BullSequana Edge

Getting Started Guide

86 A1 07FS 03 - July 2020

Atos

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

July 2020

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

Table of Contents

Preface

This guide explains how to set up the server.

See The Bull support web site for the most up-to-date product information, documentation, firmware updates, software fixes and service offers: http://support.bull.com

Important **ATTENTION: Please read carefully the safety instructions before you perform the procedures described in this manual.**
Multilingual Safety Notices Guide

Intended Readers

This guide is intended for use by administrators and operators

Chapter 1. Accessing the server for the first time

Important **The steps in this chapter must be followed in the order indicated.**

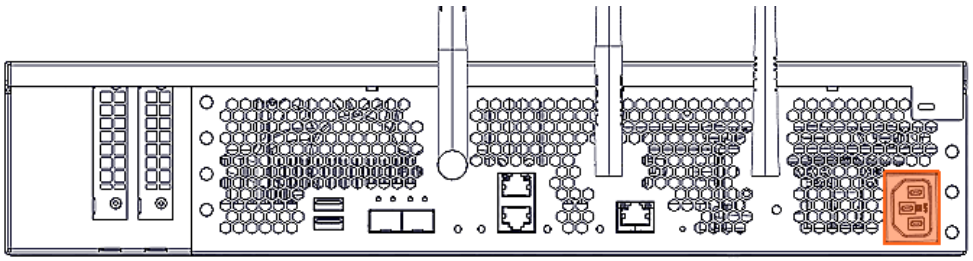
See The Installation Guide and the documentation included in the documentation portfolio for more information.

1.1. Connecting the server to the power supply

Important **The site power breaker must be OFF when the server is connected to the power supply. The site power supply must remain OFF until the system is ready to be powered on.**

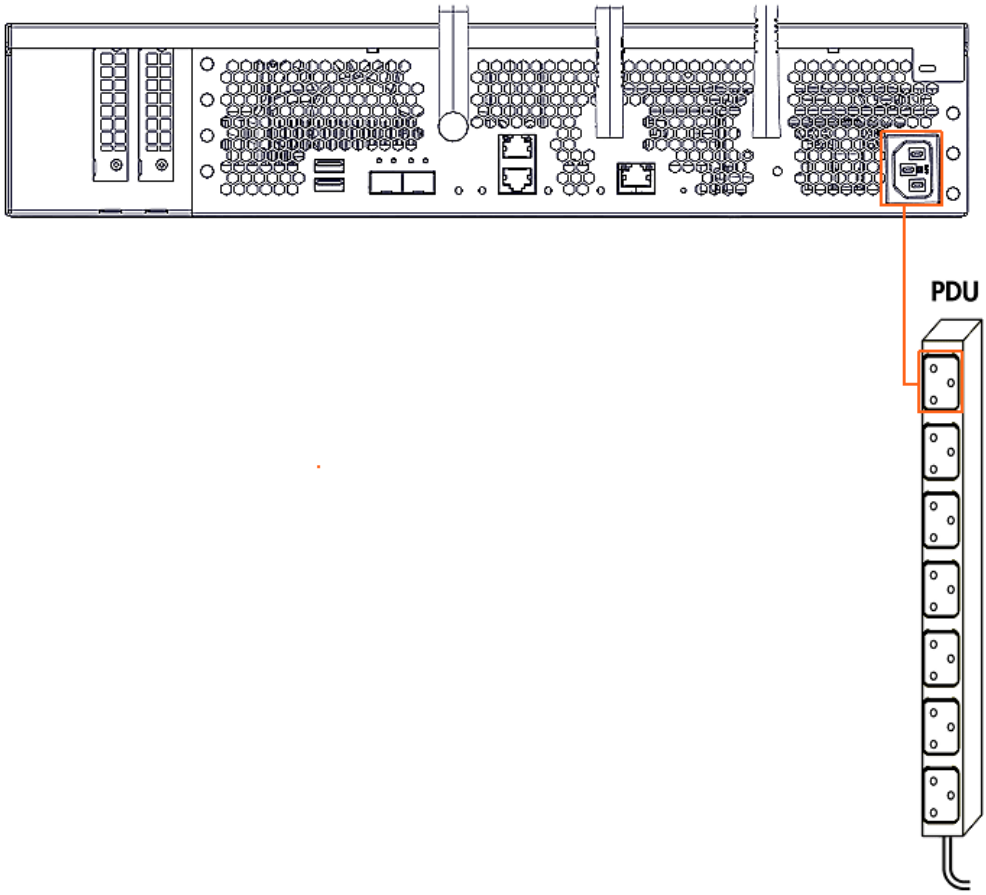
1. Locate the power supply connection.

Rear view



2. Connect the server to the power supply.
   - If the server is installed in a rack cabinet:
     i. Route the power cable along the cabinet flange to the PDU.
     ii. Plug the power cable into the required PDU.
   - For any other installation, plug the power cable into the required PDU.

Rear view

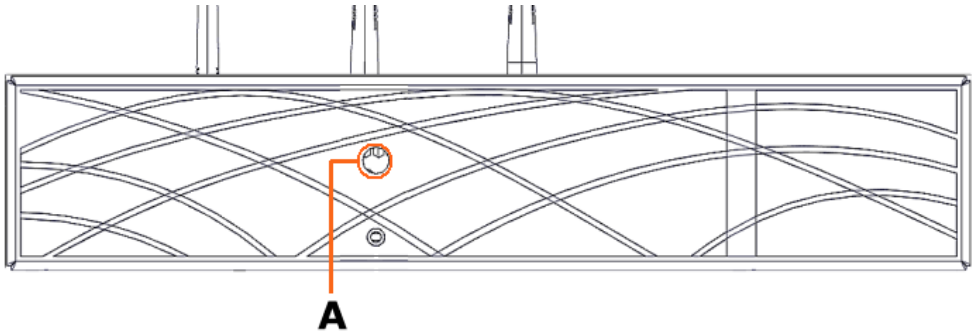


1.2. Placing the server in standby mode

Note Standby mode means that the power supply for the server is connected but not powered on. The BMC is ON but the Operating System is not launched.

1. Turn the site power breakers ON.
2. Check that the power status LED (A) blinks green to indicate that the server is in standby mode.

Front view



1.3. Connecting to the Baseboard Management Controller (BMC)

The server BMC is accessed using an IP address from the Server Hardware Console (SHC).

There are three different methods of obtaining an IP address for the server BMC:

- Directly using an auto-discovery tool
- Via a DHCP server installed on a laptop
- Via a network DHCP server

Note By default, BullSequana Edge servers are preconfigured for dynamic IP addresses.

1.3.1. Obtaining an IP address directly with an auto-discovery tool

Important **BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.**

BullSequana Edge servers support Automatic Private IP Addressing (**APIPA**). An IP address in the 169.254.xxx.xxx range will be allocated automatically, when the BMC is connected to a network without a DHCP server.

Prerequistes

A windows laptop with internet access and administrator rights

An auto-discovery tool for the IP address

The server is in standby power mode

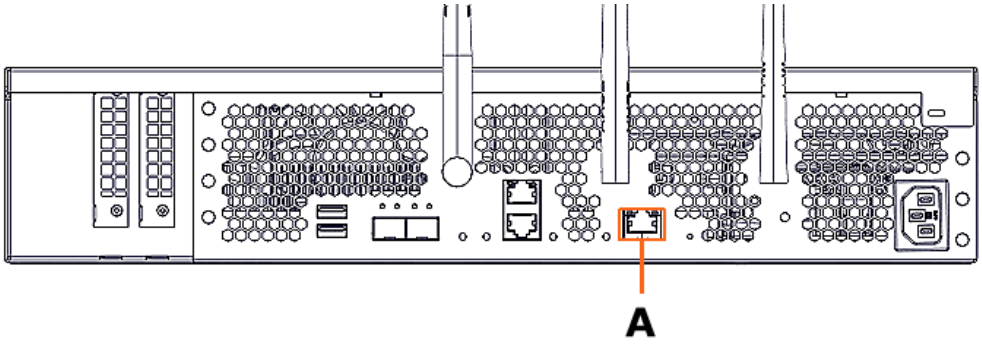
Procedure

Note In this section the Bonjour browser is used as an example of an IP address auto-discovery tool.

1. **Install Bonjour on the laptop**
   1. Download the latest **BonjourBrowserSetup.exe** file.
   2. Run **BonjourBrowserSetup.exe** with administrator rights.

2. Connect the server directly to the laptop

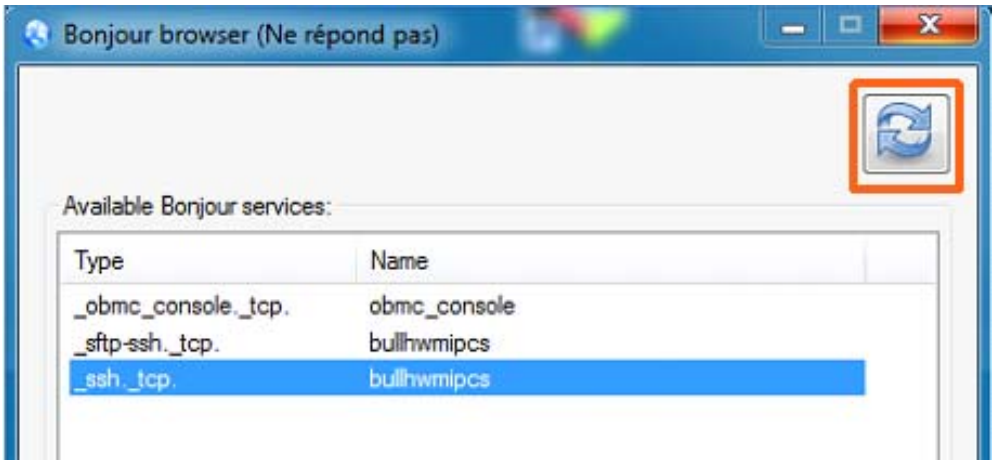
Connect the BMC port (A) of the server to the laptop computer using a RJ45 Ethernet cable.



