novascale Blade BL465

Installation and User's Guide

novascale Blade

REFERENCE
86 A1 68FE 01

novascale Blade

novascale Blade BL465

Installation and User's Guide

Hardware

July 2010

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 68FE 01

Printed in France

Trademarks and Acknowledgements

We acknowledge the rights of the proprietors of the 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 misuse.

Table of Contents

List of Figures

List of Tables

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
(安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

.לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Safety statements

Important:

Each caution and danger statement in this documentation begins with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the *Bull Safety Information* document.

For example, if a caution statement begins with a number 1, translations for that caution statement appear in the *Bull Safety Information* document under statement 1.

Be sure to read all caution and danger statements in this documentation before performing the instructions. Read any additional safety information that comes with your computer or optional device before you install the device.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	To Disconnect:
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2:

CAUTION:
When replacing the lithium battery, use only a battery recommended by the manufacturer. If your system has a module containing a lithium battery, replac it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- Throw or immerse into water
- Heat to more than 100°C (212°F)
- Repair or disassemble

Dispose of the battery as required by local ordinances or regulations.

Statement 3:

CAUTION:
When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

DANGER

Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

Statement 4:

≥ 18 kg (39.7 lb)

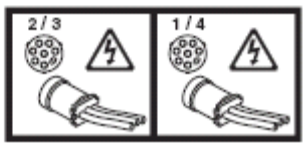
≥ 32 kg (70.5 lb)

≥ 55 kg (121.2 lb)

CAUTION:
Use safe practices when lifting.

Statement 5:

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 8:

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 12:

CAUTION:
The following label indicates a hot surface nearby.

Statement 13:

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device for electrical specifications.

Statement 20:

CAUTION:
To avoid personal injury, before lifting the unit, remove all the blades to reduce the weight.

Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

WARNING: Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. ***Lávese las manos después de usar el producto.***

Chapter 1. Introduction

The Bull novascale BL465 server is a high density, 2-node server ideally suited for virtualizated environment.

It is compatible with Bull Blade Chassis – Enterprise.

Note "Blade Chassis" is used to indicate the Bull Blade Chassis – Enterprise.

The BL465 is composed of 2 servers: a primary server and a secondary server (which will be called "node" in this guide), each server including:

- 1 system-board
- 2 multi –core Intel Xeon® microprocessors
- 16 memory-module slots
- 2 internal solid state drives (SSD)
- expansion device connectors for 1 Horizontal-compact-form-factor (CFFh) expansion card and 1 vertical-combination-I/O (CIOv) expansion card.

The primary server and the secondary server are linked with a 2-node scalability card.

The BL465 supports 4 multi-core microprocessors, 32 memory modules (DIMMS), 4 internal SSD, 2 CIOv expansion cards and 2 CFFh expansion cards.

The BL465 is able to use FlexNode partitioning. With FlexNode partitioning, you can deploy the BL465 as a single blade or as two independent servers, without having to change the physical configuration. The ability to switch between single-partition mode and stand-alone mode is provided through the management-module Web interface. For more information about FlexNode partitioning see *Working with BL465 Partitioning* on page 11.

For more information about the Management-module Web interface, see *Bull Blade Management Module User's Guide*.

This *Installation and User's Guide* provides information about:

- Setting up the blade server
- Starting and configuring the blade server
- Installing hardware options
- Installing the operating system
- Performing basic troubleshooting of the blade server

The blade server comes with a limited warranty. For information about the terms of the warranty and getting service and assistance, see the *Bull Hardware Product Warranty* document for your blade server on the *Resource DVD*. You can obtain up-to-date information about the blade server at http://www.bull.com/support.

If firmware and documentation updates are available, you can download them from http://www.bull.com/support/. The blade server might have features that are not described in the documentation that comes with the blade server, and the documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in the blade server documentation.

Record information about the blade server in the following table.

Product name	
Model number	_____
Serial number	_____

The model number and serial number are located on the ID label that is behind the control panel door on the front of the blade server, and on a label on the side of the blade server that is visible when the blade server is not in the Blade Chassis.

Note The illustrations in this document might differ slightly from the hardware.

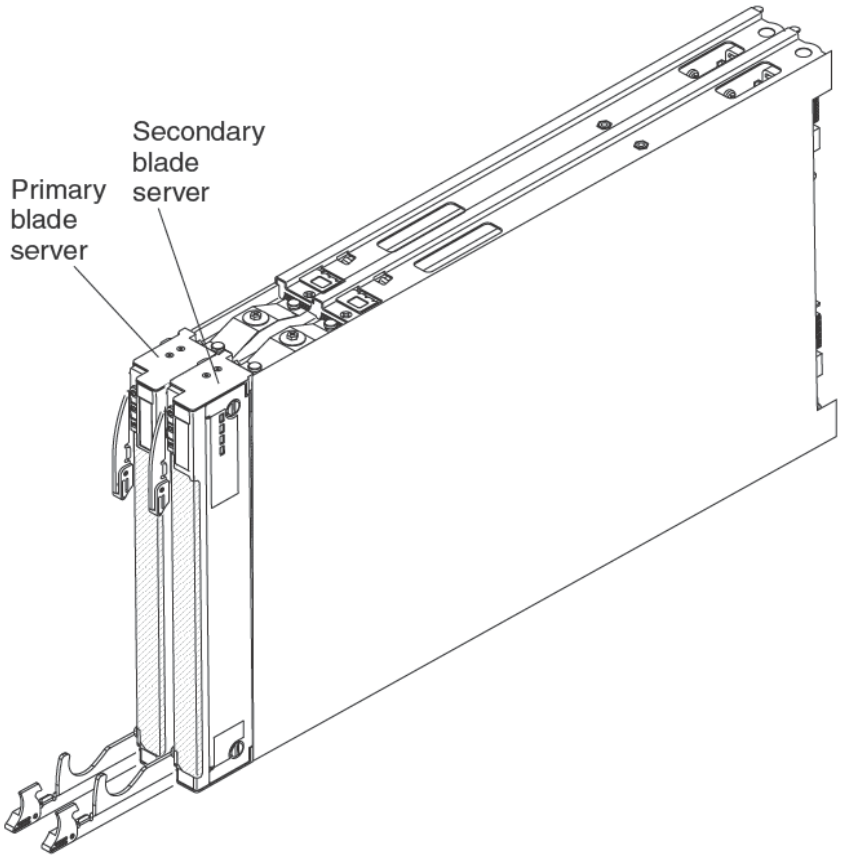


Figure 1-1. Blade server

A set of blank labels comes with the blade server. When you install the blade server in the Blade Chassis, write identifying information on a label and place the label on the Blade Chassis bezel. See the documentation for your Blade Chassis for recommended label placement.

Important

Do not place the label on the blade server itself or in any way block the ventilation holes on the blade server.

1.1 Related documentation

This *Installation and User's Guide* contains general information about the blade server, including how to install supported optional devices and how to configure the blade server. The following documentation also comes with the blade server:

Problem Determination and Service Guide

This document is in Portable Document Format (PDF) on the *Resource DVD*. It contains information to help you solve problems yourself, and it contains information for service technicians.

Safety Information

This document is in PDF on the *Resource DVD*. It contains translated caution and danger statements. Each caution and danger statement that appears in the documentation has a number that you can use to locate the corresponding statement in your language in the *Safety Attention* document.

Bull Hardware Product Warranty

This document is in PDF on the *Resource DVD*. It contains information about the terms of the warranty and getting service and assistance. Depending on your Blade product, additional documents might be included on the *Resource DVD*.

In addition to the documentation in this library, be sure to review the *Bull Blade Planning and Installation Guide* for your Blade Chassis for information to help you prepare for system installation and configuration.

1.2 Notices and statements in this document

The caution and danger statements that appear in this document are also in the multilingual *Safety Attention* document, which is on the *Resource DVD*. Each statement is numbered for reference to the corresponding statement in the *Safety Attention* document.

The following types of notices and statements are used in this document:

Note These notices provide important tips, guidance, or advice.

mportant:
These notices provide information or advice that might help you avoid inconvenient or problem situations.

Attention:
These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

CAUTION:
These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.

DANGER:
These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure, step, or situation.

1.3 Features and specifications

The following table provides a summary of the features and specifications of the blade server.

Notes

- Power, cooling, removable-media drives, external ports, and advanced system management are provided by the Blade Chassis.
- The operating system in the blade server must provide USB support for the blade server to recognize and use the removable-media drives and front-panel USB ports. The Blade Chassis uses USB for internal communications with these devices.

Blade server features and specifications
Microprocessor: Supports up to four multi-core Intel Xeon processors. **Note:** Use the Setup Utility to determine the type and speed of the microprocessors in your blade server.
Memory: • 32 dual inline memory module(DIMM) connectors. • Type: Very Low Profile (VLP) double-data rate (DDR3) DRAM. • Supports 2 GB, 4 GB, and 8 GB DIMMs with up to 256 GB of total memory on the system board.
Drives: Supports up to four solid state drives (SSD).
Predictive Failure Analysis® (PFA) alerts: • Microprocessor • Memory
Electrical input: 12 V dc
Integrated functions: • Horizontal-compact-form-factor (CFFh) expansion card interface • Vertical-combination-I/O (CIOv) expansion card interface • Local service processor: Integrated Management Module (IMM) with Intelligent Platform Management Interface (IPMI) firmware • Vitesse VSC452 iBMC controller • Integrated Matrox G200e-V video controller • LSI 1064E Serial Attached SCSI (SAS) controller • Broadcom BCM5709S dual-port Gigabit Ethernet controller • Integrated keyboard/video/mouse (cKVM) controller through IMM • Light path diagnostics • RS-485 interface for communication with the management module • Automatic server restart (ASR) • Serial over LAN (SOL) • Wake on LAN (WOL) • Redundant buses for communication with keyboard, mouse, and removable media drives • USB 2.0 for communication with the cKVM and removable media drives (an external USB port is not supported)

Size: • Height: 24.5 cm (9.7 inches) (6U) • Depth: 44.6 cm (17.6 inches) • Width: 5.8 cm (2.28 inches) • Maximum weight: 11.23 kg (24.76 lb.)
Environment (non-NEBS): • Air temperature: – Blade server on: 10° to 35° C (50° to 95° F). Altitude: 0 to 914.4 m (0 to 3000 ft) – Blade server on: 10° to 32° C (50° to 89.6° F). Altitude: 914.4 to 2133.6 m (3000 to 7000 ft) – Blade server off: 10° to 43° C (50° to 109.4° F). Altitude: 914.4 to 2133.6 m (3000 to 7000 ft) – Blade server shipping: -40° to 60° C (-40° to 140° F) • Humidity: – Blade server on: 8% to 80% – Blade server off: 8% to 80% – Blade server storage: 5% to 80% – Blade server shipment: 5% to 100% • Particulate contamination: **Attention**: Airborne particulates and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the server. For information about the limits for particulates and gases, see "*Particulate contamination*" on page 84.

Table 1-1. Blade server features and specifications

1.4 What your blade server offers

Your blade server offers features, such as the integrated management module, storage disk drive support, microprocessor technology, integrated network support, I/O expansion, large system-memory capacity, light path diagnostics LEDs, PCI Express®, and power throttling.

- **Integrated Management Module (IMM)**

  The integrated management module (IMM) combines service processor functions, video controller, the remote presence, and blue-screen capture features in a single chip. The IMM provides advanced service-processor control, monitoring, and alerting function. If an environmental condition exceeds a threshold or if a system component fails, the IMM lights LEDs to help you diagnose the problem, records the error in the IMM event log, and alerts you to the problem.

  Optionally, the IMM also provides a virtual presence capability for remote server management capabilities. The IMM provides remove server management through industry-standard interfaces:
  - Intelligent Platform Management Interface (IPMI) version 2.0
  - Simple Network Management Protocol (SNMP) version 3.0
  - Common Information Model (CIM)
  - Web browser.

  For more information, see Chapter 6, *Accessing the IMM* on page 75.

- **Dynamic System Analysis (DSA)**

  Dynamic Systems Analysis (DSA) collects and analyses system information to aid in diagnosing server problems. DSA collects the following information about the server:
  - Drive health information
  - Event logs for ServeRAID controllers and service processors
  - Hardware inventory, including PCI and USB information
  - Installed applications and hot fixes
  - Kernel modules
  - Light path diagnostics status
  - Network interface and settings
  - Performance data and details about processes that are running
  - RAID and controller configuration
  - Service processor (integrated management module) status and configuration
  - System configuration
  - Vital product data and firmware information

  DSA creates a DSA log, which is a chronologically ordered merge of the system-event log (as the IPMI event log), the integrated management module (IMM) chassis-event log (as the ASM event log), and the operating-system event logs. You can send the DSA log as a file to Bull service or view the information as a text file or HTML file.

  For more information, see the Problem Determination and Service Guide.

- **Hard disk drive support**

  The blade server supports up to four solid state drives (SSDs). You can implement RAID 0 or RAID 1 for the SSDs..

- **Microprocessor technology**
  The blade server supports up to four multi-core Intel Xeon microprocessors. For more information about supported microprocessors and their part numbers, see the *Problem Determination and Service Guide*.

  Note The optional microprocessors that Bull supports are limited by the capacity and capability of the server. Any microprocessors that you install must have the same specifications as the microprocessors that came with the servers.

- **Integrated network support**
  The blade server comes with two integrated Broadcom 5709S dual-port Gigabit Ethernet controller, which support connection to a 10 Mbps, 100 Mbps, or 1000 Mbps network through an Ethernet-compatible switch module in the Blade Chassis. The controller supports Wake on LAN® technology.

- **I/O expansion**
  The blade server has connectors on the system board for optional expansion cards for adding more network communication capabilities to the blade server.

- **Large system memory capacity**
  The blade server system board supports up to 256 GB of system memory. The memory controller provides support for up to thirty two (32) industry-standard registered ECC DDR3 on Very Low Profile (VLP) form factor DIMMs installed on the system board.

- **Light path diagnostics**
  Light path diagnostics provides light-emitting diodes (LEDs) to help you diagnose problems. For more information, see the *Problem Determination and Service Guide*.

- **PCI Express**
  PCI Express is a serial interface that is used for chip-to-chip interconnect and expansion adapter interconnect. With the blade expansion connector you can add optional I/O and storage devices.

- **Power throttling**
  Each blade server is powered by four Enterprise Voltage Regulator-Down (EVRD) 11.0 voltage regulators. By enforcing a power policy known as power-domain oversubscription, the Blade Chassis can share the power load between two power modules to ensure sufficient power for each device in the Blade Chassis. This policy is enforced when the initial power is applied to the Blade Chassis or when a blade server is inserted into the Blade Chassis.

  The following settings for this policy are available:
  - Redundant without performance impact
  - Redundant with performance impact
  - Nonredundant

  You can configure and monitor the power environment by using the management module. For more information about configuring and using power throttling, see the management-module documentation.

1.5 Reliability, availability, and serviceability features

Three of the most important features in server design are reliability, availability, and serviceability (RAS). These RAS features help to ensure the integrity of the data that is stored in the blade server, the availability of the blade server when you need it, and the ease with which you can diagnose and correct problems.

The blade server has the following RAS features:

- Customer upgrade of Flash ROM-resident code and diagnostics
- Power Policy 24-hour support center
- VPD on Memory
- Processor presence detect
- Advanced Configuration and Power Interface (ACPI)
- Automatic server restart (ASR)
- Built-in diagnostics using DSA Preboot, which is stored in integrated USB memory.
- Built-in monitoring for temperature, voltage, hard disk drives.
- Customer-upgradeable Unified Extensible Firmware Interface (UEFI) code and diagnostics
- ECC protection on the L2 cache
- Error codes and messages
- Integrated Management Module (IMM)
- Light path diagnostics feature
- Memory parity testing
- Registered ECC DDR3 memory
- Microprocessor built-in self-test (BIST) during power-on self-test (POST)
- Microprocessor serial number access
- PCI-PMI 2.2
- PCI Express 1.0a
- POST
- ROM resident diagnostics
- Service processor that communicates with the management module to enable remote blade server management
- System error logging
- Wake on LAN© capability
- Wake on PCI (PME) capability
- Wake on USB 2.0 capability

1.6 Major components of the blade server

You must remove the blade server from the Blade Chassis and remove the cover to access the components.

The following illustration shows the major components of the blade server.

