BullSequana Edge

Release Note TS 018.03

86 A1 02FS 10 - February 2022

Trademarks and Acknowledgements

Hardware

February 2022

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Table of Contents

Preface

This document gives information about all changes from the previous version.

It also gives information about restrictions, known problems and the associated workarounds.

Finally, it lists the objects delivered in the Technical State and the features of the resources provided on the Resource and Documentation DVD.

Chapter 1. Overview

1.1. Operating systems

The following versions are supported for BullSequana Edge servers.

1.1.1. Red Hat

- RHEL 7.6
- RHEL 8

Note RHEL 8.3 does not support the NVIDIA A2 GPU. Update to RHEL 8.5 to use this model of GPU.

1.1.2. VMware ESXi

- ESXi 6.5u2 and higher
- ESXi 7.0u1

For certification details check:

https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=server&productid=48883

1.1.3. Windows

Windows Server 2019

- Discrete Device Assignment of the GPUs is supported. For more details, see:

  https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-for-deploying-devices-using-discrete-device-assignment

- No Windows driver available for the WiFi PCIe card

1.2. New features and changes

This Technical State 018.03 is a patched one compared to Technical State 018.02. It provides important fixes and contains a new release of the BMC firmware.

1.3. Resolved issues

This release fixes the following issues:

- **BIOS firmware update**

  In the **Firmware** page of the SHC, the pop-up window displaying the error message 'Unable to activate image' no longer appears at the end of a successful BIOS firmware update.

- **The NVIDIA A2 GPU card is not recognized as a GPU card**

  The NVIDIA A2 GPU card is now correctly detected as a GPU card and no longer as a standard PCI card.

- **The XAN information is lost after a reset**

  When connecting to the BMC after a reset, the XAN information now remains visible.

Chapter 2. Known restrictions and issues

2.1. Platform restrictions and issues

2.1.1. LDAP authentication

Restriction

Configuring LDAP authentication is not yet possible.

2.1.2. Date and time setting

Restriction

If the time and date have been set manually, they will be reset to their default values after a BMC reboot.

It is therefore recommend to use an NTP server to set the time and date.

See BullSequana Edge Server Hardware Console Reference Guide, 86 A1 05FS for more information

2.1.3. Switching from DHCP to static IP address

Issue

In the **BMC network settings** page of the SHC, when switching from DHCP mode to the Static IP Address, the IP address details entered in the fields are deleted when the **Save Settings** button is clicked. There is therefore a high risk of ending without any IP address at all.

Workaround

To avoid this issue, click the **Add IPV4 address** button before modifying any information in the fields and only then click the **Save Settings** button.

See Section 4.1.4. Assigning a static IP address of the BullSequana Edge Server Hardware Console Reference Guide, 86 A1 05FS, for the complete correct procedure.

2.1.4. Missing static IP address

Issue

When the server is connected to the network trough the P0 port (Eth0) with a DHCP IP address and not through the BMC port (Eth1), the default static IP is not visible for the BMC port (Eth1) in the SHC **BMC network settings** page.

Workaround

Connect the BMC port (Eth1) to the network to make the IP address visible in the web page.

2.1.5. Unsuccessful boot sequence

Issue

On systems running RHEL 8.4, when the secure boot feature is activated, an out-of-date signature in the BIOS may sometimes prevent the boot.

Workaround

If this happens, perform the following operations:

1. Intercept the boot sequence.
2. Go to the Boot Secure manager menu.
3. Delete the SecureFlash1 outdated signature.

2.1.6. Sensor values

Issue

The sensor values obtained by IPMI commands when the server in On are all null except for the fan sensors.

Workaround

Use the SHC to check sensors.

2.2. Software restrictions and issues

2.2.1. Installing VMware ESXi using a PXE server

Issue

During the installation of VMware ESXi with a PXE server, the sequence hangs just after loading the `vmkusb` VMware driver.

Workaround

Disable USB support in the BIOS before the OS installation and enable it again once the installation is done.

2.2.2. Hanged BIOS boot

Issue

On servers running RHEL, when restarting the server after an Orderly Shutdown/Reboot, the BIOS Configuration menu is inaccessible. The BIOS initialization is suspended at the PchOnEndOfPei stage but the Operating System (OS) is accessible.

Workaround

Flash the BIOS firmware again to go back to normal.

