EVIDEN

BullSequana S

Release Note TS 074.02

86 A1 28FR 37 - October 2024

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark and/or patent misuse.

Hardware

October 2024

Eviden
30 bis rue du Nid de Pie
49000 Angers
FRANCE

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.

See The Bull support web site for the most uptodate product information, documentation, firmware updates, software fixes and service offers: https://support.bull.com

Chapter 1. Overview

Important **To fully address security alerts, it is recommended to check for available Operating System (OS) updates.**

1.1. Operating Systems (OS)Versions

1.1.1. VMware ESXi

Note The End of General Support for ESXi 6.5 and 6.7 was October 15, 2022. To maintain your full level of Support and Subscription Services, VMware recommends upgrading to ESXi 7.

For certification details check:

- Intel® Xeon® 1st generation processors https://www.vmware.com/resources/compatibility/search.php?deviceCategory= server&details=1&keyword=sequana&cpuSeries=122
- Intel® Xeon® 2nd generation processors https://www.vmware.com/resources/compatibility/search.php?deviceCategory= server&details=1&keyword=sequana&cpuSeries=129

BullSequana S200, S400, S800

- ESXi 6.5u3 build 14990892 or higher
- ESXi 6.7u3 build 15018017 or higher
- ESXi 7.0 or higher
- ESXi 8.0 or higher

BullSequana S1600

VMware ESXi is supported exclusively on a four-module partition of a BullSequana S1600 server. It is not supported in any other configuration.

- ESXi 6.7u3 build 15018017 or higher
- ESXi 7.0 or higher

1.1.2. Oracle

1.1.2.1. Oracle VM

Note Extended Support for Oracle VM 3.4 ends in June 2024.

Intel® Xeon® 1st generation processors	Intel® Xeon® 2nd generation processors
Oracle VM 3.4	Oracle VM 3.4

1.1.2.2. Oracle Linux

Intel® Xeon® 1st generation processors	Intel® Xeon® 2nd generation processors
Oracle Linux 7.4	• Oracle Linux 7.6 and 7.8 (UEK6) • Oracle Linux 8.1 to 8.5 (UEK6) • Oracle Linux 8.6 (UEK7) • Oracle Linux 9 (UEK7)

1.1.3. Linux

1.1.3.1. Red Hat Linux Enterprise (RHEL)

BullSequana S200, S400, S800

Intel® Xeon® 1st generation processors	Intel® Xeon® 2nd generation processors	Intel® Xeon® 2nd generation processors & Intel® DCPMM
RHEL 8: 8.1 or higher	RHEL 9: 9.0 or higher	RHEL 8: 8.4 or higher

BullSequana S1600

Intel® Xeon® 2nd generation processors	Intel® Xeon® 2nd generation processors & Intel® DCPMM
• RHEL 9: 9.0 or higher • RHEL 8: 8.1 or higher • RHEL 7: 7.6 or higher	Not supported

1.1.3.2. SUSE Linux Enterprise Server (SLES)

BullSequana S200, S400, S800

Intel® Xeon® 1st generation processors	Intel® Xeon® 2nd generation processors	Intel® Xeon® 2nd generation processors & Intel® DCPMM
SLES 12 SP5	• SLES 12 SP5 • SLES 15 SP5	Not supported

BullSequana S1600

Intel® Xeon® 2nd generation processors	Intel® Xeon® 2nd generation processors & Intel® DCPMM
• SLES 12 SP5 • SLES 15 SP5	Not supported

1.1.4. Microsoft Windows

BullSequana S200, S400, S800

Intel® Xeon® 1st generation processors	Intel® Xeon® 2nd generation processors
• Windows Server 2019 • Windows Server 2016 (with iaStorA.free.win8.64bit.4.3.0.1198 driver)	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 (with iaStorA.free.win8.64bit.4.3.0.1198 driver): all models except BullSequana S800

BullSequana S1600

Windows Server is not supported on BullSequana S1600 servers.

1.2. New Features and Changes

This Technical State (TS) 074.02 is patched one compared to TS 074.01. It brings new releases of the BMC firmware.

1.3. Resolved Issues

This release fixes the following issues.

- **Static sensor 209 event not decoded**

  The sensor name field for this sensor has been corrected and the associated event reporting an uncorrectable memory error is now correctly decoded.

- **BMC Reset to Default**

  Resetting the BMC firmware to default settings no longer causes connection problems: logging in using the default user account via the SHC or SSH after the reset is successful.

Chapter 2. Known Restrictions and Issues

2.1. Platform Restrictions and Issues

2.1.1. Server Hardware Console (SHC) Restrictions

This section applies to BullSequana S1600 servers only.

Updating Local Management Board (LMB) firmware (Clock, FPGA, LMC) is not possible from the SHC yet.
Use the Hardware Management CLIs to update the firmware.

2.1.2. Firmware Update

Issue

During the update (individual or global) of a component firmware using the Hardware Management CLIs, the update of the firmware may appear as failed.

Workaround

Check the firmware version and if it is incorrect, launch the update again.

2.1.3. Serial On LAN (SOL) Activation

Issue

When using the ipmi command "SOL activate" for Serial On LAN, there are issues with the keyboard.

Workaround

Open a SSH session on the SHC and use the terminal command.

2.1.4. IPMI In-Band Filtering

Issue

After activating IPMI in-band filtering (bmc.ipmi_filter_bios_kcs set to 1) and resetting the BMC, the OS is lost and the SSH connection freeezes.

Restriction

It is recommended to activate IPMI in-band filtering while the system is off.

2.1.5. LDAP Authentication

Issue

When the DNS server configured from the Network Settings page of the SHC belongs to the Active Directory domain, the LDAP authentication of the embedded controller fails without any error notification.

Workaround

Do not configure the DNS server before performing the LDAP authentication.

2.1.6. Mounting Virtual Media Files from the Remote Console

Issue

Installing software from a very large file via the Remote Console may fail with several medium errors reported.

Workaround

Use smaller files.

2.1.7. Locating an FDB Disk

Issue

The command designed to locate a failed FDB disk fails to switch on the disk's LED, making it impossible to locate it.

Workaround

See Description Guide to locate FDB disks

2.1.8. Fan Status Test

Issue

The fan status test available on the Test Key shows the fan speed values as unavailable.

Workaround

Reset the BMC and launch the fan status test again to display the correct fan speed values.

2.1.9. Memory module exclusion

This section applies to BullSequana S1600 servers only.

Issue

After having excluded memory modules from a secondary module, booting is not possible anymore.

Workaround

When excluding memory modules is necessary, memory exclusion must be symmetrical between both memory controllers (iMC) of the processor (CPU). Otherwise booting will not be possible.

For example, if the memory modules in the L0 and L1 slots of CPU 1 need to be excluded, the memory modules in the H0 and H1 slots of CPU 1 must also be excluded.

See Description Guide for more information on memory module slots

2.1.10. CVE-2019-11135 Vulnerability

Issue

Some Linux kernels report a `TAA CPU Present` bug.

Workaround

This means that the processor does not have the latest microcode mitigation for the CVE-2019-11135 vulnerability.

If there are no OS patch or Intel microcode patch available, it is recommended to the following lines in the grub settings:

- `tsx=off`
- `tsx_async_abort=full`

2.1.11. GPU Critical Events at Power On

Issue

On systems equipped with NVIDIA T4 GPUs, messages reporting critical events on GPU fans may appear during Power On.

Workaround

These events can be ignored as long as they happen only during Power On and are rapidly deasserted.

2.1.12. MSMI Assertion after Shutdown or Power Off

This section applies to BullSequana S1600 servers only.

Issue

MSMI events are systematically asserted for all CPUs when powering off the system via the SHC or shutting down the OS. The events are deasserted at the following power on.

Workaround

These events can be ignored: no dump is launched and it does not affect the system operation.

2.1.13. PXE boot fails

Issue

If a PCIe card is added in slot 0 of the motherboard and is connected with a cable, the PXE boot does not work (NBP transfer failed).

Workaround

Use one of the following workarounds:

- Remove the cable from the PCIe card so that the PCIe card has no active connection.
- Disable and enable again PXE on the PCIe card (Set 'Boot Mode' to 'Disabled' then set 'Boot Mode' to 'PXE'). This action moves the ports of the PCIe card to the end of the boot-list in the BIOS Boot Manager screen.

The chosen workaround must be applied to the other PCIe cards present on the server.

2.1.14. PCIe Hot-plug

This section applies to BullSequana S1600 servers only.

Restriction

Hot-plugging PCIe blades is not fully supported on all Operating Systems (OS).

2.1.15. Hot Plug of the Broadcom P210tp PCI card

Restriction

Hot-plugging the Broadcom PCI card BCM 957416A4160C is not possible. Insert or remove the card only when the operating system is stopped.

2.1.16. Module Power Supply Unit (PSU) Redundancy in 100-140 V AC Range

Restriction

When the PSU of the modules are plugged to mains with voltage between 100 and 140 V, redundancy is only ensured for modules consuming less than 1000 W.

2.2. Redfish Restrictions and Issues

LDAP authentication is only supported with Active Directory.

2.3. Software Restrictions and Issues

2.3.1. Installing and Booting from DCPMM Memory Modules

Restriction

Installing and booting from DCPMM memory modules is only supported from RHEL 7.6 onwards.

2.3.2. Incorrect Allocation of DCPMM Name Spaces to numa Node

Issue

On a server running a RedHat prior to 7.6 with DCPMM memory modules configured in Application Direct mode, the `numactl` command returns an incorrect answer.

Workaround

Update to RHEL 7.6.

2.3.3. Using SR-IOV

Issue

On a BullSequana S400 or S800 server, attempting to assign the SR-IOV passtrough to a virtual machine fails, resulting in the following error message: *unsupported configuration: host does not support passthrough of host PCI devices*

Restriction

SR-IOV is not supported on Virtual Machines running SLES 12 SP2.

SR-IOV is not supported on BullSequana S1600 servers.

2.3.4. Powering Off from the Server Hardware Console (SHC)

Issue

On servers running RHEL, clicking the Power Off button available in the Power Management page of the SHC does not result in the complete shutdown of the system.

Workaround

To get a complete shutdown, use one of the following methods:

- From the SHC:
  a. Perform a BMC reset. This makes the SHC Force Power Off available again.
  b. Perform a Force Power Off.
- Perform a Force Power Off using the `bsmpower` CLI command

For the system to successfully shutdown when using the SHC Power button Off, the Remote Console (RC) must be running and the Operating System (OS) must be configured to accept the power off request.

- With RHEL 7.3 and 7.5:
  a. In the RHEL Graphical User Interface, go to Applications > Utilities > Tweak Tool > Power > Power button action.
  b. Choose the Shutdown option.
- With RHEL 7.4:
  a. Install the acpid package.
  b. Replace /etc/acpi/actions/power.sh content with the following content:
  ```
  #!/bin/sh
  PATH=/usr/sbin:/usr/bin
  shutdown -h now
  ```
- With RHEL 7.6, 7.7:
  a. In the RHEL Graphical User Interface, go to Applications > System tools > Settings > Power > Suspend & Power Button > When the Power Button is pressed.
  b. Choose the Power Off option.

Chapter 3. Recommendations

3.1. Technical State (TS) numbering

The numbering of Technical States, TS xy.zz, changes 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 to Technical State (TS) 074.02

TS 074.01 can be installed on a system running TS 074.01 or any TS 064.0x without restriction.

If the system is running any TS 064.0x, it is recommended to skip TS 074.01 and update directly to TS 074.02.

As with any other firmware update, it is recommended to first update the Hardware Management CLI commands to the latest version: 1.5.32.

If downgrading from TS 074.01 is necessary, the Hardware Management CLI commands must first be downgraded to version 1.5.31. Contact the support team for more information.

3.3. Updating to Technical State (TS) 064.0x

TS 064.0x can be installed on a system running TS 054.01 without restriction.

Downgrading from TS 064.0x to TS 054.01 is also possible without restriction.

3.4. Updating to Technical State (TS) 054.01

TS 054.01 can be installed on a system running TS 034.04 or 044.03 without restriction.

3.5. Downgrading from Technical State (TS) 054.01

If downgrading from TS 054.01 is necessary, contact the support team.

3.6. Updating to Technical State (TS) 044.03

3.6.1. Prerequisite

Update the system to at least TS 024.01 before updating to TS 044.03.

See 3.10. Updating to Technical State (TS) 024.01 for the complete procedure

3.6.2. From Technical State (TS) 024.0x

TS 044.03 can be installed on a system running TS 024.01 or 024.02 without restriction.

3.6.3. From Technical State (TS) 034.0x

TS 044.03 can be installed on a system running TS 034.01, 034.02, 034.03 or 034.04 without restriction.

During the global update using the Hardware Management CLIs, the following error may be reported after the BMC and BIOS updated successfully:

```
- module X - Error in setting config key: Destination unavailable
```

If this happens, reset the BMC and launch the global update again.

3.7. Downgrading from Technical State (TS) 044.03

If downgrading from TS 044.03 is necessary, contact the support team.

3.8. Updating to Technical State (TS) 034.04

It is strongly recommended to update the system to TS 034.03 before updating to TS 034.04.

3.9. Updating to Technical State (TS) 034.03

As TS 034.03 is a patched one compared to TS 034.02, it can be installed on a system running TS 034.02 without restriction.

But it can also be installed directly on a system running TS 024.01, without having to update to TS 024.02, 034.01 or 034.02 beforehand.