3. Launch the Bonjour browser on the laptop

4. Refresh the Bonjour browser

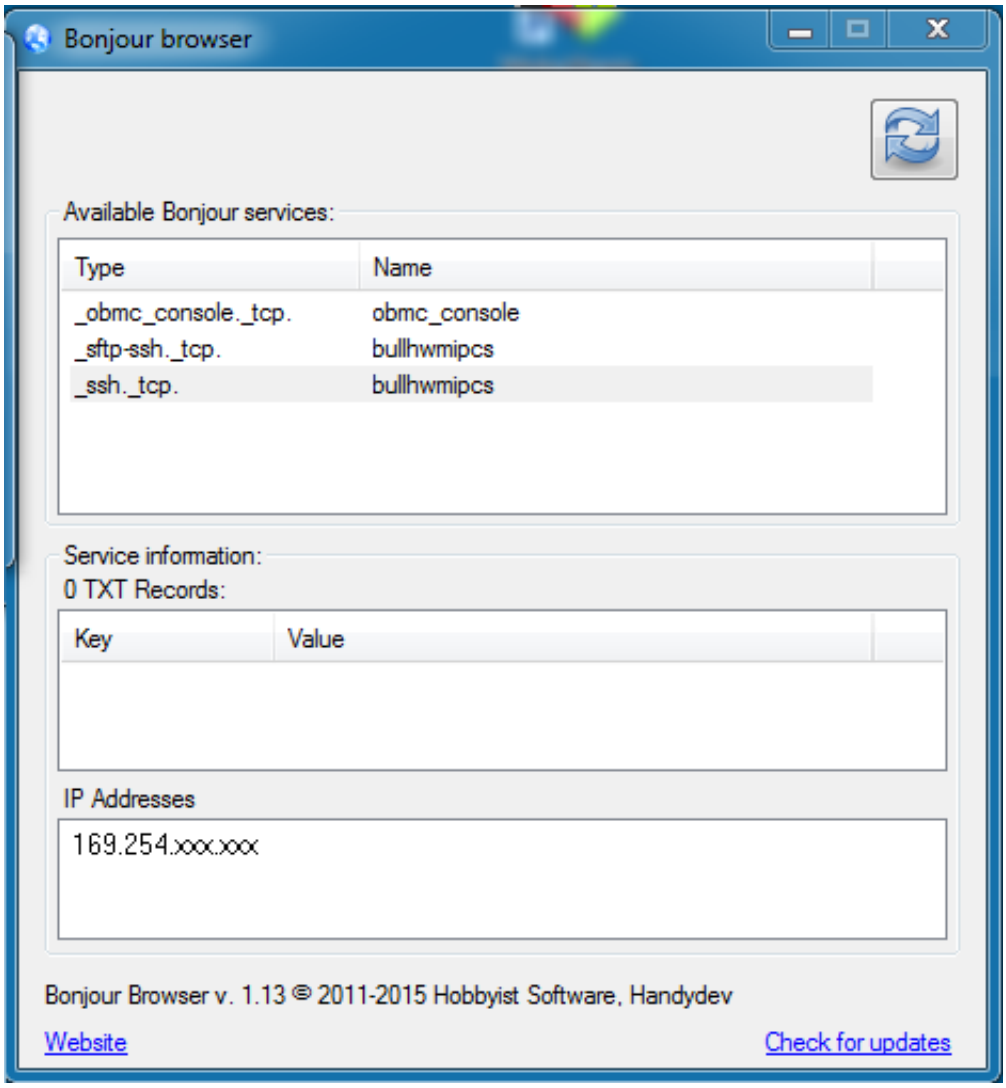
1. Click the Refresh button at the top on right of the browser window.



2. The available services are displayed.

5. Note the server IP address

1. Select the **_ssh._tcp** Bonjour service for the server BMC.
2. The Bonjour IP BullSequana Edge server IP address is displayed in the **IP Addresses** field.



3. Note the IP address indicated.

1.3.2. Obtaining an IP address via a laptop DHCP server

Important **BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.**

Prerequistes

A windows laptop computer with internet access and administrator rights

A DHCP server is installed on the laptop

The server is powered off and disconnected from the power supply

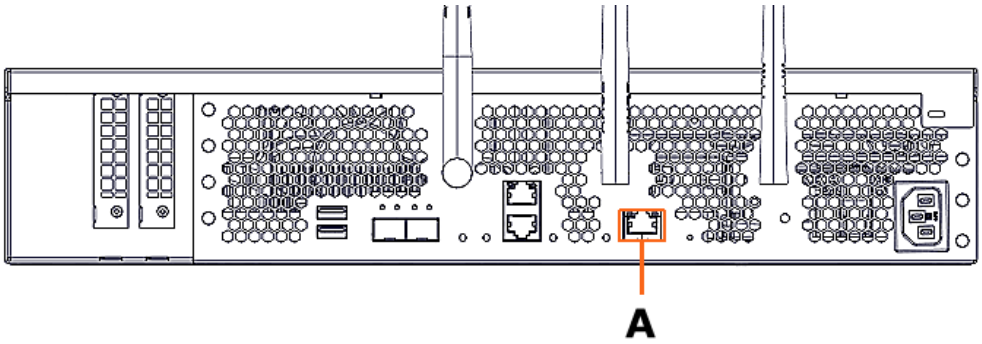
Note In this section Tftpd64 is used as an example of DHCP server installed locally on a laptop.

Procedure

1. **Install Tftpd64 on the laptop**
   1. Download the latest **Tftd64.exe** file.
   2. Run **Tftd64.exe** with administrator rights.

2. **Connect the server to the laptop**

   Connect the BMC port (A) of the server to the laptop using a RJ45 Ethernet cable.



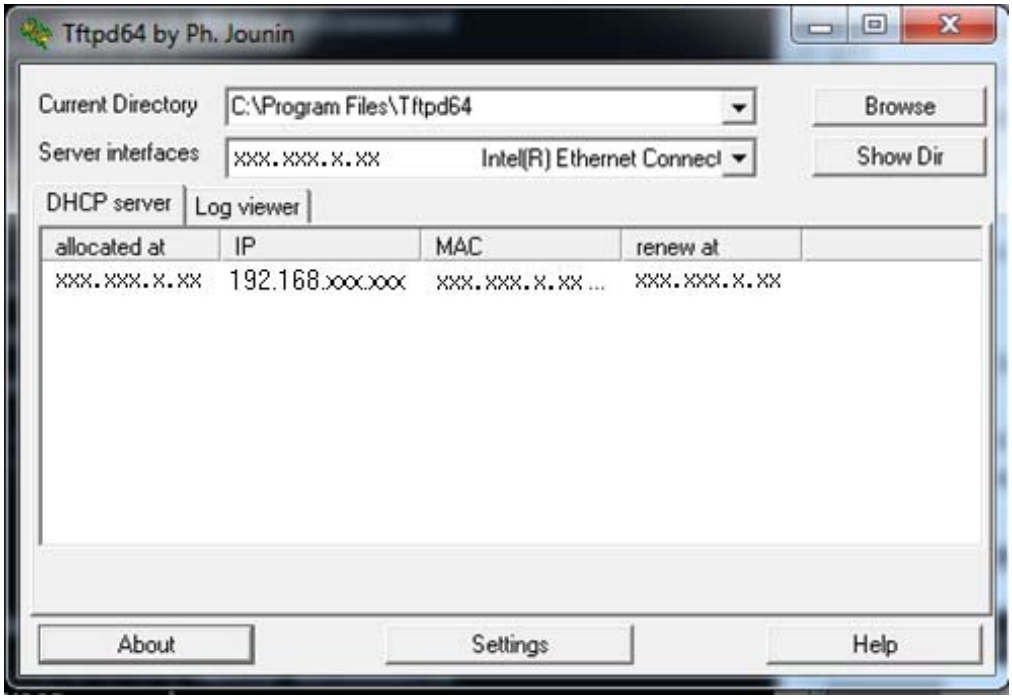
3. **Connect the server power cable to the power socket**

4. **Wait for the BMC to boot**

Note The BMC boot will take several minutes.

5. **Launch the DHCP server on the laptop**

Note The TFTPD64 DHCP server interface below is shown as an example.



6. **Note the BMC IP address indicated**

1.3.3. Obtaining an IP address via a network DHCP server

Important **BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.**

Prerequistes

A laptop computer with administrator rights

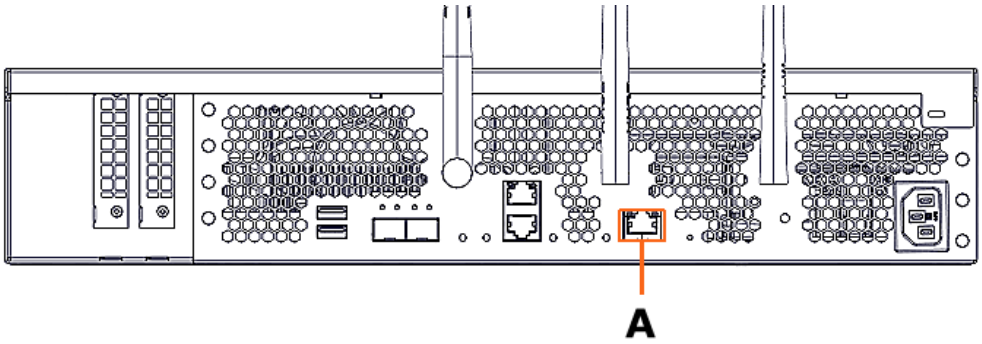
The server is in standby power mode

The LAN includes a DHCP server

Procedure

1. **Connect the server to a switch**

   Connect the BMC port (A) of the server to a 1 Gb/s Ethernet switch using a RJ45 Ethernet cable.



2. **Connect the switch to the laptop**

   Connect an Ethernet port of the laptop to the 1 Gb/s Ethernet switch using a RJ45 Ethernet cable.

3. **Connect the switch to the LAN**

   Connect the 1 Gb/s Ethernet switch using a RJ45 Ethernet cable to the LAN either via a router or directly.

4. **Access the DHCP server that is part of the LAN**

   Retrieve the IP address from the DHCP server table.

5. **Note the IP address allocated to the server BMC**

1.4. Connecting to the Server Hardware Console (SHC)

Important **The https protocol must always be used to connect to the SHC.**

See The SHC Reference Guide for more information.

