FUJITSU

FUJITSU Server PRIMERGY TX1320 M3

Upgrade and Maintenance Manual

April 2017

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Copyright 2017 FUJITSU LIMITED

All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

– The contents of this manual may be revised without prior notice.
– Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
– No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.

Microsoft, Windows, Windows Server, and Hyper V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Before reading this manual

For your safety

This manual contains important information for safely and correctly using this product.

Carefully read the manual before using this product. Pay particular attention to the accompanying manual "Safety Notes and Regulations" and ensure these safety notes are understood before using the product. Keep this manual and the manual "Safety Notes and Regulations" in a safe place for easy reference while using this product.

Radio interference

This product is a "Class A" ITE (Information Technology Equipment). In a domestic environment this product may cause radio interference, in which case the user may be required to take appropriate measures. VCCI-A

Aluminum electrolytic capacitors

The aluminum electrolytic capacitors used in the product's printed circuit board assemblies and in the mouse and keyboard are limited-life components. Use of these components beyond their operating life may result in electrolyte leakage or depletion, potentially causing emission of foul odor or smoke.

As a guideline, in a normal office environment (25°C) operating life is not expected to be reached within the maintenance support period (5 years). However, operating life may be reached more quickly if, for example, the product is used in a hot environment. The customer shall bear the cost of replacing replaceable components which have exceeded their operating life. Note that these are only guidelines, and do not constitute a guarantee of trouble-free operation during the maintenance support period.

High safety use

This product has been designed and manufactured to be used in commercial and/or industrial areas as a server.

When used as visual display workplace, it must not be placed in the direct field of view to avoid incommoding reflections (applies only to TX server systems).

The device has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk of life or body if such safety cannot be assured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Measures against momentary voltage drop

This product may be affected by a momentary voltage drop in the power supply caused by lightning. To prevent a momentary voltage drop, use of an AC uninterruptible power supply is recommended.

(This notice follows the guidelines of Voltage Dip Immunity of Personal Computer issued by JEITA, the Japan Electronics and Information Technology Industries Association.)

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by Fujitsu may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Harmonic Current Standards

This product conforms to harmonic current standard JIS C 61000-3-2.

Only for Japan: About SATA HDDs

The SATA version of this server supports HDDs with SATA / BC-SATA storage interfaces. Please note that the usage and operation conditions differ depending on the type of HDD used.

Please refer to the following internet address for further information on the usage and operation conditions of each available type of HDD:

http://jp.fujitsu.com/platform/server/primergy/harddisk/

Only for Japan:

Shielded LAN cables should be used in this product.

Version History

Issue number	Reason for update
1.0 / May 2017	Initial release

Contents

Contents

1 Introduction

This Upgrade and Maintenance Manual provides instructions for the following procedures:

- Upgrading the server configuration by adding optional hardware components
- Upgrading the server configuration by replacing existing hardware components with superior ones.
- Replacing defective hardware components

This manual focuses on on-site maintenance tasks. It is recommended to prepare each service assignment following remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual (see section "Documents you need at hand" on page 33.

CAUTION!

The document at hand comprises procedures of a wide range of complexity. Check the profile of qualification for technicians before assigning tasks. Before you start, carefully read "Classification of procedures" on page 26.

1.1 Notational conventions

The following notational conventions are used in this manual:

Text in italics	indicates commands or menu items
`fixed font`	indicates system output
`semi-bold fixed font`	indicates text to be entered by the user
"Quotation marks"	indicate names of chapters and terms that are being emphasized
►	describes activities that must be performed in the order shown
Abc	indicates keys on the keyboard
 **CAUTION!**	Pay particular attention to texts marked with this symbol! Failure to observe this warning may endanger your life, destroy the system or lead to the loss of data.
	indicates additional information, notes and tips
	indicates the procedure category in terms of complexity and qualification requirements, see "Classification of procedures" on page 26
	indicates the average task duration, see "Average task duration" on page 29

2 Before you start

Before you start any upgrade or maintenance task, please proceed as follows:

- Carefully read the safety instructions in chapter "Important information" on page 35.
- Make sure that all necessary manuals are available. Refer to the documentation overview in section "Documents you need at hand" on page 33. Print the PDF files if required.
- Make yourself familiar with the procedure categories introduced in section "Classification of procedures" on page 26.
- Ensure that all required tools are available according to section "Tools you need at hand" on page 30.

Advanced Thermal Design

The Advanced Thermal Design option allows you to operate the system with a wider temperature range of 5 °C to 40 °C, depending on your system and configuration.

This option can only be ordered from the manufacturer and is indicated by the respective logo on the identification rating plate.

CAUTION

In a system that is configured with Advanced Thermal Design, only certain components which support the respectively increased higher operating temperature range may be installed and used. For applicable restrictions, please refer to the official configurator tool.

Installing optional components

The operating manual of your server gives an introduction to server features and provides an overview of available hardware options.

Use the Fujitsu ServerView Suite management software to prepare hardware expansions. ServerView Suite documentation is available online at:
http://manuals.ts.fujitsu.com

For Japan:
http://www.fujitsu.com/jp/products/computing/servers/primergy/manual/

Please refer to the following ServerView Suite topics:

– Operation
– Virtualization
– Maintenance
– Out-Of-Band Management

For the latest information on hardware options, refer to your server's hardware configurator available online at the following address:
http://ts.fujitsu.com/products/standard_servers/index.htm

For Japan:
http://www.fujitsu.com/jp/products/computing/servers/primergy/

Please contact your local Fujitsu customer service partner for details on how to order expansion kits or spare parts. Use the Fujitsu Illustrated Spares Catalog to identify the required spare part and obtain technical data and order information. Illustrated Spares catalogs are available online at *http://manuals.ts.fujitsu.com/illustrated_spares*.

Replacing a defective component

The global error indicators on the front and rear sides of your server as well as local diagnostic LEDs on the front panel report defective hardware components that need to be replaced. For further information on the controls and indicators of your server, refer to the operating manual of your server and section "Connectors and indicators" on page 337.

If the system has been powered off in order to replace a non-hot plug unit, a system of PRIMERGY diagnostic indicators guides you to the defective component. The "Indicate CSS" button enables the indicator next to the defective component even if the server has been switched off and disconnected

from the mains. For further information, please refer to sections "Using diagnostics information" on page 49 and "Indicators on the front panel" on page 341.

If the defective component is a customer replaceable unit included in the CSS concept (Customer Self Service), the CSS indicators on the front and rear side of the server will light up.

It is recommended to prepare local maintenance tasks using remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual.

2.1 Classification of procedures

The complexity of maintenance procedures varies significantly. Procedures have been assigned to one of three unit categories, indicating the level of difficulty and required qualification.

At the beginning of each procedure, the involved unit type is indicated by one of the symbols introduced in this section.

Please ask your local Fujitsu service center for more detailed information.

2.1.1 Customer Replaceable Units (CRU)

Customer Replaceable Units (CRU)

Customer Replaceable Units are intended for customer self service and may be installed or replaced as hot-plug components during operation.

Components that the customer is entitled to replace may differ according to the service form in his country.

Hot-plug components increase system availability and guarantee a high degree of data integrity and fail-safe performance. Procedures can be carried out without shutting down the server or going offline.

Components that are handled as Customer Replaceable Units

– Hot-plug PSUs
– Hot-plug HDD/SSD modules

Peripherals that are handled as Customer Replaceable Units

– Keyboard
– Mouse

2.1.2 Upgrade and Repair Units (URU)

Upgrade and Repair Units (URU)

Upgrade and Repair Units are non hot-plug components that can be ordered separately to be installed as options (Upgrade Units) or are available to the customer through customer self service (Repair Units).

For Japan, customer allows only upgrade. For upgrade units as customer replaceable, please refer to:
http://www.fujitsu.com/jp/products/computing/servers/primergy/

Server management error messages and diagnostic indicators on the front panel and system board will report defective Upgrade and Repair Units as customer replaceable CSS components.

Upgrade and repair procedures involve shutting down and opening the server.

CAUTION!

The device may be seriously damaged or cause damage if it is opened without authorization or if repairs are attempted by unauthorized and untrained personnel.

Components that are handled as Upgrade Units

- ODDs
- Backup drives
- Expansion cards
- Battery backup units
- Memory
- USB Flash Module (UFM)
- SATA Flash module (SATA DOM)

Components that are handled solely as Repair Units

- CMOS battery
- Non hot-plug fans
- Non hot-plug HDDs

2.1.3 Field Replaceable Units (FRU)

Field Replaceable Units (FRU)

Removing and installing Field Replaceable Units involves complex maintenance procedures on integral server components. Procedures will require shutting down, opening and disassembling the server.

CAUTION!

Maintenance procedures involving *Field Replaceable Units* must be performed exclusively by Fujitsu service personnel or technicians trained by Fujitsu. Please note that unauthorized interference with the system will void the warranty and exempt the manufacturer from all liability.

Components that are handled as Field Replaceable Units

- CPUs (replacements)
- SAS/SATA backplanes
- Power backplane / power distribution board
- Front panel and front LAN connection
- System board
- Standard PSU
- Trusted Platform Module (TPM)
- iRMC microSD card

Please ask your local Fujitsu service center for more detailed information.

2.2 Average task duration

Average task duration: 10 minutes

The average task duration including preliminary and concluding steps is indicated at the beginning of each procedure next to the procedure class.

Refer to table 1 on page 29 for an overview of steps taken into account for calculating the average task duration:

Step	included	Explanation
Server shutdown	no	Shutdown time depends on hardware and software configuration and may vary significantly. Software tasks necessary before maintenance are described in section "Starting the maintenance task" on page 75.
Disassembly	**yes**	making the server available
Transport	no	Transporting the server to the service table (where required) depends on local customer conditions.
Maintenance procedures	**yes**	maintenance procedures including preliminary and concluding software tasks
Transport	no	Returning the server to its installation site (where required) depends on local customer conditions.
Assembly	**yes**	reassembling the server
Starting up	no	Booting time depends on hardware and software configuration and may vary significantly.

Table 1: Calculation of the average task duration

2.3 Tools you need at hand

When preparing the maintenance task, ensure that all required tools are available according to the overview below. You will find a list of required tools at the beginning of each procedure.

List of used screws (not valid for Japan)

Screw driver / Bit insert	Screw	Usage	Type
hexagon head 5 mm / cross PZ2 0.6 Nm		Chassis, RDX backup drive, PSU backplane, Slot bracket to expansion card, front USB3.0	M3 x 4.5 mm (silver) C26192-Y10-C67
hexagon head 5 mm / cross PZ2 0.6 Nm		System board	M3 x 6 mm (silver) C26192-Y10-C68
special bit insert one-way head 0.6 Nm		TPM screw	REM 3 x 15 mm (black) C26192-Y10-C176
Phillips PH1 0.09 Nm		UFM nylon screw	M3 x 4 mm (white) A3C40109082

Table 2: List of used screws and tools (not valid for Japan)

Screw driver / Bit insert	Screw	Usage	Type
Phillips PH1 / JIS 1012 type H1 0.4 Nm		TFM module	M2.5 x 4 mm (silver) C26192-Y10-C103 Replacement screw for A3C40137316 / LSZ: L3-25419-01
Phillips PH1 0.4 Nm		HDD cage, HDD backplane	M3 x 3.5 mm (silver) C26192-Y10-C102
Torx Plus 6 0.09 Nm		ODD latch	M2 x 4 mm (black) C26192-Y10-C166

Table 2: List of used screws and tools (not valid for Japan)

List of used screws for Japan

Screw driver / Bit insert	Screw	Usage	Type
Phillips PH2 0.6 Nm		Chassis, RDX backup drive, PSU backplane, slot bracket to expansion card, front USB3.0	M3 x 5 mm with spring and washer (silver) F6-SW2N3-05121

Table 3: List of used screws and tools (Japan)

Screw driver / Bit insert	Screw	Usage	Type
Phillips PH2 0.6 Nm		System board	M3 x 6 mm with spring and washer (silver) F6-SW2N3-06121
Special bit insert 0.6 Nm		TPM	REM 3 x 15 mm (black) C26192-Y10-C176
Phillips PH1 0.09 Nm		UFM nylon screw	M3 x 4 mm (white) A3C40109082
Phillips PH1 / JIS 1012 type H1 0.4 Nm		TFM module	M2.5 x 4 mm (silver) C26192-Y10-C103 Replacement screw for A3C40137316 / LSZ: L3-25419-01
Phillips PH1 / JIS 1012 type H1 0.4 Nm		HDD cage, HDD backplane	M3 x 4 mm (silver) CA32432-0023
Torx Plus 6 0.09 Nm		ODD latch	M2 x 4 mm (black) C26192-Y10-C166

Table 3: List of used screws and tools (Japan)

2.4 Documents you need at hand

Maintenance procedures may include references to additional documentation. When preparing the maintenance task, ensure that all required manuals are available according to the overview below.

– Ensure to store all printed manuals enclosed with your server in a save place for future reference.

– Unless stated otherwise, all manuals are available online at *http://manuals.ts.fujitsu.com* under *x86 servers*.

  In Japan use the following address:
  http://www.fujitsu.com/jp/products/computing/servers/primergy/manual/

Document	Description
"Quick Start Hardware - PRIMERGY Server TX1320 M3" leaflet " はじめにお読みください - PRIMERGY TX1320 M3 " リーフレット for Japan	Quick installation poster for initial operation, available only in printed form
"Safety notes and regulations" manual " 安全上のご注意 " for Japan	Important safety information, available online or as a printed copy
"FUJITSU Server PRIMERGY TX1320 M3 Operating Manual"	available online
"D3373 BIOS Setup Utility for FUJITSU Server PRIMERGY TX1320 M3 Reference Manual"	Information on configurable BIOS options and parameters, available online
System board and service labels	Labels inside the side / top cover outlining connectors, indicators and basic maintenance tasks

Table 4: Documentation you need at hand

Document	Description
Software documentation	– "ServerView Suite Local Service Concept (LSC)" user guide – "ServerView Operations Manager - Server Management" user guide – "iRMC S4 - Integrated Remote Management Controller" user guide
Illustrated Spares catalog	Spare parts identification and information system (not valid for Japan), available for online use or download (Windows OS) at *http://manuals.ts.fujitsu.com/illustrated_spares* or from the CSS component view of the ServerView Operations Manager
Glossary	available online
"Warranty" manual " 保証書 " for Japan	Important information on warranty regulations, recycling and service, available online, or as a printed copy
"Returning used devices" manual	Recycling and contact information, available online, or as a printed copy
"Service Desk" leaflet " サポート＆サービス " for Japan	Not applicable in Japan and other countries that have different regulations for recycling
Additional documentation	RAID documentation, available online at *http://manuals.ts.fujitsu.com* under *x86 Servers - Expansion Cards - Storage Adapters* For Japan: *http://www.fujitsu.com/jp/products/computing/servers/primergy/manual/*
Third party documentation	– Operating system documentation, online help – Peripherals documentation

Table 4: Documentation you need at hand

3 Important information

Depending on your server or the installed options some information is not valid for your server.

CAUTION!

Before installing and starting up a server, please observe the safety instructions listed in the following section. This will help you to avoid making serious errors that could impair your health, damage the server and endanger the data base.

3.1 Safety instructions

The following safety instructions are also provided in the manual "Safety Notes and Regulations" or " 安全上のご注意 ".

This server meets the relevant safety regulations for IT equipment. If you have any questions about whether you can install the server in the intended environment, please contact your sales outlet or our customer service team.

- The actions described in this manual shall be performed by technical specialists. A technical specialist is a person who is trained to install the server including hardware and software.
- Repairs to the server that do not relate to CSS failures shall be performed by service personnel. Please note that unauthorized interference with the server will void the warranty and exempt the manufacturer from all liability.
- Any failure to observe the guidelines in this manual, and any improper repairs could expose the user to risks (electric shock, energy hazards, fire hazards) or damage the equipment.
- Only valid for non hot-plug components
  Before installing/removing internal components to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the power outlet. Failure to do so can cause electric shock or damage.

Before starting up

- During installation and before operating the server, observe the instructions on environmental conditions for your server.

- If the server is brought in from a cold environment, condensation may form both inside and on the outside of the server.

  Wait until the server has acclimatized to room temperature and is absolutely dry before starting it up. Material damage may be caused to the server if this requirement is not observed.

- Only transport the server in its original packaging or in packaging that protects it from impacts and jolts.
  In Japan and APAC, transporting the server in its original packaging does not apply.

Installation and operation

- This server should not be operated in ambient temperatures above 35 °C. For servers with Advanced Thermal Design the ambient temperature can increase to 40 °C or 45 °C.
- If the server is integrated into an installation that draws power from an industrial power supply network with an IEC309 connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for type A connectors.
- The server automatically adjusts itself to a mains voltage, see the type label of your server. Ensure that the local mains voltage lies within these limits.
- This server must only be connected to properly grounded power outlets or connected to the grounded rack internal power distribution server with tested and approved power cords.
- Ensure that the server is connected to a properly grounded power outlet close to the server.
- Ensure that the power sockets on the server and the properly grounded power outlets are easily accessible.
- The On/Off button or the main power switch (if present) does not isolate the server from the mains power supply. In case of repair or servicing disconnect the server completely from the mains power supply, unplug all power plugs from the properly grounded power outlets.
- Always connect the server and the attached peripheral devices to the same power circuit. Otherwise you run the risk of losing data if, for example, the server is still running but a peripheral device (e.g. memory subsystem) fails during a power outage.

- The adequately shielded data cables must be used.

  All data and signal cables must have sufficient shielding. The use of cable type S/FTP Cat5 or higher is recommended.
  Use of unshielded or badly shielded cables may lead to increased emission of interference and/or reduced fault-tolerance of the device.

- Ethernet cabling has to comply with EN 50173 and EN 50174-1/2 standards or ISO/IEC 11801 standard respectively. The minimum requirement is a Category 5 shielded cable for 10/100 Ethernet, or a Category 5e cable for Gigabit Ethernet.

- Route the cables in such a way that they do not create a potential hazard (make sure no-one can trip over them) and that they cannot be damaged. When connecting the server, refer to the relevant instructions in this manual.

- Never connect or disconnect data transmission lines during a storm (risk of lightning hazard).

- Make sure that no objects (e.g. jewelry, paperclips etc.) or liquids can get inside the server (risk of electric shock, short circuit).

- In emergencies (e.g. damaged casing, controls or cables, penetration of liquids or foreign bodies), contact the server administrator or your customer service team. Only disconnect the server from the mains power supply if there is no risk of harming yourself.

- Proper operation of the server (in accordance with IEC 60950-1 resp. EN 60950-1) is only ensured if the server is completely assembled and the rear covers for the installation slots have been fitted (electric shock, cooling, fire protection, interference suppression).

- Only install server expansions that satisfy the requirements and rules governing safety and electromagnetic compatibility and those relating to telecommunication terminals. If you install other expansions, they may damage the server or violate the safety regulations. Information on which server expansions are approved for installation can be obtained from our customer service center or your sales outlet.

- The components marked with a warning notice (e.g. lightning symbol) may only be opened, removed or exchanged by authorized, qualified personnel. Exception: CSS components can be replaced.

- The warranty is void if the server is damaged during installation or replacement of server expansions.

- Only set screen resolutions and refresh rates that are specified in the operating manual for the monitor. Otherwise, you may damage your monitor. If you are in any doubt, contact your sales outlet or customer service center.
- Only valid for non hot-plug components
  Before installing/removing internal components to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the power outlet. Failure to do so can cause electric shock or damage.

  Internal devices remain hot after shutdown. Wait for a while after shutdown before installing or removing internal options.
- Do not damage or modify internal cables or internal devices. Doing so may cause a server failure, fire, or electric shock and will void the warranty and exempt the manufacturer from all liability.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, you must wear an earthing band on your wrist when working with this type of module and connect it to an unpainted, conducting metal part of the server.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Install the screw removed during installation/detaching internal options in former position. To use a screw of the different kind can cause a breakdown of equipment.
- The procedure of installation on this notes might change depending on a configuration of option.

Batteries

- Incorrect replacement of batteries may lead to a risk of explosion. The batteries may only be replaced with identical batteries or with a type recommended by the manufacturer.
- Do not throw batteries into the trash can.

  Batteries must be disposed of in accordance with local regulations concerning special waste.
- Make sure that you insert the battery the right way round.

- The battery used in this server may present a fire or chemical burn hazard if mistreated. Do not disassemble, heat about 100 °C (212F), or incinerate the battery.
- Replace the lithium battery on the system board in accordance with the instructions in the corresponding Upgrade and Maintenance Manual, chapter "System board and components" > "CMOS battery".
- All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). In addition, the marking is provided with the chemical symbol of the heavy metal decisive for the classification as a pollutant:

  Cd Cadmium
  Hg Mercury
  Pb Lead

Working with optical disk drives and media

When working with optical disk drives, these instructions must be followed.

CAUTION!

- Only use CDs/DVDs/BDs that are in perfect condition, in order to prevent data loss, equipment damage and injury.
- Check each CD/DVD/BD for damage, cracks, breakages etc. before inserting it in the drive.

  Note that any additional labels applied may change the mechanical properties of a CD/DVD/BD and cause imbalance and vibrations.

  Damaged and imbalanced CDs/DVDs/BDs can break at high drive speeds (data loss).

  Under certain circumstances, sharp CD/DVD/BD fragments can pierce the cover of the optical disk drive (equipment damage) and can fly out of the drive (danger of injury, particularly to uncovered body parts such as the face or neck).
- High humidity and airborne dust levels are to be avoided. Electric shocks and/or server failures may be caused by liquids such as water, or metallic items, such as paper clips, entering a drive.
- Shocks and vibrations are also to be avoided.
- Do not insert any objects other than the specified CDs/DVDs/BDs.

- Do not pull on, press hard, or otherwise handle the CD/DVD/BD tray roughly.
- Do not disassemble the optical disk drive.
- Before use, clean the optical disk tray using a soft, dry cloth.
- As a precaution, remove disks from the optical disk drive when the drive is not to be used for a long time. Keep the optical disk tray closed to prevent foreign matter, such as dust, from entering the optical disk drive.
- Hold CDs/DVDs/BDs by their edges to avoid contact with the disk surface.
- Do not contaminate the CD/DVD/BD surface with fingerprints, oil, dust, etc. If dirty, clean with a soft, dry cloth, wiping from the center to the edge. Do not use benzene, thinners, water, record sprays, antistatic agents, or silicone-impregnated cloth.
- Be careful not to damage the CD/DVD/BD surface.
- Keep the CDs/DVDs/BDs away from heat sources.
- Do not bend or place heavy objects on CDs/DVDs/BDs.
- Do not write with ballpoint pen or pencil on the label (printed) side.
- Do not attach stickers or similar to the label side. Doing so may cause rotational eccentricity and abnormal vibrations.
- When a CD/DVD/BD is moved from a cold place to a warm place, moisture condensation on the CD/DVD/BD surface can cause data read errors. In this case, wipe the CD/DVD/BD with a soft, dry cloth then let it air dry. Do not dry the CD/DVD/BD using devices such as a hair dryer.
- To avoid dust, damage, and deformation, keep the CD/DVD/BD in its case whenever it is not in use.
- Do not store CDs/DVDs/BDs at high temperatures. Areas exposed to prolonged direct sunlight or near heating appliances are to be avoided.

You can prevent damage from the optical disk drive and the CDs/DVDs/BDs, as well as premature wear of the disks, by observing the following suggestions:

– Only insert disks in the drive when needed and remove them after use.
– Store the disks in suitable sleeves.
– Protect the disks from exposure to heat and direct sunlight.

Laser information

The optical disk drive complies with IEC 60825-1 laser class 1.

CAUTION!

The optical disk drive contains a light-emitting diode (LED), which under certain circumstances produces a laser beam stronger than laser class 1. Looking directly at this beam is dangerous.

Never remove parts of the optical disk drive casing!

Modules with Electrostatic-Sensitive Devices (ESD modules)

Modules with electrostatic-sensitive devices are identified by the following sticker:

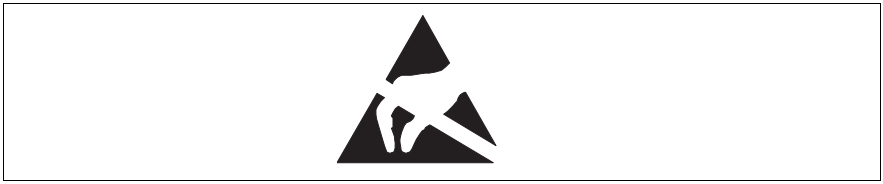

Figure 1: ESD label

The ESD label can be different.

When you handle ESD modules, you must always observe the following points:

- Switch off the server and remove the power plugs from the power outlets before installing or removing ESD modules.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, you must wear an earthing band on your wrist when working with ESD modules and connect it to an unpainted, conducting metal part of the server.
- Any devices or tools that are used must be free of electrostatic charge.

- Wear a suitable grounding cable that connects you to the external chassis of the server.
- Always hold ESD modules at the edges or at the points marked green (touch points).
- Do not touch any connectors or conduction paths on an ESD module.
- Place all the components on a pad which is free of electrostatic charge.

For a detailed description of how to handle ESD modules, see the relevant European or international standards (EN 61340-5-1, ANSI/ESD S20.20).

Transporting the server

CAUTION!

Only transport the server in its original packaging or in packaging that protects it from impacts and jolts.
In Japan and APAC, transporting the server in its original packaging does not apply.

Do not unpack the server until it is at its installation location.

If you need to lift or transport the server, ask other people to help you.

Never lift or carry the server by the handles or the Quick Release Levers (QRLs) on the front panel.

Notes on installing the server in the rack

CAUTION!

- For safety reasons, at least 2 people are required to install the server in the rack because of its weight and size.

  (For the reader in Japan, please refer to " 安全上のご注意 ".)

- Never lift the server into the rack using the QRLs (Quick Release Levers) on the front panel.
- When connecting and disconnecting cables, observe the relevant instructions in the "Important Information" chapter of the technical manual for the corresponding rack. The technical manual is supplied with the corresponding rack.
- When installing the rack, make sure that the anti-tilt mechanism is correctly fitted.

- Do not extend more than one server out of the rack simultaneously even if the tilt protection is in place. If several servers are simultaneously extended from the rack, there is a risk that the rack could tip over. See the safety information of the rack and the warning label.
- If the server/rack is intended for permanent connection to the mains only an authorized specialist (electrician) is allowed to work. Please follow the regulation of each country.
- If the server is integrated into an installation that draws power from an industrial power supply network with an IEC309 type connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for the type A connector.

Other important information

- During cleaning, observe the instructions in the corresponding Operating Manual chapter "Starting up and operation" > "Cleaning the server".
- Keep all manuals close to the server. All documentation must be included if the equipment is passed on to a third party.

3.2 ENERGY STAR

Products that have been certified compliant with ENERGY STAR and labelled are in full compliance with the specification at shipping. Note that energy consumption can be affected by software that is installed or any changes that are made to the hardware configuration or BIOS or energy options subsequently. In such cases, the properties guaranteed by ENERGY STAR can no longer be assured.

The "ServerView Operations Manager" user guide contains instructions for reading out measurement values, including those relating to current energy consumption and air temperatures. Either the Performance Monitor or the Task Manager can be used to read out CPU utilization levels.

3.3 CE conformity

:The system complies with the requirements of European Regulations. Find the CE declaration on certificate portal: *https://sp.ts.fujitsu.com/sites/certificates/default.aspx*

To open the CE declaration applicable for your system, proceed as follows:

- Select *Industry Standard Servers*.
- Select your model, e.g. *Rack server*.
- Select your system, e.g. *PRIMERGY RX2530 M1*.
- *Select CE Cert <your system>*.

CAUTION!

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

3.4 FCC Class A Compliance Statement

If there is an FCC statement on the device, it applies to the products covered in this manual, unless otherwise specified herein. The statement for other products will appear in the accompanying documentation.

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 and meets all requirements of the Canadian Interference-Causing Equipment Standard ICES-003 for digital apparatus. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in strict accordance with the instructions, may cause harmful interference to radio communications. However, there is no warranty that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Fujitsu is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Fujitsu. The correction of interferences caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

The use of shielded I/O cables is required when connecting this equipment to any and all optional peripheral or host devices. Failure to do so may violate FCC and ICES rules.

3.5 Environmental protection

Environmentally-friendly product design and development

This product has been designed in accordance with the Fujitsu standard for "environmentally friendly product design and development". This means that key factors such as durability, selection and labeling of materials, emissions, packaging, ease of dismantling and recycling have been taken into account. This saves resources and thus reduces the harm done to the environment. Further information can be found at:
http://ts.fujitsu.com/products/standard_servers/index.html

For the reader in Japan:
http://jp.fujitsu.com/platform/server/primergy/concept/

Energy-saving information

Devices that do not need to be constantly switched on should be switched off until they are needed as well as during long breaks and after completion of work.

Packaging information

This packaging information does not apply in Japan and APAC.
Do not throw away the packaging. You may need it later for transporting the server. If possible, the equipment should only be transported in its original packaging.

Information on handling consumables

Please dispose of printer consumables and batteries in accordance with the applicable national regulations.

In accordance with EU directives, batteries must not be disposed of with unsorted domestic waste. They can be returned free of charge to the manufacturer, dealer or an authorized agent for recycling or disposal.

All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). They are also marked with the chemical symbol for the heavy metal that causes them to be categorized as containing pollutants:

Cd Cadmium
Hg Mercury
Pb Lead

Labels on plastic casing parts

Please avoid sticking your own labels on plastic parts wherever possible, since this makes it difficult to recycle them.

Returns, recycling and disposal

Please handle returns, recycling and disposal in accordance with local regulations.

The device must not be disposed of with domestic waste. This device is labeled in compliance with European directive 2012/19/EU on waste electrical and electronic equipment (WEEE).

This directive sets the framework for returning and recycling used equipment and is valid across the EU. When returning your used device, please use the return and collection systems available to you. Further information can be found at:
http://ts.fujitsu.com/recycling

Details regarding the return and recycling of devices and consumables within Europe can also be found in the "Returning used devices" manual, via your local Fujitsu branch, or at:
http://ts.fujitsu.com/recycling

4 Basic hardware procedures

4.1 Using diagnostics information

Use the Fujitsu ServerView Suite management software to plan the upgrade or replacement of hardware components. Please refer to the following ServerView Suite topics:

– Operation
– Maintenance

It is recommended to prepare local maintenance tasks using remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual.

In Japan remote diagnostics procedures are not used.

Please contact your local Fujitsu customer service partner for details on the service concept and on how to order expansion kits or spare parts. Use the Fujitsu Illustrated Spares Catalog to identify the required spare part and obtain technical data and order information. Illustrated Spares catalogs are available online at *http://manuals.ts.fujitsu.com/illustrated_spares* (not valid for Japan).

In Japan the Fujitsu Illustrated Spares Catalog is not used.

Perform the following diagnostics procedures to identify defective servers and components.

4.1.1 Locating the defective server

When working in a datacenter environment, switch on the ID indicator (see section "Connectors and indicators" on page 337) on the front and rear connector panels of the server for easy identification.

- Press the ID button on the front panel, use the iRMC web frontend or the ServerView Operation Manager user interface to switch on the system identification LEDs.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual and the "Integrated Remote Management Controller" user guide.

- When using ServerView Operations Manager to toggle the ID indicator, choose *Single System View* and press the *Locate* button.
- Remember to switch off the ID indicator after the maintenance task has been concluded successfully.

4.1.2 Determining the error class

The Local Service Concept (LSC) allows you to identify defective server components. Failure events are assigned to one of two error classes:

– **Global Error** events that need to be resolved by maintenance personnel

– **Customer Self Service** (CSS) error events that may be resolved by operating personnel

Global Error and CSS LEDs (see section "Connectors and indicators" on page 337) indicate, if the defective component is a customer replaceable unit or if maintenance personnel needs to be dispatched to replace the part.

The indicators also light up in standby mode and after a server restart due to a power failure.

4.1.2.1 Global Error indicator

- Check the Global Error indicator on the front panel of the server.
- For further diagnostics, proceed as follows:
  – Hardware errors:

    Check the System Event Log (SEL) as described in section "Viewing and clearing the System Event Log (SEL)" on page 99.

  – Software / agent related errors:

    Check the ServerView System Monitor, available on Windows or Linux based servers with ServerView agents installed.

    For further information, please refer to the "ServerView System Monitor" user guide.

4.1.2.2 Customer Self Service (CSS) indicator

- ► Check the CSS indicator on the front panel or connector panel of the server.
- ► For further diagnostics, proceed as follows:
  - – Hardware errors:

    Check the System Event Log (SEL) as described in section "Viewing and clearing the System Event Log (SEL)" on page 99.
  - – Software / agent related errors:

    Check the ServerView System Monitor, available on Windows or Linux based servers with ServerView agents installed.

    For further information, please refer to the "ServerView System Monitor" user guide.

4.1.3 Locating the defective component

After determining the error class by the CSS or Global Error indicators (see section "Determining the error class" on page 50), local diagnostic indicators on the system board, HDD modules and PSUs (only slide-in units) allow you to identify the defective component.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual.

4.1.3.1 Local diagnostic indicators on the front

- ► Check the CSS indicator (see section "Connectors and indicators" on page 337) on the front panel or connector panel of the server.

In addition to local diagnostic indicators, CSS or Global Error LEDs indicate, if the defective component is a customer or field replaceable unit.

4.1.3.2 Local diagnostic indicators on the system board

Using the Indicate CSS button

- ► Shut down and power off the server.
- ► Disconnect the AC power cord(s) from the system.

  It is mandatory to disconnect power cords in order to use the Indicate CSS functionality.

- ► Press the Indicate CSS button to highlight defective components (see section "Onboard indicators and controls" on page 339).

Component LEDs

- ► Check the component LEDs on the system board and the server rear (see section "Connectors and indicators" on page 337).

In addition to local diagnostic indicators, CSS or Global Error LEDs indicate, if the defective component is a customer replaceable unit or if a service technician needs to be dispatched to replace the part (see section "Determining the error class" on page 50).

If the system has been powered off to replace a non hot-plug unit, a system of PRIMERGY diagnostics indicators guides you to the faulty component.

4.2 Shutting down the server

CAUTION!

For further safety information, please refer to chapter "Important information" on page 35.

This step is only required when upgrading or replacing non-hot plug components.

- ► Inform the system administrator that the server will be shut down and put offline.
- ► Terminate all applications.
- ► Perform the required procedures described in the preliminary steps of each upgrade or maintenance task.

► Shut down the server.

> If the system is running an ACPI-compliant operating system, pressing the On/Off button will perform a graceful shutdown.

► Switch on the ID indicator on the front and rear connector panels of the server as described in section "Locating the defective server" on page 49.

4.3 Disconnecting the power cord

Standard power supply

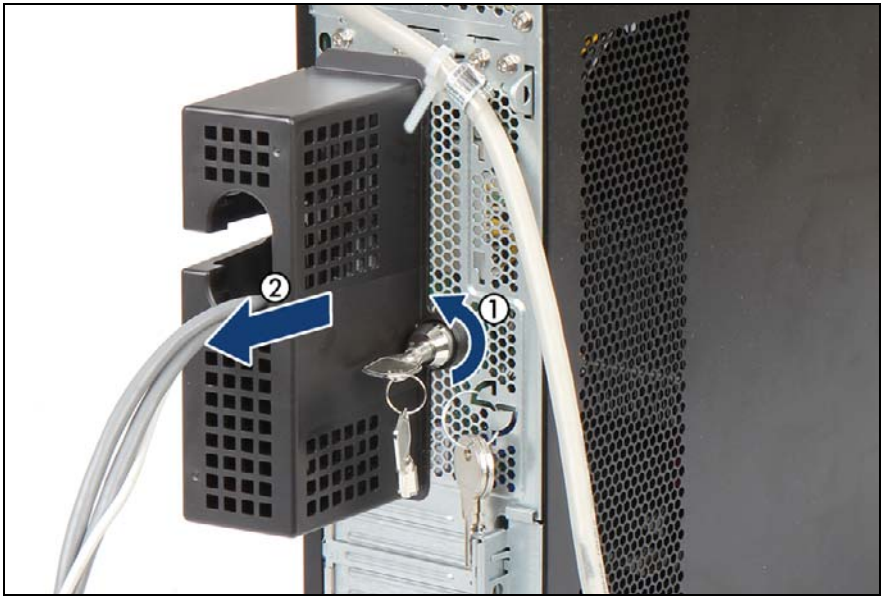

Figure 2: Removing the security cover

► Insert the key (1).

► While pressing the key on the screw turn the key counter-clockwise and remove the screw.

► Remove the security cover (2).

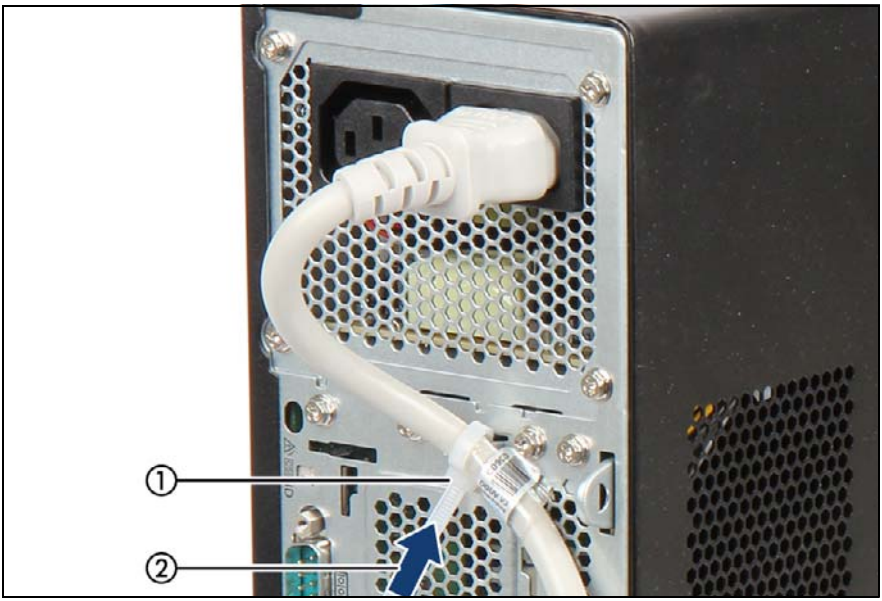

Figure 3: Removing the power cord from the PSU cable tie

- ► Pull out on the locking lever on the PSU cable tie(s) (1) and loosen the loop (2).
- ► Disconnect the power cord from the PSU and remove it from the cable tie.

Redundant power supply

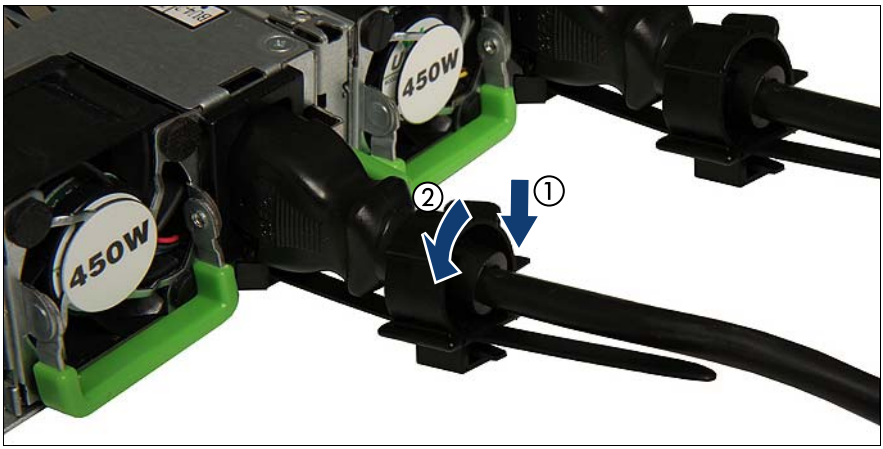

Figure 4: Unlocking the cable clamp of a PSU

- ► Press the cable clamp down until it disengages (1).
- ► Open the cable clamp (2).
- ► Disconnect the power cord from the PSU and remove it from the cable clamp).

4.4 Getting access to the component

CAUTION!

- Before removing or installing covers, turn off the server and all peripheral devices. Also unplug all power cables from the outlet. Failure to do so can cause electric shock.
- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY TX1320 M3 server must not run while the server cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

4.4.1 Removing the server cover

► Remove all external cables from the rear connector panel and expansion cards. For further information, refer to section "Connectors and indicators" on page 337.

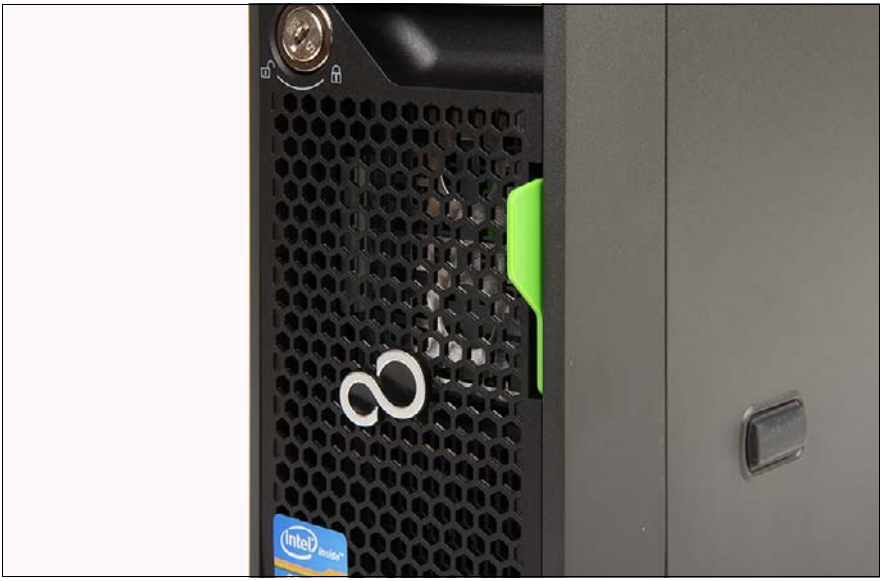

Figure 5: Removing ID card

► Remove the ID card from the server.

It may be necessary to pull out on the ID card rather firmly. However, do not apply excessive force.

Figure 6: Open the lock

► Turn the key counterclockwise to unlock the server cover.

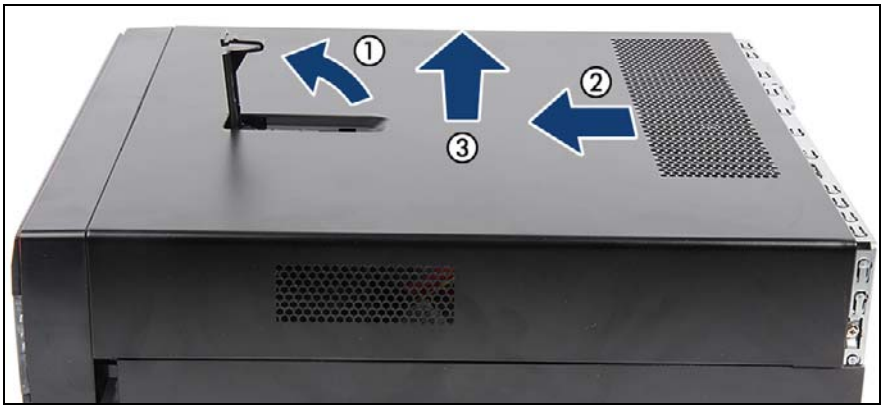

Figure 7: Removing the server cover

► Pull the locking lever up (1).

► Slide the server cover towards the front as far as it will go (2).

► Remove the server cover in a vertical motion (3).

4.4.2 Removing the drive cover

Figure 8: Removing the drive cover

► Turn the key counterclockwise (1) to unlock the drive cover and remove the key.

Depending on the setting of the green hook in the drive cover, you can open the drive cover without turning the key or only with turning the key.

► Open the drive cover carefully in the direction of the arrow (2) until the cover is released and remove it.

CAUTION!

Do not pull too hard to avoid damage to the locking mechanism.

Figure 9: Placing the drive cover in front of the HDD cover

► Place the drive cover on the HDD cover as shown.

4.4.3 Removing the HDD cover

Figure 10: Removing the HDD cover

- ► Turn the key counterclockwise (1) to unlock the drive cover and remove the key.
- ► Open the HDD cover in the direction of the arrow and remove it (2).

4.5 Reassembling

CAUTION!

- Before attaching the covers, make sure no unnecessary parts or tools are left inside the server.
- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY TX1320 M3 server must not run while the server cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

4.5.1 Installing the server cover

Figure 11: Closing the server cover

► Fit the server cover on the chassis, aligning it according to the edge guide markings on the lower server surface.

► Slide the server cover towards the rear as far as it will go (1).

► Fold down the locking lever (2).

4.5.2 Installing the HDD cover

Figure 12: Installing the HDD cover

- ► Insert the HDD cover with the lower side into the server cover (1).
- ► Close the HDD cover (2).

4.5.3 Installing the drive cover

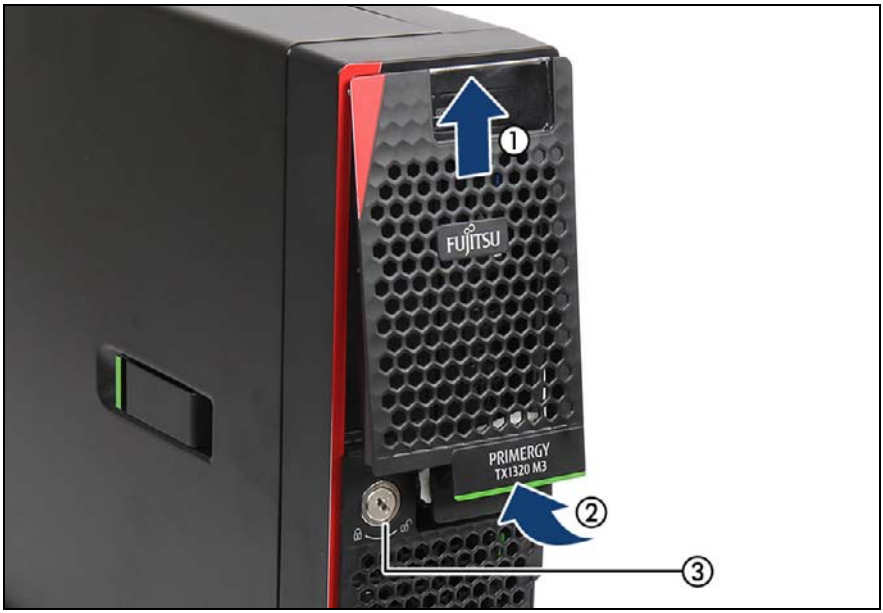

Figure 13: Installing drive cover

- ► Insert the drive cover to the upper side of the server cover (1).
- ► Close the drive cover (2).
- ► Turn the key clockwise (3).

Depending on the setting of the green hook in the drive cover, you can open the drive cover without turning the key or only with turning the key.