3.10. Updating to Technical State (TS) 024.01

Important	**Important Due to the introduction of signed firmware, it is mandatory to perform the operations described below in order to correctly update to TS 024.01.**

Before updating the server firmware to TS 024.01, it is mandatory to:

1. Update to TS 022.02, 022.03 or 022.04.
2. Update the EMM33_BMC_Bckp firmware.
   For each module, run the following command:

```
ipmi-oem -h <IP> -u <super> -p <pwd> Bull upgrade /tmp/TS24/EMM33_BMC_335100_0592.sign MC_RESTORE 0
```

In addition to updating the server firmware to TS 024.01, it is mandatory to update the EMM_REG_DUMP firmware:

1. Unzip the EMM_REGS_DUMP_1.1.zip file.

2. For each module, run the following commands:

```
bsmRegDump.sh -H <IP> -a config -f /tmp/TS24/EMM_REGS_DUMP_1.1/EMM_REGS_CPU_SKL_CSR
bsmRegDump.sh -H <IP> -a config -f /tmp/TS24/EMM_REGS_DUMP_1.1/EMM_REGS_CPU_SKL_MSR
bsmRegDump.sh -H <IP> -a config -f /tmp/TS24/EMM_REGS_DUMP_1.1/EMM_REGS_FPGA
```

In case of issues with resource discovery after the update to TS 024.01, perform an AC power cycle before updating to any later TS.

3.11. Downgrading from Technical State (TS) 024.01

If downgrading from TS 024.01 is necessary, contact the support team.

3.12. Downgrading from Technical State (TS) 022.02

BullSequana S200, S400, S800 servers

Downgrade all the firmware to their previous version using Firmware Global Upgrade.

```
bsmFwGlobalUpg.sh -H <IP> -u <user> -p <pwd> -a upg -D <customer DVD mount point> -b
```

BullSequana S1600 servers

If downgrading from TS 022.02 is necessary, contact the support team.

3.13. Updating to Technical State (TS) 021.02 or 021.03

This section applies to BullSequana S200, S400, S800 servers only.

Important **TS 021.02 introduces a shared BIOS for Intel® Xeon® 1st and 2nd generation processors.**

Firmware Global Upgrade is unaffected. Proceed as usual to update the server to TS 021.02.

3.14. Downgrading from Technical State (TS) 021.02 or 021.03

This section applies to BullSequana S200, S400, S800 servers only.

Important **TS 021.02 introduces a shared BIOS for Intel® Xeon® 1st and 2nd generation processors.**

If downgrading to the previous TS is necessary, perform the following operations:

1. Individually downgrade the BIOS_PUR043 firmware to the BIOS_SKL040 or BIOS_CCL041 firmware according to the processor generation.

2. Downgrade all the other firmware to their previous version using Firmware Global Upgrade.

3.15. Updating from older Technical States (TSs)

This section applies to BullSequana S200, S400, S800 servers only.

Important **Due to a change in the EMM33_BMC firmware's size between TS 005.04 and TS 006.02, its mandatory to update to TS 006.02 before updating to any later TS.**

If the server is running a TS preceding 006.02, perform the following steps:

1. Update FULLY to TS 006.02.
2. Perform an AC cycle an ALL modules. For each module, perform the following steps:
   a. Power off the module.
   b. Unplug the power cords.
   c. Wait until the power LEDs are off.
   d. Plug in the power cords.
   e. Power on the module.
3. Clear the Internet browser's cache before using the Server Hardware Console (SHC) for the first time.
4. Update to any later TS.

3.16. Global Update of a BullSequana S1600 Server

Update firmware using the Hardware Management CLI commands:

See Upgrade Guide and Remote Hardware Management CLI Reference Guide for more information

Note Depending on the system, there can be two or four UNB modules present in the UBox: 0 and 1 or 0, 1, 2 and 3.

1. Update the firmware of the modules globally using the `bsmFwGlobalUpg` command.

```
bsmFwGlobalUpg.sh -a upg -H <IP address> -u <user> -p <pwd> -D <path to file>
```

2. Update the UBox firmware using one of the following methods:

   - Update the UBox firmware globally using the `bsmFwGlobalUpg` command.

```
bsmFwGlobalUpg.sh -a upg -H <IP address> -u <user> -p <pwd> -D <path to file> -M 16
```

   - Update each UBox firmware individually using the `bsmFWupg` command.

     i. LMC firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E MC -d <path to file> -F EMM34_LMC_
342400_0848.bin -M 16
```

     ii. MAIN_FPGA1 firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E MAIN_FPGA1 -d <path to file> -F FPGA_
LMB_Multi_Image_wub_1_1_0_0.emm -M 16
```

     iii. MAIN_FPGA2 firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E MAIN_FPGA2 -d <path to file> -F FPGA_
LMB_Mngt_Image_wub_0_4_0_0.emm -M 16
```

     iv. CPLD firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E CPLD -d <path to file> -F CPLD_LMB_
Image_wub_0_5_0_0 -M 16
```

     v. UNB0_FPGA firmware:

```
bsmFWupg.sh -a upg -<IP address> -u <user> -p <pwd> -E UNB0_FPGA -d <path to file> -F FPGA_
UNB_Image_wub_0_8_0_0.emm -M 16
```

     vi. UNB1_FPGA firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB1_FPGA -d <path to file> -F FPGA_
UNB_Image_wub_0_8_0_0.emm -M 16
```

vii. UNB2_FPGA firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB2_FPGA -d <path to file> -F FPGA_
UNB_Image_wub_0_8_0_0.emm -M 16
```

viii. UNB3_FPGA firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB3_FPGA -d <path to file> -F FPGA_
UNB_Image_wub_0_8_0_0.emm -M 16
```

ix. BCM1_UPG firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E BCM1_UPG -d <path to file> -F ETH_
SWITCH_LMB_Image_002.bin BCM1_UPG -M 16
```

x. BCM2_UPG firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E BCM2_UPG -d <path to file> -F ETH_
SWITCH_LMB_Image_002.bin BCM2_UPG -M 16
```

xi. UNB0_CLK firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB0_CLK -d <path to file> -F CLK_UNB_
Image_003.bin -M 16
```

xii. UNB1_CLK firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB1_CLK -d <path to file> -F CLK_UNB_
Image_003.bin -M 16
```

xiii. UNB2_CLK firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB02CLK -d <path to file> -F CLK_UNB_
Image_003.bin -M 16
```

xiv. UNB3_CLK firmware:

```
bsmFWupg.sh -a upg -H <IP address> -u <user> -p <pwd> -E UNB3_CLK -d <path to file> -F CLK_UNB_
Image_003.bin -M 16
```

3.17. CVE-2013-4786 IPMI v2.0 vulnerability

To address this vulnerability, it is strongly recommended to change the super default account username.

3.18. Updating Firmware

It is recommended to update the Hardware Management CLI commands to the latest version before performing any firmware update.

3.19. Baseboard Management Controller (BMC) Firmware Update

- It is strongly recommended to power off the system before updating the BMC firmware. Otherwise, some secondary modules may be lost.
- If the PCIe slot 0 is not visible after updating the BMC firmware, do an AC/Off - AC/On to see the slot.

Note To avoid any issues with firmware update, it is strongly recommended to use the global firmware update feature available through the Hardware Management CLI commands.

3.20. FPGA_CPB Update

Update It is mandatory to update the BMC firmware before updating the FPGA_CPB firmware.

3.21. UBox FPGA Update

This section applies to BullSequana S1600 servers only.

As indicated in the documentation, it is mandatory to reset the LMC after the update of the firmware of any UBox FPGA component.

3.22. Network Adapters and Switches Firmware

When selecting firmware and device driver update, be sure to select the one that is appropriate for your operating system and in line with the specifications of the external network infrastructure.

3.23. Broadcom LSI 94XX board firmware

The firmware of these boards must be updated as follows:

Original firmware version	Update to version
14.00.00.00	14.00.02.00
13.00.00.00	13.01.00.00

3.24. Emulex LPe31000 and LPe32000 board firmware

The Direct Attach feature is only supported with the board firmware version 12.6.240.40 or higher.

3.25. Copying the default BIOS settings file

When updating to a new TS, the new default BIOS settings must be applied:

1. Save the customer's BIOS settings.
2. Apply the new default BIOS settings.
   a. Rename the new default BIOS settings file.
   b. Copy the renamed file on the server's SD card.
   c. Apply the new default BIOS settings.
3. If required, restore the customer's BIOS settings.

See Upgrade Guide for the complete procedure

3.26. Linux Kernel Boot Parameters

3.26.1. BullSequana S800 Servers

On BullSequana S800 servers with Intel® Optane® DCPMM 256 GB or 512 GB and running RHEL 7, it is necessary to apply the following parameter in the `/etc/default/grub` file:

`disable_mtrr_trim`
By default the kernel will trim any uncacheable memory out of the available memory pool based on MTRR settings. This parameter disables that behavior.

There is no need to apply this parameter on servers with Intel® Optane® DCPMM 128 GB.

3.26.2. BullSequana S1600 Servers

To allow server boot, it is necessary to add or modify the following parameters:

- In the `/etc/default/grub` file:
  - `nmi_watchdog=0`
    This parameter disables NMI watchdog.
  - `disable_mtrr_trim`
    By default the kernel will trim any uncacheable memory out of the available memory pool based on MTRR settings. This parameter disables that behavior.
  - `tsc=reliable`
    This parameter prevents from switching to acpi clock.
  - `intel_idle.max_cstate=1`
    `processor.max_cstate=1`
    `intel_pstate=disable`
    Remove these three lines for systems running 5.x Linux kernels.

Keep these three lines for systems running 4.x or lower Linux kernels. These parameters improves the stability of the system when it is under stress.

- In the `/etc/systemd/system.conf` file:

  ```
  DefaultTimeoutStartSec=900s
  DefaultTimeoutStopSec=900s
  ```

  Switching these parameters from 90s to 900s ensures that sufficient time is allowed for the boot.

3.27. Ensuring Efficient Firmware Handling of Memory Failures

BullSequana S servers have memory monitoring features built into their design (based on Intel® Predictive Failure Analysis), which are fully independent from operating system-based tools for collecting and reporting correctable and uncorrectable memory errors.

When running Linux, it is therefore recommended to disable the following features to avoid interference with error reporting tracked by the system's management:

- Error Detection And Correction (EDAC)
- the correctable error detection functionality of the kernel's Machine Check Event (MCE) handling

To disable EDAC, search and blacklist the EDAC modules.

To disable the MCE handling, set the boot parameter `mce=ignore_ce`. This boot parameter also disables logging of such events via mcelog.

3.28. Changing BIOS Settings

WARNING W082
These procedures are for advanced users only. Risk of system damage.

WARNING W083
Do not change BIOS setup settings unless directed to do so by the support team.

- To configure volMemMode to AUTO, use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n 'MEM.volMemMode 2'
```

- To enable packet poisoning by default, use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n 'SETUP.PoisonEn 1'
```

- To restore MEM.oppReadInWmm to AUTO, use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n ‘MEM.oppReadInWMM 2’
```

- To improve resilience against memory error, it is strongly recommended to enable Adaptive Double Device Data Correction (ADDDC). Use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n 'MEM.ADDDCEn 1'
```

- To avoid the issue of insufficient throttling for memory modules due to MRC calculation on systems equipped with M386AAG40MMB-CVF - 128GB Samsung - 2933 Mhz memory modules, use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n 'MEM.refreshMode 0'
```

Do not apply this setting if the system is not equipped with this particular model of memory module.

3.29. GPUs with VMware

It is mandatory to set the MMIOH BIOS parameter to 4 using the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n 'RC.MmiohBase 4'
```

Note With NVIDIA Tesla boards and if global memory size is bigger than 4 TB, set the parameter to 6.

3.30. Performance Parameters

3.30.1. BullSequana S200, S400, S800 Servers

1. It is recommended to update the defaultbiossetup file to its latest version and check that the StaleAtoSEn value is set at 1.

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a get -n 'UPI.StaleAtoSOptEn'
```

2. For systems that are running SAP Hana/SAP BW, except BullSequana S200 servers, some BIOS settings may be tuned to improve performance with Intel® Xeon® Scalable processors by disabling HW prefetchers and adjusting IRQ/RRQ threshold.

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set –n 'CPU.DCUStreamerPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set –n 'CPU.DCUIPPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set –n 'CPU.MlcSpatialPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set –n 'CPU.MlcStreamerPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set –n 'UPI.IrqThreshold 3'
```

3.30.2. BullSequana S1600 servers

1. It is recommended to update the defaultbiossetup file to its latest version and check that the StaleAtoSEn value is set at 1.

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a get -n ‘UPI.StaleAtoSOptEn’
```

2. For systems that are running SAP Hana/SAP BW, some BIOS settings may be tuned to improve performance by disabling HW prefetchers and adjusting IRQ/RRQ threshold.

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'CPU.DCUStreamerPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'CPU.DCUIPPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'CPU.MlcSpatialPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'CPU.MlcStreamerPrefetcherEnable 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'PM.WorkLdConfig 0'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'UPI.IrqThreshold 2'
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n 'CPU.L2RfoPrefetchDisable 1'
```

3.31. Mixed Memory Configurations for SAP HANA

3.31.1. BullSequana S200, S400, S800 Servers

Two specific configurations mixing memory modules are allowed under the following conditions:

- For SAP HANA only
- Using only authorized parts:

For first generation Intel® Xeon® Scalable processors	For second generation Intel® Xeon® Scalable processors
• RDIMM 3DS 128 GB (Samsung M393AAK40B42-CWD) with RDIMM 3DS 64 GB (Samsung M393A8K40B22-CWD) • LRDIMM 64 GB (Samsung M386A8K40BM2-CTD) with LRDIMM 32 GB (Samsung M386A4K40BB0-CRC)	• LRDIMM 128 GB (Samsung M386AAG40MMB-CVF) with LRDIMM 64GB (Samsung M386A8K40CM2-CVF) • RDIMM 64 GB (Samsung M393A8G40MB2-CVF) with RDIMM 32GB (Samsung M393A4K40CB2-CVF)

Note With a mix of 64 GB and 32 GB memory modules, the speed is 2 400 instead of 2 666.