Prerequistes

A laptop is connected to the server

A Chrome or Firefox browser is installed on the laptop

The server BMC has an IP address allocated

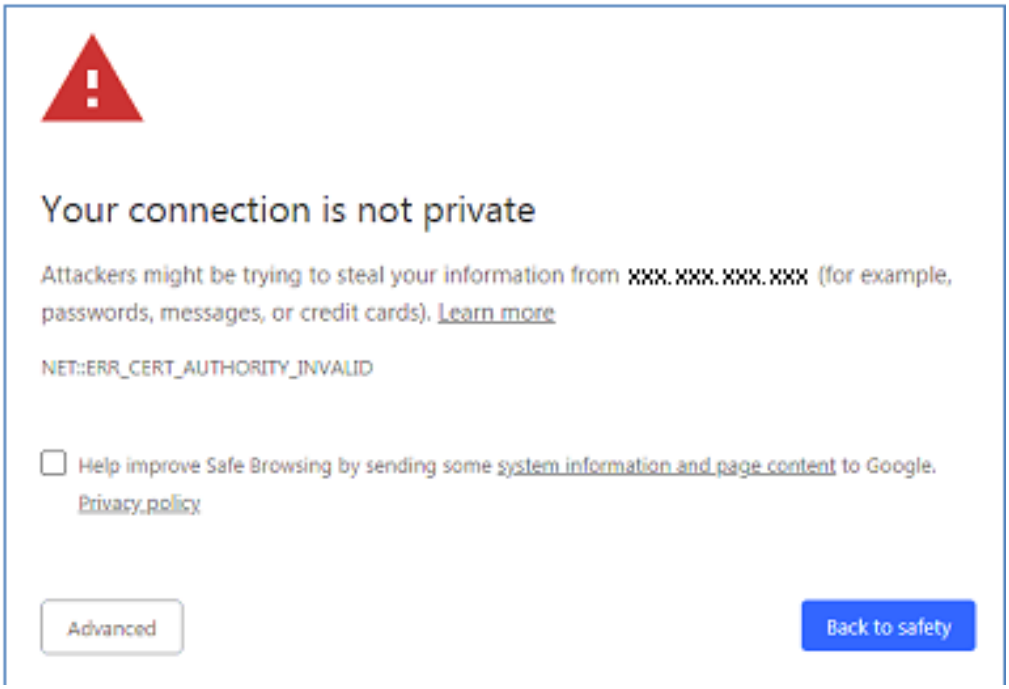
Procedure

1. **Enter the BMC IP address into the web browser address bar using the https protocol**

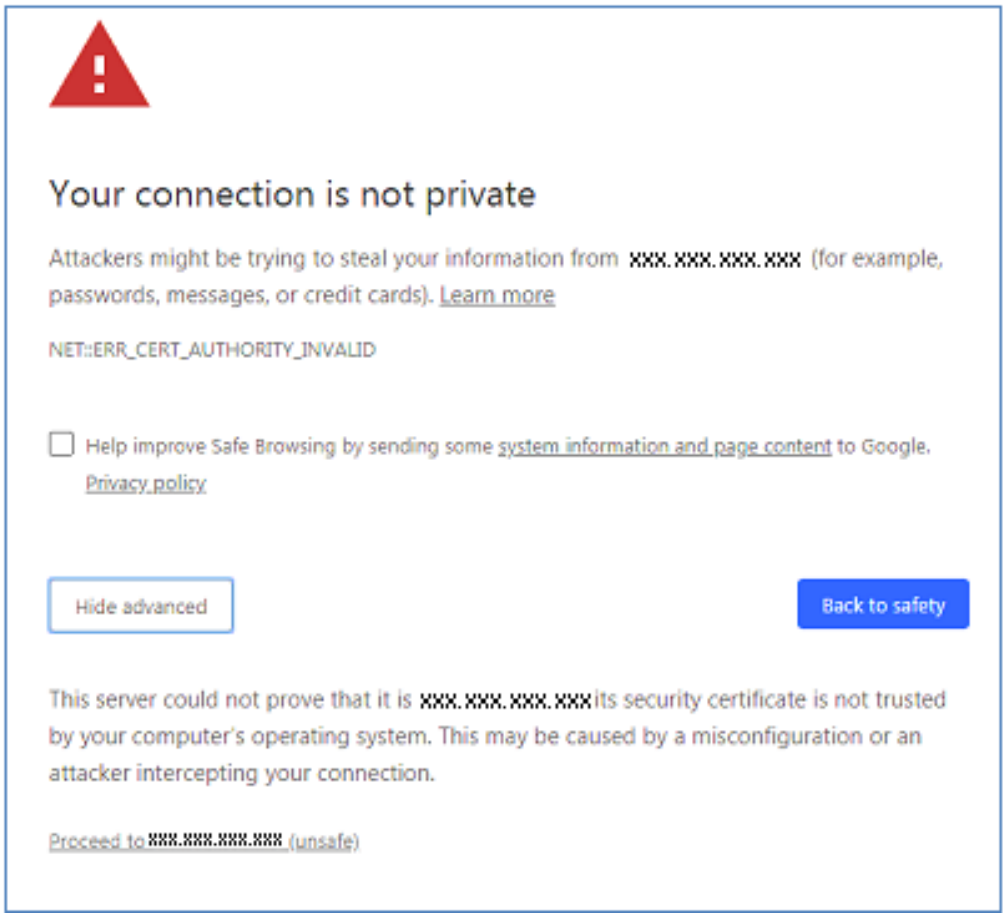
   Note The BMC IP address allocated will be in the https://192.168.xxx.xxx or the https://169.254.xxx.xxx ranges.

2. **Ignore any security warning messages**

   1. The following screens are displayed for the first connection with the Chrome browser.



2. Click **Advanced.**



3. Click **Proceed to XXX.XXX.XXX.XXX**
4. The Server Hardware Console (SHC) authentication page opens.

1.5. Logging in to the Server Hardware Console (SHC)

Prerequistes

A laptop is connected to the server

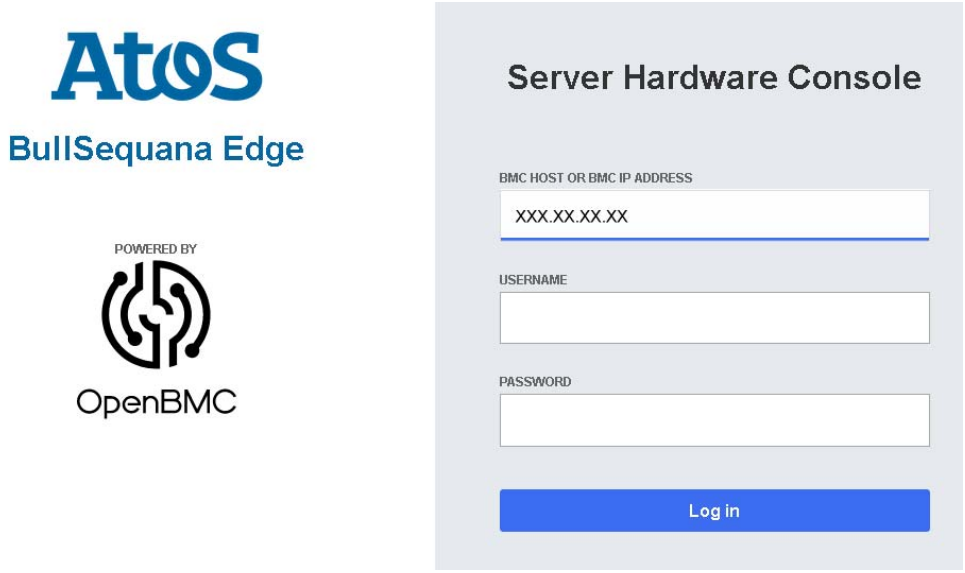
A Chrome or Firefox browser is installed on the laptop

The BMC has an IP address allocated

Procedure

1. **Connect to the SHC**

   The Server Hardware Console (SHC) authentication page opens.



Server Hardware Console (SHC)	
Username	admin
Password	pass

2. **Complete the Username and Password fields and click Log in.**

Important	**It is strongly recommended to change the default user password once initial setup is completed, taking care to record the new account details for subsequent connections.**

Chapter 2. Installing an Operating System

2.1. Powering on the server from the SHC

Important **The https protocol must always be used to connect to the SHC.**

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

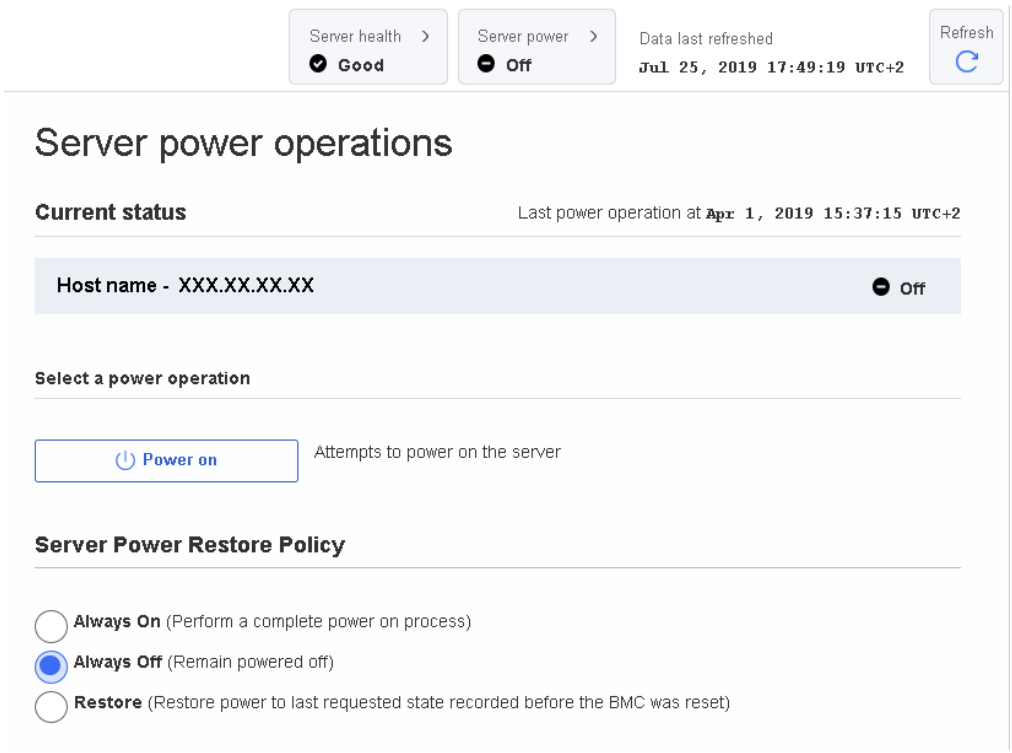
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in standby power mode

Procedure

1. Connect to the SHC
2. From the **Server control** tab, click **Server power operations**. The **Server power operations** page opens.