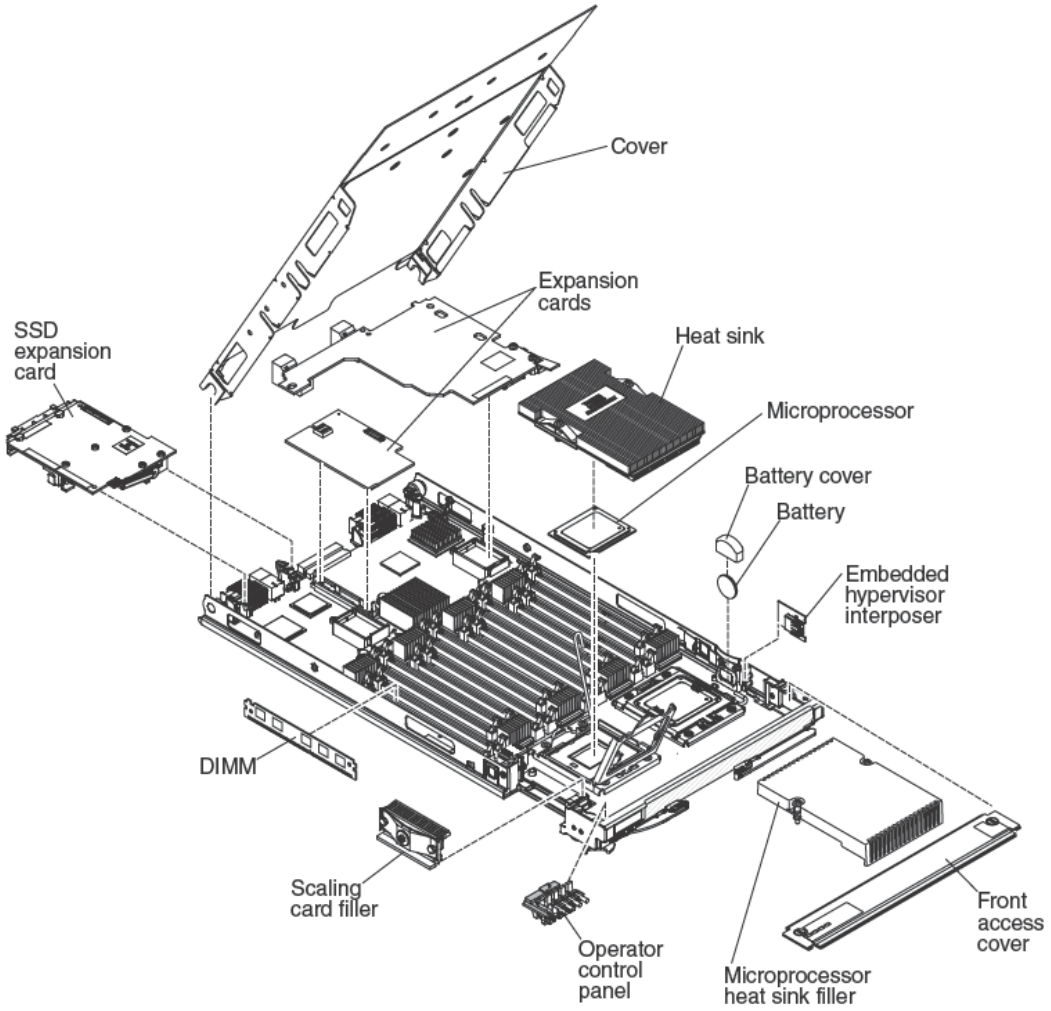
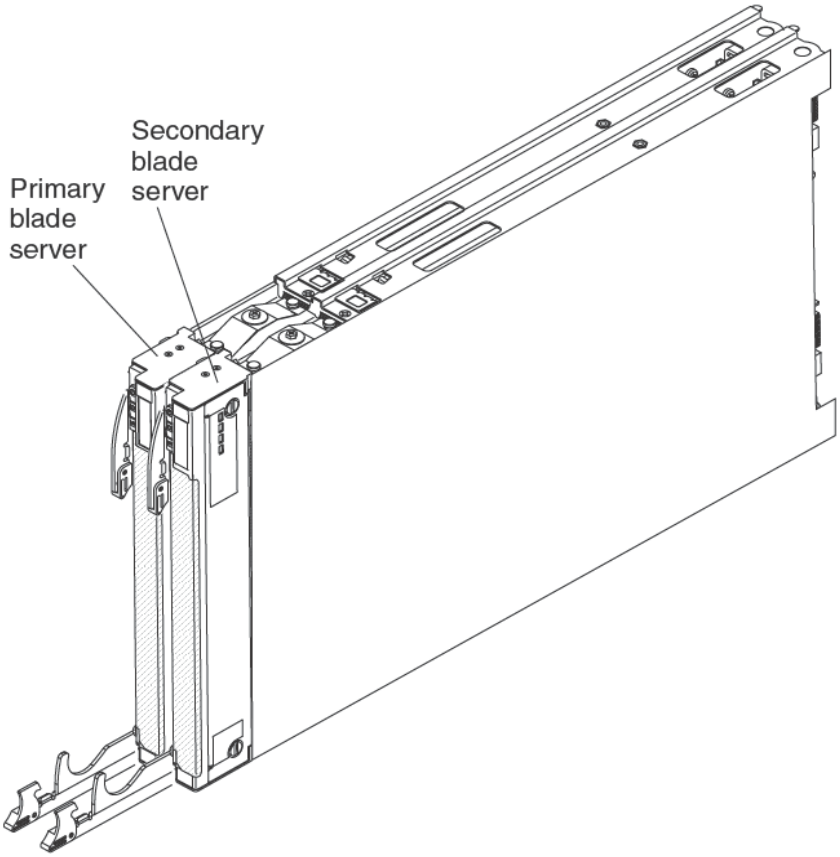


Figure 1-2. Major blade server components

1.7 Working with BL465 Partitioning

The novascale Blade BL465 supports the following implementation modes:

- **Single partition**. The complex functions as a single server that contains up to four multi-core processors and up to 32 DIMMs. When the complex is implemented as a single hardware partition, the leftmost blade server (as installed in a Blade chassis) is called the primary blade server. The blade server on the right is called the secondary blade server.



- **Stand-alone mode**. The blade servers operate independently.

Important

If you install the primary blade server in blade server bay 7 of the chassis, the secondary blade server is installed in blade server bay 8, which means that the primary blade server receives power from power domain 1 of the chassis and the secondary blade server receives power from power domain 2 of the chassis. The following situations can occur if there is a power loss to either power domain, depending on how the BL465 is implemented:

- If the BL465 is implemented in single partition mode, a loss of power to power domain 1 or power domain 2 will result in both servers in the blade going down.
- If the BL465 is implemented in stand-alone mode, a loss of power to power domain 1 will result in the entire blade going down. A loss of power to power domain 2 will result in the blade server installed in blade server bay 8 going down, but the blade server installed in blade server bay 7 will continue to function

With FlexNode processing, you can toggle between single partition mode and stand-alone mode without having to modify the physical setup of the blade servers. To toggle between modes, use the advanced management module Web interface.

For example, assume that you have created a BL465 and defined that server as a single partition through the advanced management module Web interface:

- You can toggle the BL465 to stand-alone mode through the Web interface. In stand-alone mode, you can install a different operating system on each blade server and run different applications on each blade server.
- Then, you can toggle the BL654 back to a single partition and run applications that take advantage to up to 4 processors and 32 DIMMs. The operating system that is in use is the operating system of the primary blade server.
- Later, you can toggle the BL654 back to stand-alone mode again to gain access to the operating system on the secondary blade server.

1.7.1 Single Partition Mode Considerations

The following considerations apply to the BL465 that operates as a single hardware partition:

- All UEFI settings (set through the Setup utility) should be the same on both blade slots. If they are not, the settings that are defined for the primary blade server replace the UEFI settings on the secondary server.

  Note When you upgrade the firmware for the blade servers operating in single partition mode, you only have to upgrade the primary blade server. The firmware on the secondary blade server is automatically updated. See *Using the Setup Utility* on page 60 for more information about the Setup utility.

- The primary blade server has access to the SSDs on the secondary blade server. However, the SSDs on the primary blade server cannot be combined with the SSDs on the secondary blade server to form a single RAID array. RAID arrays can be formed only using the SSDs within a blade server.

- The primary blade server has access to any I/O expansion cards that are installed in the secondary blade server. However, the I/O expansion cards in the secondary blade server cannot be used for a Serial Over LAN connection.
- If you press the power button on one blade server, both blade servers in the partition either power up or power down, depending on the state of the blade servers when you press the power button.

Chapter 2. Power, controls and indicators

This chapter describes the power features, how to turn on and turn off the blade server, and what the controls and indicators mean. This chapter also identifies the system-board connectors.

2.1 Turning on the blade server

After you connect the BL465 to power through the Blade chassis, the blade server can be started in any of the following ways:

- You can press the power-control button on the front of the BL465 (see *Blade server controls and LEDs* on page 16) to start the blade server. The power button works only if local power control is enabled for the blade server. Local power control is enabled and disabled through the advanced management module web interface.

  Notes

  - Wait until the power-on LED on the BL465 flashes slowly before you press the power button. While the service processor in the blade server is initializing and synchronizing with the management module, the power-on LED flashes rapidly, and the power-control button on the blade server does not respond. This process can take approximately 90 seconds after the blade server has been installed.
  - While the blade server is starting, the power LED on the front of the blade server is lit and does not flash. See *Blade server controls and LEDs* on page 16 for the power-on LED states.

- If a power failure occurs, the Blade chassis and the blade server can be configured to start automatically when power is restored through the management module.
- You can turn on the BL465 through the advanced management module Web interface. For more information about the advanced management module Web interface, see the *Bull Management Module User's Guide*.
- You can turn on the BL465 through the Wake on LAN feature. The blade server must be connected to power (the power-on LED is flashing slowly), the blade server must be communicating with the advanced management module, the operating system must support the Wake on LAN feature, and the Wake on LAN feature must be enabled through the advanced management module interface.

2.2 Turning off the blade server

When you turn off the BL465, it is still connected to power through the Blade chassis. The blade server can respond to requests from the service processor, such as a remote request to turn on the blade server. To remove all power from the blade server, you must remove it from the Blade chassis.

Before you turn off the blade server, you should shut down the operating system. See the operating-system documentation for information about shutting down the operating system.

The blade server can be turned off in any of the following ways:

- You can press the power-control button on the blade server, see *Blade server controls and LEDs* on page *16*). This starts an orderly shutdown of the operating system, if this feature is supported by the operating system.
- If the operating system stops functioning, you can press and hold the power-control button for more than 4 seconds to turn off the blade server.
  Attention: Pressing the button for 4 seconds forces the operating system to shut down immediately. Data loss is possible.
- The management module can turn off the blade server through the management-module Web interface.
  For additional information, see the *Bull Advanced Management Module User's Guide*.

2.3 Blade server controls and LEDs

This section describes the controls and LEDs on the blade server.

The following illustration identifies the buttons and LEDs on the BL465 control panel.

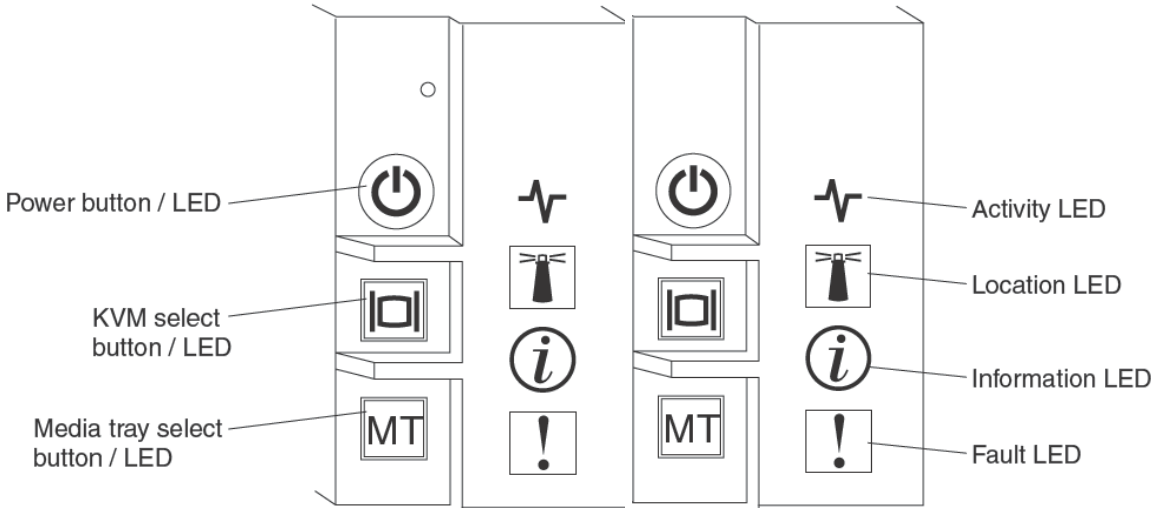


Figure 2-1. Blade server controls and LEDs

Power button/LED:

When the blade server has power, press this button to turn on or turn off the blade server.

Note The power button works only if local power control is enabled for the blade server. Local power control is enabled and disabled through the advanced management module Web interface.

After the blade server is removed from the chassis, press this button to activate the system board LEDs (light path diagnostics). See System-board LEDs for more information.

This button is also the power LED. This green LED indicates the power status of the blade server:

- **Flashing rapidly**: The LED flashes rapidly for one of the following reasons:
  - The blade server has been installed in a chassis. When you install the blade server, the LED flashes rapidly for up to 90 seconds while the integrated management module (IMM) on the blade server is initializing and synchronizing with the advanced management module.
  - The blade server does not have power permissions assigned to it through the management module.
  - The Blade chassis does not have enough power to turn on the blade server.
  - The IMM on the blade server is not communicating with the management module.
- **Flashing slowly**: The blade server has power and is ready to be turned on.
- **Lit continuously**: The blade server has power and is turned on.

When the blade server is on, pressing this button causes an orderly shutdown of the blade server so that it is safe to remove. This includes shutting down the operating system (if possible) and removing power from the blade server.

Note If you press the power button on the blade server that is part of a BL465 running as a single partition, both blade servers in the partition power on or shut down.

If an operating system is running, you might have to press the button for approximately 4 seconds to initiate the shutdown.

WARNING
Pressing the button for 4 seconds forces the operating system to shut down immediately. Data loss is possible.

KVM select button/LED:

Press this button to associate the shared Blade Chassis keyboard, video, and mouse (KVM) ports with the blade server. The LED on this button flashes while the request is being processed, and then is lit when the ownership of the keyboard, video, and mouse has been transferred to the blade server. It can take approximately 20 seconds to switch the keyboard, video, and mouse control to the blade server.

Using a keyboard that is directly attached to the management-module, you can press keyboard keys in the following sequence to switch KVM control between blade servers instead of using the KVM select button:

NumLock NumLock *blade_server_number* Enter

Where *blade_server_number* is the two-digit number for the blade bay in which the blade server is installed. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies.

If there is no response when you press the KVM select button, you can use the management-module Web interface to determine whether local control has been disabled on the blade server.

Notes

- The operating system in the blade server must provide USB support for the blade server to recognize and use the keyboard and mouse, even if the keyboard and mouse have PS/2-style connectors.
- If you install a supported Microsoft Windows operating system on the blade server while it is not the current owner of the keyboard, video, and mouse, a delay of up to 1 minute occurs the first time that you switch the keyboard, video, and mouse to the blade server. All subsequent switching takes place in the normal KVM switching time frame (up to 20 seconds).

Media-tray select button:

Press this button to associate the shared Blade Chassis media tray (removable-media drives) with the blade server. The LED on the button flashes while the request is being processed, and then is lit when the ownership of the media tray has been transferred to the blade server. It can take approximately 20 seconds for the operating system in the blade server to recognize the media tray.

If there is no response when you press the media-tray select button, you can use the management-module Web interface to determine whether local control has been disabled on the blade server.

Activity LED:

When this green LED is lit (flashing), it indicates that there is activity on the hard disk drive, external storage device, or network.

Location LED:

The system administrator can remotely turn on this blue LED to aid in visually locating the blade server. When this LED is lit, the location LED on the Blade Chassis unit is also lit. The location LED can be turned off through the management-module Web interface.

Information LED:

When this amber LED is lit, it indicates that information about a system event in the blade server has been placed in the advanced management module event log. For example, this LED can be lit for any of the following conditions:

- An attempt was made to power on the blade server but was denied permission.
- There is an invalid processor configuration on a multi-node system.
- Memory is not populated according to the recommended installation order.

The information LED can be turned off through the management module Web interface.

Fault LED:

When this amber LED is lit, it indicates that a system error has occurred in the blade server. In addition, the fault LED on the chassis system LED panel is lit.

The fault LED turns off only after the error is corrected.

Note When the fault LED turns off, you should also clear the IMM event log. Use the Setup utility to clear the IMM event log

2.4 Scalability indicators

The BL465 blade server provides scalability indicators, which are viewable through the front bezel of the blade server when it is installed in a Blade chassis. The scalability indicators remain lit until the blade server is started.

The BL465 can operate as a single hardware partition or can operate in stand-alone mode.

The scalability indicators show whether a BL465 blade server is operating as a single hardware partition.

When a BL465 blade server is operating in single partition mode, the scalability indicators move up the first server, cross over to the second server, and then move down the second blade server.

Note If you have set up a BL465 in single partition mode but when you start the blade servers, the scalability indicators for each node seem to be operating independently, there might be a problem with the configuration of the BL465.

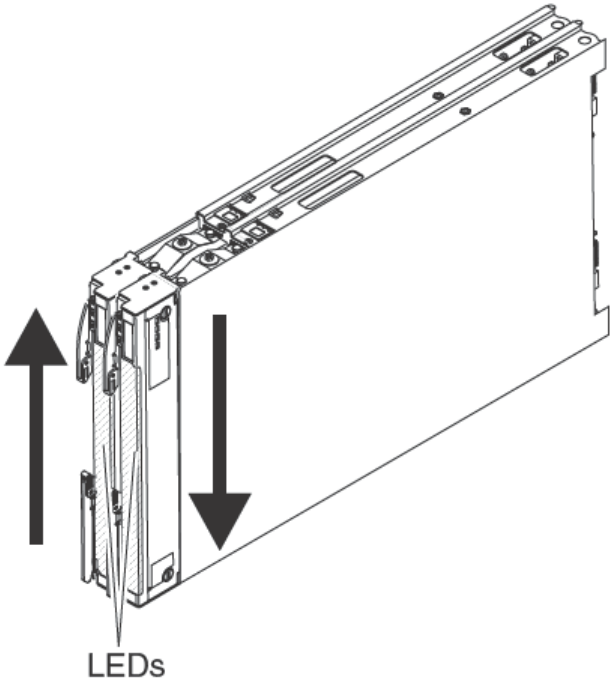


Figure 2-2. Blade scalability indicators

2.5 Blade server connectors

The BL465 is composed of 2 identical system boards.

The following illustration shows the system board components, including connectors for user-installable optional devices, in the blade server.

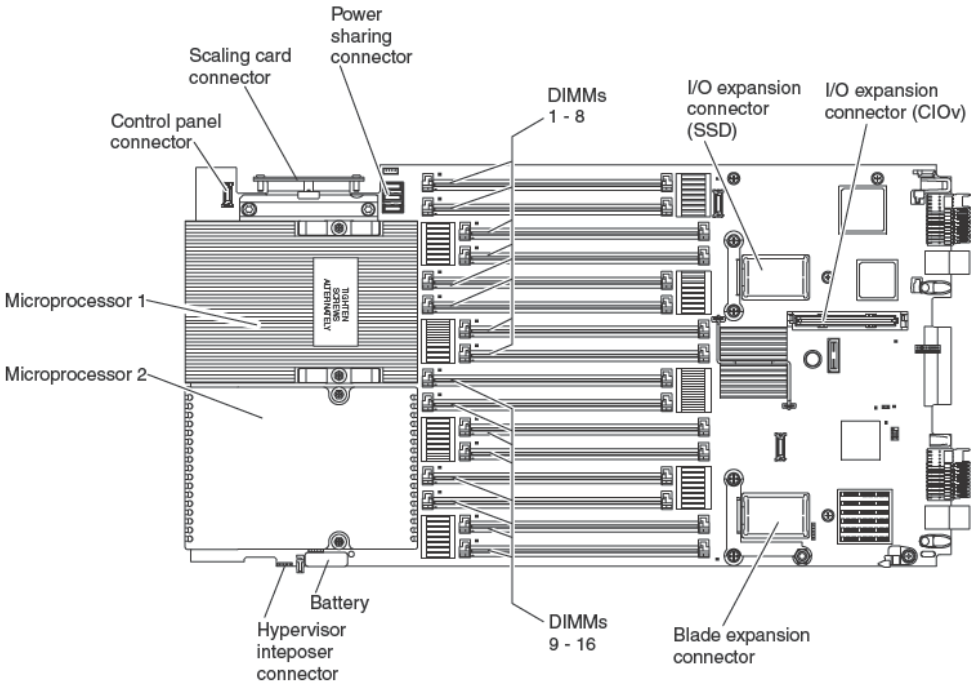


Figure 2-3. Blade server connectors

Note	The optional SSD expansion card is installed in the I/O expansion connector (SSD)

2.6 Input/Output connectors and devices

The input/output connectors that are available to the blade server are supplied by the Blade chassis. See the documentation that comes with the Blade chassis for information about the input/output connectors.

