BullSequana Edge

Getting Started Guide

86 A1 07FS 07 - July 2022

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 2022

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.**

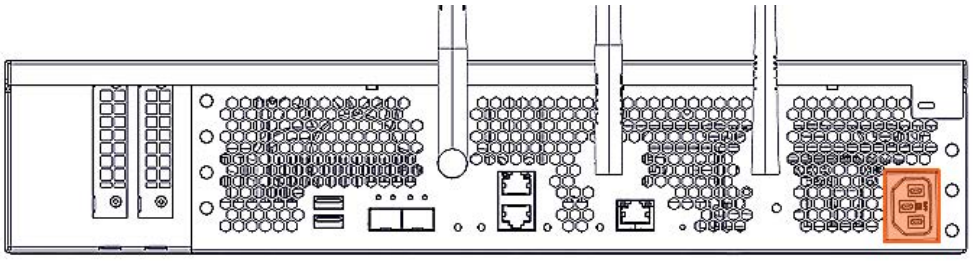
See The Installation Guide and the documentation set for more information.

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.**

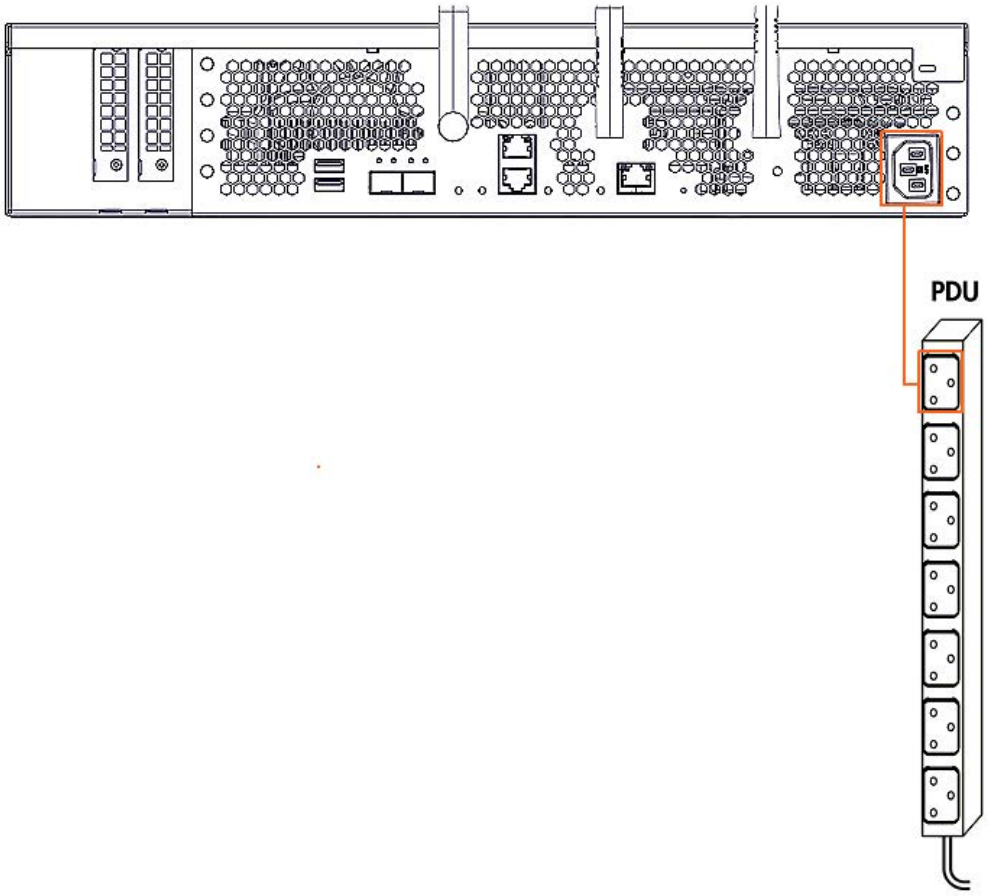
1. Locate the power supply connection.

Rear view



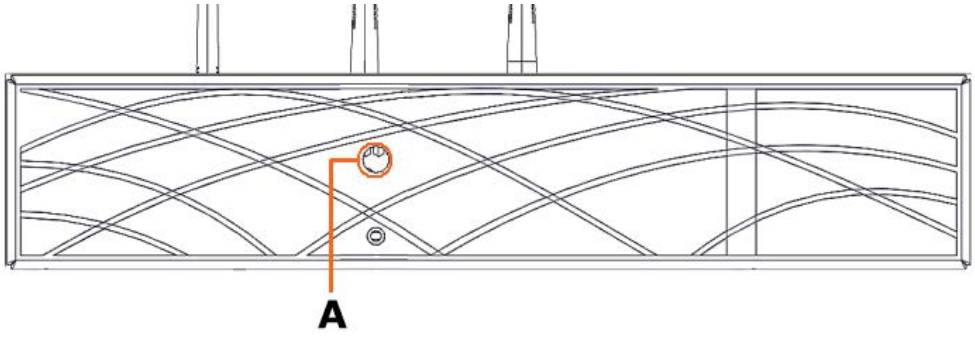
2. Connect the server to the power supply.
   - If the server is installed in a rack cabinet:
     i. Route the power cable along the cabinet flange to the PDU.
     ii. Plug the power cable into the required PDU.
   - For any other installation, plug the power cable into the required PDU.

Rear view



3. Turn the site power breakers ON.
4. Check that the power status LED (A) blinks green to indicate that the server is connected to the power supply.

Front view



1.2. Accessing the Server Hardware Console (SHC)

The first connection to the SHC can be made using either the default static IP address for the BMC, the default host name or a dynamic IP address allocated by an external DHCP server.

Important	**The procedures for the first connection to the SHC using the default BMC IP address may not apply if any default parameters or settings have changed.**

See	The SHC Reference Guide for more information about the console.

1.2.1. Connecting to the SHC using the default host name

Prerequistes

Chrome or Firefox are used to make the connection from the laptop

Procedure

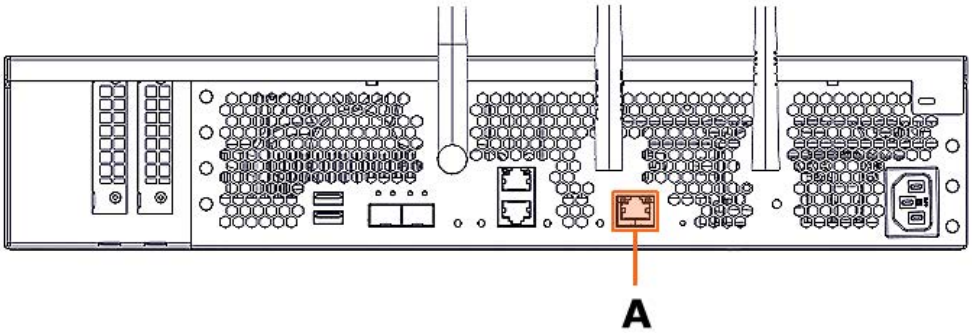
Note	This method works for all types of IP settings (static IP addresses and dynamic IP addresses). There is no need to change the IP configuration for the laptop.

1. **Connect the laptop to the server**

   Connect a laptop directly to the server BMC port (A) via a RJ45 Ethernet cable.

Important	**If a switch is used the ports must support a bandwidth of 1 Gb/s.**

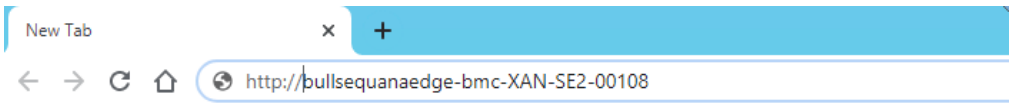
Rear view



2. **Open a web browser on the laptop**

3. **Enter the factory default host name into the address bar**

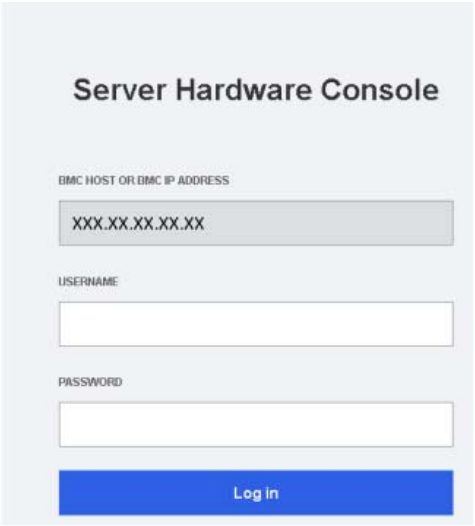
Notes
- The factory default host name is in the following format http://bullsequanaedge-bmc-<Serial_Number>.
- The serial number is written on the label at the back of the server.



4. **Ignore any security warning messages displayed**

Ignore all security warning messages including advanced messages.

The Server Hardware Console (SHC) authentication page opens.



1.2.2. Connecting to the SHC using the default IP address

Prerequistes

Chrome or Firefox are used to make the connection from the laptop

Procedure

1. **Configure a static IP address for the laptop**

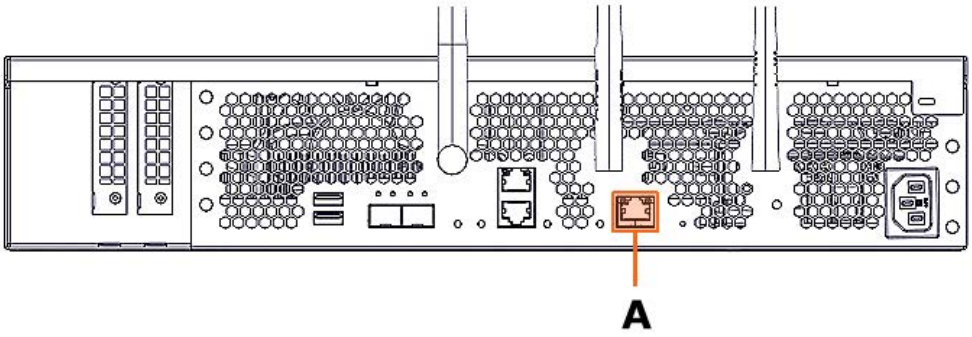
Notes
- The static IP address for the laptop must be in the same range as the default static IP address for the BullSequana Edge server.
- The default static IP address for the BullSequana Edge server is 192.168.0.2.
- The static IP address for the laptop must be different from the server static IP address, for example, 192.168.0.3, subnet:255.255.255.0, gateway: 192.168.0.254.

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

Connect a laptop directly to the server BMC port (A) via a RJ45 Ethernet cable.

Important **If a switch is used the ports must support a bandwidth of 1 Gb/s.**

Rear view



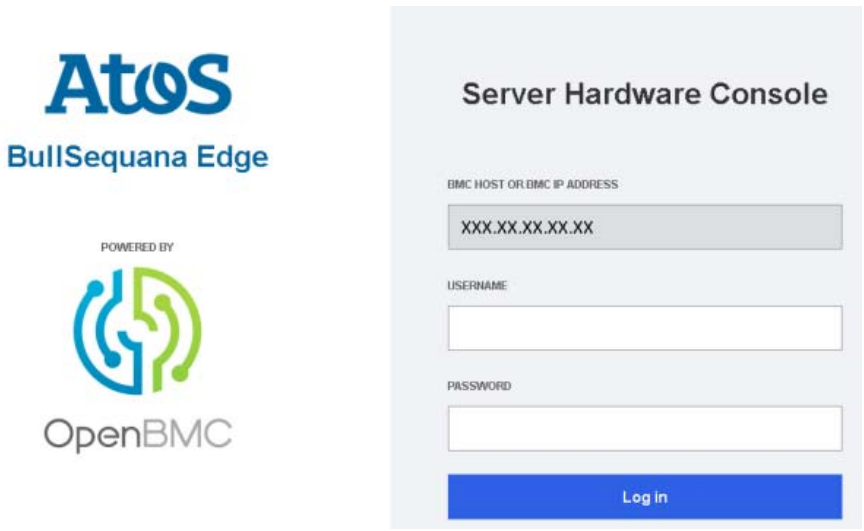
3. **Open a web browser on the laptop**

4. **Enter the BullSequana Edge default IP address, 192.168.0.2, into the address bar**

5. **Ignore any security warning messages displayed**

   Ignore all security warning messages including advanced messages.

   The Server Hardware Console (SHC) authentication page opens.



1.2.3. Connecting to the SHC using a dynamic IP addresss

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

See	Appendix A Obtaining an IP address for alternative methods to obtain an IP address dynamically.