3. Click **Power on**.

2.2. Operating system installation options

2.2.1. Using a bootable USB drive

Prerequisites

Access to the SHC is in place

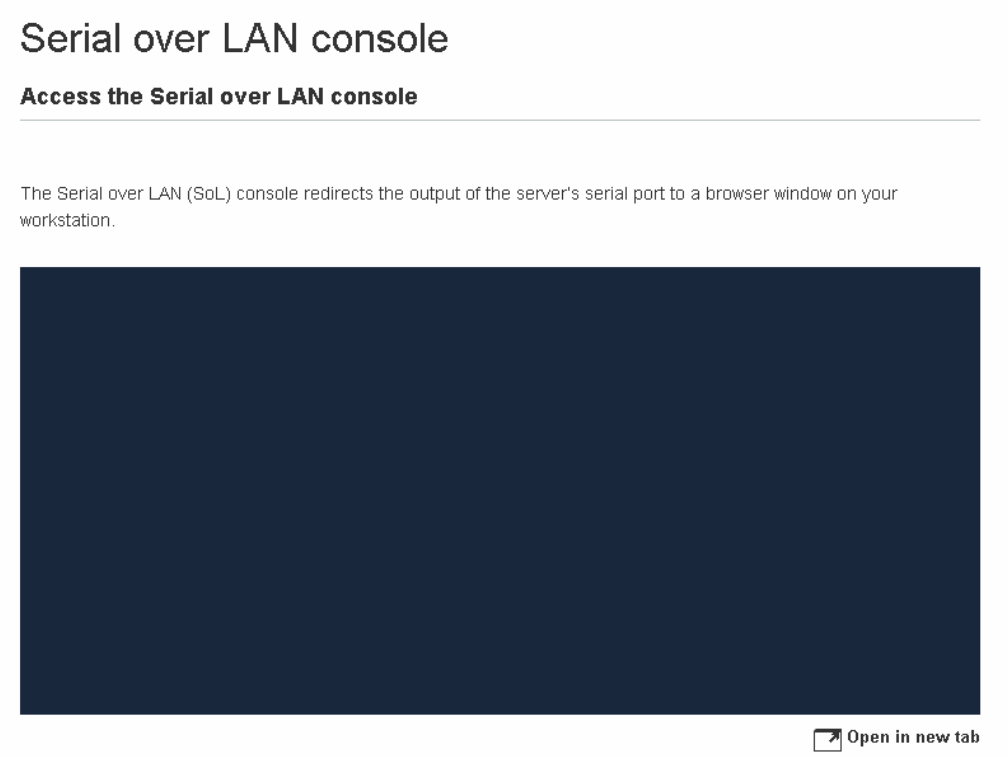
The server is powered on

A bootable USB drive with the OS to be installed is plugged into the server

Note It is recommended that the latest version of the **Rufus** tool is used to format and create the bootable USB drive.

Procedure

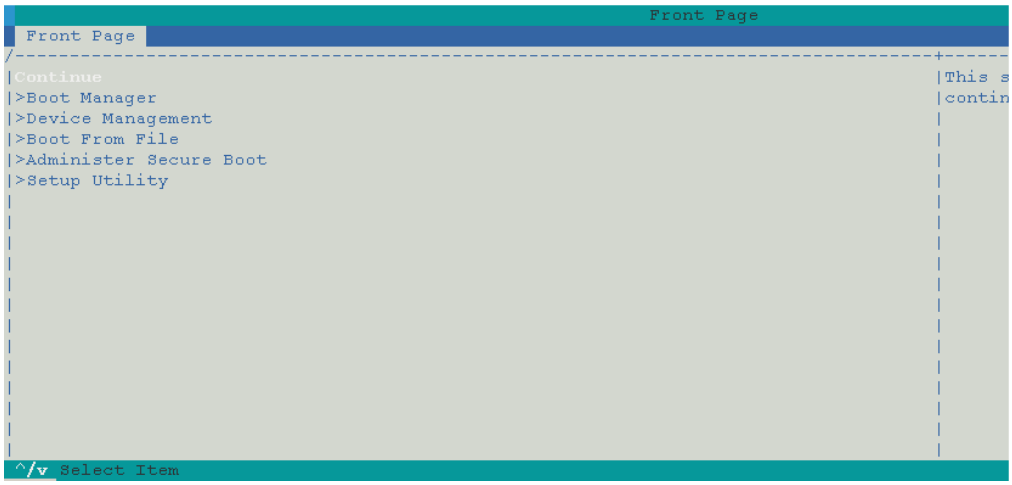
1. **Access the BIOS interface from the SHC**
   1. From the **Server control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.



   2. If required, click the **Open in new tab** link to open the console in a new window.

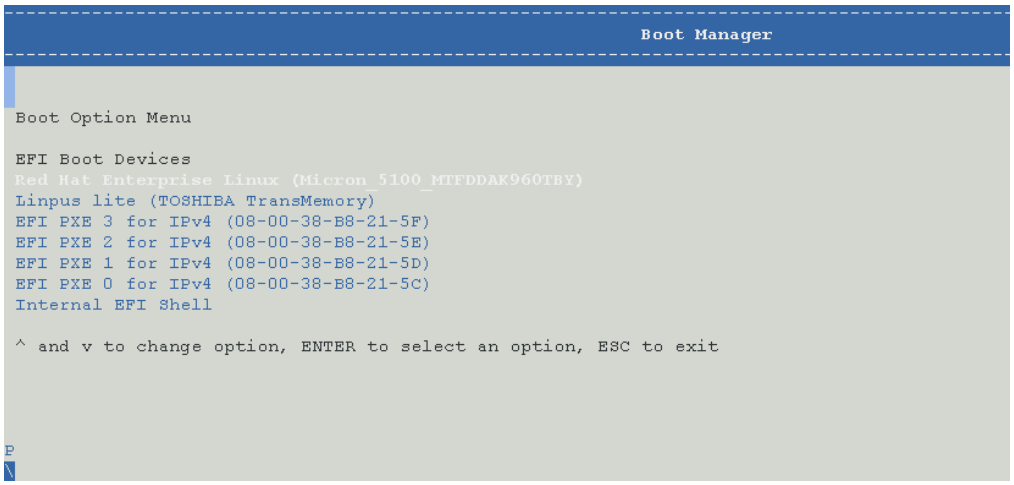
3. Click on the Serial over LAN console screen and quickly press the [Esc] key numerous times to display the BIOS interface.

Important **The [Esc] key must be pressed quickly after the Serial over LAN console window opens.**



2. Choose the boot device

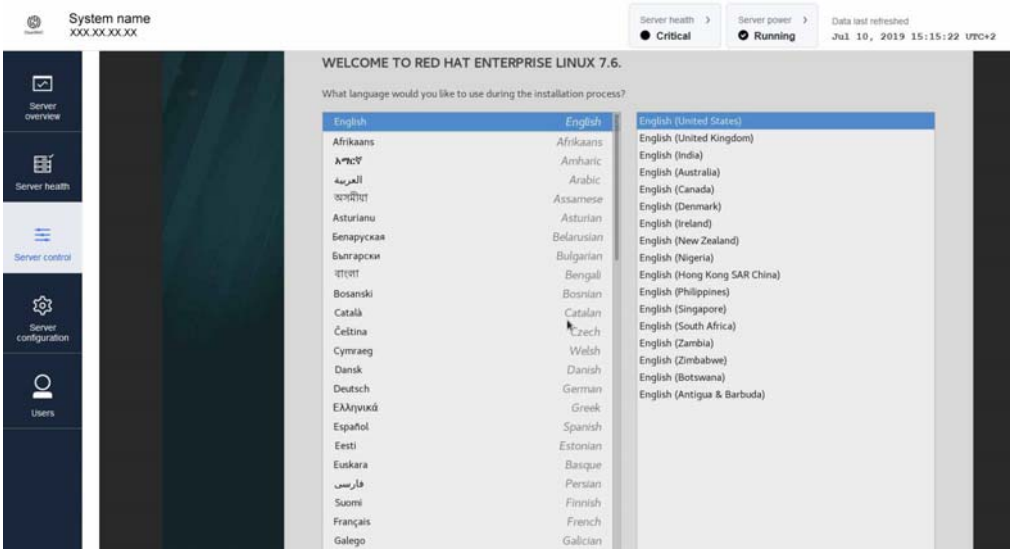
1. Select **Boot Manager** using the navigation arrows and press [Enter].
2. Select the USB drive boot device using the navigation arrows and press [Enter].



3. Follow the instructions displayed to boot from the USB drive.

3. Install the OS

1. Click **Server contro**l > **KVM**. The KVM page opens.



2. Follow the instructions displayed to install the OS.
3. Select the system settings required.

2.2.2. Using a Pre-boot eXecution Environment (PXE)

Prerequisites

Access to the SHC is in place

The server is powered on

A PXE server has been set up and is accessible

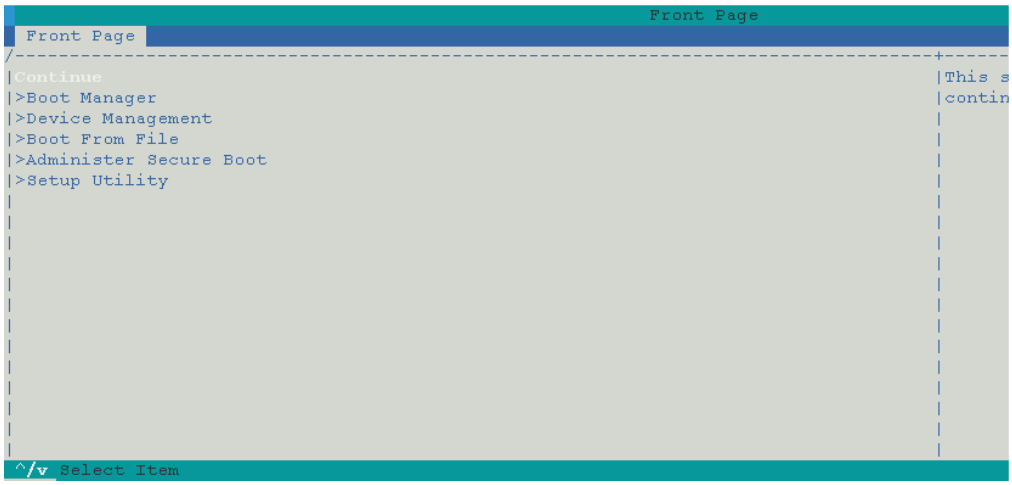
Procedure

1. **Access the BIOS interface from the SHC**
   1. From the **Server control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.