The blade server has two selection buttons on the control panel: the media tray select button and the keyboard/video/mouse select button. See *Blade server controls and LEDs* on page 16 for information about these buttons and their functions.

The Ethernet controllers on the blade server communicate with the network through the Ethernet-compatible I/O modules in the Blade chassis. Network signals to and from the blade server or any expansion cards are automatically routed to a same-network-interface I/O module through circuitry in the Blade chassis.

Chapter 3. Installing Options

This chapter provides instructions for installing optional hardware devices in the blade server. Some option-removal instructions are provided in case you have to remove one option to install another.

3.1 Installation guidelines

Before you install options, read the following information:

- Read the safety information that begins on page vii and the guidelines in *Handling static-sensitive devices* on page 24. This information will help you work safely.
- When you install your new blade server, take the opportunity to download and apply the most recent firmware updates. This step will help to ensure that any known issues are addressed and that your blade server is ready to function at maximum levels of performance. To download firmware updates for your blade server, go to http://www.bull.com/support/.
- Observe good housekeeping in the area where you are working. Place removed covers and other parts in a safe place.
- Back up all important data before you make changes to disk drives.
- Before you remove a blade server from the Blade Chassis, you must shut down the operating system and turn off the blade server. You do not have to shut down the Blade Chassis itself.
- Blue on a component indicates touch points, where you can grip the component to remove it from or install it in the blade server, or open or close a latch.
- Orange on a component or an orange label on or near a component indicates that the component can be hot-swapped, which means that if the server and operating system support hot-swap capability, you can remove or install the component while the server is running. (Orange can also indicate touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.

3.1.1 System reliability guidelines

To help ensure proper cooling and system reliability, make sure that the following requirements are met:

- To ensure proper cooling, do not operate the Blade Chassis without a blade server, expansion unit, or filler blade installed in each blade bay. See the documentation for your Blade Chassis for additional information.
- Each microprocessor socket always contains either a microprocessor dust cover and heat sink filler or a microprocessor and heat sink. If the blade server has only one microprocessor, it must be installed in microprocessor socket 1.
- Each DIMM socket always contains a memory module or filler.
- Make sure that the ventilation holes on the blade server are not blocked.
- The blade server battery must be operational. If the battery becomes defective, replace it immediately. For instructions, see the *Problem Determination and Service Guide*.

3.1.2 Handling static-sensitive devices

Attention:
Static electricity can damage the blade server and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

To reduce the possibility of damage from electrostatic discharge, observe the following precautions:

- When you work on a Blade Chassis that has an electrostatic discharge (ESD) connector, use a wrist strap when you handle modules, optional devices, or blade servers. To work correctly, the wrist strap must have a good contact at both ends (touching your skin at one end and firmly connected to the ESD connector on the front or back of the Blade Chassis).
- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully, holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an *unpainted* metal part of the Blade Chassis or any *unpainted* metal surface on any other grounded rack component in the rack in which you are installing the device for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it directly into the blade server without setting it down. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on the blade server cover or on a metal surface.
- Take additional care when you handle devices during cold weather. Heating reduces indoor humidity and increases static electricity.

3.2 Removing the blade server from the Blade Chassis

The following illustration shows how to remove a blade server or a blade filler from a Blade Chassis. The appearance of your Blade Chassis might be different, see the documentation for your Blade Chassis for additional information.

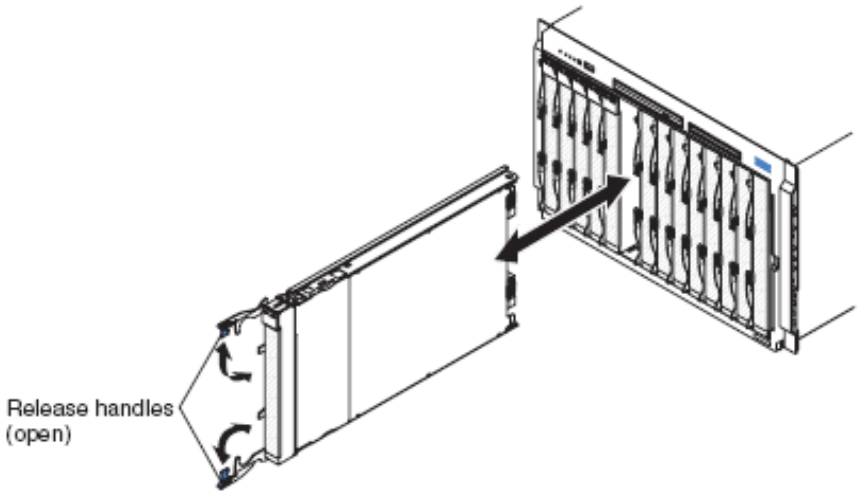


Figure 3-1. Removing the blade server from the Blade Chassis

Attention:

- To maintain proper system cooling, do not operate the Blade Chassis without a blade server, expansion unit, or blade filler installed in each blade bay.
- When you remove the blade server, note the bay number. Reinstalling a blade server into a different bay from the one it was removed from could have unintended consequences. Some configuration information and update options are established according to bay number; if you reinstall the blade server into a different bay, you might need to reconfigure the blade server.

To remove the blade server, complete the following steps:

1. If the blade server is operating, shut down the operating system; then, press the power-control button (behind the blade server control panel door) to turn off the blade server (see *Turning off the blade server* on page 16 for more information).

Attention:
If one node of the BL465 is operating in single partition mode, pressing the power button on one blade server causes both blade servers to shut down..

2. Open the two release handles as shown in the illustration. The blade server moves out of the bay approximately 0.6 cm (0.25 inch).
3. Pull the blade server out of the bay.
4. Place either a blade filler or another blade in the bay within 1 minute.

3.3 Removing the blade server cover

To open the blade server cover, complete the following steps:

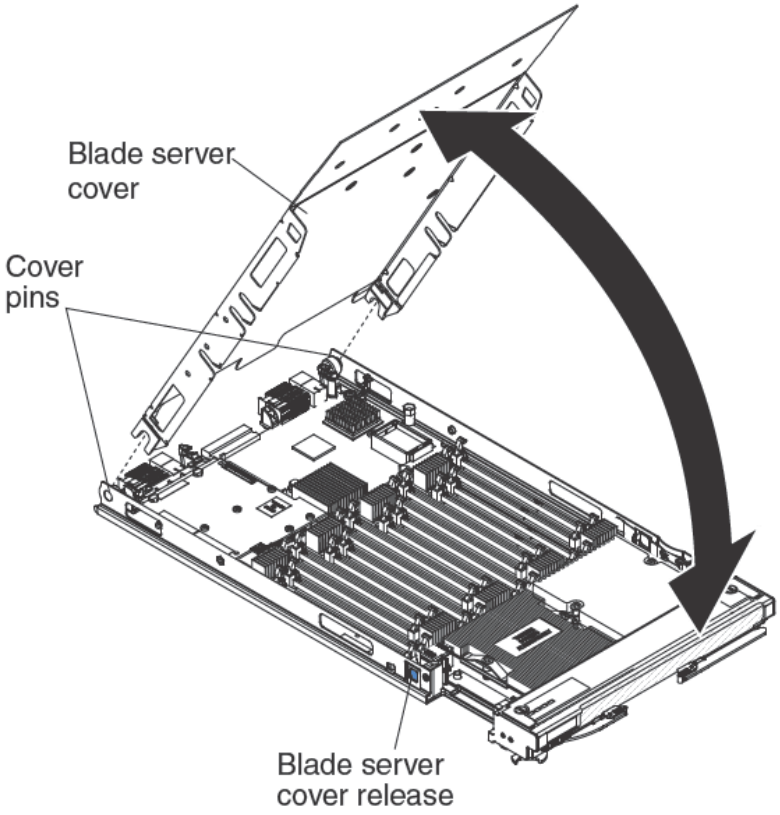


Figure 3-2. Opening the blade server cover

1. Read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25 for instructions).
3. Carefully lay the blade server on a flat, static-protective surface, with the cover side up.
4. Press the blade-cover release on each side of the blade server or expansion unit and lift the cover open, as shown in the illustration.
5. Lay the cover flat, or lift it from the blade server and store for future use.

Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

3.4 Disassembling the novascale Blade BL465

The BL465 must be disassembled to add components to each of the nodes.

Note This procedure assumes that you are disassembling a BL465 to install components in each of the modules but that you will assemble the BL465 back. If you are disassembling the BL465 to use the modules as independent, stand-alone blade servers, see the *Problem Determination and Service Guide*.

To disassemble a BL465, complete the following steps.

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Remove the cover from the topmost node (see *Removing the blade server cover* on page 26 for instructions).
3. Stand the nodes upright on a clean, flat work surface, with the 2-node scalability card facing up.
4. Release the lower handles (rotate the lower handles down) to allow the blade servers to sit flat on the work surface.

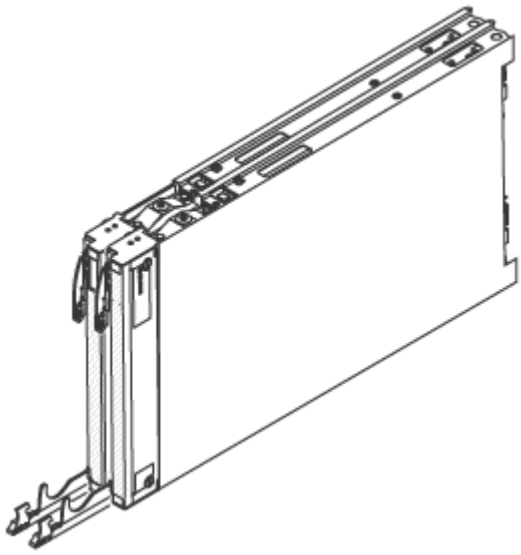


Figure 3-3. Disassembling the BL465

5. Remove the 2-node scalability card (see *Removing the 2-node scalability card* on page 29 for instructions).
6. Press the blade server cover release on each side of the blade server and lift the topmost node from the bottom node as shown in the following illustration.

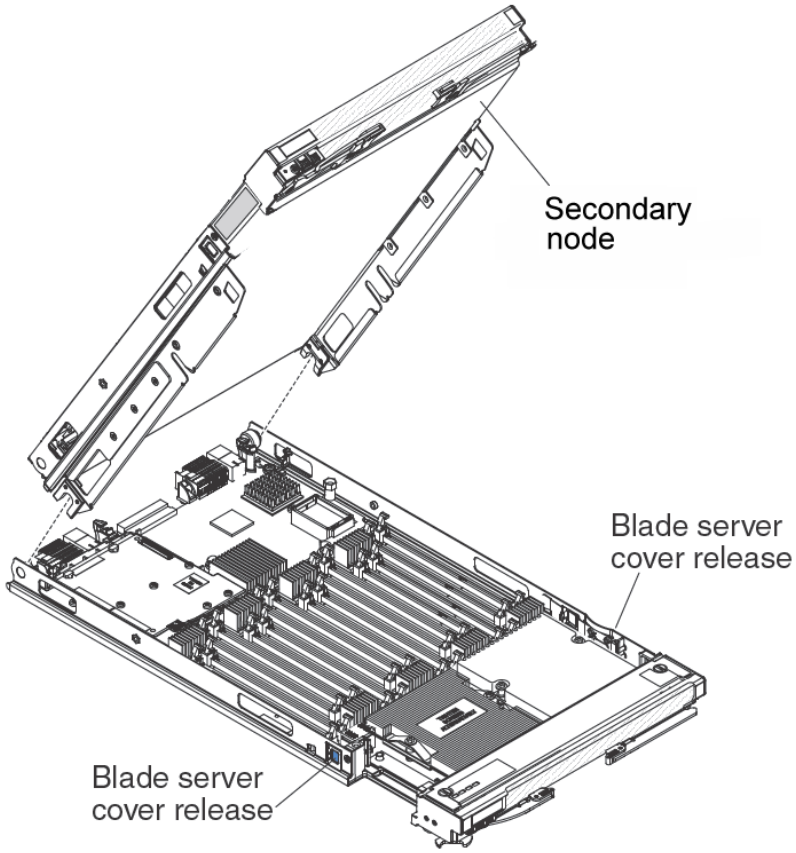


Figure 3-4. Lifting the topmost node from the bottom node

3.5 Removing the 2-node scalability card

Use this information to remove the 2-node scalability card from a blade server.

To remove the 2-node scalability card, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Loosen each screw on the 2-node scalability card, using the provided 3/16" hex driver. Alternate the loosening of each screw until both screws are removed.
3. Lift the 2-node scalability card off both blade servers and store the card in a safe place.

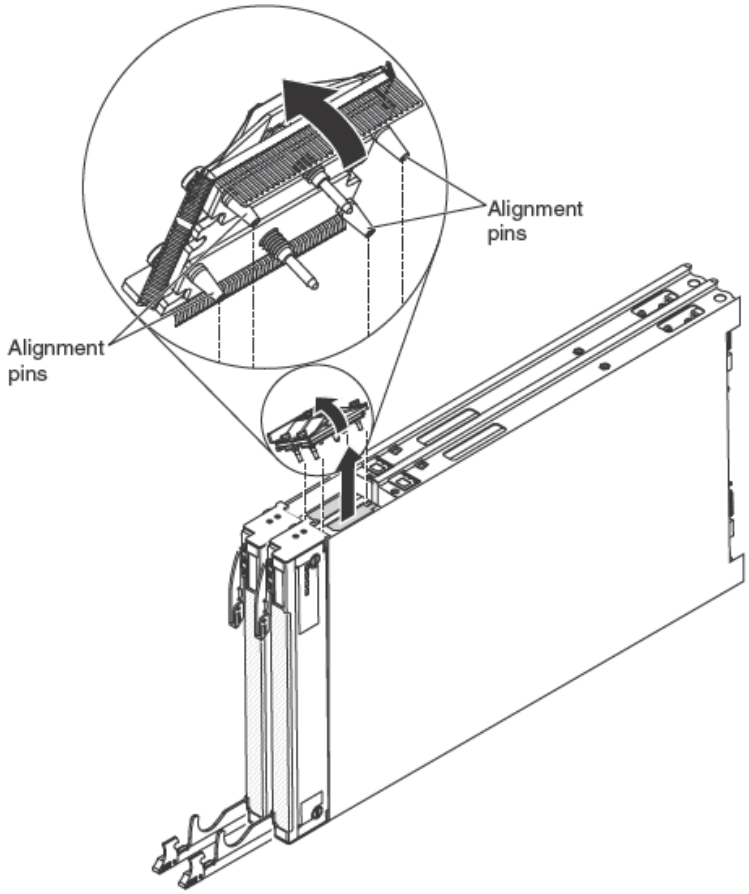


Figure 3-5. Removing the 2-node scalability card

Note When you remove the 2-node scalability card, the BL465 is no longer operational.

3.6 Installing an SSD expansion card

Use this information to install an SSD expansion card.

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If a CFFh expansion card is installed, remove it (see *Removing a CFFh expansion card* on page 47 for instructions).
3. Insert the back of the SSD expansion card into the expansion-card standoffs on the blade server and rotate the expansion card down toward the system board.

Note The expansion card standoff in the middle of the blade server has two slots. The top slot is for the CFFh expansion card. Be sure to insert the SSD expansion card into the bottom slot of the expansion-card standoff that is located in the middle of the blade server.

4. Carefully push down on the SSD expansion card (pressing on the blue label) until the expansion card is seated.

Note Make sure that the expansion card lever is in the closed position.

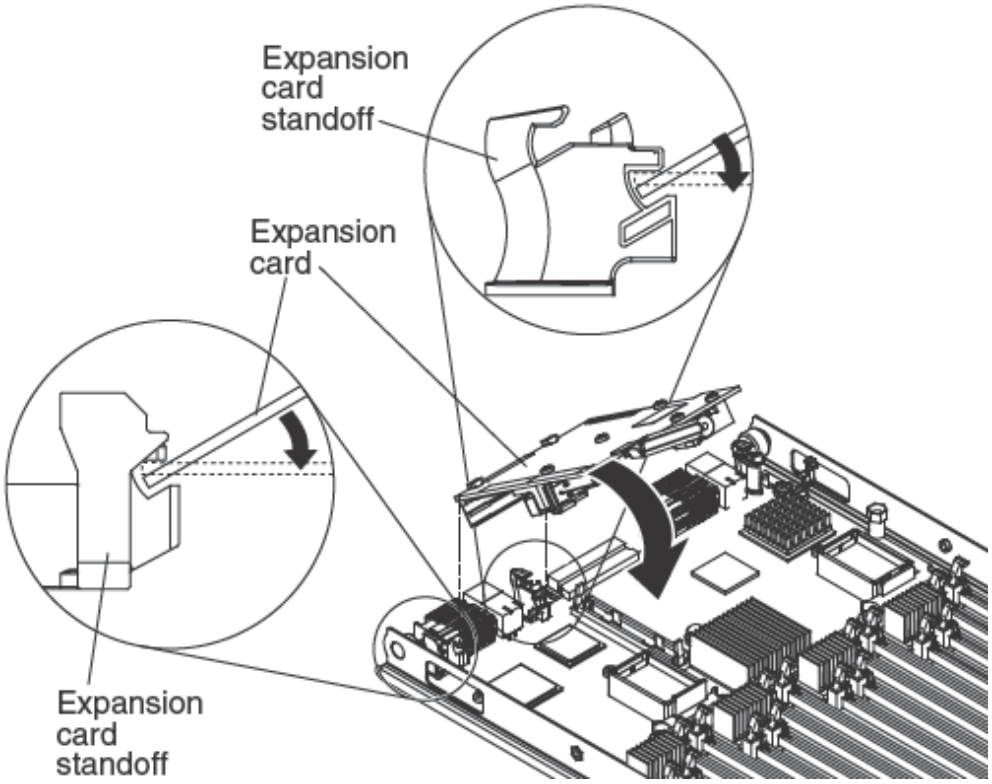


Figure 3-6. Installing an SSD expansion card

3.7 Removing an SSD expansion card

Use this information to remove an SSD expansion card.

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.

2. Locate the blue expansion card lever on the SSD expansion card and lift the lever to release the SSD expansion card from the blade expansion connector on the system board.