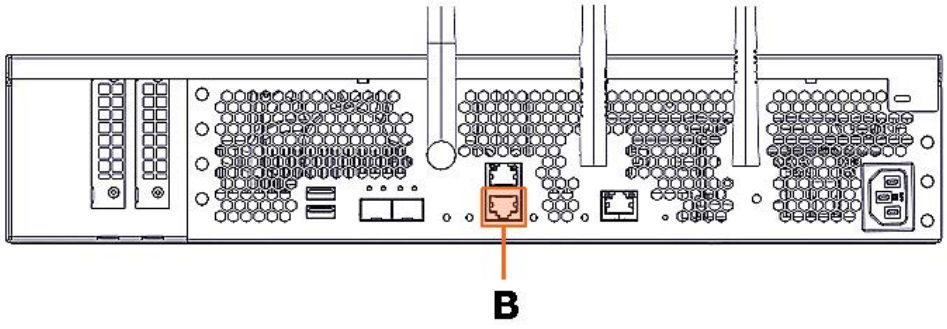
Prerequisites

- The LAN includes a DHCP server
- Access to the DHCP server allocation table is possible

Procedure

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

   Connect the switch to the 1 Gb/s Ethernet PO port (B) of the server 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**

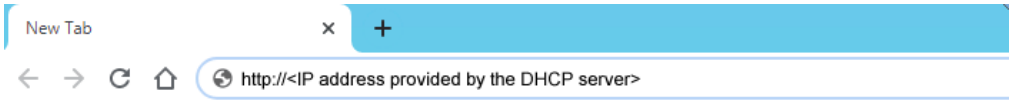
   Connect the 1 Gb/s Ethernet switch using a RJ45 Ethernet cable to the LAN having a DHCP server.

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

   Retrieve an IP address from the DHCP server table.

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

6. **Open a web browser on the laptop**

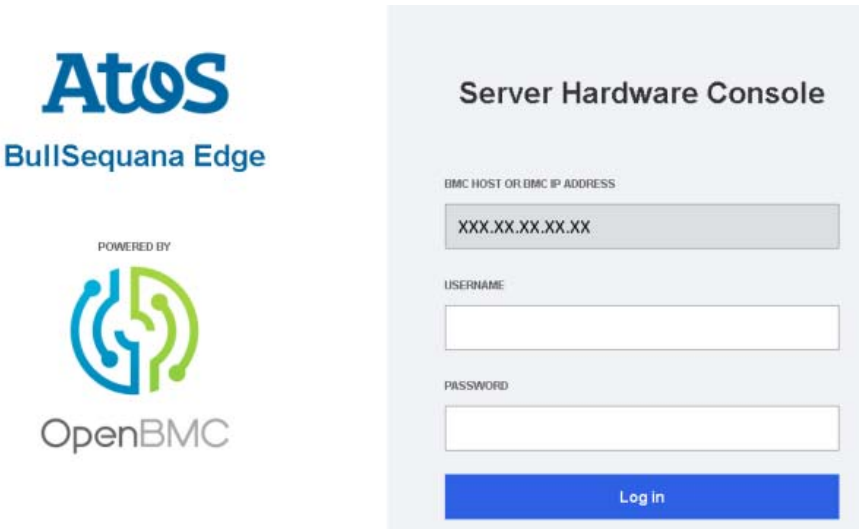


7. **Enter the dynamic IP address into the address bar**

8. **Ignore any security warning messages displayed**

   Ignore all security warning messages including advanced messages.

   The Server Hardware Console (SHC) authentication page opens.



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

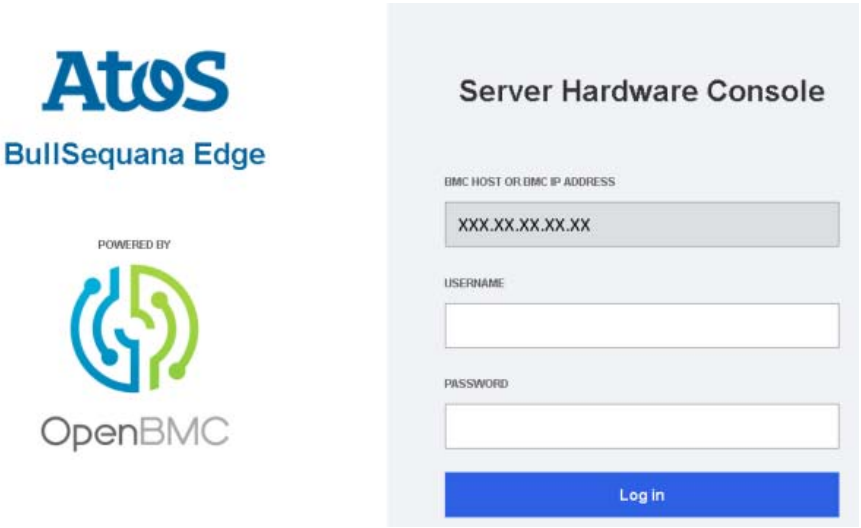
Prerequistes

- A laptop is IP connected with the BullSequana Edge server SHC
- Chrome or Firefox are used to make the connection from the laptop

Procedure

1. **Connect to the SHC**

   The Server Hardware Console (SHC) authentication page opens.



Server Hardware Console (SHC)	
BMC host name or IP address	Automatically completed with the host name or IP address according to the connection method
Username	Factory default: root
Password	Factory default: At0s!Edge

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.**

See	The SHC Reference Guide for more information.

Chapter 2. Installing an Operating System (OS)

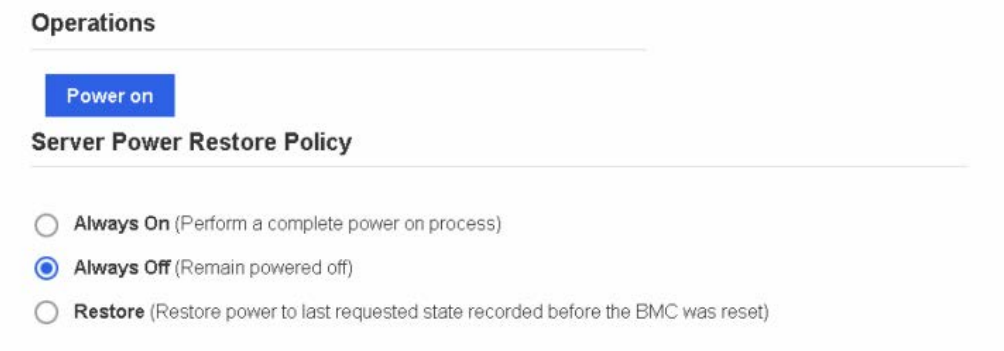
2.1. Powering on the server from the SHC

Prerequisites

The server power status is Off

Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select the power restore policy required.



4. Click **Power on**.

2.2. Operating System (OS) installation options

Choose one of the following methods to install the OS on the server:

- Using a bootable USB drive
- Using a Pre-boot eXecution Environment (PXE)
- Using a Virtual Media device

2.2.1. Using a bootable USB drive

Prerequisites

- The server power status is Running
- A bootable USB drive with the OS to be installed is plugged into the server

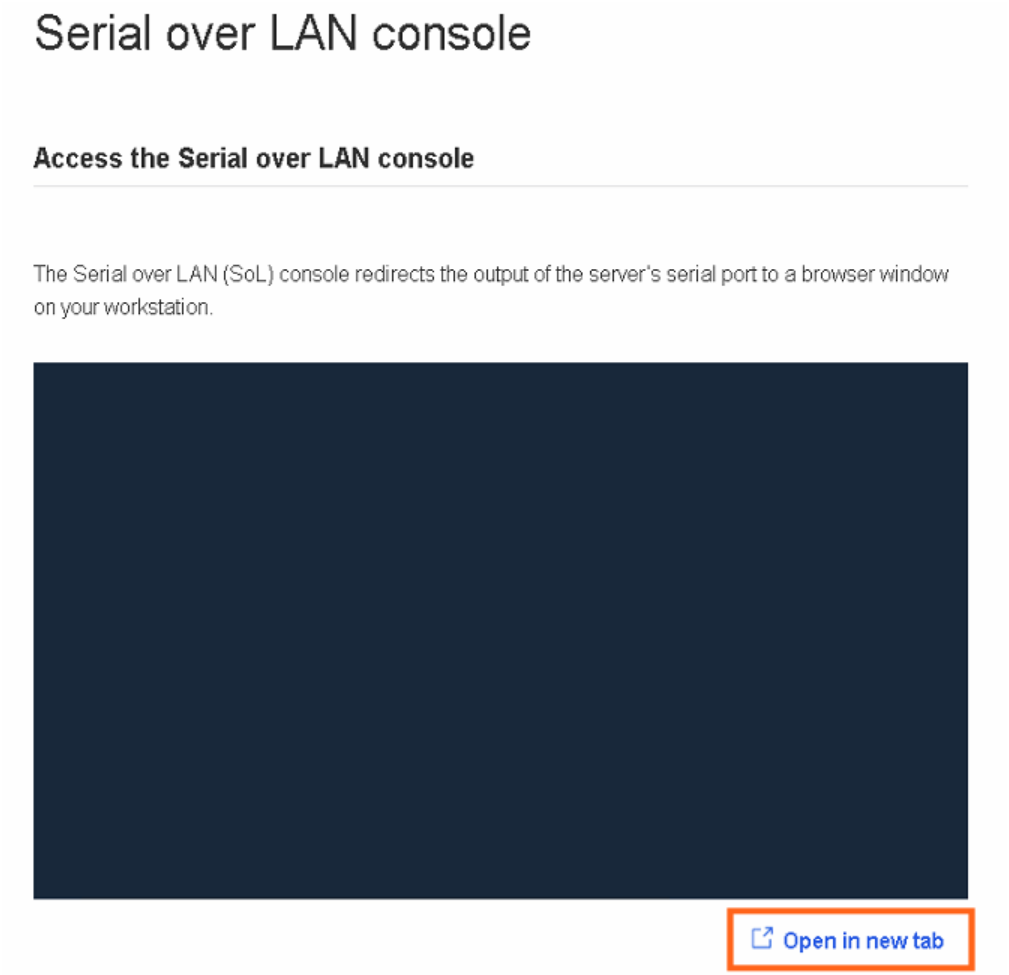
Note It is recommended that the latest version of the **Rufus** tool is used to format and create the bootable USB drive.

Procedure

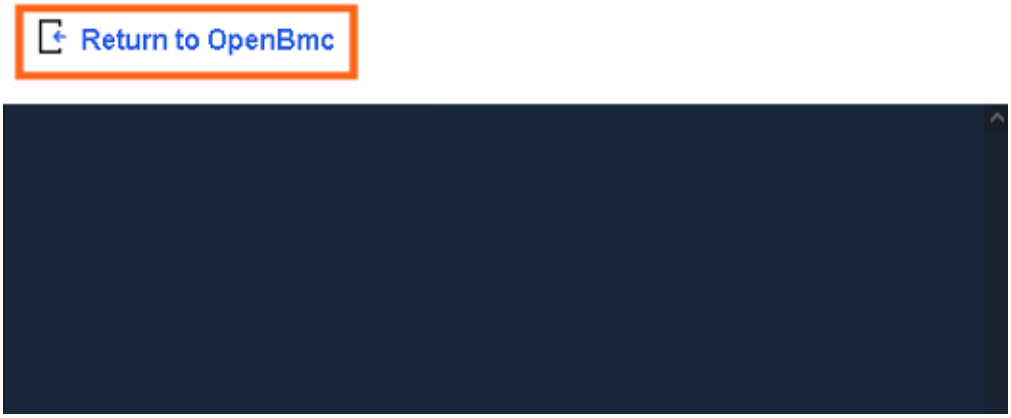
1. **Connect to the SHC**

2. **Access the BIOS interface**

   1. From the **Control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.



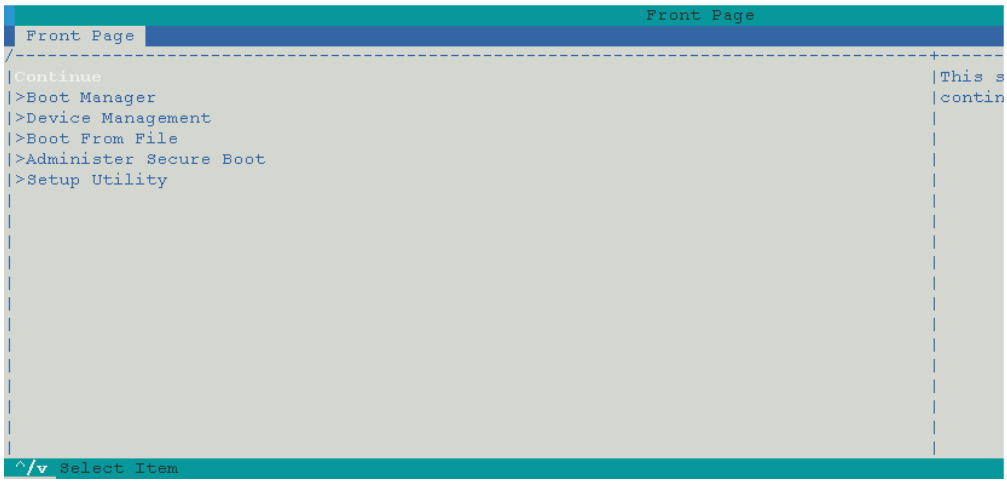
   2. If required, click the **Open in new tab** link to open the console in a new window.
   3. Click **Return to OpenBmc** to go back to the the main window.