   2. If required, click the **Open in new tab** link to open the console in a new window.

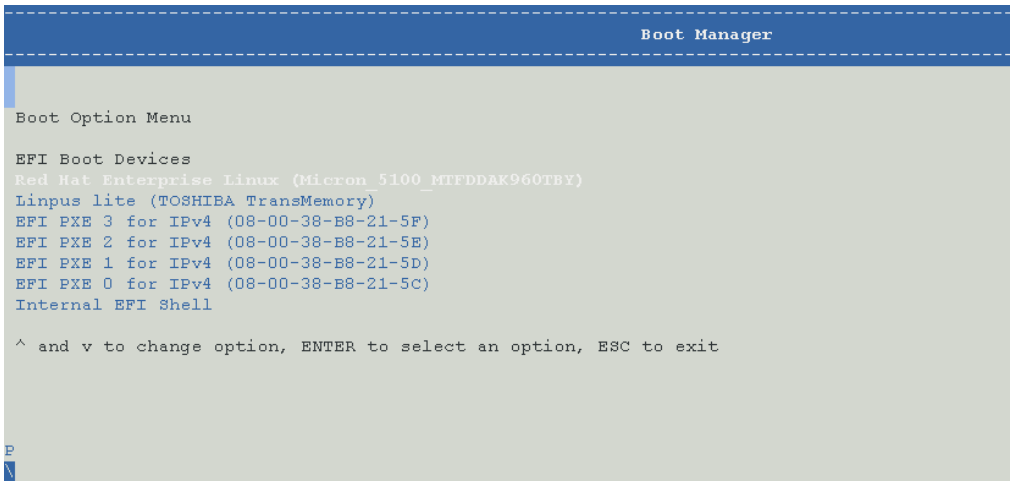
3. Click on the Serial over LAN console screen and quickly press the [Esc] key numerous times to display the BIOS interface.

Important **The [Esc] key must be pressed quickly after the Serial over LAN console window opens.**



2. Choose the boot device

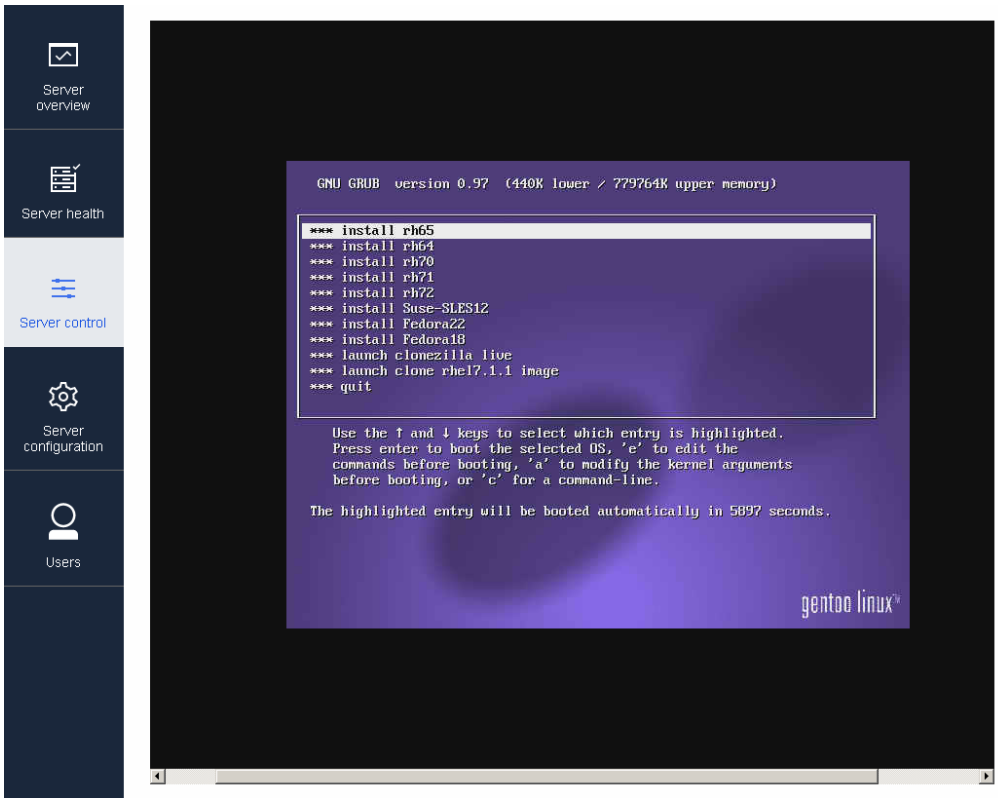
1. Select **Boot Manager** using the navigation arrows and press [Enter].
2. Select the PXE boot device using the navigation arrows and press [Enter].



3. Follow the instructions displayed on the screen to boot the OS from the PXE server.

3. Install the OS

1. Click **Server control** > **KVM**. The KVM page opens.



2. Follow the instructions displayed to install the OS.
3. Select the system settings required.

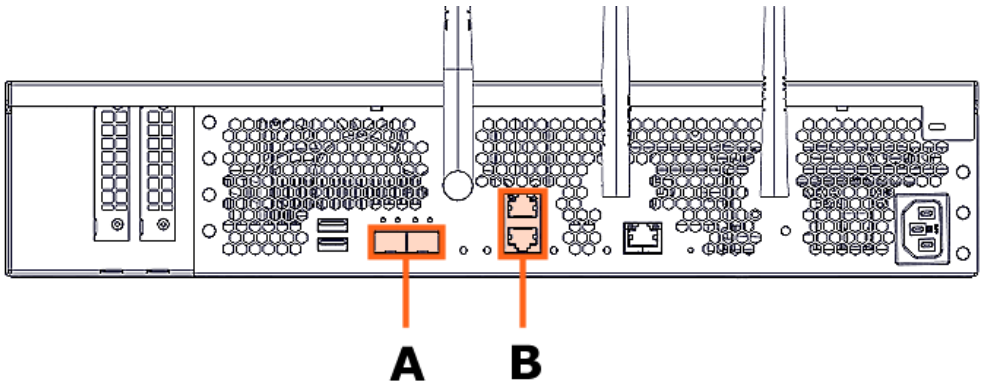
Chapter 3. Connecting to the data system

3.1. Connecting the server to the data LAN

Important **BullSequana Edge servers must be connected to Ethernet switch ports that have a minimum bandwidth of 1 Gb/s.**

1. Connect an Ethernet cable to an Ethernet port at the rear of the server.

Rear view



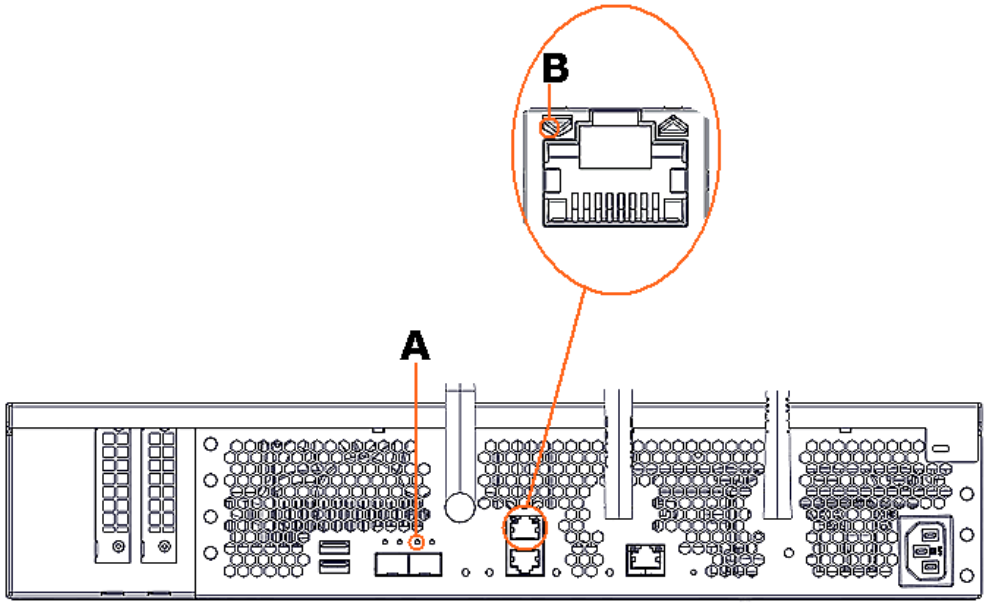
Mark	Port type
A	2 x SFP+ - 10 Gb/s Ethernet
B	2 x RJ45 - 1 Gb/s Ethernet

2. Connect the other end of the cable to the data LAN.

3.2. Checking network traffic

Check that the Ethernet LEDS (A or B) are on for the connected cables.

Rear view



See The Description Guide for more information about the LEDs at the rear of the server.

Chapter 4. Power operations

A BullSequana Edge server can be powered on and off using:

- The power button at the front of the server
- The Server Hardware Console (SHC)
- The Machine Intelligence System Management (MISM) console.

The SHC operates via a server Baseboard Management Controller (BMC) and can only intervene on one server at a time. MISM console jobs can operate on groups of servers at a time.

See The SHC Reference Guide and the Management Console User's Guide for more information.

Notes

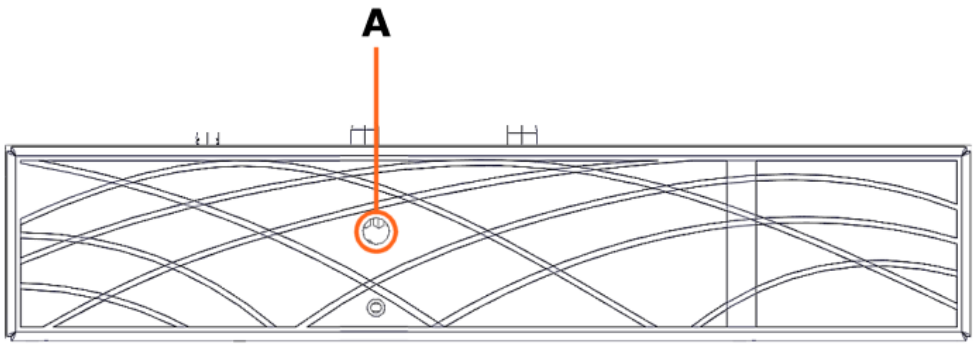
- Standby mode means that the power supply for a server is connected but not powered on. The BMC is ON but the Operating System is not launched.
- Powered on mode means that the power supply for a server is connected and powered on. The BMC is ON and the Operating System is launched.
- By default, the BMC is ON when the power supply is connected to a server.

See Description Guide for more information about the ports and LEDs.

4.1. Powering on with the power button

1. Check that the power status LED (A) is blinking green to indicate that the server is in standby mode.
2. Press the power button at the front of the server (A) for approximately one second.