This issue happens because, on servers running RHEL, clicking the **Reboot** or **Shut down** button available in the **Server power operations** page of the SHC does not result in the complete shutdown of the system. For the system to successfully shutdown, the Operating System (OS) must be configured to accept the power off request.

1. In the RHEL Graphical User Interface, go to Applications > System tools > Settings > Power > Suspend & Power Button > When the Power Button is pressed.
2. Choose the Power Off option.

Chapter 3. Recommendations

3.1. Technical State (TS) numbering

The numbering of Technical States, TS xy.zz, is done as follows:

- An increase in x indicates that this TS provides new features. It is strongly recommended to install it in order to benefit from these features. It may also include fixes.
- An increase in y indicates a maintenance TS. It provides a set of fixes and it is recommended to install it. If a problem is reported on a previous TS, it is requested to move to the last such TS first before issuing a ticket.
- An increase in the minor number zz indicates a patched TS that fixes a specific issue. Installing it is not mandatory unless you may encounter this issue or it is declared as a hot fix that may affect most clients.

3.2. Updating the system globally to a Technical State (TS)

If MISM is used to update the system globally to a TS, it is strongly recommended to install the newest MISM version first.

3.3. Machine Intelligence System Management (MISM)

3.3.1. Zabbix version compatibility

MISM is not compatible Zabbix 5 and higher.

3.3.2. Installing/Updating MISM

To update MISM from a version preceding 2.0.2, perform the following steps:

1. Backup the playbooks created by the user.
2. Uninstall any previous versions.
3. Install the new version.

3.3.3. Updating firmware from the Technical State (TS) with MISM

The TechnicalState.iso file must be mounted using one of the following methods:

- from the /mnt root directory before starting containers
- from a /mnt sub-directory. The path to the file must be changed

If the TechnicalState.iso file is mounted after starting the containers, the containers must be restarted.

3.3.4. MISM Light

For MISM Light users, it is strongly recommended to:

- Update to MISM 2.1.3 with mism_full before further updates using mism_light
- Check the values of the variables in the `external_vars.yaml` file or AWX inventory after adding playbooks

3.4. Debugging the system

When experiencing any issue with the system, it is strongly recommended to collect the BMC logs. The logs usually contain the information that will help solve the issue.

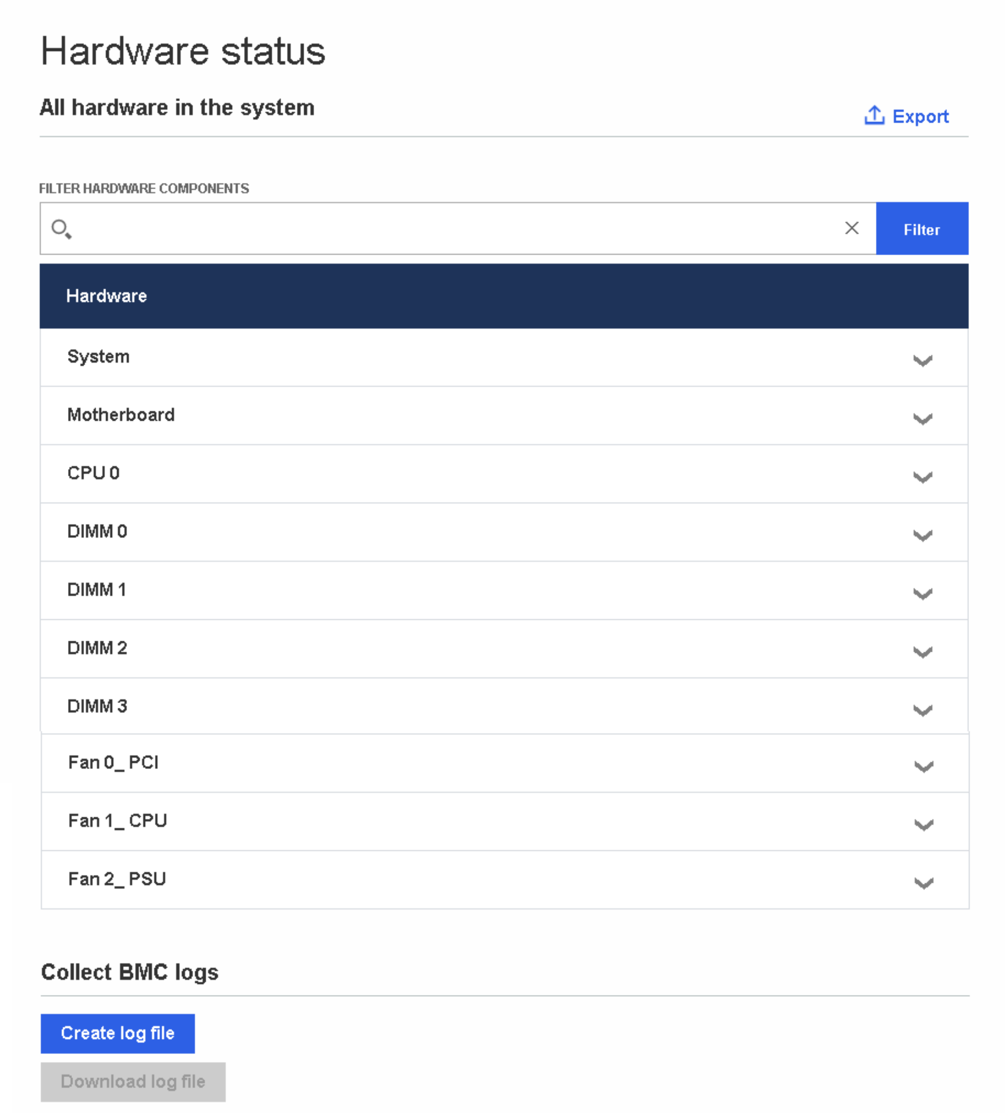
See Section 2.4. Collecting BMC logs of the BullSequana Edge Server Hardware Console Reference Guide, 86 A1 05FS, for the complete procedure.