- Following populations rules:
  - In the configuration recommended: the larger size memory module in slot 0 and the smaller size one in slot 1
  - All memory modules in slot 0 are the same and all memory modules in slot 1 are the same

3.31.2. BullSequana S1600 servers

Configurations mixing memory modules are allowed under the following conditions:

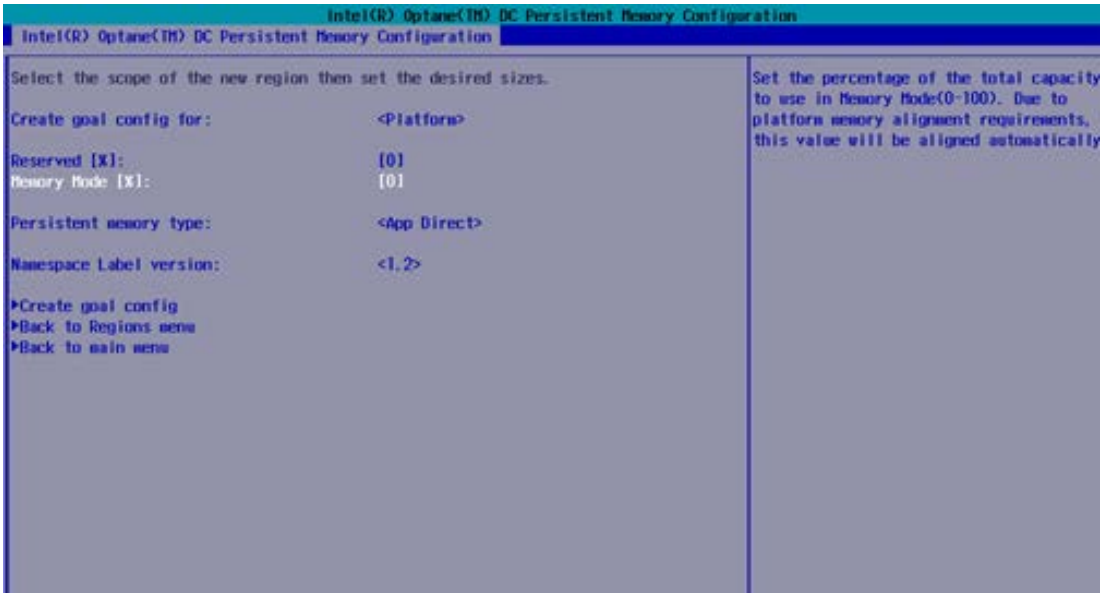
- For SAP HANA only
- Using only authorized parts:
  - LRDIMM 128 GB (Samsung M386AAG40MMB-CVF) with LRDIMM 64GB (Samsung M386A8K40CM2-CVF)
  - RDIMM 64 GB (Samsung M393A8G40MB2-CVF) with RDIMM 32GB (Samsung M393A4K40CB2-CVF)

Note With a mix of 64 GB and 32 GB memory modules, the speed is 2 400 instead of 2 666.

- Following populations rules:
  - All the memory module slots of all the modules are populated
  - Half of the memory module slots are populated with one type of memory module and the other half with the other type.
  - In the configuration recommended: the larger size memory module in slot 0 and the smaller size one in slot 1
  - All memory modules in slot 0 are the same and all memory modules in slot 1 are the same

3.32. Intel® Optane™ DCPMM for SAP HANA

Check that Intel® Optane™ DC Persistent Memory (DCPMM) configuration is as follows:



Reserved [%]: [0]

Memory Mode [%]: [0]

Persistent memory type: <App Direct>

If that is not the case, modify the configuration.

See Configuration Guide for more information on how to configure DCPMM memory modules

3.33. Downgrading the DCPMM memory module firmware

ApachePass firmware versions older than 1.2.0.5355 are no longer supported.

3.34. Servicing Memory modules

Before removing a memory module, go to the SHC Hardware Exclusion page and check that the memory module is not excluded.

If the memory module is excluded, cancel the exclusion from the SHC Hardware Exclusion page.

See SHC Reference Guide for more information on Hardware Exclusion.

3.35. MicroSD cards in Internal Dual RAID board (URS)

In order to work properly in the Internal Dual RAID board, the microSDs must be formatted correctly. Please use only those provided by Eviden representatives.

Chapter 4. Information

4.1. Bull Admin Tools

Due to critical security issues found in iCare , it has been decided that iCare is End of Support and End of Life since January 1st, 2024. It is therefore recommended to customers having iCare installed on one or several systems to uninstall it from all these systems. Check iCare documentation for this purpose.

If uninstalling iCare is not possible for operational reasons, it is recommended to dedicate a host or Virtual Machine (VM) to its usage. The access to the host or VM must be local only and restricted to administrator level, or protected by means external to the host (firewall). If iCare is only used for firmware update, the dedicated resource can also be powered at the request a legitimate user and powered off once the update is complete.

4.2. Displaying Firmware Versions

When displaying the firmware versions in the Server Hardware Console (SHC), the version of the BIOS_BKUP firmware displayed is not the same as the version of the BIOS.

The BIOS_BKUP firmware does not depend on the processor type. It is only used to reset the PEB/PEBS Ethernet connection. It does not allow to boot.

4.3. BMC User Account

The length of the user name and password of a BMC user account is limited to 16 characters.

4.4. Setting up Remote Access

In this procedure in the Getting Started Guide, the default user name and password are incorrect. The correct information is given below.

SHC	
User name	super
Password	S30XXXXX where XXXXX are the last five digits of the system serial number (XAN-S30-XXXXX)

4.5. Enabling Trusted Platform Module (TPM)

Important **Before enabling the TPM feature, it is mandatory to verify that its usage complies with local laws, regulations and policies and get approvals or licenses where applicable. Bull SAS will not be responsible for any related liabilities to any compliance issues arising from your usage of TPM violating the above mentioned requirements.**

Note Contact your sales representative or support team for any TPM retrofit operation.

Prerequisite

Motherboard (CPB) revision 11 or higher

Procedure

1. **Check that TPM is disabled.**

Using the BSM CLI commands

1. Launch the following command:

```
bsmBiosSetting.sh -H <BMC IP address> -u <user> -p <pwd> -a list | grep Tpm
```

2. Check that the settings are set as follows:

Setting	Value
PCH.XTpmLen	1
SETUP.Tpm2Enable	1
SETUP.Tpm2Operation	0
SETUP.TpmClear	0
SETUP.TpmDevice	0
SETUP.TpmHide	1
SETUP.TpmOperation	0

Using the BIOS Interface

1. Launch the BIOS interface.

See Configuration Guide

2. Select **Setup Utility** > **Security** from the main menu.
3. Check that the settings are set as follows:

Setting	Value
Current TPM Device	<Not Detected>

2. Enable TPM

1. Launch the following command:

```
bsmBiosSettings.sh -H <BMC IP address> -u <user> -p <pwd> -a set -n 'SETUP.TpmDevice 2'
```

2. Launch the following command:

```
bsmBiosSettings.sh -H <BMC IP address> -u <user> -p <pwd> -a set -n 'SETUP.TpmHide 0'
```

3. Launch the following command:

```
bsmBiosSettings.sh -H <BMC IP address> -u <user> -p <pwd> -a set -n 'SETUP.TpmOperation 1'
```

3. Check that TPM is enabled.

Using the BSM CLI commands

1. Launch the following command:

```
bsmBiosSetting.sh -H <BMC IP address> -u <username> -p <password> -a list | grep Tpm
```

2. Check that the settings are set as follows:

Setting	Value
PCH.XTpmLen	1
SETUP.Tpm2Enable	1
SETUP.Tpm2Operation	0
SETUP.TpmClear	0
SETUP.TpmDevice	2
SETUP.TpmHide	0
SETUP.TpmOperation	1

Using the BIOS Interface

1. Launch the BIOS interface.

See Configuration Guide

2. From the BIOS main menu, select Setup Utility > Security from the main menu.
3. Check that the settings are set as follows:

Setting	Value
Current TPM Device	<TPM 2.0 (DTPM)>
TPM State	All Hierarchies Enabled, UnOwned
TPM Active PCR Hash Algorithm	SHA1, SHA256
TPM Hardware Supported Hash Algorithm	SHA1, SHA256
TrEE Protocol Verson	<1. 1>
TPM Availability	<Available>
TPM Operation	<No Operation>
Clear TPM	[ ]

Chapter 5. Delivery Content

5.1. Delivered items

- Documentation, firmware and customer tools are delivered on the Resource and Documentation DVD
- BSMHW_NG is delivered on the Bull Administration Tools DVD
- VMware ESXi Installer is delivered, if ordered, on a bootable USB key
- The Eviden High-end Plug-in for vSphere web client and the Microsoft SCOM Management Pack are available on the Bull support website: https://support.bull.com

5.2. Documentation

Note A new item's row is highlighted in gray, a new version is highlighted in gray

Name	Description	Version
BullSequana S Customer Documentation Set	Complete documentation dedicated to the customer	18
BullSequana S Field Documentation Set	Complete documentation dedicated to the field	17

5.3. Platform Firmware

Notes

- A new item's row is highlighted in gray, a new version is highlighted in gray
- Intel® Xeon® 1st and 2nd generation processors now share the same BIOS firmware.
- There are two different images of the BIOS firmware: one compatible with the PEB board and the other with the PEBS board. Their versions are numbered as follows:
  - x=0 for PEBS
  - x=1 for PEB

  The managing tools are configured to automatically select the adequate BIOS image.
- The FLASH_M3WEO firmware version always reads as (0.0.0) even if the firmware has been successfully updated to a more advanced version.

Name	Description	Version
Apache Pass	Firmware for Intel® Optane™ DC Persistent Memory (DCPMM)	01.2.0 build 5446
BIOS_PUR043	BIOS firmware for both first and second generation Intel® Xeon® Scalable processors	43.58.00 build x01
CLK_UNB	Firmware image for the clock generator circuit on UNB boards	0.0.3
CPLD_IO_CPB	Flash image for the IO CPLD component on the CPB board	2.7.1.0
CPLD_LMB	Firmware image for the CPLD on the LMB board	0.5.0.0
CPLD_NBB	Flash image for the CPLD component on the NBB board	3.2.0
CPLD_P_CPB	Flash image for the CPLD component on the CPB board	2.5.3.0
EMM33_BMC	Baseboard Management Controller (BMC) firmware	33.75.00 build 0930
EMM34_LMC	Local Management Controller (LMC) firmware	34.25.00 build 0918
EMM_DEFAULT_ BIOS_SET TINGS	Default BIOS settings file	1.22

Name	Description	Version
ETH_SWITCH_ LMB	Firmware image for the Ethernet switches on the LMB board	0.0.2
ESXi_6.5_ BullSequana_S	VMware supervisor	6.5u3 build 14990892
ESXi_6.7_ BullSequana_S	VMware supervisor	6.7u3 build 15018017
FPGA_CPB	FPGA firmware for the CPB board	3.1.4.0
FPGA_FLASH_ M3WEO	Flash image for the embedded firmware of the sWitch Ethernet One Gigabit (WEO)	1.0.0
FPGA_LMB_Mngt	Management FPGA firmware for the LMB board	0.4.0.0
FPGA_LMB_Multi	Multimode FPGA for LMB board	1.1.0.0
FPGA_UNB	FPGA firmware for UNB boards	0.8.0.0
FLASH_M3WEO	FPGA image for the sWitch Ethernet One Gigabit (WEO)	2.0.0 (appears as 0.0.0)
FW_PEB	Flash image for the SPI 4Mbit 85MHz 8SOIC 256Byte per page	2.B.9
FW_PHY_PEBS	Flash image for the EEPROM 256KBIT 400KHZ 8SOIC	1.0.0
FW_URS	Flash for the SPI 4Mbit 75MHz 8SO	0.0.3
UNC_PE	Processing engine microcode for UNC	1 build 20180808
UNC_PHY	PHY firmware for UNC	1 build 20180808
UNC_SBUS	SBUS firmware for UNC	0001 build 0x101A
UNC_SERDES	SERDES firmware for UNC	0041 build 0x105C
VR_AVDD_UNC0_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_AVDD_UNC1_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_AVDD_UNC2_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_AVDD_UNC3_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_DDR_UNC0_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.3
VR_DDR_UNC1_ UNB	Configuration file for memory voltage regulator on UNB boards	0.0.3

Name	Description	Version
VR_DDR_UNC2_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.3
VR_DDR_UNC3_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.3
VR_VDD_UNC0_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_VDD_UNC1_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_VDD_UNC2_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4
VR_VDD_UNC3_UNB	Configuration file for memory voltage regulator on UNB boards	0.0.4

5.4. PEB/PEBS Ethernet Firmware

The following table gives the versions of the PEB and PEBS Ethernet firmware. Both firmware are embedded in the BIOS firmware.