Front view



3. Check that the power button LED is on and solid green to indicate that the server is powered on.

4.2. Powering on the server from the SHC

Important	**The https protocol must always be used to connect to the SHC.**

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

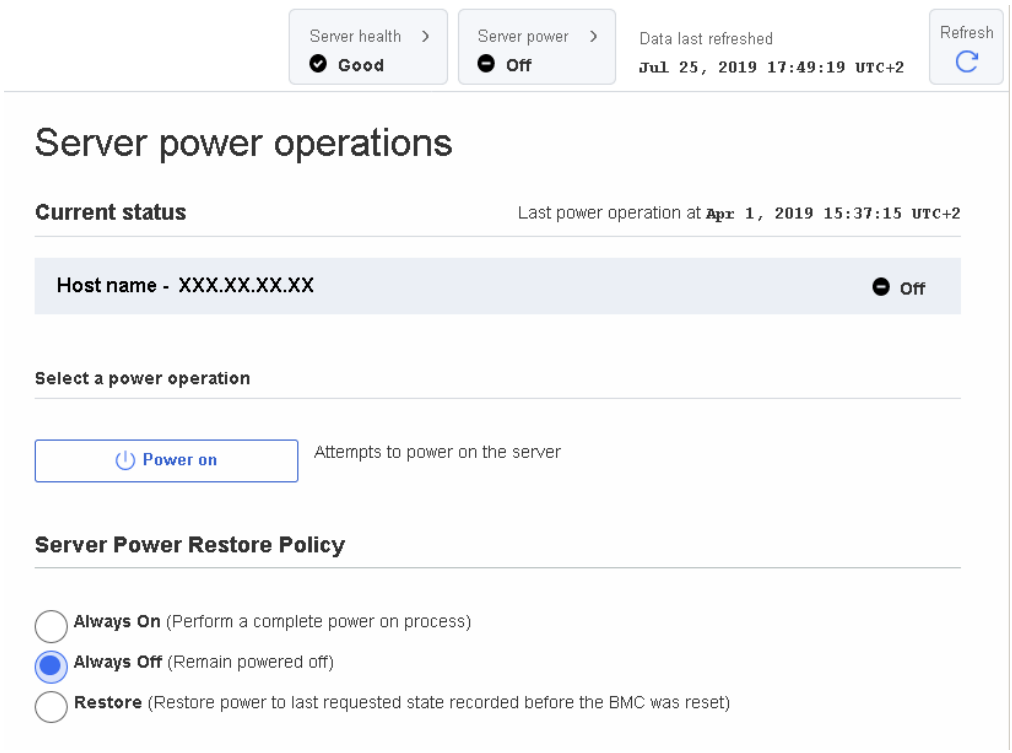
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in standby power mode

Procedure

1. Connect to the SHC
2. From the **Server control** tab, click **Server power operations**. The **Server power operations** page opens.



3. Click **Power on**.

4.3. Powering on the server from the MISM console

Important **The https protocol must always be used to connect to the MISM console.**

Prerequisites

The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in standby power mode

The MISM console is launched

Procedure

1. Launch the **Power On** job.
2. Check that the job status is **Successful**.

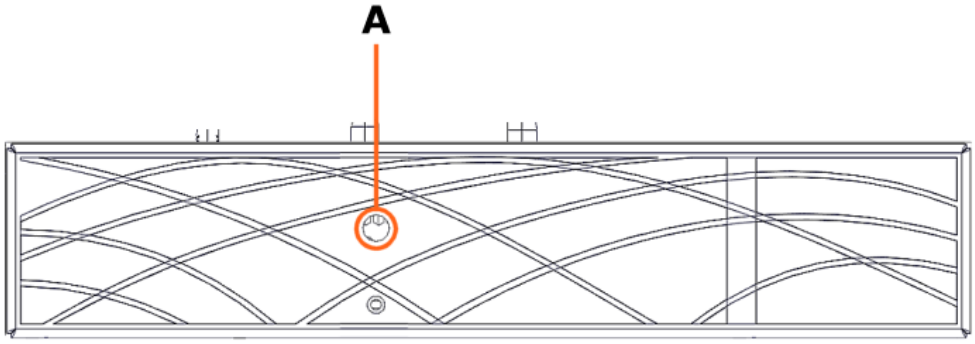
   If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check Power On** job.
4. Check that the job status is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

4.4. Powering off with the power button

1. Check that the power status LED (A) is solid green to indicate that the server is powered on.
2. Press the power button at the front of the server (A) for at least five seconds.

Front view



3. Check that the power button LED is blinking green to indicate that the server is in standby mode.

4.5. Powering off the server from the SHC

W087 **WARNING**
W087:
The Cold reboot and Immediate shutdown buttons should only be used if the Operating System is unable to respond to a Warm reboot or Orderly shutdown request.
These sequences may result in data loss and file corruption.

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

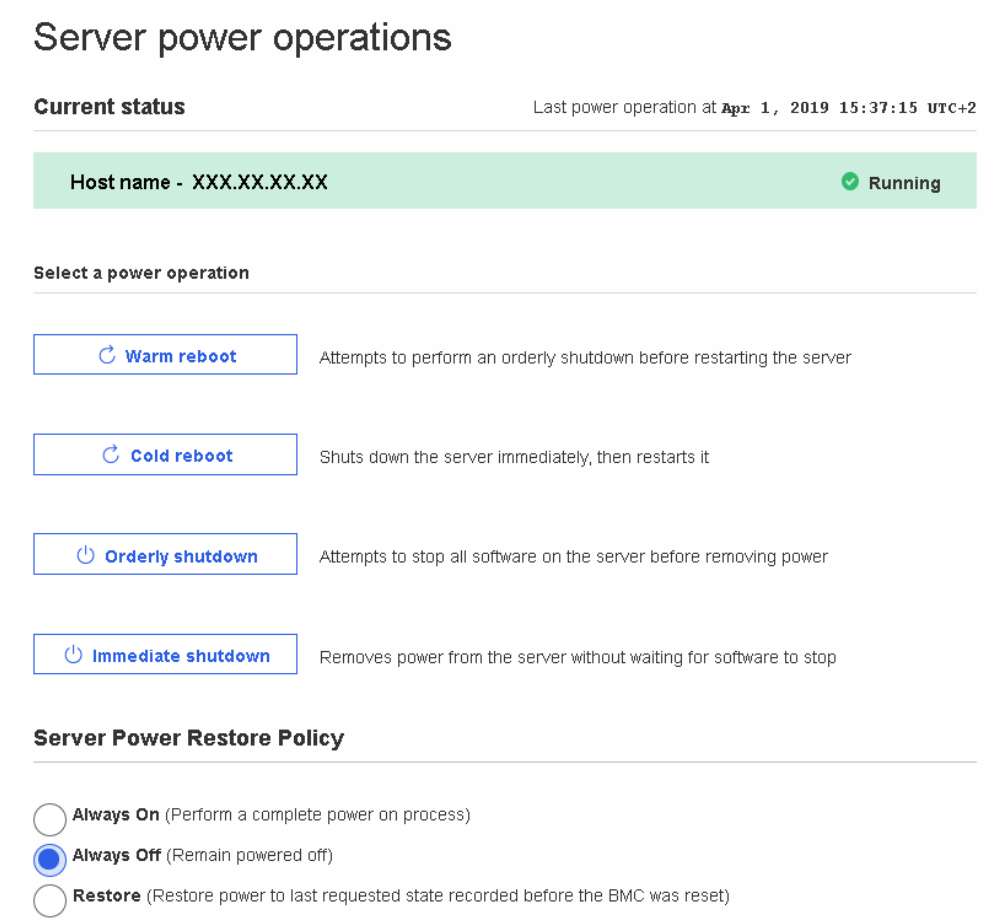
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC
2. From the **Server control** tab, click **Server power operations**. The **Server power operations** page opens.



3. Click the power operation required.

4.6. Powering off the server from the MISM console

W087  **WARNING**

W087:
The Cold reboot and Immediate shutdown buttons should only be used if the Operating System is unable to respond to a Warm reboot or Orderly shutdown request.
These sequences may result in data loss and file corruption.

Prerequisites

The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

The MISM console is launched

Procedure

1. Select the power operation:
   - **Orderly Shutdown**
   - **Immediate Shutdown**
2. Launch the selected job.
3. Check that the job status is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Check Power Off** job.
5. Check that the job status is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

Chapter 5. Server Hardware Console (SHC) maintenance operations

See The SHC Reference Guide for more information.

5.1. Checking the System Event Logs (SELs)

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

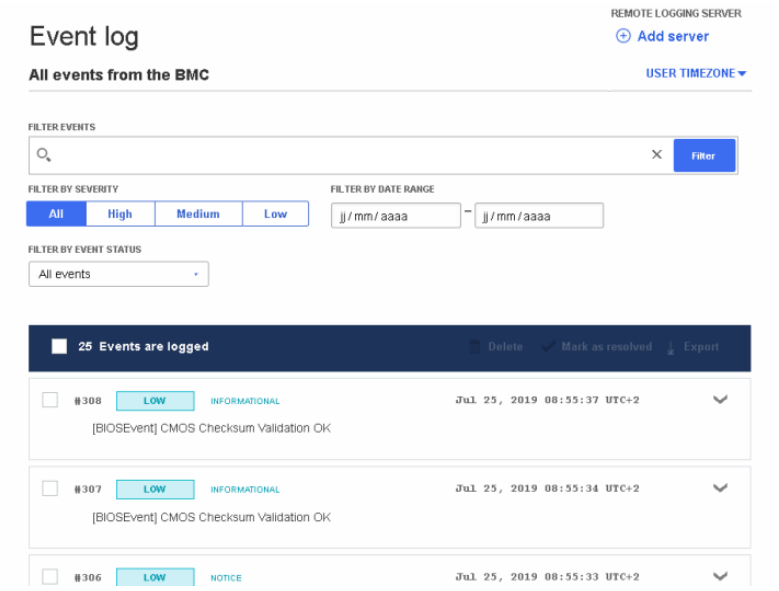
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC
2. From the **Server health** tab, click **Event log**. The **Event log** page opens.



3. Enter the event name or number in the search field.
4. Set the severity, date range and status parameters.
5. Click **Filter**.
6. **Export** the logs, as required.

Note The SELS are exported as .json data files.