Prerequisite

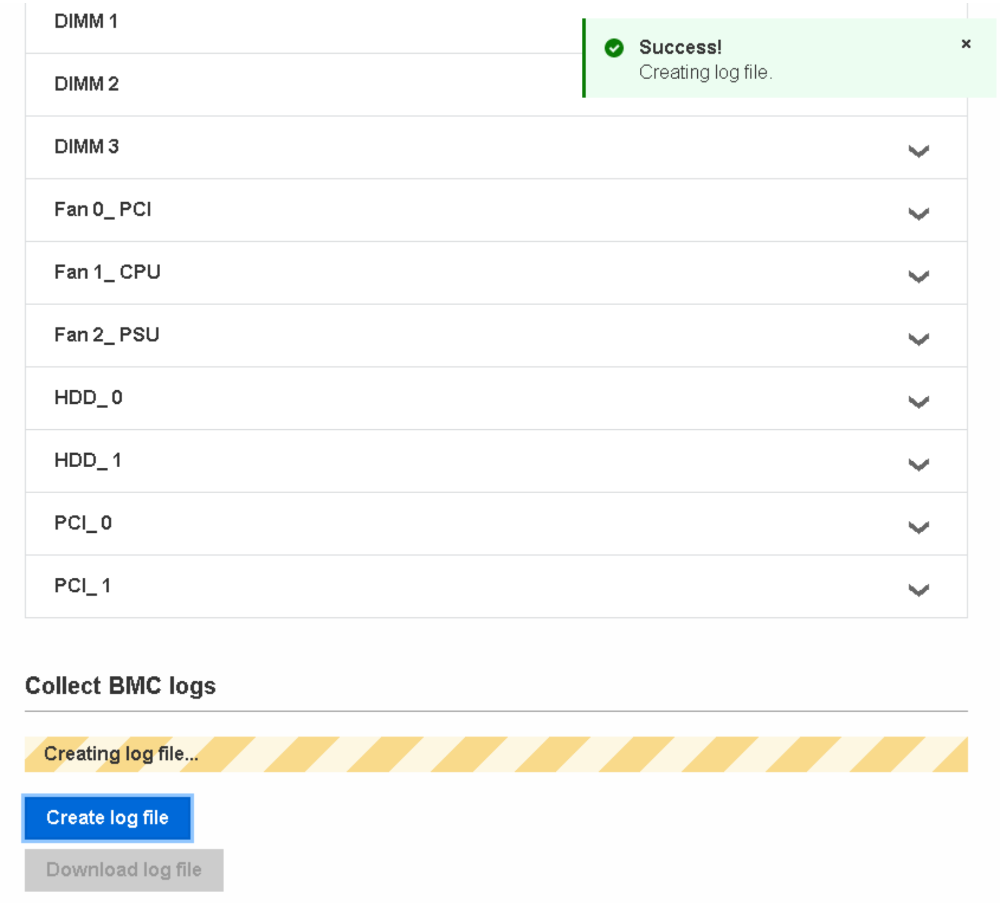
The BullSequana Edge server is in the powered on state

Procedure

1. Connect to the Server Hardware Console (SHC).
2. From the **Health** tab, click **Hardware status**. The **Hardware status** page opens.