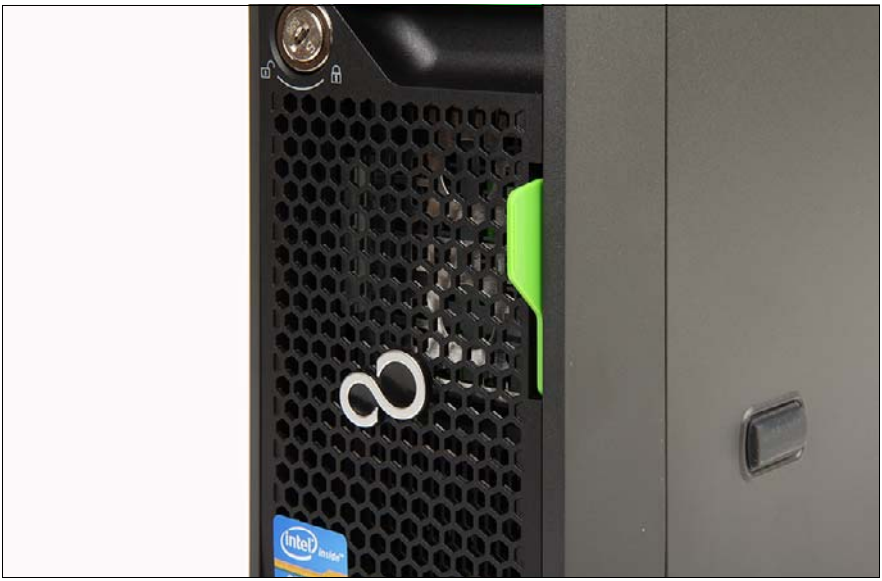

Figure 14: Installing the ID card

► Insert and slide the ID card into its slot until it locks in place.

4.6 Connecting the power cord

CAUTION!

The server supports a mains voltage in the range of 100 V - 240 V. You may only operate the server if its rated voltage range corresponds to the local mains voltage.

Standard power supply

► If applicable, connect the mains plug to a grounded mains outlet in the in-house power supply network.

► Connect the power cord to the PSU.

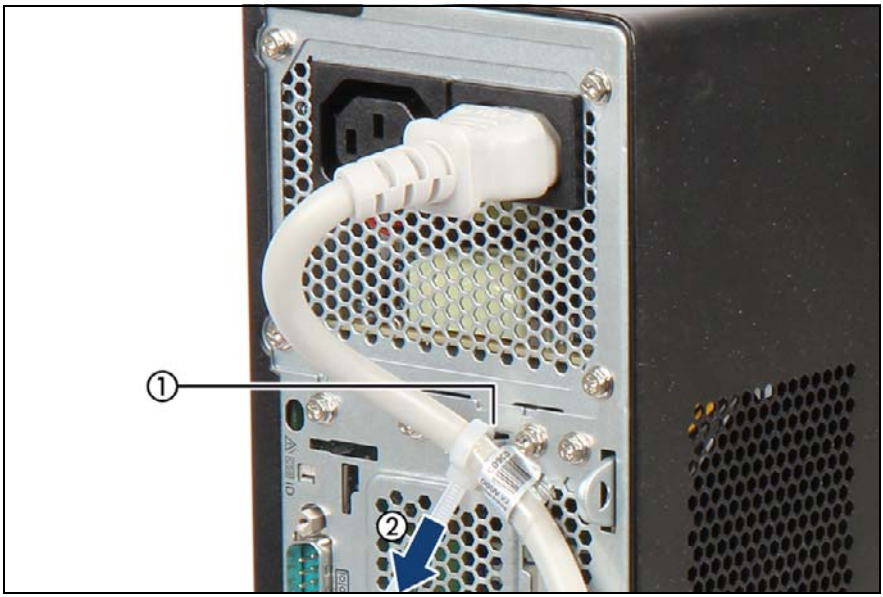

Figure 15: Securing power cord

- ► Thread the cable tie through the eye (1).
- ► Pull the cable tie tight to secure the power cable (2).

  The insulated connector cannot now be disconnected from the server accidentally.

It will take about 60 seconds until the server can be powered on.

Redundant power supply

- ► If applicable, connect the mains plugs to power outlets of the rack socket strip.

  To provide true phase redundancy, the second PSU should be connected to a different AC power source from the other PSU. If one AC power source should fail, the server will still continue to run.

- ► Connect the power cords to the PSUs.
- ► Ensure that the status indicator on the PSU is lit green (see section "Indicators on hot-plug PSUs" on page 351).

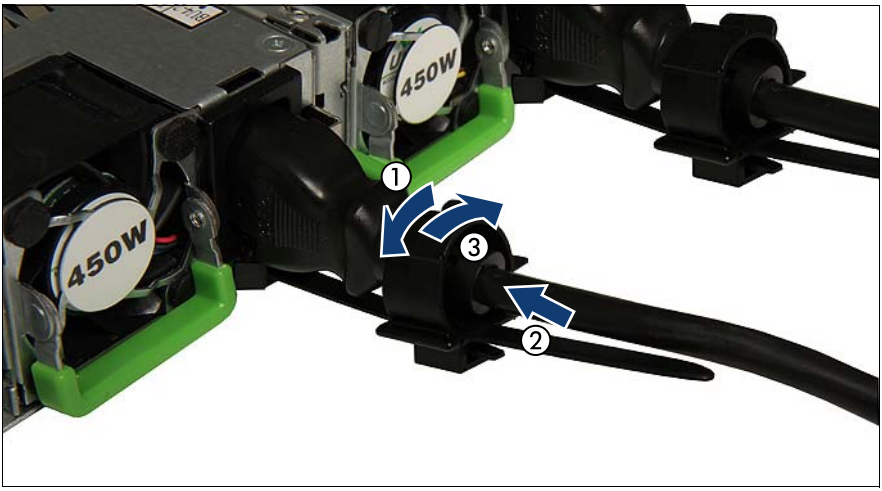

Figure 16: Example: Locking the cable clamp of a PSU

- ► Pull the cable clamp up (1).
- ► Thread the power cord through the cable clamp (2).
- ► Press the cable clamp down until it engages to secure the cable (3).

i It will take about 60 seconds until the server can be powered on.

4.7 Installing the security cover

The PRIMERGY TX1320 M3 can be equipped with an optional security cover.

Figure 17: Rear side of the server

- ► Connect the data cables to the connectors of the external connector panel (1).
- ► Insert the tabs of the security cover into the holes of the rear side of the server (2).

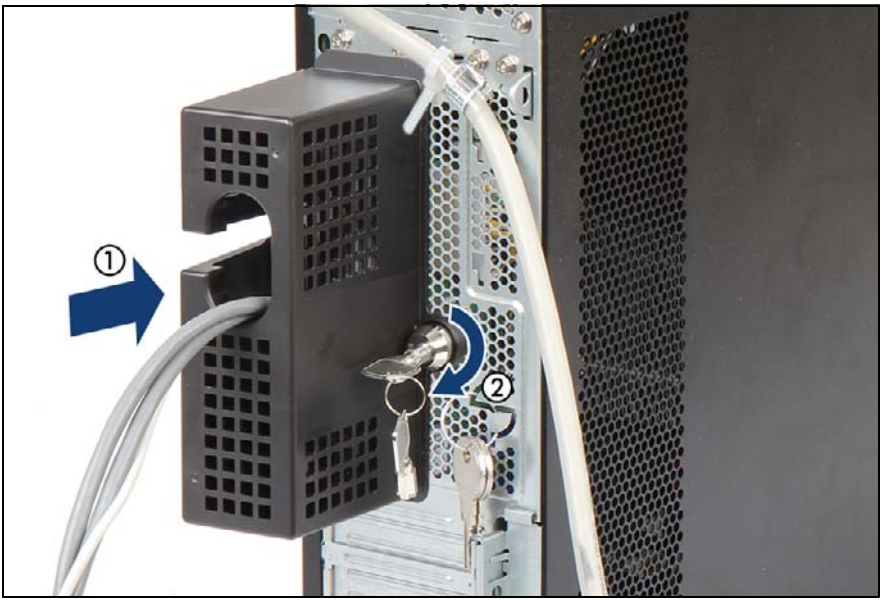

Figure 18: Installing the security cover

- ► Route the cables through the security cover (1).
- ► Insert the screw.
- ► Insert the key.
- ► While pressing the screw turn it clockwise and fasten the security cover (2).

4.8 Switching on the server

CAUTION!

- Before switching on the server, make sure the server cover is closed. In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the server must not run while the server cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

► Press the On/Off button to start up the server.

► Ensure that the power-on indicator is lit green

For more information see "Indicators on the front panel" on page 341.

4.9 Handling the 2.5-inch HDD cage

4.9.1 Removing the HDD cage

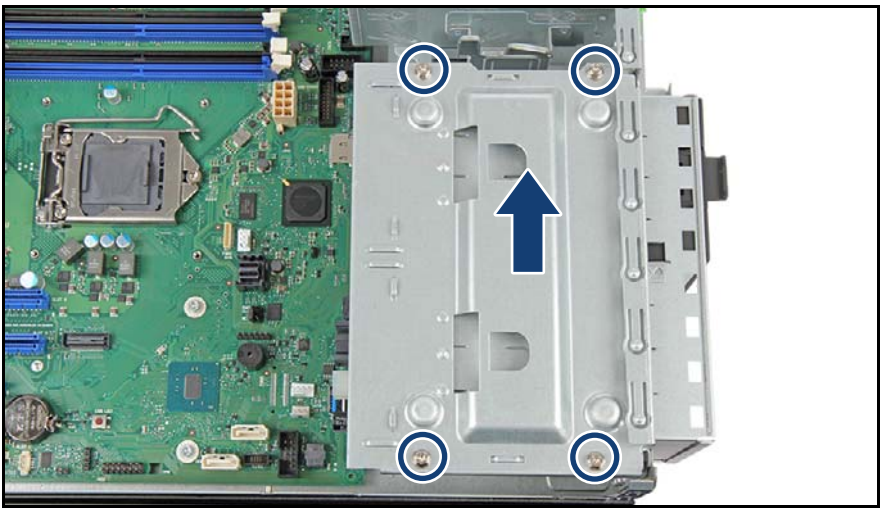

Figure 19: Removing the HDD cage (A)

- ► Remove the four screws (see circles).
- ► Lift the cover from the HDD cage.

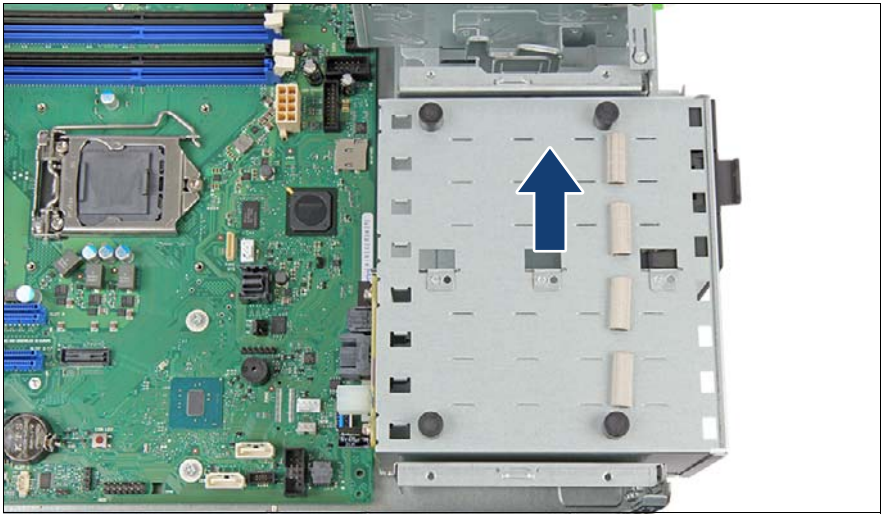

Figure 20: Removing the HDD cage (B)

► Lift the HDD cage out of the chassis (see arrow).

4.9.2 Installing the HDD cage

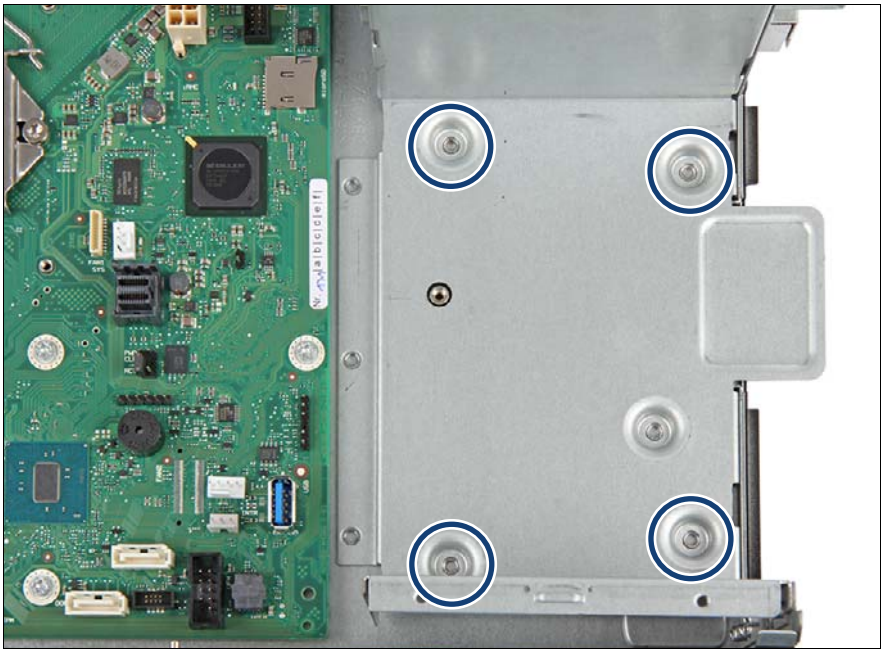

Figure 21: Recesses for the HDD cage (A)

► Note the designated recesses for the HDD cage (see circles).

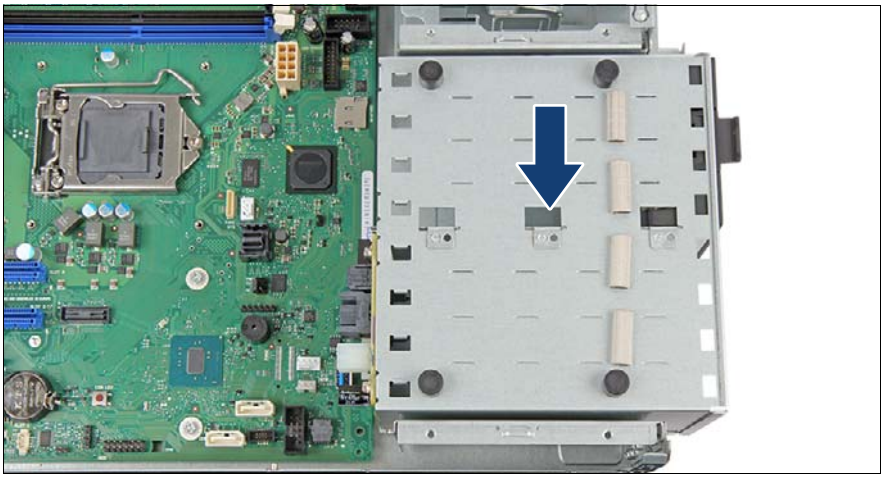

Figure 22: Installing the HDD cage (A)

► Put the HDD cage with its rubber feet into the designated recesses (see arrow).

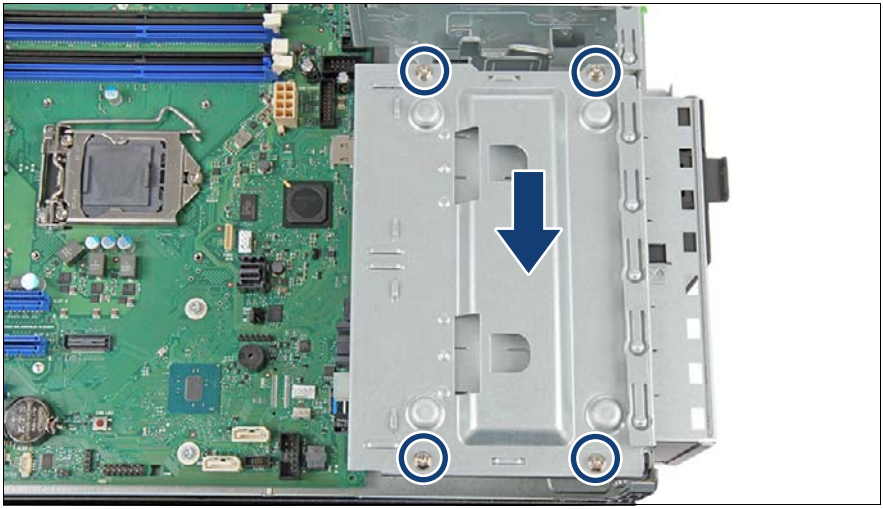

Figure 23: Installing the HDD cage (B)

► Put the cover onto the HDD cage (see arrow).

► Fasten the HDD cage with four screws and tighten them in a cross diagonal pattern (see circles).

5 Basic software procedures

5.1 Starting the maintenance task

5.1.1 Suspending BitLocker functionality

BitLocker Drive Encryption provides protection for operating system and data drives by encrypting the contents and requiring users to authenticate their credentials to access the information. In the scenario described here, BitLocker uses the compatible Trusted Platform Module (TPM) to detect if the computer's startup process has been modified from its original state.

For additional information on how to use BitLocker on a computer without a compatible TPM, please refer to the "BitLocker Drive Encryption" documentation page at *http://technet.microsoft.com/library/cc731549.aspx.*

Suspending BitLocker Drive Encryption is a temporary method for removing BitLocker protection without decrypting the drive Windows is installed on. Suspend BitLocker before modifying the server's hardware configuration or startup files. Resume BitLocker again after the maintenance procedure is complete.

CAUTION!

– With BitLocker features enabled, modifying the system configuration (hardware or firmware settings) may render the system inaccessible. The system may enter Recovery Mode and require a 48-digits recovery password to return to normal operation.

  Ensure to suspend BitLocker drive encryption before maintaining the server.

– When suspended, BitLocker uses a plain text key instead of the Trusted Platform Module (TPM) to read encrypted files. Keep in mind that information on this drive is not secure until BitLocker has been re-enabled.

► Ask the system administrator to suspend BitLocker-protection on the system volume, using the *BitLocker Drive Encryption* control panel item.

This will temporarily disable BitLocker for maintenance purposes. The volume will not be decrypted and no keys will be discarded.

For Windows Server 2008:

- Open BitLocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *BitLocker Drive Encryption*.
- Select the system volume, and click *Turn Off BitLocker*.
- From the *Turn Off BitLocker* dialog box, click *Disable BitLocker*.

For Windows Server 2008 R2 and above:

- Open BitLocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *System and Security*, and then clicking *BitLocker Drive Encryption*.
- Select the system volume, and click *Suspend Protection*.
- Click *Yes* to confirm that your data will not be protected while BitLocker is suspended.

In order to determine which features are accessible through the BitLocker setup wizard, it may be necessary to modify the BitLocker Group Policy settings.

For further information on how to suspend BitLocker drive encryption, please refer to the Microsoft TechNet library at *http://technet.microsoft.com/library/cc731549.aspx.*

Please refer to the Fujitsu web pages for more details.

5.1.2 Disabling SVOM boot watchdog functionality

The ServerView Operations Manager boot watchdog determines whether the server boots within a preset time frame. If the watchdog timer expires, the system will automatically reboot.

5.1.2.1 Viewing boot watchdog settings

Viewing boot watchdog settings in the BIOS

- Enter the BIOS.
- Select the *Server Mgmt* menu.

- Under *Boot Watchdog*, you can obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For detailed information on BIOS settings, refer to the corresponding BIOS Setup Utility reference manual.

Viewing boot watchdog settings in the iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Select the *Server Management* menu.
- Under *Watchdog Settings*, you can obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

Viewing boot watchdog settings in ServerView Operations Manager

- In ServerView Operations Manager *Single System View* select *Maintenance* from the *Information / Operation* menu.
- Under *ASR&R* select the *Watchdog* tab to obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For more detailed information, refer to the "ServerView Operations Manager - Server Management" user guide.

5.1.2.2 Configuring boot watchdog settings

If the system is to be started from removable boot media for firmware upgrade purposes, the Boot watchdog needs to be disabled before starting maintenance task. Otherwise, the Boot watchdog might initiate a system reboot before the flash process is complete.

CAUTION!

An incomplete firmware upgrade process may render the server inaccessible or result in damaged / destroyed hardware.

Timer settings can be configured in the BIOS or using the ServerView iRMC web frontend.

Configuring boot watchdog settings in the BIOS

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Watchdog* set the *Action* setting to *Continue*.
- ► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

Configuring boot watchdog settings using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Server Management* menu.
- ► Under *Watchdog Settings* select *Continue* from the *Boot Watchdog* drop down list.
- ► Click *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.1.3 Removing backup and optical disk media

- ► Ask the system administrator to eject all remaining backup or optical media from the backup or optical disk drive before removing it from the server.
- ► If the backup media cannot be ejected by conventional means, and it is mandatory that the cartridge be removed prior to returning the drive for repair or disposing it, a manual tape extraction needs to be performed. For further information on "forcible" tape ejection, please refer to the "Tape Facts" pages available to Fujitsu service partners from the following https address:
  http://jp.fujitsu.com/platform/server/primergy/harddisk/(not valid for Japan)

  For Japan, please contact Fujitsu support, if "forcible" tape ejection is necessary.

  Fujitsu does not assume responsibility for any damage to the tape drive, the data cartridge / tape or for the loss of any data resulting from manual tape extraction procedures.

5.1.4 Verifying and configuring the backup software solution

This task only applies to Japan.

Depending on the backup software solution, it may be necessary to disable or delete the backup drive from the backup software drive list before starting the maintenance task.

Further information on suitable backup software solutions and related documentation is available from the Fujitsu web pages.

5.1.5 Configuring LAN teaming

Use ServerView Operations Manager to obtain detailed information on existing LAN teams:

- In ServerView Operations Manager *Single System View* select *System Status* from the *Information / Operation* menu.
- Under *Network Interfaces* select *LAN Teaming*.
- The *Network Interfaces (Summary)* overview shows all configured LAN teams and their components. Choose a LAN team to display further details:
  - *LAN Team Properties*: Properties of the selected LAN team
  - *LAN Team Statistics*: Available statistics about the selected LAN team

For more detailed information, refer to the "ServerView Operations Manager - Server Management" user guide.

5.1.6 Note on server maintenance in a Multipath I/O environment

When booting your server offline from the ServerView Suite DVD to perform an offline BIOS / firmware update using the ServerView Update DVD or collect diagnostic data using PrimeCollect in a Multipath I/O environment, there is a risk of damaging the system configuration which may leave the system unable to boot.

This is a known restriction of Windows PE with Multipath drivers.

Using Update Manager Express

- If performing an offline BIOS / firmware update, first of all prepare the ServerView Update DVD or USB stick:
  - Download the latest ServerView Update DVD image from Fujitsu:

    ftp://ftp.ts.fujitsu.com/images/serverview

    http://www.fujitsu.com/jp/products/computing/servers/primergy/support/svsdvd/dvd/ (for Japan)
  - Burn the image to a DVD.
  - In order to create a bootable USB stick, please proceed as described in the "Local System Update for PRIMERGY Servers" user guide.
- Before using the ServerView Update DVD or USB stick in an offline environment, properly shut down the server and disconnect all external I/O connections (like LAN, FC or SAS cables) from the system. Only keep mouse, keyboard, video cable and AC power cord connected.

  Ensure that all external I/O connections are uniquely identified so that you can reconnect them into their original locations after concluding the task.

To start Update Manager Express from the (physical) Update DVD or from a USB stick, proceed as follows:

- Prepare your Update DVD or USB stick as described in the "Local System Update for PRIMERGY Servers" user guide.
- Boot the server from the prepared Update DVD or USB stick:

  DVD: ► Switch on the server.

► Right after switching on the server, insert the Update DVD into the DVD drive and close the tray.

USB: ► Connect the USB stick to the server.

► Switch on the server.

If the server does not boot from DVD or USB stick, proceed as follows:

► Reboot the server, e.g. by pressing the reset button on the front or switching the server off and then on again after a few seconds.

► Once the server has been started, press F12 to enter the boot menu.

► Use the ↑ and ↓ cursor keys to select your DVD drive or USB stick as boot device and press ENTER.

The server will now boot from the Update DVD or USB stick.

► After the boot process is complete, select your preferred GUI language.

The Update Manager Express main window will be displayed.

► Finish the intended maintenance task.

For further information, refer to the "Local System Update for PRIMERGY Servers" user guide.

Using PrimeCollect

To start PrimeCollect, proceed as follows:

- ► Before using PrimeCollect in an offline environment, properly shut down the server and disconnect all external I/O connections (like LAN, FC or SAS cables) from the system. Only keep mouse, keyboard, video cable and AC power cord connected.

  Ensure that all external I/O connections are uniquely identified so that you can reconnect them into their original locations after concluding the task.

- ► Switch on the server.
- ► Right after switching on the server, insert the ServerView Suite DVD into the DVD drive and close the drive tray.

  If the server does not boot from DVD, proceed as follows:

  - ► Reboot the server, e.g. by pressing the reset button on the front or switching the server off and then on again after a few seconds.
  - ► Once the server has been started, press F12 to enter the boot menu.
  - ► Use the ↑ and ↓ cursor keys to select your DVD drive as boot device and press ENTER.

  The server will now boot from the ServerView Suite DVD.

- ► After the boot process is complete, select your preferred GUI language.
- ► In the initial Installation Manager startup window, choose *PrimeCollect* from the *Installation Manager mode* section.
- ► Click *Continue* to proceed.
- ► Finish the intended maintenance task.

For further information, refer to the "PrimeCollect" user guide.

Concluding the procedure

- ► After the update or diagnostic procedure has been completed, shut down the server, reconnect all external I/O connections and bring the system back to normal operation.
- ► If necessary, perform this procedure for all remaining servers within the Multipath environment.

5.1.7 Switching on the ID indicator

When working in a datacenter environment or a server room, switch on the ID indicator on the front and rear connector panels of the server for easy identification.

For further information, refer to section "Locating the defective server" on page 49 or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

- Press the ID button on the front panel to switch on the system identification LEDs.

For further information, refer to section "Indicators on the front panel" on page 341.

Using the iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Under *System Overview*, click *Identify LED On* to switch on the ID indicators.

Using ServerView Operations Manager

- In ServerView Operations Manager *Single System View* press the *Locate* button in the title bar to switch on the ID indicators.

5.2 Completing the maintenance task

5.2.1 Updating or recovering the system board BIOS and iRMC

For Japan, follow the instructions provided separately.

After replacing the system board, memory or a CPU, it is essential to upgrade the BIOS and iRMC to the latest version. The latest BIOS and iRMC versions are available from the Fujitsu support internet pages at:

http://ts.fujitsu.com/support/
http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ (for Japan)

Fujitsu does not assume responsibility for any damage done to the server or for the loss of any data resulting from BIOS updates.

5.2.1.1 Updating or recovering the system board BIOS

BIOS flash procedure

- ► Perform the BIOS flash procedure as described in the "BIOS Setup Utility" reference manual of your server.

BIOS recovery procedure

- ► Perform the BIOS recovery procedure as described in the "BIOS Setup Utility" reference manual of your server.

5.2.1.2 Updating or recovering the iRMC

iRMC flash procedure

- ► Prepare a USB stick including the bootable iRMC firmware update image.
- ► Connect the USB stick containing the iRMC firmware to a USB port.
- ► Restart the server. The system will start the POST process.
- ► During POST, press F12 and select the connected USB stick as boot device. The system will detect the USB stick.

► Choose one of the following options from the update tool menu to start the iRMC update process:

Normal
Choose this option to update an existing system board.

Initial Choose this option if the system board has been replaced prior to the iRMC update procedure. This option will perform all relevant flash procedures in a row, including the iRMC firmware and bootloader.

CAUTION!

Do not interrupt the iRMC upgrade process after it has started. If the process is interrupted, the iRMC BIOS may be permanently corrupted.

If the iRMC does not work after flashing, disconnect the system from the mains and reconnect it again.

► After completion of the flash process, remove the USB stick and restart the server.

iRMC recovery procedure

► Prepare a USB stick including the bootable iRMC firmware update image.

► Ensure that the server has been shut down and disconnected from the mains as described in section "Disconnecting the power cord" on page 53.

► Connect the USB stick containing the iRMC firmware to a USB port.

► Connect the server to the mains while pushing the ID button on the front panel. Ask a second person to help you if necessary.

► Ensure that the Global Error indicator and the ID indicator are flashing to indicate that the server is entering the iRMC recovery state.

► Press the Power On/Off button. The system will start the POST process.

► During POST, press F12 and select the connected USB stick as boot device. The system will detect the USB stick.

- Choose the *Recovery_L* option from the update tool menu to start the iRMC update process.

  CAUTION!

  Do not interrupt the iRMC upgrade process after it has started. If the process is interrupted, the iRMC BIOS may be permanently corrupted.

  If the iRMC does not work after flashing, disconnect the system from the mains and reconnect it again.

- Shut down the server by pressing the power On/Off button.
- Disconnect the server from the mains to exit the iRMC recovery state.

5.2.2 Verifying system information backup / restore

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

In order to verify whether the backup or restore process has been successful, check the System Event Log (SEL) using the ServerView Operations Manager (see also section "Viewing and clearing the System Event Log (SEL)" on page 99).

After replacing the system board

- Check the SEL log files as described in section "Replacing the system board" on page 308 to verify whether the backup data on the Chassis ID EPROM has been restored to the system board:

  ```
  Chassis IDPROM: Restore successful
  ```

After replacing the Chassis ID EPROM

- Check the SEL log files as described in section "Viewing and clearing the System Event Log (SEL)" on page 99 to verify whether a backup copy of the system board settings has been transferred to the Chassis ID EPROM:

  ```
  Chassis IDPROM: Backup successful
  ```

5.2.3 Updating RAID controller firmware

After replacing the RAID controller, it is essential to upgrade the firmware to the latest version without connecting any storage devices. The latest RAID controller firmware version is available from the Fujitsu support web pages at:

http://ts.fujitsu.com/support/
http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ (for Japan)

Fujitsu does not assume responsibility for any damage done to the server or for the loss of any data resulting from firmware updates. For Japan, follow the instructions provided separately.

Using the ServerView Update Manager

For a detailed description on how to update the RAID controller firmware using the ServerView Update Manager or Update Manager Express (UME), please refer to the following manuals:

– ServerView Update Manager:
"ServerView Update Management" user guide
– ServerView Update Manager Express:
"Local System Update for PRIMERGY Servers" user guide

Using the flash tool

The latest firmware files are available as ASPs (Autonomous Support Packages) for Windows or as DOS tools from the Fujitsu support web pages at:

http://ts.fujitsu.com/support/
http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ (for Japan)

- ► Select *Drivers & Downloads*.
- ► From the *Select Product* drop down lists, choose your PRIMERGY server or enter its serial or ident number into the search field.
- ► Select your operating system and version.
- ► Select the desired component type (e.g. SAS RAID).
- ► Select your controller from the device list to expand a compilation of available drivers and firmware.
- ► Select the desired file and click *Download* for further instructions.

5.2.4 Enabling Option ROM scan

In order to configure an expansion card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. The card's firmware is called by the system BIOS upon reboot and can be entered and configured.

Option ROM can be enabled permanently (e.g. in case of a boot controller that may require frequent setup) or temporarily for one-time configuration. When permanently enabling a controllers's Option ROM, keep in mind that only two Option ROMs can be activated in the system board BIOS at a time.

- ► Enter the BIOS.
- ► From the *Advanced* menu select *Option ROM Configuration*.
- ► Identify the desired PCI slot and set its *Launch Slot # OpROM* setting to *Enabled.*
- ► Save your changes and exit the BIOS.

Up to two Option ROMs can be activated in the system board BIOS at a time.

For detailed information on how to access the BIOS and modify settings, refer to corresponding BIOS Setup Utility reference manual.

When the enabled expansion card is initialized during the POST phase of the boot sequence, a key combination is displayed temporarily to enter the expansion card's firmware.

- ► Press the displayed key combination.
- ► Modify the expansion card firmware options as desired.
- ► Save your changes and exit the firmware.

The expansion card's option ROM can now be disabled in the system board BIOS.

Exception: If the expansion card controls a permanent boot device, the card's Option ROM has to remain enabled.

5.2.5 Reconfiguring the backup software solution

This task only applies to Japan.

Disabling backup drives

Depending on the backup software solution, it may be necessary to disable or delete the backup drive from the backup software drive list and reconfigure backup jobs after completing the maintenance task.

Further information on suitable backup software solutions and related documentation is available from the Fujitsu web pages.

Re-enabling backup drives

If a backup drive has been disabled or deleted from the backup software drive list as described in section "Verifying and configuring the backup software solution" on page 79, it has to be re-enabled to complete the maintenance task.

- ► Re-enable backup drives and revise backup software settings and cronjobs.

  Further information on suitable backup software solutions and related documentation is available from the Fujitsu web pages.

5.2.6 Resetting the boot retry counter

The boot retry counter is decremented from its preset value every time the POST watchdog initiates a system reboot. When the value has reached ’0’, the system will shut down and power off.

5.2.6.1 Viewing the boot retry counter

The current boot retry counter status is available in the BIOS:

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Retry Counter* the current number of remaining boot attempts is displayed. The value is further decremented with every failed boot attempt or system reboot resulting from critical system errors.
- ► Exit the BIOS.

5.2.6.2 Resetting the boot retry counter

The boot retry counter should be reset to its original value concluding every service task.

Please note, if the customer does not know about the original boot retry values:

If the system boots up and no further errors occur within 6 hours after that successful boot attempt, the boot retry counter will automatically be reset to its default value. Please take into account, that the specified number of boot attempts can only be determined after this period of time.

If the customer knows about the original boot retry values, proceed as follows to reset or configure the boot retry counter:

Resetting the boot retry counter in the BIOS

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Retry Counter* press the [+] or [-] keys to specify the maximum number of boot attempts (0 to 7).
- ► Exit the BIOS.

Resetting the boot retry counter using the ServerView Operations Manager

- In the ServerView Operations Manager *Administration* view, select *Server Configuration*.
- If more than one server is managed in SVOM, select the target server and click *Next*.
- From the *Server Configuration* menu pane, choose *Restart Options*.
- Under *Reboot Retries*, specify the maximum number of boot attempts (0 to 7) in the *Default for reboot tries* field.

Resetting the boot retry counter using iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Select the *Server Management* menu.
- The following boot retry counter settings are available under *ASR&R Options:*
  - Under *Retry counter max* specify the maximum number of attempts to boot the operating system (0 to 7).
  - Under *Retry counter* the current number of remaining boot attempts is displayed. Overwrite this value with the maximum number of boot attempts specified above in order to reset the boot retry counter.
- Click *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.7 Resetting the error status after replacing memory modules or CPUs

5.2.7.1 Memory modules

ServerView Operations Manager may report a defective memory module in case of a memory error.

Important note

After replacing a defective memory module, please check if the error counter has been reset automatically. If the memory slot is still marked as failed, please reset the error counter manually using one of the methods below.

Using the iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Select the *System Information* menu.
- Under *System Components*, select the check boxes next to the affected memory modules.
- From the drop down list, select *Reset Error Counter*.
- Click *Apply* for the changes to take effect.

Using ServerView Maintenance Tools (Windows only)

- Launch the ServerView Maintenance Tools:
  - Windows Server 2008 R2 and below:
    Start > *(All) Programs* > *Fujitsu* > *ServerView Suite* > *Agents* > *Maintenance Tools*
  - Windows Server 2012 and above:
    Start > *Apps* > *Fujitsu* > *Maintenance Tools*
- Choose the *Memory* status tab.
- Select the memory module which shows the pre-failure status.
- Click on *Reset Status*.

  The *Reset Status* button will only be available if the selected memory module contains errors.
- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

Using the command line interface (Linux/VMware only)

The memory error counter can be reset using the `meclear` utility which is part of the ServerView agents for Linux.

`meclear` (Memory Module Error Counter Reset Utility) allows to reset the error count collected for a memory module, for example after it has been replaced.

For further details, please refer to the `meclear` manual pages.

- Log in as root.
- Enter the command below, followed by ENTER:
  `/usr/sbin/meclear`
- Select the number of a memory module with a status other than "OK" or "Not available".
- Repeat the step above until all memory modules show the "OK" status.
- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

5.2.7.2 CPUs

ServerView Operations Manager may report a defective CPU in case of a critical error.

Important note

After replacing a defective CPU, the error counter must be reset manually using one of the methods below.

Using ServerView Maintenance Tools (Windows only)

- Launch the ServerView Maintenance Tools:
  - Windows Server 2008 R2 and below:
    Start > *(All) Programs* > *Fujitsu* > *ServerView Suite* > *Agents* > *Maintenance Tools*
  - Windows Server 2012 and above:
    Start > *Apps* > *Fujitsu* > *Maintenance Tools*
- Choose the *CPU* status tab.
- Select the CPU which shows the pre-failure status.
- Click on *Reset Status*.
- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

Using the command line (Linux only)

Proceed as follows to reset the error counter of a specific CPU:

- Log in as root.
- Enter the command below, followed by ENTER:
  - For rack and tower servers (RX and TX server series):
    `/usr/sbin/eecdcp -c oc=0609 oi=<CPU#>`
  - For blade and scale-out servers (BX and CX server series):
    `/usr/sbin/eecdcp -c oc=0609 oi=<CPU#> cab=<cabinet nr>`

    To identify the cabinet number, enter the following command:
    `/usr/sbin/eecdcp -c oc=E204`

    `<CPU#>` parameters are "0" for CPU 1 and "1" for CPU 2.

- If the error status cannot be reset with the method above, please use the following procedure for resetting the error counter of all CPUs:
  - Log in as root.
  - Enter the commands below, followed by ENTER:

    1. ```
       /etc/init.d/srvmagt stop
       /etc/init.d/srvmagt_scs stop
       /etc/init.d/eecd stop
       /etc/init.d/eecd_mods_src stop
       ```
    2. ```
       cd /etc/srvmagt
       ```
    3. ```
       rm -f cehist.bin
       ```
    4. ```
       /etc/init.d/eecd_mods_src start
       /etc/init.d/eecd start
       /etc/init.d/srvmagt start
       /etc/init.d/srvmagt_scs start
       ```
- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

5.2.8 Enabling SVOM boot watchdog functionality

If ServerView Operations Manager boot watchdog functionality has been disabled for firmware upgrade purposes (see section 5.1.2 on page 76), it has to be re-enabled to complete the maintenance task.

Timer settings can be configured in the BIOS or using the ServerView iRMC web frontend:

Configuring boot watchdog settings in the BIOS

- Enter the BIOS.
- Select the *Server Mgmt* menu.
- Under *Boot Watchdog* set the *Action* setting to *Reset*.
- Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

Configuring boot watchdog settings using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Server Management* menu.
- ► Under *Watchdog Settings* ensure that the check box next to Boot Watchdog is selected. From the drop down list choose *Reset* and specify the desired timeout delay.
- ► Click *Apply* for the changes to take effect.

i For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.9 Enabling replaced components in the system BIOS

When a CPU, an expansion card, or a memory module fails, the defective component will be set to *Disabled* or *Failed* in the system BIOS. The server will then reboot with only the intact hardware components remaining in the system configuration. After replacing the defective component, it needs to be re-enabled in the system board BIOS.

- ► Enter the BIOS.
- ► Select the *Advanced* menu.
- ► Select the status menu of the desired component:
  - CPUs: *CPU Status*

    i This option is only available for multi-processor systems.
  - Memory: *Memory Status*
  - Expansion cards: *PCI Status*
- ► Reset replaced components to *Enable*.
- ► Save your changes and exit the BIOS.

i For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

5.2.10 Verifying the memory mode

If a memory module fails, the server will reboot and the defective module will be disabled. As a result, the current operation mode (e.g. Mirrored Channel mode) may no longer be available due to a lack of identical memory module pairs. In this case, the operation mode will automatically revert to Independent Channel Mode.

For detailed information on memory operation modes available for your server, refer to section "Modes of operation" on page 224.

After replacing the defective module(s) the memory operation mode is automatically reset to its original state. It is recommended to verify that the operation mode has been correctly.

- Enter the BIOS.
- Select the *Advanced* menu.
- Under *Memory Status* verify that none of the memory modules are marked as *Failed*.
- Save your changes (if applicable) and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

5.2.11 Verifying the system time settings

This task only applies to Linux and VMware environments.

After the system board has been replaced, the system time is set automatically. By default, the RTC (Real Time Clock) time standard is set as the local time.

If a Linux OS is used and the hardware clock has been configured as UTC (Universal Time, Coordinated) in the operating system, the BMC local time may not be mapped correctly.

- ► After replacing the system board, ask the system administrator whether the RTC or UTC time standard is to be used as system time.

  If the system time (RTC) is set to UTC, the SEL (System Event Log) time stamps may differ from the local time.

- ► Enter the BIOS.
- ► Select the *Main* menu.
- ► Under *System Time* and *System Date* specify the correct time and date.

  By default, the system time set in the BIOS is RTC (Real Time Clock) local time. If your IT infrastructure relies on universally accepted time standards, set the *System Time* to UTC (Universal Time, Coordinated) instead. Greenwich Mean Time (GMT) can be considered equivalent to UTC.

- ► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual

5.2.12 Viewing and clearing the System Event Log (SEL)

5.2.12.1 Viewing the SEL

You can view the System Event Log (SEL) using the ServerView Operations Manager or the ServerView iRMC web frontend:

Viewing the SEL in ServerView Operations Manager

- In ServerView Operations Manager *Single System View* select *Maintenance* from the *Information / Operation* menu.
- Under *Maintenance* select *System Event Log*.
- Select the message type(s) you want to display:
  - Critical events
  - Major events
  - Minor events
  - Informational events

Note on the SVOM Driver Monitor

The *Driver Monitor* view gives you an overview of the monitored components as well as the associated events contained in the system event log on the managed server.

Under *Monitored Components* the monitored components are listed. If a component has the status *Warning* or *Error*, you can select it in the list and click *Acknowledge*. This confirms the event on the server side. You may have to log on to the server beforehand. The status of the component will then be reset to *ok*. To see the new status you must refresh the *Driver Monitor* view with *Refresh*.

For detailed information on how to view and sort the SEL using ServerView Operations Manager, refer to the "ServerView Operations Manager - Server Management" user guide.

Viewing the SEL using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Event Log* and choose the *Internal Event Log* submenu.
- ► Under *Internal Event Log Content* the SEL is being displayed. In order to filter the list, select the check boxes next to the desired event types and press *Apply* for the changes to take effect.

i For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.12.2 Clearing the SEL

You can clear the System Event Log (SEL) using the ServerView iRMC web frontend:

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Event Log* and choose the *Internal Event Log* submenu.
- ► Under *Internal Event Log Information* click *Clear Internal Event Log* to clear the SEL.

i For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.13 Updating the NIC configuration file in a Linux and VMware environment

In order to prevent errors caused by changing network device names (*eth<x>*), it is recommended to store the MAC address (hardware address) of a network interface card in the related NIC configuration file of the Linux OS.
When replacing a network controller or the system board with onboard LAN controllers in a server running Linux OS, the MAC address will change but not automatically be updated in the definition file.

In order to prevent communication problems, it is necessary to update the changed MAC address stored in the related *ifcfg-eth<x>* definition file.

To update the MAC address, proceed as follows:

i Procedures may differ depending on your Linux OS or the definition file on the client system. Use the following information as reference. Ask the system administrator to change the definition file.

► After replacing a network controller or the system board, switch on and boot the server as described in section "Switching on the server" on page 69.

kudzu, the hardware configuration tool for Red Hat Linux, will launch at boot and detect the new and / or changed hardware on your system.

kudzu may not launch at boot depending on the client's environment.

► Select *Keep Configuration* and *Ignore* to complete the boot process.

► Use the *vi* text editor to specify the MAC address in the HWADDR section of the *ifcfg-eth<x>* file:

The MAC address can be found on the type label attached to the system board or network controller.