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

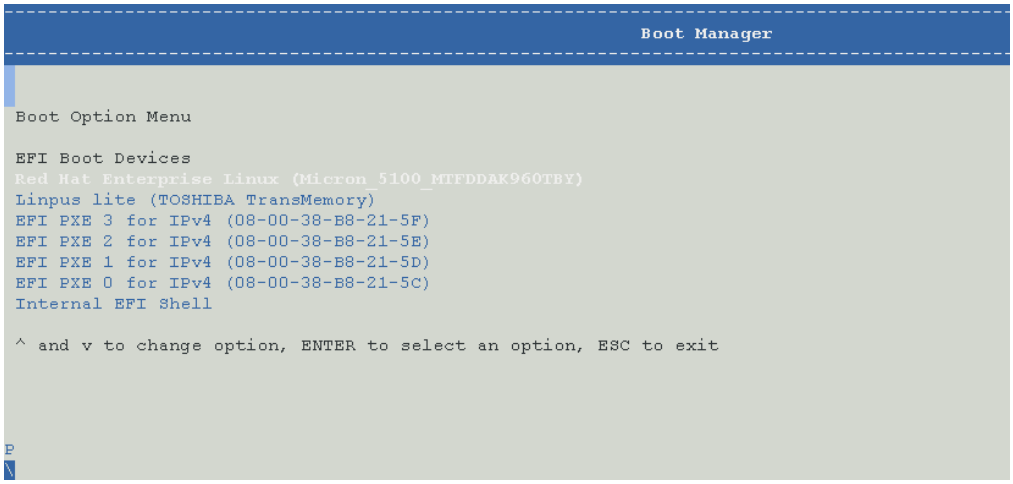
Important **The [Esc] key must be pressed quickly after the Serial over LAN console window opens.**

The BIOS interface opens.



3. Choose the boot device

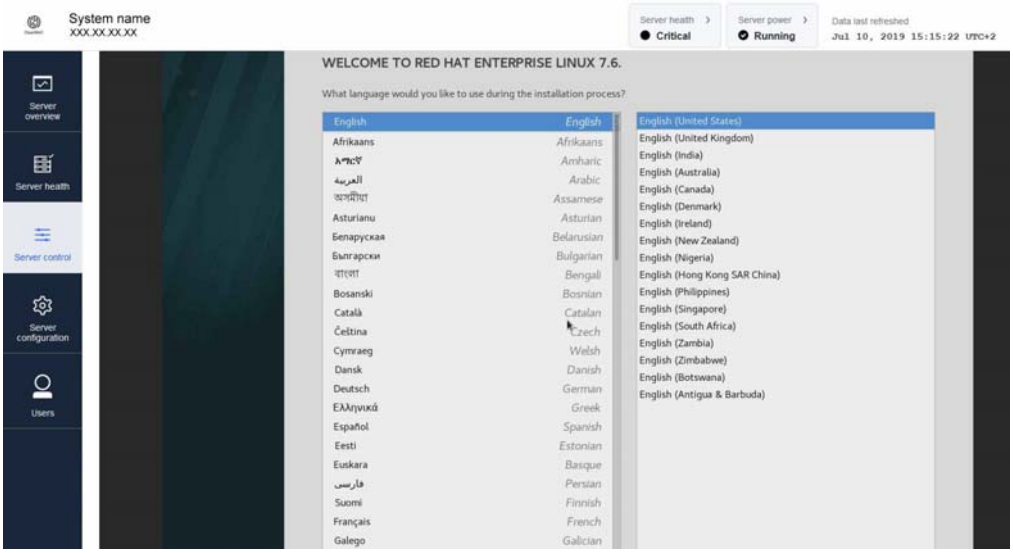
1. Select **Boot Manager** using the navigation arrows and press [Enter].
2. Select the USB drive boot device using the navigation arrows and press [Enter].



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

4. 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

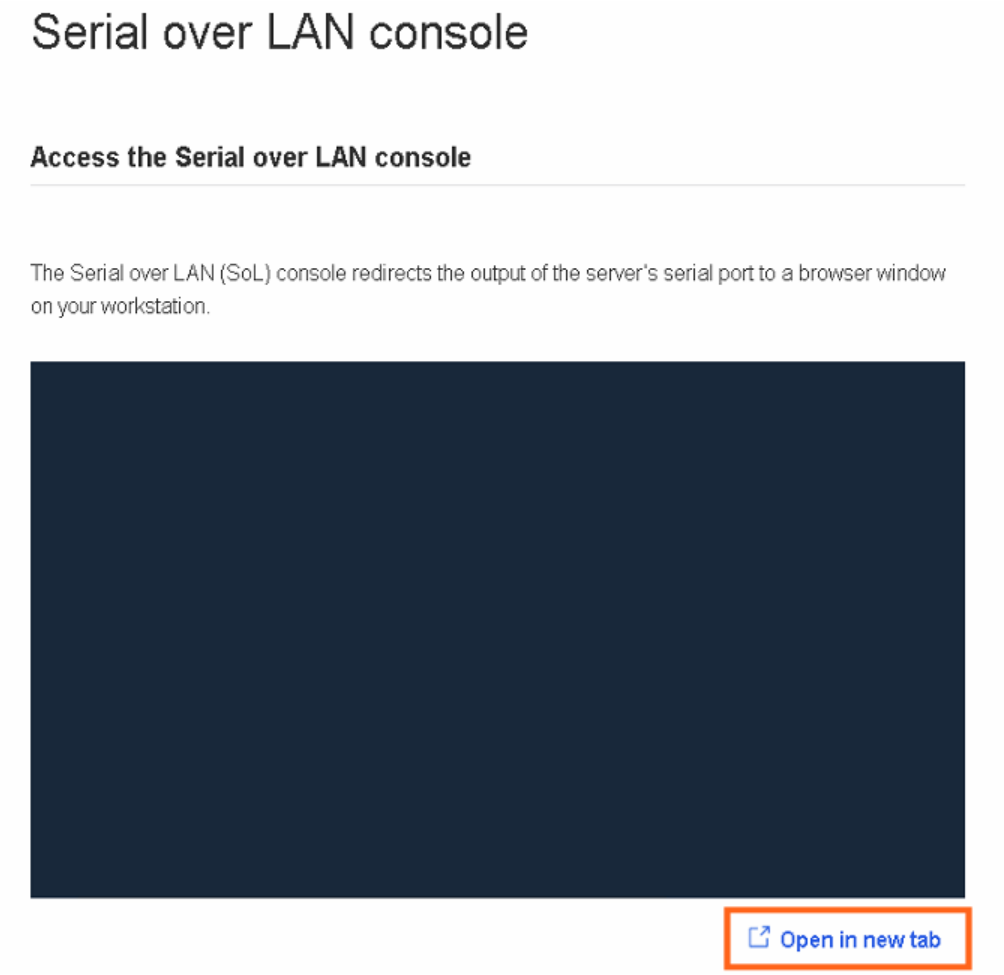
- The server power status is Running
- A PXE server has been set up and is accessible

Procedure

1. **Connect to the SHC**

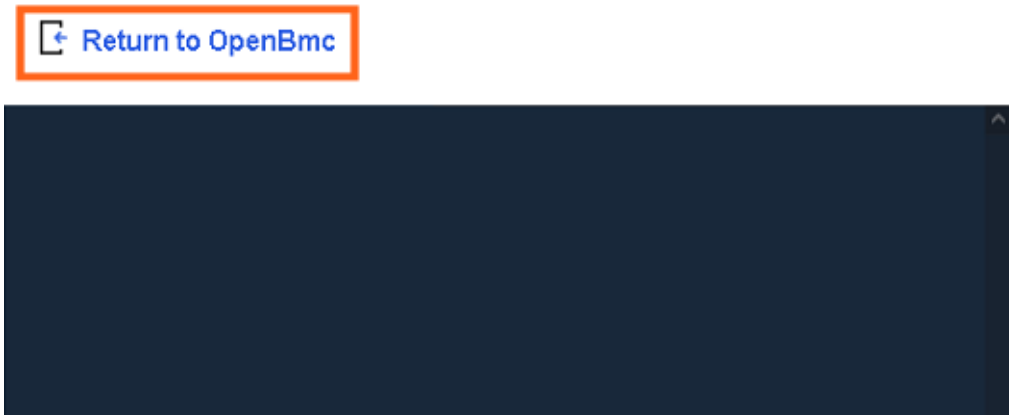
2. **Access the BIOS interface**

   1. From the **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.

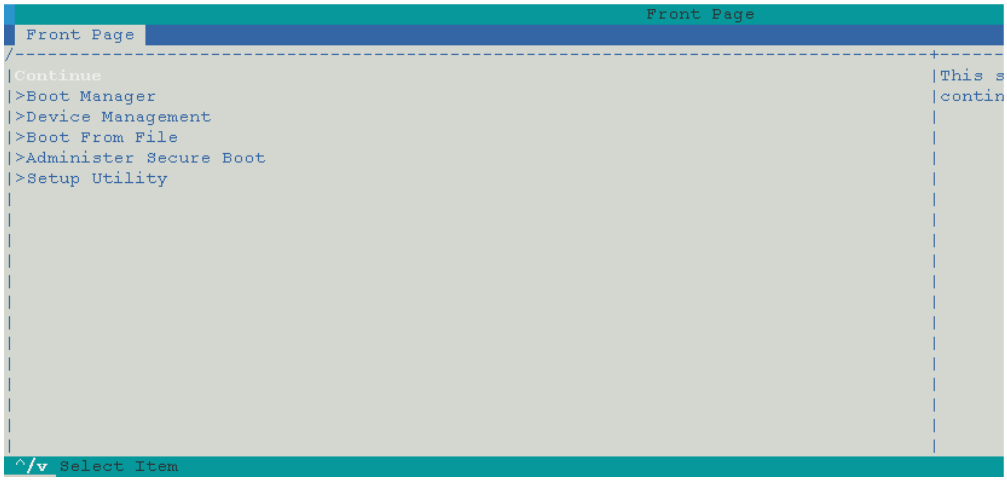
3. Click **Return to OpenBmc** to go back to the the main window.



4. 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.**

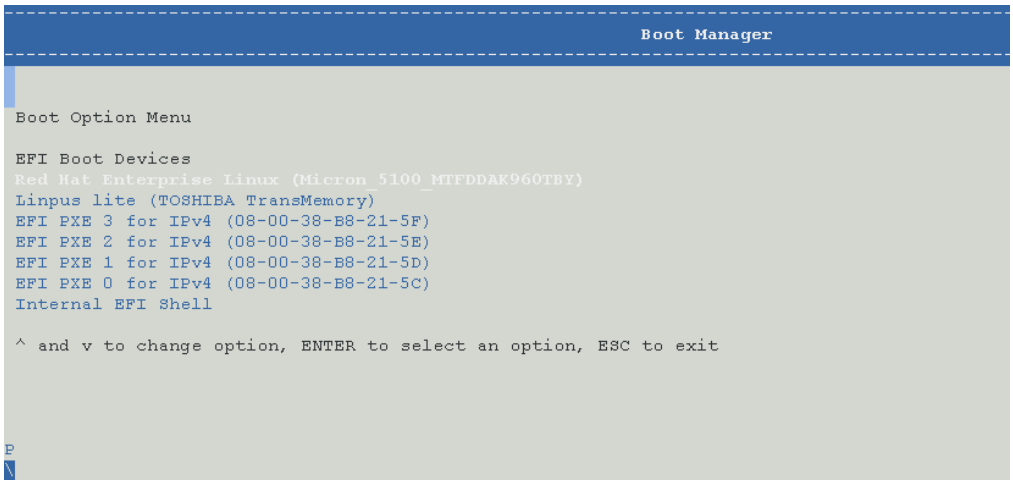
The BIOS interface opens.



3. Choose the boot device

1. Select **Boot Manager** using the navigation arrows and press [Enter].

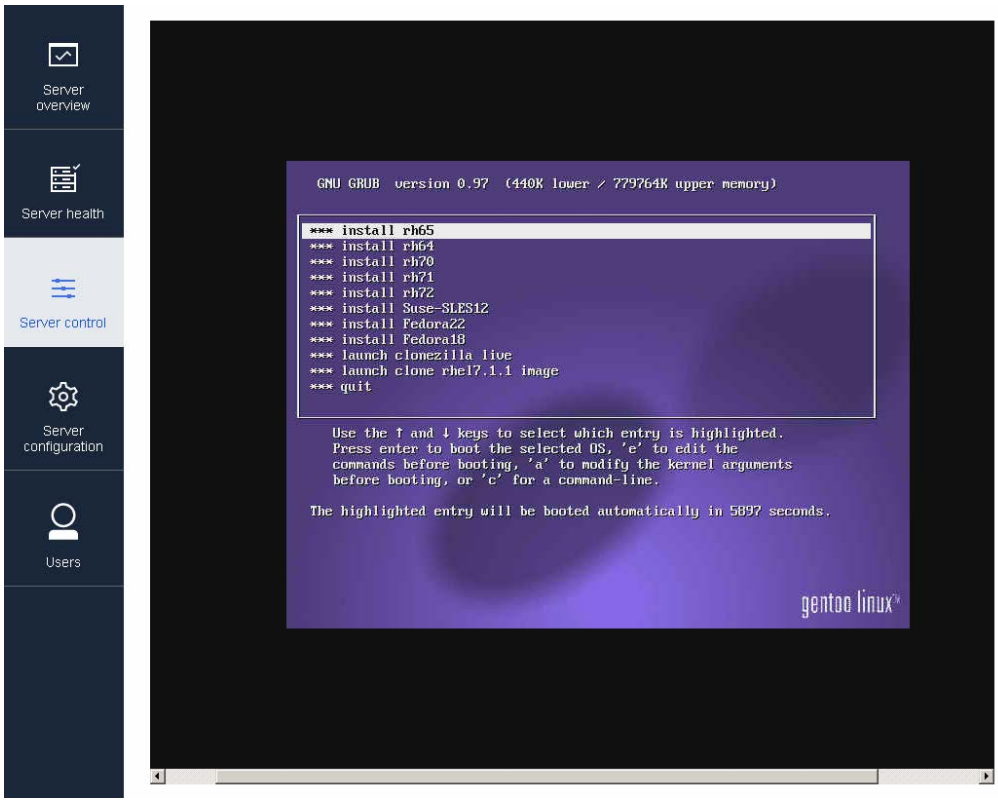
2. Select the PXE boot device using the navigation arrows and press [Enter].