Name	Description	Version	Build number
FW_X722/X557_Intel	Embedded Ethernet chip for PEB	5.15	800027C5
FW_88E1512_Intel	Embedded Ethernet chip for PEBS	5.15	80002782

5.5. Adapter Firmware

Notes

- A new item's row is highlighted in gray, a new version is highlighted in gray
- The firmware used for the Emulex_PCIe_LPe31002-M6 adapter is also used for the following adapters:
  - Emulex_PCIe_LPe16002-M6
  - Emulex_PCIe_LPe31004-M6
  - Emulex_PCIe_LPe32002-M6
  - Emulex_PCIe_LPe32004-M6
- For vSAN configurations, the recommended firmware version for the LSI_SAS_9305-16i adapter is 16.00.09.00
- The recommended firmware package version for the QLogic_ QL41212HLCU adapters is 2.11.4. It is also recommended to set the following BIOS settings:
  - Link Speed set to 25Gbps
  - FEC Mode set to Fire Code

Name	Version
Boadcom_MegaRaid_NVMe_9560-16i_ 9540-2M2	Package: 52.28.0-5305 (MR 7.28) Firmware: 5.280.00-3972
Broadcom_PCIe_BCM957416A4160C	214.0.253.1
Emulex_PCIe_LPe12002-M8	fw202a4 - UniversalBootCode1220a3 OneCommandManagerCLI 12.2.299.20
Emulex_PCIe_LPe31002-M6	12.6.240.40 OneCommandManagerCLI 12.6.240.33-1
Emulex_PCIe_LPe35XXX-LPe36XXX	14.2.673.40
Ethernet_Intel_I350-X520	23.5.2
LSI_MegaRaid_SAS_9361-16i	Package: 24.22.0-0045 Firmware: 4.740.00-8433
LSI_MegaRaid_SAS_9361-8i	Package: 24.21.0-0091 Firmware: 4.680.01-8446
LSI_MegaRAID_SAS_9460-16i	Package: 51.12.0-3027 (MR 7.12) Firmware: 5.120.00-2904
LSI_SAS_9300_8e	P16:16.00.01.00

Name	Version
LSI_SAS_9300-8i	P16:16.00.01.00
LSI_SAS_9305-16i	Firmware: 16.00.12.00 / 16.00.09.00 BIOS: 08.37.02.00 UEFI BSD: 18.00.03.00
LSI_SAS_9500-8i	28.00.00.00
LSI_SAS_9500-16i	28.00.00.00
Mellanox_ConnectX-4	12.27.1016
Mellanox_ConnectX-4Lx	14.27.1016
Mellanox_ConnectX-5	16.31.1014
QLogic_QL41212HLCU	Package: 2.11.4
SolarFlare_SFN8522	SF-103848 FW 4.15.5.1007-1 SF-107601 FW 8.0.3.1001-1

5.6. Customer Tools

Note A new item's row is highlighted in gray, a new version is highlighted in gray

Name	Description	Version
EMM_REGS_DUMP	This set of files gives the list of registers to dump in CPU and FPGA devices in case of CATERR detection or of IPMI dump command	1.1
EMM33_BMC_Bckp	The backup image of the Baseboard Management Controller (BMC) firmware	33.51.00 build 0592
mc-setup	A Linux Utility used to discover the embedded management board's MAC address and to change the embedded management board's IP address	1.2.1 build 2
MceLog_For_RHEL7	A Linux tool dedicated to collect MCE logs on servers running RHEL 7	158 build 50
MceLog_For_SLES	A Linux tool dedicated to collect MCE logs on servers running SLES	1.48 build 1.13
Plug_in_For_SCOM	A set of tools to allow monitoring of BullSequana S servers by Microsoft System Center Operations Manager (SCOM)	1.0.1 build 161
plug_in_for_vSphere _ Web_Client	Eviden High-end Server Plug-in for vSphere Web Client	3.0
psetup	A Windows Utility used to discover the embedded management board's MAC address and to change the embedded management board's IP-address.	1.2.4

5.7. Management Information Base (MIB)

Note (*) indicates a new version, (**) indicates a new item.

Name	Description	Version
MIB_bull_ PlatformManagement	Defines Platform Management SNMP interfaces of Eviden servers	201807171200Z
MIB_ PlatformEventTraps	The Platform Event Trap definition file. This MIB (Management Information Base) file is used by SNMP (Simple Network Management Protocol) managers to receive server hardware events	2.3.8

5.8. Bull Admin Tools

Note (*) indicates a new version, (**) indicates a new item.

Name	Description	Version
BSMHW_NG	A set of prompt commands, based on free IPMI open source commands, used to manage server or device hardware. These commands can be used to return information and status and/ or to remotely control and configure server hardware	1.5.32
Bull_Admin_Tools_VM_ Appliance	An appliance that delivers Bull Administration tools on CentOS system	4.6.0

Chapter 6. History of previous versions

6.1. All Models

6.1.1. TS 074.01 (May 2024)

New Features and Changes

BIOS_PUR043

- Integrated Insyde code drop 58 aligned with Intel Purley Refresh reference code 628.P.59 (BKC 2024.1 IPU PV)
- Multiple security fixes:

  CVE-2019-17178, CVE-2022-46758, CVE-2023-22612, CVE-2021-38578, CVE-2021-38575, CVE-2022-33985, CVE-2023-25600, CVE-2021-38576, CVE-2023-28468, CVE-2022-40982, CVE-2023-2004, CVE-2023-30633, CVE-2023-31041, CVE-2023-24932, CVE-2022-1292, CVE-2022-2097, CVE-2023-0286, CVE-2022-4304, CVE-2023-0215, CVE-2022-4450, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-39284, CVE-2023-34195, CVE-2023-3817, CVE-2023-3446, CVE-2022-32471, CVE-2023-4807, CVE-2023-28149, CVE-2023-47252, CVE-2023-40238, CVE-2023-45234, CVE-2023-45229, CVE-2023-45232, CVE-2023-45233, CVE-2023-45230, CVE-2023-45235, CVE-2022-36763, CVE-2022-36764

EMM33_BMC

- Updated Dropbear to version 2024.84
- Updated OpenSSL to version 1.1.1w
- Updated Lighttpd to version 1.4.74
- Applied Eviden look and feel to SHC
- Added cpu serial number, S-spec/QDF number as model and the display of all processor contents in raw form to Redfish Processors URI "/redfish/v1/Systems/Server/Processors/Module2_CPU0
- Added ability to load dump reg files on secondary modules through Redfish
- Added confirm password box for bind dn password and check that password meets upper/lower/numeric and special character) requirement
- Added partitions power status to Redfish System schema

Adapters

The following adapters are now supported:

- Broadcom MegaRAID 9560-8i
- Broadcom MegaRAID 9560-16i
- Boradcom HBA 9500-8i
- Broadcom HBA 9500-16i

Bull Admin Tools

Due to critical security issues found in iCare , it has been decided that iCare is End of Support and End of Life since January 1st, 2024. It is therefore recommended to customers having iCare installed on one or several systems to uninstall it from all these systems. Check iCare documentation for this purpose.

If uninstalling iCare is not possible for operational reasons, it is recommended to dedicate a host or Virtual Machine (VM) to its usage. The access to the host or VM must be local only and restricted to administrator level, or protected by means external to the host (firewall). If iCare is only used for firmware update, the dedicated resource can also be powered at the request a legitimate user and powered off once the update is complete.

Resolved Issues

All Models

- **Enabling Secure LDAP**

  Enabling Secure LDAP is now possible from the **Authentication** page of the SHC.

  See SHC Reference Guide

- **Autocomplete attribute for SHC fields**

  The Autocomplete attribute has been deactivated for the **User name** and **Password** fields of the SHC Reference Guide**Authentication** page.

- **Updating the defaultbiossetup file**

  Updating the defaultbiossetup file on a multi-module server using Redfish commands is now possible.

  The following curl command copies the defaultbiossetup file onto the primary and secondary modules.It also overwrite the biossetup file with the contents of the defaultbiossetup file. Finally, this curl command sets the BIOS settings to the new default values.

```
curl --insecure --noproxy "<IP>" -F 'file=@/<source_path>/defaultbiossetup' -F 'name=defaultbiossetup' -H "Expect:" -v -u <user>:<password> 'http://<IP>:8080/redfish/v1/Upload'
```

BullSequana S1600

- **LMB Sensors**

  All PSx Pin and Pout sensor threshold values are now correctly set.

- **Hiding the BMC management port**

  Setting the network.hide_mgt_port key now ensures that the management port (BMC) is no longer visible under OS after reboot.

6.1.2. TS 064.04 (September 2023)

New Features and Changes

This Technical State 064.04 is a patched one compared to Technical State 064.03. It provides a new release of the default BIOS settings file.

It is strongly recommended to apply the new default BIOS settings.

See Upgrade Guide for information on how to apply the default BIOS settings

EMM33_BMC

The BMC firmware present in this TS fixes a BMC-FPGA bug to avoid sudden BMC crashes during system power on.

EMM_DEFAULT_BIOS_SETTINGS

Local Machine Check Exception (LMCE) is now enabled by default. Possible settings for SETUP.LmceEn are 0 = Disabled (old default) and 1 = Enabled (new default).

6.1.3. TS 064.03 (August 2023)

New Features and Changes

This Technical State 064.03 is a patched one compared to Technical State 064.02. It provides security fixes and contains new releases of the BIOS and BMC firmware.

BIOS_PUR043

- Integrate Insyde code drop 48 aligned with Intel Purley Refresh reference code 622.D07 (BKC 2022.2 IPU PV)
- Integrate Insyde code drop 49 aligned with Intel Purley Refresh reference code 623.D09 (BKC 2022.3 IPU PV)
- Integrate Insyde code drop 50 aligned with Intel Purley Refresh reference code 626.P01 (BKC 2023.1 IPU PV)
- Multiple security fixes:

  CVE-2022-24350, CVE-2022-24351, CVE-2022-26350, CVE-2022-27405, CVE-2022-29275, CVE-2022-29276, CVE-2022-29277, CVE-2022-30283, CVE-2022-30771, CVE-2022-30772, CVE-2022-30774, CVE-2022-31243, CVE-2022-32469, CVE-2022-32470, CVE-2022-32471, CVE-2022-32473, CVE-2022-32474, CVE-2022-32475, CVE-2022-32476, CVE-2022-32477, CVE-2022-32478, CVE-2022-32953, CVE-2022-32954, CVE-2022-32955, CVE-2022-33905, CVE-2022-33906, CVE-2022-33907, CVE-2022-33908, CVE-2022-33909, CVE-2022-33982, CVE-2022-33983, CVE-2022-33984, CVE-2022-33985, CVE-2022-34301, CVE-2022-34302, CVE-2022-34303, CVE-2022-34325, CVE-2022-35408, CVE-2022-35893, CVE-2022-35894, CVE-2022-35895, CVE-2022-35896, CVE-2022-36338

- Add WRSDIS bit check to HSTI security report in BIOS log to show bit status. Lock MSR_IA32_DEBUG_INTERFACE early during CPU init. Add HSTI report check for the MSR lock state
- Do not send Custom refresh rate reverted warning to BMC since this is Intel POR for high capacity DIMMs
- Add timeout to UNC temp sensor read to prevent hang when no valid response is received
- Fix “OemMemRasEventHandler: Invalid node, channel, and/or dimm” and “DistributeRasEventToHandler() : Invalid Parameter” when processing memory errors
- Fix register overflow warning on SkyLake
- Change CSR encryption from MD5SUM to SHA256
- Enable LMCE (Local Machine Check Exception) for MCA Recovery

- Add PCIe segment number to several BIOS log messages
- Bugfix for BullSequana S1600, correct segment number for SMBIOS type 9 records and segment groups

EMM33_BMC

- OpenSSL update to version 1.1.1u
- Add support for RPR board ID > 5 and RPL board ID > 4 with A30 GPUs

6.1.4. TS 064.02 (September 2022)

New features and changes

There are no changes whatsoever between Technical Sate (TS) 064.01 and TS 064.02. TS 064.02 exists for purely administrative reasons.

6.1.5. TS 064.01 (August 2022)

New features and changes

All Platform Firmware and Documentation

The terms master module and slave module have been replaced with the terms primary module and secondary module respectively.

BIOS_PUR043

- Integrate Insyde code drop 46
- Multiple security fixes:
  - Using variable lock protocol to lock "SystemSupervisorPw" and "SystemUserPw" variables to prevent form malware to modify these variables at runtime. (CVE-2021-43613)
  - DxeCore: Unlimited recursion in FV processing can corrupt memory. (CVE-2021-28210)
  - An SMM arbitrary code execution may allow attacker modify SPI flash and launch the BIOS bootkit. (CVE-2021-33625)
  - Bug Fix: CVE-2021-33627

Resolved issues

All models

- **Redfish: bmc.tls_version configuration key**

  The bmc.tls_version key now allows to select correctly the supported version of TLS on the Redfish web server.

- **Missing message for aborted dump**

  A message is now displayed when a server dump is not taken because the SD card is in read-only mode.

BullSequana S1600 Server

- **Missing sensor information in collected logs**

  Memory information for module 0 is now correctly included in the collected logs.

- **Error message during firmware update**

  The following error message no longer occurs when using the `bsmFwGlobalUpg.sh -M 16` command to update of the UBox firmware:
  `Use of uninitialized value $compo in pattern match (m//) at /opt/BSMHW_NG/bin/bsmFwGlobalUpg.pl line 1860.`

6.1.6. TS 054.01 (May 2022)

New Features and Changes

ApachePass

This firmware is coming from Purley Refresh 2021.2 IPU PV Intel® Optane™ PMem VIP Kit 684863.