Example:

In order to modify the definition file for network controller 1, enter the following command:

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth1
```

In *vi*, specify the new MAC address as follows:

```
HWADDR=xx:xx:xx:xx:xx:xx
```

► Save and close the definition file.

► For the changes to take effect, you need to reboot the network by entering the following command:

```
# service network restart
```

If the system board or network controller offers multiple LAN ports, it is necessary to update the remaining *ifcfg-eth<x>* definition files accordingly.

► Update the NIC configuration file to reflect the new card sequence and MAC address.

5.2.14 Resuming BitLocker functionality

If BitLocker Drive Encryption has been suspended for maintenance purposes (see section "Suspending BitLocker functionality" on page 75), it has to be re-enabled to complete the service task.

If BitLocker Drive Encryption has been suspended prior to replacing components you won't be asked for a recovery key when rebooting the server after the maintenance task. However, if BitLocker functionality has not been suspended, Windows will enter recovery mode and ask you to input recovery key for further booting.

- ► In this case, ask the system administrator to enter the recovery key in order to boot the operating system.

► Ask the system administrator to enable the previously suspended BitLocker-protection on the system volume, using the *BitLocker Drive Encryption* control panel item:

For Windows Server 2008:

- ► Open BitLocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *BitLocker Drive Encryption*.
- ► Select the system volume, and click *Turn On BitLocker*.

For Windows Server 2008 R2 and above:

- ► Open BitLocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *System and Security*, and then clicking *BitLocker Drive Encryption*.
- ► Select the system volume, and click *Resume Protection*.

For further information on how to resume BitLocker drive encryption, please refer to the Microsoft TechNet library at *http://technet.microsoft.com/library/cc731549.aspx.*

Please refer to the Fujitsu web pages for more details.

5.2.15 Performing a RAID array rebuild

After replacing an HDD that has been combined into a RAID array, RAID rebuild will be performed completely unattended as a background process.

- ► Ensure that the RAID array rebuild has started normally. Wait until the progress bar has reached at least one percent.
- ► Inform the customer about the remaining rebuild time, based on the displayed duration estimate.

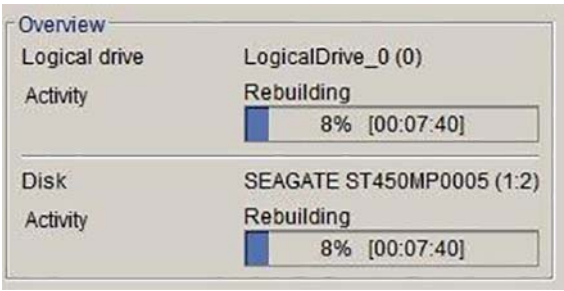

Figure 24: Progress bar (RAID array rebuild)

CAUTION!

The system is now operational, however, data redundancy will not be available until the RAID array rebuild is complete. Depending on the HDD capacity the overall process can take up to several hours, in some cases even days.

You may notice a slight performance impact during rebuild.

5.2.16 Looking up changed MAC / WWN addresses

When replacing a network controller, the MAC (Media Access Control) and WWN (World Wide Name) addresses will change.

In addition to the procedures described below, MAC / WWN addresses can also be found on the type label attached to a network controller or system board.

5.2.16.1 Looking up MAC addresses

- ► Enter the ServerView iRMC web frontend.
- ► Select the *System Information* menu.
- ► Under *Network Inventory*, you will find detailed information on each network controller in the managed PRIMERGY server, including its MAC address.

  This information is only available with the iRMC S4 or above.

  Only network controllers supporting the Command Line Protocol (CLP) will be displayed.
- ► Inform the customer about the changed MAC address.

5.2.16.2 Looking up WWN addresses

Emulex FC / FCoE adapters

- ► Enable the network controller's Option ROM in the system board BIOS as described in section "Enabling Option ROM scan" on page 88.
- ► Restart the server.
- ► During boot, as soon as the Emulex BIOS utility option appears, press ALT + E or CTRL + E.
- ► Under *Emulex Adapters in the System* you will find all available Emulex adapters and their WWN addresses.
- ► Note down the new 16-digit WWN address.
- ► Press Esc to exit the Emulex BIOS utility.
- ► Inform the customer about the changed WWN address.

QLogic FC adapters

- ► Enable the network controller's Option ROM in the system board BIOS as described in section "Enabling Option ROM scan" on page 88.
- ► Restart the server.
- ► During boot, as soon as the QLogic BIOS utility option appears, press ALT + Q or CTRL + Q.
- ► Under *Select Host Adapter* use the arrow keys ↑/↓ to select the desired FC / FCoE adapter and press Enter.

- From the *Fast!UTIL Options* menu, select *Configuration Settings*, and press Enter.
- From the *Configuration Settings* menu, select *Adapter Settings*, and press Enter.
- Note down the new 16-digit WWN address found under *Adapter Port Name*.
- Press Esc to return to the main menu and exit the QLogic BIOS utility.
- Inform the customer about the changed WWN address.

5.2.17 Using the Chassis ID Prom Tool

The Chassis ID EPROM located on a dedicated Chassis ID board or on your server's front panel board contains system information like server name and model, housing type, serial number and manufacturing data.
In order to integrate your system into the ServerView management environment and to enable server installation using the ServerView Installation Manager, system data needs to be complete and correct.

After replacing the Chassis ID EPROM, system information has to be entered using the Chassis ID Prom tool. The tool and further instructions are available from the Fujitsu web pages.

- Select your PRIMERGY system from the main area of the page.
- From the categories selection, choose *Software & Tools Documentation*.
- In the *Tools* area click *Tools: Chassis-IDProm Tool* to download the file (*tool-chassis-Idprom-Tool.zip*).

For Japan, follow the instructions provided separately.

Note on Advanced Thermal Design (ATD)

If the Advanced Thermal Design (ATD) option is available and has been enabled for your server, please set information within the Chassis ID Prom Tool accordingly.
The ATD option can only be ordered from the manufacturer as a factory preset. To find out if your server is ATD-enabled, check for the ATD logo on the identification rating plate.
For ATD logo and further information on Advanced Thermal Design (ATD), please refer to your server's operating manual.

CAUTION!

Please note that you can only set the ATD flag. Resetting the ATD flag using the Chassis ID Prom Tool is not possible!

5.2.18 Configuring LAN teaming

Use ServerView Operations Manager to obtain detailed information on existing LAN teams:

- In ServerView Operations Manager *Single System View* select *System Status* from the *Information / Operation* menu.
- Under *Network Interfaces* select *LAN Teaming*.
- The *Network Interfaces (Summary)* overview shows all configured LAN teams and their components. Choose a LAN team to display further details:
  - *LAN Team Properties*: Properties of the selected LAN team
  - *LAN Team Statistics*: Available statistics about the selected LAN team

For more detailed information, refer to the "ServerView Operations Manager - Server Management" user guide.

5.2.18.1 After replacing / upgrading LAN controllers

- You need to restore the configuration for the LAN Teaming, using the LAN driver utility or OS teaming software.

  Ensure that the controllers have been assigned as primary or secondary according to your requirements.

For details, refer to the relevant LAN driver manual.

5.2.18.2 After replacing the system board

- ► Confirm with the customer whether the onboard LAN controller you have replaced has been used as part of a LAN teaming configuration.
- ► If LAN teaming has been active, you will need to restore the configuration using the LAN driver utility after replacing the system board.

For details, refer to the relevant LAN driver manual.

5.2.19 Switching off the ID indicator

Press the ID button on the front panel, or use the iRMC web frontend or ServerView Operations Manager to switch off the ID indicator after the maintenance task has been concluded successfully.

For further information, refer to section "Locating the defective server" on page 49 or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

- ► Press the ID button on the front panel to switch off the ID indicators.

Using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Under *System Overview*, click *Identify LED Off* to switch off the ID indicators.

Using ServerView Operations Manager

- ► In ServerView Operations Manager *Single System View* and press the *Locate* button in the title bar to switch off the ID indicator.

5.2.20 Performing a fan test

Notes on replacing a defective fan

After replacing a defective system fan or PSU containing a defective fan, the fan error indicators will stay lit until the next fan test. By default, a fan test is automatically started every 24 hours. The first automatic fan test being performed after replacing a fan will turn off the fan error indicator.

If you want to start the fan test manually, you can do so by following the description below:

Executing the fan test via the iRMC Web interface

- Log into the iRMC web interface.
- Under *Sensors* select *Fans*.
- Select the replaced fan in the system fans group and click *Start Fan Test*.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

Executing the fan test via ServerView Operations Manager

- Open the ServerView Operations Manager and log in.
- Under *Administration* select *Server Configuration*.
- In the hierarchy tree of the *Server list* tab, select the server to be configured.
- In the right-hand side of the window, specify the details on the selected server and confirm your entries by clicking *GO...*.

  In the left-hand section of the window, the *Configuration* tab is being activated.
- In the navigation area of the *Configuration* tab, select *Other Settings*.
- Under *Daily Fan Test*, set the daily fan test time to a few minutes from the current time. (Ensure to note down your previous setting.)
- Click *Save Page*.
  The fan test will be started at the specified time.
- After the fan test is complete, restore the time setting to its initial value and click *Save Page*.

For more detailed information, refer to the "ServerView Operations Manager" user guide.

For Japan: Executing the fan test via Chassis ID Prom Tool

Please follow the instructions provided separately.

6 Power supply unit (PSU)

Safety notes

CAUTION!

- Do not disassemble the PSU. Doing so may cause electric shock.
- Areas around the PSU may remain extremely hot after shutdown. After shutting down the server, wait for hot components to cool down before removing the PSU.
- When installing the PSU, be sure to confirm that the connector of the PSU is not damaged or bent.
- Do not insert your hands in the PSU slot when removing the PSU. Doing so may cause electric shock.
- If the PSU is hard to remove, do not pull out it by force.
- The PSU is heavy, so handle it carefully. If you drop it by mistake, injuries may result.
- For further safety information, please refer to chapter "Important information" on page 35.

6.1 Basic information

The server can be equipped:

– with a standard PSU (permanently built-in)

  The PSU adjusts automatically to any mains voltage in the range of 100 V - 240 V.

– or up to two hot-plug PSUs (slide-in units)

  In its basic configuration, the server has one PSU that adjusts automatically to any mains voltage in the range of 100 V - 240 V. Besides the PSU, a second PSU can be installed optionally to serve as a redundant PSU. If one PSU fails, the second PSU in the redundant configuration ensures operation can continue uninterrupted and the defective PSU can be replaced during operation (hot-plug).

– or one hot-plug PSU and a Fujitsu battery unit (FJBU)

Besides the PSU, an FJBU can be installed optionally as a modular UPS. When power fail happened, the server can operate via FJBU for a while. The FJBU can be replaced during operation (hot-plug).

CAUTION!

The server supports a mains voltage in the range of 100 V - 240 V. You may only operate the server if its rated voltage range corresponds to the local mains voltage.

6.2 Standard power supply

6.2.1 Replacing the standard PSU

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

6.2.1.1 Preliminary steps

You are advised to perform this routine with the server in a horizontal position.

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

6.2.1.2 Removing the standard PSU

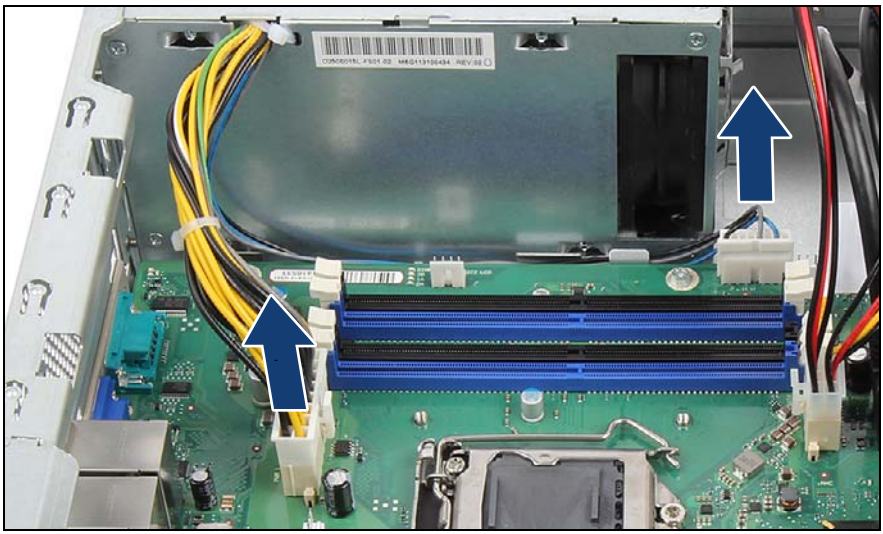

Figure 25: Disconnecting the power cables

► Disconnect the two power cables from the system board connectors "PC2009" and "PWR1".

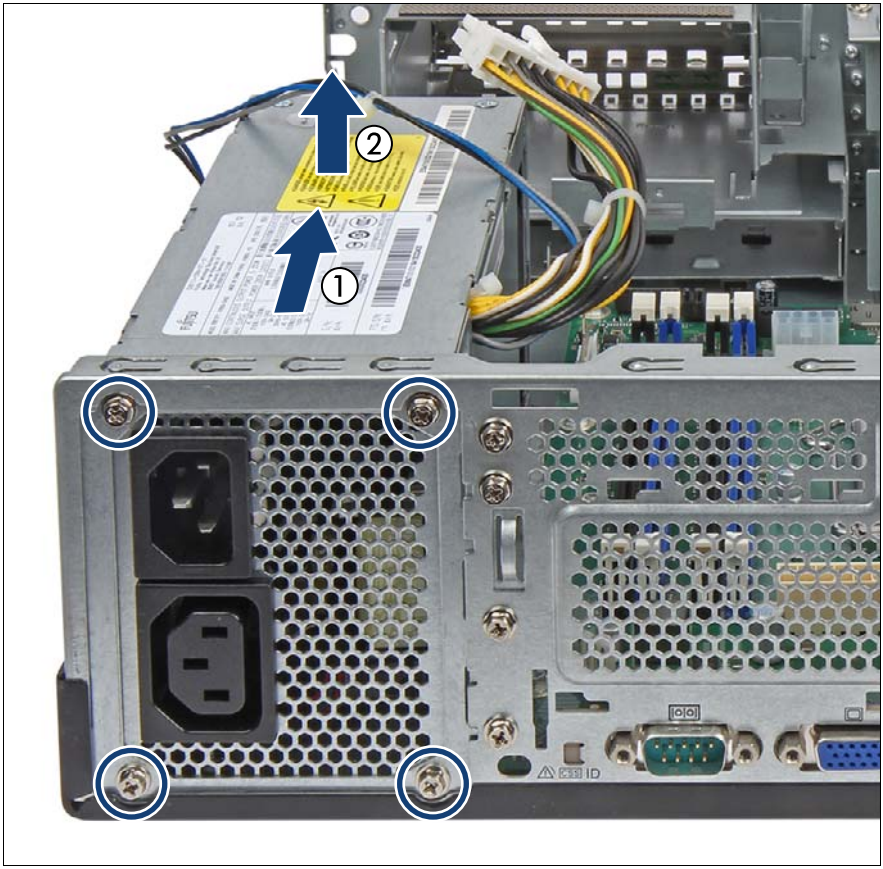

Figure 26: Removing the PSU

- ► Remove the four screws (see circles).
- ► Slide the defective PSU inward by 3 cm (1) to disengage the locking mechanism.
- ► Lift the defective PSU out of the chassis (2).

6.2.1.3 Installing the PSU

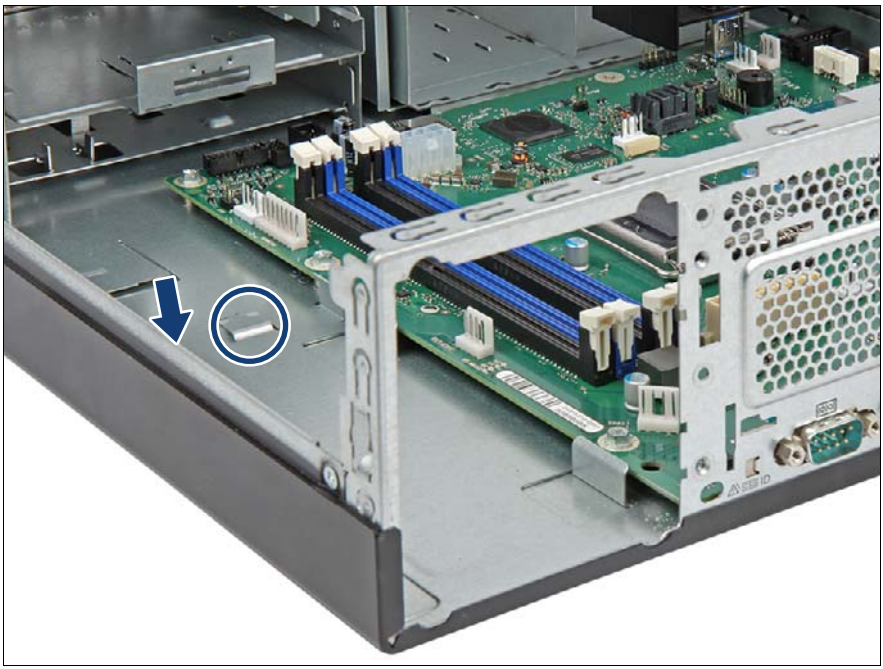

Figure 27: Hooks in the bottom of the chassis

► Take note of the two hooks (see arrow and circle).

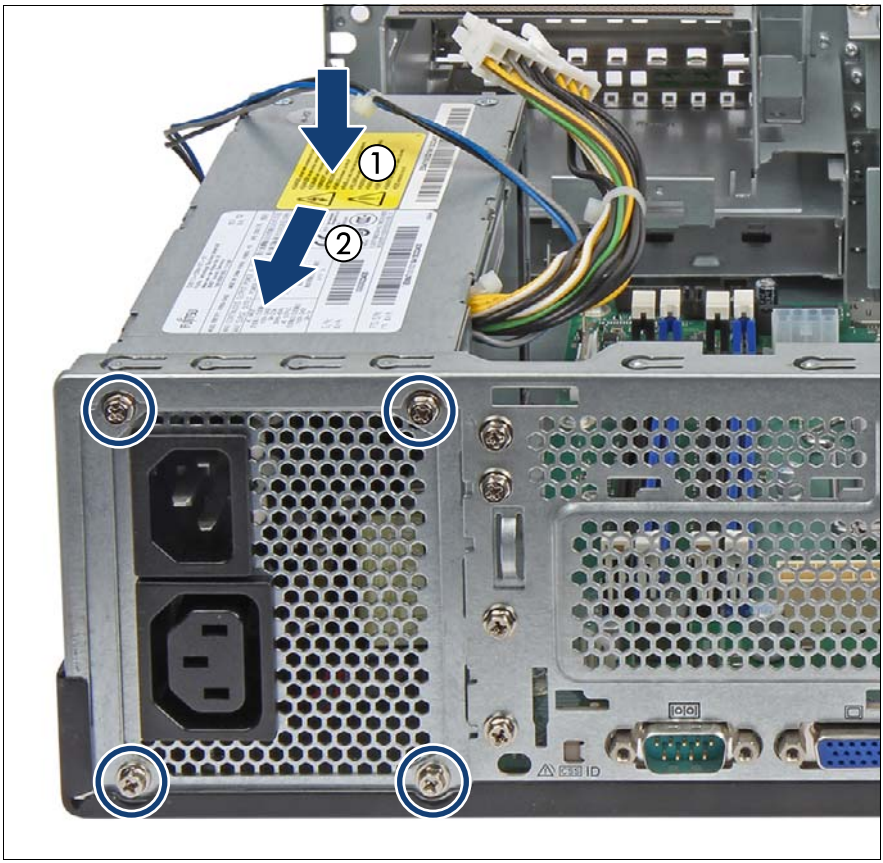

Figure 28: Installing the standard PSU

- ► Insert the PSU into the chassis leaving a gap of about 3 cm to the rear chassis wall (1).
- ► Ensure that the hooks on the chassis (see circle in figure 27) engages with the notch on the lower surface of the PSU.
- ► Slide the new PSU towards the rear of the chassis (2).
- ► Fasten the PSU with four screws (see circles).

6.2.1.4 Connecting internal power cables

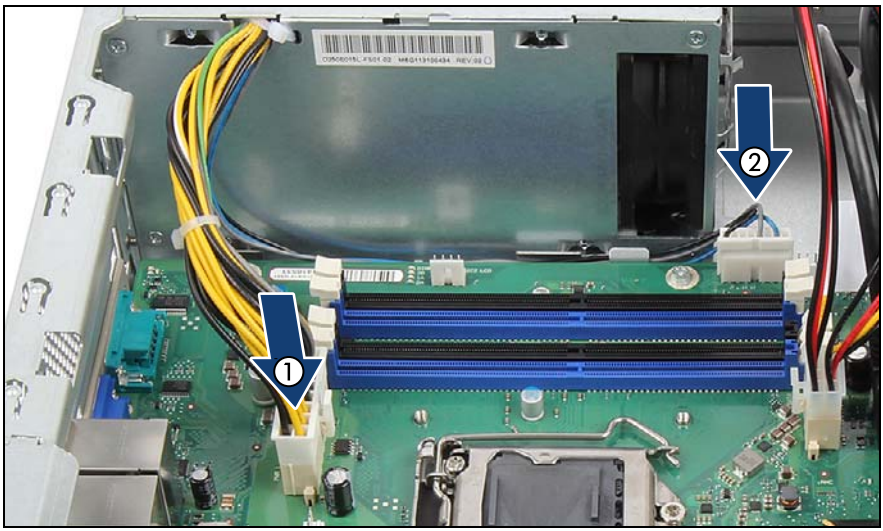

Figure 29: Connecting internal power cables

- ► Connect the power cable to the connector "PWR 1" on the system board (1).
- ► Connect the PSU power management cable to the connector "PC2009" on the system board (2).

6.2.1.5 Concluding steps

- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Performing a fan test" on page 108
- ► "Resuming BitLocker functionality" on page 102

6.3 Redundant power supply

Figure 30: PSU bays

6.3.1 Installing hot-plug PSUs

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools:	tool-less

6.3.1.1 Preliminary steps

No steps needed.

6.3.1.2 Removing the dummy cover

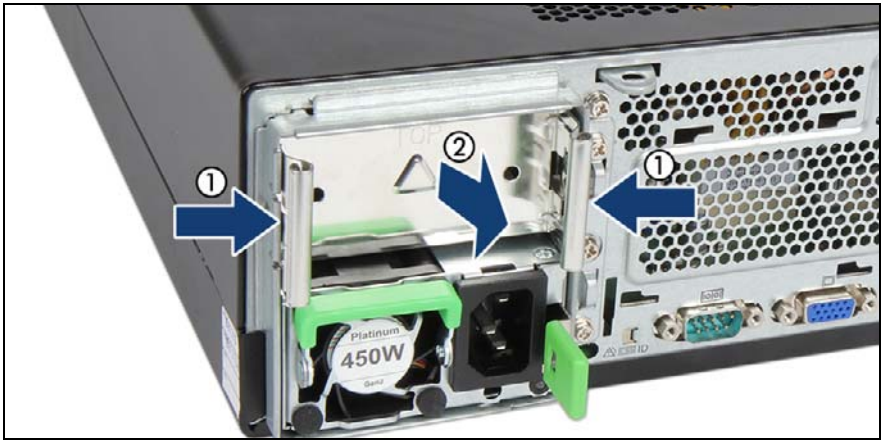

Figure 31: Removing the dummy cover

► Press in on both release latches (1) and remove the dummy cover (2).

CAUTION!

Keep the dummy cover for future use. If a PSU is removed and not immediately replaced by a new one, a dummy cover must be replaced in the bay to comply with applicable EMC regulations and satisfy cooling requirements.

6.3.1.3 Installing a hot-plug PSU

Figure 32: Installing a hot-plug PSU

- ► Push the hot-plug PSU into its bay (1) as far as it will go until the locking latch (2) snaps in place.
- ► If applicable, fold down the handle on the hot-plug PSU.

Make sure that the PSU engages correctly in the bay and is locked in position. This is the only way to prevent the PSU from sliding out of its bay and being damaged during transportation.

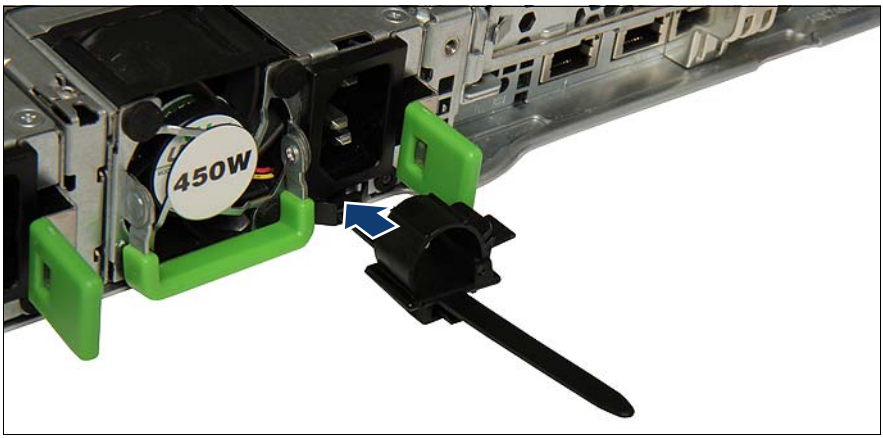

Figure 33: Installing the cable tie

- ► Push the cable tie into the corresponding hole until it clicks in.

6.3.1.4 Concluding steps

► "Connecting the power cord" on page 64

6.3.2 Removing hot-plug PSUs

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools:	tool-less

6.3.2.1 Preliminary steps

► Remove the AC power cord from the hot-plug PSU as described in section "Disconnecting the power cord" on page 53.

CAUTION!

In order to ensure uninterrupted operation, observe the following instructions:

► Before disconnecting a hot-plug PSU, ensure that sufficient power supply is available for your system configuration with the remaining hot-plug PSU(s).

6.3.2.2 Removing a hot-plug PSU

Figure 34: Removing a hot-plug PSU

- ► Fold up the handle on the hot-plug PSU (1).
- ► Press in on the green locking latch (2).
- ► While keeping the green locking latch pressed, pull the hot-plug PSU out of its bay (3).

CAUTION!

Never leave the bay for the hot-plug PSU empty for more than two minutes during operation. Otherwise, excessive temperatures could damage system components.

6.3.2.3 Installing a dummy cover

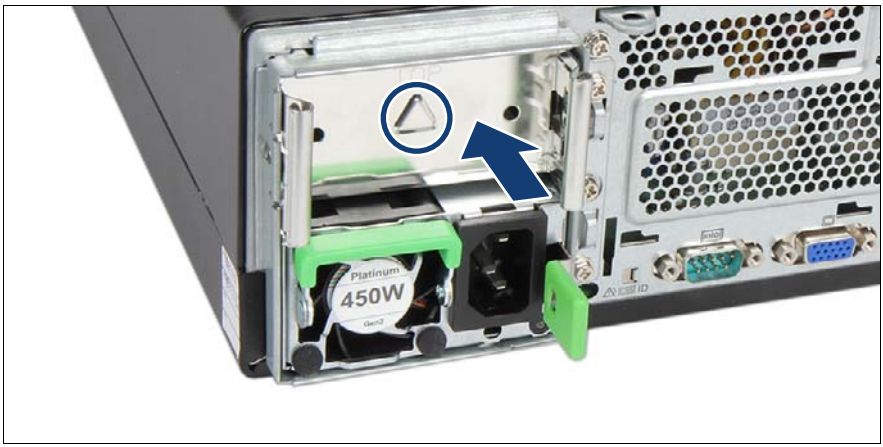

Figure 35: Installing a dummy cover

- ► Insert the dummy cover into the empty bay with the impressed arrow symbol facing to the left (see circle).
- ► Push the dummy cover into its bay until it locks in place.

CAUTION!

Always install dummy covers into unused PSU bays to comply with applicable EMC regulations and satisfy cooling requirements.

6.3.3 Replacing hot-plug PSUs

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

CAUTION!

- When replacing a hot-plug PSU in a non-redundant PSU configuration, the server must be switched off first.
- Ensure to replace a defective hot-plug PSU by a new module of the same type.

6.3.3.1 Preliminary steps

- ► "Locating the defective server" on page 49
- ► Only when replacing a PSU in a non-redundant configuration: "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53

6.3.3.2 Removing the defective hot-plug PSU

- ► Identify the defective PSU using the server management software.
- ► Remove the hot-plug PSU as described in "Removing a hot-plug PSU" on page 122.

6.3.3.3 Installing the new hot-plug PSU

- ► Install the hot-plug PSU as described in section "Installing a hot-plug PSU" on page 120.

6.3.3.4 Concluding steps

- ► Connect the power cord to the new hot-plug PSU and secure it with a cable tie as described in section "Connecting the power cord" on page 64.

- Only when replacing a hot-plug PSU in a non-redundant configuration: "Switching on the server" on page 69
- "Performing a fan test" on page 108

6.3.4 Replacing the power distribution board

Field Replaceable Unit (FRU)

Hardware: 25 minutes

Tools:	hexagon head, 5 mm / cross PZ2 Phillips PH2 (for Japan)

6.3.4.1 Preliminary steps

- "Locating the defective server" on page 49
- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- If applicable, remove the ODD as described in section "Removing the ODD" on page 250.
- If applicable, remove the RDX drive as described in section "Removing the RDX drive" on page 259.

6.3.4.2 Removing the hot-plug PSU

- Remove all hot-plug PSUs as described in "Removing a hot-plug PSU" on page 122.

6.3.4.3 Removing the power distribution board

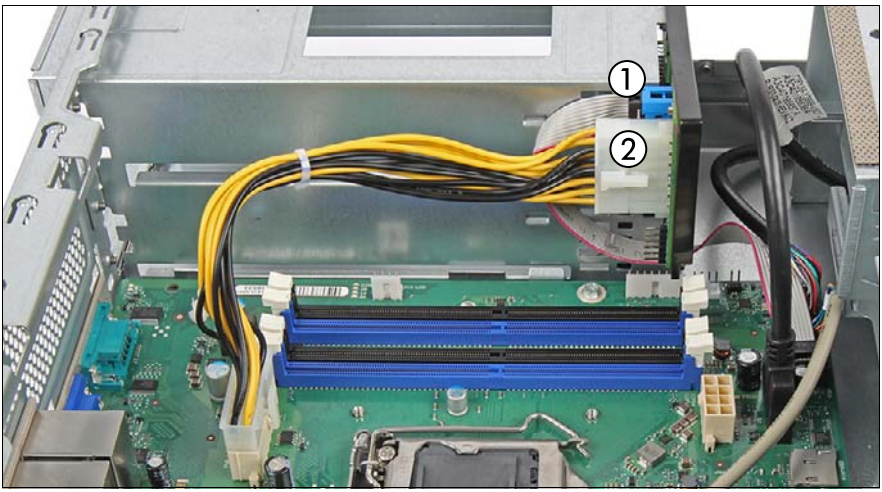

Figure 36: Disconnecting cables from the power distribution board

► Disconnect both cables from the power distribution board (1, 2)

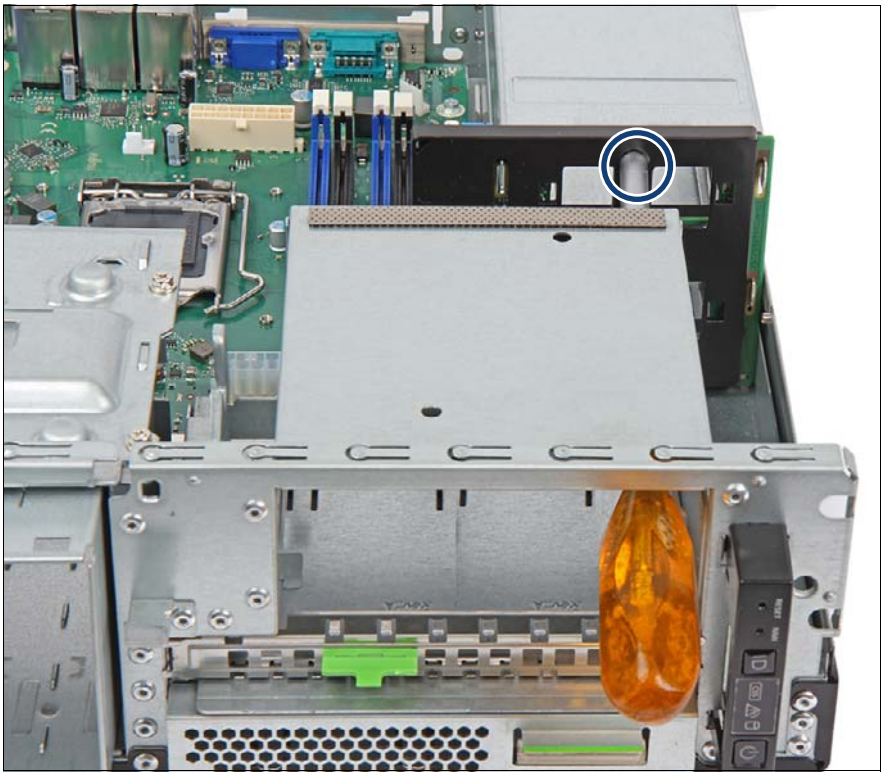

Figure 37: Removing power distribution board

- ► Remove one screw (see circle).
- ► Remove the power distribution board upwards.

6.3.4.4 Installing the power distribution board

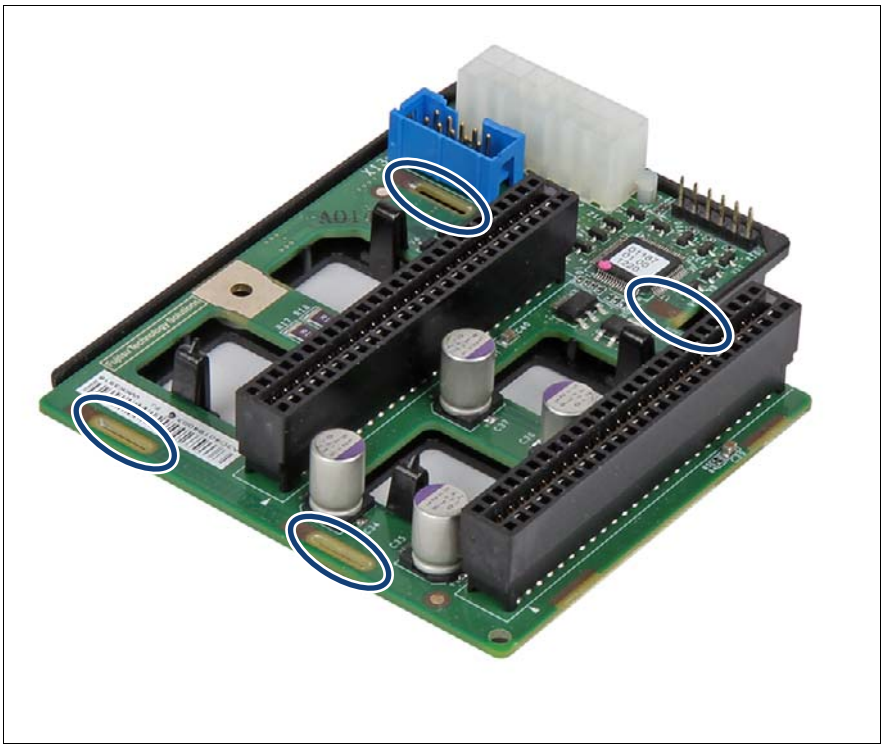

Figure 38: Recesses in the power distribution board

► Take note of the four recesses (see ovals).

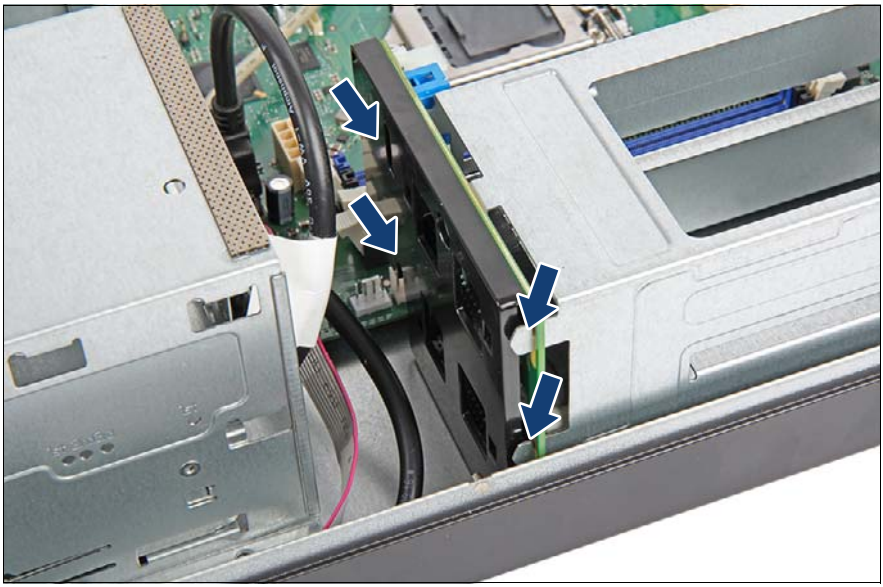

Figure 39: Replacing the power distribution board (A)

► Hook the power distribution board in the hooks at both sides of the PSU cage (see arrows).

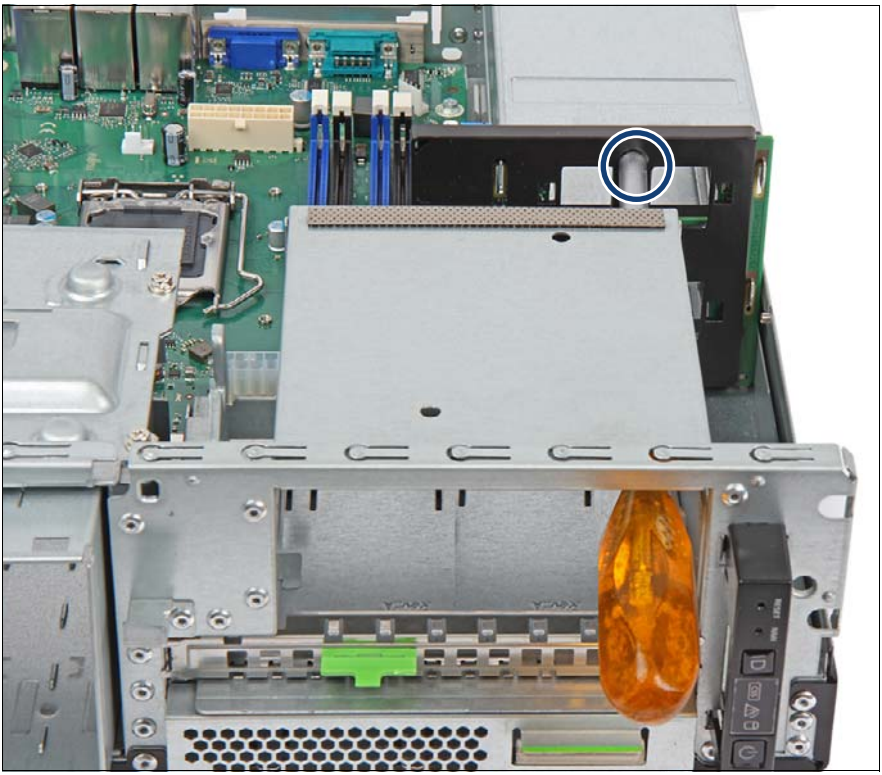

Figure 40: Replacing the power distribution board (B)

► Fasten the power distribution board through the empty drive bay with one screw (see circle).

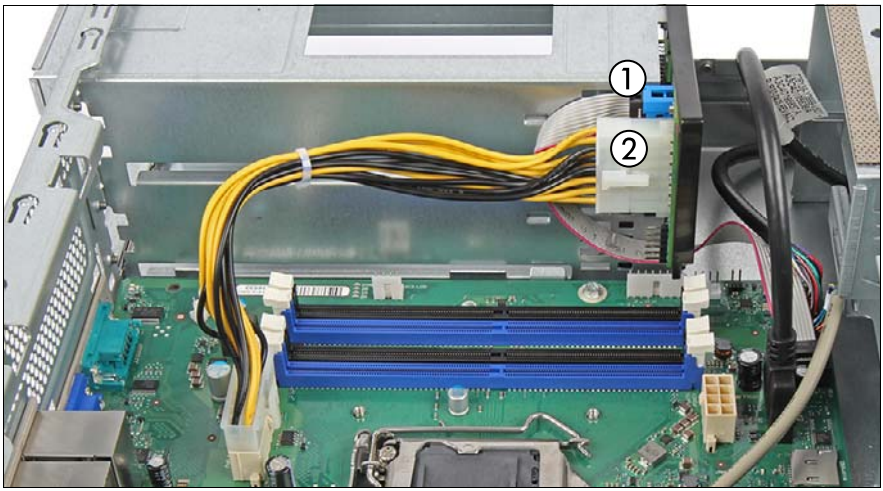

Figure 41: Connecting the power distribution board

- Connect the signal cable to the connector "X13" on the power distribution board (1).
- Connect the power cable to the connector "X10" on the power distribution board (2).

6.3.4.5 Installing the hot-plug PSUs

- Install the PSUs as described in section "Installing hot-plug PSUs" on page 118.

6.3.4.6 Concluding steps

- If applicable, install the RDX drive as described in section "Installing the RDX drive" on page 254.
- If applicable, install the ODD as described in section "Installing the ODD" on page 245.
- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Suspending BitLocker functionality" on page 75

6.4 Fujitsu battery unit (FJBU)

6.4.1 Installing the FJBU

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

6.4.1.1 Preliminary steps

No steps needed.

6.4.1.2 Removing the dummy cover