5.2. Checking the hardware status

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

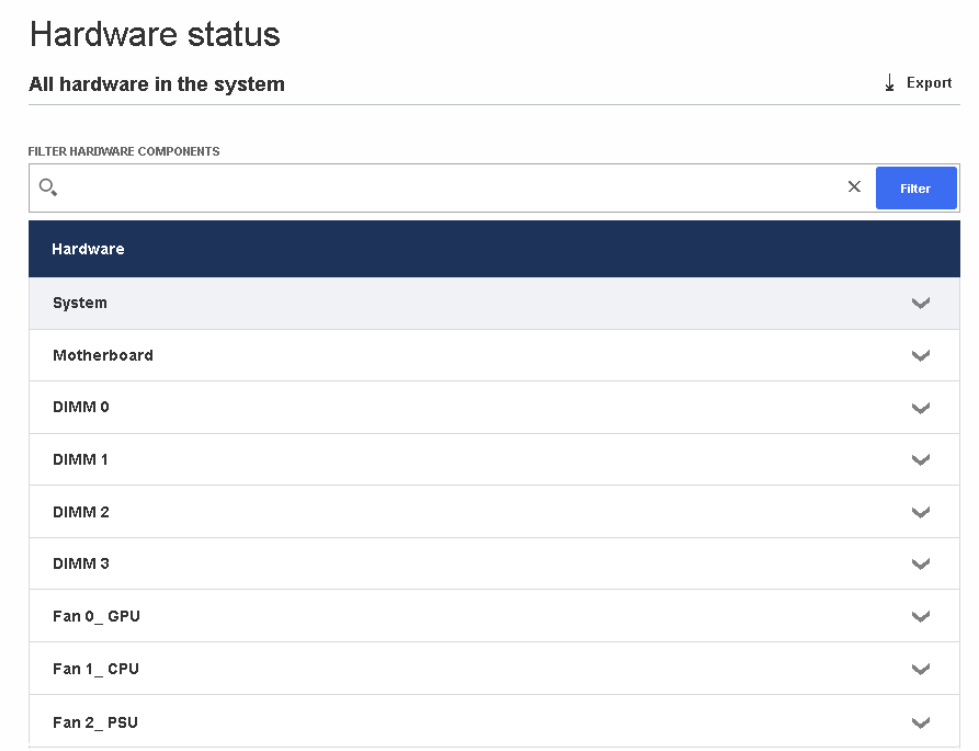
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC
2. From the **Server health** tab, click **Hardware status**. The **Hardware status** page opens.



3. Enter the hardware component in the search field.
4. Click **Filter**.
5. **Export** the hardware details, as required.

Note The hardware details are exported as .json data files.

5.3. Checking the sensors

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

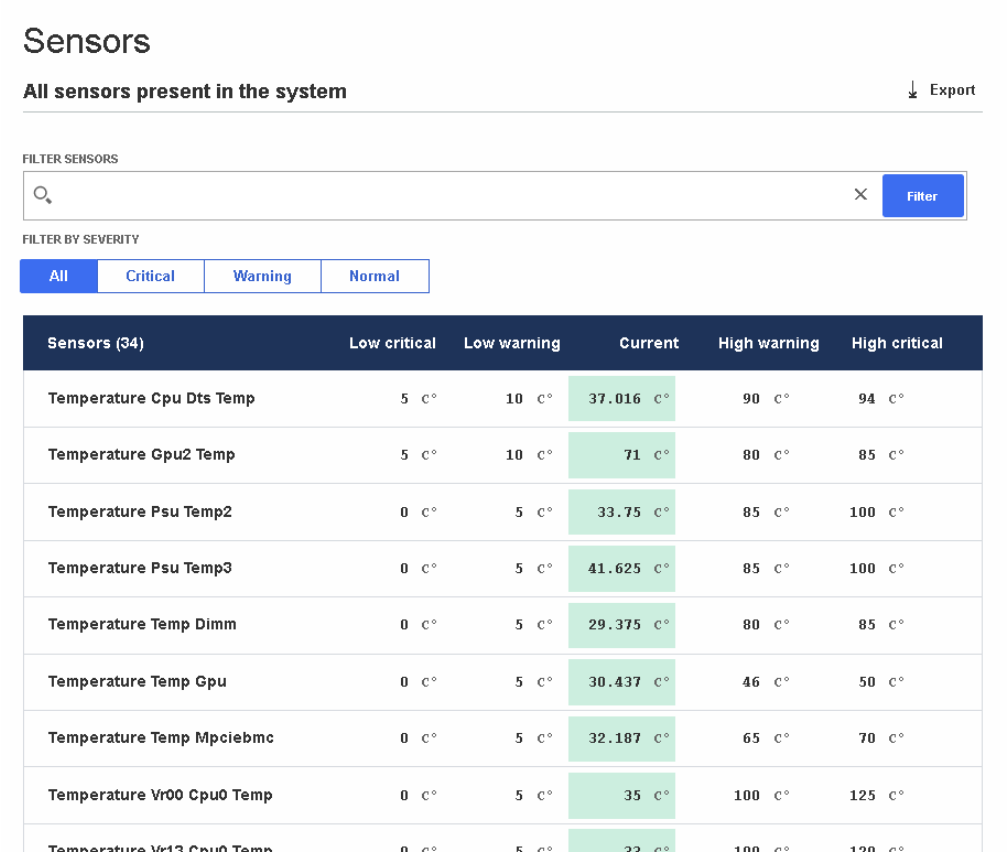
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC
2. From the **Server health** tab, click **Sensors**. The **Sensors** page opens.



Sensors (34)	Low critical	Low warning	Current	High warning	High critical
Temperature Cpu Dts Temp	5 C°	10 C°	37.016 C°	90 C°	94 C°
Temperature Gpu2 Temp	5 C°	10 C°	71 C°	80 C°	85 C°
Temperature Psu Temp2	0 C°	5 C°	33.75 C°	85 C°	100 C°
Temperature Psu Temp3	0 C°	5 C°	41.625 C°	85 C°	100 C°
Temperature Temp Dimm	0 C°	5 C°	29.375 C°	80 C°	85 C°
Temperature Temp Gpu	0 C°	5 C°	30.437 C°	46 C°	50 C°
Temperature Temp Mpciebmc	0 C°	5 C°	32.187 C°	65 C°	70 C°
Temperature Vr00 Cpu0 Temp	0 C°	5 C°	35 C°	100 C°	125 C°
Temperature Vr13 Cpu0 Temp	0 C°	5 C°	33 C°	100 C°	120 C°

3. Enter the sensor name in the search field.
4. Set the severity parameter.
5. Click **Filter**.
6. Use the **Export** option to export the sensor states, as required.

Note The sensor states are exported as .json data files.

5.4. Checking the system logs

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

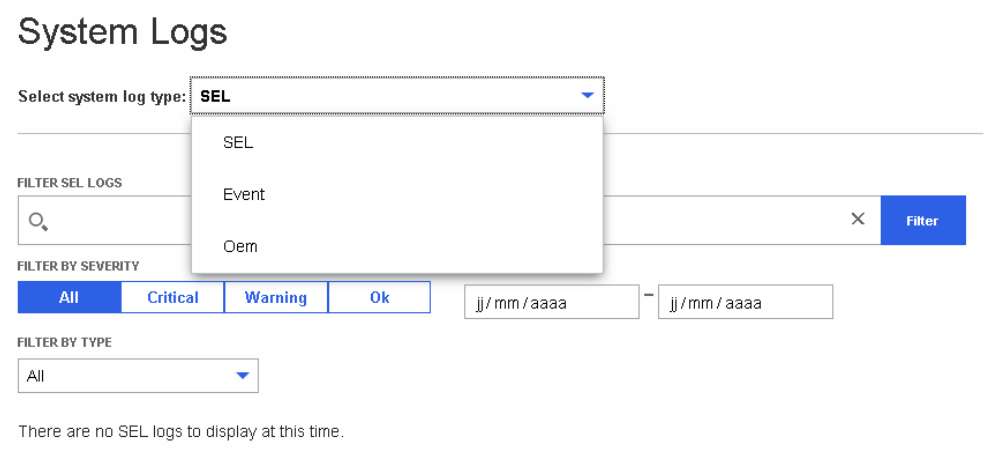
The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC
2. From the **Server health** tab, click **System logs**. The **System logs** page opens.



3. Select the system log type from the drop down list.
4. Set the log name, severity and date range parameters.
5. Click **Filter**.

5.5. Managing firmware versions

Important **The BMC firmware must be updated before the BIOS and CPLD firmware.**

See The Bull support web site for the most up-to-date product information, documentation, firmware updates, software fixes and service offers: http://support.bull.com

The SHC can be used to change firmware boot priorities and to update BMC, BIOS and CPLD firmware files.

5.5.1. Checking firmware versions

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

A laptop is connected to the server BMC port

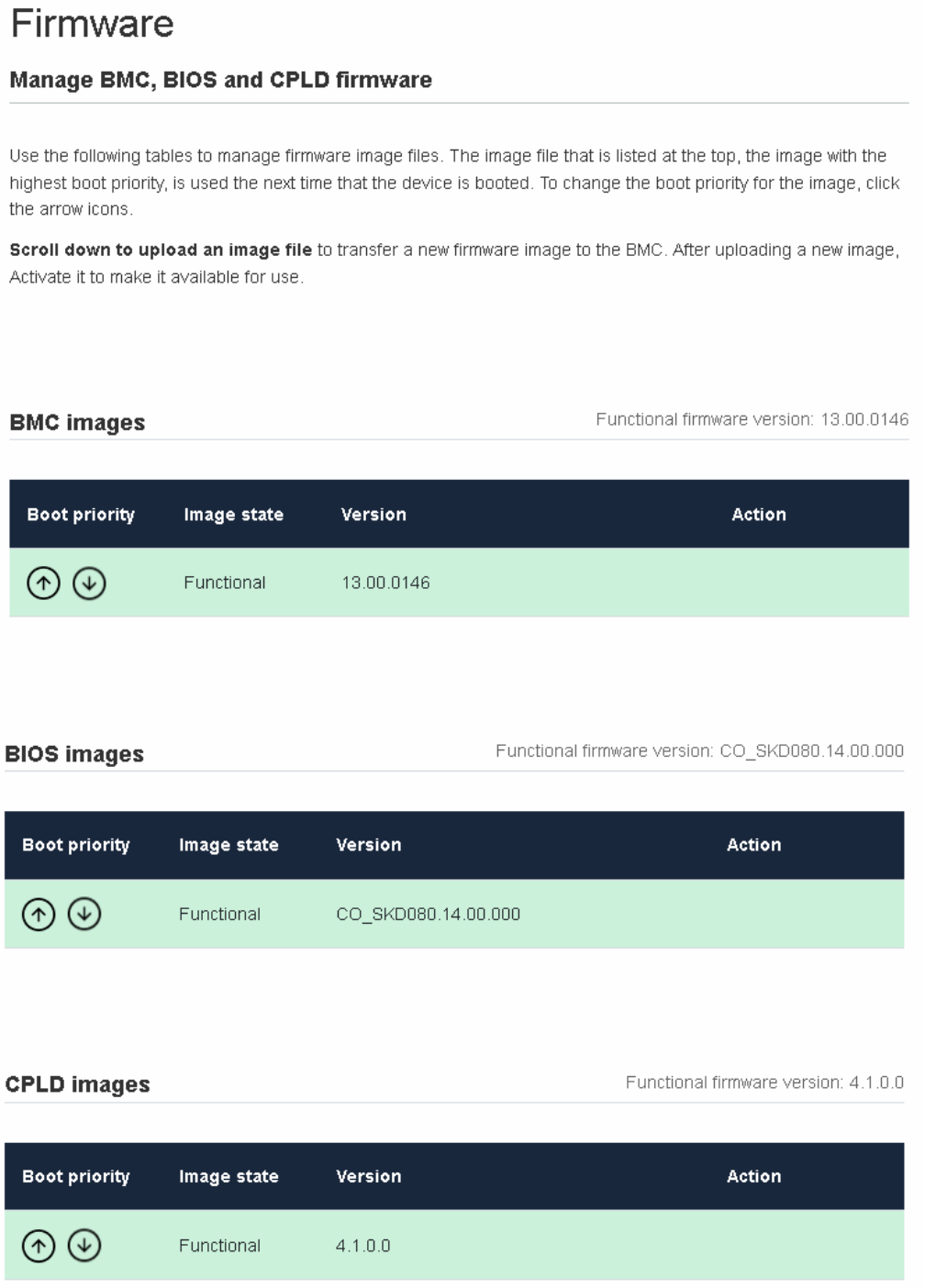
The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. Connect to the SHC

2. From the **Server configuration** tab, click **Firmware**. The **Firmware** page opens.



3. Check the BMC, BIOS and CPLD functional image versions listed.

5.5.2. Updating the BMC firmware

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

A laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the standby power mode

Procedure

1. **Check the server power status**

   Check that the server is in the standy power mode.