3. Rotate the SSD expansion card up and lift it away from the expansion-card standoffs.

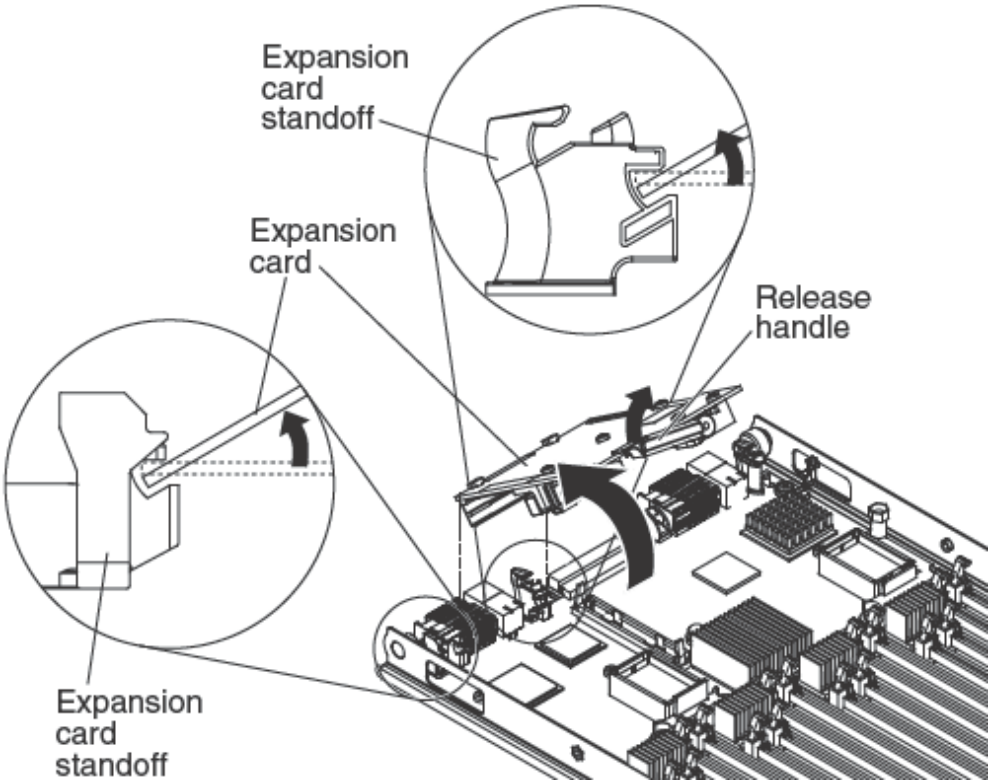


Figure 3-7. Removing an SSD expansion card

3.8 Installing a solid state drive

Use this information to install a solid state drive.

You can install up to two solid state drives in the SSD expansion card. The blade server supports using RAID 0 or RAID 1 when two storage drives are installed.

See *Using the LSI Logic Configuration Utility program* on page 71 for information about RAID configuration.

To install a solid state drive, complete the following steps:

1. Remove the SSD expansion card (see *Removing an SSD expansion card* on page 31 for instructions).
2. Turn over the SSD expansion card.

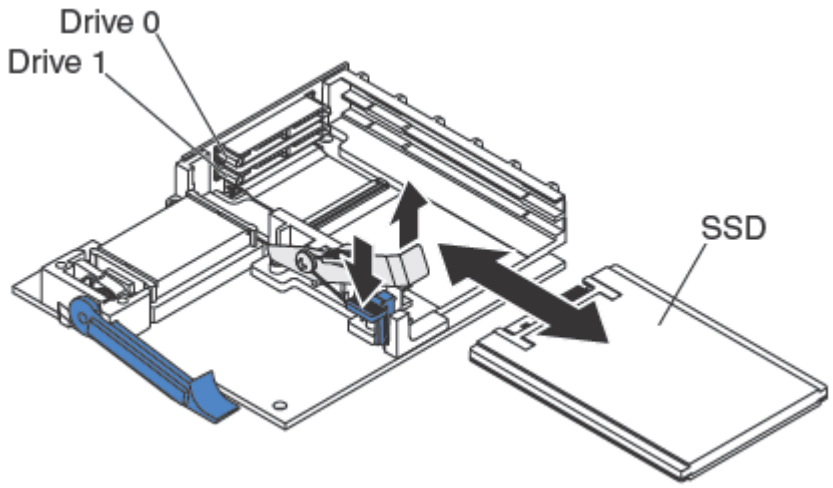


Figure 3-8. Installing a solid state drive

3. Touch the static-protective package that contains the solid state drive to any *unpainted* metal surface on the Blade chassis or any *unpainted* metal surface on any other grounded rack component; then, remove the solid state drive from the package.
4. Slide the solid state drive into the slot until it is firmly seated in the connector.
5. If you have a second solid state drive to install, repeat steps 3 and 4.
6. Close the retention lever and secure it with the blue tab.

Note You might have to press the blue tab before you close the retention lever.

7. Install the SSD expansion card (see *Installing an SSD expansion card* on page 30 for instructions).

3.9 Removing a solid state drive

Use this information to remove a solid state drive.

The blade server has a solid state drive expansion card for installing or removing solid state drives. To remove a solid state drive, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Remove the SSD expansion card (see *Removing an SSD expansion card* on page 31 for instructions).
3. Turn over the SSD expansion card.

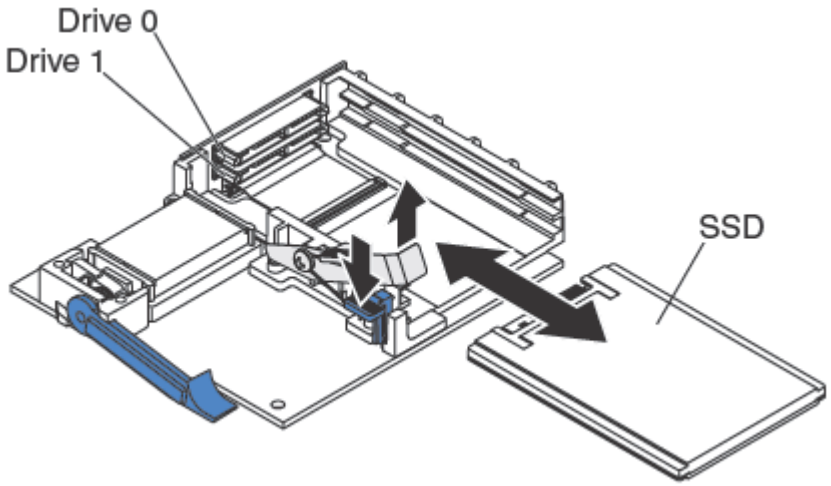


Figure 3-9. Removing a solid state drive

4. Press down on the blue tab. The retention lever automatically opens so that the solid state drive or drives are accessible.
5. Slide the solid state drive out of the slot.

Note When you remove a drive from the SSD expansion card, consider labeling the drive to indicate the slot from which the drive was removed so that you can install the drive back into the same slot.

6. Close the retention lever and secure it with the blue tab.

Note You might have to press the blue tab before you close the retention lever.

3.10 Installing a DIMM

Each node has a total of 16 direct inline memory modue (DIMM) slot. The BL465 supports very low profile (VLP) DDR3 DIMMs with error code correction (ECC) in 2 GB, 4 GB and 8 GB capacities.

Depending on the memory mode that is set in the Setup utility, each node can support a minimum of 16 GB and a maximum of 128 GB of system memory on the system board in a node of 2 processors.

Memory must be installed in pairs of DIMMs per processor installed. DIMMs must be the same size, speed, and technology within installed pairs.

The following table lists the memory configurations and installation order for each node when two processors are installed.

Installed DIMMs	DIMM Connector															
	Buffer		Buffer		Buffer		Buffer		Buffer		Buffer		Buffer		Buffer	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4 DIMMs	X			X					X			X				
6 DIMMs	X			X	X			X	X			X				
8 DIMMs	X			X	X			X	X			X	X			X
10 DIMMs	X	X	X	X	X			X	X			X	X			X
12 DIMMs	X	X	X	X	X			X	X	X	X	X	X			X
14 DIMMs	X	X	X	X	X	X	X	X	X	X	X	X	X			X
16 DIMMs	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Important

In the BL465, the DIMMs must be installed to have a balance of memory among processors. Additional memory can be installed in the top-most node of the BL465 so that you do not need to disassemble the BL465 server.
For example, if you are installing four DIMMs in a BL465, you would install two DIMMs (in sockets 1 and 4) of each node

For two processors installed in each node, memory mirroring is set up as follows in each node:

DIMM Quadrant	Mirrored Quadrant
DIMM 1, DIMM 2, DIMM 3, DIMM 4	DIMM 5, DIMM 6, DIMM 7, DIMM 8
DIMM 9, DIMM 10, DIMM 11, DIMM 12	DIMM 13, DIMM 14, DIMM 15, DIMM 16

The BL465 also supports memory sparing, in which the contents of the failing DIMM are transferred to the spare DIMM.

Note To enable memory sparing, the DIMMs installed for each processor must be identical.

For two processors installed in each node, memory sparing is set up as follows in each node:

DIMM Pair	Spare Pair
DIMM 1, DIMM 4	DIMM 2, DIMM 3
DIMM 5, DIMM 8	DIMM 6, DIMM 7,
DIMM 9, DIMM 12	DIMM 10, DIMM 11
DIMM 13, DIMM 14	DIMM 15, DIMM 16

To install a DIMM, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Read the documentation that comes with the DIMMs.
3. If the blade server is installed in a Blade Chassis unit, remove it (see *Removing the blade server from the Blade Chassis* on page 25 for instructions).
4. Carefully lay the blade server on a flat, static-protective surface.
5. Open the blade server cover (see *Removing the blade server cover* on page 26 for instructions).
6. Locate the DIMM connectors (see *Blade server connectors* on page 20). Determine which DIMM connector you will be installing memory into.
7. If another memory module is already installed in the DIMM connector, remove it (see *Removing a* on page 37).
8. Touch the static-protective package that contains the DIMM to any *unpainted* metal surface on the Blade Chassis unit or any *unpainted* metal surface on any other grounded rack component in the rack in which you are installing the DIMM for at least 2 seconds; then, remove the DIMM from its package.

9. To install the DIMMs, repeat the following steps for each DIMM that you install:

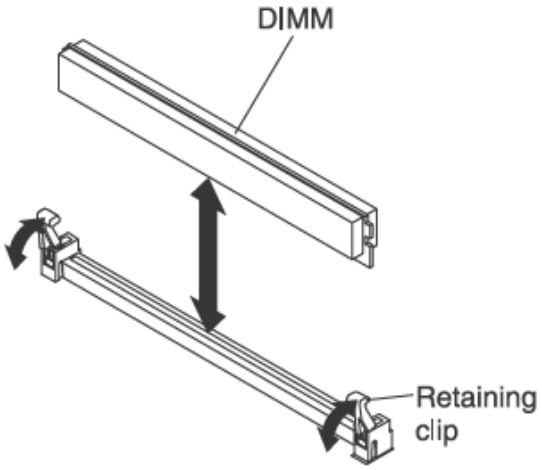


Figure 3-10. Installing a DIMM

a. Make sure that the retaining clips are in the open position, away from the center of the DIMM connector.

b. Turn the DIMM so that the DIMM keys align correctly with the connector on the system board.
Attention: To avoid breaking the retaining clips or damaging the DIMM connectors, handle the clips gently.

c. Press the DIMM into the DIMM connector. The retaining clips will lock the DIMM into the connector.

d. Make sure that the small tabs on the retaining clips are in the notches on the DIMM. If there is a gap between the DIMM and the retaining clips, the DIMM has not been correctly installed. Press the DIMM firmly into the connector, and then press the retaining clips toward the DIMM until the tabs are fully seated. When the DIMM is correctly installed, the retaining clips are parallel to the sides of the DIMM.

3.11 Removing a DIMM

Use this information to remove a dual inline memory module (DIMM) from the blade server.

The following illustration shows how to remove a DIMM from the blade server.

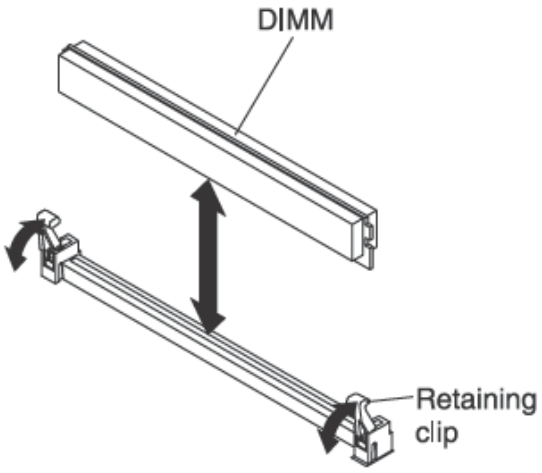


Figure 3-11. Removing a DIMM

To remove a DIMM, complete the following steps:

1. Read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25).
3. Open the blade server cover (see *Removing the blade server cover* on page 26).
4. Locate the DIMM connectors (see *Blade server connectors* on page 20). Determine which DIMM you want to remove from the blade server.

   Attention: To avoid breaking the retaining clips or damaging the DIMM connectors, handle the clips gently.
5. Move the retaining clips on the ends of the DIMM connector to the open position by pressing the retaining clips away from the center of the DIMM connector.
6. Using your fingers, pull the DIMM out of the connector.

3.12 Installing a hypervisor key

Use these instructions to install a hypervisor key in the blade server.

If you are using the BL465 blade server in a virtualized environment, you might have to install a hypervisor key, depending on the virtualization software that you are using. If it is configured as a single hardware partition, install the hypervisor key in the bottom (left) node in the BL465.

If in the BL465 the two nodes are operating independently, you might have to install a hypervisor key in each node. To determine whether you need a hypervisor key, see the documentation that comes with your virtualization software.

The following illustration shows the installation of the hypervisor key.

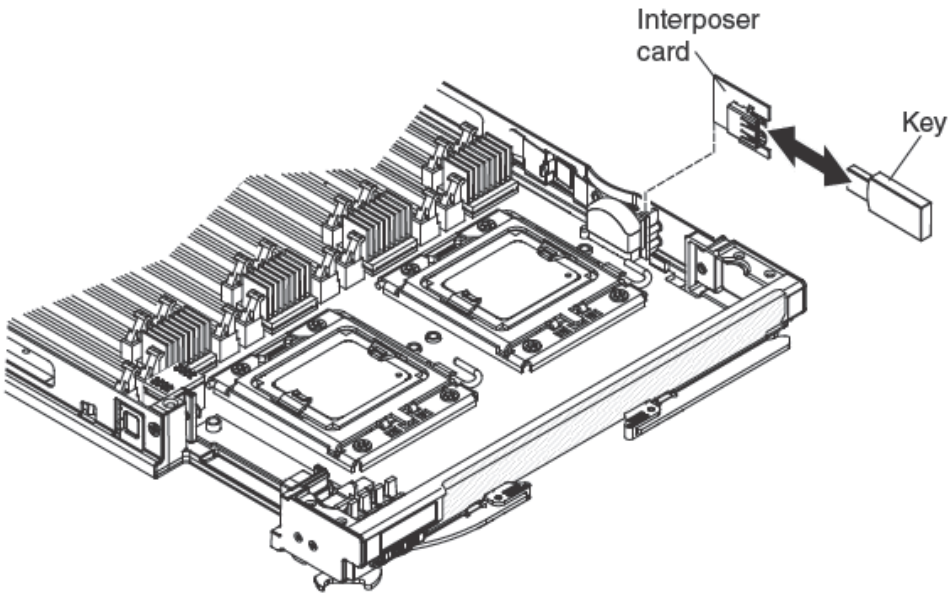


Figure 3-12. Installing a hypervisor key

To install a hypervisor key, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25 for instructions).
3. Carefully lay the blade server on a flat, static-protective surface.
4. Open the blade server cover (see *Removing the blade server cover* on page 26 for instructions).

5. Remove the access panel:

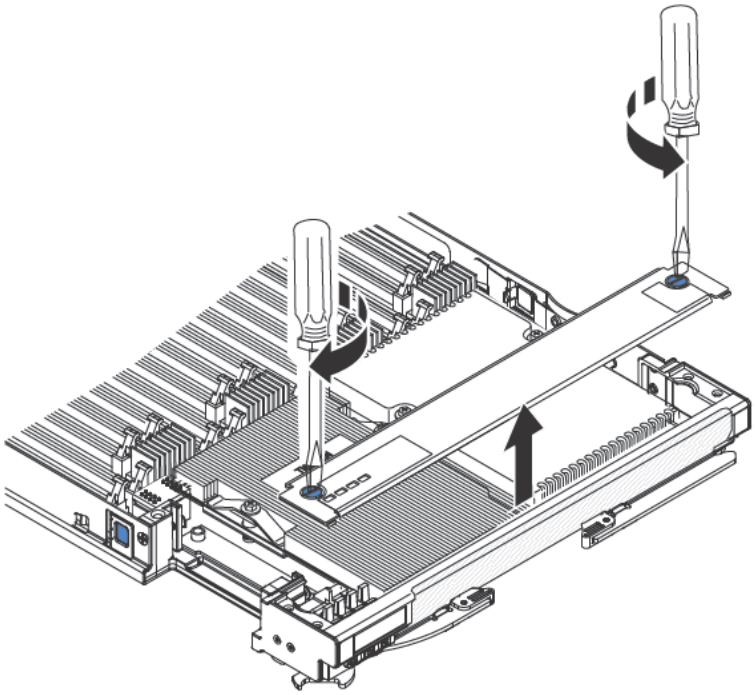


Figure 3-13. Removing the access panel

   a. Using a screwdriver or a coin, turn each of the screws toward the middle of the blade server until they are in the unlocked position.

   b. b. While you lift the back of the access panel, slide the panel away from the bezel.

6. Remove the hypervisor interposer:

   a. Locate the hypervisor interposer on the system board (see *Major components of the blade server* on page 10).

   b. Press down on the front edge of the hypervisor interposer to disengage the hypervisor interposer from the hypervisor interposer card guide.

   c. Carefully lift the hypervisor interposer up from the system board.

7. Touch the static-protective package that contains the hypervisor key to any *unpainted* metal surface on the Blade Chassis or any *unpainted* metal surface on any other grounded rack component for at least 2 seconds, then remove the hypervisor key from its static-protective package.

8. Install the hypervisor key into the hypervisor adapter:

   a. Orient the connector on the hypervisor key with the connector on the hypervisor adapter.

   b. Use your fingers to push the hypervisor key into the hypervisor adapter.