- Remove the dummy cover as described in section "Removing the dummy cover" on page 119.

6.4.1.3 Installing a FJBU

Figure 42: Installing a FJBU

► Push the FJBU into its bay (see arrow) as far as it will go until the locking latch snaps in place.

CAUTION!

Ensure that the FJBU properly engages in its bay and is locked in position in order to prevent it from sliding out of the chassis during transportation.

6.4.1.4 Concluding steps

► No steps needed.

To execute auto shutdown after power fail, you should install FJBU management software. How to install and configure the FJBU management software, please refer to “Fujitsu battery unit" User Guide.

6.4.2 Removing the FJBU

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

6.4.2.1 Preliminary steps

► No steps needed.

6.4.2.2 Removing a FJBU

Figure 43: Removing a FJBU

► Press in on the green locking latch (1).

► While keeping the green locking latch pressed, pull the FJBU out of its bay (2).

CAUTION!

Never leave the bay for the FJBU empty for more than two minutes during operation. Otherwise, excessive temperatures could damage system components.

6.4.2.3 Installing a dummy cover

► Install the dummy cover as described in section "Installing a dummy cover" on page 123.

CAUTION!

Always install dummy covers into unused PSU bays to comply with applicable EMC regulations and satisfy cooling requirements.

6.4.3 Replacing the FJBU

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools:	tool-less

6.4.3.1 Preliminary steps

► "Locating the defective server" on page 49

6.4.3.2 Removing the defective FJBU

► Remove the FJBU as described in "Removing a FJBU" on page 134.

6.4.3.3 Installing the new FJBU

► Install the FJBU as described in section "Installing a FJBU" on page 133.

6.4.3.4 Concluding steps

► No steps needed.

6.5 Converting a standard PSU to a redundant PSU

The standard PSU can be replaced by a redundant PSU. The redundant PSU consists of up to two PSUs (slide-in units). The upgrade kit contains only one PSU (for PSU redundancy the second PSU must be additionally ordered).

The upgrade kit for the redundant PSU consists of the following parts:
– PSU cage with power distribution board (incl.power cables)
– one hot-plug PSU
– dummy cover (if only one hot-plug PSU is installed, you have to install the dummy cover in the second bay)
– several screws

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

6.5.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

6.5.2 Removing the standard PSU

► Remove the standard PSU as described in section "Removing the standard PSU" on page 113.

Figure 44: Removing the standard PSU frame (A)

► Remove the five screws (see circles).

Figure 45: Removing the standard PSU frame (A)

► Remove the standard PSU frame in the direction of the arrow.

6.5.3 Installing PSU cage

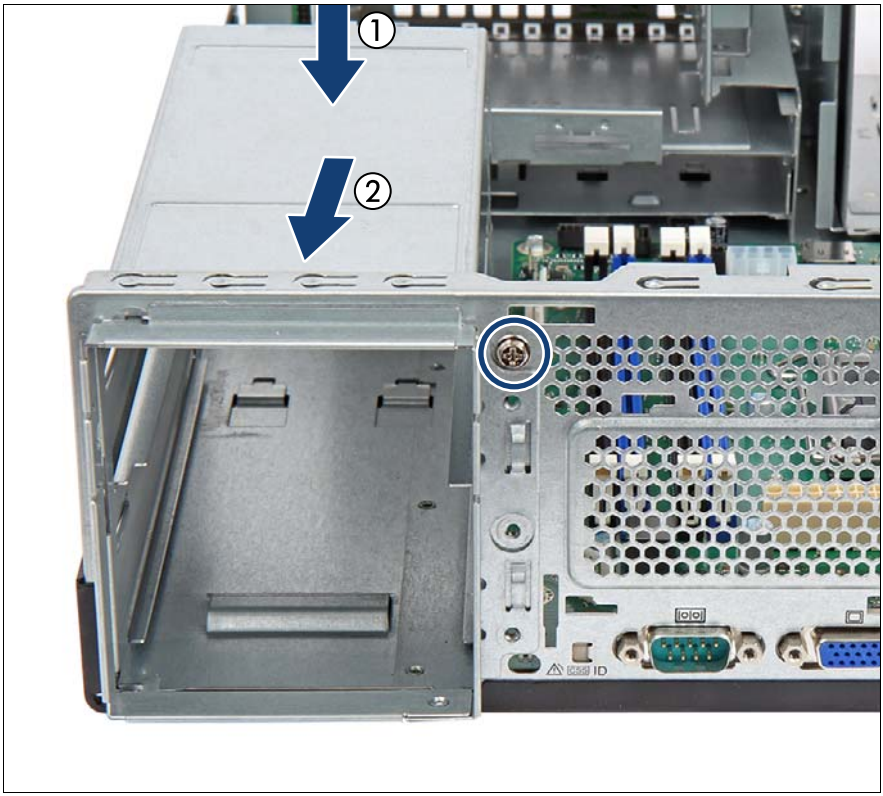

Figure 46: Installing the PSU cage (A)

- ► Take note of the two hooks (see figure 27).
- ► Insert the PSU cage into the chassis leaving a gap of about 3 cm to the rear chassis wall (1).
- ► Ensure that the hooks on the chassis (see circle in figure 27) engages with the notch on the lower surface of the PSU cage.
- ► Slide the new PSU cage towards the rear of the chassis (2).
- ► Fasten the PSU cage with one screws (see circle).

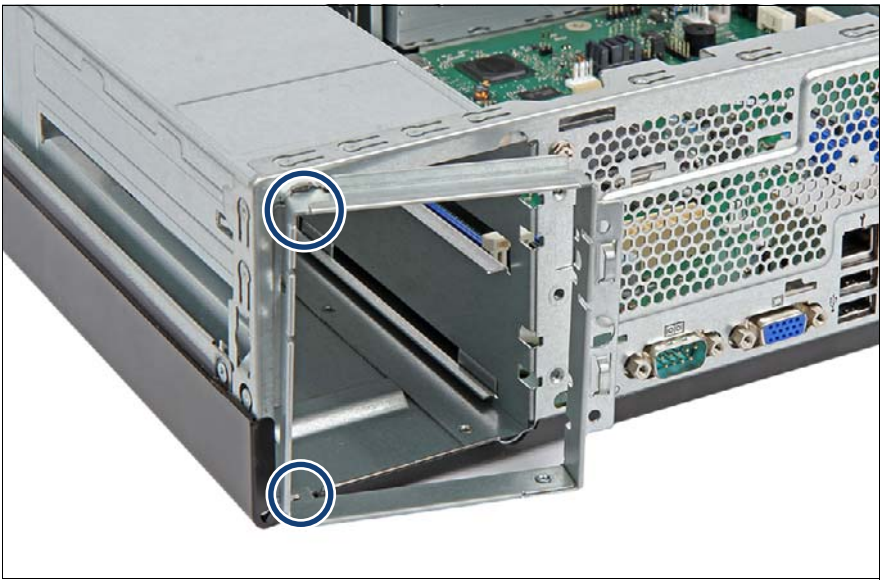

Figure 47: Installing the redundant PSU frame (A)

► Install the redundant PSU frame at a slight angle.

The hooks (see circles) must engage in the recesses.

Figure 48: Installing the redundant PSU frame (A)

► Fasten the PSU with three screws (see circles).

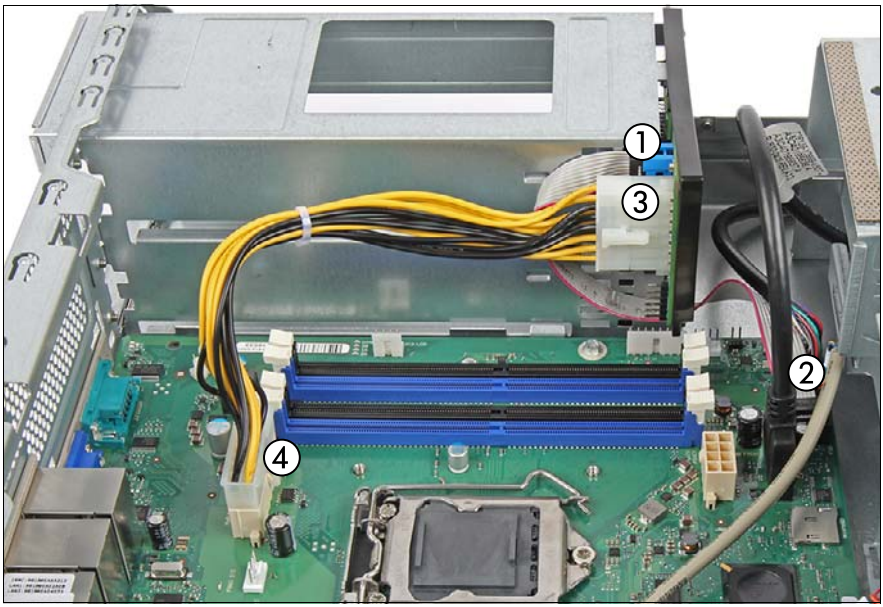

Figure 49: Connecting the redundant power distribution board

- Connect the signal cable:
  - To the "X13" on the power distribution board (1)
  - To the connector "P30" on the system board (2).
- Connect the power cable:
  - To the connector "X10" on the power distribution board (3)
  - To the connector "PWR 1" on the system board (4).
- Install the hot-plug PSU(s) as described in "Installing a hot-plug PSU" on page 120.
- If applicable, install a FJBU as described in "Installing a FJBU" on page 133.
- If one bay remains empty, install the dummy cover as described in "Installing a dummy cover" on page 123.

6.5.4 Concluding steps

- "Reassembling" on page 61

- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

7 Hard disk drive (HDD) / solid state drive (SSD)

CAUTION!

- The HDD or SSD must not be removed from the installation frame by anyone except a service technician.
- The HDD/SSD modules (drives) must all be marked clearly so that they can be reinstalled into their original mounting locations after replacement. Otherwise, data may be lost.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Before removing an HDD, wait for about 30 seconds until the disk has stopped spinning completely.
- When an HDD is starting up, a resonant noise may be audible for a short while. This does not indicate a failure.
- Depending on the OS, you can configure the write cache settings for the HDDs. If a power failure should occur while the write cache is enabled, cached data may be lost.
- When disposing of, transferring, or returning an HDD or SSD, wipe out the data on the drive for your own security.
- Rough handling of HDDs may damage the stored data. To cope with any unexpected problems, always back up important data. When backing up data to another HDD, you should make backups on a file or partition basis.
- Be careful not to hit the HDD or bring it into contact with metallic objects.
- Handle the HDD and SSD on a shock and vibration free surface.
- Do not use the HDD and SSD in extremely hot or cold locations, or locations with extreme temperature changes.
- Never attempt to disassemble the HDD or SSD.
- For further safety information, please refer to chapter "Important information" on page 35.

7.1 Basic information

The HDDs or SSDs which can be ordered for your server are supplied already mounted in an installation frame so that defective drives can be replaced and new drives can be added during operation. The HDD or SSD and the installation frame together make up the HDD module or SSD module.

The server is shipped with one of the following HDD or SSD subsystems:

– 3.5-inch HDD subsystem:

  Up to two 3.5-inch SAS/SATA HDD modules can be installed. Each HDD module can accommodate an SAS/SATA HDD with a maximum height of 1 inch. The HDD module is connected to the HDD backplane wirelessly. This allows HDD modules to be plugged in or pulled out easily.

  Hybrid configurations of SAS and SATA HDD modules are not supported.

– 2.5-inch HDD/SSD subsystem:

  Up to four (one HDD backplane), eight (two HDD backplanes) 2.5-inch SAS/SATA HDD/SSD modules can be installed. Each HDD/SSD module can accommodate a SAS/SATA HDD or SATA SSD with a 2.5-inch format. The HDD/SSD modules are connected to the HDD backplane wirelessly. This allows HDD/SSD modules to be plugged in or pulled out easily. If the server has a corresponding RAID configuration, defective HDD/SSD modules can also be replaced during operation.

  Hybrid configurations of SAS and SATA HDD/SSD modules are not supported.

For information on RAID controllers controlling the HDD/SSD modules see chapter "Expansion cards and backup units" on page 187.

7.2 2.5-inch HDD/SSD configurations

7.2.1 Equipping the 2.5-inch HDDs/SSDs

– SSDs are always equipped before installing HDDs.

– If only one HDD/SSD module is installed, the HDD/SSD module will be installed in position 0. Free bays must be equipped with a dummy module.

7.2.2 Configuration with up to four HDD/SSD modules

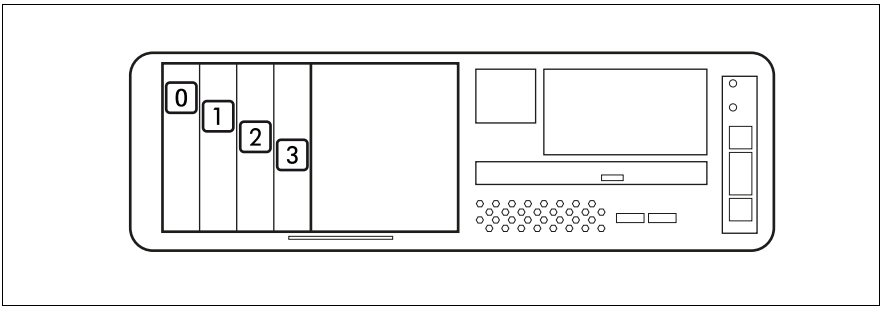

Figure 50: Configuration with up to four 2.5-inch HDDs/SSDs

The HDD/SSD numbering as listed in the ServerView RAID Manager:

Position	Logical drive number	ServerView RAID Manager display name
0	0	Vendor Product (0)
1	1	Vendor Product (1)
2	2	Vendor Product (2)
3	3	Vendor Product (3)

7.2.3 Configuration with up to eight HDDs/SSDs

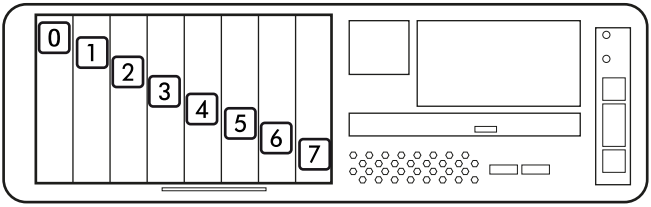

Figure 51: Configuration with up to eight 2.5-inch HDDs/SSDs

The HDD/SSD numbering as listed in the ServerView RAID Manager:

Position	Logical drive number	ServerView RAID Manager display name
0	0	Vendor Product (0)
1	1	Vendor Product (1)
2	2	Vendor Product (2)
3	3	Vendor Product (3)
4	4	Vendor Product (4)
5	5	Vendor Product (5)
6	6	Vendor Product (6)
7	7	Vendor Product (7)

f a server system has been configured without any HDDs, keep the HDD bay marked with “Test” free for test purposes. During hardware checks, a HDD will be installed into this bay. Afterwards this HDD is replaced by a HDD dummy module.

7.2.4 Installing 2.5-inch HDD/SSD modules

Customer Replaceable Unit (CRU) **Hardware: 5 minutes**

Tools: tool-less

7.2.4.1 Preliminary steps

- "Removing the drive cover" on page 58
- "Removing the HDD cover" on page 60

7.2.4.2 Removing a 2.5-inch HDD/SSD dummy module

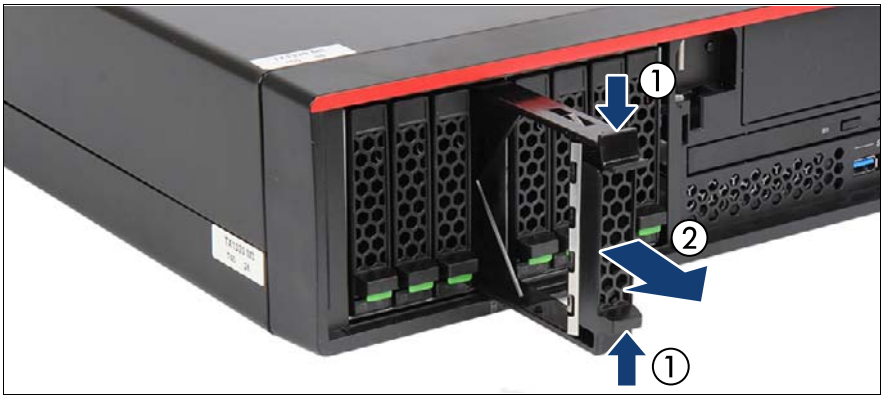

Figure 52: Removing a 2.5-inch HDD/SSD dummy module

- Press both tabs together (1) and pull the dummy module out of its bay (2).

CAUTION!

Save the dummy module for future use.
Always replace dummy modules into unused HDD/SSD bays to comply with applicable EMC regulations and satisfy cooling requirements.

7.2.4.3 Installing a 2.5-inch HDD/SSD module

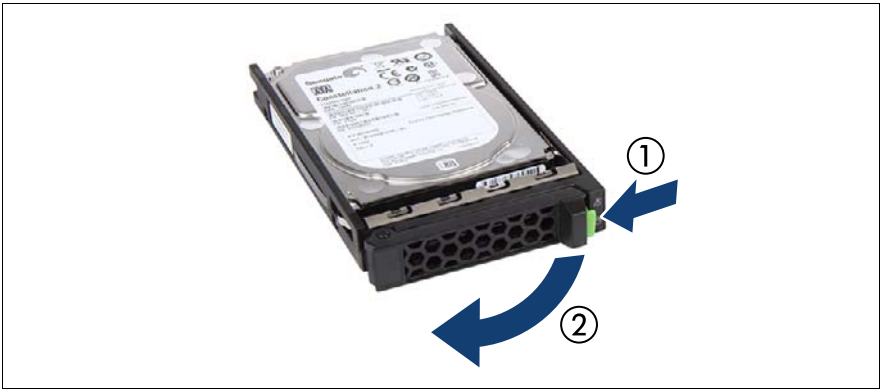

Figure 53: Opening the 2.5-inch HDD/SSD module locking lever

► Pinch the green locking clips (1) and open the locking lever (2).

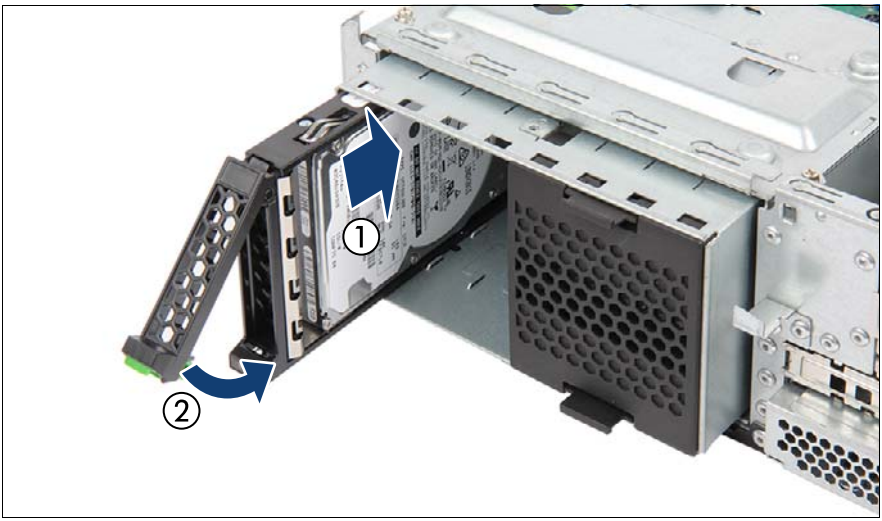

Figure 54: Inserting the 2.5-inch HDD/SSD module

► Insert the HDD/SSD module into a drive bay and carefully push back as far as it will go (1).

► Close the locking lever to lock the HDD/SSD module in place (2).

7.2.4.4 Concluding steps

- "Installing the HDD cover" on page 62
- "Installing the drive cover" on page 63

Please refer to your controller manual to configure the installed HDD.

7.2.5 Removing 2.5-inch HDD/SSD modules

Customer Replaceable Unit (CRU) **Hardware: 5 minutes**

Tools: tool-less

7.2.5.1 Preliminary steps

- If the HDD/SSD module to be removed is combined into a RAID array, please proceed as follows:

RAID level	Procedure
RAID 0	Only remove an HDD module combined in a RAID 0 array if defective. **CAUTION!** Removing an operational HDD module will result in data loss!
RAID 1 RAID 5	Removing an HDD module from a RAID 1 or RAID 5 array will not result in data loss. However, the removed drive needs to be replaced immediately by an HDD module of the same or larger capacity. After replacing the HDD module, RAID rebuild will be performed as a background process as described in section "Performing a RAID array rebuild" on page 103.

In order to permanently remove an operational HDD module that is part of a RAID array from the server, you first need to delete the array using ServerView RAID Manager.

CAUTION!

All data on all HDDs/SSDs in the array will be lost when deleting the RAID array! Be sure to back up your data before deleting a RAID array.

For further information, please refer to the "ServerView Suite RAID Management" user guide.

- ► "Removing the drive cover" on page 58
- ► "Removing the HDD cover" on page 60

7.2.5.2 Removing a 2.5-inch HDD/SSD module

- ► Pull the HDD/SSD module out a few centimeters.
- ► Wait about 30 seconds to allow the HDD to spin down.

This is not necessary when removing an SSD.

This period is necessary for the RAID controller to recognize that an HDD module has been removed and for the HDD to come to a stop.

- ► Pull the HDD/SSD module completely out of its bay.

7.2.5.3 Installing a 2.5-inch HDD/SSD dummy module

CAUTION!

If the removed HDD/SSD module is not replaced immediately, always replace a dummy module into the unused HDD/SSD bay to comply with applicable EMC regulations and satisfy cooling requirements.

Figure 55: Installing a 2.5-inch HDD/SSD dummy module

► Push the dummy module into the empty bay until it engages.

7.2.5.4 Concluding steps

► "Removing the HDD cover" on page 60

► "Installing the drive cover" on page 63

7.2.6 Replacing a 2.5-inch HDD/SSD module

Customer Replaceable Unit (CRU) **Hardware: 5 minutes**

Tools: tool-less

CAUTION!

- Only remove an HDD/SSD module during operation if the drive is not currently being accessed. Observe the indicators for the corresponding HDD/SSD modules, see "FUJITSU Server PRIMERGY TX1320 M3 Operating Manual".
- An HDD/SSD module can be replaced while the system is in operation.

  RAID configuration with a RAID controller:

Only RAID level 1, 10, 5, 50, 6 or 60 is allowed.

RAID configuration without a RAID controller:
Please follow the instruction of each software e.g. VSAN, Storage Spaces, and Storage Spaces Direct, provided separately to use the software RAID function of OS or Hypervisor.

- All HDD/SSD modules (drives) must be uniquely identified so that they can be reinstalled in their original bays later. If this is not done, existing data can be lost.

7.2.6.1 Preliminary steps

- ► "Removing the drive cover" on page 58
- ► "Removing the HDD cover" on page 60
- ► "Locating the defective server" on page 49
- ► "Local diagnostic indicators on the front" on page 51

7.2.6.2 Removing a 2.5-inch HDD/SSD module

- ► "Removing a 2.5-inch HDD/SSD module" on page 152

7.2.6.3 Installing a 2.5-inch HDD/SSD module

- ► "Installing a 2.5-inch HDD/SSD module" on page 150

7.2.6.4 Concluding steps

- ► "Performing a RAID array rebuild" on page 103
- ► "Installing the HDD cover" on page 62
- ► "Installing the drive cover" on page 63

7.2.7 Replacing the 4 x 2.5-inch HDD backplane 1

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Replacing the SAS backplane: Phillips PH2 / (+) No. 2 screw driver

7.2.7.1 Preliminary steps

The 2.5-inch HDD SAS/SATA backplane is mounted on the drive cage. It is not necessary to remove the drive cage before replacing the SAS/SATA backplane

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Removing 2.5-inch HDD/SSD modules" on page 151

  The HDD/SSD modules need not to be removed completely. But if you want to remove them nevertheless, check if all HDD/SSD modules are uniquely identified so that you can reinsert them into their original bays.

- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175

7.2.7.2 Removing the HDD backplane

- Disconnect all cables from the HDD backplane.

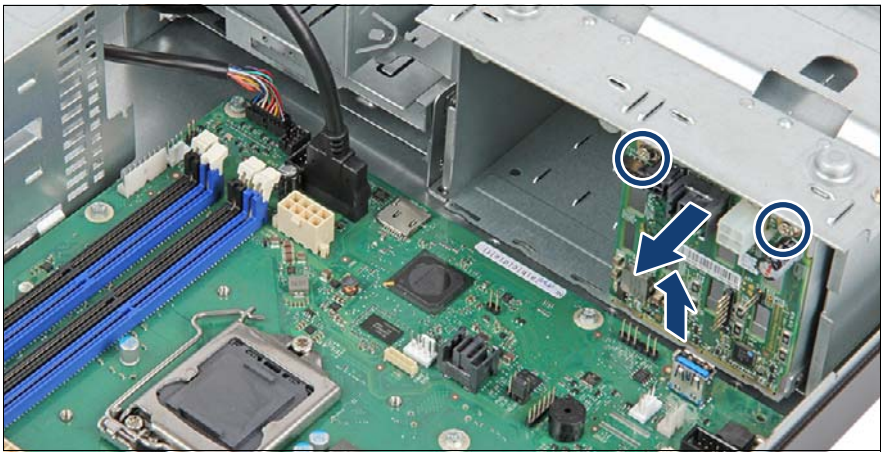

Figure 56: Removing the HDD backplane

- ► Remove the two screws (see circles).
- ► Lift the HDD backplane up and remove it from the HDD cage (see arrows).

7.2.7.3 Installing the HDD backplane

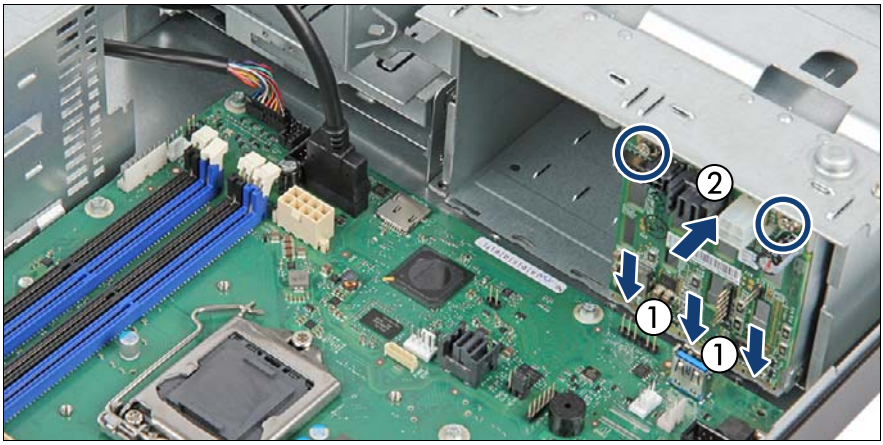

Figure 57: Installing the HDD backplane

- ► Insert the HDD backplane in the three hooks on the bottom of the HDD cage (1).
- ► Fasten the HDD backplane with two screws (2).

7.2.7.4 Connecting HDD backplane 1

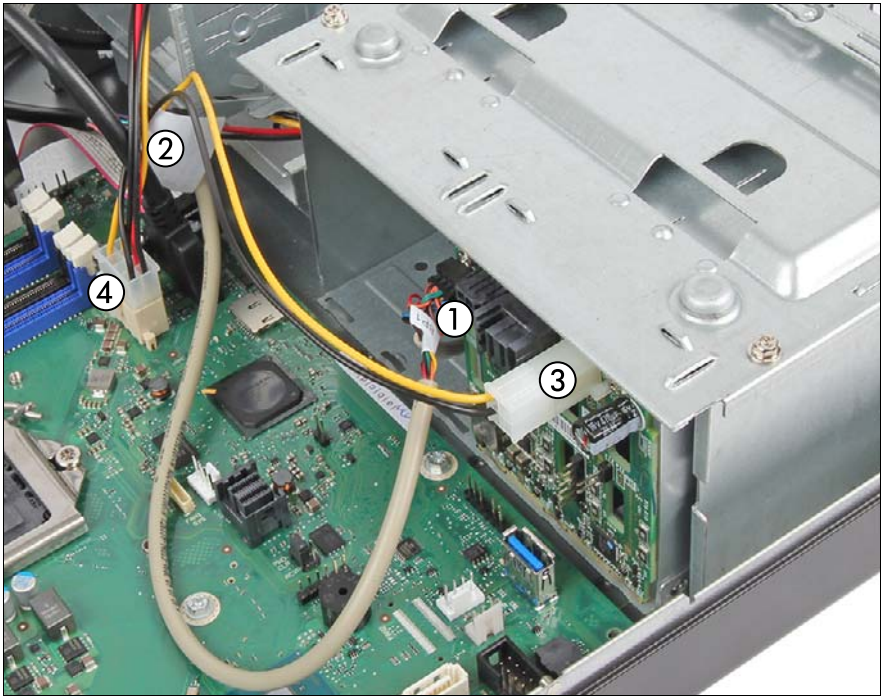

Figure 58: Connecting HDD backplane 1 (A)

- ► Connect the OOB cable:
  - – Connector "BP1" to connector "X11" on the HDD backplane 1 (1)
  - – Connector "SB" to the connector "I2C5" on the system board (2)
- ► Connect the power cable:
  - – Connector "P2" to connector "PWR" on the HDD backplane 1 (3)
  - – Connector "P1" to the connector "SATA POWER" on the system board (4)

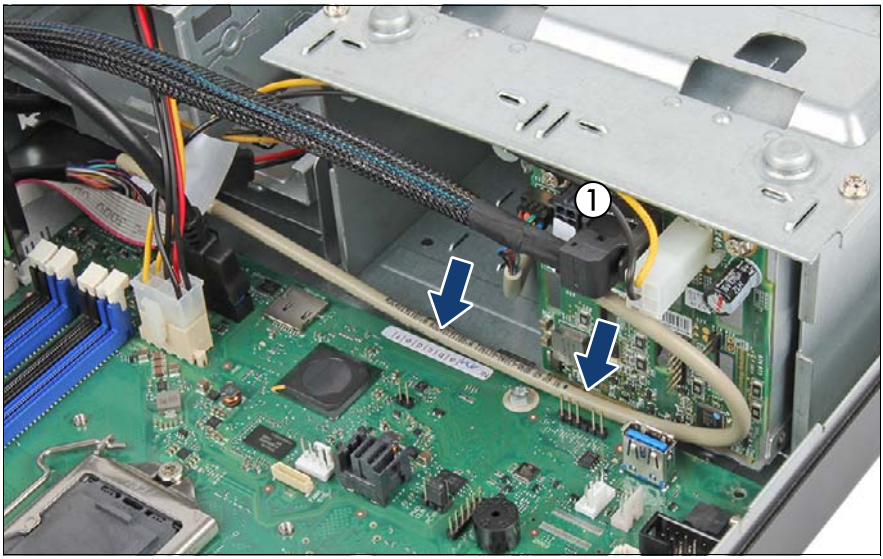

Figure 59: Connecting HDD backplane 1 (B)

- ► Connect the short connector of the SATA cable to the connector "X9" on the HDD backplane 1 (1).
- ► Route the OOB cable as shown (see arrows).

For the cable plan see section "Cabling" on page 319.

7.2.7.5 Concluding steps

- "Installing the HDD fan module" on page 179
- "Reassembling" on page 61
- "Installing 2.5-inch HDD/SSD modules" on page 148
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

7.2.8 Upgrading from 4x to 8x 2.5-inch HDD/SSD configuration

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Replacing the SAS backplane: Phillips PH2 / (+) No. 2 screw driver

7.2.8.1 Preliminary steps

The 2.5-inch HDD SAS/SATA backplane is mounted on the drive cage. It is not necessary to remove the drive cage before replacing the SAS/SATA backplane

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Removing 2.5-inch HDD/SSD modules" on page 151

The HDD/SSD modules need not to be removed completely. But if you want to remove them nevertheless, check if all HDD/SSD modules are uniquely identified so that you can reinsert them into their original bays.

- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175
- "Removing the HDD cage" on page 70

7.2.8.2 Installing the HDD backplane 2

► Install the HDD backplane 2 as described in section "Installing the HDD backplane" on page 156.

7.2.8.3 Connecting HDD backplane 1 and 2

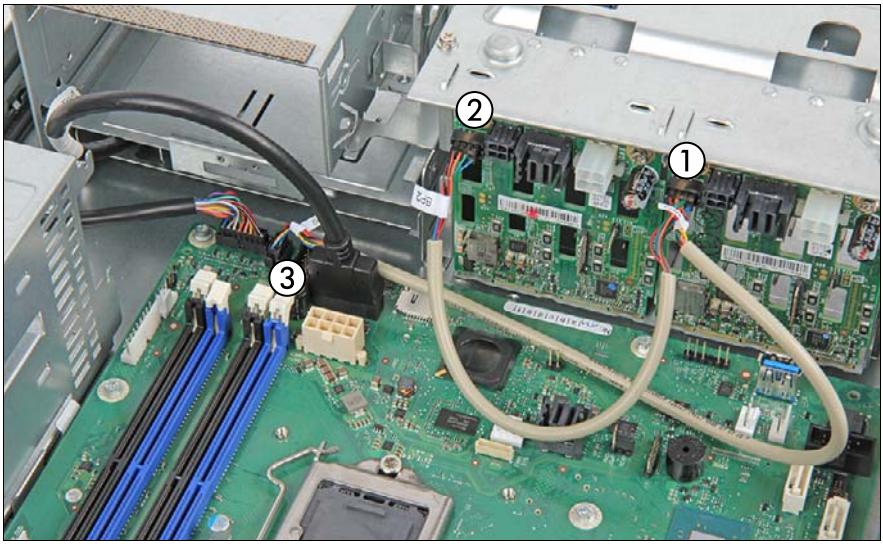

Figure 60: Connecting HDD backplanes (A)

► Connect the OOB cable:

- Connector "BP1" to connector "X11" on the HDD backplane 1 (1)
- Connector "BP2" to connector "X11" on the HDD backplane 2 (2)
- Connector "SB" to the connector "I2C5" on the system board (3)

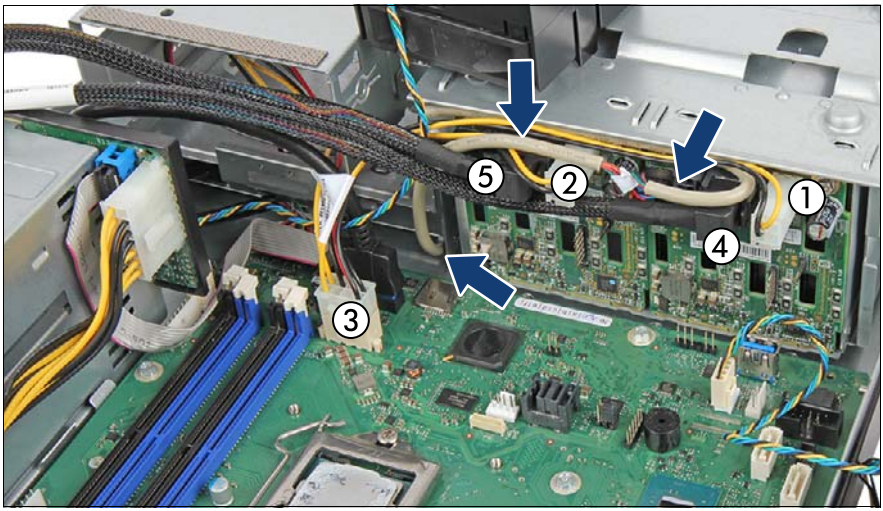

Figure 61: Connecting HDD backplanes (B)

- Connect the power cable:
  - Connector "P2" to connector "X40" on the HDD backplane 1 (1)
  - Connector "P3" to connector "X40" on the HDD backplane 2 (2)
  - Connector "P1" to the connector "SATA POWER" on the system board (3)
- Connect both SAS cables:
  - Short connector to the connector "X9" on the HDD backplane 1 (4)
  - Short connector to the connector "X9" on the HDD backplane 2 (5)
- Route the OOB cable as shown (see arrows).

For the cable plan see section "Cabling" on page 319.

7.2.8.4 Concluding steps

- "Installing the HDD cage" on page 72
- "Installing the HDD fan module" on page 179
- "Reassembling" on page 61
- "Installing 2.5-inch HDD/SSD modules" on page 148

- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

7.3 3.5-inch HDD configurations

7.3.1 Equipping the 3.5-inch HDDs/SSDs

– The PRIMERGY TX1320 M3 server can be equipped with up to two 3.5-inch non hot-plug SAS/SATA HDDs.

– 3.5-inch HDD configurations support enhanced integrated mirroring functionality and RAID level 0/1 with 2 HDDs.

7.3.2 Configuration with up to two HDDs

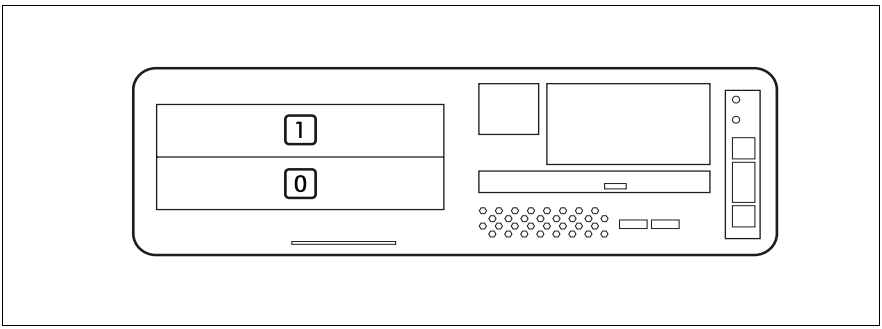

Figure 62: Configuration with up to two 3.5-inch HDDs

The HDD/SSD numbering as listed in the ServerView RAID Manager:

Position	Logical drive number	ServerView RAID Manager display name
0	0	Vendor Product (0)
1	1	Vendor Product (1)

SAS connectivity

Controller	Channel	Connection
Onboard SATA	1	Connect the mSAS connector on the SATA Y-cable C11 to system board connector "SATA1-4.
Onboard SATA		Connect the mSAS connector on the SATA Y-cable C11 to SAS controller connector "MLC1".

7.3.3 Installing 3.5-inch HDD modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

7.3.3.1 Preliminary steps

- ► "Shutting down the server" on page 52
- ► "Getting access to the component" on page 55
- ► "Configuration with up to two HDDs" on page 162

7.3.3.2 Installing a 3.5-inch HDD module

Figure 63: Inserting the 3.5-inch HDD module (A)

- ► Loosen the two knurled screws (see circles).
- ► Insert the HDD module into a drive bay and carefully push back as far as it will go (1).

Figure 64: Inserting the 3.5-inch HDD module (B)

- ► Tighten the two knurled screws (see circles).
- ► If applicable, install the second 3.5-inch HDD module.

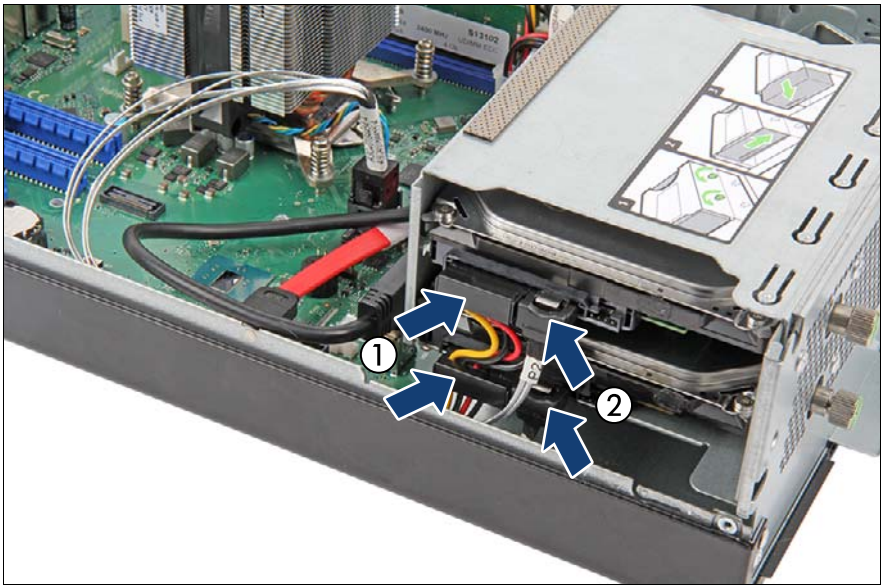

Figure 65: Connecting the 3.5-inch HDD module(s)

- Connect the power cable(s) to the HDD(s) (1):
  - P2 to the lower HDD
  - P3 to the upper HDD
- Connect the SATA connector(s) on the SATA Y-cable to the HDD(s) (2):
  - P1 to the lower HDD
  - P2 to the upper HDD
- If applicable, remove the protective cap from the mSAS connector on SATA Y-cable C11.

7.3.3.3 Concluding steps

- "Installing the server cover" on page 61

Please refer to your controller manual to configure the installed HDD.

7.3.4 Removing 3.5-inch HDD modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

7.3.4.1 Preliminary steps

► If the HDD/SSD module to be removed is combined into a RAID array, please proceed as follows:

RAID level	Procedure
RAID 0	Only remove an HDD module combined in a RAID 0 array if defective. **CAUTION!** Removing an operational HDD module will result in data loss!