2. **Connect to the SHC**

3. **Upgrade the firmware**

   1. From the **Server configuration** tab, click **Firmware**. The **Firmware** page opens.
   2. Specify the new firmware file location.
      a. Either click **Upload firmware** to upload an image file from a workstation.
      b. Or click **Download firmware** to download an image file from a TFTP server.

4. **Activate the new BMC image**

   1. Click **Activate** for the new BMC image.
   2. Confirm the activation with a BMC reboot. Click **Continue**.

Notes
- When the BMC is rebooted the browser loses contact with the BMC for several minutes. The normal log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.
- Earlier firmware versions disappear from the BMC image list once a new version has been activated.

5.5.3. Updating the BIOS and CPLD firmware

Important	**Check that the latest BMC firmware version is installed. If not, the BMC firmware must be updated before the BIOS and CPLD firmware.**

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

A laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in the powered on state

Procedure

1. **Connect to the SHC**

2. **Power off the server**
   1. From the **Server control** tab, click **Server power operations**. The **Server power operations** page opens.
   2. Click **Orderly shutdown.**

3. **Upgrade the firmware**
   1. From the **Server configuration** tab, click **Firmware**. The **Firmware** page opens.
   2. Specify the new firmware file location.
      a. Either click **Upload firmware** to upload an image file from a workstation.
      b. Or click **Download firmware** to download an image file from a TFTP server.

4. **Power on the server**
   1. From the **Server control** tab, click **Server power operations**. The **Server power operations** page opens.
   2. Click **Power on**.
   3. The new firmware is now active.

Chapter 6. MISM maintenance operation

Maintenance operations can be performed from the Machine Intelligence System Management (MISM) console.

See	See the Management Console User's Guide for more information.

6.1. Rebooting Baseboard Management Controllers (BMCs)

Prerequisites

The laptop is connected to the server BMC port

The server BMC has an IP address allocated

The server is in standby power mode

The MISM console is launched

Procedure

1. Launch the **Reboot bmc** job.
2. Check that the job status is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check BMC alive** job.
4. Check that the job status is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

6.2. Updating firmware

Important

- **The BMC must be rebooted after an update of its firmware. If the reboot variable is set as False, it must be done manually for the update to be effective.**
- **The host must be powered off before updating the BIOS or CPLD firmware. If the forceoff variable is set as False, it must be done manually.**

6.2.1. Updating firmware globally

Two-step operation

1. **Review which firmware will be updated**
   1. Launch the **Evaluate firmware update from Technical State** job.

   Note The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

   2. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

2. **Update the firmware**
   1. Launch the **Update firmware from Technical State** job.

   Note The following variables must be indicated as inventory variables or as job extra variables:

   - technical_state_path
   - reboot
   - forceoff

   2. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.
   3. Launch the **Firmware inventory - Active** job to get firmware versions.
   4. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

Three-step operation

1. **Review which firmware will be updated**
   1. Launch the **Evaluate firmware update from Technical State** job to know which firmware will be updated.

   Note The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

   2. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

2. **Upload the firmware**

   1. Launch the **Upload firmware images from Technical State** job.

   Note The path to the Technical State file must be indicated as an inventory variable or as a job extra variable.

   2. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

   3. Launch the **Firmware inventory - Ready** job to get firmware versions.

   4. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

3. **Activate the firmware**

   1. Launch the **Activate firmware updates** job.

   Note The following variables must be indicated as inventory variables or as job extra variables:

   - reboot
   - forceoff

   2. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

   3. Launch the **Firmware inventory - Active** job to get firmware versions.

   4. Check that the job is **Successful**.

      If the job status is **Failed**, check the output of the job in the text window.

6.2.2. Updating firmware individually

1. Launch the **Update firmware from file** job.

Note The following variables must be indicated as inventory variables or as job extra variables:

- reboot
- forceoff
- file_to_update

2. Check that the job is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

3. Launch the **Firmware inventory - Active** job to get firmware versions.

4. Check that the job is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

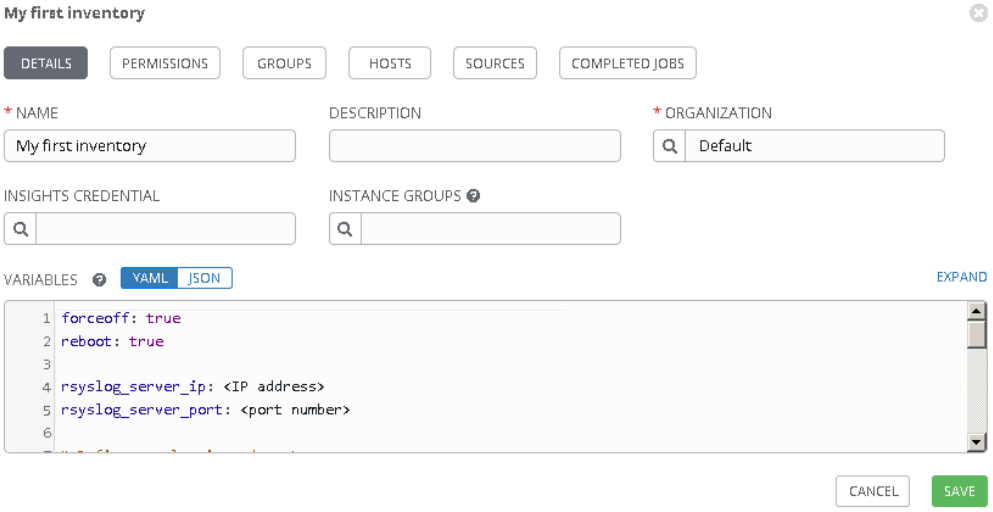
6.3. Enabling syslog forwarding

Prerequisites

The syslog server is configured for messaging

Procedure

1. Indicate the syslog server IP address and port as variables in the inventory.



2. Launch the **Set Rsyslog Server IP** job.
3. Check that the job is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.
4. Launch the **Set Rsyslog Server Port** job.
5. Check that the job is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.
6. Launch the **Check Rsyslog Server IP and Port** job to check the syslog server parameters.
7. Check that the job is **Successful**.

   If the job status is **Failed**, check the output of the job in the text window.

Appendix A. IPMI Out of Band (OOB) support

By default, IPMI OOB support is disabled for the BullSequana Edge server BMC.

A.1. Enabling IPMI OOB support

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

The server BMC has an IP address allocated

A laptop connected to the server

Procedure

1. Connect to the server via **SSH**.
2. Export the BMC credentials:

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

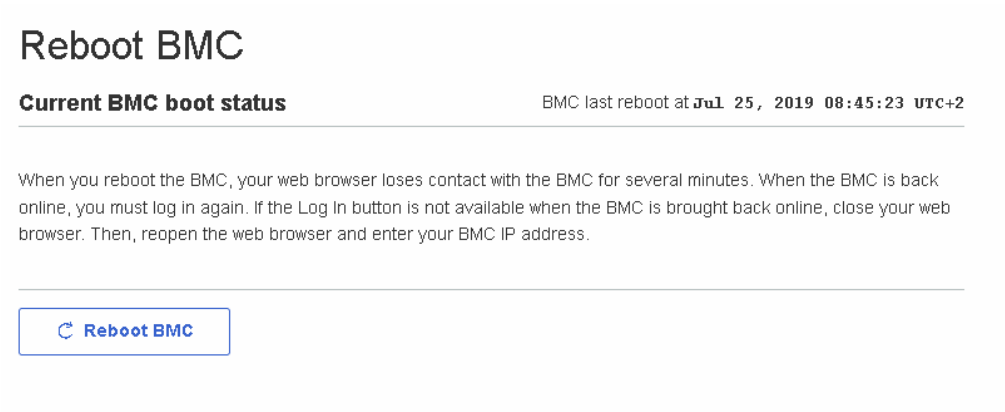
Note Any BMC user account with administrator rights may be used.

3. Reset the BMC to the default factory settings:

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

Note After the BMC reset to the factory settings, only the admin default user account with its default password can be used to connect to the BMC.

4. Connect to the SHC.
5. From the **Server control** tab, click **Reboot BMC**. The **Reboot BMC** page opens.



6. Click the **Reboot BMC** button.

Note When the BMC is rebooted the browser loses contact with the BMC for several minutes. The log in procedure must be performed when the BMC is back online. If the log in button is not available, close the browser, reopen it and enter the BMC IP address.

7. Enable IPMI OOB support:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X PUT -d '{"data": "true"}'
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

8. Check that IPMI OOB support is enabled:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X GET
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

IPMITOOL commands can now be used to manage the server.

A.2. Disabling IPMI OOB support

Prerequisites

A laptop computer with the Chrome or Firefox browser installed

The server BMC has an IP address allocated

A laptop connected to the server

Procedure

1. Connect to the server via **SSH**.
2. Export the BMC credentials:

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

Note Any BMC user account with administrator rights may be used.

3. Disable IPMI OOB support:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X PUT -d '{"data": "false"}'
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

4. Check that IPMI OOB support is disabled:

```
curl -c cjar -b cjar -k -H "Content-Type: application/json" -X GET
https://${bmc}/xyz/openbmc_project/ipmi/support/attr/Functional
```

IPMITOOL commands can no longer be used to manage the server.

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