9. Install the hypervisor adapter:
    a. Orient the connector on the hypervisor interposer with the interposer connector on the system board, aligning the pins on the side of the hypervisor interposer with the pinholes on the interposer connector (see “Blade server connectors” on page 20).
    b. Use your fingers to push the adapter into the connector on the blade server. **Attention:** Be careful not to damage the pins on the hypervisor interposer.
10. Install the access panel:

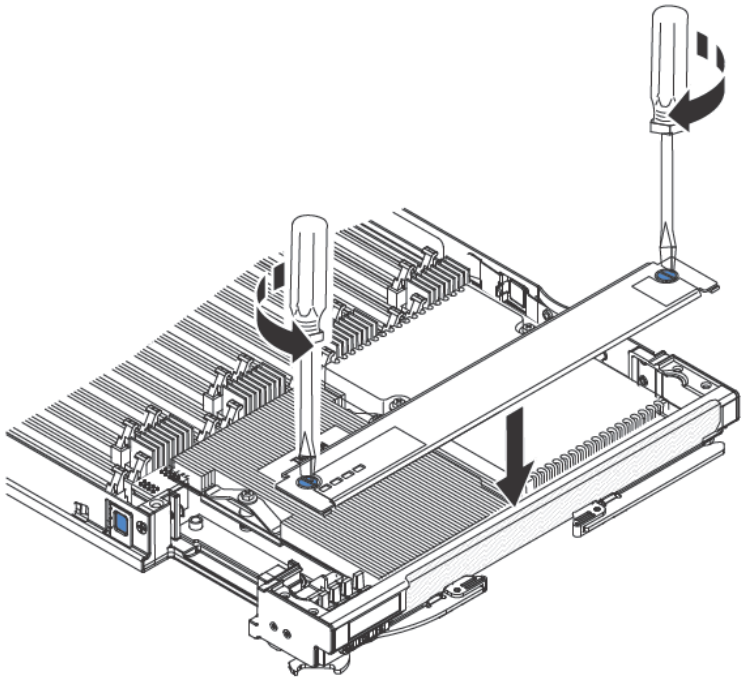


Figure 3-14. Installing the access panel

    a. Make sure that the screws on the access panel are in the open position (the screw insert is parallel to the side of the access panel).
    b. Slide the back of the cover under the blade server bezel, aligning the screws with the slots on the blade server.
    c. Using a screwdriver or a coin, turn each of the screws away from the middle of the blade server until it is in the locked position.

3.13 Removing a hypervisor key

Use this information to remove a hypervisor key from the blade server.

The following illustration shows the removal of a hypervisor key.

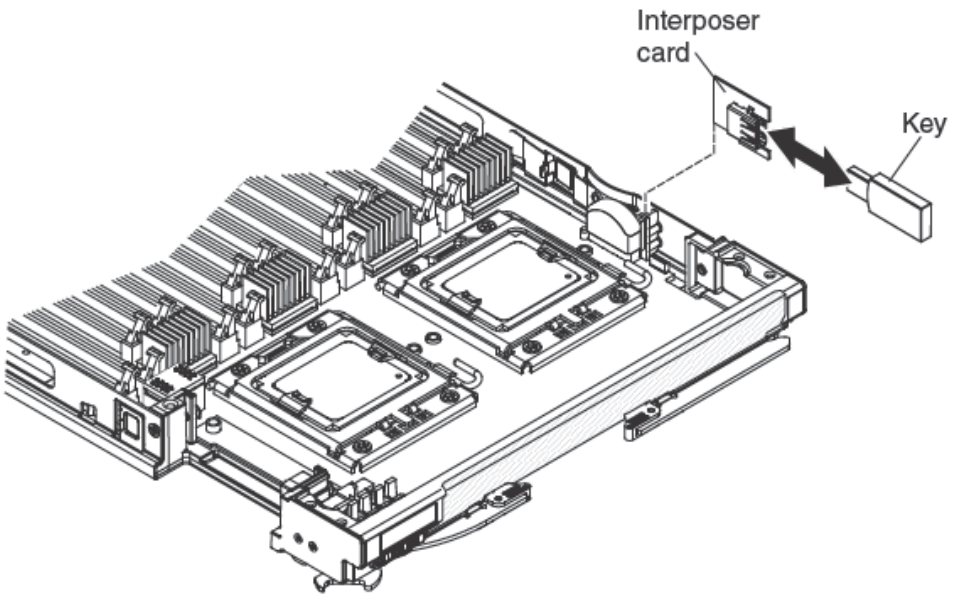


Figure 3-15. Removing a hypervisor key

To remove a hypervisor key, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25 for instructions).
3. Carefully lay the blade server on a flat, static-protective surface.
4. Open the blade server cover (see *Removing the blade server cover* on page 26 for instructions).

5. Remove the access panel:

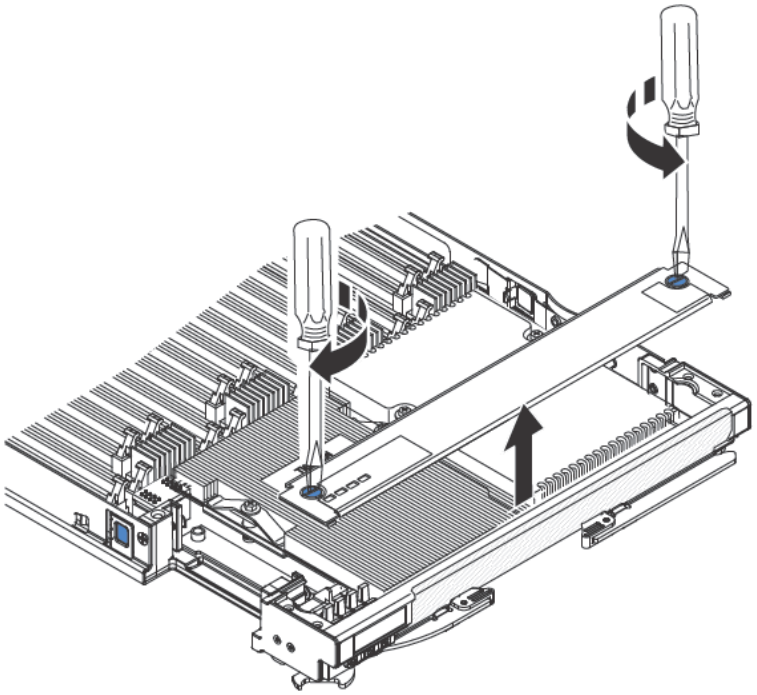


Figure 3-16. Removing the access panel

   a. Using a screwdriver or a coin, turn each of the screws toward the middle of the blade server until they are in the unlocked position.
   b. While you lift the back of the access panel, slide the panel away from the bezel.

6. Locate the hypervisor interposer on the system board (see *Major components of the blade server* on page 10).

7. Press down on the front edge of the hypervisor interposer to disengage the hypervisor interposer from the hypervisor interposer card guide.

8. Carefully lift the hypervisor interposer up from the system board.

9. Pull the hypervisor key away from the hypervisor interposer.

3.14 Installing an I/O-expansion card

The following sections describe how to install the following expansion cards:

- CFFh expansion cards, for example:
  - QLogic Ethernet and 4 GB Fibre Channel Expansion Card
  - QLogic 2-Port 10Gb Converged Network Adapter
  - QLogic Ethernet and 8 GB Fibre Channel Expansion Card
  - Broadcom 4-Port 10 Gb Ethernet Expansion Card (CFFh)
  - Emulex Virtual Fabric Adapter
- CIOv expansion cards, for example:
  - QLogic 8 Gb Fibre Channel Expansion Card
  - QLogic 4 Gb Fibre Channel Expansion Card

Note CIOv expansion card is supported for all combinations.

The following illustration shows the cards that are supported in a blade server.

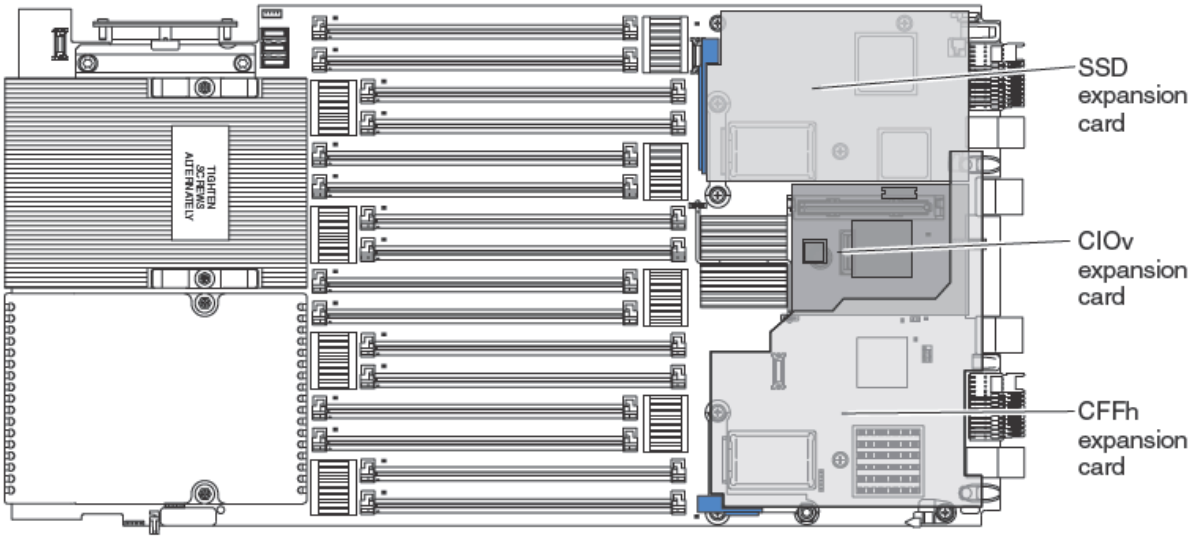


Figure 3-17. Cards supported in a blade server

For information about installing an SSD expansion card, see *Installing an SSD expansion card* on page 30.

3.14.1 Installing a CIOv expansion card

Use these instructions to install a CIOv-form-factor expansion card in the blade server.

The blade server supports a vertical-combination-I/O (CIOv) expansion card and a horizontal-combination-form-factor (CFFh) expansion card. The following illustration shows the location and installation of a CIOv expansion card

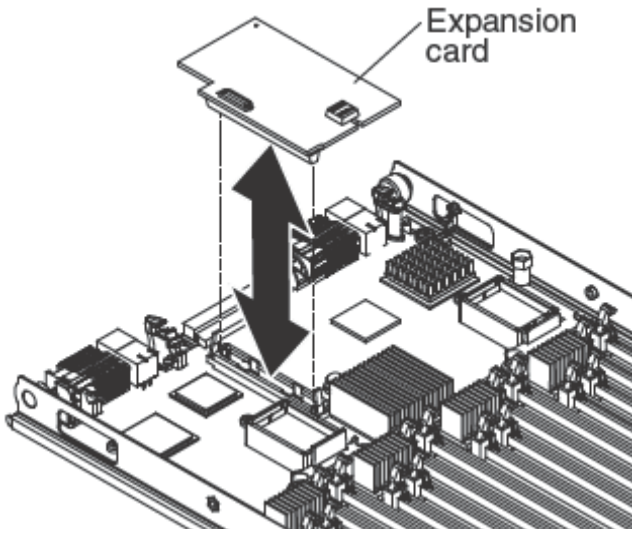


Figure 3-18. Installing a CIOv form-factor expansion card

To install a CIOv expansion card, complete the following steps:

1. Read the safety information that begins on page vii and Installation guidelines on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25 for instructions).
3. Carefully lay the blade server on a flat, static-protective surface.
4. Open the blade server cover (see *Removing the blade server cover* on page 26 for instructions).
5. If a CFFh expansion card is installed, remove it (see *Removing a CFFh expansion card* on page 47).
6. Locate the CIOv expansion connector (see *Blade server connectors* on page 20).
7. Touch the static-protective package that contains the expansion card to any *unpainted* metal surface on the Blade Chassis or any *unpainted* metal surface on any other grounded rack component; then, remove the expansion card from the package
8. Orient the connector on the expansion card with the CIOv expansion connector on the system board; then, press the card into the CIOv expansion connector.

9. Firmly press on the indicated locations to seat the expansion card.

> **Note** For device-driver and configuration information to complete the installation of the expansion card, see the documentation that comes with the expansion card

10. If you have other options to install or remove, do so now; otherwise, go to *Completing the installation* on page 49.

3.14.2 Installing a CFFh expansion card

> **Note** The horizontal combination-form-factor expansion cards are supported in Bull Blade Chassis-Enterprise only.

Use these instructions to install a compact-form-factor expansion card in the blade server.

The blade server supports a horizontal-combination-form-factor (CFFh) expansion card. The following illustration shows how to install a CFFh expansion card.

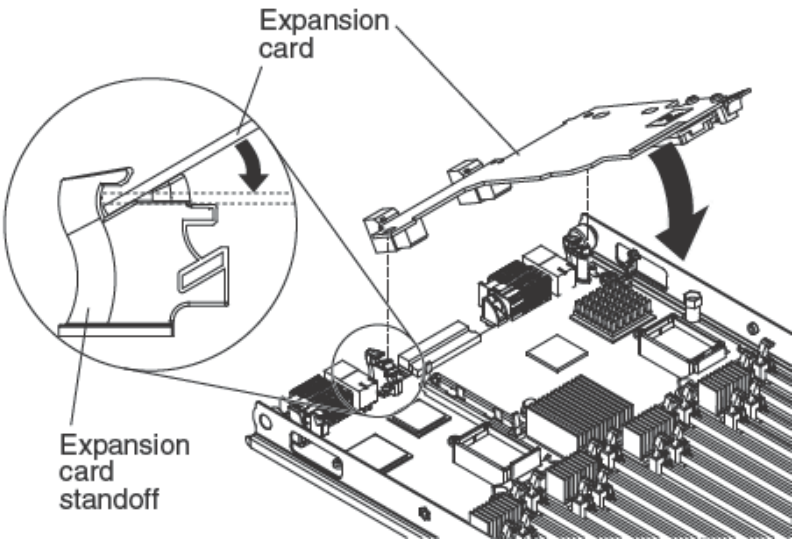


Figure 3-19. Installing a CFFh expansion card

To install a CFFh expansion card, complete the following steps:

1. Read the safety information that begins on page vii and Installation guidelines on page 23.
2. Turn off the blade server.
3. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page *25* for instructions).
4. Carefully lay the blade server on a flat, static-protective surface.

5. Open the blade server cover (see *Removing the blade server cover* on page 26).

6. Locate the blade server expansion connector (see *Blade server connectors* on page 20).

7. If a cover is installed on the blade expansion connector, remove it by using your fingers to lift the cover from the blade expansion connector.

8. Touch the static-protective package that contains the expansion card to any *unpainted* metal surface on the Blade Chassis or any *unpainted* metal surface on any other grounded rack component for at least 2 seconds, then remove the I/O expansion card from its static-protective package.

9. Orient the expansion card and slide the slots at the back end of the card onto the pins on the expansion-card standoff; then, gently pivot the card into the blade server expansion connector.

10. Firmly press on the indicated locations to seat the expansion card.

> **Note** For device-driver and configuration information to complete the installation of the I/O expansion card, see the documentation that comes with the expansion card.

11. If you have other devices to install or remove, do so now; otherwise, go to *Completing the installation* on page 49.

3.15 Removing an I/O expansion card

The following sections describe how to remove the following expansion cards:

- CFFh
- CIOv

For information about removing an SSD expansion card, see *Removing an SSD expansion card* on page 31.

3.15.1 Removing a CFFh expansion card

Use these instructions to remove a compact-form-factor expansion card from the blade server.

To remove a CFFh expansion card, complete the following steps:

1. Read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25).
3. Carefully lay the blade server on a flat, static-protective surface.
4. Open the blade server cover (see *Removing the blade server cover* on page 26).
5. Locate the CFFh expansion card. The CFFh is installed into the blade expansion connector (see *Blade server connectors* on page 20).
6. Locate the release lever on the CFFh expansion card; then, use your finger to lift up on the release lever to loosen the expansion card from the expansion connector.
7. Use your fingers to hold the edge of the CFFh expansion card where it connects to the blade expansion connector; then, lift up on the card.

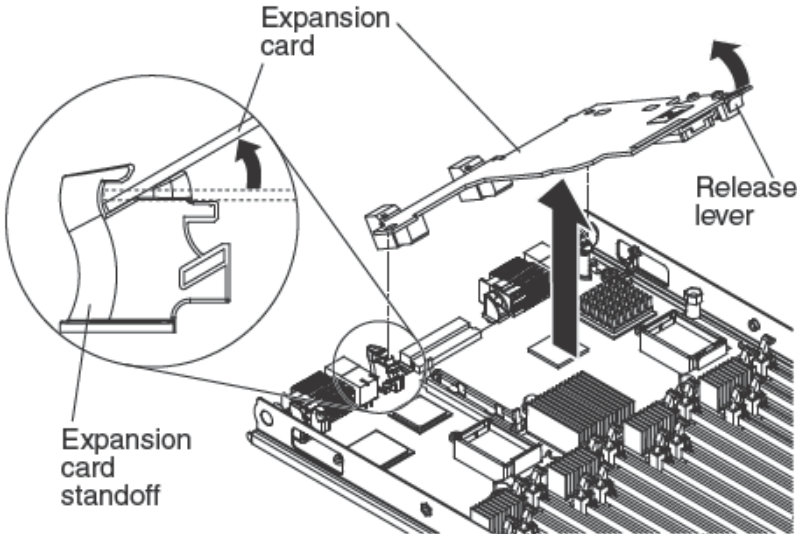


Figure 3-20. Removing a CFFh expansion card

8. Pull the card away from the expansion card standoff.

3.15.2 Removing a CIOv expansion card

Use these instructions to remove a CIOv-form-factor expansion card in the blade server.

The following illustration shows how to remove a vertical-combination-I/O (CIOv) expansion card.

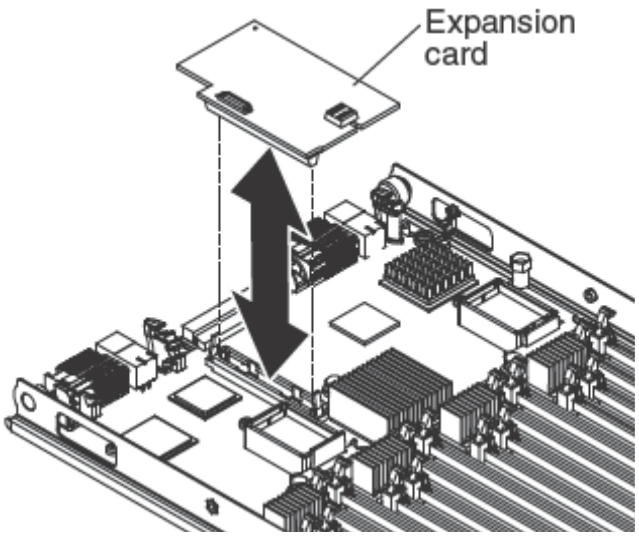


Figure 3-21. Removing a CIOv form-factor expansion card

To remove a CIOv expansion card, complete the following steps:

1. Read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. If the blade server is installed in a Blade Chassis, remove it (see *Removing the blade server from the Blade Chassis* on page 25).
3. Carefully lay the blade server on a flat, static-protective surface.
4. Open the blade server cover (see *Removing the blade server cover* on page 26).
5. If a CFFh expansion card is installed, remove it (see *Removing a CFFh expansion card* on page 47).
6. Locate the CIOv expansion connector (see *Blade server connectors* on page 20).
7. Using your fingers, move the retaining clips away from the CIOv card; then, lift the card out of the connector.