RAID 1	Removing an HDD module from a RAID 1 array will not result in data loss. However, the removed drive needs to be replaced immediately by an HDD module of the same or larger capacity. After replacing the HDD module, RAID rebuild will be performed as a background process as described in section "Performing a RAID array rebuild" on page 103.

In order to permanently remove an operational HDD module that is part of a RAID array from the server, you first need to delete the array using ServerView RAID Manager.

CAUTION!

All data on all HDDs/SSDs in the array will be lost when deleting the RAID array! Be sure to back up your data before deleting a RAID array.

For further information, please refer to the "ServerView Suite RAID Management" user guide.

- "Shutting down the server" on page 52
- "Getting access to the component" on page 55

7.3.4.2 Removing a 3.5-inch HDD module

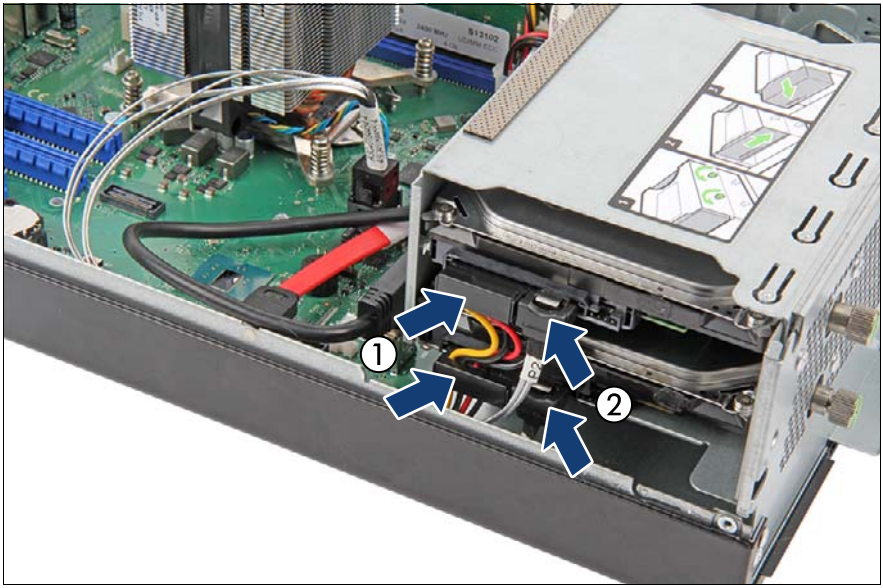

Figure 66: Disconnecting the 3.5-inch HDD module(s)

- Disconnect the SATA power cable from the HDDs to be removed (1):
- Disconnect the two SATA connectors on the SATA Y-cable from the HDD to be removed (2):

Figure 67: Removing the 3.5-inch HDD module

- ► Loosen the two knurled screws (see circles).
- ► Pull the HDD module out of the bay.

7.3.4.3 Concluding steps

- ► "Installing the server cover" on page 61

7.3.5 Replacing a 3.5-inch HDD module

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

CAUTION!

- Only remove an HDD module during operation if the drive is not currently being accessed. Observe the indicators on the HDD module, see section "Indicators on the hot-plug HDD/SSD module" on page 345.
- An HDD module can be replaced while the system is in operation.

  RAID configuration with a RAID controller:
  Only RAID level 1, 10, 5, 50, 6 or 60 is allowed.

  RAID configuration without a RAID controller:
  Please follow the instruction of each software e.g. VSAN, Storage Spaces, and Storage Spaces Direct, provided separately to use the software RAID function of OS or Hypervisor.
- All HDD modules (drives) must be uniquely identified so that they can be reinstalled in their original bays later. If this is not done, existing data can be lost.

7.3.5.1 Preliminary steps

- ► "Locating the defective server" on page 49
- ► "Locating the defective component" on page 51

7.3.5.2 Removing a 3.5-inch HDD module

- ► Remove the HDD module as described in section "Removing a 3.5-inch HDD module" on page 168

7.3.5.3 Installing a 3.5-inch HDD module

► Install the HDD module as described in section "Installing a 3.5-inch HDD module" on page 164

7.3.5.4 Concluding steps

► "Performing a RAID array rebuild" on page 103

8 Fans

Safety notes

CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- For further information, please refer to chapter "Important information" on page 35.

8.1 Basic information

The PRIMERGY TX1320 M3 server features two different HDD fan modules.

Since the system fan is not redundant, it has to be replaced immediately in case of defects or pre-failure events.

8.2 HDD fan module 2.5-inch variant

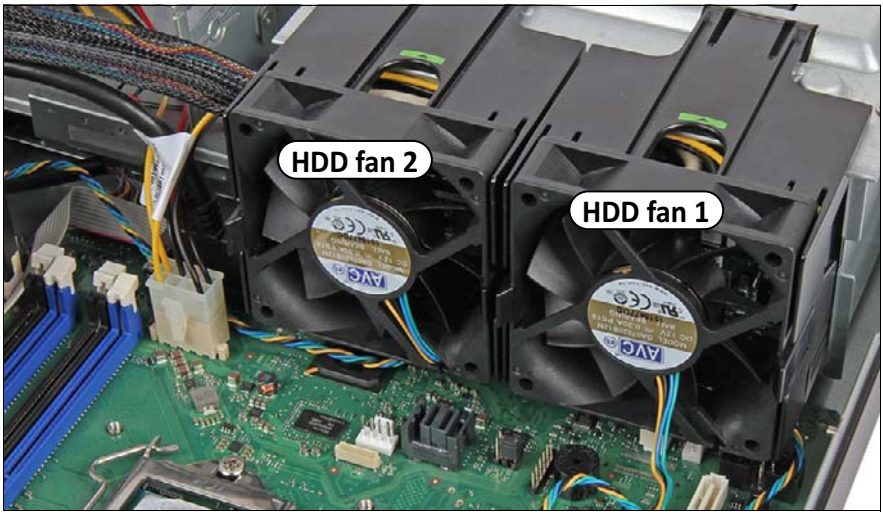

Figure 68: HDD fan position

8.2.1 Replacing the HDD fan module

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

8.2.1.1 Preliminary steps

- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

8.2.1.2 Removing the HDD fan module

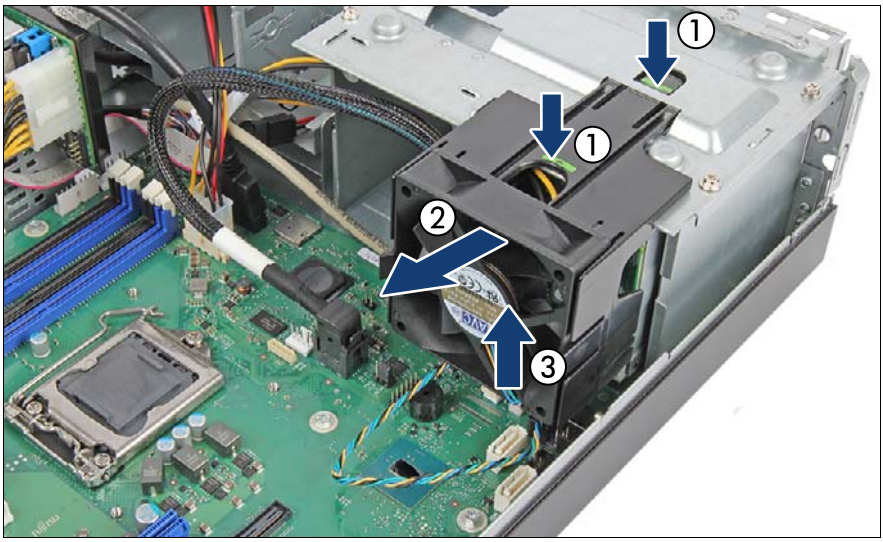

Figure 69: Removing the HDD fan module fan module

- ► Press on the two green tabs (1) and remove the HDD fan module from the HDD cage (2).
- ► Disconnect the fan cable from system board (3).

8.2.1.3 Removing the fan from the holder

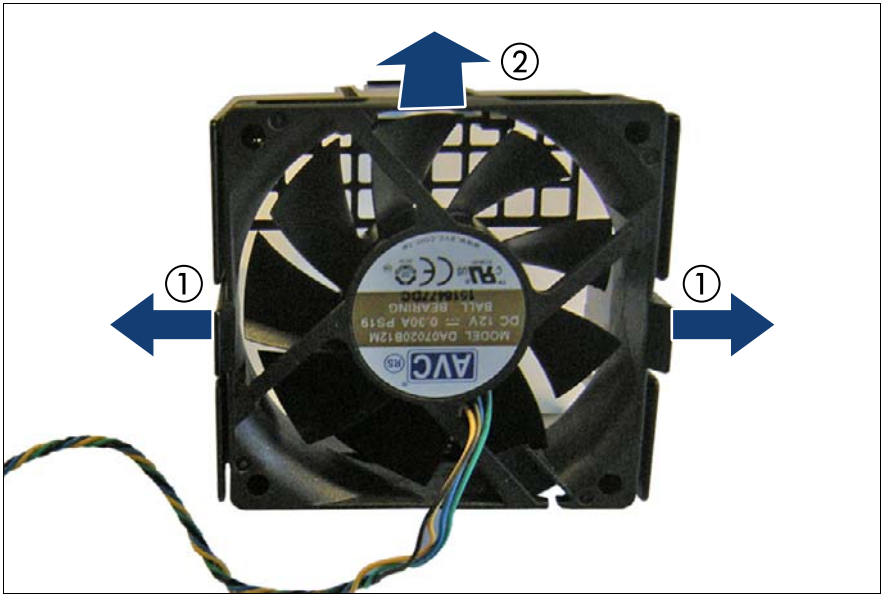

Figure 70: Example: Removing the fan from the holder (2.5-inch)

- ► Pull the two notches outwards (1) and remove the fan holder in the direction of the arrow (2).

8.2.1.4 Preparing the HDD fan module

Only necessary if 8 HDD modules are installed.

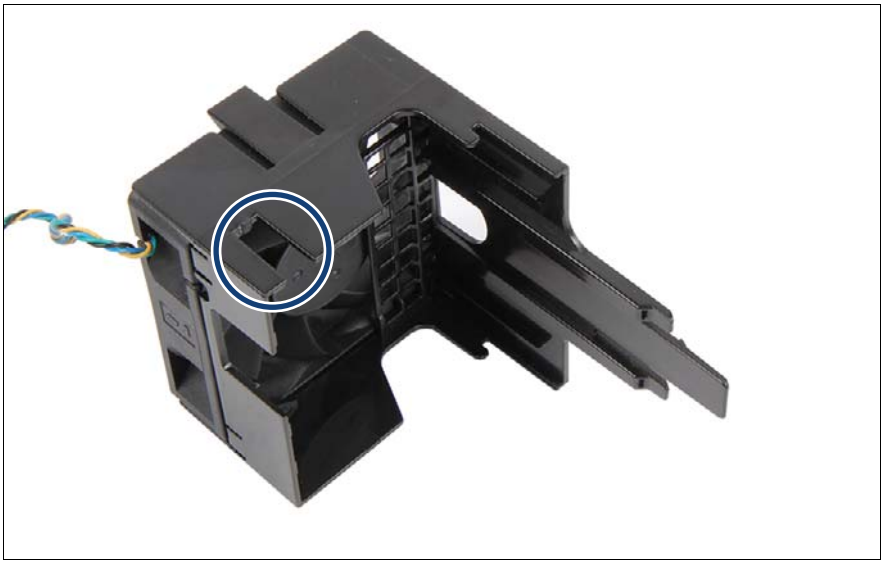

Figure 71: HDD fan module - breakout

► Break the small plastic tooth out of the second HDD fan module (see circle) so that the USB cable to the RDX backup drive can be run through the outbreak.

8.2.1.5 Installing the fan into the holder

Figure 72: Example: Installing the fan into the holder (2.5-inch)

► Insert the fan into the holder (see arrow).

8.2.1.6 Installing the HDD fan module

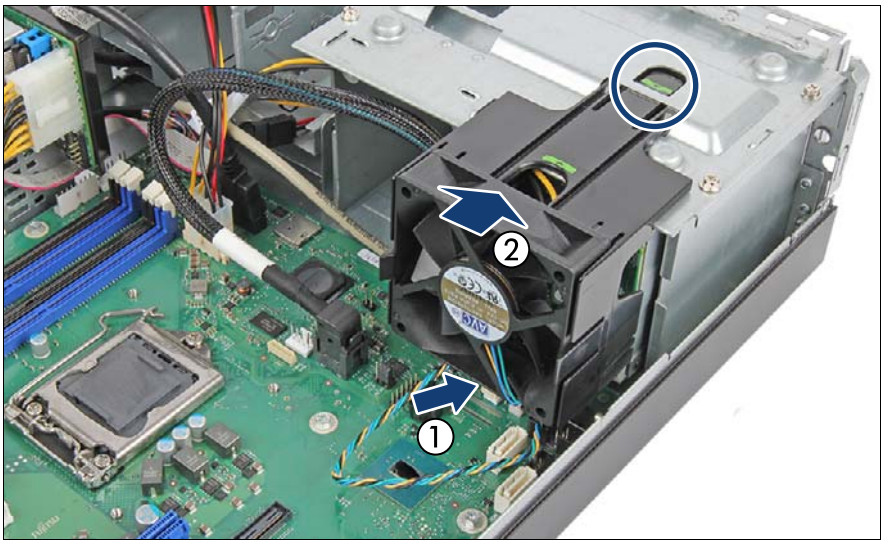

Figure 73: Installing the HDD fan module

► Connect the fan cable to system board connector "FAN2 SYS" (1).

For the second HDD fan module use the system board connector "FAN4 SYS".

► Attach the fan module on the top of the HDD cage (2) and slide it until it locks in place (see circle).

8.2.1.7 Cable routing

Figure 74: Cable routing for the first HDD fan module

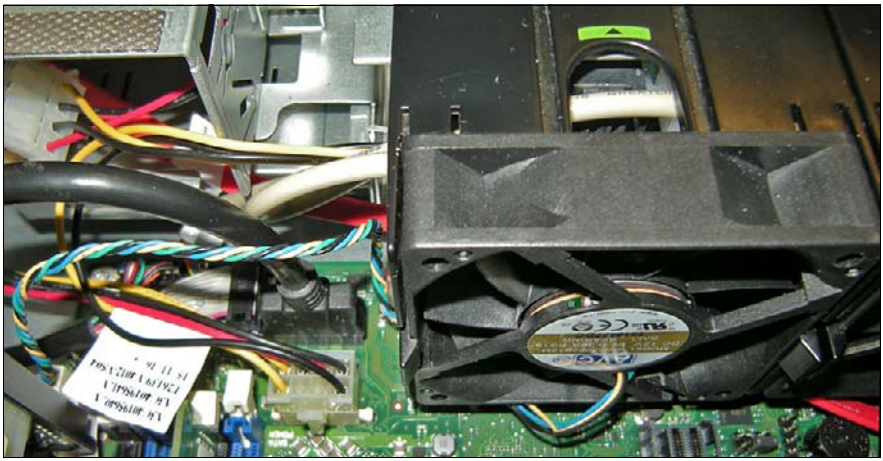

Figure 75: Cable routing for the second HDD fan module

► Route the cable as shown in the figure 74 or figure 75.

8.2.1.8 Concluding steps

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

► "Performing a fan test" on page 108

8.3 Replacing the HDD fan module (3.5-inch variant)

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

8.3.1 Preliminary steps

- "Locating the defective server" on page 49
- "Local diagnostic indicators on the system board" on page 52
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

8.3.2 Removing the HDD fan module

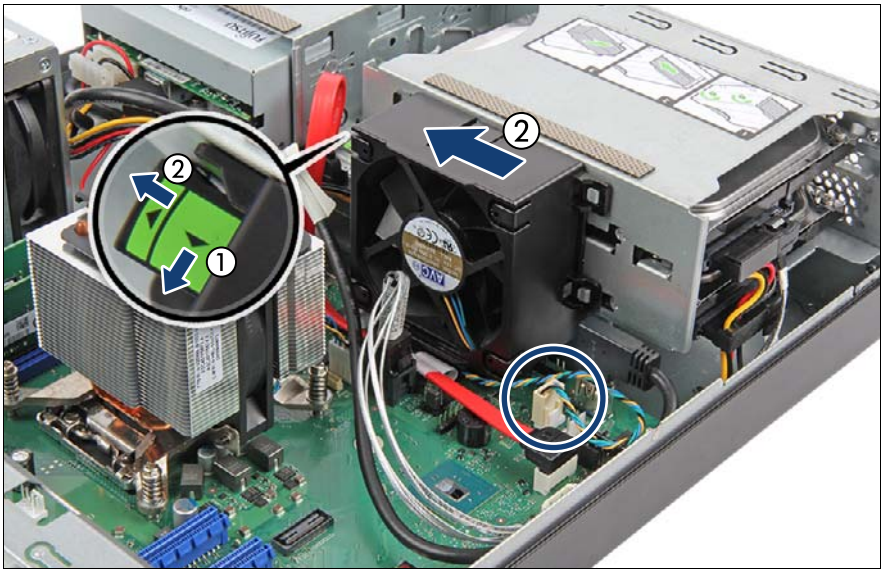

Figure 76: Removing the HDD fan module

- ► Pull the locking lever away from the HDD cage to disengage the fan module (1).
- ► Pull the lever in the shown direction (2) and remove the fan module.
- ► Disconnect the fan cable from system board (see circle).

8.3.3 Removing the fan from the holder

– Remove the fan from the holder as described in section "Removing the fan from the holder" on page 176.

8.3.4 Installing the fan into the holder

– Install the fan into the holder as described in section "Installing the fan into the holder" on page 178.

8.3.5 Installing the HDD fan module

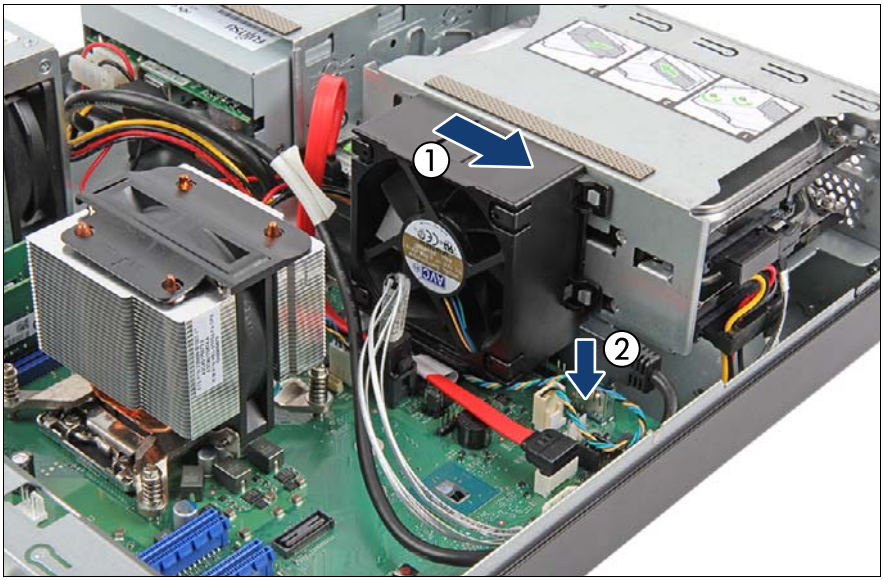

Figure 77: Installing the HDD fan module

- ► Insert the HDD fan module into the chassis.
- ► Engage the HDD fan at the rear of the HDD cage and slide it to the right (1) until it locks in place.
- ► Connect the fan cable to system board connector "FAN2 SYS" (2).

8.3.5.1 Cable routing

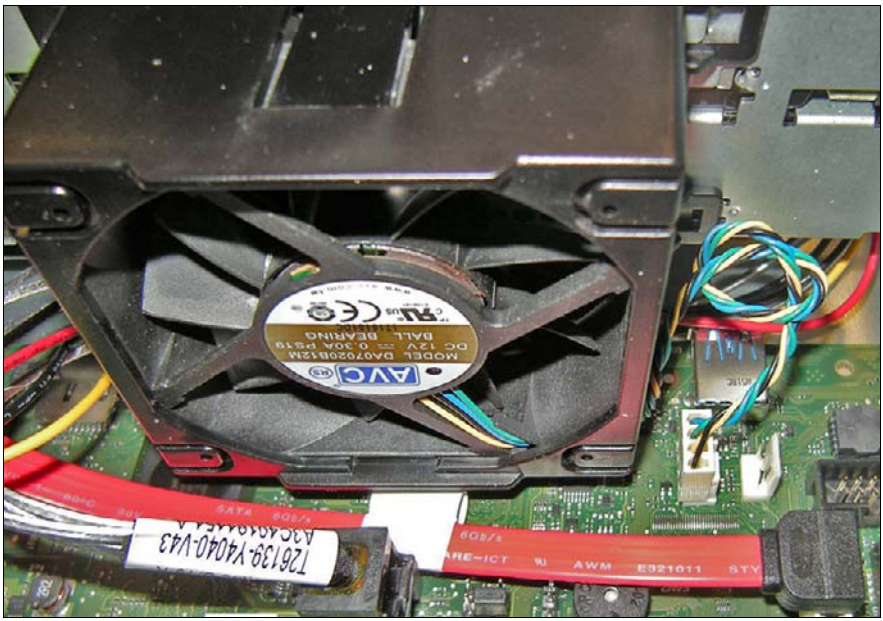

Figure 78: Cable routing for the HDD fan module

► Route the cable as shown.

8.3.6 Concluding steps

► "Reassembling" on page 61
► "Connecting the power cord" on page 64
► "Switching on the server" on page 69
► "Performing a fan test" on page 108

9 Expansion cards and backup units

Safety notes

CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- For further information, please refer to chapter "Important information" on page 35.

9.1 Basic information

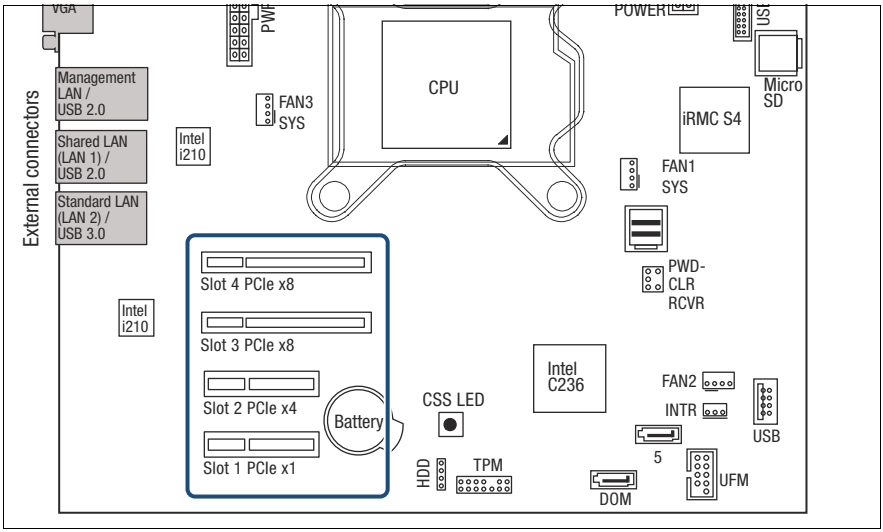

Figure 79: PCI slot overview

PCI slot	Type	Function
1	PCIe x1	slot for optional 32-bit PCI riser board (mechanical width: x4)
2	PCIe x4	Preferred slot for PCIe graphics card(mechanical width: x4)
3	PCIe x8	Preferred slot for SAS HDD controllers (mechanical width: x8)
4	PCIe x8	dedicated slot for boot controllers (mechanical width: x8)

Expansion card overview

	Max pcs per system	Slot no			
		1	2	3	4
SAS/RAID controller					
PRAID EP580i (planned)	1	-	-	-	-
PRAID EP540i (planned)	1	-	-	-	-
RAID Ctrl SAS 12G (D3216) Cougar4 / PRAID EP400i	1	-	-	-	1
RAID Ctrl SAS 12G (D3216) Cougar4 / PRAID EP420i	1	-	-	-	1
Modular RAID Lynx4 (3307/A1x) PRAID CP400i	1	-	-	-	1
Ethernet controller					
PLAN AP 1x1Gbit Cu Intel I210-T1 (Beaver Lake)	2	3	2	1	4
PLAN CP 4x1Gbit Cu Intel I350-T4 (Stonylake-QP)	2	3	2	1	4
PLAN CP 2x1Gbit Cu Intel I350-T2 (Stonylake-DP)	2	3	2	1	4
PLAN EP X710-DA2 2x 10Gb SFP+	1	-	2	1	3
PLAN EP OCe14102 2x 10Gb	1	-	2	1	3
PLAN EP X550-T2 2x 10GBASE-T	1	-	2	1	3
SAS controller					
PSAS CP400i (D3327)	1	-	2	1	-
Miscellaneous					
Nvidia NVS315 PCI-E x16, 1GB, Dual-DVI-I or Dual VGA Graphics Card	1	-	2	1	-
TPM 1.2 Module (D3127-A1x)	1	-	-	-	1
TPM 2.0 Module (D3127)	1	-	-	-	1

For the latest information of the installing order, refer your server's hardware configurator available online at the following address:
http://ts.fujitsu.com/products/standard_servers/index.htm

For Japan:
http://jp.fujitsu.com/platform/server/primergy/system/

9.2 Handling slot brackets

9.2.1 Installing a slot bracket

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

Use the low profile bracket perforated for relevant controllers.

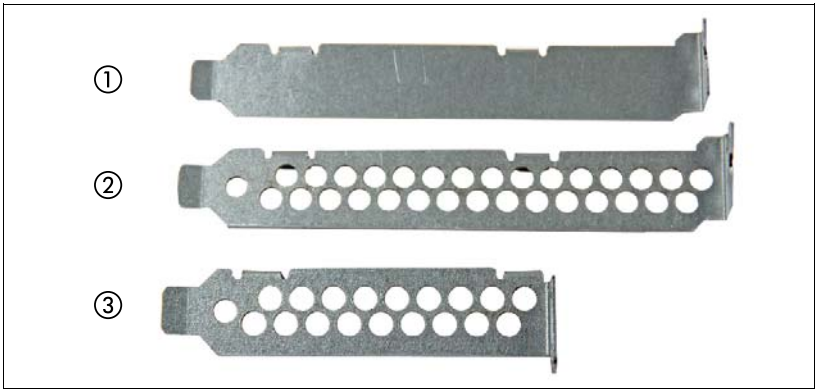

Figure 80: Perforated and non-perforated slot brackets

1	Full height bracket non-perforated
2	Full height bracket perforated
3	Low profile bracket perforated

Installing the slot bracket

- ► Place the controller on the mounting tabs on the slot bracket.
- ► Fasten the slot bracket to the controller with two M3 x 4.5 mm screws.

Example network adapter

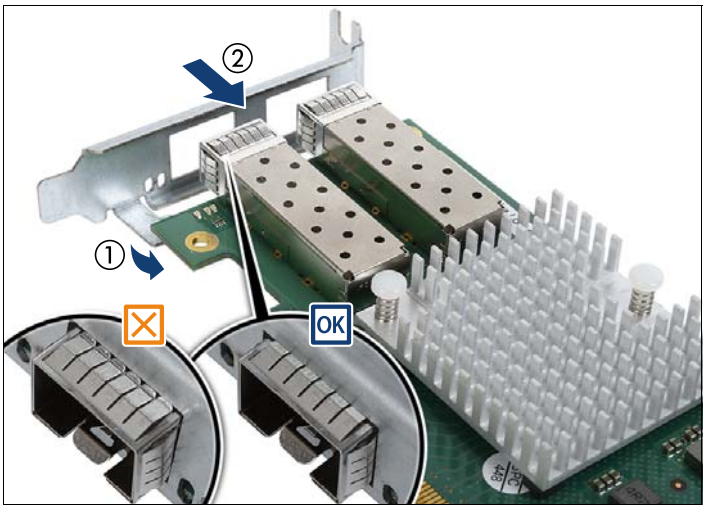

Figure 81: Example: Placing the slot bracket

- ► Place the controller on the slot bracket (1).
- ► Carefully shift the slot bracket towards the controller (2).
- ► Ensure that the ESD springs properly engage with the slot bracket as shown (see circles).

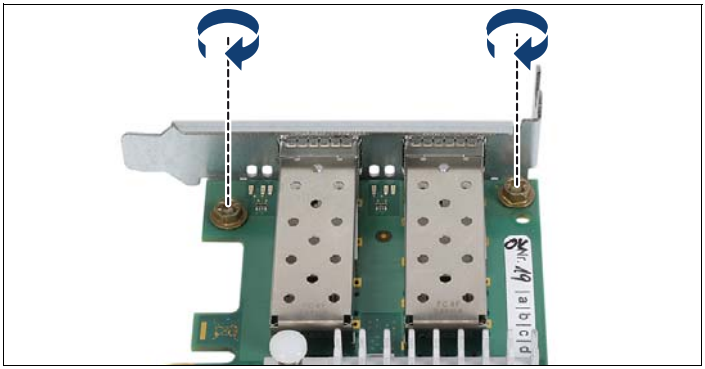

Figure 82: Example: Fastening the slot bracket

- ► Fasten the slot bracket to the controller with two M3 x 4.5 mm screws.

9.2.2 Removing a slot bracket

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.2.2.1 Removing the slot bracket

- ► Remove the two screws.
- ► Remove the controller from the mounting tabs on the slot bracket.

9.3 Handling SFP+ transceiver modules

For Fiber Channel over Ethernet (FCoE) configurations, the ethernet server adapter is equipped with one or two SFP+ (small form-factor pluggable) transceiver modules.

9.3.1 Installing SFP+ transceiver modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	tool-less

Preparing the SFP+ transceiver module

Figure 83: Removing the protective cap

- ► Remove the SFP+ transceiver module from its protective packaging.
- ► Remove the protective cap from the new/additional SFP+ transceiver module.

CAUTION!

– Always keep the protective caps attached to the SFP+ transceiver modules and fiber-optic cable connectors until you are ready to make a connection.

– Save the protective cap for future use.

Figure 84: Unlatching the locking bail

- ► Carefully unlatch and fold down the locking bail on the SFP+ transceiver module.

Inserting the SFP+ transceiver module

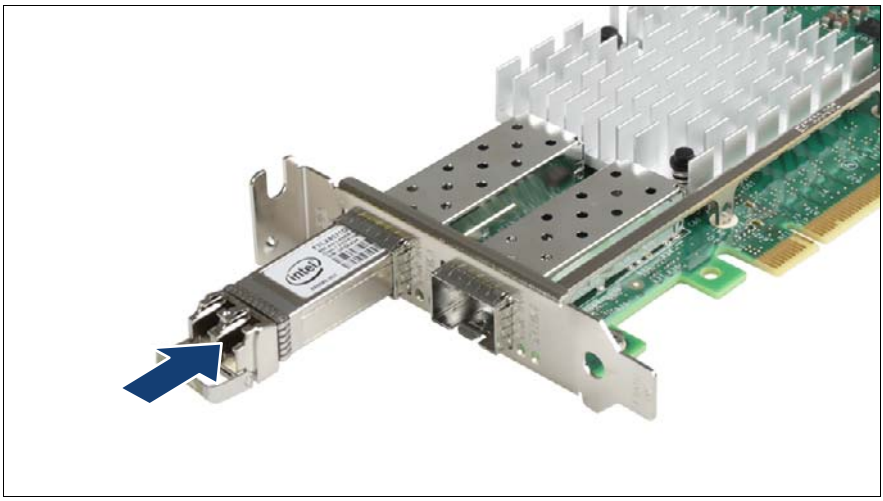

Figure 85: Inserting the SFP+ transceiver module

- Insert and slide the SFP+ transceiver module into the socket connector as far as it will go.

  If only one slot is equipped with a SFP+ transceiver module, use the left connector as shown.

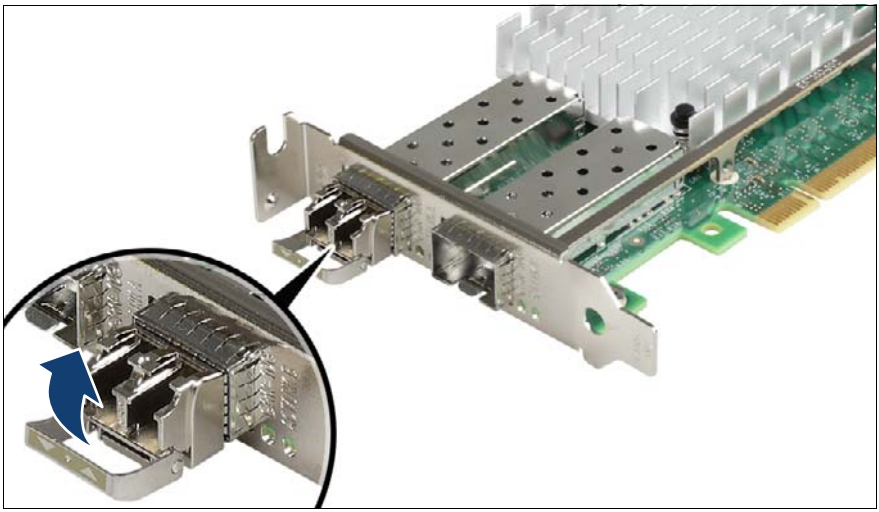

Figure 86: Latching the locking bail

► Carefully fold up and latch the locking bail.

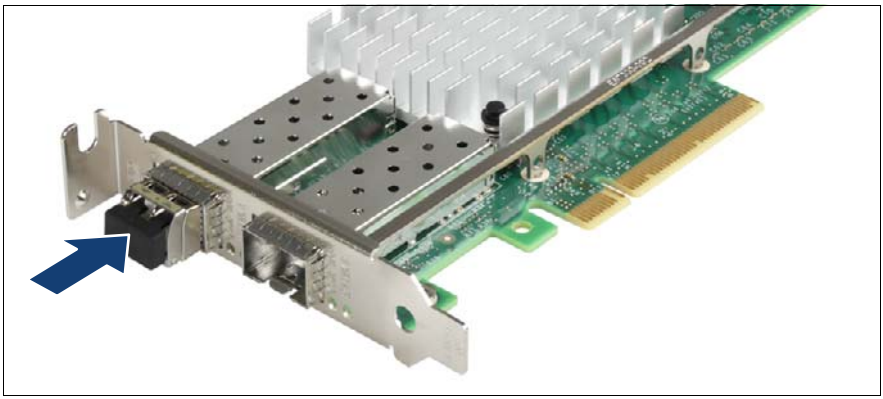

Figure 87: Installing the protective cap

► If the SFP+ transceiver module is not immediately connected to an LC connector, attach the protective cap to the SFP+ transceiver module.

Installing the secondary SFP+ transceiver module

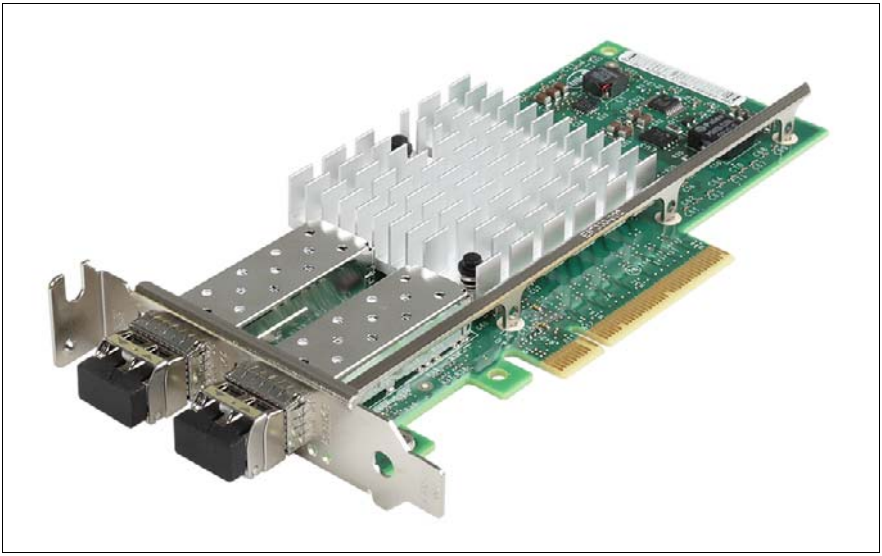

Figure 88: Installing the secondary SFP+ transceiver module

► If applicable, install the secondary SFP+ transceiver module accordingly.

9.3.2 Removing an SFP+ transceiver module

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

For Fiber Channel over Ethernet (FCoE) configurations, the ethernet server adapter is equipped with one or two SFP+ (small form-factor pluggable) transceiver modules.

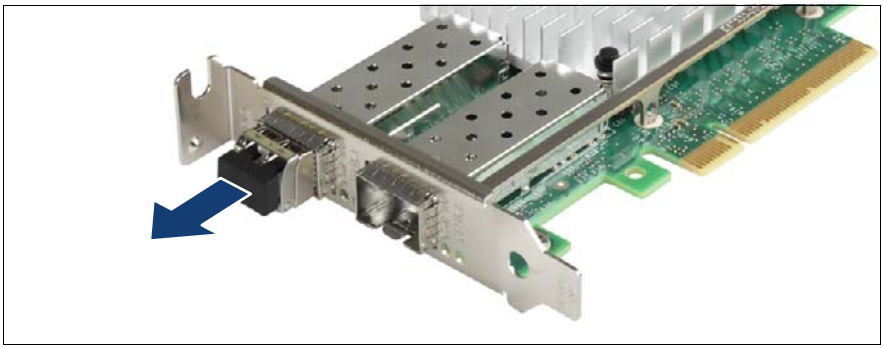

Figure 89: Removing the protective cap

► If present, remove the protective cap from the SFP+ transceiver module.

CAUTION!

Save the protective cap for future use.

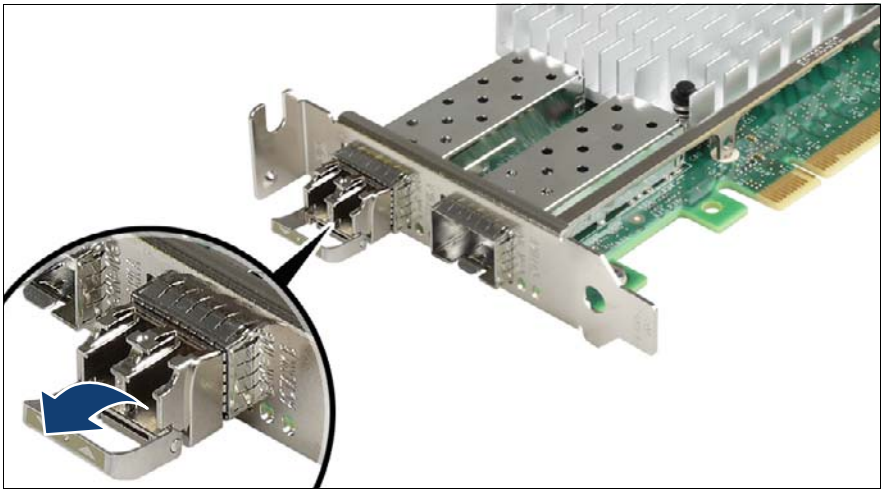

Figure 90: Unlatching the locking bail

► Carefully unlatch and fold down the locking bail on the SFP+ transceiver module to eject the transceiver from the socket connector.

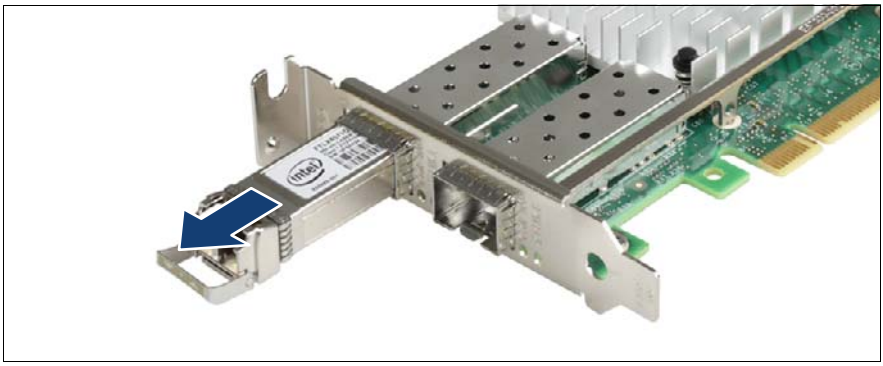

Figure 91: Removing the SFP+ transceiver module

- Pull the SFP+ transceiver module out of its socket connector.
- Attach the protective cap to the SFP+ transceiver module.

Place the removed SFP+ transceiver module in an antistatic bag or other protective environment.

9.4 Expansion cards

9.4.1 Installing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Software: 5 minutes

Tools:	tool-less

9.4.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Configuring LAN teaming" on page 79
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

9.4.1.2 Removing a PCI slot cover

Figure 92: Opening the PCI slot bracket clamp

► Fold up the PCI slot bracket clamp.

Figure 93: Removing the PCI slot cover

► Remove the PCI slot cover.

CAUTION!

Keep the slot cover for future use. Always replace slot covers into unused PCI slot openings to comply with applicable EMC regulations and satisfy cooling requirements.

9.4.1.3 Installing an expansion card

- ► Remove the expansion card from its protective packaging.

  For further instructions regarding controller settings, please refer to the accompanying documentation.

- ► If applicable, attach the required slot bracket to the expansion card as described in section "Installing a slot bracket" on page 190.

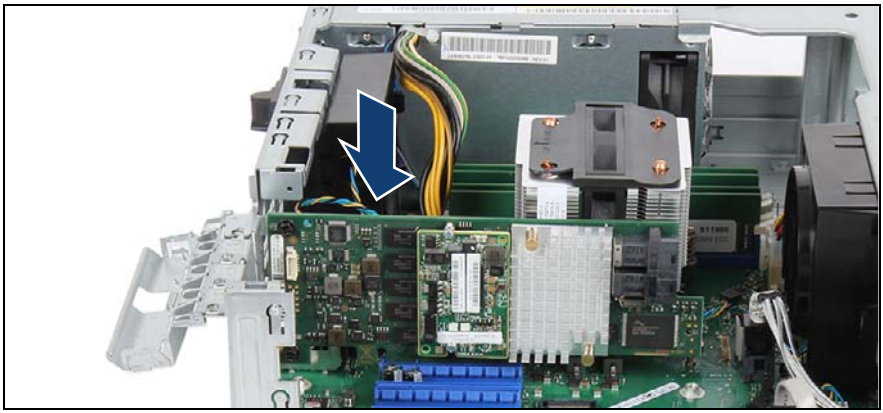

Figure 94: Installing the expansion card

- ► Carefully insert the expansion card into the desired PCI slot and press down firmly until it is fully seated in the slot.

  Slot 4 is the preferred slot for SAS RAID controllers.

- ► Fold down slot bracket clamp until it locks in place.
- ► If applicable, install SFP+ transceiver modules into the replacement expansion card, as described in section "Installing SFP+ transceiver modules" on page 192.

9.4.1.4 Connecting cables to the expansion card

► If applicable, connect internal cables to the expansion card.

For the cable plan see section "Cabling" on page 319.

9.4.1.5 Concluding steps

► "Reassembling" on page 61

► If applicable, connect external cables to the expansion card.

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

► "Updating RAID controller firmware" on page 87

► "Enabling Option ROM scan" on page 88

► "Resuming BitLocker functionality" on page 102

► "After replacing / upgrading LAN controllers" on page 106

9.4.2 Removing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

9.4.2.1 Preliminary steps

- "Locating the defective server" on page 49
- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- If applicable, disconnect external cables to the expansion card.
- "Getting access to the component" on page 55

9.4.2.2 Removing an expansion card

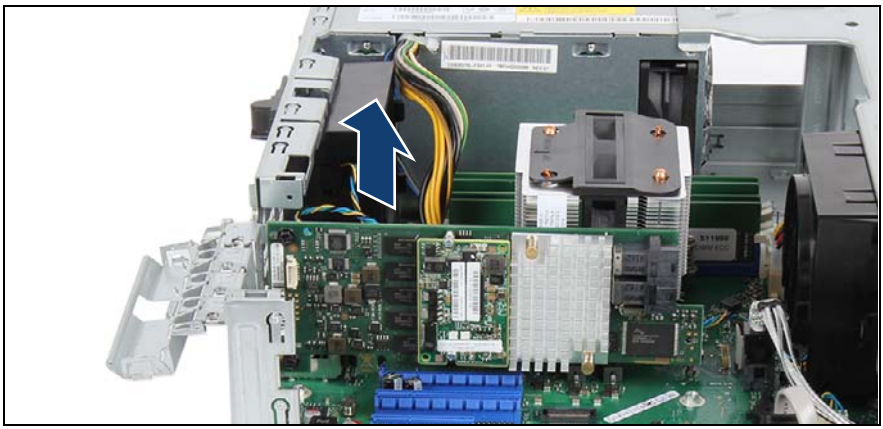

Figure 95: Removing an expansion card

- ► Fold up the locking handle on the slot bracket clamp.
- ► If applicable, remove SFP+ transceiver modules from the expansion card, as described in section "Removing an SFP+ transceiver module" on page 196.
- ► Carefully remove the expansion card from its slot.

9.4.2.3 Installing a PCI slot cover

CAUTION!

Always replace slot covers into unused PCI slot openings to comply with applicable EMC regulations and satisfy cooling requirements.

Figure 96: Installing a PCI slot cover

- Insert a PCI slot cover into the unused PCI slot opening.
- Fold down PCI slot bracket clamp until it locks in place.

9.4.2.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

9.4.3 Replacing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Software: 5 minutes

Tools: tool-less

Note on network settings recovery

When replacing network controllers or the system board, network configuration settings in the operating system will be lost and replaced by default values. This applies to all static IP address and LAN teaming configurations.

Ensure to note down your current network settings before replacing a network controller or the system board.

9.4.3.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Configuring LAN teaming" on page 79
- "Locating the defective server" on page 49
- If applicable, ensure to note down your current network settings in the operating system.
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- If applicable, disconnect external cables to the expansion card.
- "Getting access to the component" on page 55
- "Locating the defective component" on page 51

9.4.3.2 Removing an expansion card

- "Removing an SFP+ transceiver module" on page 196
- "Removing expansion cards" on page 202

9.4.3.3 Installing an expansion card

- "Installing expansion cards" on page 198
- "Installing SFP+ transceiver modules" on page 192

9.4.3.4 Connecting cables to the expansion card

- If applicable, connect internal cables to the expansion card.

  For the cable plan see section "Cabling" on page 319.

9.4.3.5 Concluding steps

- "Reassembling" on page 61
- If applicable, connect external cables to the expansion card.
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Enabling replaced components in the system BIOS" on page 96
- "Updating RAID controller firmware" on page 87
- "Resuming BitLocker functionality" on page 102
- After replacing a network controller in a server running Linux OS, "Updating the NIC configuration file in a Linux and VMware environment" on page 100
- If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard).

  Configuration of network settings should be performed by the customer. For further information, please refer to section "Note on network settings recovery" on page 205.
- If applicable, restore LAN teaming configurations, see "After replacing / upgrading LAN controllers" on page 106
- Inform the customer about changed WWN and MAC addresses, see "Looking up changed MAC / WWN addresses" on page 103

9.4.4 Replacing TFM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH1 / (+) No.1 screw driver

9.4.4.1 Preliminary steps

- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

9.4.4.2 Removing the defective TFM

- Remove the depending expansion card as described in section "Removing expansion cards" on page 202.

Example RAID controller D3216

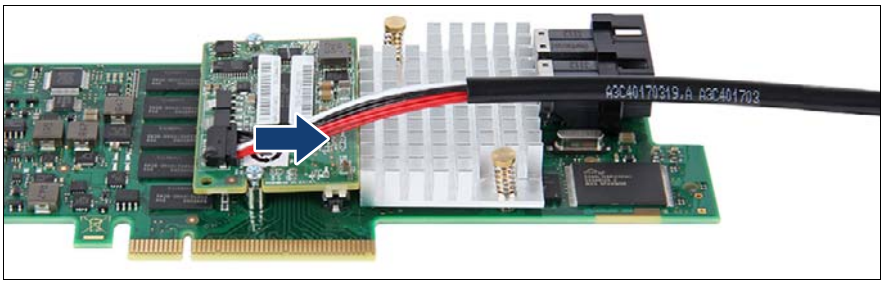

Figure 97: Disconnecting the FBU adapter cable from the TFM

- Disconnect the FBU adapter cable from the TFM.

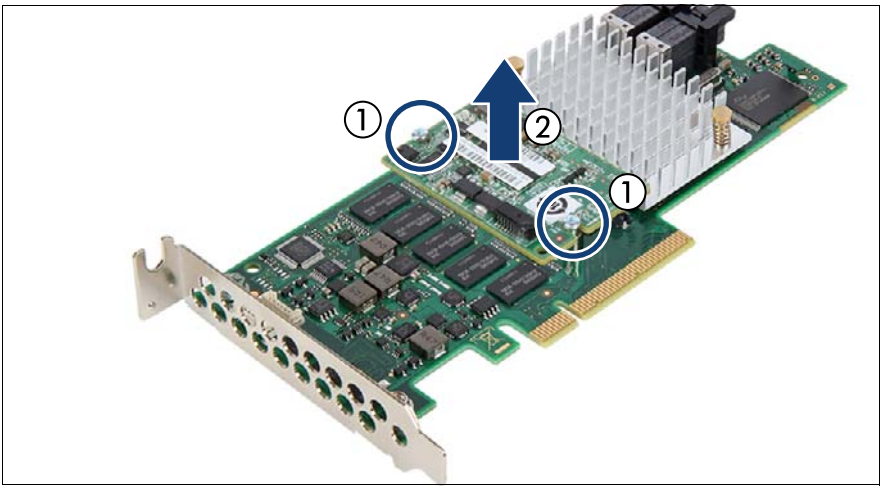

Figure 98: Removing the TFM

- ► Remove the two screws (1).
- ► Remove the TFM (2).

Note for replacing the TFM:
The two spacer bolts can remain on the RAID controller.

9.4.4.3 Installing a TFM

Example RAID controller D3216

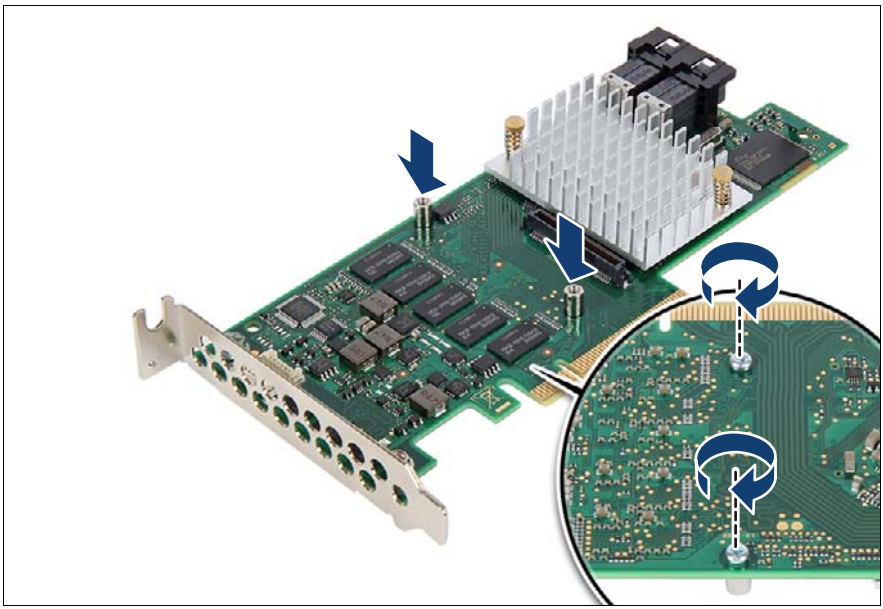

Figure 99: Installing the TFM (A)

► If no TFM has been installed before: fit the two spacer bolts on the RAID controller.

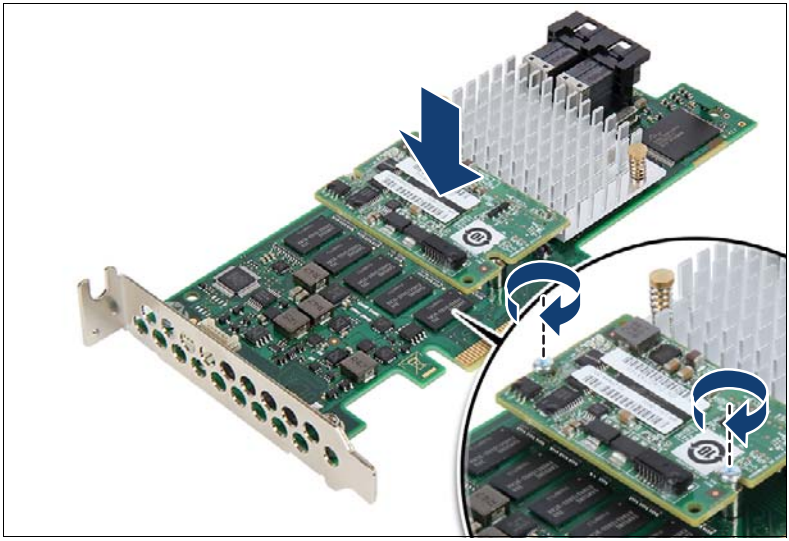

Figure 100: Installing the TFM (B)

► Secure the TFM on the RAID controller with the two screws from the TFM kit.

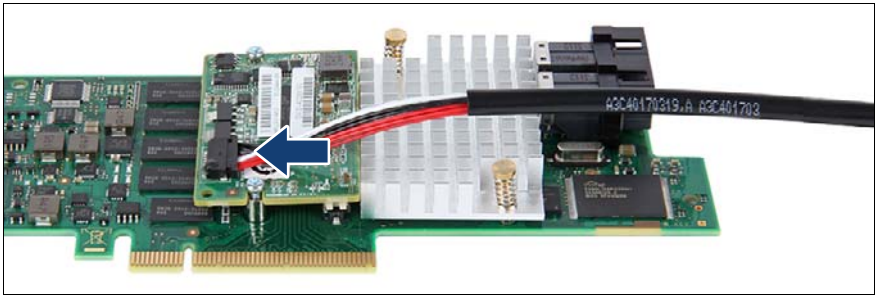

Figure 101: Connecting the FBU adapter cable

► Connect the FBU adapter cable to the TFM.

► Install the SAS RAID controller as described in section "Installing expansion cards" on page 198.

9.4.4.4 Concluding steps

► "Reassembling" on page 61

► If applicable, connect external cables to the expansion card.

- "Connecting the power cord" on page 64
- "Switching on the server" on page 69

9.5 Backup Units

The FBU backs up the memory contents of the RAID controller in the event of a power failure. You can install one FBU.

9.5.1 Installing an FBU

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH1 / (+) No.1 screw driver (for installing the TFM)

9.5.1.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Disconnecting the front USB connector" on page 273

9.5.1.2 Preparing the FBU

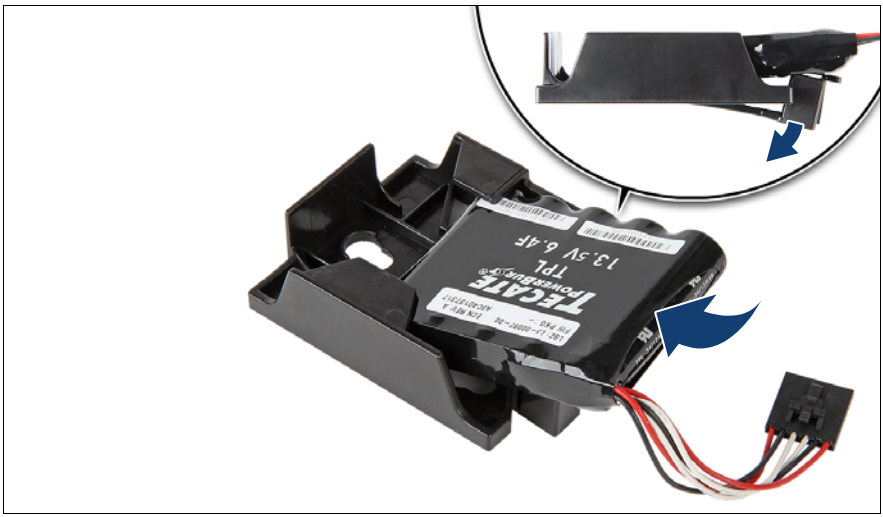

Figure 102: Installing the FBU in the holder (A)

- ► At a slight angle, fit the FBU under both retaining brackets of the holder.
- ► Push in the FBU until it locks in place.

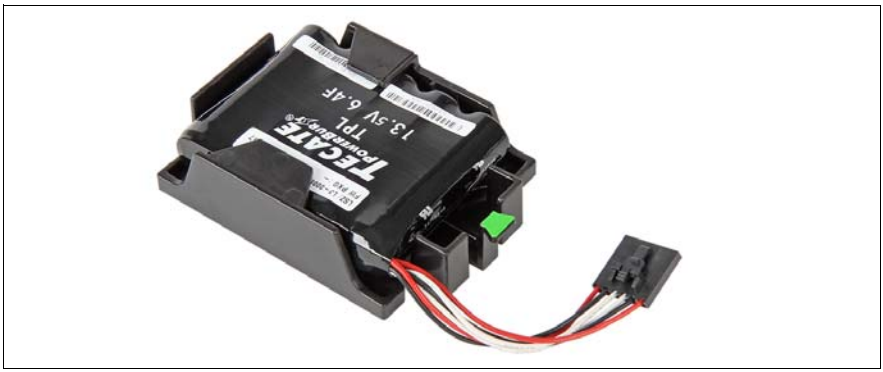

Figure 103: Installing the FBU in the holder (B)

- ► Ensure that the FBU is properly seated in the holder as shown.

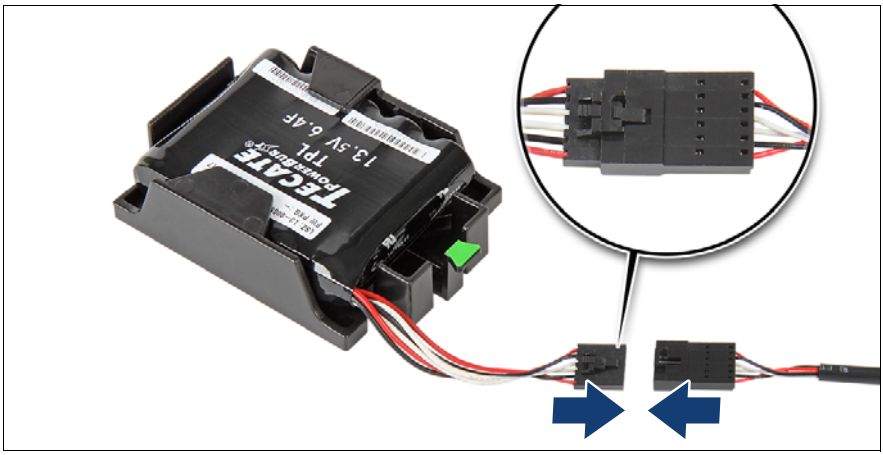

Figure 104: Connecting the FBU adapter cable to the FBU

► Connect the cable end on the FBU to the FBU adapter cable as shown.

9.5.1.3 Removing the FBU holder

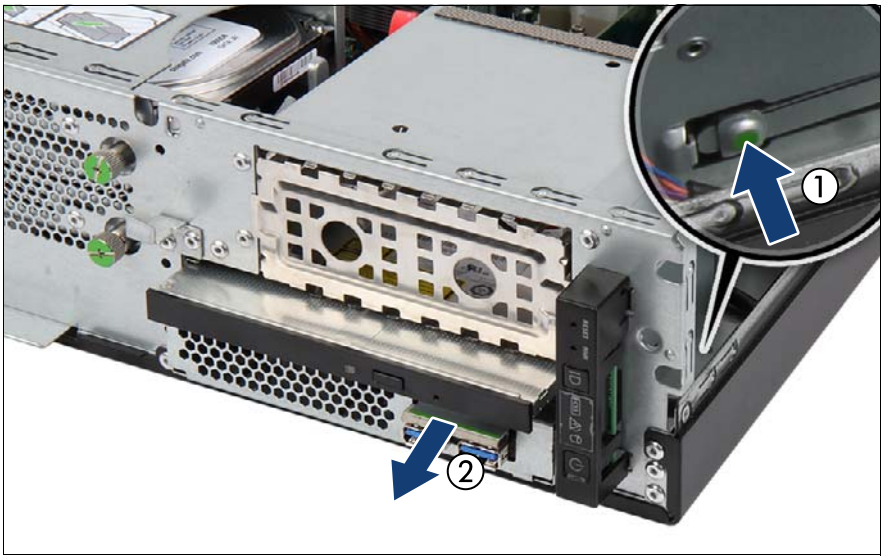

Figure 105: Removing the FBU holder