3. Click **Create log file**.



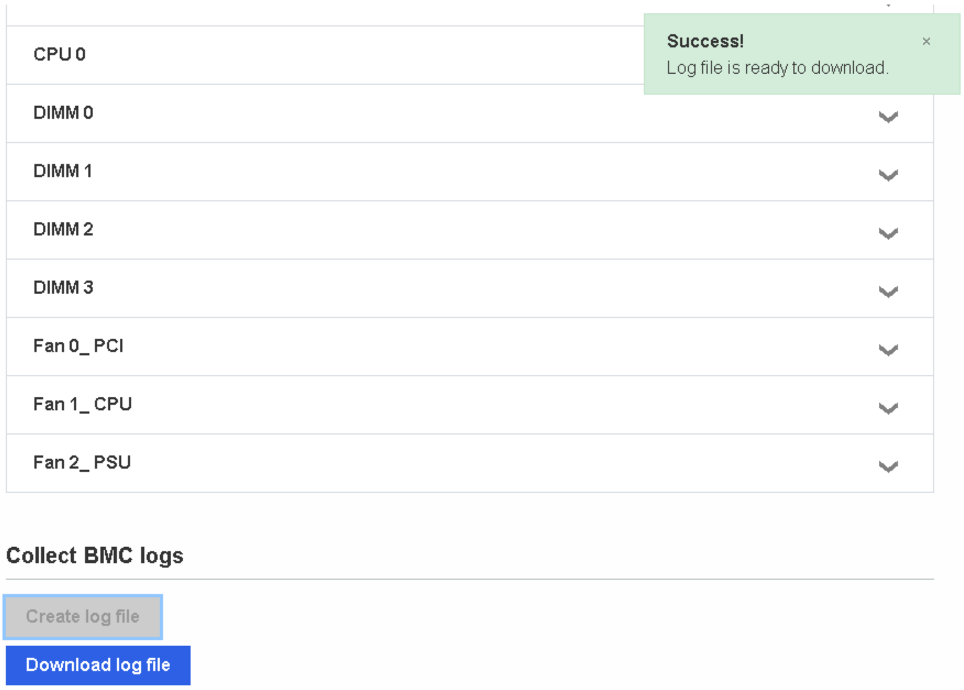
Success!
Creating log file.

Collect BMC logs

Creating log file...

Note This operation may take a long time to complete.

4. Wait for the BMC log file to be created.

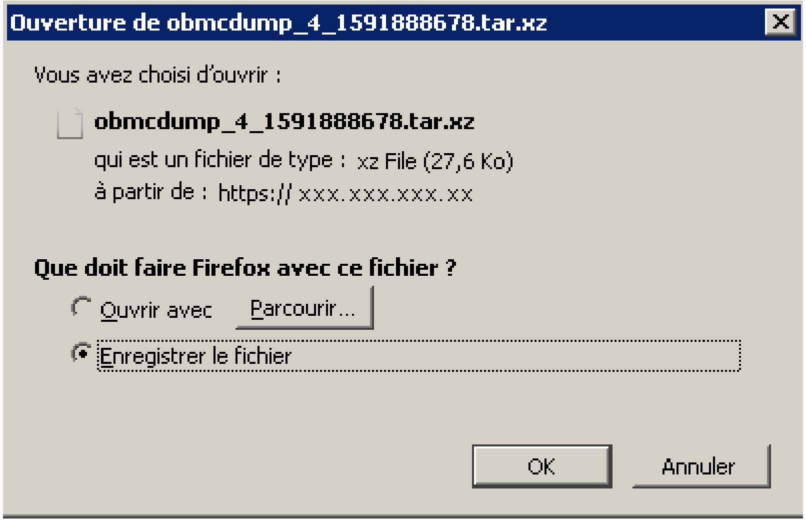


Success!
Log file is ready to download.