BIOS_PUR043

- Integrate Insyde code drop 45
- Multiple security fixes:
  - AtaLegacySmm: CommBuffer inside of SMI handler is not checked (CVE-2021-41842)
  - Stack buffer overflow vulnerability leads to arbitrary code execution in UEFI DisplayTypeDxe DXE driver (CVE-2021-42059)
  - Int15ServiceSmm: SMM callout vulnerability in combined DXE/SMM driver (CVE-2021-42060)
  - Instead of passing information to SMM by CPU register in FvbServicesRuntimeDx e, changing to use gEfiSmmCommunicationProtocolGuid (CVE-2021-42554)
  - UsbCoreDxe: SMM callout vulnerability in combined DXE/SMM driver (CVE-2021-43323)
- Other security fixes (CVE-2020-27339, CVE-2021-33626, CVE-2021- 33627, CVE-2021-41841):
  - An SMM arbitrary code execution may allow content can be controlled by attacker who attains operating system privilege
  - HddPassword: SMM arbitrary code execution may allow attacker to modify SPI flash and launch the BIOS bootkit
  - FwBlockServiceSmm: SMM memory corruption vulnerability in combined DXE/SMM driver on device (SMRAM write)
  - AhciBusDxe: SMM callout vulnerability in combined DXE/SMM on device (SMM arbitrary code execution) AhciBusDxe: SMM callout vulnerability in combined DXE/SMM driver
- New defaultbiossetup version 1.21
- New Apache Pass (DCPMM) firmware version 1.2.0.5446
- Updated VFR compiler

- Updated the ACPI version from 6.2 to 6.3
- Added SRAT affinity entries for UBOX PCI addresses on BullSequana S1600
- Fixed fatal machine checks in MC Bank 0 (Instruction Fetch Unit) which were occurring at the end of the boot
- Changed the setup option for Refresh Watermarks to Low to reduce susceptibility to Rowhammer-style attacks

CPLD_IO_CPB

- Shifty clock debounced and used
- Constraints set for the clocks used in the design

EMM33_BMC

- KVM Console screen shot through Redfish API
- Config key smc.CleanSDcard for SDcard cleanse
  smc.CleanSDcard = 0 means no cleaning (default)
  smc.CleanSDcard = 1 quick clean (reformatting)
  smc.CleanSDcard = 2 deep clean (total erase, duration: 1h30)
- Add new configuration key “bmc.ssh_fips140_2_mode = yes/no” in which only the highlighted hashes/ciphers will be supported to be compliant with fips140-2 standard
- Dropbear updated to version 2020.81
- Add message log for platform dump abort. Due to SD card or system issues.
  "Platform dump will not be taken - SD card issue"
  "Platform dump will not be taken - System issue"
- Add new configuration key bmc.reset_redfish_cert to reset the redfish certificate. Set this key to ‘yes’ and reboot the BMC. After reboot, the redfish certificate is reset to default and the key is set to ‘no’
- When SHC LDAP authentication is enabled, if a user is not found in LDAP then the user is authenticated locally
- Add config key bmc.tls_version and implement tls version support based on the key
  Setting the minimum tls version for the BMC is as follows:
  Set config key “bmc.tls_version=X” (where X is the desired version [default: 0]).
  Reboot the BMC.
  X can be a number from 0 to 3 and each number represents the following:
  0 = minimum version is tls1
  1 = minimum version is tls1.1
  2 = minimum version is tls1.2
  3 = minimum version is tls1.3

- New default WEB group available: “sshOnly”. Users in this group will only get SSH permission
- Allow Dropbear SSH server public key authentication
- Clean SDcard feature. When the configuration key cleanSDcard is set to true, on next BMC boot the SDcard will be cleaned and the cleanSDcard key is reset to false
- When the configuration key disable_insecure is set to true the following ports: 8080 24 40024 41024 42024 43024 60004 will be disabled on next BMC boot
- Dropbear SSH server has been updated to version 2020.80
- OpenSSL has been updated to version 1.1.1 (TLS 1.3)
- A new configuration key "Physical_machine_tag" has been added and can be set through BSMHW-CLI or Redfish. For Redfish, an OEM property "Physical machine tag" has been added to Chassis Schema. This value is readable under OS in SMBIOS table type 1in field “Family”
- A new configuration key "smc.lastknown_SD_CID" has been added. This key contains the CID (Card Identifier) of the SDcard. This key is filled at BMC init and can be read through BSM-CLI command.
  If the SDcard is replaced by a new one, a message “SD card has been changed” is sent into the message log of the BMC
- In-band IPMI commands filtering.
  When the configuration key bmc.ipmi_filter_bios_kcs is set to enable only some specific IPMI commands are authorized.
  BIOS 43.41.00 is a prerequisite for this feature. If you activate this feature and if you use a BIOS prior to BIOS version 43.41.00 then the OS won’t boot
- Two new mew messages have been added for Post Package Repair BIOS feature: "FPT: Row Failure" and "FPT: Post Package Repair row repaired"

EMM_DEFAULT_BIOS_SETTINGS

- CPU.IoAntiStarvationMode (IO Anti-starvation Mode)
  Enables or disables IO Anti-starvation Mode (only when 2LM memory regions are present).
  Possible settings are 0 = Disable and 1 = Enable (default)
- MEM.AdvMemTestPpr (Adv MemTest PPR)
  This option enables/disables PPR flow for MemTest.
  Possible settings are 0 = Disable and 1 = Enable (default)
- MEM.ColumnCorrectionDisable (Column Correction Disable)
  Disable turns ON Column Correction feature. Enable turns OFF Column Correction feature.
  Possible settings are 0 = Disable (default) and 1 = Enable

- MEM.SmartTestKey (Smart Test Key)
  Number of SmartTestKey. Value in hexadecimal format.
  Possible settings are 0 (default) to 0xFFFFFFFF

- PCI.PostedInterruptThrottle (Posted Interrupt Throttle)
  Enables or disables Posted Interrupt IERR Mitigation which increases the time posted interrupts are throttled to prevent overwhelming the queues.
  Possible settings are 0 = Disable and 1 = Enable (default)

- SETUP.DisableFastString (Disable Fast String after first poison error)
  If this option is enabled, Fast string support will be disabled after processor detects the first poison error.
  Possible settings are 0 = Disable (default) and 1 = Enable

- Changed settings to reduce susceptibility to Rowhammer style attacks:

  - MEM.CustomRefreshRateEn (Custom Refresh Enable)
    Default setting changed from 0 = Disable to 1 = Enable

  - MEM.PanicWm (Refresh Watermarks)
    Default setting changed from 0 = Auto to 2 = Low

- Support for the Intel BIOS Shared SW Architecture (BSSA) Design for Test (DFT) feature has been removed to address a security vulnerability identified in CVE-02021-0144. The following settings have been removed:

  - MEM.BiosSsaBacksideMargining

  - MEM.BiosSsaCmdAll

  - MEM.BiosSsaCmdVref

  - MEM.BiosSsaCtlAll

  - MEM.BiosSsaDebugMessages

  - MEM.BiosSsaDisplayTables

  - MEM.BiosSsaEarlyReadIdMargining

  - MEM.BiosSsaEridDelay

  - MEM.BiosSsaEridVref

  - MEM.BiosSsaLoopCount

  - MEM.BiosSsaPerBitMargining

  - MEM.BiosSsaPerDisplayPlots

  - MEM.BiosSsaRxDqs

  - MEM.BiosSsaRxVref

- MEM.BiosSsaStepSizeOverride
- MEM.BiosSsaTxDq
- MEM.BiosSsaTxVref
- MEM.EnableBiosSsaRMT
- MEM.EnableBiosSsaRMTonFCB

Resolved Issues

All models

- **BMC Serial Console - SSH SOL Typing Not Enabled**

  A SSH SOL session user is no longer prevented from typing or seeing characters after a BMC reset.

- **BMC Serial Console - Connection to SSH SOL port impossible**

  The connection to the BMC SSH SOL port is no longer prevented after a graceless shutdown of a previous SSH session.

- **MSMI Event during OS Reboot**

  Rebooting the OS no longer involves an MSMI event.

- **Redfish: Uploading the defaultbiossetting file**

  When the /redfish/v1/Upload URI is used to upload the defaultbiossetting file, the file is now copied on all the modules, not just the master module.

- **Redfish: Setting AD user group roles**

  The curl command to configure the roles for each AD user group is now functional.

- **Redfish: Restricted operations for LDAP users**

  Performing any admin operations, other than a Power On or Off, is now possible as an LDAP user.

BullSequana S1600 Server

- **Redfish: Update status during UBox firmware update**

  The update status now changes during the update of a UNBx_FPGA firmware.

- **BMC crash during partitioning**

  Frequently partitioning the system no longer causes the BMC of the module from which the partitioning is performed to crash and restart.

6.1.7. TS 044.03 (September 2021)

New Features and Changes

ApachePass

This firmware is coming from Purley Refresh IPU 2020.2 PV Intel® Optane™ PMem VIP Kit 1000618.

BIOS_PUR043

- Fix no Intel Persistent Memory Configuration tab in Device Manager
- Change event to trigger locking SMM region so that locking message is logged
- Update bootlist info at OS launch, fix logical to physical module maps
- Increase leaky bucket threshold and decrease drip interval. Increase leaky bucket threshold from 1000 to 2000. Decrease drip interval from 10.00 hours (at 2933 MHz) or 11.00 hours (at 2666 MHz) to 5.00 / 5.50 hours
- New defaultbiossetup version 1.20
- New official UNC microcode release with workaround for Buried-M issue. Disabling MWC bypass is also required for this to work
- Re-enable buried-M in setup default settings to improve remote memory latency

Note Note The buried-M feature does not apply to glueless servers

- Log Power-Up PPR event to BMC
- Suppress 2x refresh disabled warning for high capacity 16Gb DIMMs since this is Intel platform memory POR (Plan of Record)
- Update PCH 10GbE firmware to version 5.15 from Intel release 2021_WW07_LBG_B2_LEK_PKG
- Update X722Drv.efi from Intel Lan Driver package v26.0 (E4505X5.EFI)
- Correction for a regression that can cause BIOS to crash if a key is pressed on the remote console application. This can occur after the initial console screen and the end of grub or other initial boot manager

EMM33_BMC

PPR (Post Package Repair) support

EMM_DEFAULT_BIOS_SETTINGS

- Increase the default setting for the correctable memory error leaky bucket threshold inMEM.spareErrTh from 1000 to 2000

- Decrease the default setting for the leaky bucket drip interval from 11.00 hours (at 2666 MHz) or 10.00 hours (at 2933 MHz) to 5.50 / 5.00 hours. This is accomplished by decreasing MEM.leakyBktLo from 31 to 30 and MEM.leakyBktHi from 32 to 31

Resolved Issues

All models

- **Force Power Off and Hide Management Port**

  Unselecting the **Hide Management Port** option in the SHC **Network Configuration** page after having powered off the system using **Force Power Off** no longer leads to network connection issues at the next OS boot.

- **Recurring Fan Error Messages**

  The presence of a faulty FDB fan no longer causes the BMC message log to be rapidly full or timeouts on IPMI commands.

- **Inaccessible SHC after a new partitioning**

  Using custom partition names no longer causes the SHC to become inaccessible after doing a new partitioning of the server.

BullSequana S1600 Server

Shutdown Command Ineffective

The system not shutting down after running the shutdown -h now command does not happen anymore.

6.1.8. TS 034.04 (March 2021)

New Features and Changes

This Technical State (TS) 034.04 is a patched one compared to TS 034.03. It provides important fixes and contains new releases of the following firmware:

- BIOS_PUR043
- EMM_DEFAULT_BIOS_SETTINGS

BIOS_PUR043

Fixes data corruption issue in BullSequana S1600 servers where buried-M optimization is enabled. Buried-M was disabled by setting `CPU.enabledBuriedCA` to 0 in previous BIOS release. In this BIOS release Buried-M is now enabled by setting `CPU.enabledBuriedCA` to 1 in BIOS default settings file.

Note Note The buried-M feature does not apply to glueless servers.

EMM_DEFAULT_BIOS_SETTINGS

Change default setting for `CPU.enableBuriedCA` from 0 (Disabled) to 1 (Enabled) to improve remote memory latency.

6.1.9. TS 034.03 (February 2021)

New Features and Changes

This Technical State 034.03 is a patched one compared to Technical State 034.02. It provides important fixes and contains new releases of the following firmware:

- BIOS_PUR043
- EMM33_BMC

Resolved Issues

All models

- **LDAP authentication**

  SHC authentication using Active Directory is now working correctly.

- **Redfish: Data1 and Data2 fields**

  Data1 and Data2 are now persistent: they do not disappear after a BMC restart anymore.

BullSequana S1600 Server

- **Redfish: bmc.physical_machine_tag key**

  Once set, the bmc.physical_machine_tag key is now visible using Redfish.

- **System under Suse OS stuck after reboot**

  The reboot command now functions correctly: the system no longer gets struck during the boot sequence.

6.1.10. TS 034.02 (November 2020)

New Features and Changes This Technical State 034.02 is a patched one compared to Technical State 034.01. It provides security fixes and contains new releases of the following firmware:

- BIOS_PUR043
- EMM33_BMC
- EMM_DEFAULT_BIOS_SETTINGS

6.1.11. TS 034.01 (October 2020)

New Features and Changes

BIOS_PUR043

- Revised LC6/SCI timeout check and added SCI register dump
- Increased timeout for SMM CPU synchronization
- Update Gbe X722 Uefi driver from 3.8.07 to 4.3.05 to fix unhealthy Gbe driver warning in device manager
- Add new setup setting CPU.enableBuriedCA that allows enabling/disabling performance feature "buried-M" for machines with UNC. This setting is disabled by default
- Enable error reporting in UNC after UNC DDR memory initialization to avoid false error signaling
- New defaultbiossetup version 1.15
- ADDDC (Adaptive Double Device Data Correction) is enabled by default for x4 DIMMs on the BullSequana S series. A new "Auto" option for MEM.ADDDCEn enables or disables ADDDC depending on the platform type.