► Press on the green tab (1 close-up) and pull the FBU holder out of its bay (2).

9.5.1.4 Installing the FBU

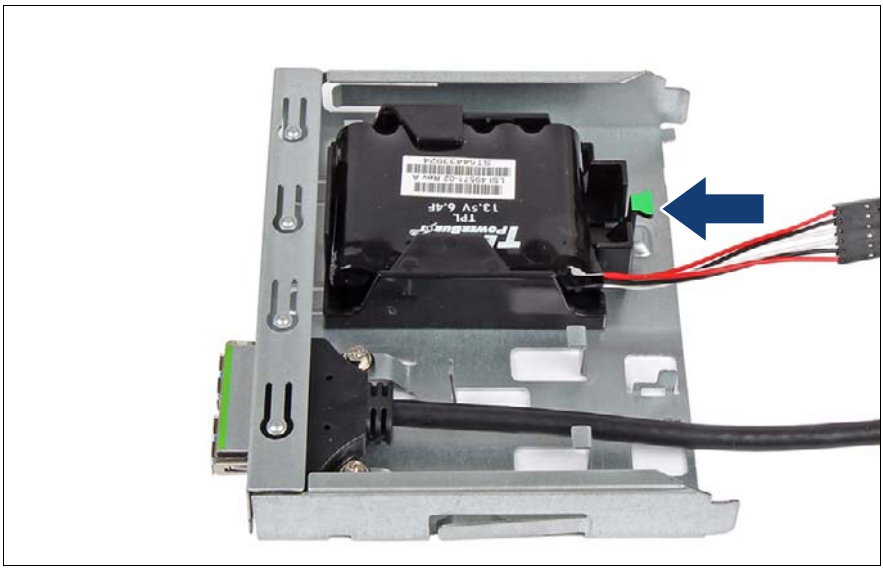

Figure 106: Installing the FBU (A)

► Insert the holder into the FBU holder so that the three hooks rest in the holder and slide it in the direction of the arrow until it locks in place.

Figure 107: Installing the FBU (B)

► Insert the FBU holder into the corresponding bay and slide it into the bay as far as it will go (see arrow).

9.5.1.5 Connecting the FBU

► If applicable, install the TFM as described in section "Installing a TFM" on page 209.

► Connect the FBU adapter cable to the TFM as described in section "Installing a TFM" on page 209.

► Install the RAID controller with the TFM as described in section "Installing an expansion card" on page 200.

9.5.1.6 Concluding steps

► "Connecting the front USB connector" on page 271

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

► "Updating RAID controller firmware" on page 87

9.5.2 Removing an FBU

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

CAUTION!

- Dispose of used battery properly. Keep away from children.
- Do not throw flash backup units into the trash can. Batteries must be disposed of in accordance with local regulations concerning special waste.

9.5.2.1 Preliminary steps

- ► "Locating the defective server" on page 49
- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► "Getting access to the component" on page 55
- ► "Disconnecting the front USB connector" on page 273

9.5.2.2 Removing the FBU from the holder

- ► Disconnect the FBU adapter cable from the TFM as described in section "Removing the defective TFM" on page 207.
- ► Remove the holder as described in section "Removing the FBU holder" on page 213.

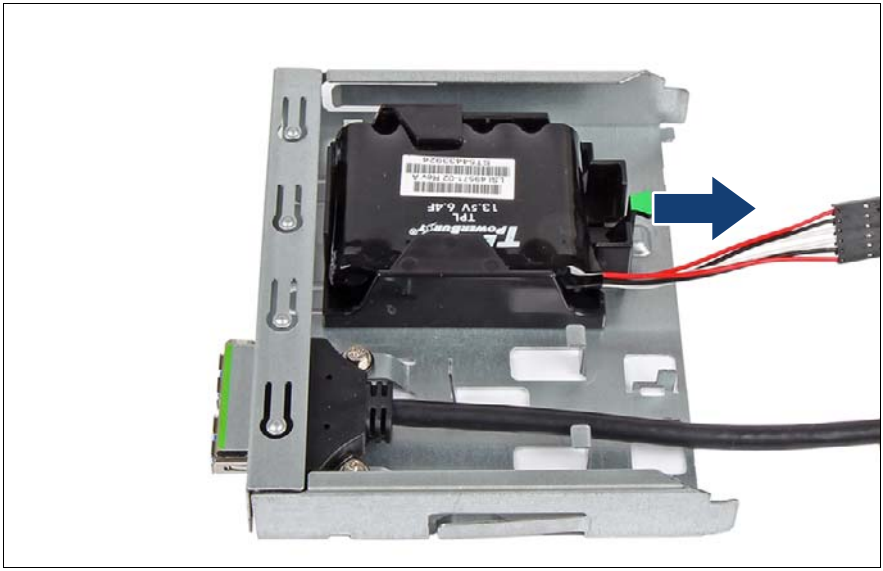

Figure 108: Removing the FBU

► Slide the holder in the direction of the arrow and remove the it from the FBU holder.

9.5.2.3 Disconnecting the FBU cable from the FBU

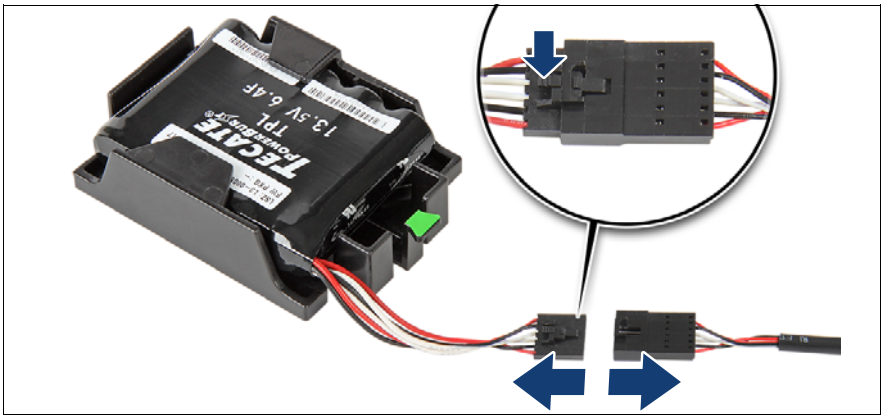

Figure 109: Disconnecting the FBU cable from the FBU

► Disconnect the cable end on the FBU from the FBU adapter cable as shown.

9.5.2.4 Installing the holder

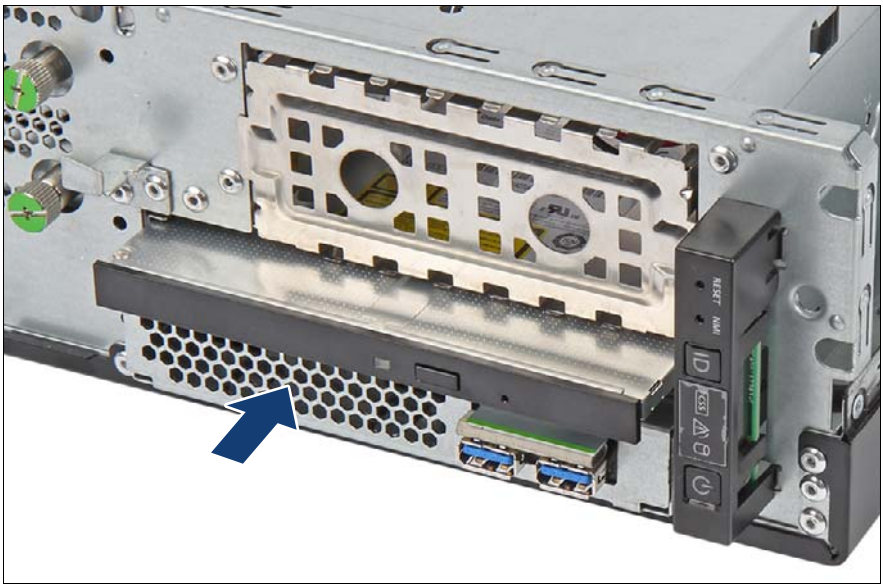

Figure 110: Removing the FBU

► Insert the holder into the corresponding bay and slide it into the bay as far as it will go (see arrow).

9.5.2.5 Concluding steps

► Connect the FBU adapter cable to the TFM as described in section "Installing a TFM" on page 209.

► "Connecting the front USB connector" on page 271

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

9.5.3 Replacing an FBU

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

CAUTION!

- Dispose of used battery properly. Keep away from children.
- Do not throw flash backup units into the trash can. Batteries must be disposed of in accordance with local regulations concerning special waste.

9.5.3.1 Preliminary steps

- ► "Locating the defective server" on page 49
- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► "Getting access to the component" on page 55
- ► "Disconnecting the front USB connector" on page 273

9.5.3.2 Removing the FBU

- ► Disconnect the cable end on the FBU from the FBU adapter cable as described in section "Disconnecting the FBU cable from the FBU" on page 217.
- ► Remove the FBU as described in section "Removing the FBU from the holder" on page 216.

9.5.3.3 Installing the new FBU

- ► Install the FBU as described in section "Installing the FBU" on page 214.
- ► Connect the FBU as described in section "Connecting the FBU" on page 215.

9.5.3.4 Concluding steps

- "Connecting the front USB connector" on page 271
- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Updating RAID controller firmware" on page 87

10 Main memory

Safety notes

CAUTION!

- Do not install unsupported third party memory modules. For further information on supported memory modules, refer to section "Basic information" on page 222.
- Memory modules remain hot after shutdown. Wait for components to cool down before installing or removing memory modules to prevent burns.
- Do not insert and remove memory modules repeatedly. Doing so may cause failures.
- Pressing out the securing clips on the memory module connector will eject the installed memory module. To prevent damage and injuries eject memory modules carefully without applying excessive force.
- For further information, please refer to chapter "Important information" on page 35.

10.1 Basic information

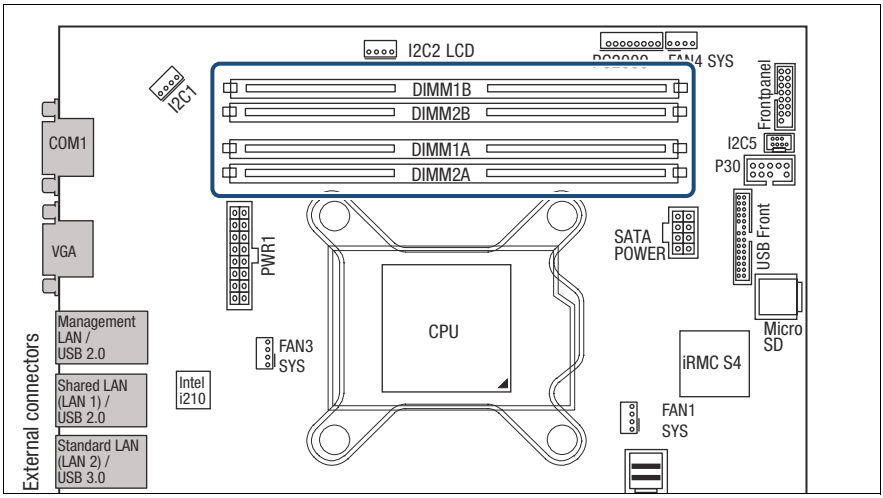

Figure 111: Slots of the main memory

The system board offers four memory slots.

Total memory size: up to 64 GB

10.1.1 Memory sequence

– Populate memory slot 1 / channel A (DIMM-1A) first.

– Within all channels memory slot 1 must be populated prior to slot 2.

– Install memory modules within a channel in descending order of capacity: higher capacity in slot 1, lower capacity in slot 2.

Channel		A		B	
Slot ID		1A	2A	1B	2B
DIMM #	1	o			
	2	o		o	
	3	o	o	o	
	4	o	o	o	o

Table 5: Mounting order - dual channel mode and single channel mode: Single CPU

10.1.2 Modes of operation

– The maximum performance can be achieved in a symmetric dual-channel configuration. Therefore both channels have to be populated with the same amount of memory. The DRAM device technology (1 Gbit / 2 Gbit / 4 Gbit) may vary from one channel to the other.

– If the amount of memory differs between the two channels, the system board will run in dual-channel asymmetric mode.

– Regardless of the mode, all DIMMs will run at the highest common frequency that is allowed by the SPD Data of the DIMMs and the maximum speed of the selected configuration.

– Single-channel mode is used if one memory module is populated in DIMM 1A.

10.2 Installing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

10.2.1 Preliminary steps

- ► "Suspending BitLocker functionality" on page 75
- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► "Getting access to the component" on page 55

10.2.2 Selecting the memory slot

- ► Choose the memory slot according to the configuration rules in "Basic information" on page 222.

10.2.3 Installing a memory module

► Identify the desired memory slot see section "Basic information" on page 222.

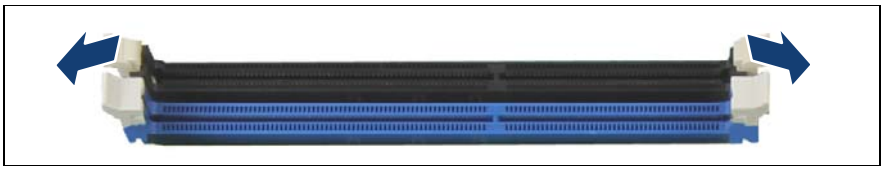

Figure 112: Opening the securing clips

► Press the securing clips on both sides of the memory slot concerned outward.

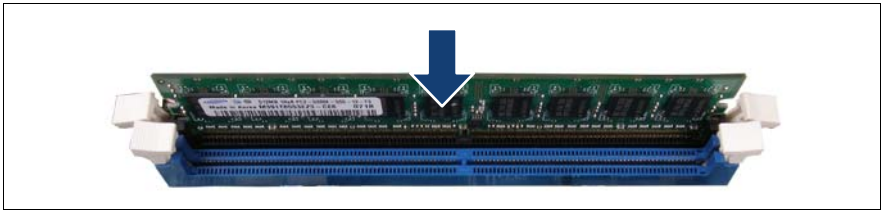

Figure 113: Installing a memory module

► Align the notch on the bottom of the module with the crossbar in the slot.

► Press down on the memory module until the securing clips snap into the cutouts at each end of the module.

10.2.4 Concluding steps

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

► "Updating or recovering the system board BIOS and iRMC" on page 84

► If applicable, "Verifying the memory mode" on page 97

► "Resuming BitLocker functionality" on page 102

10.3 Removing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	tool-less

10.3.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

10.3.2 Removing a memory module

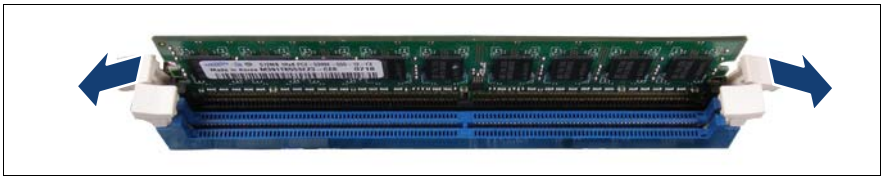

Figure 114: Removing memory modules (A)

- Eject the desired memory module by pressing out the securing clips at each end of the memory slot.

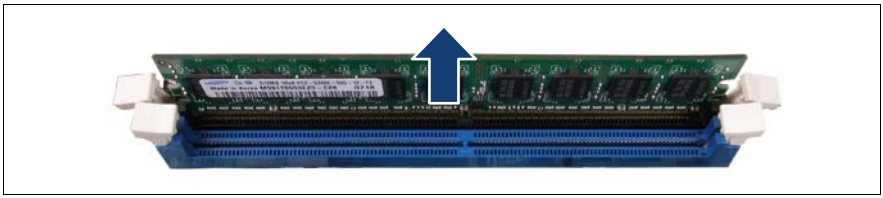

Figure 115: Removing memory modules (B)

- Remove the ejected memory module.

10.3.3 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- If applicable, "Updating or recovering the system board BIOS and iRMC" on page 84
- "Resuming BitLocker functionality" on page 102

10.4 Replacing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

10.4.1 Preliminary steps

- Identify the defective memory slot using the server management software.
- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Locating the defective component" on page 51

10.4.2 Removing the defective memory module

- Remove the memory module as described in section "Removing a memory module" on page 226.

10.4.3 Installing the new memory module

- Install the memory module as described in section "Installing a memory module" on page 225.

10.4.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resetting the error status after replacing memory modules or CPUs" on page 92
- "Enabling replaced components in the system BIOS" on page 96
- "Verifying the memory mode" on page 97
- "Resuming BitLocker functionality" on page 102

11 Processor (CPU)

Safety notes

CAUTION!

- Do not install unsupported CPUs. For further information on supported CPUs, refer to section "Basic information" on page 230.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- When removing or installing the CPU, be careful not to touch or bend the spring contacts on the CPU socket.
- Never touch the underside of the CPU. Even minor soiling such as grease from the skin can impair the CPU's operation or destroy the CPU.
- For further information, please refer to chapter "Important information" on page 35.

11.1 Basic information

11.1.1 Supported CPUs

– one Intel® Quad-Core Xeon E3-12xxv6 or one Dual Core i3-7xxx

– one CPU socket LGA 1151

For system relevant information, refer to your server's hardware configurator available online at the following address:
http://ts.fujitsu.com/products/standard_servers/index.htm

For Japan:
http://www.fujitsu.com/jp/products/computing/servers/primergy/

11.2 Upgrading or replacing the CPU

Field Replaceable Unit (FRU)

Hardware: 15 minutes
Software: 5 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

CAUTION!

CPUs are extremely sensitive to electrostatic discharge and must be handled with care. After a CPU has been removed from its protective sleeve or from its socket, place it upside down on a nonconducting, antistatic surface. Never push a CPU over a surface.

11.2.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- If applicable, "Locating the defective component" on page 51
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

11.2.2 Removing the heat sink

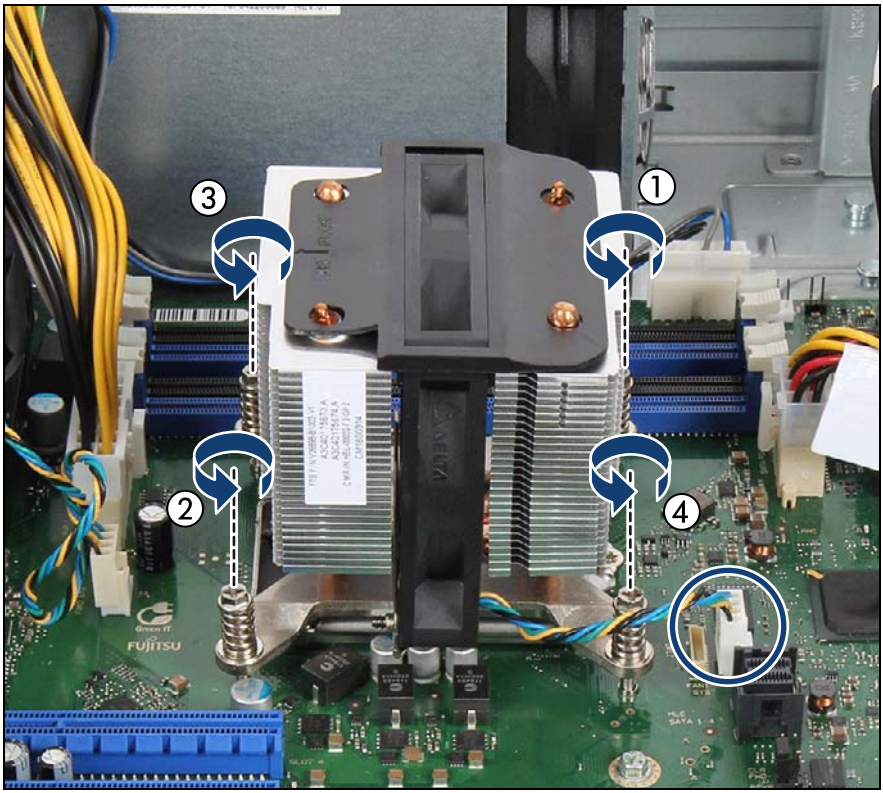

Figure 116: Removing the heat sink

- ► Disconnect the CPU fan cable to the connector "FAN1 SYS" on the system board (see circle).
- ► Loosen the four captive screws on the heat sink in a crossover pattern (1-4).
- ► Carefully twist the heat sink back and forth to detach it from the CPU. This may be necessary due to the adhesive quality of the thermal paste located between the heat sink and CPU.

CAUTION!

Pay special attention not to damage any system board components surrounding the CPU socket.

- ► Lift the heat sink out of the chassis.
- ► Thoroughly clean residual thermal paste from the surface of the heat sink and the CPU using a lint-free cloth.

11.2.3 Removing the CPU

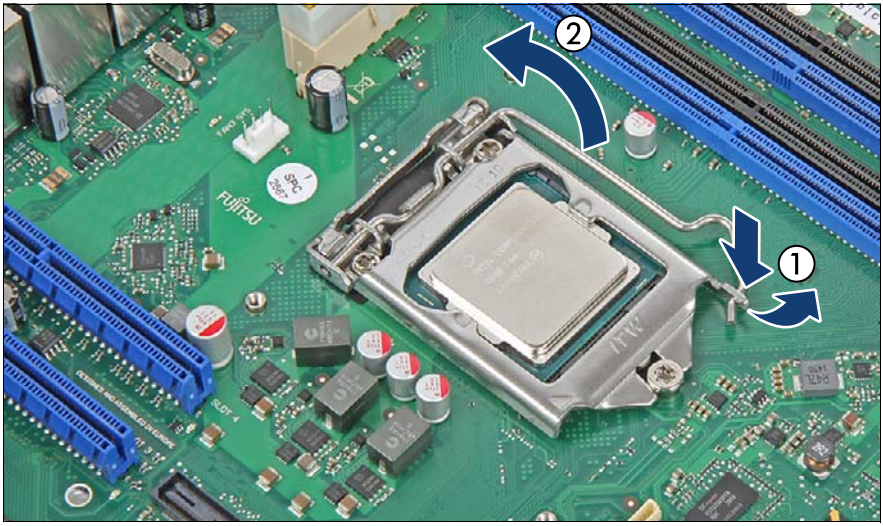

Figure 117: Unlatching the socket lever

- ► Unlatch the socket lever by pushing it down and away from the socket (1).
- ► Fold back the socket release lever (2).

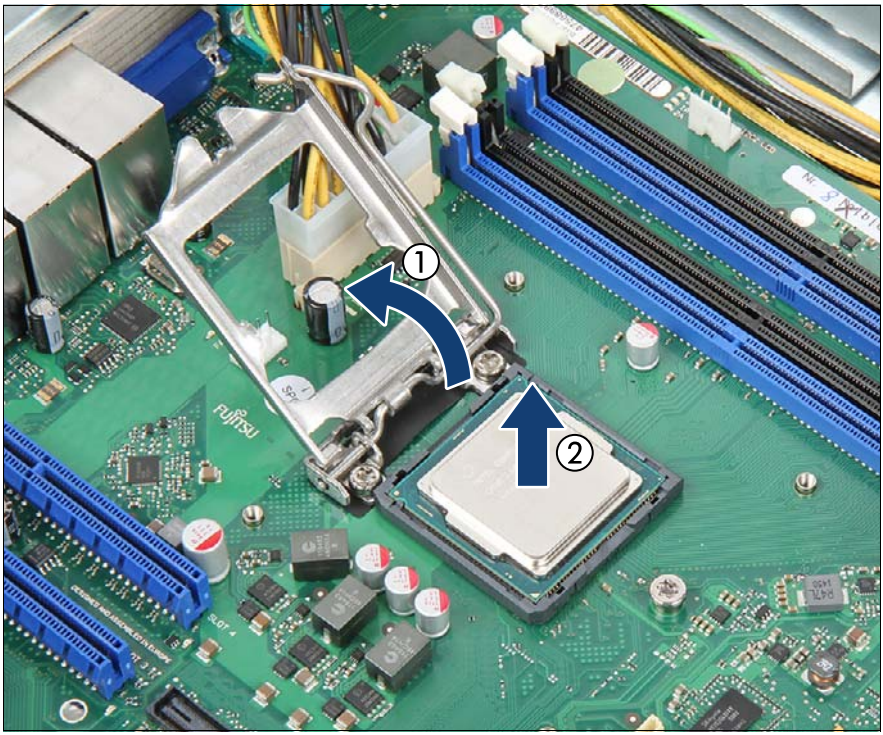

Figure 118: Removing the CPU

- ► Rotate the socket lever to lift the load plate away from the socket (1).
- ► Make sure that the load plate is in the fully open position.
- ► Carefully remove the CPU from its socket in a vertical motion (2).

CAUTION!

Be careful not to touch or bend the spring contacts on the CPU socket.

11.2.4 Installing the CPU

- ► Confirm that the CPU model number printed on the top of the CPU fits with the requirements.
- ► If applicable, remove the protective cap from the bottom side of the CPU.

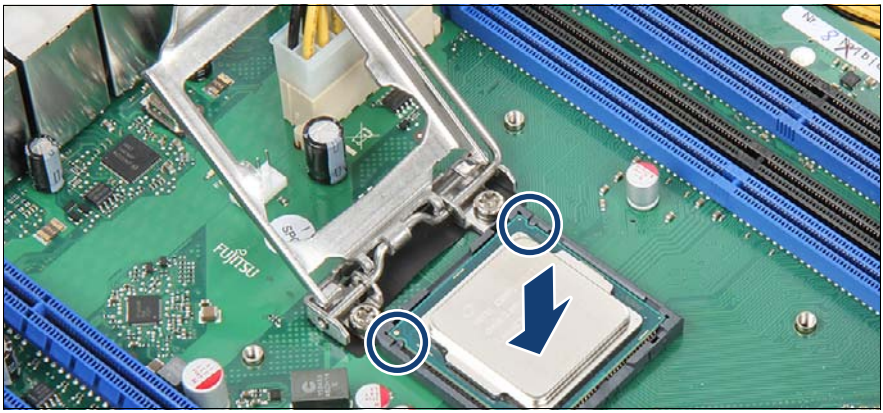

Figure 119: Installing the CPU

- ► Hold the CPU with your thumb and index finger. Make sure that the notches on the CPU align with the posts on the socket (see circles).
- ► Lower the CPU straight down without tilting or sliding it in the socket.

CAUTION!

- – Ensure that the CPU is level in the socket.
- – Be careful not to touch or bend the pins on the CPU socket.
- – Never touch the underside of the CPU. Even minor soiling such as grease from the skin can impair the CPU's operation or destroy the CPU.
- – Ensure not to scrape or dent the CPU edges.

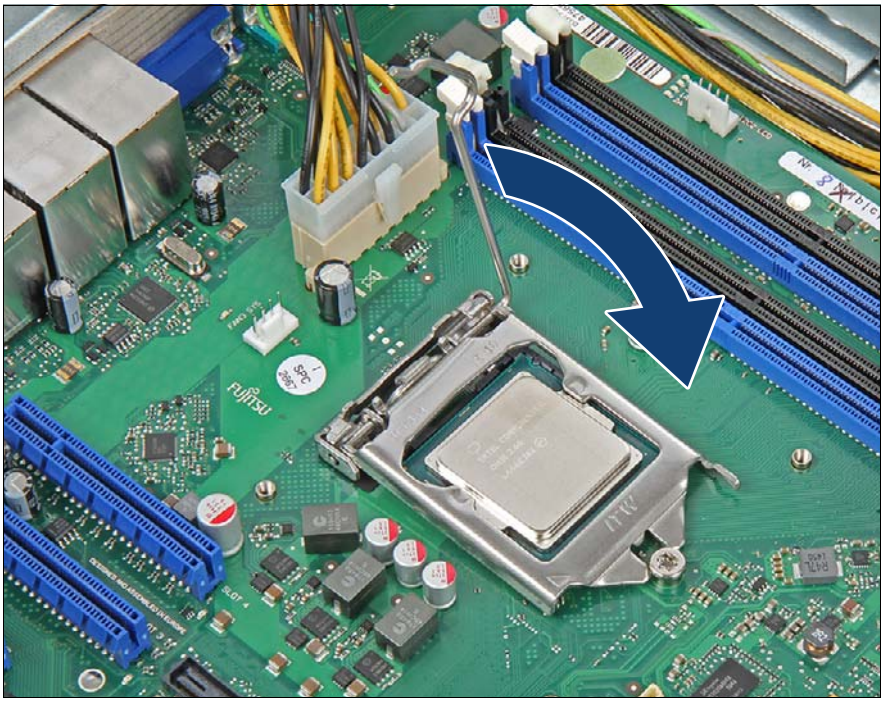

Figure 120: Closing the load plate (A)

► Lower the load plate over the CPU while leaving the socket lever in the open position.

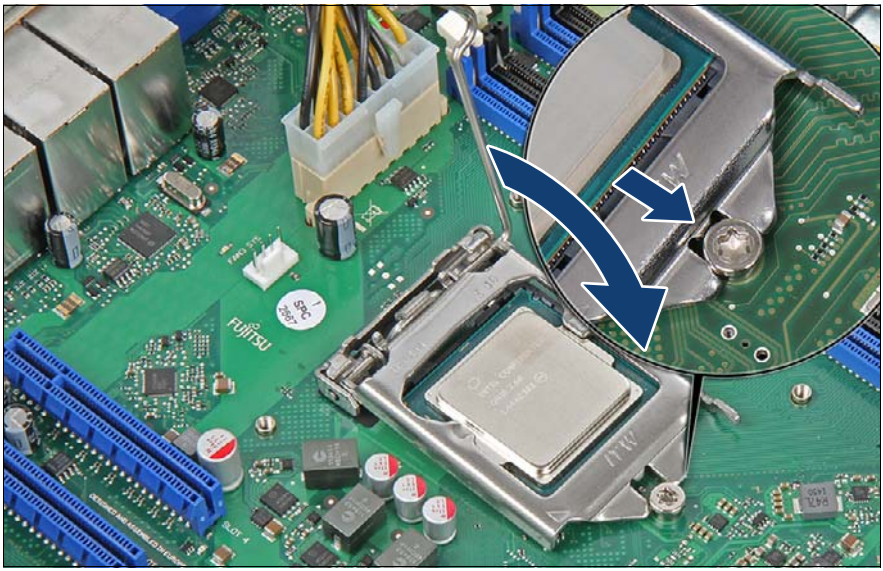

Figure 121: Closing the load plate (B)

► Lower the socket lever while making sure that the front edge of the load plate slides under the shoulder screw cap (see close-up) as the lever is lowered.

Figure 122: Latching the socket lever

► Latch the socket lever under the load plate tab.

11.2.5 Applying thermal paste

For Japan, the service engineer must follow the instruction provided separately.

If the CPU upgrade or replacement kit contains a new heat sink, a thin layer of thermal compound has already been pre-applied to its lower surface. In this case, please proceed with section "Installing the heat sink" on page 239.

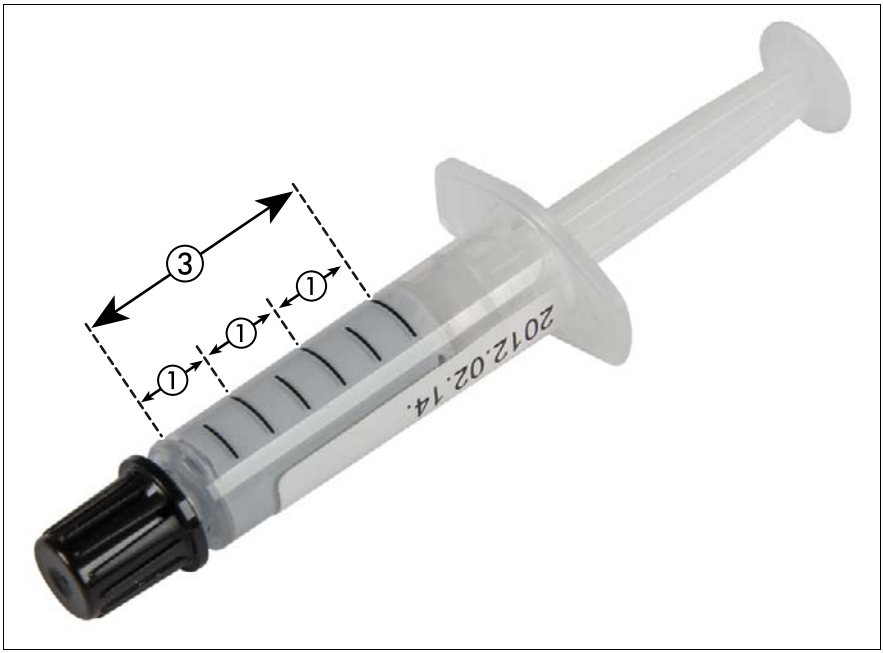

Figure 123: Thermal paste syringe

One thermal compound syringe (FTS-FSP:P304000004) contains thermal paste for three CPUs.

In order to determine the correct amount of thermal paste (equal to 1.0 gram), divide the grey area of the syringe up into three equal segments.

Add graduation marks to the syringe using a permanent marker to help you apply the thermal paste.

Figure 124: Applying thermal paste

► Apply a small point-shaped amount of thermal paste (1.0 gram, see description above) to the center of the CPU surface as shown.

CAUTION!

Do not mix different types of thermal paste.

11.2.6 Installing the heat sink

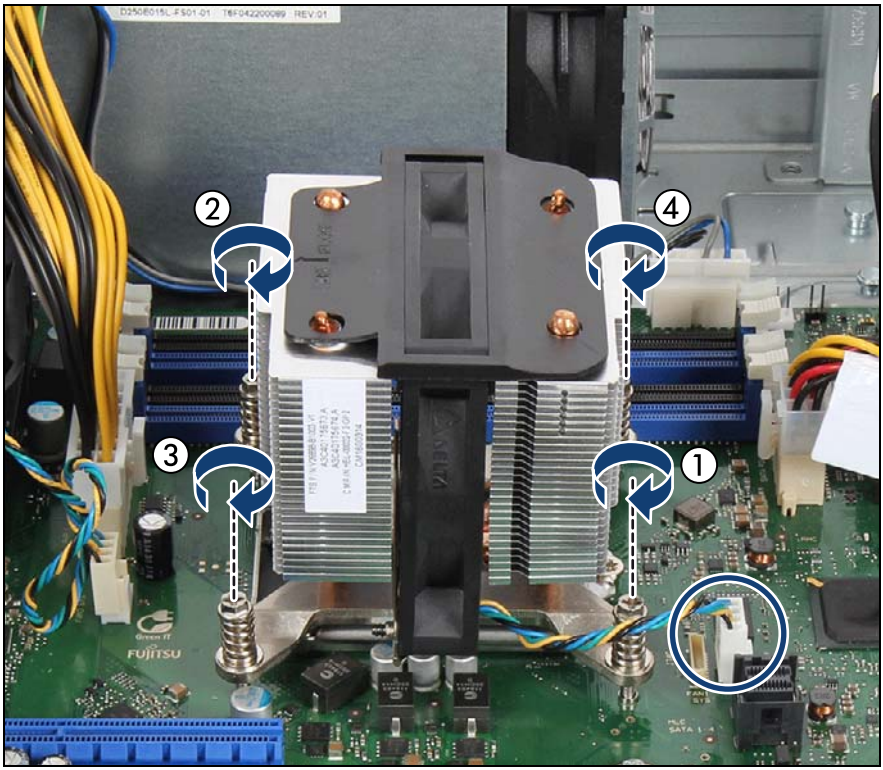

Figure 125: Installing the heat sink (B)

- ► Ensure that the heat sink cooling fins match the direction of the airflow!
- ► Carefully seat the heat sink on the four threaded holes as shown.

CAUTION!

– Ensure that the screws on the heat sink are properly seated on the threaded holes.

- ► Fasten the four captive screws on the heat sink in a crossover pattern (torque 6.0 Nm, the description of this torque value doesn't apply for Japan.) (1-4).
- ► Connect the CPU fan cable to the connector "FAN1 SYS" on the system board (see circle).

11.2.7 Concluding steps

- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69

When the system is powered on after a CPU has been replaced or upgraded, the Global Error indicator will start flashing with the error message `CPU has been changed`. This only indicates that the CPU configuration has been altered. There is no technical problem.

In order to turn off the Global Error indicator, please proceed as follows:

- ► Restart the system and wait for screen output to appear.
- ► Press the F2 function key to enter the BIOS.
  If assigned, enter the BIOS password and press Enter.
- ► In the *Save & Exit* menu, select *Save Changes and Exit* or *Save Changes and Reset*.
- ► Ensure that the Global Error indicator has stopped flashing.

– If applicable, "Updating or recovering the system board BIOS and iRMC" on page 84

– "Resetting the error status after replacing memory modules or CPUs" on page 92

– "Enabling replaced components in the system BIOS" on page 96

– "Resuming BitLocker functionality" on page 102

11.3 Replacing the heat sink

Field Replaceable Unit (FRU)

Hardware: 15 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

11.3.1 Preliminary steps

- "Locating the defective server" on page 49
- "Disconnecting the power cord" on page 53
- "Shutting down the server" on page 52
- "Getting access to the component" on page 55

11.3.2 Removing the defective heat sink

- Remove the heat sink as described in section "Removing the heat sink" on page 231.
- Remove the residual thermal paste from the CPU surface.
- Clean the CPU surface using a lint-free cloth.

11.3.3 Installing the new heat sink

- Remove the protective cover on the underside of the new heat sink.

CAUTION!

Do not touch the thermal paste on the underside of the heat sink.

- Install the heat sink as described in section "Installing the heat sink" on page 239.

11.3.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Performing a fan test" on page 108

12 Accessible drives

Safety notes

CAUTION!

- Before installing an accessible drive, acquaint yourself with the drive's user documentation.
- When inserting an accessible drive into the server, ensure not to pinch or strain any connected cables.
- When installing an accessible drive, hold it by its sides. Applying force to the top of the casing may cause failures.
- When disposing of, transferring, or returning a backup drive, ensure that all backup media has been removed from the drive.
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- For further safety information, please refer to chapter "Important information" on page 35.

12.1 Basic information

Mounting order for accessible drives

PRIMERGY TX1320 M3 server offers a 5.25-inch slimline SATA ODD bay and 3.5-inch USB backup drive bay:

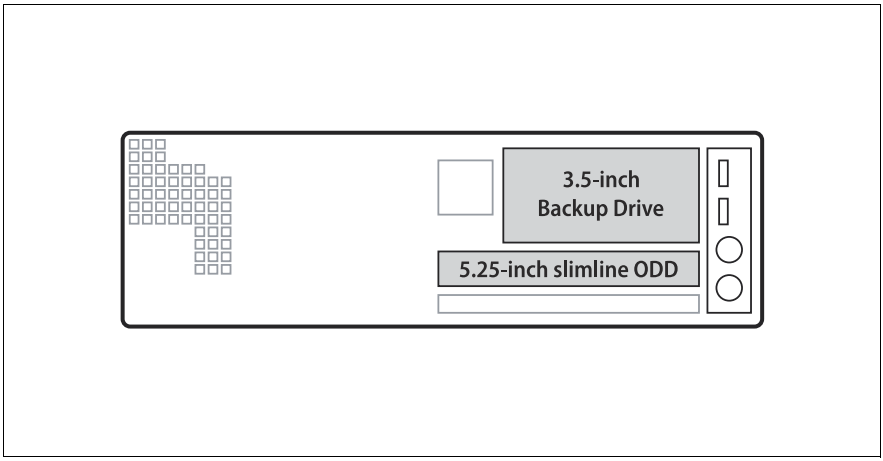

Figure 126: Accessible drives mounting order

	Accessible drive	Max. #
5.25-inch bay2	ODD	1
3.5-inch bay	Backup drive	1

Table 6: Accessible drive mounting sequence

12.2 Optical disk drive (ODD)

12.2.1 Installing the ODD

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: Phillips (+) No. 1 screw driver

12.2.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

12.2.1.2 Removing the ODD filler cover

Figure 127: Removing the ODD filler cover

► Grip the green ODD latch of the ODD filler cover (see arrow), pull out the cover and remove it from its installation bay.

CAUTION!

Save the ODD filler cover for future use.
Always replace dummy modules into unused drive bays to comply with applicable EMC regulations and satisfy cooling requirements.

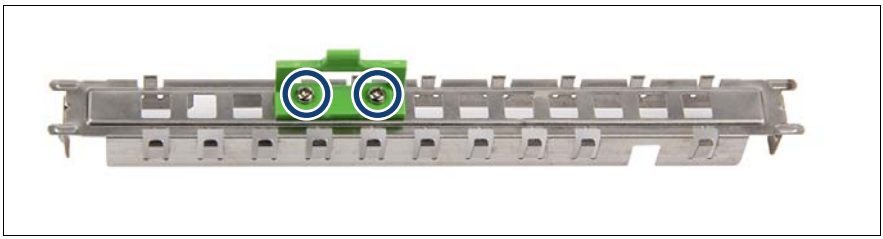

Figure 128: Removing the ODD latch

► Unscrew and remove the green ODD latch (see circles).

12.2.1.3 Installing the ODD latch

Figure 129: Installing the ODD latch on the ODD

► Fasten the ODD latch with two screws to the rear side of the ODD (see circles).

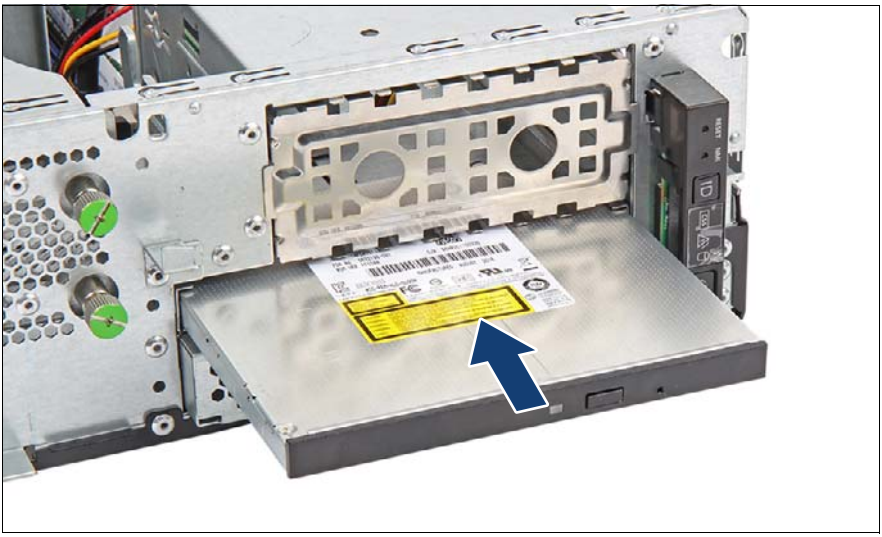

Figure 130: Installing the ODD

► Push the ODD into the bay (see arrow) simultaneously pressing the front of the ODD slightly down until the ODD latch engages.

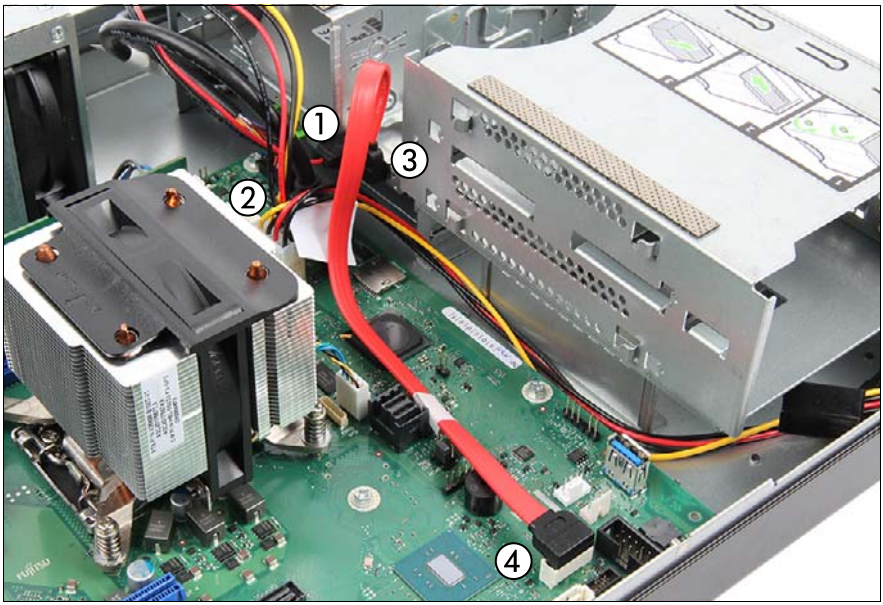

Figure 131: Connecting cables to the ODD

- Connect the power cable:
  - Connector "P5" to the connector "PWR" on the ODD (1).
  - Connector "P1" to the connector "SATA POWER" on the system board (2).
- Connect the SATA cable:
  - To the connector "SATA" on the ODD (3).
  - To the connector "SATA5" on the system board (4).

12.2.1.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

For the cable plan see section "Cabling" on page 319.

12.2.2 Removing the ODD

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips (+) No. 1 screw driver

12.2.2.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Removing backup and optical disk media" on page 78
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

12.2.2.2 Removing an ODD

- Disconnect all cables from the ODD.

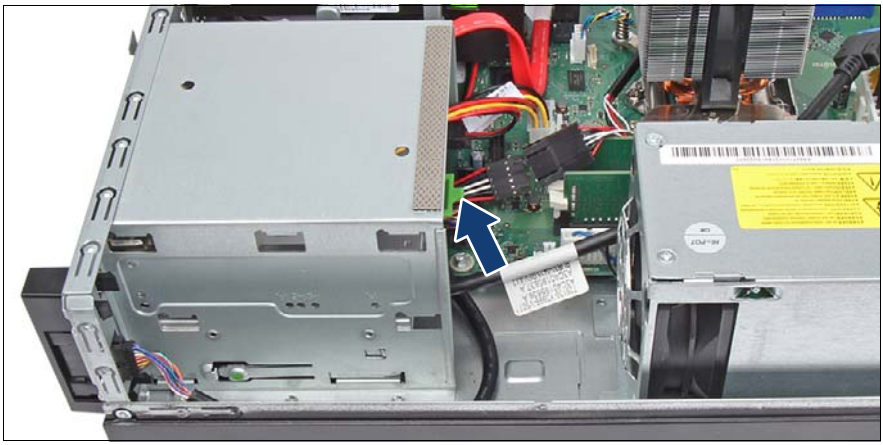

Figure 132: Unlocking the ODD

- Press the ODD latch in direction of the arrow until it disengages

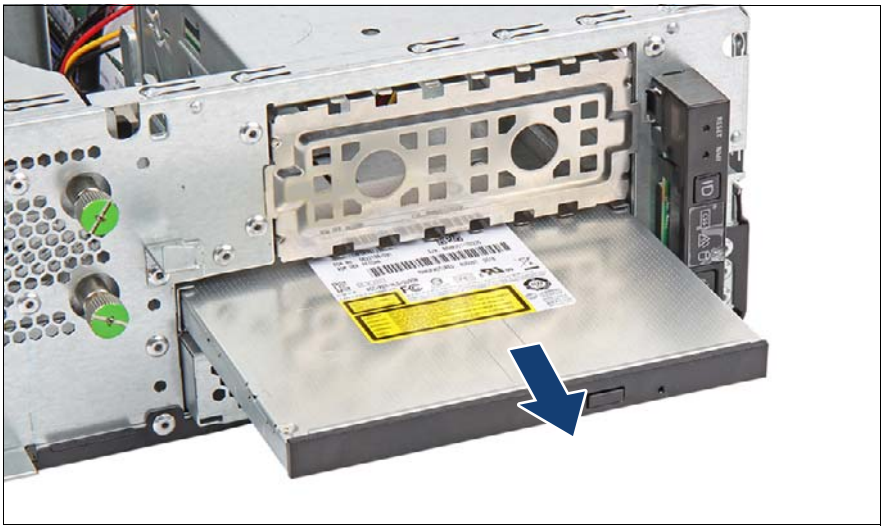

Figure 133: Removing the ODD

► Pull the ODD out of the bay (see arrow).

Figure 134: Removing the ODD latch

► Remove the two screws (see circles).

- ► Remove the ODD latch.
- ► If no new ODD will be installed:
  - ► Fasten the ODD latch with two screws to the ODD filler cover (see figure 128).
  - ► Insert the ODD filler cover into the empty ODD bay.

Figure 135: Install the ODD filler cover

- ► Install the ODD filler cover (see arrow).

12.2.2.3 Concluding steps

- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69
- ► "Resuming BitLocker functionality" on page 102

12.2.3 Replacing the ODD

Field Replaceable Unit (FRU)

Hardware: 15 minutes

Tools: Phillips (+) No. 1 screw driver

12.2.3.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Removing backup and optical disk media" on page 78
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

12.2.3.2 Removing the ODD

- Remove the ODD as described in section "Removing the ODD" on page 250.

12.2.3.3 Installing the ODD

- Install the ODD as described in section "Installing the ODD" on page 245.