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

4. 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.

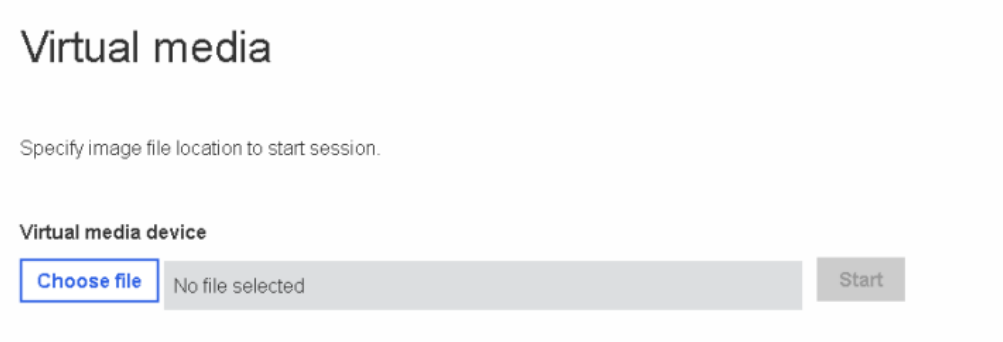
2.2.3. Using a Virtual Media device

Prerequisites

The location of the virtual media ISO file is known

Procedure

1. **Select the Operating System ISO file**
   1. Connect to the **SHC.**
   2. From the **Control** tab, click **Virtual Media**. The **Virtual Media** page opens.



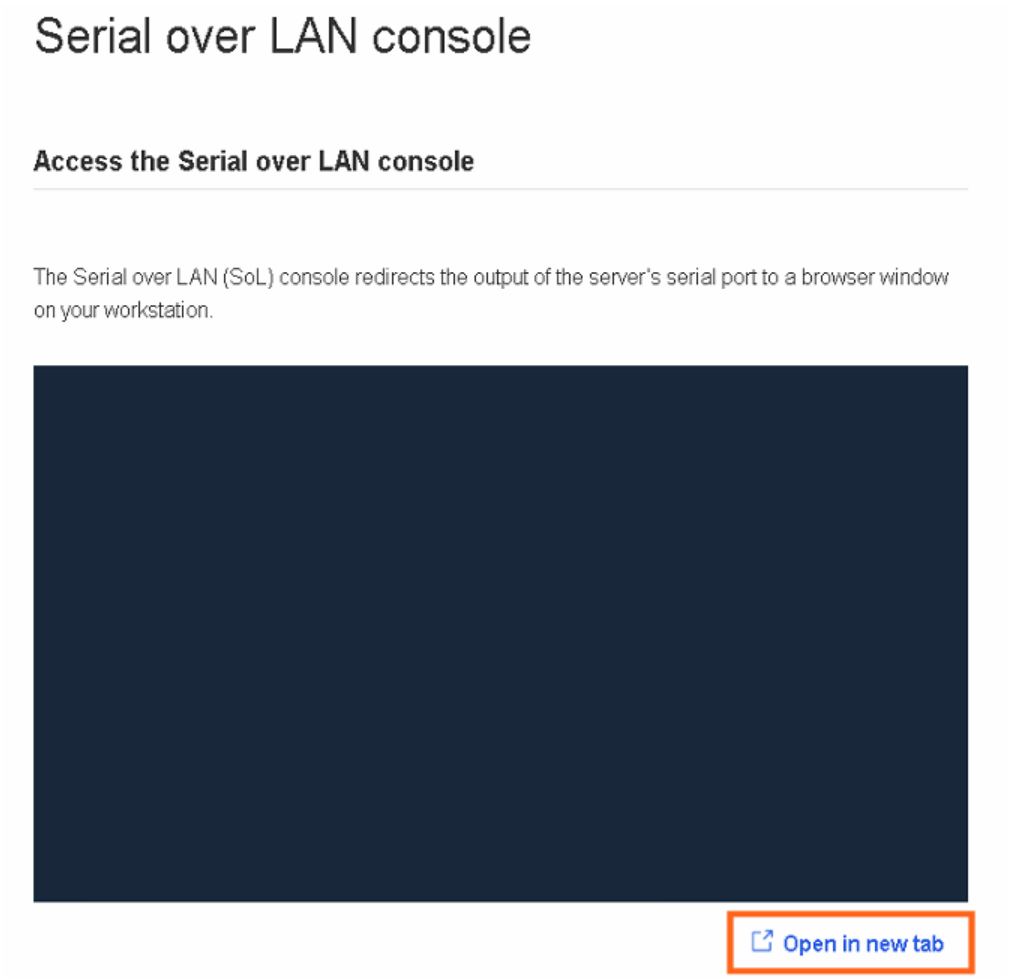
   3. Click **Choose file**.
   4. Select an ISO file for the boot.
   5. Click **Start**.

2. **Boot the server**

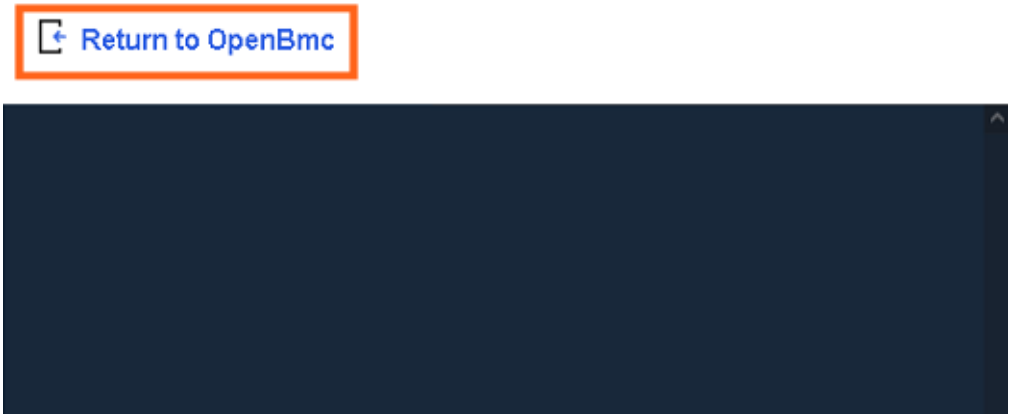
   Start the server or reboot if already started.

3. Access the BIOS interface

1. From the **Control** tab, click **Serial over LAN console**. The **Serial over LAN console** page opens.



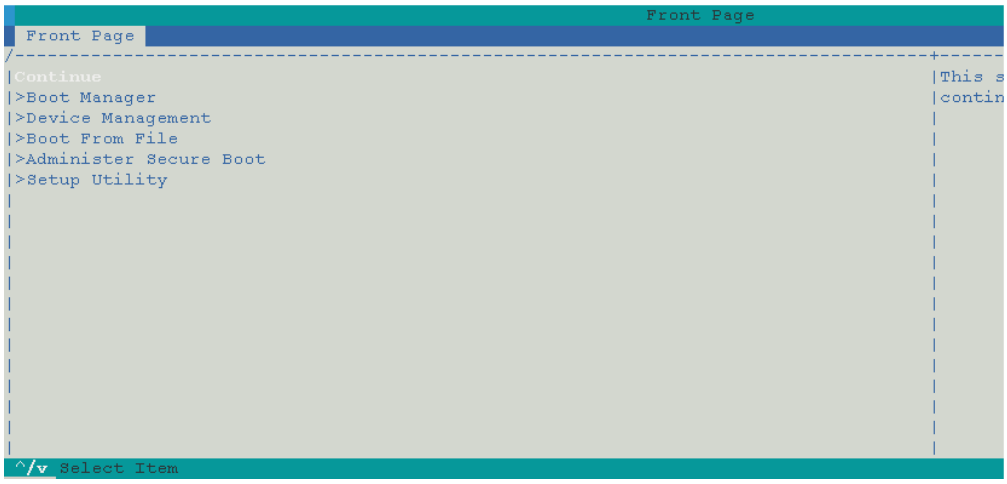
2. If required, click the **Open in new tab** link to open the console in a new window.
3. Click **Return to OpenBmc** to go back to the the main window.



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

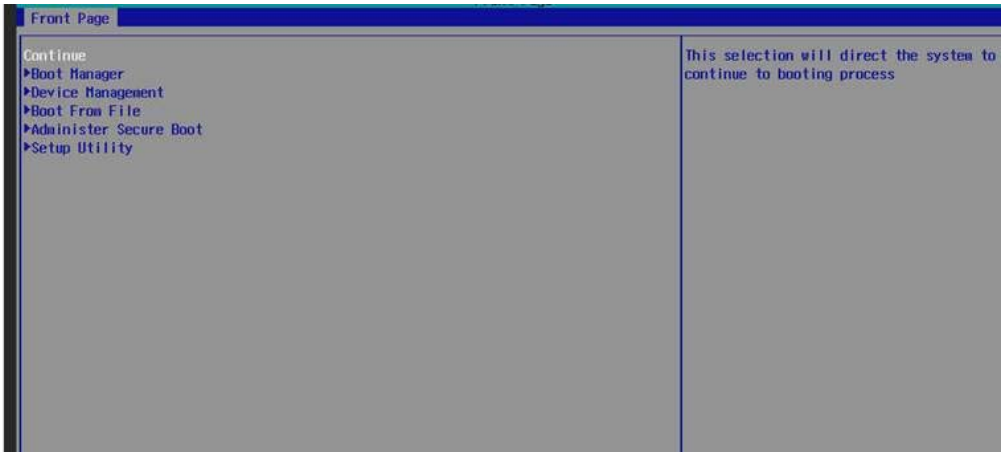
Important **The [Esc] key must be pressed quickly after the Serial over LAN console window opens.**

The BIOS interface opens.



4. Switch to the KVM interface

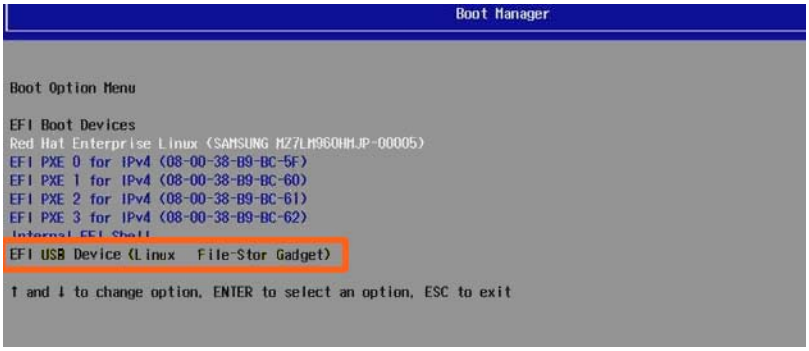
1. In the SHC from the **Control** tab, click **KVM.**



2. Click **Boot Manager**.

5. Select the EFI image for the boot

1. Select the EFI USB device using the navigation arrows and press **Enter**.



Note The position of the EFI USB device may vary in the Boot Option menu.

2. Follow the instructions displayed to boot from the EFI USB device.

6. Install the OS

1. Follow the instructions displayed to install the OS.

2. Select the system settings required.

2.3. Accessing the server Operating System (OS)

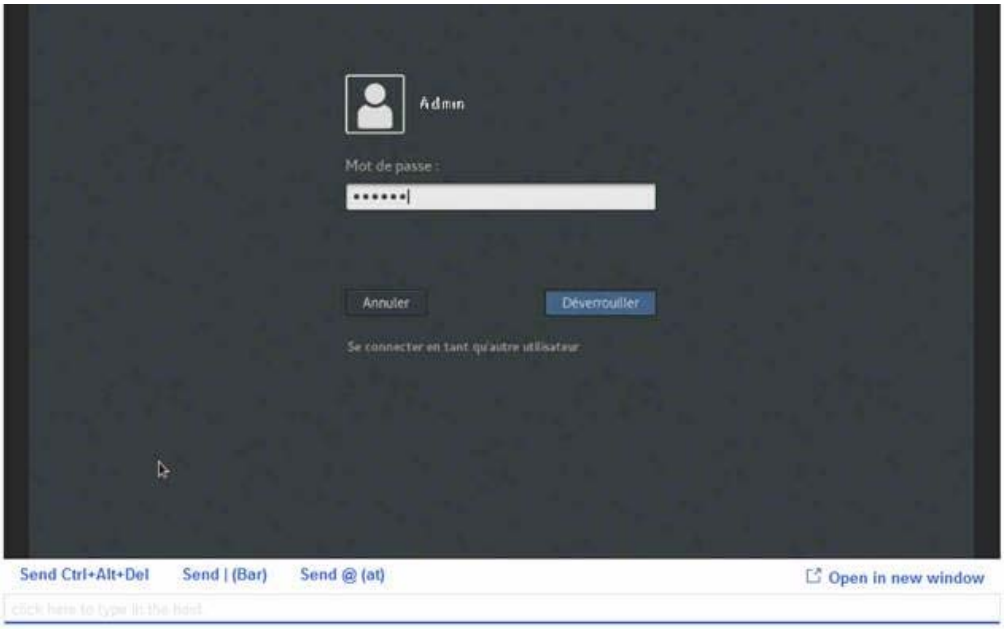
Prerequisites

The server power status is Running

Procedure

1. Connect to the SHC
2. From the **Control** tab, click **KVM**. The **IP KVM** page opens.

3. Click the **click here to type in the host** field. The operating system desktop opens.



Note Input text can be entered in the operating system environment or in the **click here to type in the host** KVM field.