Collect BMC logs

5. When the **Success** message appears, click **Download log file**

6. Save the archive of the BMC logs, as required.



Ouverture de obmcdump_4_1591888678.tar.xz

Vous avez choisi d'ouvrir :

obmcdump_4_1591888678.tar.xz

qui est un fichier de type : xz File (27,6 Ko)

à partir de : https:// xxx.xxx.xxx.xx

Que doit faire Firefox avec ce fichier ?

○ Ouvrir avec Parcourir...

● Enregistrer le fichier

Chapter 4. Information

4.1. Baseboard Management Controller (BMC) user accounts

This section applies to systems that are being updated from a TS older than TS 017.02 to TS 017.02 or higher.

The default BMC user admin no longer exists from TS 017.02 onwards. However, effective deletion of this account will only happen after a reset to default factory settings.

4.1.1. First connection to the BMC after the TS update

When connecting to the BMC for the first time after the update of the system, changing the user account password is requested whichever account is being used for the connection.

In order to avoid changing the password of a custom user account, do on of the following action:

- If you know the root account password (different from the one indicated in this release note), connect to the BMC using this account and change its password, taking care to record the new account details for subsequent connections.
- If you do not know the root account password (different from the one indicated in this release note), connect to the BMC using the admin account and change its password, taking care to record the new account details for subsequent connections.

Note A password must be between eight and twenty characters long and contain at least 1 lowercase letter, 1 upper case letter, 1 number and 1 special character.

4.1.2. First connection to the BMC after a reset to default factory settings

When connecting to the BMC for the first time after a reset to default factory settings, proceed as follows:

1. Use the following default user parameters.

BMC default user	
Username	root
Password	At0s!Edge

2. Change the default user password once initial setup is completed, taking care to record the new account details for subsequent connections.

Notes

- A password must be between eight and twenty characters long and contain at least 1 lowercase letter, 1 upper case letter, 1 number and 1 special character.
- If a reset to default factory settings is performed, the root user password will be switched back to its default value and will have to be changed again.

4.2. SSH connection

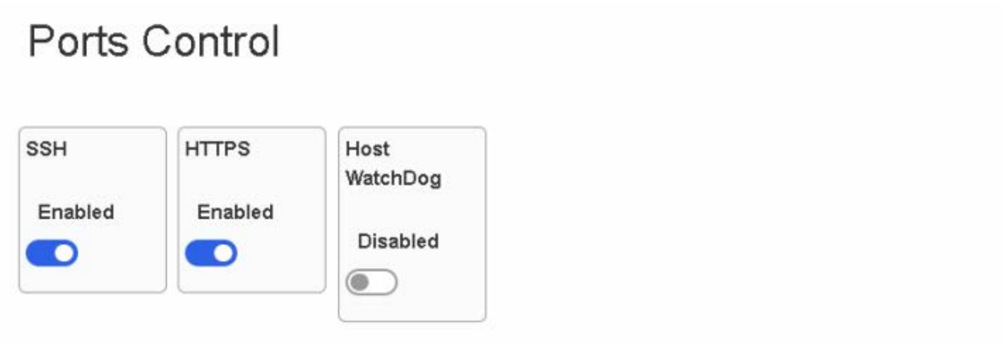
Note An issue in this release prevents the SSH from being deactivated by the BMC firmware update.

Updating the BMC firmware deactivates the SSH. To establish an SSH connection to the system after the firmware update, start by activating the SSH using the SHC.

See Section 3.11. Enabling port security controls of the BullSequana Edge Server Hardware Console Reference Guide, 86 A1 05FS, for the related procedure.

Procedure

1. Connect to the Server Hardware Console (SHC).
2. From the **Control** tab, click **Security Settings**. The **Ports Control** page opens.



Ports Control

SSH

Enabled

HTTPS

Enabled

Host WatchDog

Disabled

3. Click the SSH switch to enable the SSH.

Chapter 5. Delivery content

5.1. Delivered items

- Documentation and firmware are delivered on the Resource and Documentation DVD
- Machine Intelligence System Management (MISM) is delivered on the Bull support website: http://support.bull.com

Notes
- A new product row is highlighted in grey.
- A new version is highlighted in grey.