12.2.3.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

12.3 Backup drive (RDX)

12.3.1 Installing the RDX drive

Upgrade and Repair Unit (URU)

Hardware: 10minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

12.3.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

12.3.1.2 Removing the drive filler cover

- Remove the HDD fan module(s) as described in section "Removing the HDD fan module" on page 175.

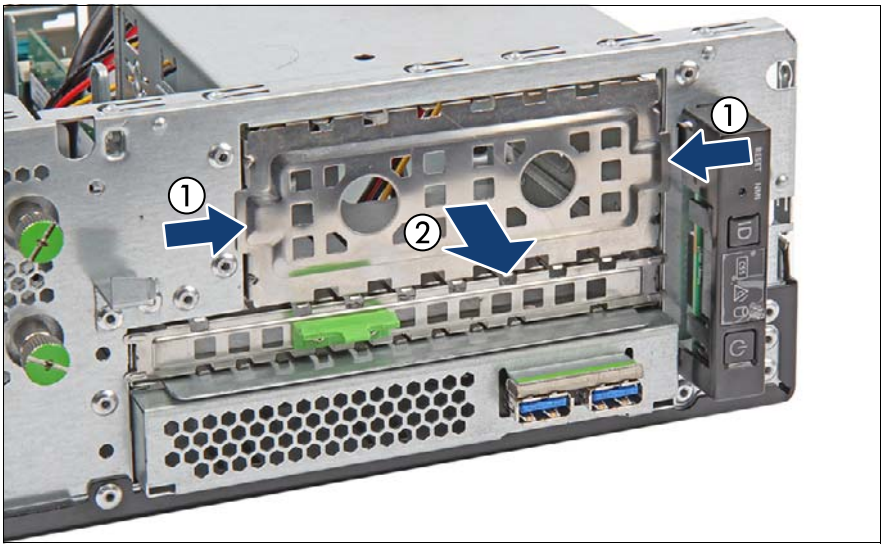

Figure 136: Removing the backup drive filler

► Hold the backup drive filler cover by its two handle recesses (1) and pull it out of the installation bay (2).

CAUTION!

Save the drive filler cover for future use.
Always replace dummy modules into unused drive bays to comply with applicable EMC regulations and satisfy cooling requirements.

12.3.1.3 Installing the RDX drive

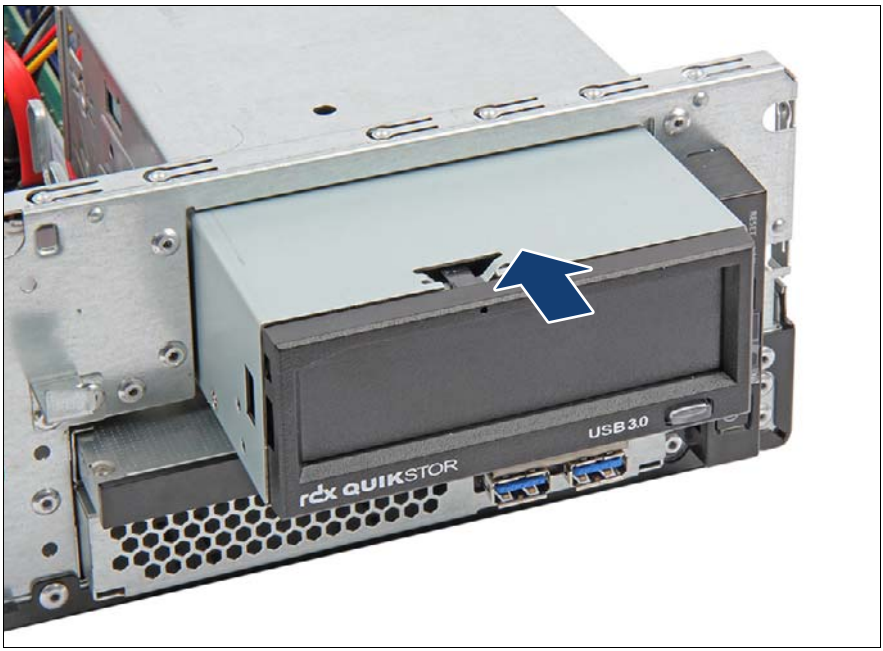

Figure 137: Installing the RDX drive (A)

- ► Insert the RDX drive into its installation bay.
- ► Carefully push back until the backup drive cover plate is flush with the front panel.

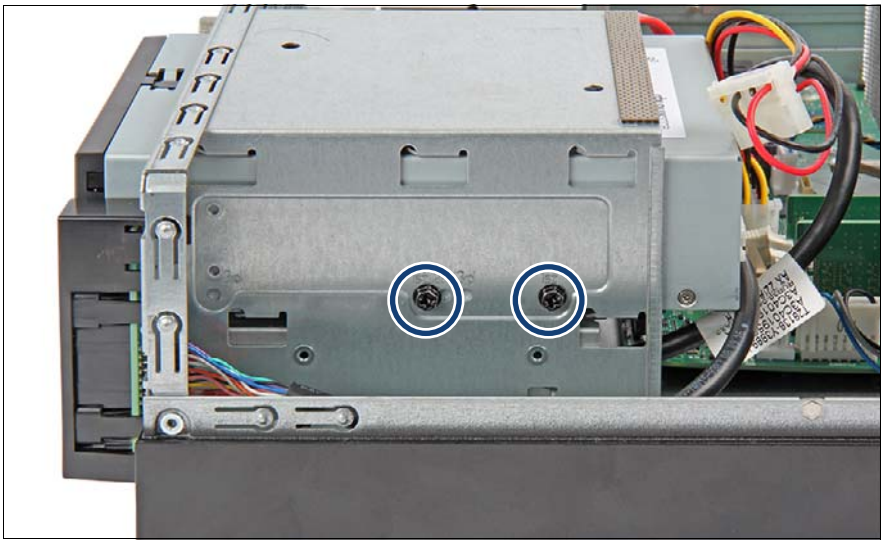

Figure 138: Installing the RDX drive (B)

► Fasten the RDX drive to the drive cage with two screws.

Use the screw hole marked "1st".

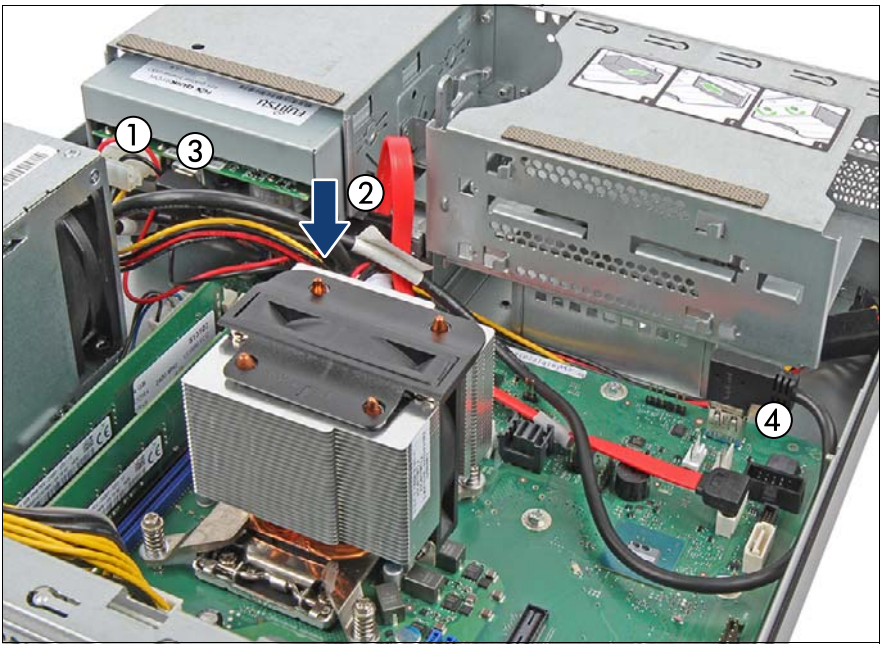

Figure 139: Connecting cables to the RDX drive

► Connect the power cable:

  – Connector "P4" to the connector "PWR" on the RDX drive (1).

  – Connector "P1" to the connector "SATA POWER" on the system board (2).

– Connect the USB cable:

  – To the connector "USB" on the RDX drive (3).

  – To the connector "USB" on the system board (4).

► In case of a 8x 2.5-inch HDD/SSDS configuration the following step is necessary: "Preparing the HDD fan module" on page 177.

  ► Prepare the second HDD fan module as described in section "Preparing the HDD fan module" on page 177.

  ► Install the HDD fan module(s) as described in section "Installing the HDD fan module" on page 179.

12.3.1.4 Concluding steps

- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69
- ► "Resuming BitLocker functionality" on page 102
- ► "Verifying and configuring the backup software solution" on page 79

For the cable plan see section "Cabling" on page 319.

12.3.2 Removing the RDX drive

Field Replaceable Unit (FRU)

Hardware: 10minutes

Tools:	Removing accessible drives: Phillips PH2 / (+) No. 2 screw driver

12.3.2.1 Preliminary steps

- ► "Suspending BitLocker functionality" on page 75
- ► "Removing backup and optical disk media" on page 78
- ► "Shutting down the server" on page 52
- ► "Shutting down the server" on page 52
- ► "Getting access to the component" on page 55

12.3.2.2 Removing the RDX drive

- ► Remove the HDD fan module(s) as described in section "Removing the HDD fan module" on page 175.
- ► Disconnect all cables from the RDX drive.

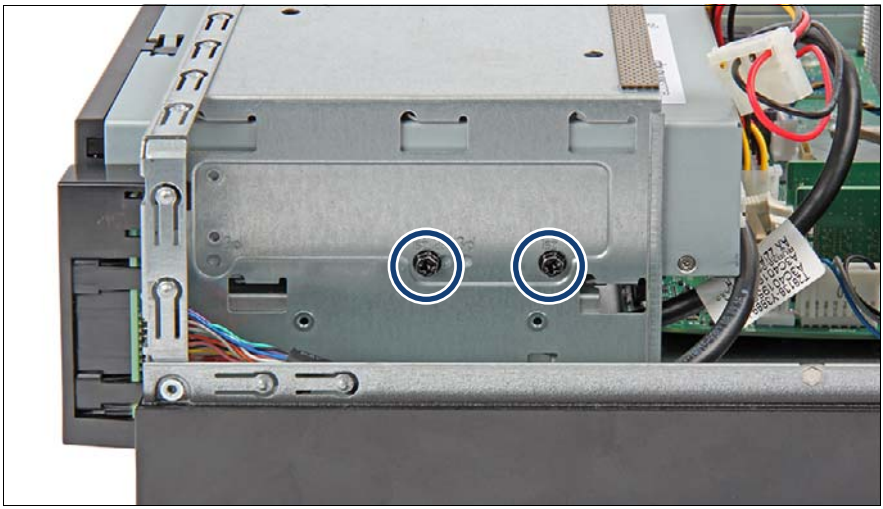

Figure 140: Removing the RDX drive (A)

► Remove the two screws (see circles).

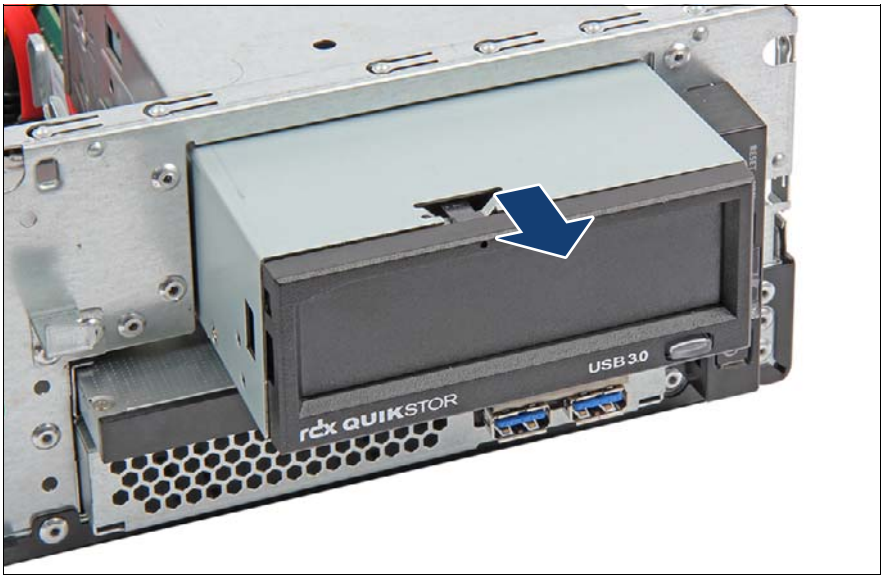

Figure 141: Removing the RDX drive (B)

► Pull the RDX drive out of its bay.

12.3.2.3 Inserting the drive filler

Figure 142: Inserting the drive filler cover

- ► Insert the drive filler cover (see arrow).
- ► Install the HDD fan modules as described in section "Installing the HDD fan module" on page 179.

12.3.2.4 Concluding steps

- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69
- ► "Resuming BitLocker functionality" on page 102
- ► "Verifying and configuring the backup software solution" on page 79

12.3.3 Replacing the RDX drive

Field Replaceable Unit (FRU)

Hardware: 10minutes

Tools:	Removing accessible drives: Phillips PH2 / (+) No. 2 screw driver

12.3.3.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Removing backup and optical disk media" on page 78
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

12.3.3.2 Replacing a RDX drive

- "Removing the RDX drive" on page 259
- "Installing the RDX drive" on page 254

12.3.3.3 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102
- "Verifying and configuring the backup software solution" on page 79

13 Front panel

Safety notes

CAUTION!

- When inserting the front panel module into the server, ensure not to pinch or strain any connected cables.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "Important information" on page 35.

13.1 Front panel module

13.1.1 Replacing the front panel module

Field Replaceable Unit (FRU)

Hardware: 10 minutes
Software: 5 minutes

Tools: tool-less

Note on system information backup / restore

The front panel module contains the Chassis ID EPROM that contains system information like server name and model, housing type, serial number and manufacturing data.

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

When replacing the front panel module, the system information like server name and model, housing type, serial number and manufacturing data are not restored automatically. So never forget to re-configure it manually by Chassis ID Prom Tool.

CAUTION!

For that reason the front panel and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

13.1.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

13.1.1.2 Removing the front panel module

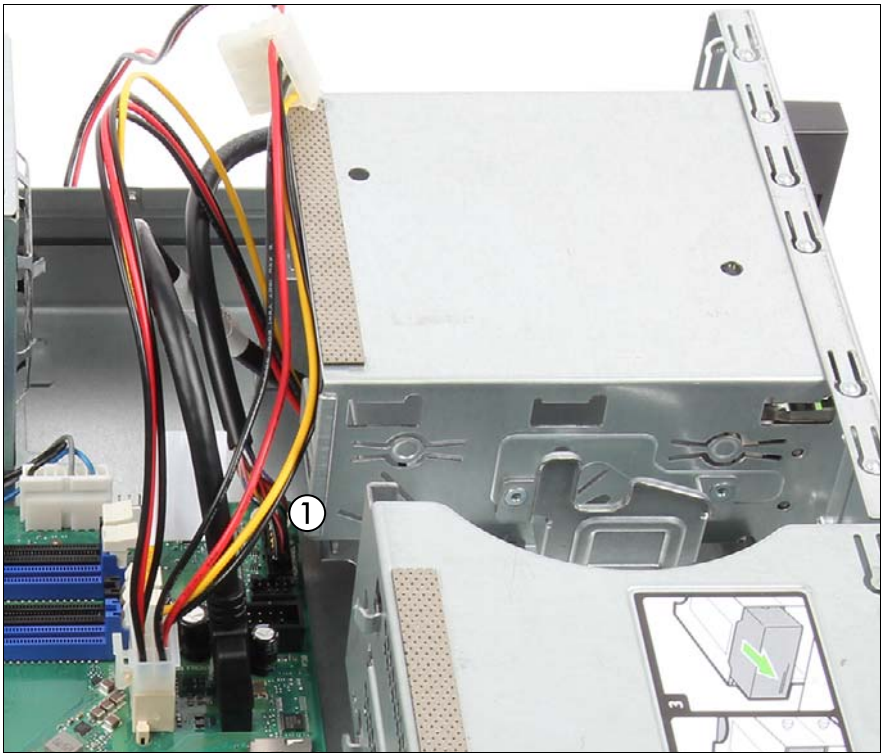

Figure 143: Disconnecting front panel cable

- Disconnect the front panel cable from the system board (1).

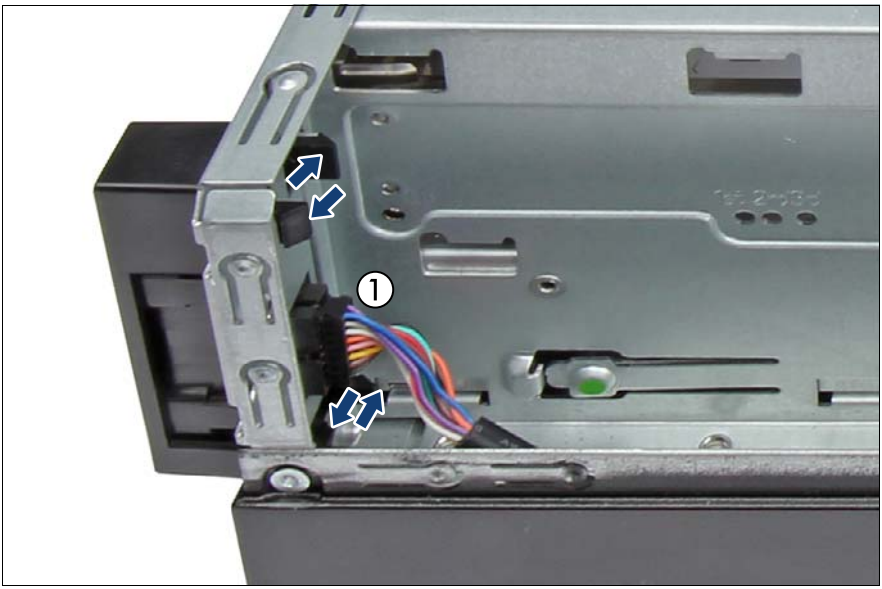

Figure 144: Removing the front panel module

- ► Disconnect the front panel cable from the front panel module (1).
- ► Disengage the retention hooks of the front panel module (see arrows).
- ► Remove the front panel module.

13.1.1.3 Installing the front panel module

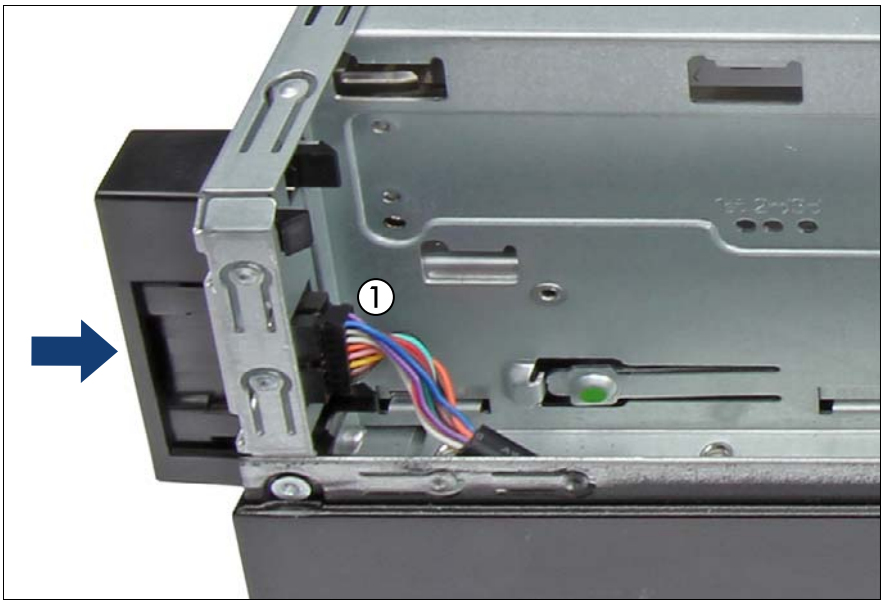

Figure 145: Inserting the front panel module

- ► Insert the front panel module as shown and carefully push in until it locks in place (see arrow).
- ► Connect the front panel cable to the front panel module (1).

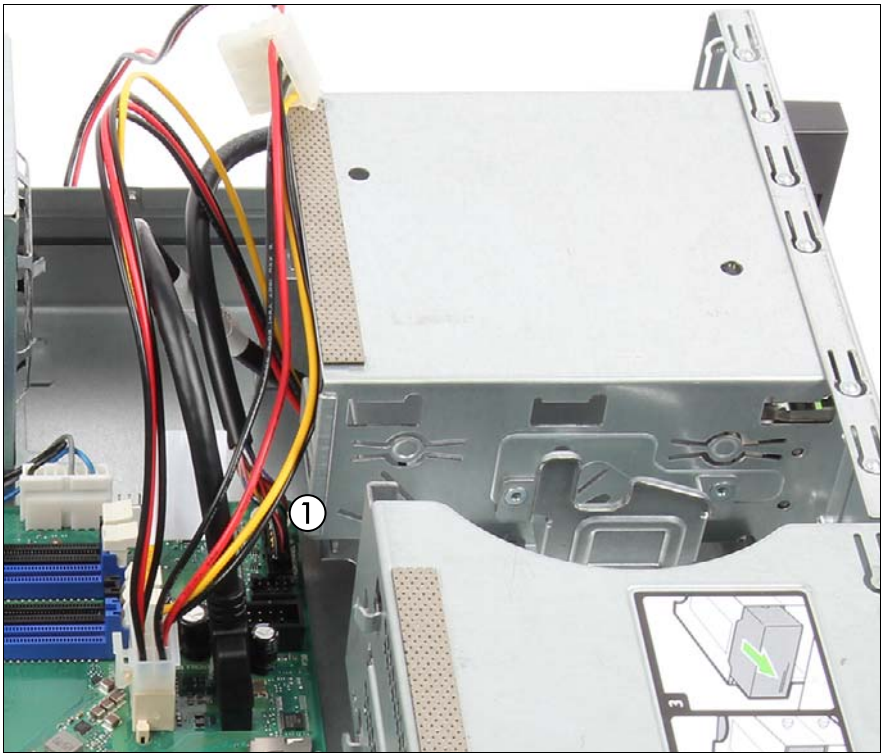

Figure 146: Connecting the front panel cable to the system board

► Connect the front panel cable to the connector "Frontpanel" on the system board (1).

13.1.1.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Verifying system information backup / restore" on page 86
- "Using the Chassis ID Prom Tool" on page 105
- "Resuming BitLocker functionality" on page 102

13.2 Front USB connector

13.2.1 Installing a front USB connector

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

13.2.1.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

13.2.1.2 Removing the holder

- Remove the holder as described in section "Removing the FBU holder" on page 213.
- If applicable, disconnect the FBU adapter cable from the TFM as described in section "Removing the defective TFM" on page 207.

13.2.1.3 Installing the front USB connector

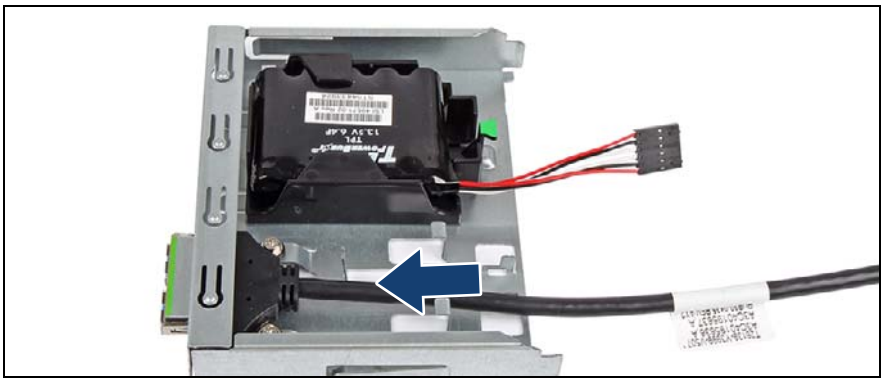

Figure 147: Installing the front USB connector

- ► Place the front USB connector on the holder and slide it into the holder until it locks in place (see arrow).
- ► Fasten the USB front connector with two screws.

Figure 148: Installing the front USB connector

- ► Insert the holder into the corresponding bay and slide it into the bay as far as it will go (see arrow).

13.2.1.4 Connecting the front USB connector

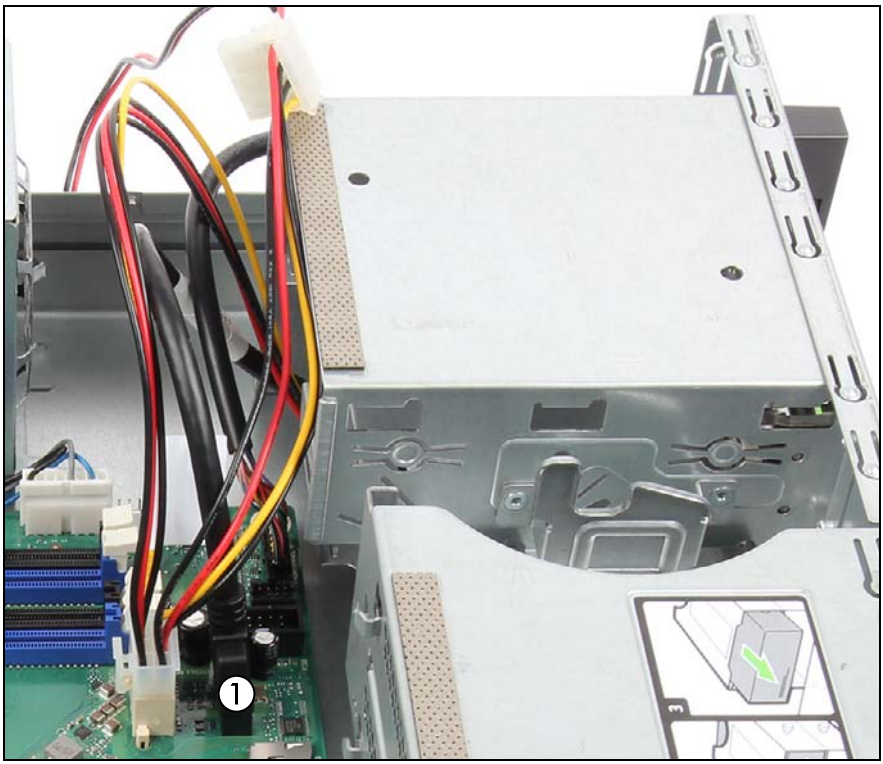

Figure 149: Connecting front USB connector cable

- Connect the front USB connector cable end to the connector "Front USBI" on the system board (1).
- If applicable, connect the FBU adapter cable to the TFM as described in section "Installing a TFM" on page 209.

13.2.1.5 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Updating RAID controller firmware" on page 87

13.2.2 Removing a Front USB connector

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

13.2.2.1 Preliminary steps

- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

13.2.2.2 Disconnecting the front USB connector

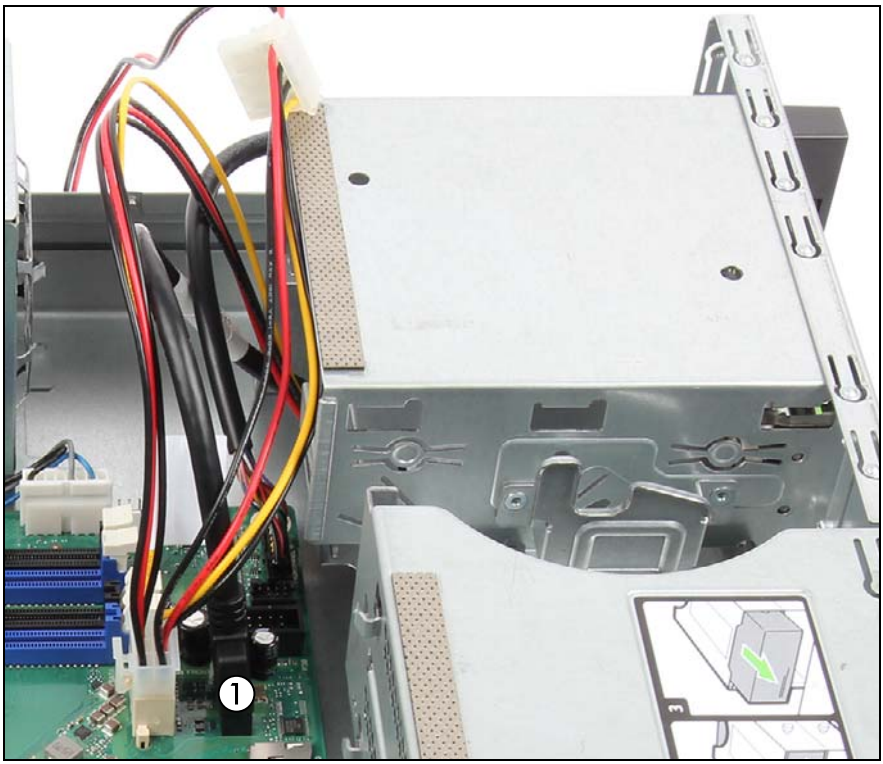

Figure 150: Disconnecting front USB connector cable

- ► Disconnect the cable end of the front USB connector (1).
- ► If applicable, disconnect the FBU adapter cable from the TFM as described in section "Removing the defective TFM" on page 207.

13.2.2.3 Removing the front USB connector from the holder

- ► Remove the holder as described in section "Removing the holder" on page 269.

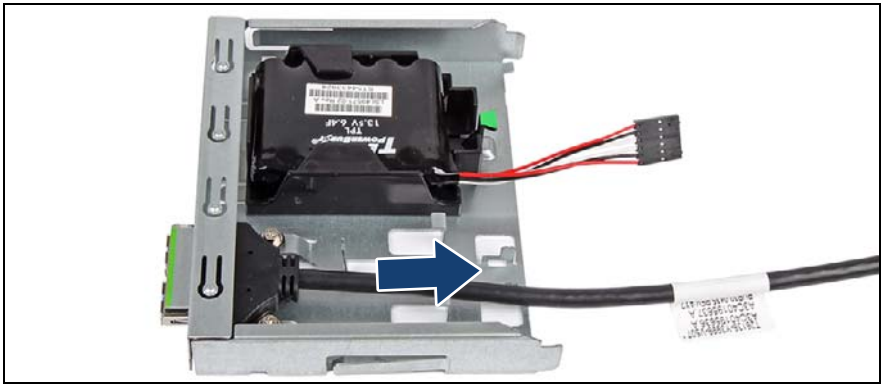

Figure 151: Removing the front USB connector

- ► Remove the two screws.
- ► Remove the front USB connector from the holder (see arrow).

13.2.2.4 Installing the holder

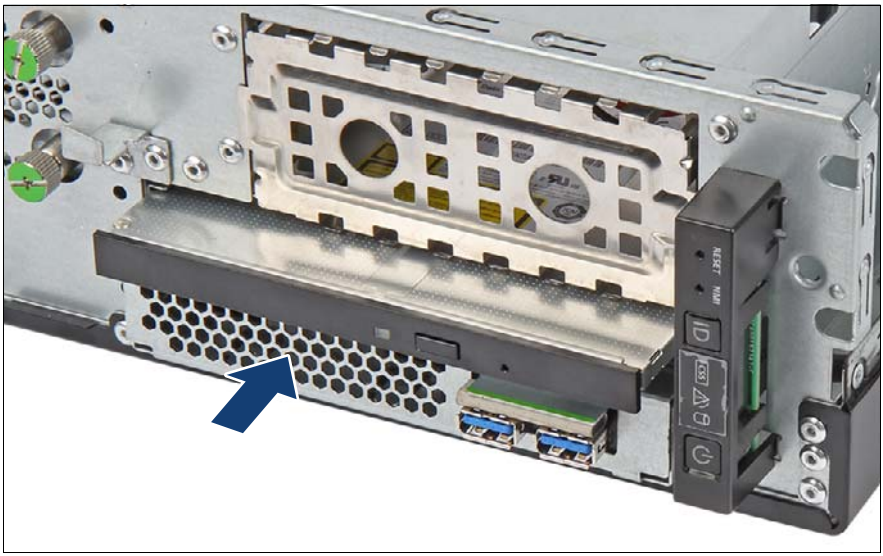

Figure 152: Installing the holder

- ► Insert the holder into the corresponding bay and slide it into the bay as far as it will go (see arrow).

- If applicable, connect the FBU adapter cable to the TFM as described in section "Installing a TFM" on page 209.

13.2.2.5 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69

13.2.3 Replacing a front USB connector

 **Upgrade and Repair Unit (URU)**

 **Hardware: 10 minutes**

Tools: Phillips PH2 / (+) No. 2 screw driver

13.2.3.1 Preliminary steps

- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

13.2.3.2 Removing the front USB connector

- Disconnect the cable end of the front USB connector as described in section "Disconnecting the front USB connector" on page 273.
- Remove the front USB connector as described in section "Removing the front USB connector from the holder" on page 273.

13.2.3.3 Installing the new front USB connector

- Install the front USB connector as described in section "Installing the front USB connector" on page 270.C

- Connect the front USB connector as described in section "Connecting the front USB connector" on page 271.

13.2.3.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Updating RAID controller firmware" on page 87

14 System board and components

Safety notes

CAUTION!

- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "Important information" on page 35.

14.1 Basic information

This section provides instructions for the system board and the following components:

- CMOS battery

  CMOS memory (volatile BIOS memory) and the real-time clock are powered by a lithium coin cell (CMOS battery). This cell lasts up to ten years, depending on ambient temperature and use.

  If the CMOS battery is depleted or falls below minimum voltage levels, it need to be replaced immediately.

- UFM (USB Flash Module)

  The server can be equipped with a USB Flash Module (UFM).

- TPM (Trusted Platform Module)

  The system board is optionally equipped with a Trusted Platform Module (TPM). This module enables programs from third party manufacturers to store key information, for example drive encryption using Windows Bitlocker Drive Encryption.

- SATA DOM (SATA Flash Module)

  With the Innodisk Serial ATA Disk on Module (SATADOM) an internal SSD is offered. This SSD can be configured as a boot device or data storage device.

- iRMC microSD card

  The iRMC microSD card is necessary for using the embedded Lifecycle Management (eLCM) functionality of the iRMC.

14.2 CMOS battery

14.2.1 Replacing the CMOS battery

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less; recommended: tooth pick

Safety notes

CAUTION!

- The CMOS battery must be replaced with an identical battery or with a battery type recommended by the manufacturer.
- Keep lithium batteries away from children.
- Do not throw batteries into the trash can. Lithium batteries must be disposed of in accordance with local regulations concerning special waste.
- For further safety information, please refer to section "Environmental protection" in the operating manual of your server.
- **Ensure to insert the CMOS battery the with the positive pole facing up!**

14.2.1.1 Preliminary steps

- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

14.2.1.2 Replacing the defective CMOS battery

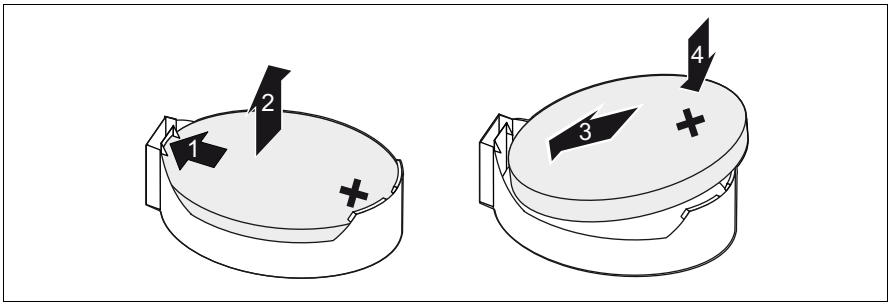

Figure 153: Replacing the CMOS battery

- Press the locking spring into direction of the arrow (1), so that the CMOS battery jumps out of its socket.
- Remove the CMOS battery (2).

CAUTION!

Sharp tools such as screw drivers might damage system board components in case of slipping.

If the CMOS battery cannot be ejected without the help of a tool, it is recommended to use a tooth pick.

- Insert a new CMOS battery of the same type into the socket (3) and (4).

14.2.1.3 Concluding steps

- Dispose of the CMOS battery in accordance with local regulations concerning special waste.
- "Reassembling" on page 61
- "Connecting the power cord" on page 64

- "Switching on the server" on page 69
- "Verifying system information backup / restore" on page 86
- "Verifying the system time settings" on page 98

14.3 USB Flash Module (UFM)

14.3.1 Installing the UFM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

14.3.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

14.3.1.2 Installing the UFM

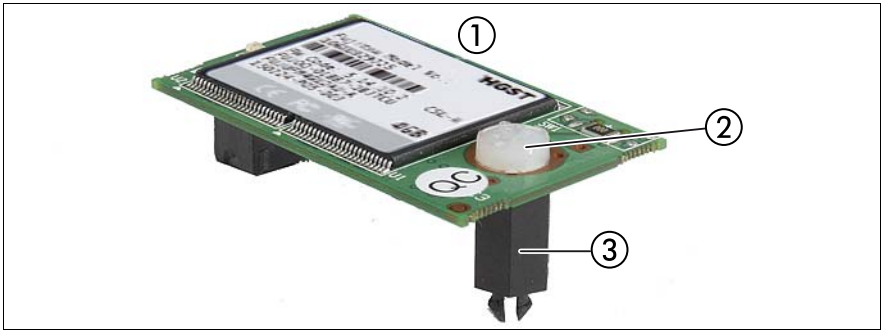

Figure 154: UFM kit

1	USB Flash Module (UFM)	2	UFM spacer
3	UFM nylon screw		

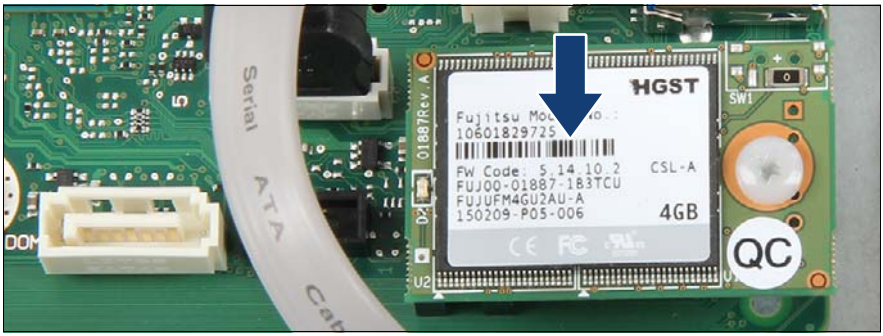

Figure 155: Installing the UFM

The onboard position of the UFM connector can be found in section "Connectors and indicators" on page 337.

- Remove the HDD fan module(s) as described in section "Removing the HDD fan module" on page 175.
- Connect the UFM to the system board. The UFM spacer must click into the hole on the system board.
- Install the HDD fan module(s) as described in section "Installing the HDD fan module" on page 179.

14.3.1.3 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

14.3.1.4 Software configuration

In order to install the ESXi to the USB Flash Module (UFM), the VMware ESXi installer CD is required.To obtain the ESXi installer CD by purchasing the OEM Media Kit, or downloading the ESXi Custom Image ISO file from VMware's website and burn the image to the CD.
https://www.vmware.com/go/download-vsphere.

To Install the ESXi to the USB Flash Module (UFM) by following the steps below:

- Disconnect all storage devices from the server beside the USB Flash Module (UFM).
- Power on the server. Once the server has been started, then enter the BIOS setup menu and select the DVD drive as primary boot device.
- Insert the CD into the DVD drive and reboot the server. The sever will boot from the installer CD.
- Follow the on-screen instructions to install the ESXi. When the installation is complete, you will be asked to reboot the server.
- While the server is rebooting, enter the BIOS setup menu again and select the USB Flash Module (UFM) as primary boot device.

The installation of the ESXi to the USB Flash Module (UFM) is complete.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

For Japan
In order to setup the ESXi, please refer to the corresponding version of the "VMware vSphere Software Description" from the following URL and reinstall ESXi to the USB Flash Module.
http://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

14.3.2 Removing the UFM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: – Phillips PH1 / (+) No. 1 screw driver

14.3.2.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

14.3.2.2 Removing the UFM

Figure 156: Removing the UFM

- Remove the HDD fan module(s) as described in section "Removing the HDD fan module" on page 175.
- Remove the nylon screw of the UFM (1).
- Disconnect and remove the UFM (2).

The UFM spacer remains on the system board.

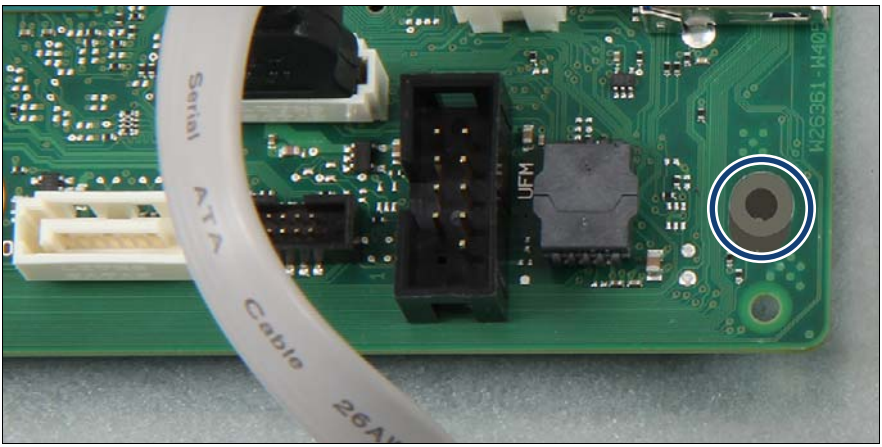

Figure 157: Remaining UFM spacer

CAUTION!

UFM contains customer information (e.g. IP address, License etc.). After removing the UFM, you must pass the UFM to the customer.

- Install the HDD fan module(s) as described in section "Installing the HDD fan module" on page 179

14.3.2.3 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

14.3.3 Replacing the UFM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools:	– Phillips PH1 / (+) No. 1 screw driver – combination pliers and flat nose pliers

14.3.3.1 Preliminary steps

- ► "Suspending BitLocker functionality" on page 75
- ► "Locating the defective server" on page 49
- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► "Getting access to the component" on page 55

14.3.3.2 Removing the defective UFM

- ► Remove the UFM as described in section "Removing the UFM" on page 283.
- ► The UFM spacer remains on the system board.

CAUTION!

UFM contains customer information (e.g. IP address, License etc.). After replacing the UFM, you must pass the defective UFM to the customer, and ask for disposal. If the disposal of the defective UFM is requested by the customer, you break it according to the following procedure, and dispose it.

Figure 158: Tools for breaking the UFM

Figure 159: UFM breaking method

► Use a long nose pliers and a combination pliers to break the UFM in half as shown in the figure.

14.3.3.3 Installing the new UFM

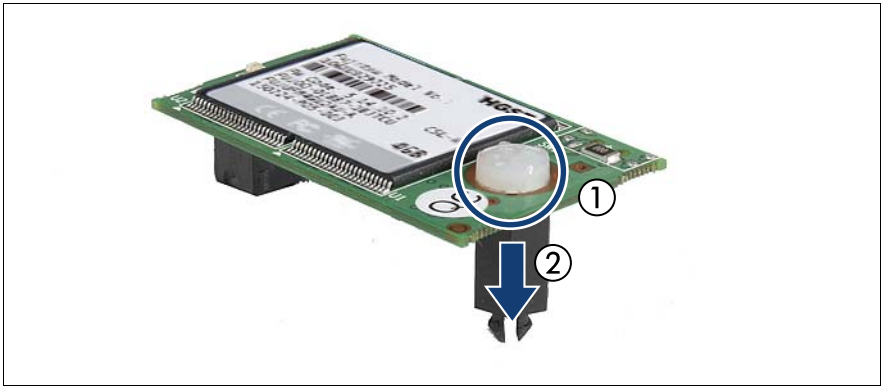

Figure 160: Preparing the new UFM

- ► Remove the nylon screw from the new UFM (1).
- ► Remove the UFM spacer (2).

Figure 161: Installing the UFM

- ► Connect the UFM to the system board and the remaining UFM spacer (1).
- ► Fasten the UFM to the UFM spacer with the nylon screw (2).
- ► Install the HDD fan module(s) as described in section "Installing the HDD fan module" on page 179

14.3.3.4 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

14.3.3.5 Software configuration

To install the ESXi to the USB Flash Module (UFM) refer to "Software configuration" on page 282.

14.4 Trusted Platform Module (TPM)

14.4.1 Installing the TPM

Field Replaceable Unit (FRU)

Hardware: 5 minutes
Software: 5 minutes

Tools:
- Bit screw driver
- TPM bit insert (*)

(*) For Japan:

- TPM module fixing tool (S26361-F3552-L909)

14.4.1.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

14.4.1.2 Installing the TPM

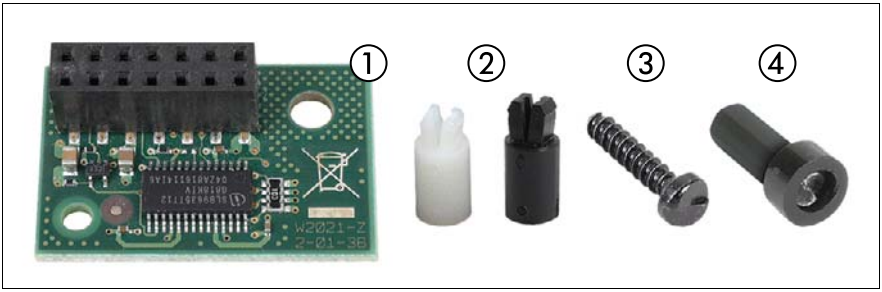

Figure 162: TPM kit

1	TPM (Trusted Platform Module)	3	Special screw for TPM
2	TPM spacer The black TPM spacer is not used in this server.	4	TPM bit insert for TPM special screw

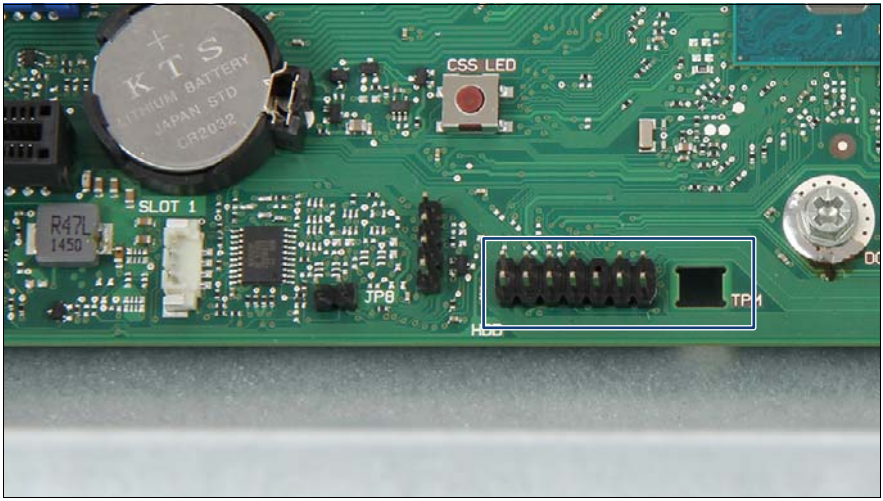

Figure 163: Position on the system board

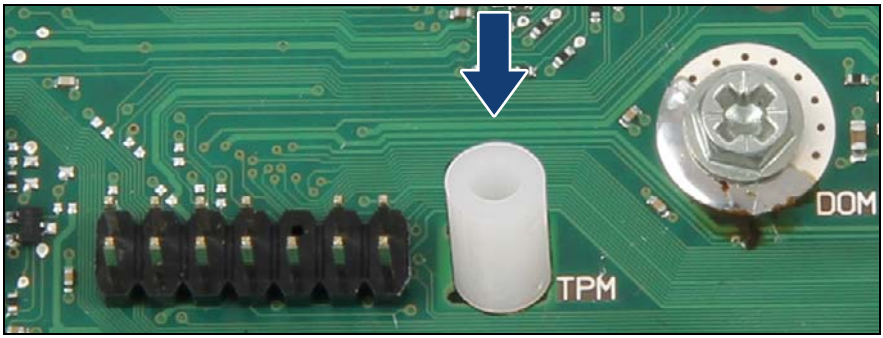

Figure 164: Inserting the TPM spacer on the system board

► Snap the TPM spacer into the cut-out in the system board.

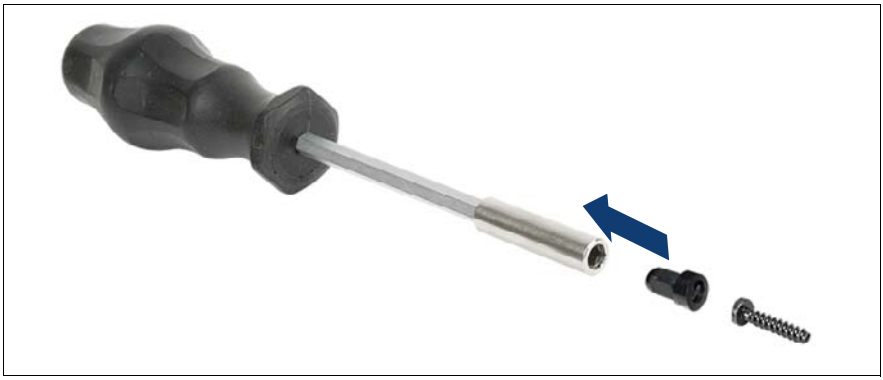

Figure 165: TPM bit insert

► Attach the TPM bit insert or TPM module fixing tool (for Japan) to a bit screw driver.

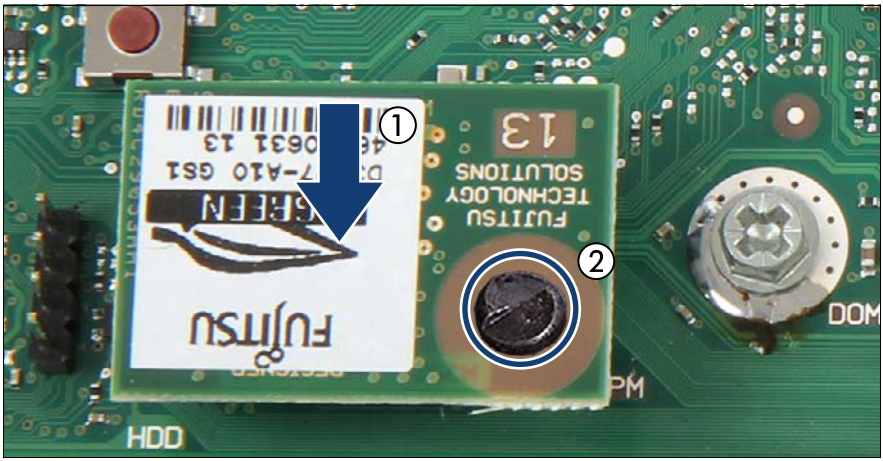

Figure 166: Installing the TPM

- Connect the TPM to the system board (1).
- Fasten the TPM with the special screw for the TPM using the TPM bit insert or TPM module fixing tool (for Japan) (2).

CAUTION!

Do not fasten the screw too firmly. Stop it by extent where the head of the screw lightly touches the TPM (torque value of 0.6 Nm).

14.4.1.3 Concluding steps

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102
- Enable TPM in the system board BIOS. Proceed as follows:
  - Switch on or restart your server.
  - As soon as the startup screen appears, press the F2 function key to enter the BIOS.
  - Select the *Advanced* menu.
  - Select the *Trusted Computing* submenu.

- ► Set the *TPM Support* and *TPM State* settings to *Enabled*.
- ► Under *Pending TPM operation*, select the desired TPM operation mode.
- ► Save your changes and exit the BIOS.

For more information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

14.4.2 Removing the TPM

Field Replaceable Unit (FRU)

Hardware: 30 minutes

Tools: Removing the system board:

– Phillips PH2 / (+) No. 2 screw driver

Removing the TPM:

– Bit screw driver
– flat nose pliers
– TPM bit insert (*)

(*) For Japan:

– TPM module fixing tool (S26361-F3552-L909)

CAUTION!

Advise your contact persons that they must provide you with all recovery keys which belong to the system to restore them in the TPM later.

14.4.2.1 Preliminary steps

- ► Before removing the TPM, it is necessary to remove BitLocker-protection from the computer and to decrypt the volume.
  Ask the system administrator to turn off BitLocker-protection using the BitLocker setup wizard available either from the Control Panel or Windows Explorer:
  - ► Open Bitlocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *Bitlocker Drive Encryption*.

Administrator permission required: If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