4. Perform server operations, as required.

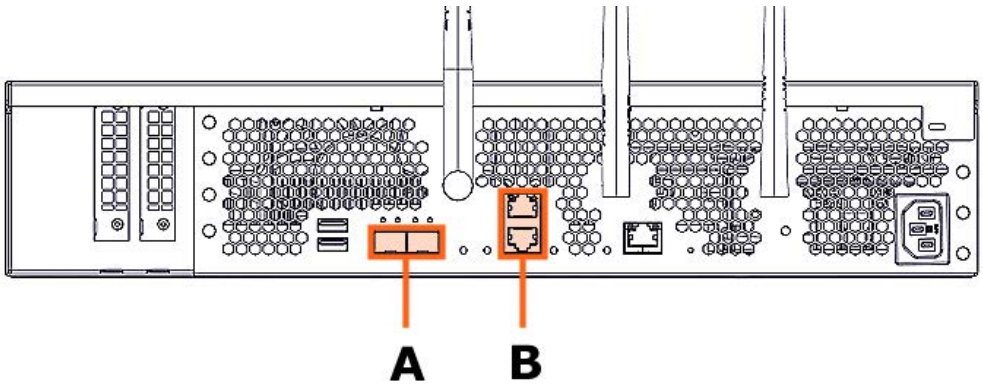
Chapter 3. Connecting to the data system

3.1. Connecting the server to the data LAN

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

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

Rear view



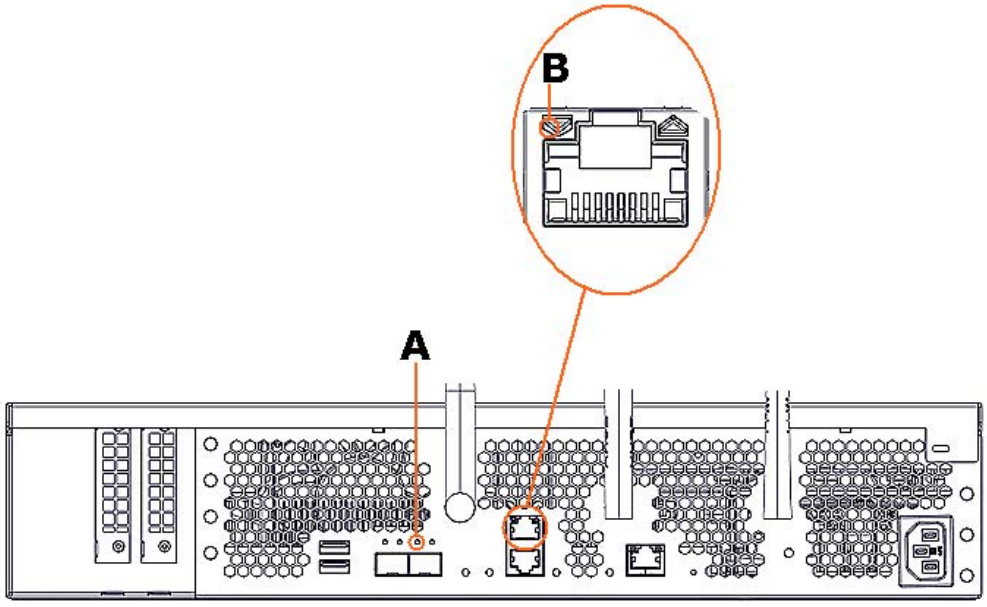
Mark	Port type
A	2 x SFP+ - 10 Gb/s Ethernet
B	2 x RJ45 - 1 Gb/s Ethernet

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

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

4.1. Powering methods

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.

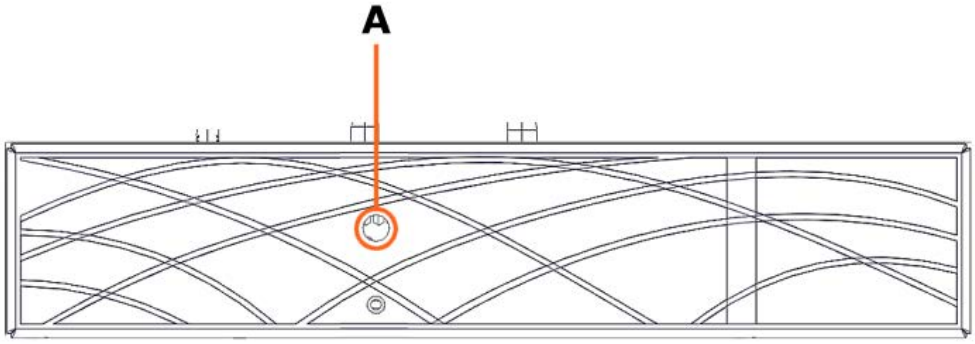
The SHC operates via a server Baseboard Management Controller (BMC) and can only intervene on one server at a time. MISM console jobs can operate on groups of servers at a time.

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

4.2. Powering on the server with the power button

1. Check that the power status LED (A) is blinking green to indicate that the server power status is Off.
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 power status is Running.

4.3. Powering on the server from the SHC

Prerequisites

The server power status is Off

Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select the power restore policy required.

4. Click **Power on**.

4.4. Powering on the server from the MISM console

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

Prerequisites

The server power status is Off

Procedure

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

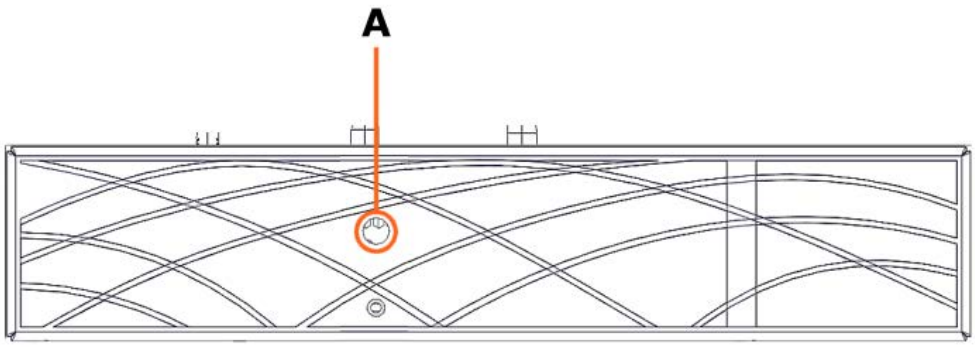
   If the job status is **Failed**, check the output of the job in the text window.
3. Launch the **Check Power On** job.
4. Check that the job status is **Successful**.

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

4.5. Powering off the server with the power button

1. Check that the power status LED (A) is solid green to indicate that the server power status is Running.
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 power status is Off.

4.6. Powering off the server from the SHC

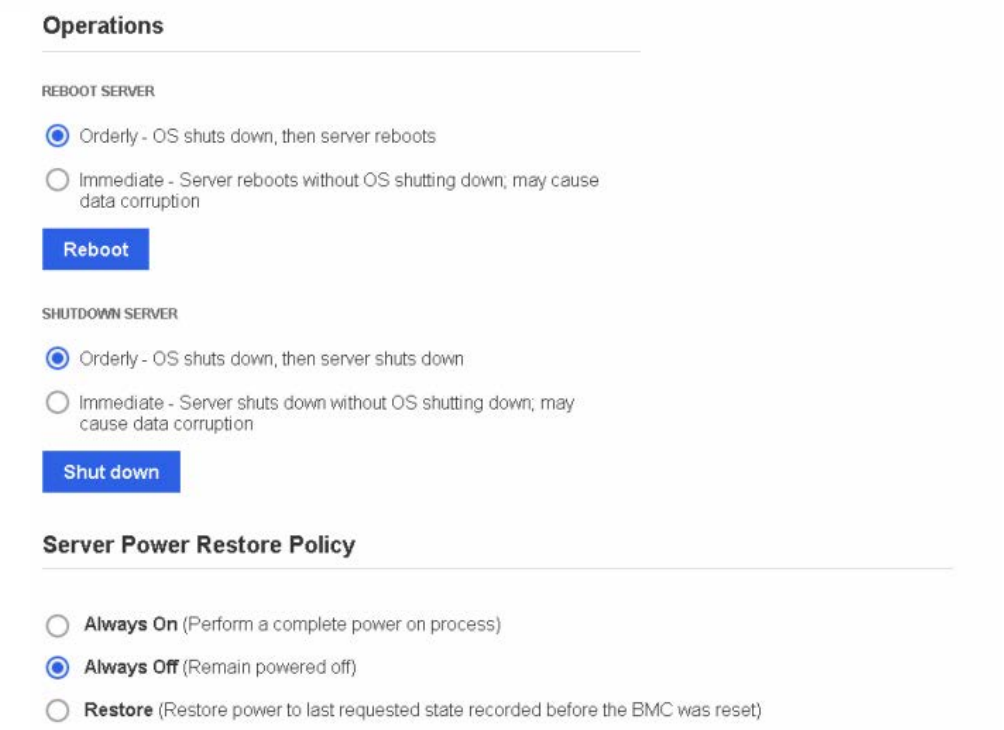
W087 **WARNING**
W087:
The immediate reboot and shutdown buttons should only be used if the Operating System is unable to respond to an orderly reboot or shutdown request.
These sequences may result in data loss and file corruption.

Prerequisites

The server power status is Running

Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.
3. In the **Operations** section, select either the reboot or shut down option required.



4. Select the power restore policy required.
5. Click **Reboot** or **Shut down**.

4.7. Powering off the server from the MISM console

W087  **WARNING**

W087:
The immediate reboot and shutdown buttons should only be used if the Operating System is unable to respond to an orderly reboot or shutdown request.
These sequences may result in data loss and file corruption.

Prerequisites

The server power status is Running

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.

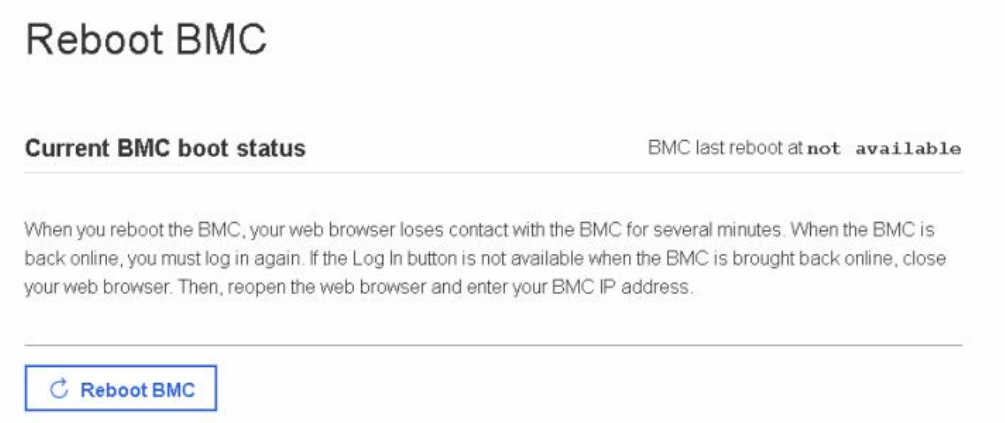
Chapter 5. Server Hardware Console (SHC) maintenance operations

See The SHC Reference Guide for more information.

5.1. Rebooting the Baseboard Management Controller (BMC)

Procedure

1. Connect to the SHC
2. From the **Control** tab, click **Reboot BMC**. The **Reboot BMC** page opens.



3. 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.