5.2. Documentation

Name	Description	Version
BullSequana Edge Customer Documentation Set	Complete documentation dedicated to the customer	08
BullSequana Edge Field Documentation Set	Complete documentation dedicated to the field	08

5.3. Platform firmware

Name	Description	Version
BIOS_SKD080	BIOS firmware	80.18.02 build 003
CPLD_MIPCS	Flash image for the CPLD component	4.3.0.0
Lora_Soft_Kit	Toolkit for using the LoRa Wireless Communication Module	1.0
OMF_MIPCS	Server Hardware Console (SHC) firmware	53.01 build 0001
VR_PCH_CPU0_MIPCS	Configuration file for processor voltage regulator on the motherboard	1.0.0
VR_PVCCIN_CPU0_MIPCS	Configuration file for processor voltage regulator on the motherboard	1.0.0
VR_PVCCIO_CPU0_MIPCS	Configuration file for processor voltage regulator on the motherboard	1.0.0
VR_PVDDQ_AB_CPU0_MIPCS	Configuration file for memory voltage regulator on the motherboard	1.0.0
VR_PVDDQ_DE_CPU0_MIPCS	Configuration file for memory voltage regulator on the motherboard	1.0.0

5.4. Administration Tools

Name	Description	Version
MISM	A web application used for hardware maintenance	2.1.9

Chapter 6. History of previous versions

6.1. TS 018.02 (November 2021)

New features and changes

OMF_MIPCS

- Merge with OpenBMC 2.9. Correction of the OpenBMC vulnerability on crafted IPMI messages is included.
- Update fan control algorithm

MISM

- Warning: start / stop scripts from dockerhub separated
- Update_from_atos_dockerhub.sh script shell to update versions

Resolved issues

Collecting BMC logs

It is no longer necessary to manually delete the oldest log files when the maximum number of log files that can be stored is reached.

When the maximum number of log files is reached, all log files are deleted.

6.2. TS 017.02 (June 2021)

New features and changes

OMF_MIPCS

- The default password of the root account has been changed. It is now At0s!Edge.
- After a reset to factory settings and first login, the user is asked to change the password for the root account
- The admin account has been removed
- SSH is now deactivated

Resolved issues

- **Intrusion status**

  It is now possible to clear the intrusion status in the **Chassis intrusion** page of the SHC.

- **Baseboard Management Controller (BMC) firmware update**

  During the update of the BMC firmware via the SHC or MISM, the message indicating the failure to upload the file is no longer displayed.

  This issue was fixed by TS 016.02 and will not be encountered during the update of the system to TS 017.02.

- **BIOS and CPLD firmware update**

  After the update of the BIOS or CPLD firmware, the firmware no longer stays in active mode when it should be in functional mode.

- **Failed BIOS firmware update**

  After the BIOS firmware update, the error message Unable to activate image is no longer displayed in the SHC **Firmware** page when the update is indicated as successful in the event log.

- **Baseboard Management Controller (BMC) SSL certificate**

  The unexpected certificate error, preventing the curl commands from running, no longer appears in the event log.

6.3. TS 016.02 (January 2021)

New features and changes

BIOS_SKD080

- Send TPM status to EMM
- Update Gbe X722 PXE driver to 4.3.05

CPLD_MIPCS

Factory reset detection logic

OMF_MIPCS

OpenBMC 2.8 merged code and associated features

LORA_SOFT_KIT

- First official release
- Support RedHat 7 distribution
- Support RedHat 8 distribution

MISM

- There are two separate deliverables for MISM:
  - MISM_full for full installation
  - MISM_light for light installation or update, which contains only AWX playbooks, AWX plugins, Zabbix templates, Zabbix external scripts and shell scripts
- MISM is delivered with a backup and a restore script for AWX and Zabbix databases
- The installation of Python tzlocal is optional: date will have no time localization indication (+02, -01…) if not installed

Resolved issues

- **Server Hardware Console (SHC) user accounts**

  It is now possible to create user accounts with different access rights.
- **Intrusion detection**

  False intrusion detections no longer appear in the **Intrusion Detection** page of the SHC and in the event logs.
- **Cold or Warm Reboot**

  The **Immediate Reboot** (formerly **Cold reboot**) or **Orderly Reboot** (formerly **Warm reboot**) buttons in the **Server power operations** page of the SHC function now correctly.