Note Note With ADDDC enabled, there is an application dependent performance impact, typically a few percent, because the Paging Policy is changed from Open Adaptive to Closed. If the performance impact becomes a problem, the setting should be changed back to Disabled.

- SDDC+1 (Single Device Data Correction Plus One) is disabled by default because only single bit errors can be corrected after transition to the +1 state
- SMBus hang error recovery is enabled by default
- Fast Cold Boot is disabled by default
- Check for UPI lane width reduction and send event to the BMC
- Workaround for missing UNC DIMM SPD data
- Disable ME sensor #128 that reports USB2 device connection and disconnection in SEL (USB link that connects BMC USB device seems to disconnect from time to time for unknown reason)
- Force BIOS to attempt correcting UPI link with a cold reset instead of halting the system with assertion in some error condition:
  - When discovered link has one valid port in a side and invalid peer port in other

side

  - When an AP Socket is discovered but hasn't come out of reset

- Enhance SMM MCA Error Handler: Process and report all MCA Banks that have Valid bit set and not only the ones that raise SMI when CATERR occurs
- Reenable PCI resource table dump in BIOS traces for glueless system and keep it disabled for system with UNC
- Update Intel PCH 10GbE firmware from LAN Enabling Kit 2020-ww22-lbg-b2-lek-pkg

EMM33_BMC

- Redfish: support of firmware update for all the LMB/UNB components
- Full SPD DIMM serial number and date code added in Web FRU display page and identity card. BIOS_PUR043.39.01 is a prerequisite
- The SHC WEB page for firmware update is now greyed when connected on a slave module. Firmware update through SHC is now only supported from master module
- SHC: a new group has been added
  - Group name: noWeb
  - IPMI Privilege level: OEM
  - A user in this BMC group won’t be able to open a HTTP session meaning that connection to the GUI won’t be possible
  - A user in this group will only be allowed to launch IPMI commands
- SHC: LMC LED ID management for LMB0, UNB0, UNB1, CLK0, CLK1
- SHC: LMC reset capability added

EMM_DEFAULT_BIOS_SETTINGS

Add new setup option CPU.enableBuriedCA to enable buriedCA in all processors (used on MESCA3 16S only) Possible settings are 0 = Disabled (default) and 1 = Enabled

ETH_SWITCH_LMB

- ETH_SWITCH_LMB firmware versioning feature added
- Failsafe feature while updating ETH_SWITCH_LMB firmware to avoid upgrade of incorrect firmware file added

Resolved Issues

All models

- **System crash with FPGA EPO**

  To prevent this issue, the following parameters have been modified:

  - the Vin_ON and Vin_OFF thresholds in BMC firmware
  - the timing logic for DDR VR Power Good Signals in CPB FPGA

- **Updating the BIOS Firmware**

  The BIOS firmware update through the SHC now ends correctly without any contradictory messages being displayed

- **Redfish: Disappearing properties in Accounts**

  Account properties whose string includes spaces are now correctly managed.

- **Redfish: Firmware update**

  The BIOS and FPGA_CPB firmware updates now take place without any issues.

Server

- **Reset of the LMC**

  Resetting the LMC is now possible from the SHC.

- **LMB and UNB module identification LEDs**

  Management of the LMB and UNB module identification LEDs is now possible from the SHC.

- **ERR_SCI_LINK_FAILURE after OS reboot**

  The timeout delay has been modified in the BIOS firmware to prevent the hang of the system restart after rebooting the OS.

6.1.12. TS 024.02 (August 2020)

New Features and Changes

This Technical State 024.02 is a patched one compared to the Technical State 024.01. It contains new releases of the following firmware.

CPLD_P_CPB

Adds issue fixes

EMM33_BMC Fixes

SHC security vulnerabilities

EMM34_LMC

Adds issue fixes

FPGA_CPB

Adds issue fixes

Resolved Issues

All models

- **System shutdown with CATERR error**

  In rare cases, the system shuts down and a CATERR error is signaled.

- **PCI boards link down**

  In rare cases, the link of all the PCI boards goes down at the same time and the drivers of the PCI boards are unable to re-establish it.

- **Undetected PCI boards**

  In rare cases, at power on, some PCI boards are not started up and therefore not detected by the system.

BullSequana S1600 Server

UNC shutdown

In rare cases, the fan management algorithm reports an incorrect UNC temperature value (over 4000°C) and shuts down the UNC.

6.1.13. TS 024.01 (June 2020)

New Features and Changes

BIOS_PUR043

- Update GbE Binary for PEB and PEBS These binaries contain the fixes for Port 0 drop after Force Power Off and the Port 0 "down" in the OS after re-enabling port 0
- Add new setup option SETUP.BiosSetupVersion. This read-only setting cannot be modified in the BIOS setup utility
- BIOS now sends warning message to BMC when UPI link failed to initialize in full width because it will cause significant performance reduction if one or more UPI link work in half width
- Fix vulnerability: this new BIOS forbids access to SPI flash descriptor from CPU so malicious software can’t corrupt SPI flash
- Add new setup option PCH.DisableShutdownCycle. If set to 1, this option disables PCH response to shutdown message sent from CPU to PCH on catastrophic CPU error. PCH responds to this message by triggering warm reset to avoid potential data corruption caused by CPU unpredictable behavior after catastrophic error. However, this warm reset might also prevent BMC from reading CPU error registers, making it more difficult to find out the root cause of the catastrophic error. So, it is recommended to disable PCH response to shutdown cycle on machines where we want to investigate crashes
- In BIOS 43.37.08.x14 it was required to launch Device Manager to make boot option for iSCSI device appear in boot list. This BIOS fixes this issue: if an Ethernet card configured as iSCSI is present you no longer have to enter Device Manager to boot from a network drive connected to this card
- Fix password check on OS boot: in previous BIOS 43.37.08.x14 there was a problem when supervisor password was enabled in BIOS setup. BIOS would check password on entry into setup utility (which was normal and expected) but also on on OS boot (which was unexpected). This BIOS fixes this issue: when supervisor password is enabled in BIOS setup there is no password check on OS boot, only on entry into setup utility
- In previous BIOS 43.37.08.x14 it was not possible to use IPMI boot device command to boot VMware from USB stick. This BIOS fixes this issue
- BIOS now stops after SCI link init timeout because it is considered a fatal error (BMC firmware will be notified and shut down the machine)
- Report CPU-to-UNC UPI link init failure to BMC. BIOS stops after link init timeout because it is a fatal error. BMC will shut down the machine
- Report secondary module data transfer failure to BMC. BIOS stops after data transfer timeout because it is a fatal error. BMC will shut down the machine

- Clean up UPI link retries in MC banks on BullSequana S1600 servers. Linux will no longer report machine checks in MC banks 5/12 in Linux boot log
- Fix LAN drop problem in Force Power Off

CPLD_P_CPB

Added support for URS to interface BMC and Cyprus chip

EMM_DEFAULT_BIOS_SETTINGS

- Add new setup option SETUP.BiosSetupVersion. The setup version is in an integer format (no dot). For this release, it is 112. The setup version can be viewed using the following command:

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a get -n 'SETUP.BiosSetupVersion'
```

Note Note The setup version should not be modified. It is intended to be read-only

- Change MEM.allowCorrectableError from 1 (Enable) to 2 (AUTO), where AUTO now means DISABLE. The result of this change is to disable the channel if there are FPT errors during memory training
- Add new setup option PCH.DisableShutdownCycle. The default is 0 (Disable). If set to 1, this option disables PCH response to shutdownmessage sent from CPU to PCH on catastrophic CPU error. PCH responds to this message by triggering warm reset to avoid potential data corruption caused by CPU unpredictable behavior after catastrophic error. However, this warm reset might also prevent BMC from reading CPU error registers, making it more difficult to find out the root cause of the catastrophic error. So, it is recommended to disable PCH response to shutdown cycle on machines when investigating crashes:

```
bsmBiosSettings.sh -H <IP> -u <user> -p <pwd> -a set -n ' PCH.DisableShutdownCycle 1'
```

- Add new setup option MEM.Type16Windows. The default is 0 (Disable). It is recommended to set it to 1 (Enable) on Windows systems to report the maximum memory capacity in the Type 16 SMBIOS structure in the format expected by Windows:

```
bsmBiosSettings.sh -H <IP> -u u<user> -p <pwd> -a set -n ‘MEM.Type16Windows 1'
```

EMM33_BMC

- BullSequana S1600: Hardware reset button in SHC is greyed
- BIOS trace is enabled by default
- New version of openssl 1.0.2u
- UPI lane reduction detected and logged into BMC message log

- New config key to force HiTDP config
- Internet Explorer 11 is no longer supported, use Google Chrome or Mozilla Fiirefox
- URS support: RAID configuration status and SD Card 0 and 1 status are monitored and displayed in the sensor page of the SHC
- A timeout error event for UPI link initialization has been added. In some rare cases BIOS can hang indefinitely while waiting for the UPI links to the UNCs to become ready. This event is decoded by the BMC
- Redfish:
  - Now enabled by default
  - Improved response time
  - Support of SEL Clear log action added
  - Active Directory configuration can now be displayed
  - Added PEBS to software inventory
  - Disallow ReadOnly accounts from using Patch in Bios Settings
- Signed firmware update support: this firmware version implements the control of firmware signature during the update process. Only signed firmware can be updated from this version. Update of non signed firmware will be refused

EMM34_LMC

- UNB Fan Control algorithm
- Signed firmware update support: this firmware version implements the control of firmware signature during the update process. Only signed firmware can be updated from this version. Update of non signed firmware will be refused

FPGA_CPB

- Changes to Turn ON ID LED when reset button pressed is implemented
- Error dump feature during abrupt shutdown due to EPO, CATERROR and THERMTRIP implemented

Resolved Issues

All Models

- **Faulty memory module information missing from the SHC**

  When a DCU error (Poison error) is detected, the faulty memory module is now identified in the Server Hardware Console (SHC).

- **Memory module exclusion**

  Excluding a memory module using the Hardware Management CLIs is now possible.

- **Slave modules unavailable**

  Having unavailable slave modules after booting no longer happens.

- **Redfish: DCPMM memory modules**

  The MemoryDeviceType is now correctly set to IntelOptane for DCPMM memory modules.

- **Redfish: PEBS firmware**

  For systems equipped with PEBS modules, the PEBS firmware are now listed in the redfish/v1/UpdateService/SoftwareInventory.

BullSequana S1600 servers

- **iCare: Incorrect event owner in the System Even Log viewer**

  There are no longer any discrepancies in the event owners.

- **iCare: Failed update of FPGA_LMB_Mngt during global firmware update**

  The FPGA_LMB_Mngt_Image firmware (LMB MAIN_FPGA2) is now correctly updated during firmware global update.

6.1.14. TS 022.04 (July 2020)

New Features and Changes

This Technical State 022.04 is a patched one compared to the Technical State 022.03. It contains new releases of the following firmware.

BIOS_PUR043

- Fixes SHC security vulnerabilities
- Adds new setting PCH.DisableShutdownCycle

  This setting can be used to prevent the reset of the system in order to investigate a crash and collect exhaustive dumps.

  It is set to 0 by default, meaning the reset of the system will happen.

  If it is set to 1, the reset will be prevented. It is recommended to set the setting to 1 only when investigating a problem.

CPLD_P_CPB

Adds issue fixes

EMM33_BMC

Fixes SHC security vulnerabilities

FPGA_CPB

Adds issue fixes

Resolved Issues

This release fixes the following issues.

- **System shutdown with CATERR error**

  In rare cases, the system shuts down and a CATERR error is signaled.

- **PCI boards link down**

  In rare cases, the link of all the PCI boards goes down at the same time and the drivers of the PCI boards are unable to re-establish it.

- **Undetected PCI boards**

  In rare cases, at power on, some PCI boards are not started up and therefore not detected by the system.

6.1.15. TS 022.03 (January 2020)

New Features and Changes

This Technical State 022.03 is a patched one compared to the Technical State 022.02. It contains new releases of the following firmware:

- BIOS_PUR043
- EMM33_BMC

Resolved Issues

All Models

Connection to the BMC lost

On a multi-module compute box, if the Hide Management Port option is selected in the SHC of each module, a Force Power Off results in the loss of the connection to the BMC.

BullSequana S1600 servers

Reboot under OS impossible

Restarting the system under OS is not possible: the booting sequence gets stuck and the system cannot be powered off.

6.1.16. TS 022.02 (December 2019)

New Features and Changes

ApachePass firmware

New wipeout script "startup.nsh rev 1.1": allows to clear the content of DCPMM memory modules in Application Direct mode.

BIOS_PUR043 firmware

- Support BullSequana S1600 servers
- Update Gbe X722 Uefi driver from 2.0.36 to 3.8.07 to fix unhealthy Gbe driver in device manager
- Report correctly uncorrectable fatal error generated by Data Cache Unit (DCU) Machine Check Bank 1 in BMC as Fatal error instead of no-Fatal error
- Updated to Intel PurleyRefresh reference code BKC19ww26 (New ApachePass firmware image required version (5395))
- Update PCH ME Firmware to latest version SPS_E5_04.01.04.323.0
- Update first generation Intel® Xeon® Scalable processor H0 microcode to version mb750654_02000064
- Update second generation Intel® Xeon® Scalable processor B0 microcode to version mbf50656_0400002b
- Update second generation Intel® Xeon® Scalable processor B1 microcode to version mbf50657_0500002b
- Update second generation Intel® Xeon® Scalable processor A0 microcode to version mb750655_03000012
- Fix "IPMI Watchdog timer expired" event logged in BMC messages after 20 min when booting FrontPage or Setup
- Update PEB and PEBS 10GbE firmware to 4.10 version from Lewisburg Enabling Kit "2019_WW23_LBG_B2_LEK_PKG"
- Fast boot is disabled by default. To enable it, use the following command:

```
bsmSetConfParam.sh -H BMC_IP -u super -p pass -k 'bmc.bios.enable_traces' -x yes
```

- New default setup settings file v1.9

EMM33_BMC firmware

Redfish:

- assetTag field management
- Support of SSL certificate for https access through redfish
- it is possible to update some firmware through redfish interface
- it is possible to get or set any BIOS setting
- Active Directory user's group support
- support of Managers/{BMC_Instance}/LogServices schema
- support Managers/{BMC_Instance}/EthernetInterface schema
- support Managers/{BMC_Instance}/NetworkProtocol schema
- adding LDAP enable attribute for authentication through LDAP or not. It is persistent (ie over a BMC reset)
- monitoring of redfish services for automatic restart if a service stop
- adding two OEM attributes 'data1' and 'data2' in chassis schema. The usage is customer dependent. They are persistent (ie over a BMC reset)
- add slave support for log-service messages

EMM34_LMC firmware

Logging of UNC Error Dump Registers post CATERR event assertion

EMM_DEFAULT_BIOS_SETTINGS file

The defaultbiossetup file has been updated to include all BIOS settings contained in BIOS_PU043.36. This includes the settings to disable PCIe ports on module 4 and above:

- PCI.PciePortDisableMx_y (where x = module# and y = port #)
- default = 2 (AUTO)

FPGA_LMB_Mngt firmware

Error dump feature implemented

FPGA_LMB_Multi firmware

Clock measurement improvements for 100MHz

FPGA_UNB firmware

Clock measurement improvements for 100MHz

Resolved Issuees

Redfish

- https connection is now supported
- The Count attribute for ProcessorSummary is now correctly implemented

All models

FPGA Update

The update of the FPGA_CPB firmware, using the CLI commands or the Server Hardware Console (SHC), is now completed normally.

BullSequana S1600 servers

- **System Hard Reset or Reboot**

  Performing a system hard reset or reboot from the Operating System (OS) is now possible.

- **Incomplete FRU Information**

  The FRU information of the UBox components, displayed in the SHC FRU Information page, is now complete

- **Incorrect Total Memory Size**

  The Memory Size value displayed in the SHC Power Management is now correct: the value displayed is the memory size of the partition.

- **IPMI Out-Of-Band Deactivation**

  The deactivation of IPMI OOB from the slave module is now propagated to the slave modules.

6.2. BullSequana S200, S400, S800 Servers

6.2.1. TS 021.03 (September 2019)

New Features and Changes

This Technical State 021.03 is a patched one compared to the Technical State 021.02. It contains new releases of the following firmware:

- EMM33_BMC
- FPGA_CPB

Resolved Issues

This release fixes the following issues.

- **Motherboard (CPB) failure**

  There are some very rare corner cases where transition from very low current to very high current in the Voltage Regulator (VR) of the CPU may damage this VR and so causes a mother board failure.

- **Server Hardware Console (SHC) with /var full**

  On BullSequana S200 servers, the SHC version 33.38.00 may hang due to the /var file system being full.

6.2.2. TS 021.02 (July 2019)

New Features and Changes

BIOS_PUR043

- Integrate Insyde code drop 34 aligned with PurleyRefresh BKC19ww16 (Intel® DCPMM firmware image required revision (5375))
- Update PCH ME Firmware to latest version SPS_E5_04.01.04.296.0
- Support second generation Intel® Xeon® Scalable processor stepping A0, B1, H0
- Update first generation Intel® Xeon® Scalable processor H0 microcode to version mb750654_0200005e
- Update second generation Intel® Xeon® Scalable processor microcodes
  - B0 to version mbf50656_04000024
  - B1 to version mbf50657_05000024
  - A0Intel® Optane™ DC Persistent Memory (DCPMM) to version mb750655_03000010
- Added "Fast Boot" option, that help to reduce BIOS traces and therefore boot time. Can be activated with a BMC key:
  - bsmSetConfParam.sh -H BMC_IP -u super -p pass -k 'bmc.bios.enable_traces' -x yes|no
  - pmsmMC.py config –n bmc-node –s bmc.bios.enable_traces=yes|no
- Make BIOS boot automatically the next Bootable Device without displaying Popup Fail
- Log Intel® DCPMM runtime health status changes and uncorrectable (poison) memory errors to the BMC. To enable this logging, either:
  - Apply the default settings from the defaultbiossetup.1.8 file:

```
bsmBiosSettings.sh -H ip -u user -p password -a reset
```

  - Enter the following commands:

```
bsmBiosSettings.sh -H ip -u user -p password -a set -n 'SETUP.FnvErrorEn 1'
```

```
bsmBiosSettings.sh -H ip -u user -p password -a set -n 'SETUP.FnvErrorLowPrioritySignal 1'
```

```
bsmBiosSettings.sh -H ip -u user -p password -a set -n 'SETUP.FnvErrorHighPrioritySignal 1'
```

- Dump Model Id and Stepping of each processor in multimodule system
- Fix unexpected VMware crash when the Page Retirement feature is activated

EMM_DEFAULT_BIOS_SETTINGS

Note The defaultbiossetup file is common to first and second generation Intel® Xeon® Scalable processors.

- Disable MEM.setSecureEraseAllDIMMs setting changed from 1 (Enable) to 0 (Disable). Default setting in defaultbiossetup file was incorrect. This setting, when enabled, causes persistent Intel® DCPMM to be erased during the boot when security on the memory module is enabled and locked.
- Enable Intel® DCPMM RAS support by enabling the following settings:
  - SETUP.FnvErrorEn changed from 0 (DISABLE) to 1 (ENABLE)
  - SETUP.FnvErrorHighPrioritySignal changed from 0 (DISABLE) to 1 (SMI_SIGNAL)
  - SETUP.FnvErrorLowPrioritySignal changed from 0 (DISABLE) to 1 (SMI_SIGNAL)
- Enable XptPrefetchEn for second generation Intel® Xeon® Scalable processors

EMM33_BMC

- The udpsrv/tftp server in the BMC does NOT do a DNS lookup for name resolution anymore. This prevents having time-out during the tftp transfers when the DNS is not accessible
- In Configuration -> BMC Settings -> Messages web page of the SHC, when enabling Syslog forwarding feature, the System Event Log events are now sent to the remote syslog in addition to the messages logs
- In Configuration -> BMC Settings->Network web page of the SHC, it is now possible to disable IPMI OOB access
- In Configuration -> BMC Settings->Network web page of the SHC, it is now possible to hide eth0 port to the operating system
- Display firmware version of Intel® DCPMM in web interface
- Sensor list and values have been added in the log collect function of the SHC
- A progression bar has been added in the power management web page when powering on or off the server
- The green power LED is now used to indicate boot sequence
- This release is the first release that brings the support of Redfish. Please refer to the Redfish documentation to have detailed on which features are supported

Resolved Issues

- **Getting FRU Information on Mellanox ConnectX-4 Adapters**

  There are no more discrepancies between the adapter FRU information displayed by the Server Hardware Console (SHC) and the results of the lspciconf_m3.pl script.

- **SHC Messages Page Unreachable**

  Using the ¨ character in a user message no longer renders the Messages page unreachable.

- **PEBS SFP Fault Messages**

  The out of place message is no longer displayed when no cables are plugged into to the PEBS.

- **WEO Fault Signal**

  A WEO fault signal message is no longer issued.

- **System crash when the Page Retirement feature is activated**

  There are no longer system crash after several correctable memory errors when the Page Retirement feature is activated. The SDDC+1 and Page Retirement features may have been disabled as part of the temporary workaround. After the installation of the TS 021.02, enable them with the following CLI commands:

```
bsmBiosSettings.sh -H X.X.X.X -u super -p <password> -a set -n 'MEM.SddcPlusOneEn 1'
```

```
bsmBiosSettings.sh -H X.X.X.X -u super -p <password> -a set -n 'MEM.PageRetireEn 1'
```

6.2.3. TS 020.03 (May 2019)

New Features and Changes

This Technical State 020.03 is a patched one compared to the Technical State 020.02. It contains new releases of the following firmware:

- BIOS_CCL041
- BIOS_SKL040
- EMM33_BMC

Resolved Issues

- **Unexpected Server Hardware Console (SHC)**

  Reboot The SHC does not reboot unexpectedly anymore.

- **Incorrect USB Ports found by Microsoft WS2019 Cert test**

  The test now finds the correct type and number of USB ports.

6.2.4. TS 020.02 (March 2019)

New features and changes

General

This version supports the following main new features:

- Second generation Intel® Xeon® Scalable processors
- Intel® DCPMM memory modules

BIOS_SKL040

- Supports display of Eviden logo on the BIOS access screen
- Add 2 corrections for BIOS settings that could return to default values and cause loss of customer settings:
  - Preventing reset BIOS settings to default in case of CMOS issue (battery or checksum)
  - Avoid copying defaultbiossetup file to current biossetup file (then resetting configuration) prior to the transfer of the current BIOS settings back to EMM, at the end of BIOS phase
- RAS: supports Partial Memory Mirroring, adapt the event sent to BMC in consequence
- Enable data poisoning but let Viral disabled, used for error containment
- Update Intel® Server Platform Services manageability engine firmware version to SPS_E5_04.00.04.393.0
- First generation Intel® Xeon® Scalable processor microcode has evolved to MB750654_02000050 in Intel's Reference Code

CPLD_P_CP

PEB Phy reset and SPI Mux selection logic changed to take care of corner cases of PEB flash corruption during AC Power ON/OFF operation.

EMM_DEFAULT_BIOS_SETTINGS

- Configure volMemMode to AUTO instead of 1LM to natively support MemoryMode (2LM) required by DCPMM memory modules
- Enable packet poisoning by default to allow a better errors containment

EMM33_BMC

- Support of DCPMM memory modules
- New Atos branding support

- An informative message is added in the message log during boot if the memory size is different from the one stored during previous boot
- An informative message is added in the message log during boot if the number of CPUs is different from the one stored during previous boot
- User can add free text in BMC message log through web interface: Maintenance > Maintenance Operations > Add User Message
- New RAS event: Partial Memory Mirroring activated
- A new option is available to User in Maintenance > Remote Console Setting > User Specific > "Launch Remote Console in Java WEB Start" to enable/disable the use of Java Web Start to launch the Remote Console
- Improvement in security, some deprecated ciphers have been disabled:
  - SEED-SHA, RC4-SHA, RC4-MD5, DES-CBC3-SHA, DES-CBC-SHA, EXP-DES-CBC-SHA, EXP-RC2-CBC-MD5, EXP-RC4-MD5
  - No possibility of enabling enable-weak-ssl-ciphers - support have been removed in openssl
  - SSL v3 is disabled

FPGA_CPB

- Implemented BMC watchdog time out reset counter
- Support to reset PCH and PEB PHY using ASRAM register

Resolved issues

Note The four first issues listed below are actually resolved by the TS 007.02 but were missing from its release note.

- **Ethernet Activity LEDs**

  PEB Ethernet LEDs behave now correctly.

See Description Guide for more information on LED behavior

- **Fan Messages at Power On**

  No more inconsistent fan status messages are issued at Power On.

- **Power Supply Unit (PSU) Redundancy Sensor**

  The Power Redundancy sensor is now reliable to check power supply.

- **Dismounting and Mounting Back a Module from a Partition**

Partitioning from the SHC after having dismounted and mounted back a module from a partition on a multi-module with a partition made of two modules is now possible.

- **Memory Module exclusion**

  Excluding a memory module from the SHC is now possible.

- **BIOS Update**

  Using the Preserve NVRAM option when updating the BIOS firmware does not lead to PEB/PEBS issues anymore.

Note To avoid any issues with firmware update, it is strongly recommended to use the global firmware update feature available through iCare or the BSM CLI commands.

6.2.5. TS 007.02 (November 2018)

New features and changes

BIOS_SKL040

- Add new entry "12TB" for MMIOH_Base setting in BIOS setup to solve a failure with VMware ESXi and Tesla GPU cards
- Update first generation Intel® Xeon® Scalable processor microcode for security issues Spectre_NG and L1TF (SA-00115 and SA-00161) to version MB750654_0200004D
- Fix the ACPI SLIT table when SNC is enabled, now the table is getting the correct distances
- Implement Page Retire mechanism for VMware (remove memory pages when too much corrected errors occur) by using CMCI interface. This mechanism is controlled with 3 new settings and enabled by default:
  - MEM.PageRetireEn: Activate or not the Page Retire (0=Disable/1=Enable)
  - MEM.PageRetireErrThreshold: Num of errors in a timeframe (default:10)
  - MEM.PageRetireThresholdWindow: Timeframe in hours (default:24)
- Remove "Lacking IO resources" warning because it is only useful in Legacy mode not UEFI mode
- Workaround for UPI Topology issue, rerun several times the process instead of aborting immediately (max 4 times)
- Send additional information to EMM when error with DIMMs to know if memory is excluded or not
- Use BIOS Code drop 59

CPLD_IO_CPB

Filter removed from BMC hang status signal to decrease action delay during the BMC hang event Filter added for BMC hang status signal

EMM33_BMC

- New version of OpenSSL 1.0.2k, to increase the security level (support of TLS 1.2)
- New version of OpenLDAP 2.4.46

EMM_DEFAULT_BIOS_SETTINGS

- Revert UPI.StaleAtoSOptEn to 1, mistakenly switched to 0
- Add a revision number to the defaultbiossetup file, name will now have the following naming: "defaultbiossetup.X.Y"
  - X= Major revision (example: adding or removing settings)
  - Y= Minor revision (example: changing settings values)

Important **The revision number must be removed from the name before the file is uploaded to BMC.**

- To avoid any compatibility issues with USB devices, all the USB ports located at the front of the server are configured as USB2 ports. Default value are switched to 0 instead of 1.
  - PCH.PchUsbSsPort_3 : control topmost connector
  - PCH.PchUsbSsPort_4 : control bottommost
  - PCH.PchUsbSsPort_5 : control middle
- Add 3 new BIOS settings for VMware Page Retirement
  - MEM.PageRetireEn : Activate or not the Page Retire (0=Disable/1=Enable)
  - MEM.PageRetireErrThreshold : Num of errors in a Timeframe (default:20)
  - MEM.PageRetireThresholdWindow : Timeframe value (default:24 hours)

  To modify the settings, use the following command:

```
bsmBiosSettings.sh -H <IP address> -u <user> -p <pwd> -a set -n '<parameter> <value>'
```

FPGA_CPB

- ASRAM operating frequency changed to 100Mhz from 200Mhz
- PEB buffer was in Flip Flops. To do timing closure, this is changed to RAM
- FPGA_CS_N signal is double synced before using in the counter
- Latches were there in CAT Error and CPU F/U/C Error Timers and this are removed
- Clock enable signals were used as clocks in few places so these are changed too
- The 6.25MHz clock to shifty bus logic were output of counter earlier. Now this clock is generated from PLL itself
- Some dangling logics are removed

- Clock and other timing constraints were updated to make sure there are no internal timing issue
- Latches were there in Sync block and these are removed now

FPGA_M3WEO

- Fixed major revision ID
- The following registers were wrongly mapped for module 1 and module 2:
  - SPI1_register_addr_B16 - o_SPI1_register_addr_B17
  - o_SPI2_register_addr_B16
  - o_SPI2_register_addr_B17

  This been corrected: the following operations will now function correctly.
  - FRU Read/Write
  - BCM register Read/Write
  - BCM Flash Read/Write
  - M3WEO register access for module 1 and module 2

Resolved issues

- **FAN Regulation Messages**

  Fan speed is now suitably regulated: there are no longer multiple alarming fan speed sensor statuses or messages in the System Event Log (SEL).

- **Mounting Drives as Virtual Media**

  Virtual Media now works correctly with two drives. Be aware that clicking on Connect or Disconnect in the Virtual Media dialog box causes the existing virtual media to be disconnected and a new USB device to be connected with the updated virtual media configuration.

  Also, clicking on Virtual Media Connect or Disconnect buttons while an installation is running from virtual media is likely to interrupt the installation.

- **PXE Boot with a Mellanox_ConnectX-4Lx Adapter**

  With the adapter firmware provided with this TS, the UEFI firmware is now installed by default. Consequently, booting with PXE is no longer an issue. If this adapter is part of the server, be sure to update its firmware to the latest version.

- **IO Port Resource Message**

  The irrelevant *Lacking IO port resource* message no longer appears when booting.

6.2.6. TS 006.02 (August 2018)

New Features and Changes

BIOS_SKL040

- Enable StaleAtoSEn BIOS setting by default to improve performance

See Chapter 4. Recommendations for more information on performance improvement

- Fix BullSequana S800 USB booting timeout for VMware
- UPI warning message sent to BMC only when failure in fast mode
- Suppress UPI warning for non-existing UPI link
- Avoid errors on Intel® Xeon® Scalable processors with only two UPI links
- Fix in DMAR table avoiding error messages with RHEL
- Fix Bootdev issues with bootable USB or VMware
- Provide relevant memory module location information in case of memory failure or warning (module/socket/iMC/channel/dim/rank)
- Fix SRAT APIC and X2APIC affinity structures

EMM33_BMC

- In Messages log, BIOS messages are not displayed as BMC messages anymore
- Support of OEM model 38 in SNMP traps

FPGA_CPB

- Logic used to run RPL_FAN at full speed changed
- ID LED turning ON or OFF logic moved to IOCPLD

Resolved Issues

- **Power Consumption Sensors**

  The CPU power consumption sensors now reports correct values.

- **WEO fault Message**

  A WEO fault message is no longer issued when the WEO sensor has no reading.

- **Boot Manager Entries**

  When there are more than 15 entries in the boot manager, each entry is now assigned a unique EFI network number.

- **Memory Module Messages during BIOS Initialization**

  Inconsistent warning messages about the memory modules are no longer issued during BIOS initialization.

- **Updating Firmware from the Server Hardware Console (SHC)**

  When a firmware update is successful, the following message is no longer displayed:
  Please wait for the connection to be established.

- **Missing Processors When Booting the server**

  There no longer processors missing from the configuration with the following message in the SEL:
  `18:14:01 BMC Message BIOS Init Warning Message on Module: 0 DIMM: ([Major-code:58h; Minor-code:02h])`

6.2.7. TS 005.04 (June 2018)

New features and changes

EMM33_BMC

New release fixing the following issues:

- Incorrect system name displayed by the NFC tag
- DFM LEDs turning on red randomly

FPGA_CPB

New release fixing the following issue: DFM fans always running at full speed

Resolved Issues

- **Incorrect system name displayed by the NFC tag**

  There are no longer errors in the system name displayed by the NFC tag.

- **DFM LEDs turning on red randomly**

  The DFM LEDs do not become red randomly anymore.

- **DFM fans always running at full speed**

  The DFM fans are now running at suitable speed.

6.2.8. TS 005.03 (May 2018)

New features and changes

EMM33_BMC

New release fixing the following issue: DFM fans randomly unavailable with TS 005.02.

Resolved Issues

DFM fans randomly unavailable with TS 005.02

With the present release of the EMM33_BMC firmware, the fans are running normally, without random faults.

6.2.9. TS 005.02 (March 2018)

New features and changes

BIOS_SKL040

- Intel fix for Spectre and Meltdown issues
- Memory SddcPlusOne RAS feature enabled by default
- Fixed excluded dimm display in setup memory topology
- Improved PatrolScrubbing logging messages on error
- The integrated Gbe controller is now reported to the Server Hardware Console (SHC)
- Improved dmidecode type9 display for PCIe slots information
- The Press Esc line is now displayed at 60% of window height for small screens. • Added Rank Sparing RAS feature (1 or 2 spare ranks)
- Improved RAS messages sent to SHC for SDDC, ADDDC, RankSparing, Leaky Bucket RAS features

EMM33_BMC

- Changed display of identification LED for better understanding of actions
- SEL events can be displayed in multiple or single web pages
- Added the SEL binary file to Collect Log files
- Partitioning is now available from the SHC, including from a slave console
- Boot device and instance can be selected from the SHC. This is used to set parameters that direct the system boot to a particular option after a system power up or reset. This feature is the same as the IPMI boot device option
- PCIe hot plug is available under Red Hat and Suse only
- On the Power Management web page, Force Power Off, Force Power Cycle, Hard Reset and Diagnostic Dump commands need to be confirmed
- The "super" user name can be modified from the SHC
- Implemented reset to default function

FPGA_CPB

Fans run at FULL SPEED when the SHC hangs in power on state

Resolved Issues

- **Simultaneous power on of different partitions**

  Powering on two modules of different partitions simultaneously is now possible.

- **Update on a BullSequana S800 Server**

  Inconsistent messages are no longer issued at power on after updating the FPGA on a BullSequana S800 server.

- **BullSequana S200 Server BIOS Update with Error in SEL**

  Inconsistent messages are no longer issued when the BIOS update is successful.

- **Unable to Update Bios with the Preserved Nvram Option**

  Updating the BIOS firmware from the SHC with the preserved Nvram option is now possible. On a multi-module server, every module is updated successfully.

- **ESXi 6.5 Installation Failure on USB Raid SD Card (URS)**

  Installing ESXi 6.5 on a USB Raid SD Card (URS) with Virtual Media is now possible without failure.

- **Updating the SHC firmware on a multi-module server**

  The SHC will not show the firmware update as completed if it is not completed on all modules.

6.2.10. TS 004.02 (January 2018)

This Technical State 004.02 is a patched one compared to the Technical State 004.01. It addresses the Intel Meltdown/Spectre patch.

See The Technical Support Bulletin 400-18-02 for more details, available on the Bull Support Website: https://support.bull.com

6.2.11. TS 004.01 (December 2017)

First delivery

6.3. BullSequana S1600 Servers

6.3.1. TS 016.02 (September 2019)

New Features and Changes

This Technical State 016.02 is a patched one compared to the Technical State 16.1. It contains new release of the EMM33_BMC firmware.

This release supports iCare 2.7.0 with restrictions.

See Section 2.1.1. Server Hardware Console (SHC) Restrictions for more information on iCare restrictions

Bull Support website https://support.bull.com to download iCare 2.7.0

6.3.2. TS 016.01 (August 2019)

New features and changes

BIOS_CCL042

- OSB (opportunistic snoop broadcast) is disabled if UNC is present
- New reference code 584.D01 (BKC 19ww16)
- New microcode mbf50657_05000024 for second generation Intel® Xeon® Scalable processor stepping B1
- BIOS setup settings are no longer hard-coded. They can be changed via BSM CLI
- New setup settings 'PCIePortDisableMx' allow disabling PCIE root ports in modules 4 to 15 (in previous BIOS version you could disable PCIE root ports in modules 0 to 3 only)

CPLD_LMB

- CPLD IPMI Upgrade Bug fix. The xcf file of CPLD is updated with operation field XFLASH Erase, Program, Verify
- BMC push button reset press status logging and clear option implemented

EMM_DEFAULT_BIOS_SETTINGS

- This file must be uploaded to the BMC SD card with BSM CLI command without any revision number extension:

```
bsmBiosSettings.sh -H [IP] -a copy -f [path_to]/defaultbiossetup
```

- This file is used in 2 cases:
  - when the current bios setting file is missing on SD card, it is created based on defaultbiossetup
  - When we run a BSM CLI command "reset", current bios setting file is replaced by defaultbiossetup (user settings are lost):

```
bsmBiosSettings.sh -H ip -u super -p pass -a reset
```

- Disable MEM.setSecureEraseAllDIMMs setting changed from 1 (Enable) to 0 (Disable). Default setting in defaultbiossetup file was incorrect. This setting, when enabled, causes persistent DCPMM memory to be erased during the boot when security on the DIMM is enabled and locked
- Enable XptPrefetchEn for second generation Intel® Xeon® Scalable processors

EMM33_BMC

- Collect log show SEL, sensors and messages for LMBs
- The udpsrv/tftp server in the BMC doesn’t do any more a DNS lookup for name resolution. This prevent from having time-out during the tftp transfers when the DNS is not accessible.

EMM34_LMC

- Platform Event traps emitted by LMC firmware contain LMB board serial number and board ident information
- The udpsrv/tftp server in the BMC doesn’t do any more a DNS lookup for name resolution. This prevent from having time-out during the tftp transfers when the DNS is not accessible

FPGA_CPB

- CPU0,CPU1 PROCHOT signals are now being driven from FPGA to CPU based on the CPU0 and CPU1 VRHOT signals which causes CPUs to throttle.
- MEMHOT signals also being driven from FPGA based on the memory VRHOT signals.

Resolved issues

- **Unresponsive Module 0 CPU Purley Board (CPB)**

  After an AC OFF/ON of the system, the CPB board of the module 0 now responds to ping requests.

- **Accessing Slave Modules System Event LOG (SEL)**

  On a server partitioned in two four-module partitions, the SEL of the slave modules is now displayed in the SHC web interface of the master module.

- **BIOS Firmware Update**

  The update of the BIOS firmware now succeeds without occasional errors.

- **CPLD_LMB Firmware Update**

  The update of the CPLD_LMB firmware with the BSMCLI command now succeeds.

6.3.3. TS 015.01 (June 2019)

New features and changes

CPLD_NBB

- Enclosure management disk locate feature included
- NVMe disk power sequence state machine changed to handle 3.3V AUX fault under standby

EMM33_BMC

- In Configuration -> BMC Settings -> Messages web page of the SHC, when enabling Syslog forwarding feature, the System Event Log events are now sent to the remote syslog in addition to the messages logs
- In Configuration -> BMC Settings->Network web page of the SHC, it is now possible to disable IPMI OOB access
- In Configuration -> BMC Settings->Network web page of the SHC, it is now possible to hide eth0 port to the operating system
- In Maintenance -> Maintenance Operations -> Add Users Message web page of the SHC, it is now possible to add a free text message in the message log
- Sensors list and values have been added in the log collect function of the SHC
- A progression bar has been added in the power management Web page when powering on or off the server
- The green power LED is now used to indicate system state flow
- The display of the SEL events for the LMC in WEB monitoring interface is available
- Clock loss monitoring is available
- UNC Error pins monitoring (U,F) available

EMM34_LMC

- Added SMC feature for Board ID /Revision ID
- Web changes for displaying LMB's SEL tab in master Web page
- UNC error monitoring support added
- Enabling lmb/unb 100Mhz clock measurement

EMM_DEFAULT_BIOS_SETTINGS

Enable XptPrefetchEn:

UPI.XptPrefetchEn changed from 0 (DISABLE) to 2 (AUTO) – AUTO results in ENABLE.

Resolved issues

- **CPU Purley Board (CPB) Firmware Update**

  It is now possible to update the firmware of the CPB board using the BSM CLI commands.

- **Repartitioning a two four-module partitioned system**

  It is now possible to repartition a four-module partition that is powered off without having to power off the other four-module partition.

6.3.4. TS 014.01 (April 2019)

First delivery