Important **The date and time will be lost following a BMC reboot if they have been set manually. It is recommended to use NTP to set the date and time to preserve the settings when the BMC is rebooted.**

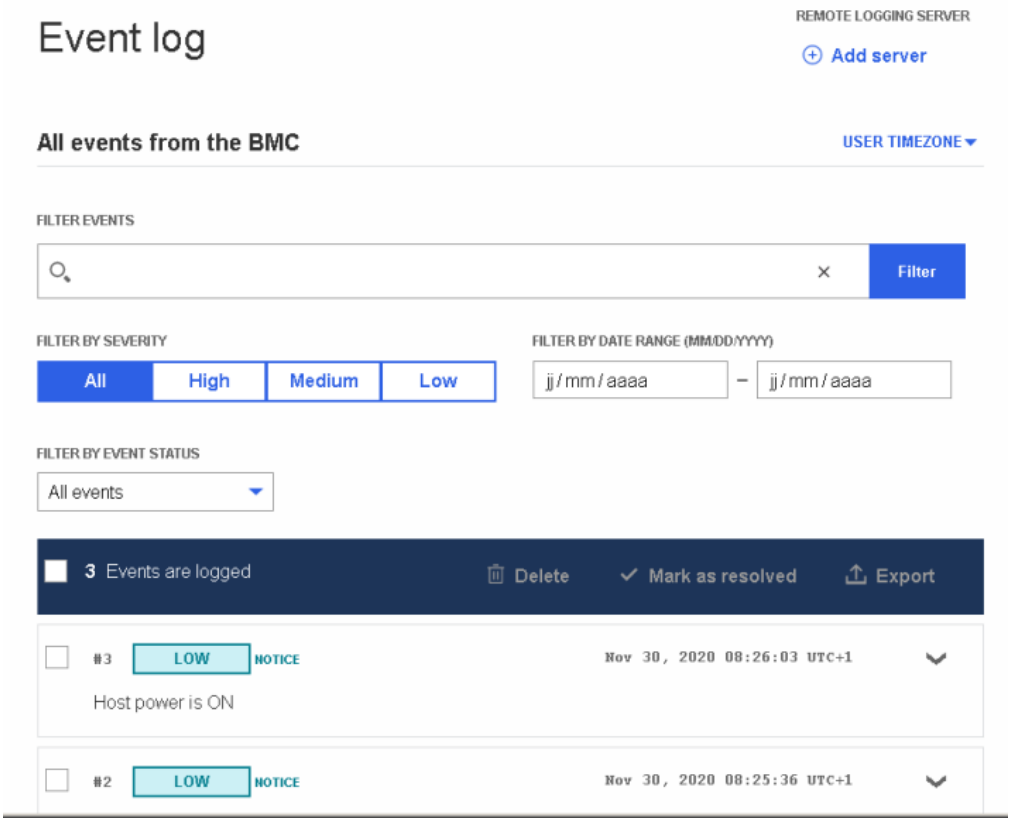
5.2. Checking event logs

Prerequisites

The server power status is Running

Procedure

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



3. Set the log name, severity and date range parameters.
4. Click **Filter**. The list of logged events is displayed.

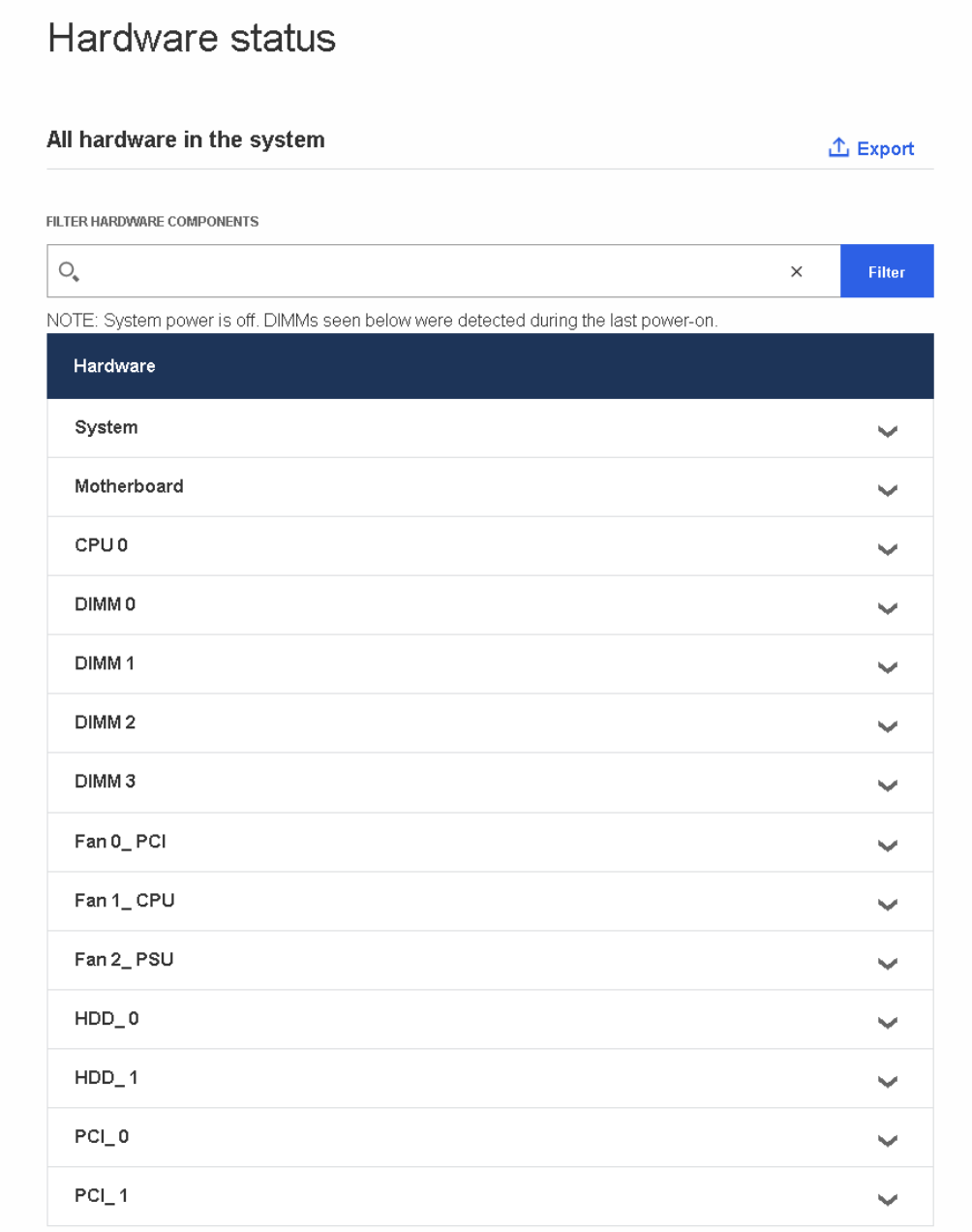
5.3. Checking the hardware status

Prerequisites

The server power status is Running

Procedure

1. Connect to the SHC
2. From the **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.

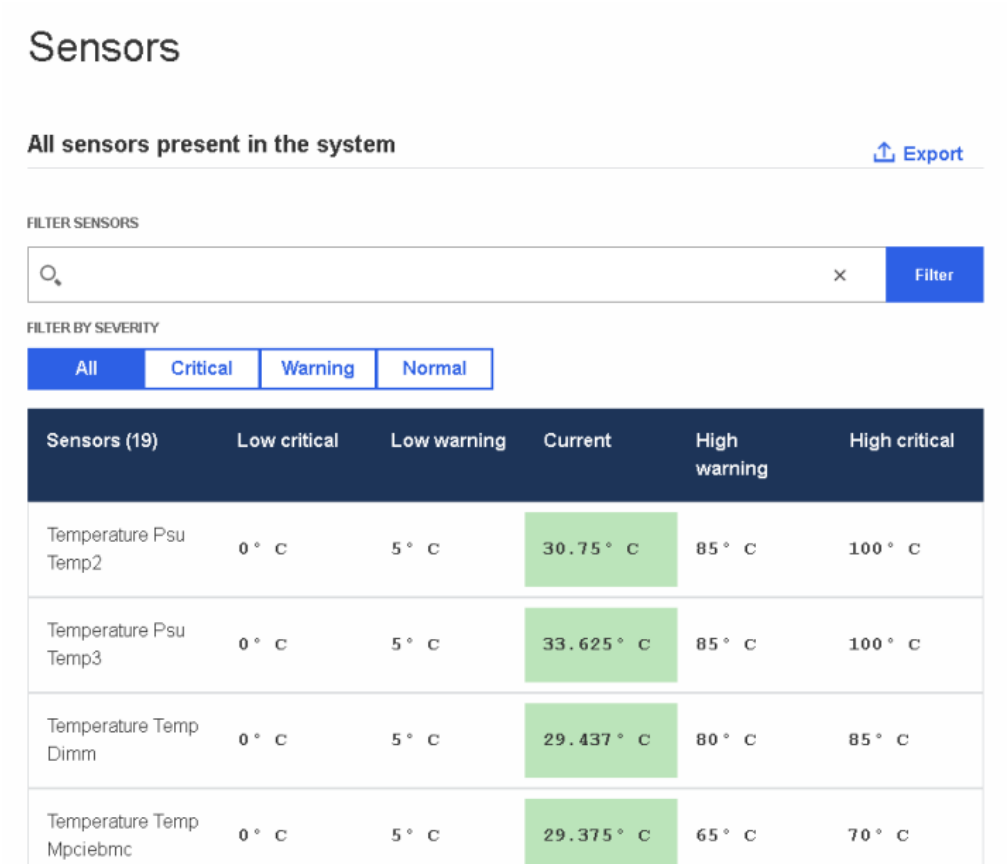
5.4. Checking the sensors

Prerequisites

The server power status is Running

Procedure

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



Severity	Description
GREEN	NORMAL Operation correct. No problem has been detected.
ORANGE	WARNING A problem has been detected that may need preventive or corrective action.
RED	CRITICAL A problem has been detected. Immediate preventive or corrective action is required.

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

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

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.

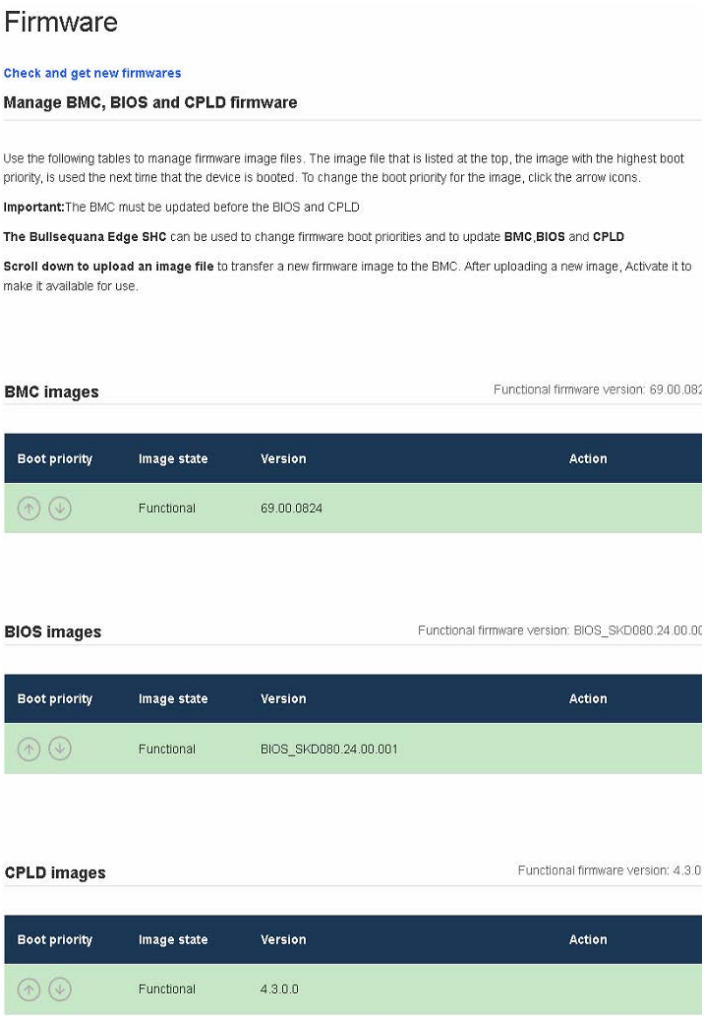
5.5.1. Checking firmware versions

Prerequisites

The server power status is Running

Procedure

1. Connect to the SHC
2. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.



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

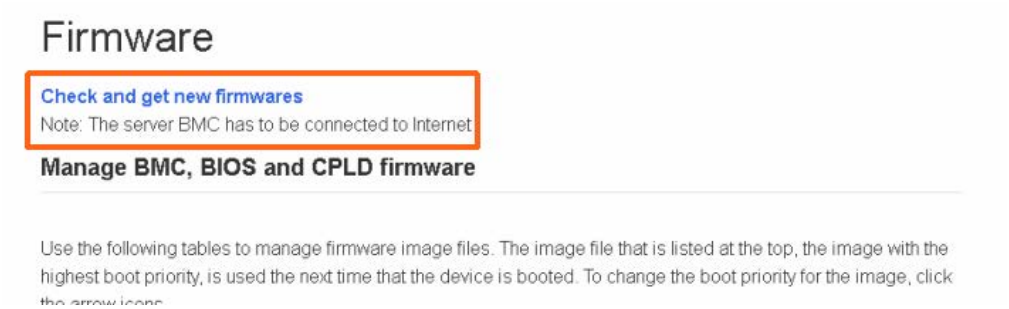
5.5.2. Checking the firmware is up-to-date

Prerequisites

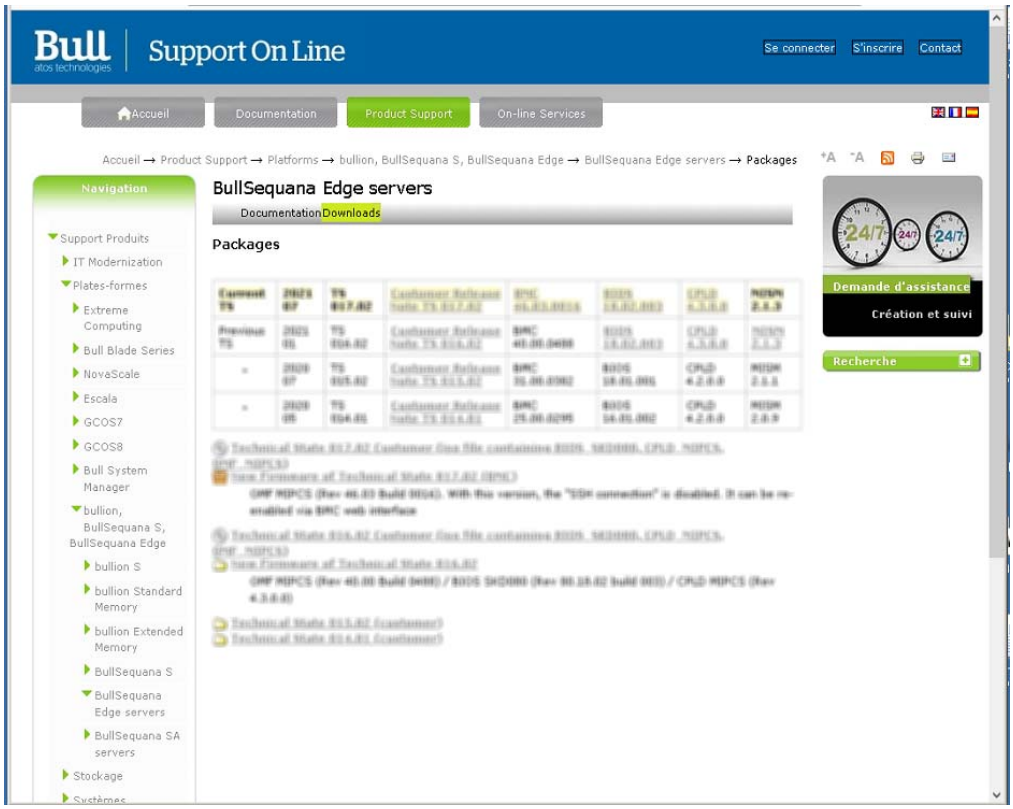
- A laptop computer with the Chrome or Firefox browser installed
- Connection to the internet
- The server power status is Running

Procedure

1. Connect to the SHC
2. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
3. Click **Check and get new firmware**.



The support web site opens with the latest firmware list.