6.4. TS 015.02 (August 2020)

New features and changes

BIOS_SKD080

- Fix for Automatic failover booting feature
- Reference Code version RC 06.D51
- Fixes for Windows Server 2019 certification for Secure Boot and memory options (one DIMM set per channel, unused channels set disabled)

OMF_MIPCS

- Adding network routes feature
- Log collect feature

Resolved issues

- **Connection to the BMC in Zeroconf mode**

  Connection to the Baseboard Management Controller (BMC) in Zeroconf mode using the BMC port is now possible.

- **BIOS firmware version file**

  The BIOS version file is now correctly generated after a firmware update.

- **BMC reboot on a powered off host**

  Rebooting the BMC on a powered off host does not automatically restart the host anymore.

- **Automatic boot to PXE interfaces**

  The automatic boot runs correctly, without requiring human intervention anymore.

- **Visibility of the host serial number in the BIOS**

  The host serial number is now visible in the BIOS when it is accessed via a guest Operating System (OS).

6.5. TS 014.01 (May 2020)

New features and changes

BIOS_SKD080

- Generate signed BIOS image
- Reference Code version RC 06.D34
- Updated Intel Xeon Skylake-D processor microcode to version 02000065
- Updated the Management Engine (ME) SPS firmware to version SPS_ SoC-X_04.00.04.112
- Detect chassis intrusion in standby, during boot and in runtime and take actions based on BMC settings

MISM

- New Zabbix template for BullSequana Edge Host
- New Zabbix template for BullSequana Edge Map
- BullSequana Edge Zabbix Icons
- Added two missing sensors as items and their associated graph in Zabbix
  - Power psu-iout (Amperes)
  - Total power (Watts)
- Prerequisites helping script with NO warranty

OMF_MIPCS

- IPMI Out Of Band support
- Signed firmware support for BIOS, BMC and CPLD firmware

Resolved issues

- **Sensor display in Idle or Off state**

  Sensor display values are now correctly implemented for systems in Idle or Off state.
- **Date and hour settings in the Server Hardware Console (SHC)**

  Manually setting the date and hour is now possible from the SHC.
- **Powering the server off**

  Powering off the server using the Power button is now possible.
- **Encrypted passwords**

  Password encryption in the controlling console (Ansible Tower) is now fully implemented and no longer hinders job launches.

6.6. TS 006.02 (December 2019)

New features and changes

BIOS_SKD080

- Print BMC and CPLD Version in BIOS log
- Chassis intrusion detection (Note: if chassis is open, the system will not boot)

OMF_MIPCS

New user ‘admin’ has been created

After the update of the BMC firmware to the version provided in this TS, it is necessary to run the following commands in ssh so that the new user information is taken into account:

1. Export the BMC credentials using the following command:

```
export bmc=<user>:<pwd>@<BMC IP>
```

2. Perform the reset to default factory settings of the BMC using the following command:

```
curl -b cjar -k -H 'Content-Type: application/json' -X POST -d '{"data":[]}'
https://${bmc}/xyz/openbmc_project/software/action/Reset
```

MISM

- Full installation through install.sh and start/stop.sh scripts
- Zabbix monitoring

Resolved issues

- **KVM interface in the Server Hardware Console (SHC)**

  Using the Refresh button no longer makes the Keyboard Video Mouse page unavailable.

- **Wireless connection configuration**

  Configuring LTE or WiFi for BMC is now possible through the SHC.

- **BMC WiFi connection**

  The user is now warned that the entered password is incorrect and the connection unsuccessful.

- **BMC WiFi connection after a BMC reboot**

  Connection to the BMC WiFi is now automatically restored after rebooting the BMC.

6.7. TS 005.01 (September 2019)

New features and changes

BIOS_SKD080

- New Bakerville Code Drop 14
- Support for sending memory module and PCIe errors to the Server Hardware Console (SHC)
- Update to SMBIOS Type 0/1 Information
- Send processor microcode version information to the SHC
- Send processor SKU number, PCH information, processor signature and number of enabled cores to the SHC

OMF_MIPCS

Identification of failing components including physical position

MISM

- MIPM renames as MISM
- start/stop/uninstall/remove_user_data scripts
- add_playbooks separate script to allow light delivery after first install

Resolved issues

Server Hardware Console (SHC) user accounts

Creating a new user account in the SHC web interface is now possible.

6.8. TS 004.01 (June 2019)

First delivery

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE