is good.

[bin][h][imm] >>> I'm not a master, nothing else to do!
```

Troubleshooting and Monitoring

To check the logs and ensure the streaming is functioning with one node marked as primary, run the following CLI command. A sample output is shown below.

NOTE: This step is only useful for the new CEE version and is not required for performing a rollback.

```
cloud-user@cndp-spr12-k8-master-1:~$ echo "0--------------------------------
";kubectl logs postgres-0 -n $(kubectl get pods -A | grep postgres | awk '{print
$1}' | head -1) | tail -1 ; echo "1--------------------------------"; kubectl logs
postgres-1 -n $(kubectl get pods -A | grep postgres | awk '{print $1}' | head -1) |
tail -1; echo "2--------------------------------"; kubectl logs postgres-2 -n
$(kubectl get pods -A | grep postgres | awk '{print $1}' | head -1) | tail -1

0--------------------------------

[2021-01-08 21:34:55] [INFO] monitoring primary node "pg-postgres-0" (ID: 1000) in
normal state

1--------------------------------

[2021-01-08 21:36:39] [INFO] node "pg-postgres-1" (ID: 1001) monitoring upstream
node "pg-postgres-0" (ID: 1000) in normal state

2--------------------------------

[2021-01-08 21:38:33] [INFO] node "pg-postgres-2" (ID: 1002) monitoring upstream
node "pg-postgres-0" (ID: 1000) in normal state
```

Support for Multiple Labels in Bulkstats (CEE)

In the previous release, SMI supported the "namespace" label by default and only one additional label can be configured. In this release, you can configure bulkstats based on more than one label.

Configuration

To configure an additional label, use the following sample configuration.

```
bulk-stats query 4Gi_ContainerMemoryUsage

expression "sum (go_memstats_heap_inuse_bytes

{pod=~'smf-nodemgr.*'}

) by (pod)"

label pod

exit
```

Support Hyper-Threading for KVM or UPF

Hyper-Threading (HT) is the Intel term for simultaneous multithreading. In this process, a CPU splits each of its physical cores into virtual cores, which are known as threads. In this release, the UCS server supports HT technology to increase the CPU performance by doubling the number of CPU virtual cores. This technology impacts the Isolation CPU setting, VM CPU allocation and UPF CPU Worker Count setting.

NOTE: You must run the following custom out-of-service upgrade procedure to apply updates to Postgres DB.

Limitation

If the hyperthreading setting is changed from enabled to disabled, the KVM node must be re-deployed.

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/series.html

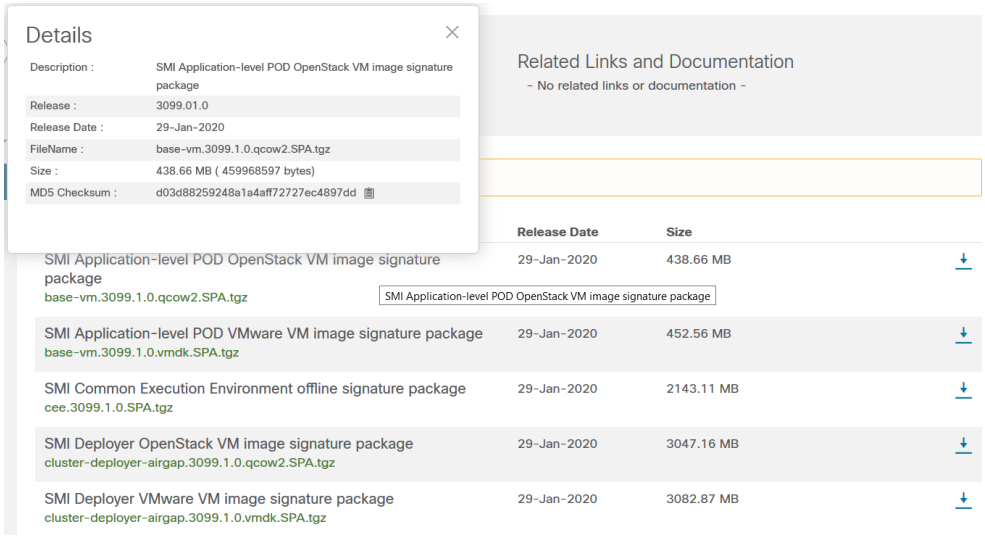
Installation and Upgrade Notes

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

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

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

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

Bug ID	Headline
CSCvx15282	KVM cluster sync / upgrade may fail at TASK [bm-ucs : Ensure UCS software is applied properly]

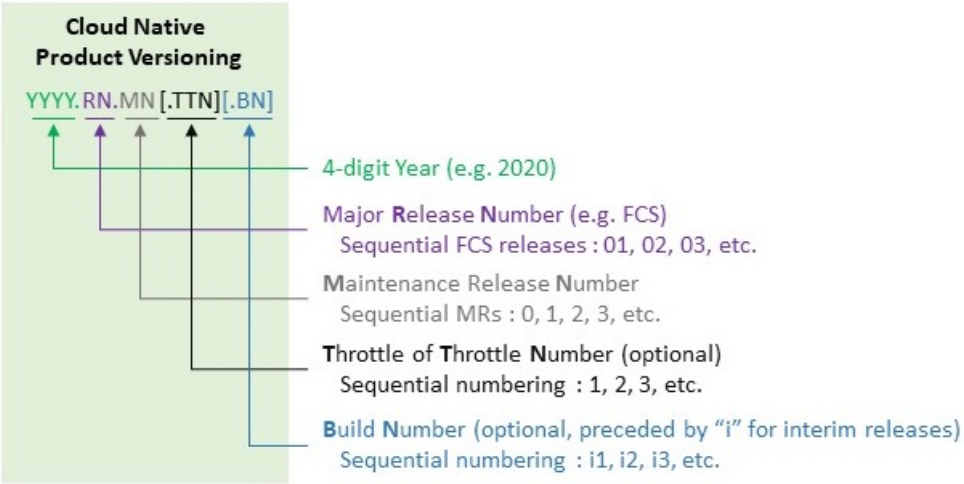
Resolved Bugs for this Release

None for this release.

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
base-vm.<version>.qcow2.SPA.tgz	The application-level POD OpenStack VM image signature package. This package contains the base qcow2 VM image as well as the release signature, certificate, and verification information.
base-vm.<version>.vmdk.SPA.tgz	The application-level POD VMware VM image signature package. This package contains the base vmdk VM 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.
cluster-deployer-airgap.<version>.qcow2.SPA.tgz	The SMI Deployer OpenStack VM image signature package. This package contains the Deployer qcow2 VM image as well as the release signature, certificate, and verification information.
cluster-deployer-airgap.<version>.vmdk.SPA.tgz	The SMI Deployer VMware VM image signature package. This package contains the Deployer vmdk VM 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.