4. Download the latest versions, if more up-to-date versions are available.

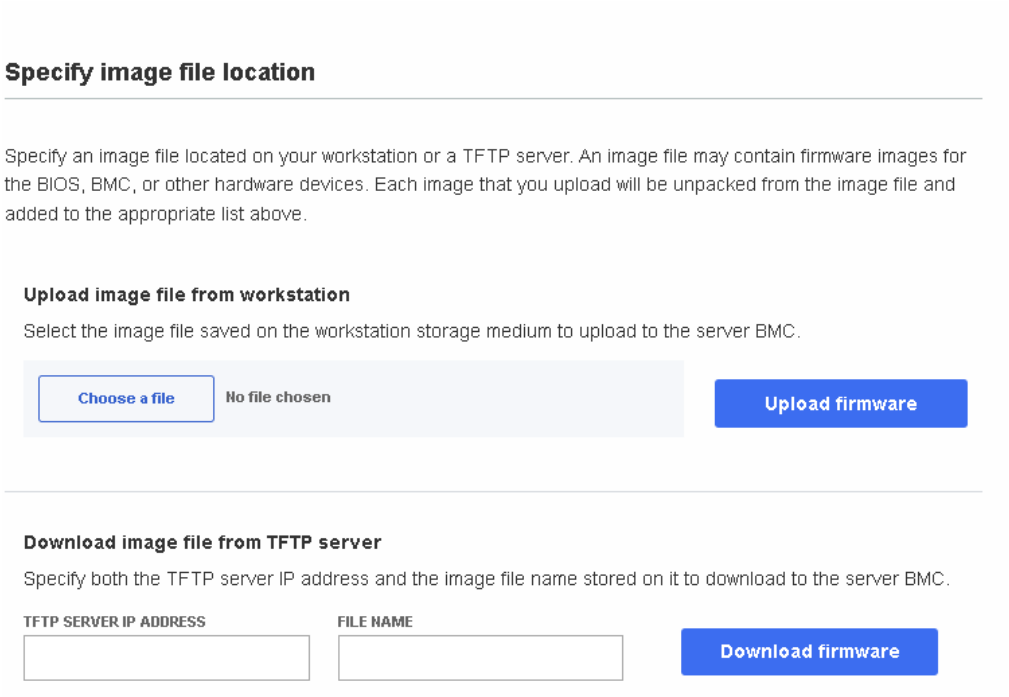
5.5.3. Updating the BMC firmware

Prerequisites

The server power status is Off or Running

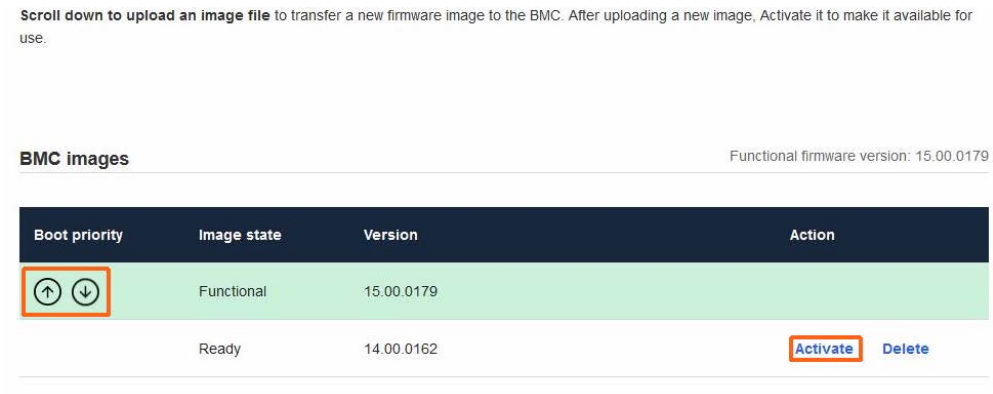
Procedure

1. **Check the server power status**
2. **Connect to the SHC**
3. **Update the firmware**
   1. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
   2. From the **Specify image file location** section:
      a. Either click **Choose a file** > **Upload firmware** to upload an image file from a workstation.
      b. Or click **Download firmware** to download an image file from a TFTP server.

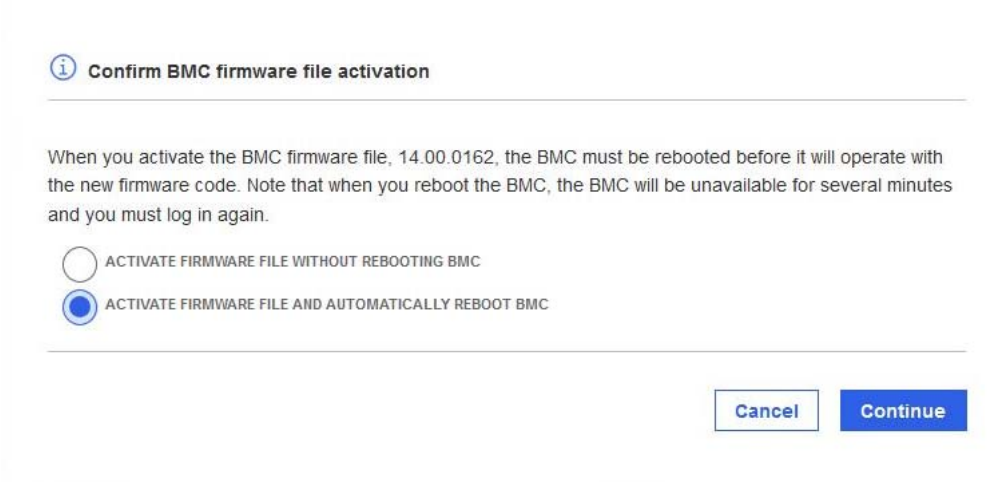


4. Activate the BMC image

1. Select the BMC image using the boot priority arrows.
2. Click **Activate.**



3. The Confirm BMC firmware file activation page opens. Click **Activate firmware file and automatically reboot BMC**.



4. 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.

5.5.4. Updating the BIOS and CPLD firmware

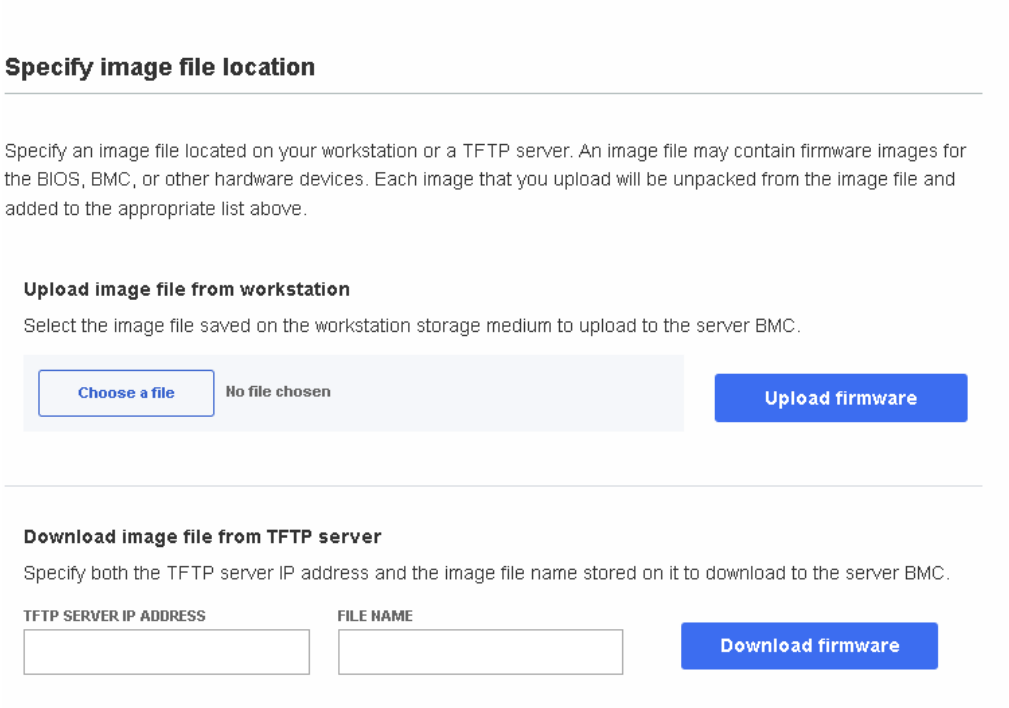
Important	**Check that the latest BMC firmware version is installed. If not, the BMC firmware must be updated before the BIOS and CPLD firmware.**

Prerequisites

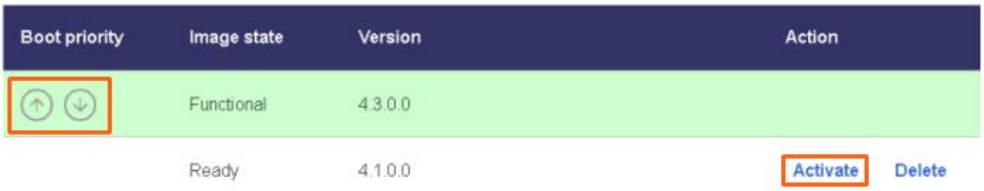
The server power status is Off

Procedure

1. **Check the server power status**
2. **Connect to the SHC**
3. **Update the firmware**
   1. From the **Configuration** tab, click **Firmware**. The **Firmware** page opens.
   2. From the **Specify image file location** section:
      a. Either click **Choose a file** > **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 firmware**
    1. Select the firmware using the boot priority arrows.
    2. Click **Activate.**



5. **Wait two to three minutes and then refresh the page**

    The firmware is now active.

6. **Power on the server**
    1. From the **Control** tab, click **Server power operations**. The **Server power operations** page opens.

    2. In the **Operations** section, click **Power on**.

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 power status is Off
- The MISM console is launched

Procedure

Important **The date and time will be lost following a BMC reboot if they have been set manually. It is recommended to use NTP to set the date and time to preserve the settings when the BMC is rebooted.**

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.

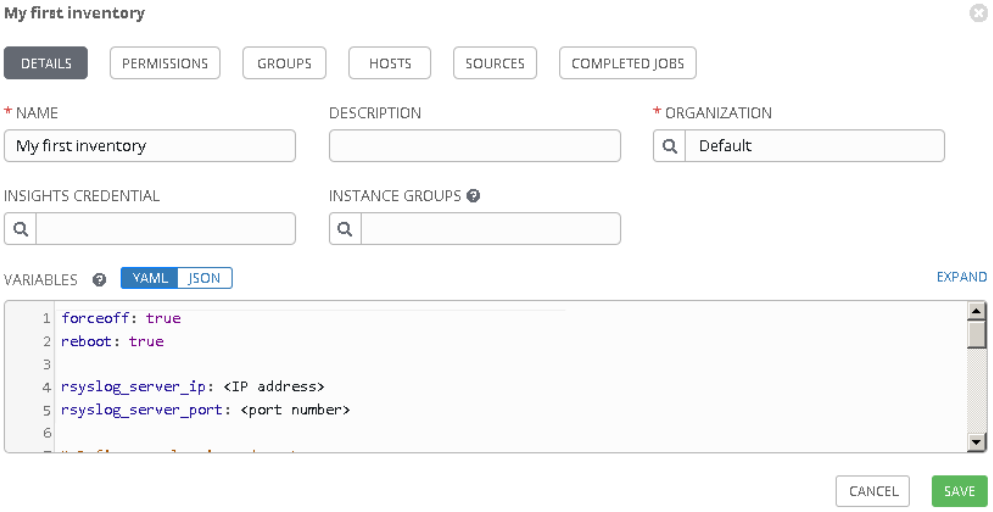
6.3. Enabling syslog forwarding

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. Obtaining an IP address

If after the first connection the server host name or the default static IP address is changed, or the SHC IP settings (BMC port, P0 port) have been changed from the default settings, the connection may be made using an IP address attributed dynamically using the following methods:

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

A.1. Obtaining an IP address with an auto-discovery tool

Important **BullSequana Edge servers must be connected to Ethernet switch ports that support a 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 SHC is connected to a network without a DHCP server.