3.16 Completing the installation

To complete the installation, complete the following tasks.

1. Assemble the 2-nodes blade if necessary (see *Assembling the BL465* on page 49).
2. Close the blade server cover (see *Installing the blade server cover* on page *54*).

Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

3. Reinstall the blade server into the Blade Chassis (see *Installing the blade server in a Blade Chassis* on page 56).
4. Turn on the blade server (see *Turning on the blade server* on page *15*). If you have just connected the power cords of the Blade Chassis to electrical outlets, you must wait until the power-on LED on the blade server flashes slowly before you press the power-control button.
5. For certain optional devices, you might have to run the blade server Setup Utility (see *Chapter 4, Configuring the blade server*, on page *59*). See the documentation that comes with your optional device for additional information.

3.16.1 Assembling the BL465

Use this information to assemble the BL465.

To assemble the BL465, you will need the following parts:

- Two Blade nodes
- 2-node scalability kit, which includes the 2-node scalability card, the scalability tray, and the 3/16" hex driver.

To assemble the BL465, complete the following steps.

Note Make sure that you installed a hypervisor key in the primary blade server, if required, to use the BL465 as a single hardware partition in a virtualized environment.

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Install the scalability tray in the topmost module (see *Installing the scalability tray* on page 50 for instructions).
3. Attach the blade server with the scalability tray to the bottom module.

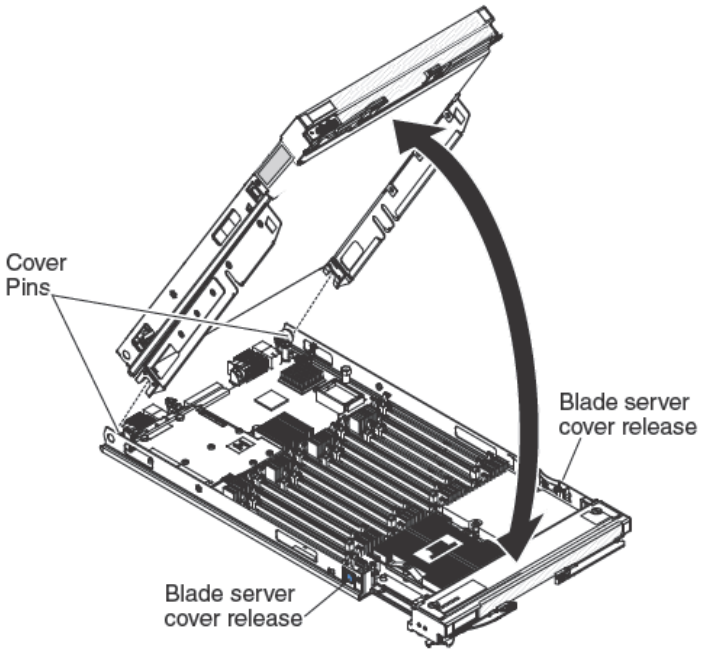


Figure 3-22. Attaching the blade server with the scalability tray to the bottom module

a. Lower the topmost blade server so that the slots at the rear slide down onto the pins at the rear of the bottom blade server, as shown in the illustration.

b. b. Pivot the topmost blade server to the closed position, as shown in the illustration, until it clicks into place.

4. Install the 2-node scalability card (see *Installing the 2-node scalability card* on page 52).

3.16.1.1 Installing the scalability tray

Use this information to install the scalability tray on a blade server.

To install the scalability tray, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.

2. Carefully lay the blade server on a flat, static-protective surface, with the cover side down.

3. Align the scalability tray flush with the blade server in the start position. The pins on the scalability tray should be aligned with the holes in the blade server.

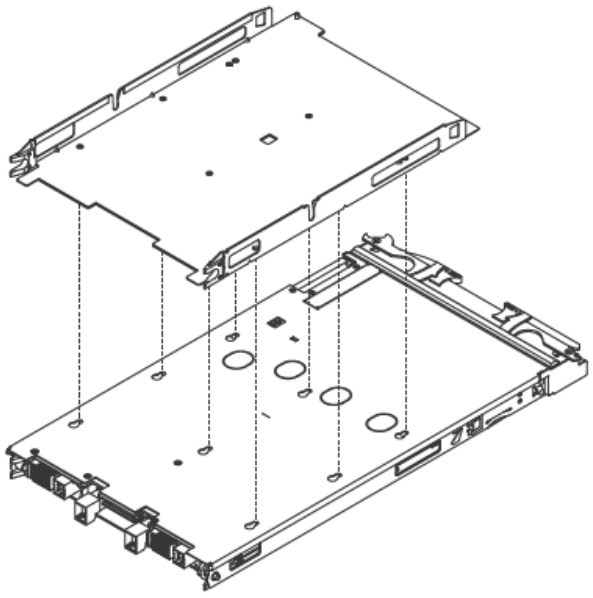
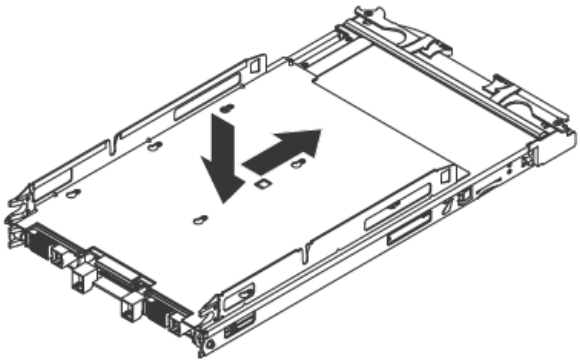


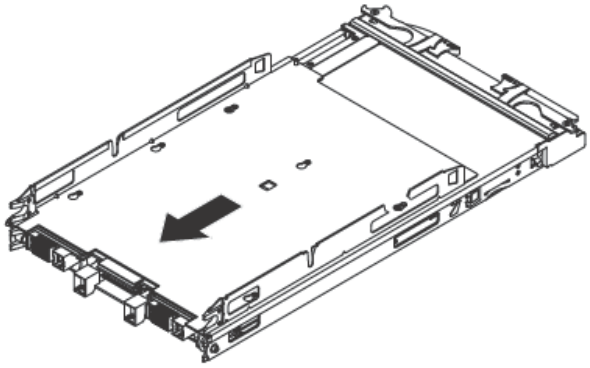
Figure 3-23. Installing the scalability tray

4. Pressing down firmly on the middle of the tray, slide the scalability tray forward toward the bezel until there is an audible click on each side of the blade server.



5. Attempt to pull the scalability tray back to ensure that the scalability tray is firmly seated.

6. Look in the holes on each side of the blade server to ensure that the spring plates are engaged.

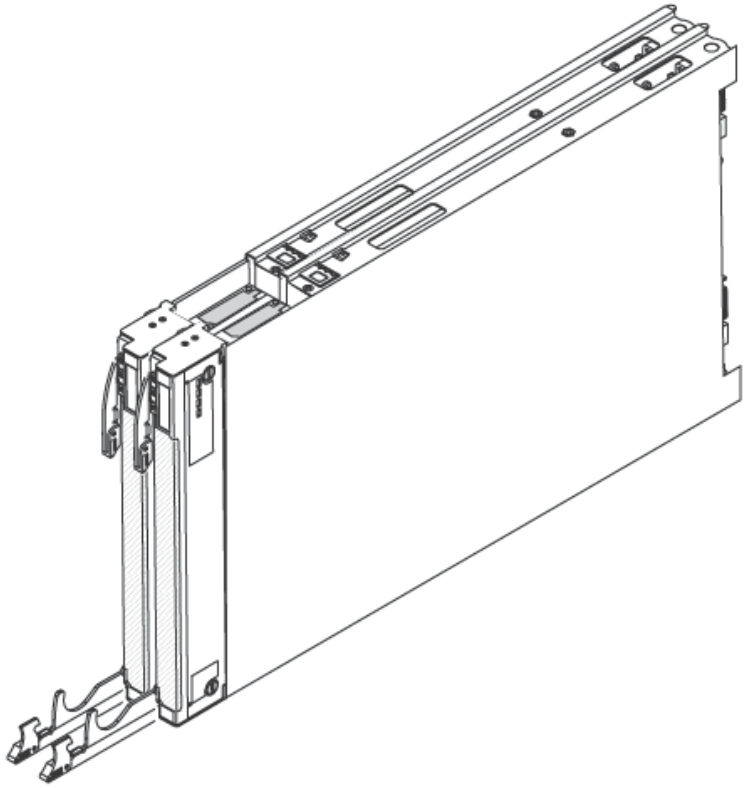


3.16.1.2 Installing the 2-node scalability card

Use this information to install the 2-node scalability card on a blade server.

To install the 2-node scalability card, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Stand the blade servers upright on a clean, flat work surface, with the scalability connector on the blade servers facing up.
3. Release the lower handles (rotate the lower handles down) to allow the blade servers to sit flat on the work surface.



4. Align the pins on the bottom of the 2-node scalability card with the holes on the scalability connector on the blade server.
5. Press down firmly so that the 2-node scalability card is flush with the scalability connector on the blade server.

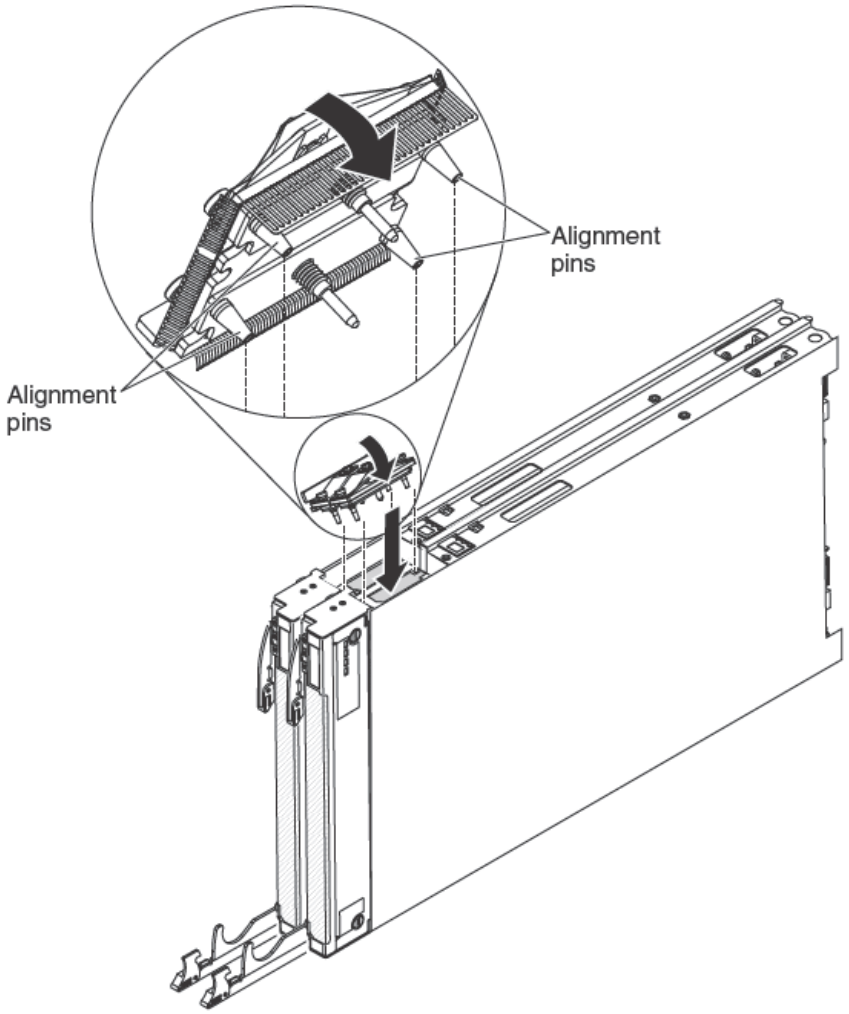


Figure 3-24. Installing the 2-node scalability card

6. Make sure that the 2-node scalability card is flush with the edge of the blade server.
7. Alternately tighten the screws on the 2-node scalability card by hand to ensure that the screw threads start properly.

Important

Always hand tighten each screw before you use the 3/16" hex drive

8. Alternately tighten each screw on the 2-node scalability card using the 3/16" hex driver. Alternate the tightening of each screw until both screws are tightened.

Note If you are using a torque driver, the correct torque is 15 in-lb.

3.16.2 Installing the blade server cover

Use these instructions to install and close the cover for a blade server or for the topmost module in a BL465.

Attention:
You cannot insert the blade server into the Blade Chassis until the cover is installed and closed or an expansion unit is installed. Do not attempt to override this protection.

Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

To install and close the blade server cover, complete the following steps:

1. Before you begin, read the safety information that begins on page vii and *Installation guidelines* on page 23.
2. Carefully lay the blade server on a flat, static-protective surface, orienting the blade server with the bezel pointing toward you.
3. Lower the cover so that the slots at the rear slide down onto the pins at the rear of the blade server, as shown in the illustration. Before you close the cover, make sure that all components are installed and seated correctly and that you have not left loose tools or parts inside the blade server.

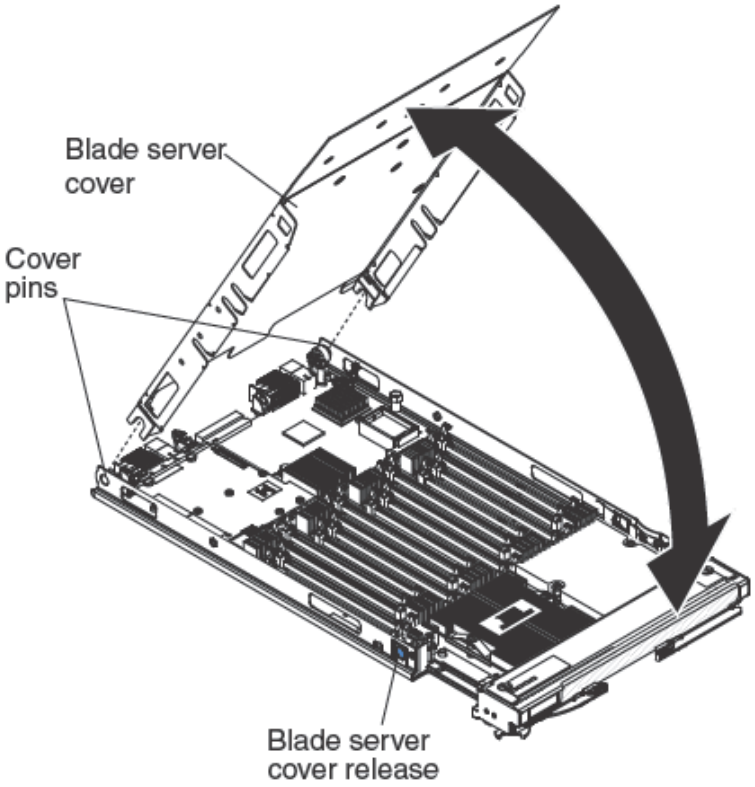


Figure 3-25. Installing and closing the blade server cover

4. Pivot the cover to the closed position, as shown in the illustration, until it clicks into place.

5. Install the blade server into the Blade Chassis (see *Installing the blade server in a Blade Chassis* on page 56).

3.16.3 Installing the blade server in a Blade Chassis

The following illustration shows how to install a blade server into a Blade Chassis. The appearance of your Blade Chassis might be different, see the documentation for your Blade Chassis for additional information.

To install a blade server in a Blade Chassis, complete the following steps:

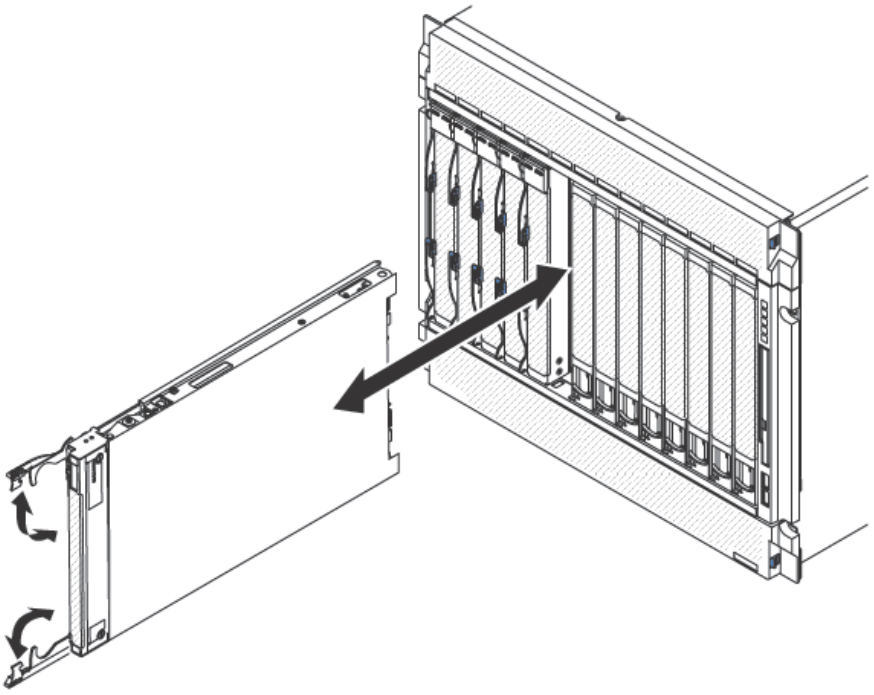


Figure 3-26. Installing the blade server in a Blade Chassis

Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

1. Read the safety information that begins on page vii and *Installation guidelines* on page 23 through *Handling static-sensitive devices* on page 24.

2. Select the bay for the blade server; at least one blade bay is required.

Notes 1. When any blade server or option is in any blade bays 7 through 14, power modules must be present in all four power-module bays. For additional information, see the *Installation and User's Guide* that comes with the Blade Chassis.

2. If you are reinstalling a blade server that you removed, you must install it in the same blade bay from which you removed it. Some blade server configuration information and update options are established according to blade server bay number. Reinstalling a blade server into a different blade server bay number from the one which it was removed can have unintended consequences, and you might have to reconfigure the blade server.
3. To help ensure proper cooling, performance, and system reliability, make sure that each blade bay on the front of the Blade Chassis contains a blade server, expansion unit, or blade filler. Do not operate a Blade Chassis for more than 1 minute without a blade server, expansion unit, or blade filler in each blade bay.

3. Make sure that the release handles on the blade server are in the open position (perpendicular to the blade server).

4. Slide the blade server into the blade bay until it stops.

5. Push the release handles on the front of the blade server to the closed position.

Note After the blade server is installed, the IMM in the blade server initializes and synchronizes with the management module. This process takes approximately two minutes to complete. The power-on LED flashes rapidly, and the power-control button on the blade server does not respond until this process is complete

6. Turn on the blade server (see *Turning on the blade server* on page *15* for instructions).

7. Make sure that the power-on LED on the blade server control panel is lit continuously, indicating that the blade server is receiving power and is turned on.

8. If you have other blade servers to install, do so now.

If this is the initial installation for the blade server in the Blade Chassis, you must configure the blade server through the Setup Utility and install the blade server operating system. See *Updating the blade server configuration* on page 58, and *Chapter 5*, *Installing the operating system*, on page 73 for details.

If you have changed the configuration of the blade server or if you are installing a different blade server from the one that you removed, you must configure the blade server through the Setup Utility, and you might have to install the blade server operating system. For more information see *Using the Setup Utility* on page 60.

3.16.4 Updating the blade server configuration

When the blade server starts for the first time after you add or remove an internal option, you might receive a message that the configuration has changed. The Setup Utility automatically starts so that you can save the new configuration settings. See *Using the Setup Utility* on page 60 for more information about the Setup Utility.

Some options have device drivers that you must install. See the documentation that comes with each option for information about installing device drivers.

The blade server operates as a symmetric multiprocessing (SMP) server, regardless of how many microprocessors are installed. For optimum performance, you must upgrade the operating system to support SMP. See *Chapter 5*, *Installing the operating system*, on page *73* for details. and your operating-system documentation for additional information.

Chapter 4. Configuring the blade server

There are several components on the blade server that you can configure and several methods for configuring those components.

Note: If you intend to use the BL465 in single partition mode, you must partition the blade before you turn it on or begin the configuration process. See *Partitioning a novascale Blade BL465* on page 60 for information.

Typically, you complete the following steps to configure the blade server:

1. Configure the Unified Extensible Firmware Interface (UEFI) firmware for the blade server. You can configure the UEFI firmware by using the Setup utility or the Advanced Settings Utility (ASU).

2. Set the boot protocol. To set the boot protocol, use either the Setup Utility or the Preboot Execution Environment (PXE) boot agent utility program.

   Note You can temporarily redefine the boot order by using the Boot menu program that is provided with the blade server firmware.

3. Configure the RAID array.
   You can install up to two solid state drives in each node of the BL465 and implement RAID level-0 (striping) or RAID level-1 (mirror) arrays in operating systems. For the BL465, you must configure the RAID by using the LSI Configuration Utility program (see *Using the LSI Logic Configuration Utility program* on page 71).

   Note If you are implementing a BL465 in single partition mode, you cannot combine the SSD in both the primary and the secondary server to define a RAID array. RAID arrays can be defined using only the SSDs within a blade server.

   If an optional RAID expansion card is installed, you can use it to control all the storage drives that are installed in the blade server. See the documentation that comes with the expansion card for information on how to configure the RAID array.

Important

You must create the RAID array *before* you install the operating system on the blade server.

4. Configure the integrated management module (IMM). To configure the IMM, use either the Setup utility or the Advanced Settings Utility (ASU).

5. Update the blade server firmware.

After you configure the blade server, you can install the operating system and update device drivers (see Chapter 5, *Installing the operating system* on page 73 for more information).

4.1 Partitioning a novascale Blade BL465

Before you configure the nodes that are part of a BL465 operating in single partition mode, you must partition the BL465.

For more information about BL465 and operating modes, see *Working with BL465 Partitioning* on page 11.

To partition a BL465, complete the following steps:

1. From the advanced management module Web interface, click **Scalable Complex→ Configuration**.
2. Select one or more of the modules that are part of the BL465.
3. Click **Available actions → Create partition**.

4.2 Using the Setup Utility

To start the Setup Utility, complete the following steps:

1. Turn on the blade server (see *Turning on the blade server* on page *15*).
2. Immediately give the blade server control of the Blade Chassis shared keyboard, video, and mouse ports.
   - If you are managing the blade server by using the Blade system console, press the KVM select button on the blade server (see *Blade server controls and LEDs* on page *16* for information).
   - If you are managing the blade server from a remote location, see the Management Module documentation for information and instructions.
3. When the prompt `Press <F1> Setup` is displayed, press F1. If you have set an administrator password, you must type the administrator password to access the full Setup-utility menu. If you do not type the administrator password, a limited Setup-utility menu is available.
4. Follow the instructions on the screen.

The following menu items are on the Setup utility main menu. Depending on the version of the Unified Extensible Firmware Interface (UEFI), some menu items might differ slightly from these descriptions. Use the help within the Setup utility for more information on the available menu items and selections.

- **System Information**
  Select this choice to view information about the server. When you make changes through other choices in the Setup utility, some of those changes are reflected in the system information; you cannot change settings directly in the system information. This choice is on the full Setup utility menu only.
  - **System Summary**
    Select this choice to view configuration information, including the ID, speed, and cache size of the microprocessors, machine type and model of the server, the serial number, the system UUID, and the amount of installed memory.
  - **Product Data**
    Select this choice to view the system-board identifier, the revision level or issue date of the firmware, the integrated management module and diagnostics code, and the version and date.

  This choice are on the full UEFI Setup Utility menu only.
- **System Settings**
  Select this choice to view or change the server component settings.
  - **Adapters and UEFI Drivers**
    Select this choice to view information about the adapters and UEFI drivers installed on the server.

    Note: Before you configure a UEFI-compatible device, you should update the firmware for your blade server. See "Updating firmware and device drivers" on page 62 for information about how to update the firmware for your blade server.
    To configure a UEFI-compatible expansion card, complete the following steps:
    1. Select **Please refresh this page first** and press Enter.
    2. Select the device driver that you want to configure and press Enter.
    3. When you have finished changing settings, press Esc to exit from the program; select **Save** to save the settings that you have changed.
  - **Processors**
    Select this choice to view or change the processor settings.
  - **Memory**
    Select this choice to view or change the memory settings.
  - **Devices and I/O Ports**
    Select this choice to view or change assignments for devices and input/output (I/O) ports. You can configure the remote console redirection, enable or disable integrated Ethernet controllers, and the SAS controller. If you disable a device, it cannot be configured, and the operating system will not be able to detect it (this is equivalent to disconnecting the device).
    You can also choose to enable or disable adapter option ROM support. Disabling support can potentially improve the time it takes the blade server to start.
  - **Power**
    Select this choice to view or change Active Energy Manager (AEM) power capping to control power consumption and processor performance states.

- **Operating Modes**
  Select this choice to determine operational settings, such as operating mode (acoustic, efficiency, or performance) and memory speed.
- **Integrated Management Module**
  Select this choice to view or change the settings for the integrated management module (IMM).
  - **POST Watchdog Timer**
    Select this choice to view or enable the POST watchdog timer.
  - **POST Watchdog Timer Value**
    Select this choice to view or set the POST loader watchdog timer value.
  - **Reboot System on NMI**
    Enable or disable restarting the system whenever a nonmaskable interrupt (NMI) occurs. **Disabled** is the default.
  - **Commands on USB Interface Preference**
    Select this choice to specify whether the Ethernet over USB interface is enabled or disabled.

    Note: This option is primarily for older operating systems that have problems with USB communications device class (CDC) Ethernet interfaces.
    Disabling this option will cause the following issues:
    - Online update packages will not work.
    - Updates that use Bootable Media Creator (BoMC) will not work because BoMC uses the LAN over USB interface.
    - You must install the IPMI device driver to use ASU to change the IMM or UEFI configuration.
    - You cannot set the IMM OS Loader watchdog.
    - Portable and installable Dynamic Systems Analysis (DSA) will not be able to obtain any IMM information.
  - **Network Configuration**
    Select this choice to view the system management network interface port, the IMM MAC address, the current IMM IP address, and host name; define the static IMM IP address, subnet mask, and gateway address, specify whether to use the static IP address or have DHCP assign the IMM IP address, save the network changes, and reset the IMM.
  - **Reset IMM to Defaults**
    Select this choice to reset the IMM to the default settings.
  - **Reset IMM**
    Select this choice to reset the IMM.

  - **Legacy Support**
    Select this choice to view or set legacy support.
    - **Force Legacy Video on Boot**
      Select this choice to enable or disable force INT video support, if the operating system does not support UEFI video output standards. The default is **Enable**.
    - **Rehook INT**
      Select this choice to enable or disable devices from taking control of the boot process. The default is **Disable**.
    - **Legacy Thunk Support**
      Select this choice to enable or disable UEFI to interact with PCI mass storage devices that are non-UEFI compliant. The default is **Enable**.
  - **System Security**
    Select this choice to view or configure security options.
  - **Adapters and UEFI Drivers**
    Select this choice to view information about the adapters and UEFI drivers installed in the server.
  - **Network**
    Select this choice to view or configure the network device options, such as iSCSI, PXE, and Broadcom.
  - **Trusted Platform Module (TPM)**
    Select this choice to view and configure TPM settings.

- **Date and Time**
  Select this choice to set the date and time in the server, in 24-hour format (*hour*:*minute*:*second*).
  This choice is on the full UEFI Setup Utility menu only..

- **Start Options**
  Select this choice to view or change the start options, including the startup sequence, keyboard NumLock state, PXE boot option, and PCI device boot priority. Changes in the startup options take effect when you start the server.
  The startup sequence specifies the order in which the server checks devices to find a boot record. The server starts from the first boot record that it finds. If the server has Wake on LAN hardware and software and the operating system supports Wake on LAN functions, you can specify a startup sequence for the Wake on LAN functions. For example, you can define a startup sequence that checks for a disc in the CD-RW/DVD drive, then checks the hard disk drive, and then checks a network adapter.
  This choice is on the full UEFI Setup Utility menu only.

- **Boot manager**
  Select this choice to view, add, delete, or change the device boot priority, boot from a file, select a one-time boot, or reset the boot order to the default setting.

- **System Event logs**
  Select this choice to enter the System Event Manager, where you can view the error messages in the system event logs. You can use the arrow keys to move between pages in the error log.

The system event logs contain all event and error messages that have been generated during POST, by the systems-management interface handler, and by the system service processor. Run the diagnostic programs to get more information about error codes that occur. See the *Problem Determination and Service Guide* for instructions on running the diagnostic programs.

Important: If the system-error LED on the front of the server is lit but there are no other error indications, clear the IMM system-event log. Also, after you complete a repair or correct an error, clear the IMM system-event log to turn off the system-error LED on the front of the server.

  - **POST Event Viewer**
    Select this choice to enter the POST event viewer to view the POST error messages.
  - **IMM System Event Log**
    Select this choice to view the IMM system event log.
  - **Clear IMM System Event log**
    Select this choice to clear the IMM system event log.

- **User Security**
  Select this choice to set, change, or clear passwords.
  You can set, change, and delete a power-on password and an admin password through this selection. If you set a power-on password, you must type the power-on password to complete the system startup and to have access to the Configuration/Setup Utility menu.
  You can use any combination of up to from 6 to 20 characters (A - Z, a - z, and 0 - 9) for passwords. Keep a record of your password in a secure place.
  If you forget the power-on password, you can regain access to the blade server either by removing the blade server battery and then reinstalling it or by using the power-on password override switch (see the *Problem Determination and Service Guide* for instructions).
- **Save settings**
  Select this choice to save the changes that you have made in the settings.
- **Restore Settings**
  Select this choice to cancel the changes that you have made in the settings and restore the previous settings.
- **Load Default Settings**
  Select this choice to cancel the changes that you have made in the settings and restore the factory settings.
- **Exit Setup**
  Select this choice to exit from the Setup utility. If you have not saved the changes that you have made in the settings, you are asked whether you want to save the changes or exit without saving them.

4.3 Using the PXE boot agent utility program

Use the Preboot Execution Environment (PXE) boot agent utility program to select the boot protocol and other boot options and to select a power-management option.

Notes

- The blade server does not support Remote Program Load (RPL) selection for the boot protocol option.
- Enabling PXE might reduce the number of optional expansion modules that your blade server can manage.

To start the PXE boot agent utility program, complete the following steps:

1. Turn on the server.
2. When the `Broadcom NetXtreme Boot Agent vX.X.X` prompt is displayed, press Ctrl+S. You have 2 seconds (by default) to press Ctrl+S after the prompt is displayed.
3. Follow the instructions on the screen to change the settings of the selected items.

4.4 Using the Boot Selection Menu program

The Boot Selection Menu program is a built-in, menu-driven configuration utility program that you can use to temporarily redefine the first startup device without changing settings in the Setup utility.

To use the Boot Selection Menu program, complete the following steps:

1. Turn off the blade server.
2. Restart the blade server.
3. Press F12 (**Select Boot Device**). If a bootable USB mass storage device is installed, a submenu item (**USB Key/Disk**) is displayed.
4. Use the Up Arrow and Down Arrow keys to select an item from the Boot Selection Menu and press **Enter**.

The next time the blade server starts, it returns to the startup sequence that is set in the Setup utility.

4.5 Using the Advanced Setting Utility (ASU)

Configuring You can use the Advanced Settings Utility (ASU) to modify firmware settings from the command line on multiple operating systems, such as Linux, Windows, and Windows Professional Edition (PE).

You can use the ASU to perform the following tasks:

- Modify selected firmware UEFI settings without the need to restart the blade server to access F1 settings.
- Modify selected settings in integrated management module (IMM) based blade servers for the IMM firmware.
- Modify a limited number of VPD settings on IMM-based blade servers.
- Modify iSCSI boot settings.

4.5.1 Updating the Universal Unique Identifier (UUID)

The Universal Unique Identifier (UUID) must be updated when the system board is replaced.

The Universal Unique Identifier (UUID) must be updated when the system board is replaced. Use the Advanced Settings Utility (ASU) to update the UUID in the UEFI-based server. The ASU is an online tool that supports several operating systems. Make sure that you download the version for your operating system. You can download the ASU from the Bull Support Web site. To update the UUID, complete the following steps.

1. Download the Advanced Settings Utility (ASU)

2. ASU sets the UUID in the Integrated Management Module (IMM). Select one of the following methods to access the Integrated Management Module (IMM) to set the UUID:
   - Online from the target system (LAN or keyboard console style (KCS) access)
   - Remote access to the target system (LAN based)
   - Bootable media containing ASU (LAN or KCS, depending upon the bootable media)

3. Copy and unpack the ASU package, which also includes other required files, to the server. Make sure that you unpack the ASU and the required files to the same directory. In addition to the application executable (asu or asu64), the following files are required:
   - For Windows based operating systems:
     – ibm_rndis_server_os.inf
     – device.cat
   - For Linux based operating systems:
     – cdc_interface.sh

4. After you install ASU, use the following command syntax to set the UUID:
   `asu set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value> [access_method]`
   Where:
   <uuid_value>

Up to 16-byte hexadecimal value assigned by you.

[access_method]

The access method that you selected to use from the following methods:

- Online authenticated LAN access, type the command:
  `[host <imm_internal_ip>] [user <imm_user_id>] [password <imm_password>]`

  Where:

  imm_internal_ip
  The IMM internal LAN/USB IP address. The default value is 169.254.95.118.

  imm_user_id
  The IMM account (1 of 12 accounts). The default value is USERID.

  imm_password
  The IMM account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

  Note: If you do not specify any of these parameters, ASU will use the default values. When the default values are used and ASU is unable to access the IMM using the online authenticated LAN access method, ASU will automatically use the unauthenticated KCS access method.

  The following commands are examples of using the userid and password default values and not using the default values:

  Example that does not use the userid and password default values:
  `asu set SYSTEM_PROD_DATA.SYsInfoUUID <uuid_value> user <user_id> password <password>`

  Example that does use the userid and password default values:
  `asu set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>`

- Online KCS access (unauthenticated and user restricted):
  You do not need to specify a value for *access_method* when you use this access method.

  Example:
  `asu set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>`
  The KCS access method uses the IPMI/KCS interface. This method requires that the IPMI driver be installed. Some operating systems have the IPMI driver installed by default. ASU provides the corresponding mapping layer.

  See the *Advanced Settings Utility Users Guide* for more details.

- Remote LAN access, type the command:

  Note: When using the remote LAN access method to access IMM using the LAN from a client, the *host* and the *imm_external_ip* address are required parameters.
  `host <imm_external_ip> [user <imm_user_id>[[password <imm_password>]`

  Where:

  imm_external_ip

The external IMM LAN IP address. There is no default value. This parameter is required.

imm_user_id

The IMM account (1 of 12 accounts). The default value is USERID.

imm_password

The IMM account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

The following commands are examples of using the userid and password default values and not using the default values:

Example that does not use the userid and password default values:

```
asu set SYSTEM_PROD_DATA.SYsInfoUUID <uuid_value>
host <imm_ip> user <user_id> password <password>
```

Example that does use the userid and password default values:

```
asu set SYSTEM_PROD_DATA.SysInfoUUID <uuid_value>
host <imm_ip>
```

5. Restart the server.

4.5.2 Updating the DMI/SMBIOS data

The Desktop Management Interface (DMI) must be updated when the system board is replaced.

The Desktop Management Interface (DMI) must be updated when the system board is replaced. Use the Advanced Settings Utility (ASU) to update the DMI in the UEFI-based server. The ASU is an online tool that supports several operating systems. Make sure that you download the version for your operating system. You can download the ASU from the Bull Support Web site. To update the DMI, complete the following steps.

1. Download the Advanced Settings Utility (ASU)

2. ASU sets the DMI in the Integrated Management Module (IMM). Select one of the following methods to access the Integrated Management Module (IMM) to set the DMI:
   - Online from the target system (LAN or keyboard console style (KCS) access)
   - Remote access to the target system (LAN based)
   - Bootable media containing ASU (LAN or KCS, depending upon the bootable media)

3. Copy and unpack the ASU package, which also includes other required files, to the server. Make sure that you unpack the ASU and the required files to the same directory. In addition to the application executable (asu or asu64), the following files are required:
   - For Windows based operating systems:
     – ibm_rndis_server_os.inf
     – device.cat
   - For Linux based operating systems:
     – cdc_interface.sh

4. After you install ASU, Type the following commands to set the DMI:

   ```
   asu set SYSTEM_PROD_DATA.SysInfoProdName &ltm/t_model>
   [access_method]
   asu set SYSTEM_PROD_DATA.SysInfoSerialNum &lts/n>
   [access_method]
   asu set SYSTEM_PROD_DATA.SysEncloseAssetTag &ltasset_tag>
   [access_method]
   ```

   Where:

   <m/t_model>
   The server machine type and model number. Type mtm xxxxyyy, where *xxxx* is the machine type and *yyy* is the server model number.