Note This method also works if the SHC is connected via the BMC port to a LAN with a DHCP server or if the BMC port is configured with a static IP address.

Prerequisites

Note If the BMC port has been set to dynamic (and not the default factory static setting), and connected by cable to a LAN without a DHCP server, the SHC Link local address has to be set for the BMC port (this is the default setting).
If necessary, perform a factory reset via the factory reset button or use the P0 port with Link local address set for the P0 port.

See The Description Guide and the Customer Service Guide for more information about resetting the server to the default factory settings.

A windows laptop with internet access and administrator rights

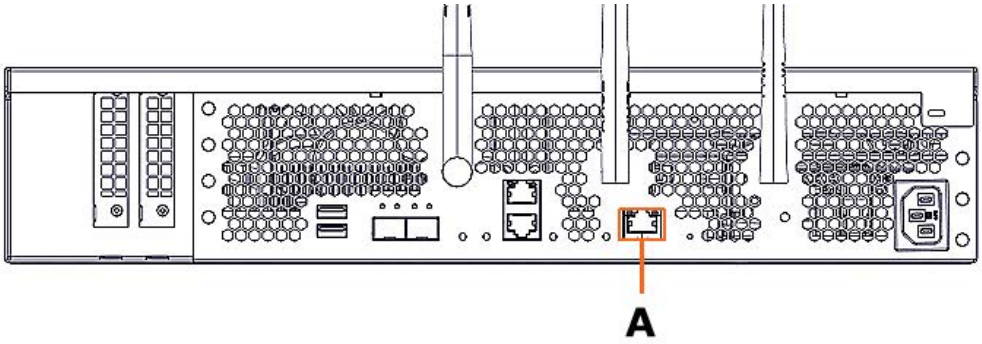
Procedure

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**

2. Connect the server to the laptop

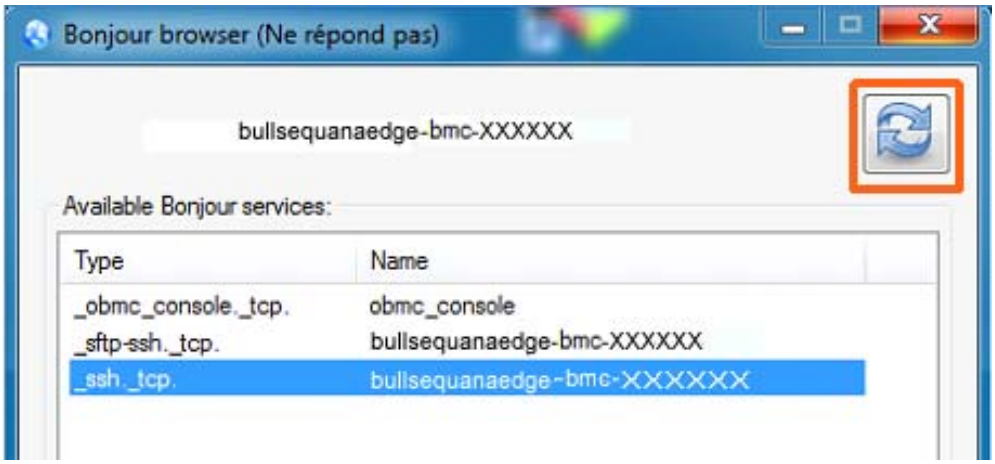
Connect the BMC port (A) of the server to the laptop computer using a RJ45 Ethernet cable or via a 1 Gb/s switch.



3. Launch the Bonjour browser on the laptop

4. Refresh the Bonjour browser

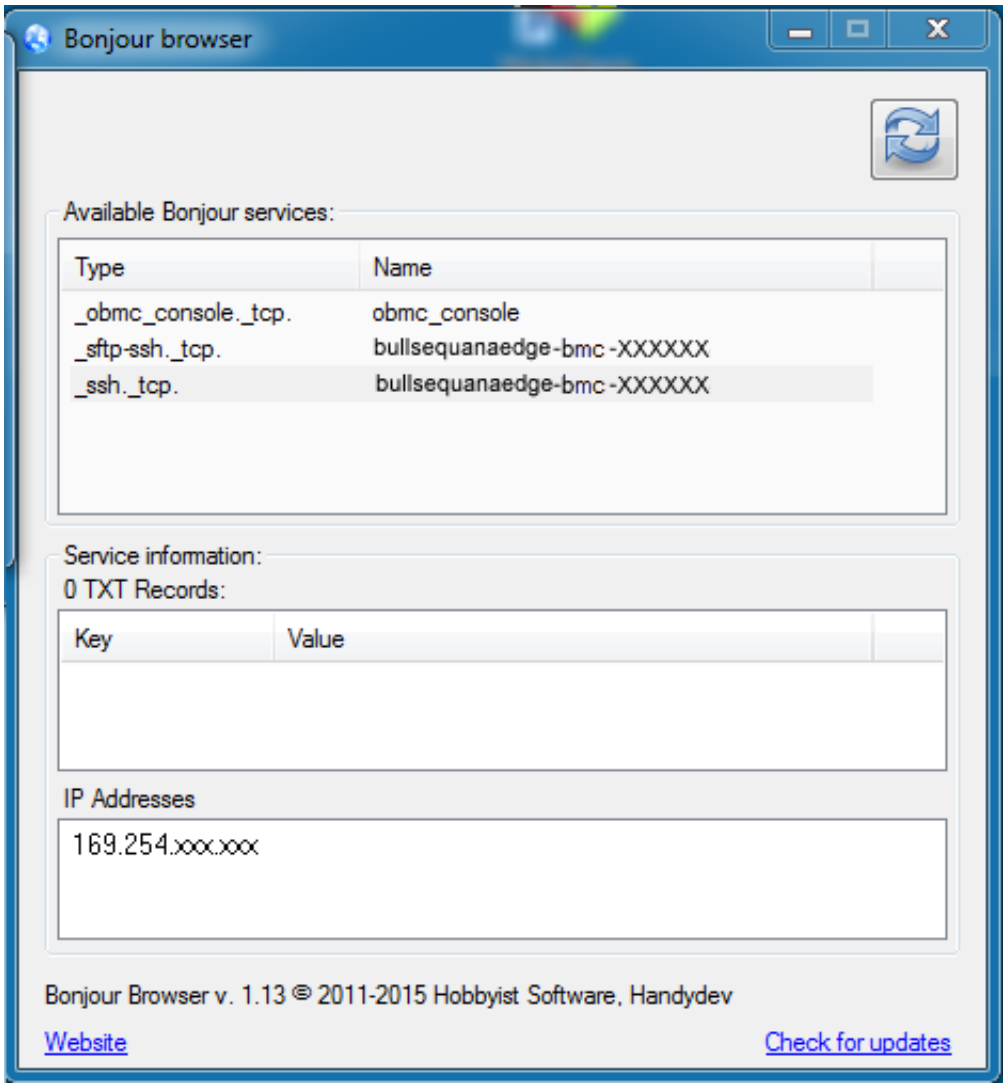
1. Click the Refresh button at the top on right of the browser window.



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.

6. Enter the IP address into the web browser

A.2. Obtaining an IP address via a laptop DHCP server

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

Prerequisites

- The P0 port is configured for dynamic IP addresses (default factory setting)

See The Description Guide and the Customer Service Guide for more information about resetting the server to the default factory settings.

- A windows laptop computer with internet access and administrator rights

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

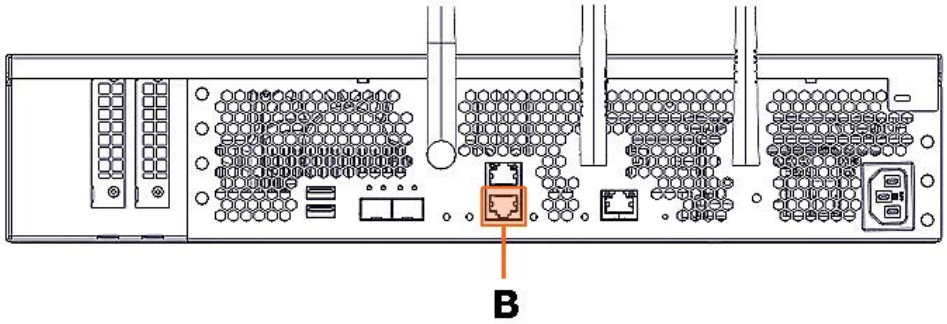
Procedure

1. Install Tftpd64 on the laptop

1. Download the latest **Tftpd64.exe** file.
2. Run **Tftpd64.exe** with administrator rights.

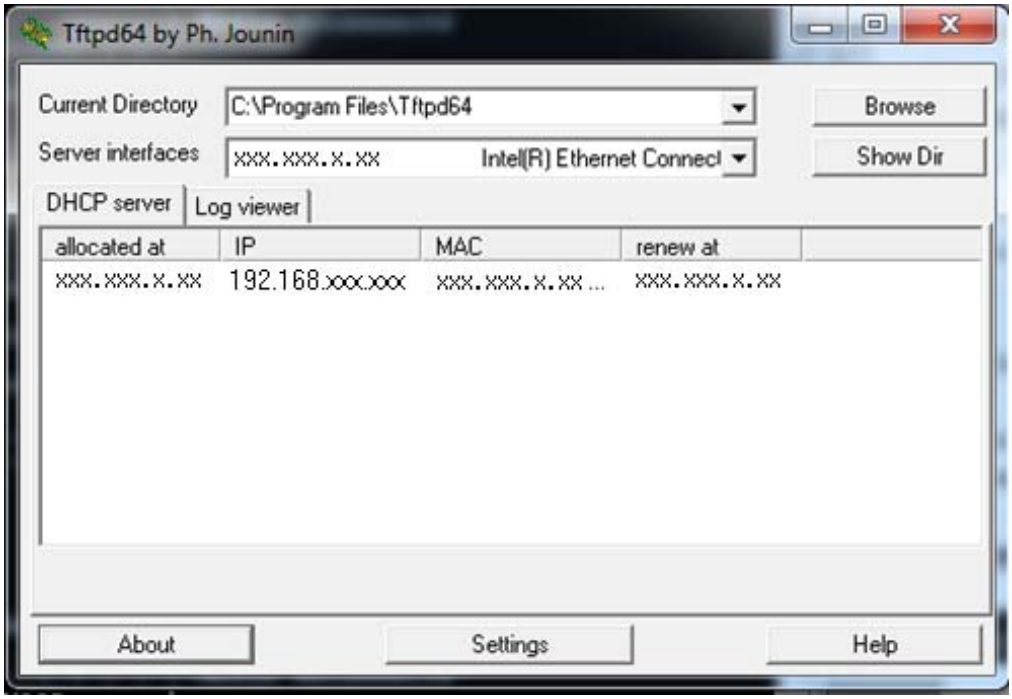
2. Connect the laptop to the server

Connect the laptop to the 1 Gb/s Ethernet PO port (B) of the server using a RJ45 Ethernet cable.



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

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



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

5. **Enter the IP address into the web browser**

Appendix B. IPMI Out of Band (OOB) support

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

B.1. Enabling IPMI OOB support

Prerequisites

- A laptop computer with the Chrome or Firefox browser installed
- The server BMC has an IP address allocated

Procedure

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

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

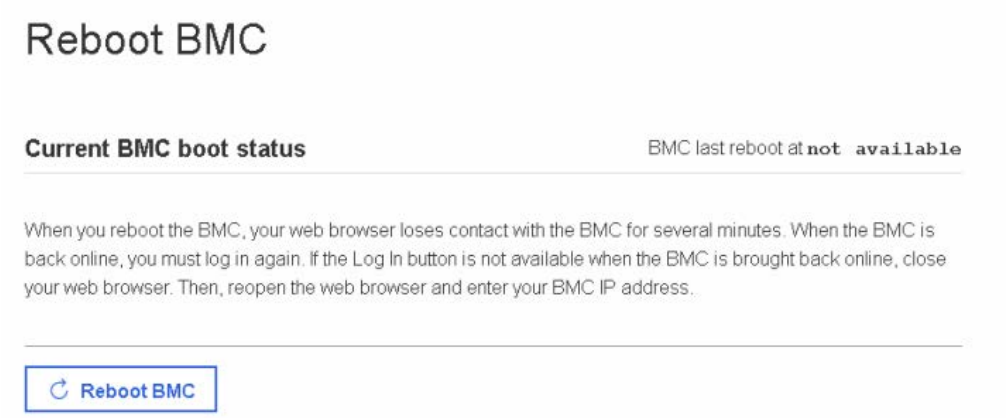
Note Any BMC user account with administrator rights may be used.

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 default user account with its default password can be used to connect to the BMC.

4. Connect to the SHC
5. From the **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.

Important **The date and time will be lost following a BMC reboot if they have been set manually. It is recommended to use NTP to set the date and time to preserve the settings when the BMC is rebooted.**

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.

B.2. Disabling IPMI OOB support

Prerequisites

The server BMC has an IP address allocated

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