   <s/n> The serial number on the server. Type sn zzzzzzz, where *zzzzzzz* is the serial number.

   <asset_method>
   The server asset tag number. Type `asset aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa`, where *aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* is the asset tag number.

   [access_method]
   The access method that you select to use from the following methods:

   - Online authenticated LAN access, type the command:
     `[host &ltimm_internal_ip>] [user &ltimm_user_id>][password <imm_password>]`

     Where:

     imm_internal_ip
     The IMM internal LAN/USB IP address. The default value is 169.254.95.118.

     imm_user_id
     The IMM account (1 of 12 accounts). The default value is USERID.

     imm_password
     The IMM account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

     Note: If you do not specify any of these parameters, ASU will use the default values. When the default values are used and ASU is unable to access the IMM using the online authenticated LAN access method, ASU will automatically use the following unauthenticated KCS access method.
     The following commands are examples of using the userid and password default values and not using the default values:

     Examples that do not use the userid and password default values:

     ```
     asu set SYSTEM_PROD_DATA.SYsInfoProdName <m/t_model> --
     user
     <imm_user_id> --password <imm_password>
     asu set SYSTEM_PROD_DATA.SYsInfoSerialNum <s/n> --user
     <imm_user_id> --password <imm_password>
     asu set SYSTEM_PROD_DATA.SYsEncloseAssetTag <asset_tag>
     --user
     <imm_user_id> --password <imm_password>
     ```

     Examples that do use the userid and password default values:asu set
     `SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> asu set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> asu set`

```
SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
```

- Online KCS access (unauthenticated and user restricted):
  You do not need to specify a value for *access_method* when you use this access method.
  The KCS access method uses the IPMI/KCS interface. This method requires that the IPMI driver be installed. Some operating systems have the IPMI driver installed by default. ASU provides the corresponding mapping layer.
  The following commands are examples of using the userid and password default values and not using the default values:

  Examples that do not use the userid and password default values:
  ```
  asu set SYSTEM_PROD_DATA.SYsInfoProdName &ltm/t_model>
  asu set SYSTEM_PROD_DATA.SYsInfoSerialNum &lt;s/n>
  asu set SYSTEM_PROD_DATA.SYsEncloseAssetTag
  &ltasset_tag>
  ```

- Remote LAN access, type the command:

  Note: When using the remote LAN access method to access IMM using the LAN from a client, the *host* and the *imm_external_ip* address are required parameters.
  ```
  host <imm_external_ip> [user <imm_user_id>][password
  <imm_password>]
  ```

  Where:

  imm_external_ip
  The external IMM LAN IP address. There is no default value. This parameter is required.

  imm_user_id
  The IMM account (1 of 12 accounts). The default value is USERID.

  imm_password
  The IMM account password (1 of 12 accounts). The default value is PASSW0RD (with a zero 0 not an O).

  The following commands are examples of using the userid and password default values and not using the default values:

  Examples that do not use the userid and password default values:
  ```
  asu set SYSTEM_PROD_DATA.SYsInfoProdName <m/t_model> --
  host <imm_ip> --user <imm_user_id> --password
  <imm_password>
  asu set SYSTEM_PROD_DATA.SYsInfoSerialNum <s/n> --host
  <imm_ip> --user <imm_user_id> --password <imm_password>
  asu set SYSTEM_PROD_DATA.SYsEncloseAssetTag <asset_tag>
  --host
  <imm_ip> --user <imm_user_id> --password <imm_password>
  ```

  Examples that do use the userid and password default values:
  ```
  asu set SYSTEM_PROD_DATA.SysInfoProdName <m/t_model> --
  host <imm_ip>
  asu set SYSTEM_PROD_DATA.SysInfoSerialNum <s/n> --host
  <imm_ip>
  asu set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
  --host
  <imm_ip>
  ```

5. Restart the server.

4.6 Using the LSI Logic Configuration Utility program

You can use the LSI Logic Configuration Utility program to perform the following tasks:

- Set the device boot order.
- Add or remove devices from the bootlist.
- Manage the RAID configuration.

To start the LSI Logic Configuration Utility program, complete the following steps:

Note The LSI controller on your blade server is a UEFI compatible device and can also be configured through the Setup utility for your blade server (see see *Using the Setup Utility* on page 60).

1. Turn on the blade server, and make sure that the blade server is the owner of the keyboard, video, and mouse.
2. When the `<<<Press Ctrl-C to start LSI Logic Configuration Utility>>>` prompt is displayed, press Ctrl-C.
3. Use the arrow keys to select the controller from the list of adapters; then, press Enter.
4. Follow the instructions on the screen to change the settings of the selected items; then, press Enter. If you select **RAID Properties, SAS Topology** or **Advanced Adapter Properties**, additional screens are displayed.

4.7 Updating firmware and device drivers

Bull periodically makes UEFI code, service processor (IMM) firmware, diagnostic firmware updates, and device driver updates available for the blade server. Several methods are available to update the firmware for the blade server.

Note: Typically, you update the firmware before you install the operating system and update device drivers after the operating system is installed.

If you are updating the firmware for the blade servers in a BL465 operating in single partition mode, you only have to update the firmware for the primary blade server. When you update the firmware for the primary blade server, the firmware for the secondary blade server is updated as well.

You can update the firmware and device drivers for the blade server by using one of the following methods.

Important: To avoid problems and to maintain system performance, always make sure that the UEFI code, service processor (IMM) firmware, and diagnostic firmware levels are consistent in all blade servers within the Blade chassis.

- Downloading the firmware and device drivers from http://www.bull.com/support. Follow the instructions that come with the firmware and device drivers to install them.

You can also create a *ServerGuide Setup and Installation* CD for deploying Windows operating systems and updates on supported systems.

Chapter 5. Installing the operating system

To install the operating system on a blade server, download the latest operating-system installation instructions from the Bull Support web site: http://www.bull.com/support/ and install the operating system.

Important

The operating system in the blade server must provide USB support for the blade server to recognize and use the keyboard, mouse, and removable-media drives. The Blade Chassis uses USB for internal communication with these devices.

Chapter 6. Accessing the IMM

Unlike a baseboard management controller, the IMM does not require IPMI device drivers or USB daemons for in-band IMM communication. Instead, a LAN over USB interface enables in-band communications to the IMM; the IMM hardware on the system board presents an internal Ethernet interface from the IMM to the operating system. LAN over USB is also called the *USB in-band interface* in the IMM Web interface.

In a BL465, each IMM is shown as a LAN over USB device in the operating system. For each blade server in the BL465 to be a unique and known IP address, both blade servers have different default IP addresses. The default IP address for the primary blade server is 169.254.95.118, and the Keyboard Controller Style (KCS) address is 0x6CA8.

For packets to be routed correctly from the host to the IMMs, each of the LAN over USB interfaces must appear on a separate subnet to the host. The IMM implements a DHCP server that services only the LAN over USB interface. It assigns the subnet mask on the LAN over USB interfaces for the host to 255.255.255.0.

The following table shows the IP addresses for each of the modules in a BL465.

Blade server	Logical node ID	IMM IP address	Host address	Host subnet	Host subnet mask	Keyboard Controller Style (KCS) address
Primary	0	169.265.95.118	169.254.95.120	169.254.95.0/24	255.255.255.0	0x8CA6
Secondary	1	169.265.96.118	169.254.96.120	169.254.96.0/24	255.255.255.0	0x8CA8

Table 6-1. LAN over USB addresses

LAN over USB devices are not aware of LAN over USB devices in other partitions. Therefore, if you configure the two blade servers as two independent partitions in a BL465, each blade server is considered to the primary blade server of the hardware partition that contains that blade server. The logical ID of the primary in each partition is 0 and the default IP address of each primary blade server is 169.254.95.118.

6.1 Potential conflicts with the LAN over USB interface

In some situations, the IMM LAN over USB interface can conflict with certain network configurations, applications, or both. For example, Open MPI attempts to use all of the available network interfaces on a server. Open MPI detects the IMM LAN over USB interface and attempts to use it to communicate with other systems in a clustered environment. The LAN over USB interface is an internal interface, so this interface does not work for external communications with other systems in the cluster.

6.2 Resolving conflicts with the IMM LAN over USB interface

Use any of the following actions to resolve LAN over USB conflicts with network configurations and applications:

- For conflicts with Open MPI, configure the application so it does not attempt to use this interface.
- Take down the interface (run **ifdown** under Linux).
- Remove the device driver (run **rmmod** under Linux).
- Disable the LAN over USB interface from the advanced management module Web interface:

  1. Log in to the advanced management module (AMM) Web interface.
  2. In the navigation pane, click **Blade Configuration** under the **Blade Tasks** heading.
  3. Scroll down to the Service Processor LAN over USB interface are on the Blade Configuration web page. The section lists all blades in the chassis which are capable of enabling and disabling the LAN over USB interface.
  4. Select the check boxes next to the blade or blades that you want to enable or disable.
  5. Click the **Disable** button to disable the LAN over USB interface on the selected blades.

6.3 Configuring the LAN over USB interface manually

An IMM must be configured to use the LAN over USB interface. The firmware update package or Advanced Settings Utility attempt to perform the setup automatically, if needed. If the automatic setup fails or if you prefer to set up the LAN over USB manually, use one of the following processes.

For more information about LAN over USB configuration on different operating systems, see the white paper *Transitioning to UEFI and IMM* on http://www.bull.com/support.

6.3.1 Installing the LAN over USB Windows device driver

When you install Windows, there will be an unknown RNDIS device in the device manager. A Windows INF file is provided, that identifies this device. The signed version of the INF is included in all of the Windows versions of the IMM, UEFI, and DSA update packages. Perform the following steps to install `ibm_rndis_server_os.inf`.

Note These steps only need to be performed if the server is running a Windows operating system and the `ibm_rndis_server_os.inf` file has not been previously installed. The file needs to be installed only once. It is required by Windows operating systems to detect and use the LAN over USB functionality.

1. Obtain a Windows version of the server UEFI code packakge (see *Updating firmware and device drivers* on page 71 for more information).

2. Extract `the ibm_rndis_server_os.inf` and `device.cat` files from the firmware update package and copy them to the \WINDOWS\inf subdirectory.

   Note You can use the `–x path` command-line interface option to extract the files. For more information about this option, see the readme file that comes with the update package.

3. For Windows 2003: Install the `ibm_rndis_server_os.inf` file by right-clicking on the file and selecting **Install**. This generates a PNF file of the same name in `\WINDOWS\inf`.
   For Windows 2008: Go to **Computer Management**, then **Device Manager** and find the RNDIS Device. Select **Properties > Driver > Reinstall driver**. Point the server to the `\Windows\inf` directory where it can find the `ibm_rndis_server_os.inf` file and install the device.

4. Go to **Computer Management** then **Device Manager** and right-click on **Network adapters** and select **Scan for hardware changes**. A small pop-up confirms that the Ethernet device is found and installed. The New Hardware Wizard starts automatically.

5. When you are prompted with the question, "Can Windows connect to Windows Update to search for software?", select **No, not this time**. Click **Next** to continue.

6. When you are prompted with the question, "What do you want the wizard to do?", select **Install from a list or specific location (Advanced)**. Click **Next** to continue.

7. When you are prompted with the statement, "Please choose your search and installation options", select **Don't search. I will choose the driver to install**. Click **Next** to continue.

8. When you are prompted with the statement, "Select a hardware type, and then click Next", select **Network adapters**. Click **Next** to continue.

9. You are prompted with the statement, "Completing the Found New Hardware Wizard". Click **Finish**.

   Note A new local area connection appears and might state, "This connection has limited or no connectivity". Ignore this message

10. Go back to the Device Manager. **IBM USB Remote NDIS Network Device** appears under **Network Adapters**.

11. Use the Network Configuration option of the Setup utility to view or set the IP address. See Table 6-1 on page 75 for information about the IP addresses. See *Using the Setup Utility* on page 60 for information about the Setup utility.

6.3.2 Installing the LAN over USB Linux device driver

Versions of Linux since RHEL5 Update 3 and SLES10 Service Pack 2 support the LAN over USB interface by default. This interface is detected and displayed during the installation of these operating systems.

See Table 6-1 on page 75 for information about the IP addresses.

Note Older Linux distributions might not detect the LAN over USB interface, and might require manual configuration. For information about configuring LAN over USB on specific Linux distributions, see the white paper *Transitioning to UEFI and IMM* on http://www.bull.com/support.

The IMM LAN over USB interface requires that the usbnet and cdc_ether drivers be loaded. If the drivers have not been installed, use modprobe to install them. When these drivers are loaded, the IMM USB network interface shows up as a network device in the operating system. To discover the name that the operating system has assigned to the IMM USB network interface, type:

```
dmesg | grep -i cdc ether
```

Chapter 7. Solving problems

Use these instructions to resolve any problems you may encounter while installing the blade server.

If you install the blade server in the Blade Chassis and the blade server does not start, perform the following actions:

- Make sure that the Blade Chassis is correctly connected to a power source.
- Reseat the blade server in the Blade Chassis (see *Installing the blade server in a Blade Chassis* on page *56*).
- If the power-on LED is flashing slowly, turn on the blade server (see *Turning on the blade server* on page *15*).
- If you have just added a new optional device or component, make sure that it is correctly installed and compatible with the blade server and its components. If the device or component is not compatible, remove it from the blade server, reinstall the blade server in the Blade Chassis, and then restart the blade server.

If the blade server does not start after you have performed the preceding actions, see the *Problem Determination and Service Guide* for your blade server on the *Resource DVD*.

7.1 Diagnostic tools overview

The following tools are available to help you diagnose and solve hardware-related problems:

- **POST codes, error messages, and error logs**
  The POST error codes indicate the detection of a problem. See the *Problem Determination and Service Guide* for more information.
- **Troubleshooting tables**
  The troubleshooting tables list problem symptoms and actions to correct the problems. See the *Problem Determination and Service Guide* for your blade server.
- **Light path diagnostics**
  Use light path diagnostics LEDs on the system board to diagnose system errors. If the system-error LED on the system LED panel on the front or rear of the Blade Chassis is lit, one or more error LEDs on the Blade Chassis components also might be lit. These LEDs help identify the cause of the problem. Blade server error LEDs are described in the *Problem Determination and Service Guide* for your blade server.
- **Dynamic System Analysis (DSA) Installable and Portable Edition diagnostic program**
  DSA Installable and DSA Portable diagnostic programs collect and analyze system information to aid in the diagnosing of system problems. These programs operate while the operating system is running, and therefore include operating system-related information in their collection. DSA Installable and DSA Portable diagnostic programs collect the following information about the server:
  - Drive health information
  - Event logs for ServeRAID controllers and service processors
  - Hardware inventory, including PCI and USB information

- Light path diagnostics status
- LSI RAID and controller configuration
- Network interfaces and settings
- ServeRAID configuration
- Service processor status and configuration
- System configuration
- Vital product data, firmware, and Unified Extensible Firmware Interface (UEFI) configuration
- Microprocessor, input/output hub, and UEFI error logs
- Scalability link status
- Operating System information, such as device drivers and installed applications

DSA creates a DSA log, which is a chronologically ordered merge of the system-event log (as the IPMI event log), the integrated management module (IMM) chassis-event log (as the ASM event log), and the operating-system event logs. You can send the DSA log as a file to Bull service or view the information as a text file or HTML file.

Note If you are unable to find the system-error logs in the blade server firmware code, view the system-event log in the Blade Chassis management module.

- **Dynamic System Analysis (DSA) Preboot diagnostic program**

The DSA Preboot diagnostic programs are stored in read-only memory and collect and analyze system information to aid in diagnosing server problems.
The diagnostic programs collect the following information about the server:

- Drive health information
- Event logs for ServeRAID controllers and service processors
- Hardware inventory, including PCI and USB information
- Light path diagnostics status
- LSI RAID and controller configuration
- Network interfaces and settings
- ServeRAID configuration
- Service processor status and configuration
- System configuration
- Vital product data, firmware, and Unified Extensible Firmware Interface (UEFI) configuration
- Microprocessor, input/output hub, and UEFI error logs
- Scalability Link status

DSA creates a DSA log, which is a chronologically ordered merge of the system-event log (as the IPMI event log), the integrated management module (IMM) chassis-event log (as the ASM event log), and the operating-system event logs. You can send the DSA log as a file to Bull service or view the information as a text file or HTML file.
DSA Preboot offers the following diagnostic tests of your server:

- Microprocessor
- Memory
- IMM I_2C
- Optical (CD or DVD) drive
- Ethernet controller

For more information about diagnostic programs and error messages, see the *Problem Determination and Service Guide*.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just more information about our products, Bull provides a wide variety of sources to assist you. This appendix indicates where to go for additional information about Bull and Bull products, what to do if you experience a problem with your Bull Blade system, and who to call for service if necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Check for updated BIOS, firmware, or operating system device drivers for your system. The Bull Warranty terms and conditions state that you, the owner of the Bull product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your Bull service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to http://www.bull.com/support and check for information to help you solve the problem.
- Gather the following information to provide to Bull service. This data will help Bull service quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Bull 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system BIOS and firmware levels
  - Other pertinent information such as error messages and logs

You can solve many problems without outside assistance by following the troubleshooting procedures that are provided in your system and software documentation. Most systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, refer to the appropriate software documentation.

If you have not been able to solve the problem yourself, contact your Bull Support Representative.

Using the documentation

Information about your Bull Blade system and pre-installed software, if any, is available in the documentation that comes with your system. The documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Bull maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.bull.com/support and select your system.

Appendix B. Notices

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from Bull.

Maximum memory may require replacement of the standard memory with an optional memory module.

Bull makes no representation or warranties regarding non-Bull products and services, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

Bull makes no representations or warranties with respect to non-Bull products. Support (if any) for the non-Bull products is provided by the third party, not Bull.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Particulate contamination

Use the particulates and gases specifications to create a safe operating environment for your blade server.

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the server that is described in this document. Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the server to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Bull determines that the levels of particulates or gases in your environment have caused damage to the server, Bull may condition provision of repair or replacement of servers or parts on implementation of appropriate remedial measures to mitigate such environmental contamination.
Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1]ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2]The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3]ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Table B-1. Limits for particulates and gases

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. Bull encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed.

Notice:

This mark applies only to countries within the European Union (EU) and Norway.

This appliance is labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

注意:

このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE)のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque:

Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'étiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local Bull representative.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Bull is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user ’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d’Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Bull cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-Bull option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese Class A warning statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Chinese Class A warning statement

声　　明

此为 A 级产品。在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japanese Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 68FE 01