- To turn off BitLocker and decrypt the volume, click *Turn Off BitLocker*, and then click *Decrypt the volume*.

Decrypting the volume may be time-consuming. By decrypting the volume, all of the information stored on that computer is decrypted.

For further information on how to disable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Please refer to the Fujitsu web pages for more details.

- Disable TPM in the system board BIOS. Proceed as follows:
  - Switch on or restart your server.
  - As soon as the startup screen appears, press the F2 function key to enter the BIOS.
  - Select the *Advanced* menu.
  - Select the *Trusted Computing* submenu.
  - Set the *TPM Support* and *TPM State* settings to *Disabled*.
  - Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

- "Locating the defective server" on page 49
- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55

14.4.2.2 Removing the TPM

- Remove the system board as described in section "Removing the system board" on page 310.

► Lay the system board on a soft, antistatic surface with its component side facing down.

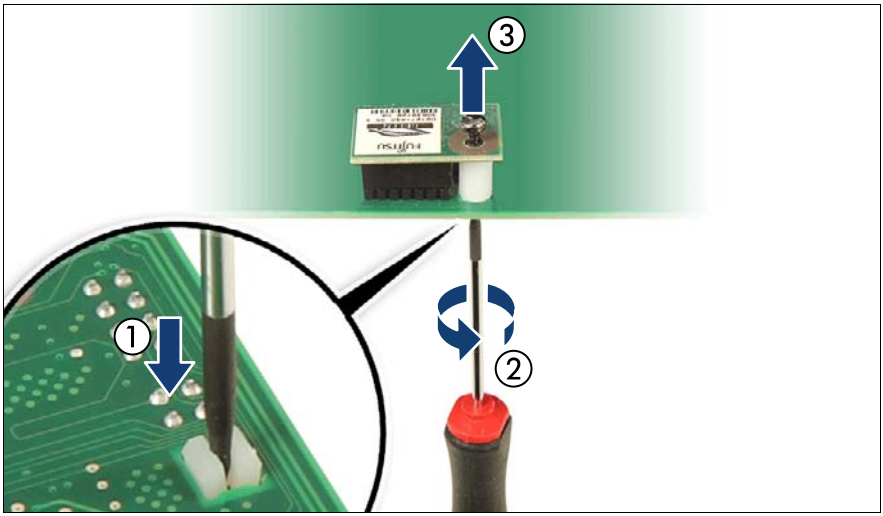

Figure 167: Removing the TPM screw

► Locate the slotted lower end of the TPM screw (1).

► Carefully loosen the TPM screw using a thin slotted screw driver (e.g. watchmaker's screw driver) or the dedicated TPM screw driver (for Japan) (2).

CAUTION!

Ensure to turn the screw **clockwise** in order to remove it!

Slowly and carefully increase the pressure on the screw until it begins to turn. The effort when loosing the screw should be as low as possible.

Otherwise the thin metal bar may break, rendering it impossible to loosen the screw.

► Remove the TPM screw (3).

► Remove the TPM on the upper side of the system board.

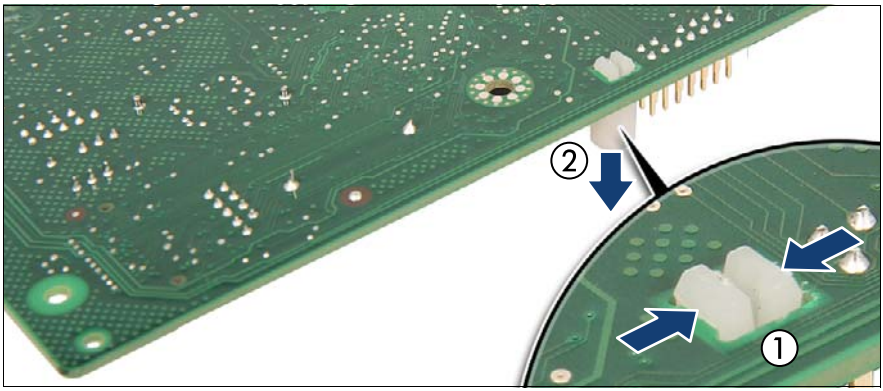

Figure 168: Removing the TPM spacer

► Using a flat nose pliers, press together the hooks on the TPM spacer (1, see close-up) and remove it from the system board (2).

If the TPM is to be replaced, the TPM spacer may remain on the system board.

14.4.2.3 Concluding steps

► "Installing the system board" on page 313

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

14.4.3 Replacing the TPM

Field Replaceable Unit (FRU)

Hardware: 40 minutes

Tools: Removing the system board:

- Phillips PH2 / (+) No. 2 screw driver

Replacing the TPM:

- Bit screw driver
- TPM bit insert (*)
- flat nose pliers
- thin slotted screw driver (2 x 0.4 mm) (*)

(*) For Japan:

- Dedicated TPM screw driver (CWZ8291A)
- TPM module fixing tool (S26361-F3552-L909)

CAUTION!

Advise your contact persons that they must provide you with all recovery keys which belong to the system to restore them in the TPM later.

14.4.3.1 Preliminary steps

- "Suspending BitLocker functionality" on page 75
- "Locating the defective server" on page 49
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175

14.4.3.2 Removing the defective TPM

- ► Remove the TPM as described in section "Removing the TPM" on page 292.
- ► Leave the TPM spacer on the system board when removing the defective TPM.

14.4.3.3 Installing the new TPM

The TPM spacer is already present on the system board.

- ► Install the TPM as described in section "Installing the TPM" on page 288

14.4.3.4 Concluding steps

- ► "Installing the HDD fan module" on page 179
- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69
- ► "Resuming BitLocker functionality" on page 102

You can find information on configuring the TPM in the corresponding BIOS Setup Utility reference manual.

14.5 SATA DOM

14.5.1 Installing the SATA DOM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

14.5.1.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175

14.5.1.2 Installing the SATA DOM

Figure 169: SATA DOM

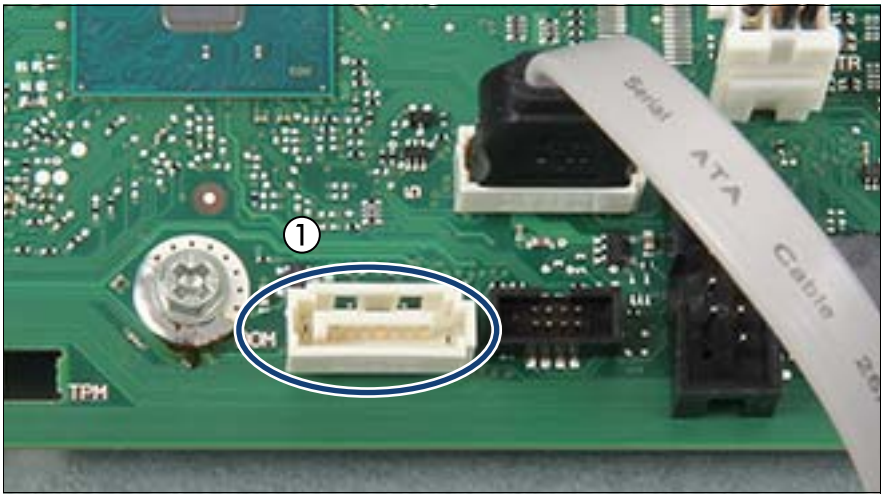

Figure 170: Position SATA DOM

1	Position for the SATA DOM

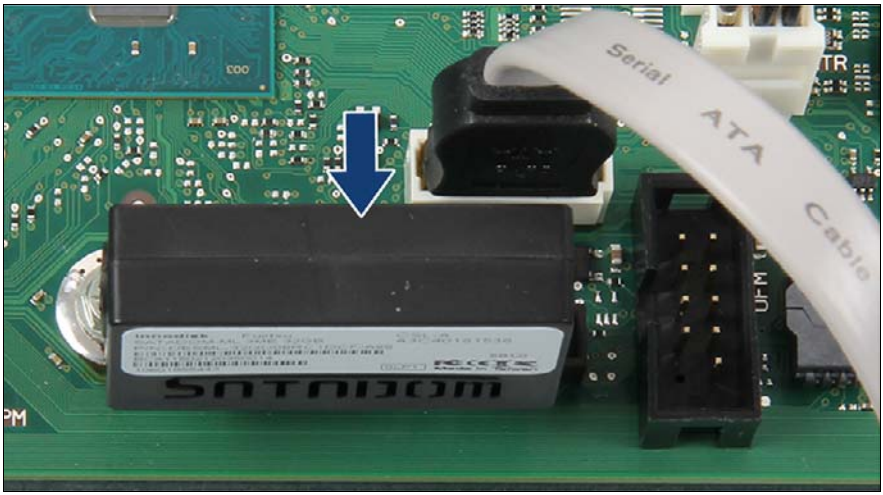

Figure 171: Installing the SATA DOM

► Connect the SATA DOM to the connector "DOM" on the system board.

The onboard position of the SATA DOM slot can be found in section "Connectors and indicators" on page 337.

14.5.1.3 Concluding steps

► "Installing the HDD fan module" on page 179
► "Reassembling" on page 61
► "Connecting the power cord" on page 64
► "Switching on the server" on page 69

14.5.2 Removing the SATA DOM

Upgrade and Repair Units (URU)

Hardware: 5 minutes

Tools: tool-less

14.5.2.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175

14.5.2.2 Removing the SATA DOM

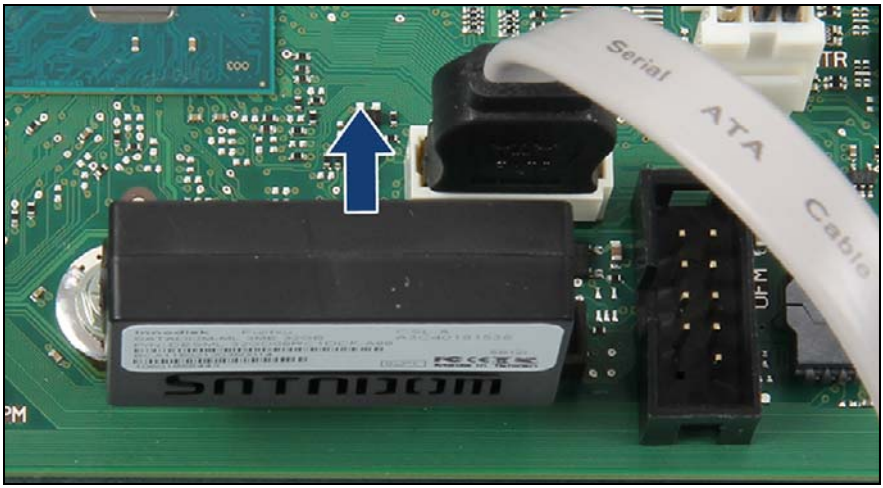

Figure 172: Removing the SATA DOM

- Remove the HDD fan module(s) as described in section "Removing the HDD fan module" on page 175.
- Firmly remove the SATA DOM out of its connector.

- Install the HDD fan module(s) as described in section "Installing the HDD fan module" on page 179.

14.5.2.3 Concluding steps

- "Installing the HDD fan module" on page 179
- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69

14.5.3 Replacing the SATA DOM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

14.5.3.1 Preliminary steps

- "Locating the defective server" on page 49
- "Suspending BitLocker functionality" on page 75
- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the HDD fan module" on page 175

14.5.3.2 Replacing the SATA DOM

- Remove the defective SATA DOM as described in section "Removing the SATA DOM" on page 301.
- Install the new SATA DOM as described in section "Installing the SATA DOM" on page 298.

14.5.3.3 Concluding steps

- "Installing the HDD fan module" on page 179
- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69
- "Resuming BitLocker functionality" on page 102

14.6 iRMC microSD card

The iRMC microSD card is necessary for using the embedded Lifecycle Management (eLCM) functionality of the iRMC. It requires a valid eLCM license key, which is always purchased together with the iRMC microSD card and activated through the iRMC web frontend.

For further information, please refer to the “ServerView embedded Lifecycle Management (eLCM)” user guide.

14.6.1 Installing the iRMC microSD card

Field Replaceable Unit (FRU)

Hardware: 40 minutes

Tools: Tool-less

14.6.1.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the system board" on page 310

14.6.1.2 Installing the iRMC microSD card

- Remove the system board as described in section "Removing the system board" on page 310.

Figure 173: iRMC microSD card

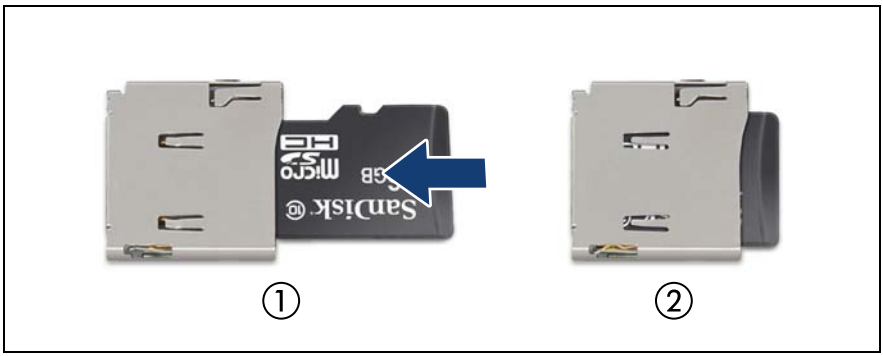

Figure 174: Installing the iRMC microSD card

- With the label facing up, insert the iRMC microSD card into the microSD card slot (1) as far as it will go (2).

  The onboard position of the microSD card slot can be found in section "Connectors and indicators" on page 337.

- Install the system board as described in section "Installing the system board" on page 313.

14.6.1.3 Concluding steps

- "Installing the system board" on page 313

- "Reassembling" on page 61
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69

14.6.2 Removing the iRMC microSD card

Field Replaceable Unit (FRU)

Hardware: 40 minutes

Tools: Side-cutting pliers

14.6.2.1 Preliminary steps

- "Shutting down the server" on page 52
- "Disconnecting the power cord" on page 53
- "Getting access to the component" on page 55
- "Removing the system board" on page 310

14.6.2.2 Removing the iRMC microSD card

- Remove the system board as described in section "Removing the system board" on page 310.

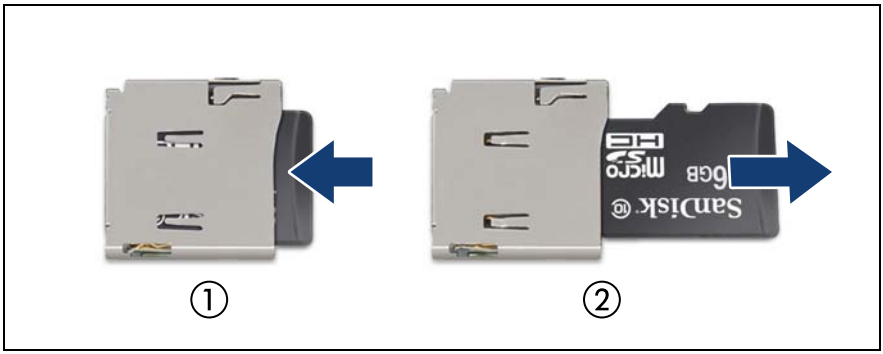

Figure 175: Removing the iRMC microSD card

- ► To eject the iRMC microSD card, gently push it in and then let go (1).
- ► Pull the iRMC microSD card straight out of its slot (2).

CAUTION!

The iRMC microSD card contains customer information. After replacing the iRMC microSD card, hand the defective card over to the customer.

- ► Install the system board as described in section "Installing the system board" on page 313.

14.6.2.3 Concluding steps

- ► "Installing the system board" on page 313
- ► "Reassembling" on page 61
- ► "Connecting the power cord" on page 64
- ► "Switching on the server" on page 69

14.6.3 Replacing the iRMC microSD card

Field Replaceable Unit (FRU)

Hardware: 40 minutes

Tools: Side-cutting pliers

14.6.3.1 Preliminary steps

- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► "Getting access to the component" on page 55
- ► "Removing the system board" on page 310

14.6.3.2 Replacing the iRMC microSD card

- ► Remove the system board as described in section "Removing the system board" on page 310.

► Remove the defective iRMC microSD card as described in section "Removing the iRMC microSD card" on page 305.

CAUTION!

The iRMC microSD card contains customer information. After replacing the iRMC microSD card, hand the defective card over to the customer. If the customer requests disposal of the defective iRMC microSD card, proceed as follows:

► Using a pair of side-cutting pliers, cut the iRMC microSD card in half.

– Install the new iRMC microSD card as described in section "Installing the iRMC microSD card" on page 303

– Install the system board as described in section "Installing the system board" on page 313.

14.6.3.3 Concluding steps

► "Installing the system board" on page 313

► "Reassembling" on page 61

► "Connecting the power cord" on page 64

► "Switching on the server" on page 69

14.7 System board

14.7.1 Replacing the system board

Field Replaceable Unit (FRU)

Hardware: 50 minutes
Software: 10 minutes

Tools: Replacing the system board:
- Phillips PH2 / (+) No. 2 screw driver
- Magnifying glass for inspecting CPU socket springs (recommended)

Replacing the TPM:
- Bit screw driver
- flat nose pliers
- TPM bit insert (*)
- thin slotted screw driver (2 x 0.4 mm) (*)

(*) For Japan:

- Dedicated TPM screw driver (CWZ8291A)
- TPM module fixing tool (S26361-F3552-L909)

If a UFM is installed:

- Phillips PH1 / (+) No. 1 screw driver

Note on TPM

The system board can be equipped with an optional TPM (Trusted Platform Module). This module enables third party programs to store key information (e. g. drive encryption using Windows Bitlocker Drive Encryption).

If the customer is using TPM functionality, the TPM has to be removed from the defective system board and connected to the new system board. For a detailed description, please refer to section "Replacing the TPM" on page 296.

The TPM has to be enabled in the system BIOS.

CAUTION!

– Before replacing the system board, ask the customer whether TPM functionality is used.

– If the customer is using TPM functionality, remove the TPM from the old system board and install it on the new system board.

  Advise your contact persons that they must provide you with all recovery keys which belong to the system to restore them in the TPM later.

Note on system information backup / restore

The front panel module contains the Chassis ID EPROM that contains system information like server name and model, housing type, serial number and manufacturing data.

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

CAUTION!

For that reason the front panel and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

Note on network settings recovery

When replacing network controllers or the system board, network configuration settings in the operating system will be lost and replaced by default values. This applies to all static IP address and LAN teaming configurations.

Ensure to note down your current network settings before replacing a network controller or the system board.

14.7.1.1 Preliminary steps

- ► "Locating the defective server" on page 49
- ► "Note on network settings recovery" on page 309
- ► "Suspending BitLocker functionality" on page 75

- ► "Shutting down the server" on page 52
- ► "Disconnecting the power cord" on page 53
- ► Disconnect all external cables.
- ► "Getting access to the component" on page 55
- ► Remove the corresponding HDD fan: "Fans" on page 173
- ► Remove the following components from the system board:
  - – Heat sink: see section "Removing the heat sink" on page 231

    Leave the CPU on the defective board for now.
  - – Memory modules: refer to section "Removing memory modules" on page 226

    Ensure to take note of the memory modules' mounting positions for reassembly.
  - – Expansion cards: refer to the section "Removing expansion cards" on page 202

    Ensure to take note of the controllers' mounting positions and cable connections for reassembly.
  - – UFM: refer to section "Removing the UFM" on page 283

    Remove the UFM spacer from the defective system board and fasten it to the UFM with the UFM screw.
  - – SATA DOM (if applicable): refer to section "Removing the SATA DOM" on page 301

14.7.1.2 Removing the system board

- ► Disconnect all cables from the system board.
- ► If applicable, remove all HDDs as described in section"Removing 2.5-inch HDD/SSD modules" on page 151.
- ► If applicable, remove the HDD cage as described in section "Removing the HDD cage" on page 70.
- ► If applicable, remove the RDX drive as described in section "Removing the RDX drive" on page 259.

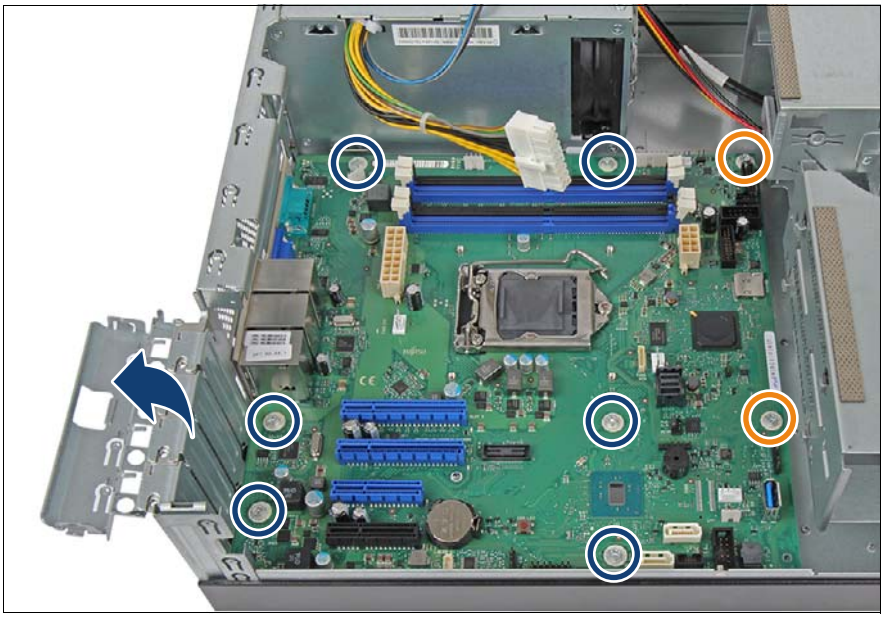

Figure 176: Screws system board

- ► Fold open the PCI slot bracket clamp (see arrow) to better reach the two screws in the bottom left corner.
- ► Remove the eight screws from the system board (see blue and orange circles, orange circles show the centering bolts).

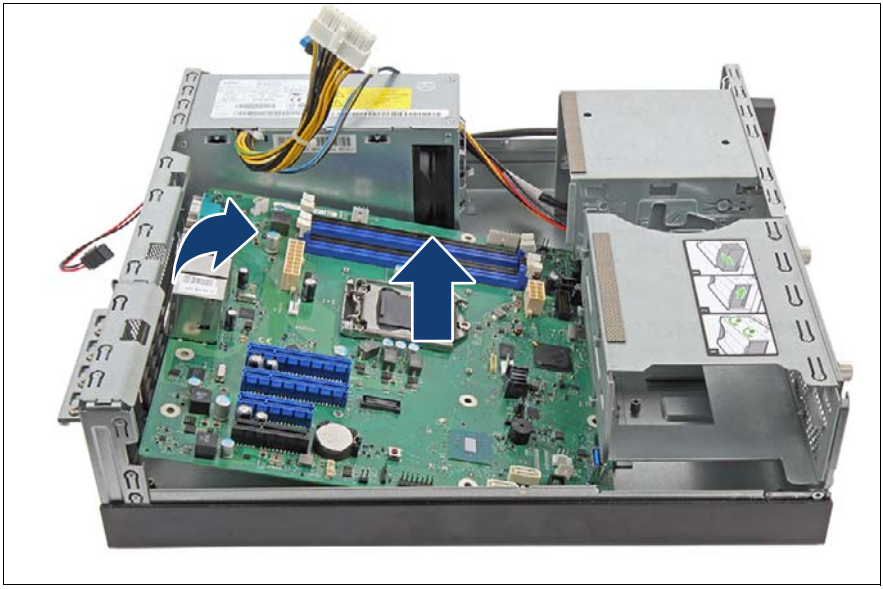

Figure 177: Removing the system board

► Use both hands to lift the system board carefully out of the chassis in a slight angle. Thereby you pull the connectors out of the connector panel (see arrows).

CAUTION!

Always take the system board with both hands!

Never lift the system board one-sided or at a heat sink, because the solder connections between the socket and the system board come under tension and increase the risk of damage and malfunction!

Don’t damage the EMI springs which are essential to comply with applicable EMC regulations and satisfy cooling requirements and fire protection measures.

► Place the removed and the new system board on an antistatic surface.

► If applicable, remove the TPM as described in section "Removing the TPM" on page 292.

► If applicable, remove the iRMC microSd card as described in section "Removing the iRMC microSD card" on page 305.

14.7.1.3 Installing the system board

- ► If applicable, install the iRMC microSd card as described in section "Installing the iRMC microSD card" on page 303.
- ► If applicable, install the TPM as described in section "Installing the TPM" on page 288.
- ► Check the settings on the new system board (see section "Onboard settings" on page 353).
- ► Insert the system board by holding it at a slight angle. Slide the connectors into the connector panel (see figure 177).
- ► Lower the system board carefully into the chassis.
- ► Adjust the system board. If necessary adjust the position of the system board with a gentle twisting motion (orange circles in figure 176 on page 311 show the centering bolts).
- ► Fasten the system board with the eight screws (see figure 176).
- ► Remove the protective plastic cover from the CPU socket of the new system board
- ► Remove the CPU from the defective system board as described in section "Removing the CPU" on page 232.
- ► Confirm that the CPU model number printed on the top of the CPU fits with the requirements.
- ► Install the CPU on the new system board as described in section "Installing the CPU" on page 233.
- ► Fit it onto the socket of the defective system board which will be sent back to spares.

  Returned system boards without this cover probably have to be scrapped.

- ► If applicable, install the RDX drive as described in section "Installing the RDX drive" on page 254.
- ► If applicable, install the HDD cage as described in section "Installing the HDD cage" on page 72.
- ► If applicable, install all HDDs as described in section"Installing 2.5-inch HDD/SSD modules" on page 148.

14.7.1.4 Concluding steps

- Connect all cables to the system board. For the cable plans see section "Cabling" on page 319.
- Reinstall all remaining system board components as shown in the related sections:
  - SATA DOM (if applicable): refer to section "Installing the SATA DOM" on page 298
  - UFM (if applicable): refer to section "Installing the UFM" on page 280
  - Memory modules: refer to section "Installing a memory module" on page 225

    Make sure that you reinstall each memory module in the slot it was located before the replacement.
  - Heat sinks: refer to section "Installing the heat sink" on page 239
  - Expansion cards: refer to section "Expansion cards" on page 198

  Make sure that you reinstall each card in the slots it was located before the replacement.
- "Reassembling" on page 61
- Connect all external cables.
- "Connecting the power cord" on page 64
- "Switching on the server" on page 69

  When the system is powered on after a CPU has been replaced or upgraded, the Global Error indicator will start flashing with the error message `CPU has been changed`. This only indicates that the CPU configuration has been altered. There is no technical problem.

  In order to turn off the Global Error indicator, please proceed as follows:

  - Restart the system and wait for screen output to appear.
  - Press the F2 function key to enter the BIOS.
    If assigned, enter the BIOS password and press Enter.
  - In the *Save & Exit* menu, select *Save Changes and Exit* or *Save Changes and Reset*.
  - Ensure that the Global Error indicator has stopped flashing.

- "Verifying the system time settings" on page 98
- "Updating or recovering the system board BIOS and iRMC" on page 84
- If applicable, activate TPM functionality in the system BIOS under *Security* > *TPM (Security Chip) Setting* > *Security Chip*. For more information, refer to the corresponding BIOS Setup Utility reference manual.
- "Verifying system information backup / restore" on page 86
- If customer BIOS settings are not restored automatically, please change the settings manually (using the information collected during "preliminary steps"). If you couldn't determine the BIOS version, ask the customer to reconfigure all BIOS settings and the password.
- "Looking up changed MAC / WWN addresses" on page 103
- "Updating the NIC configuration file in a Linux and VMware environment" on page 100
- Connect all external cables.
- "Resuming BitLocker functionality" on page 102
- If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard).

  Configuration of network settings should be performed by the customer. For further information, please refer to section "Note on network settings recovery" on page 309.

- If applicable, restore LAN teaming configurations as described in section "After replacing the system board" on page 107

15 Cables

15.1 Overview cables

Ref.	Name	Number	Routing
C1	CBL_FRONTPANEL	T26139-Y4015-V303	CablingFrontpanel
C2	CBL_USB_360	T26139-Y3999-V507	CablingFrontpanel
C3	CBL SATA ODD	T26139-Y4028-V306	CablingAccDrives
C4	CBL_MoBo_DRV_Pw_35	T26139-Y4012-V505	CablingPower35inchHDD
C5	CBL_MoBo_DRV_Pw_25	T26139-Y4012-V504	CablingPower25inchHDD
C6			
C8			
C9			
C10	CBL_SAS30_300_SgTw	T26139-Y4040-V51	CablingData4/8x25inchSAS_HDD CablingData25inchSATA_HDD
C11	CBL_SAS30_SATA_350	T26139-Y4040-V43	CablingData35inchSATA_HDD CablingData35inchSATA_HDD_EP4
C12	CBL_OOB_HDD_2BP	T26139-Y4015-V608	CablingData4/8x25inchSAS_HDD CablingData25inchSATA_HDD
C20	CBL_PDB_MoBo_Pw	T26139-Y3952-V511	CablingRedundatPSU
C21	CBL_PDB_MoBo_Sig	T26139-Y3956-V4	CablingRedundatPSU
C23	CBL_USBA_TO_USBB	T26139-Y4039-A40	CablingAccDrives
C24	CBL_BBU	T26139-Y4031-V101	CablingData4/8x25inchSAS_HDD CablingData35inchSATA_HDD_EP4
C25	CBL_SATA_Ext_400	T26139-Y4028-V402	CablingOptionSATADOM
C26			

Figure 178: List of used cables

15.2 Connectors D3373

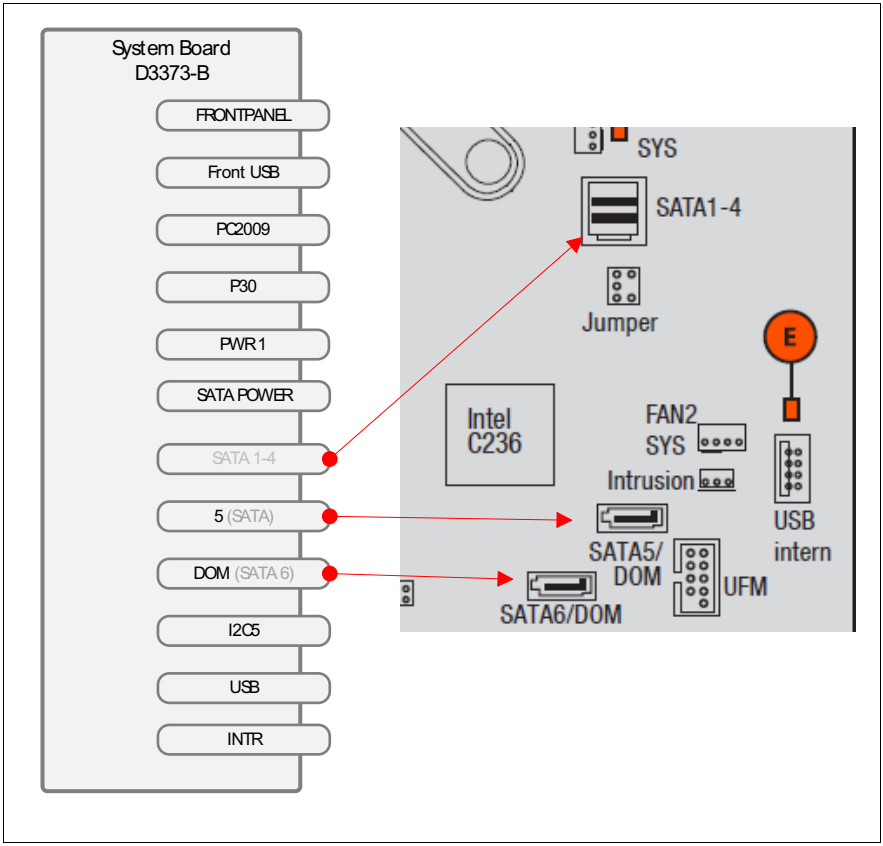

Figure 179: Connectors D3373

15.3 Cabling

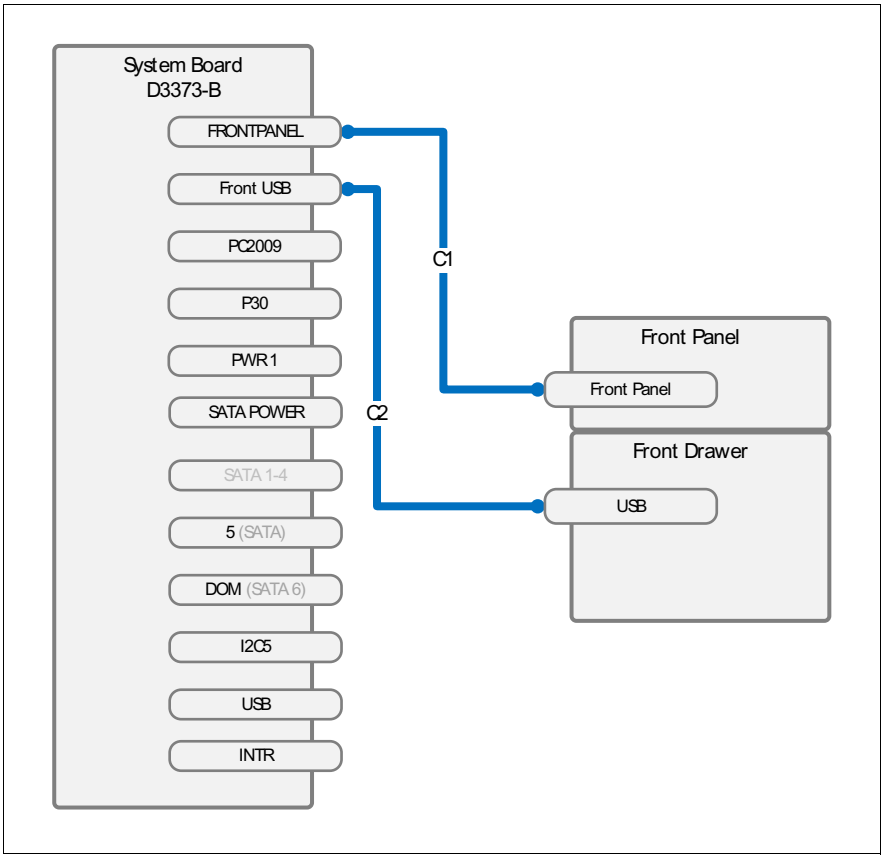

Figure 180: Cabling front panel

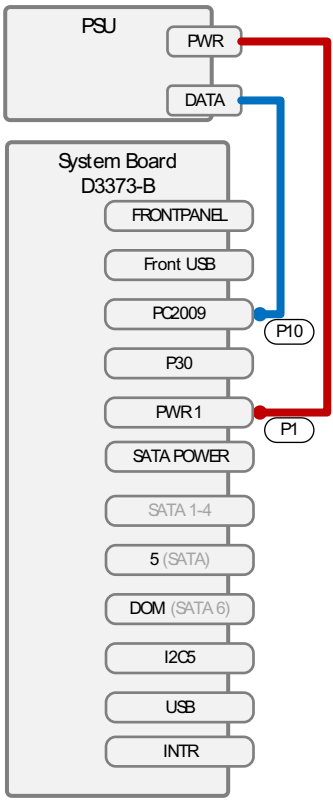

Figure 181: Cabling standard PSU

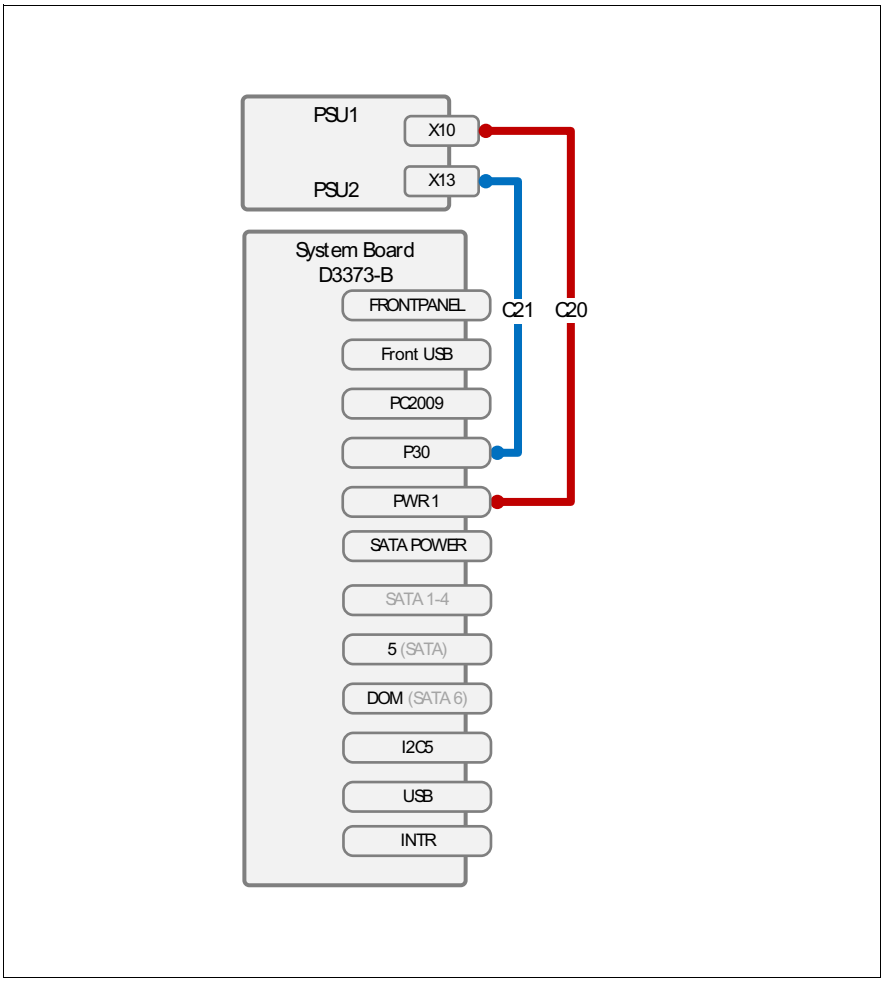

Figure 182: Cabling redundant PSU

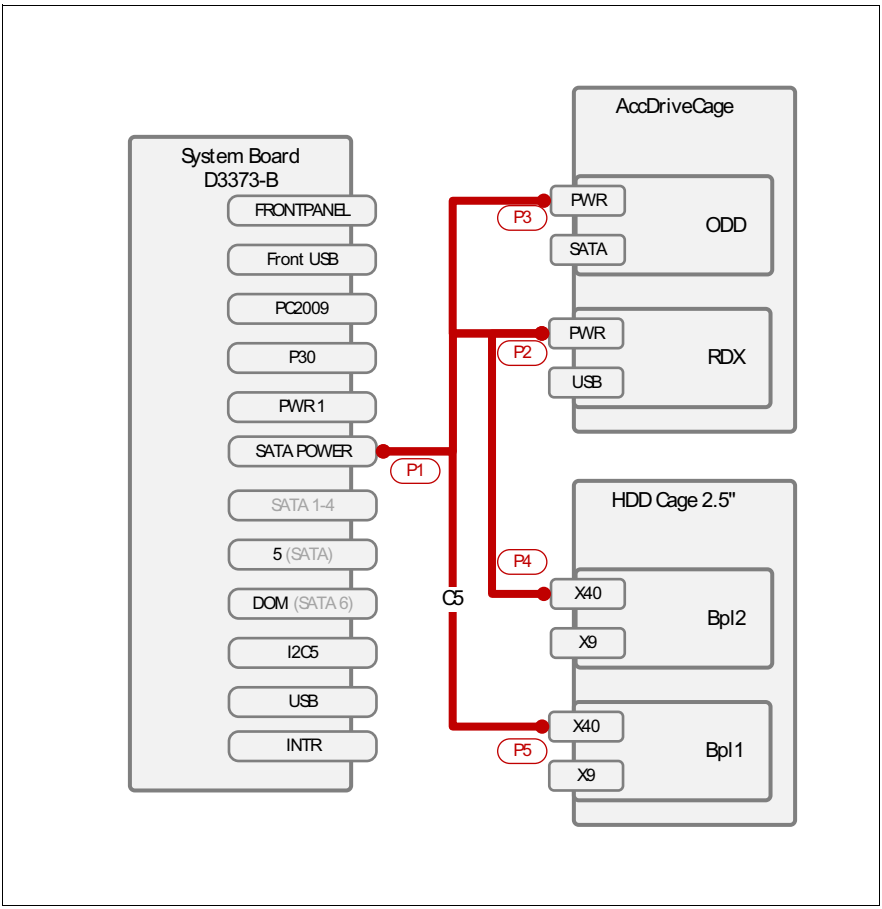

Figure 183: Cabling power 2.5-inch HDD

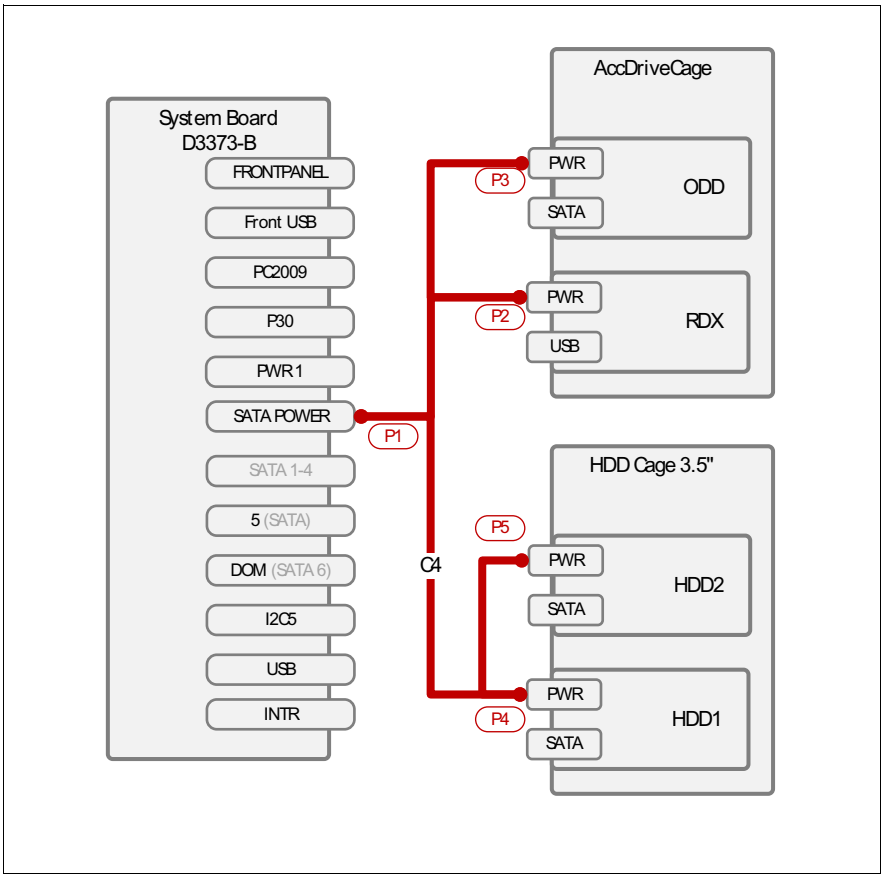

Figure 184: Cabling power 3.5-inch HDD

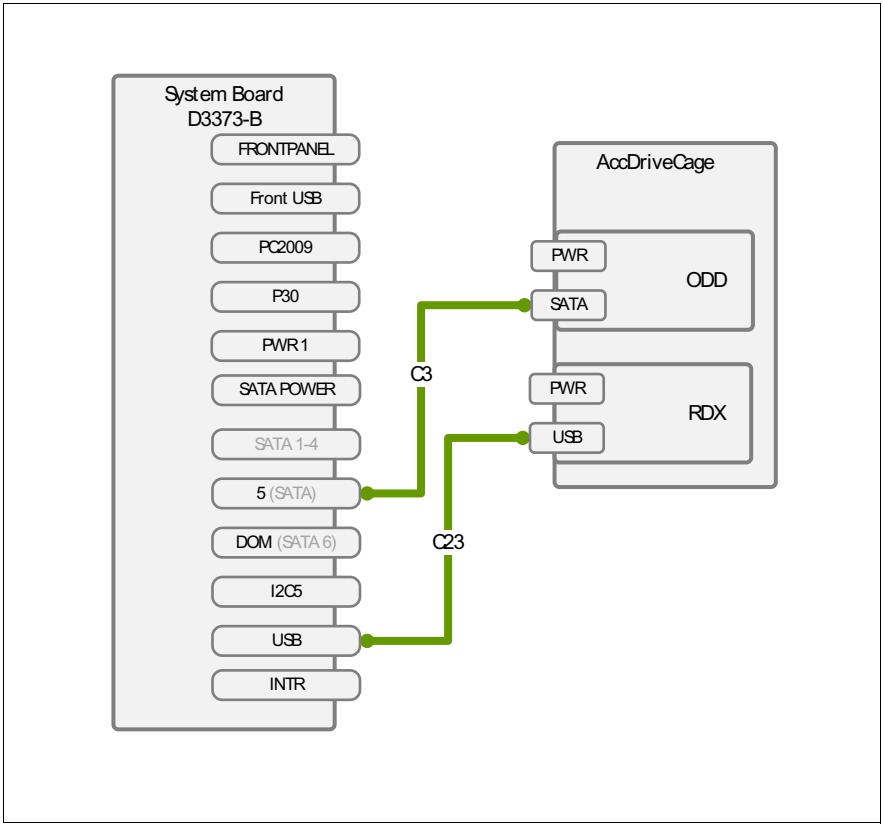

Figure 185: Cabling accessible drives

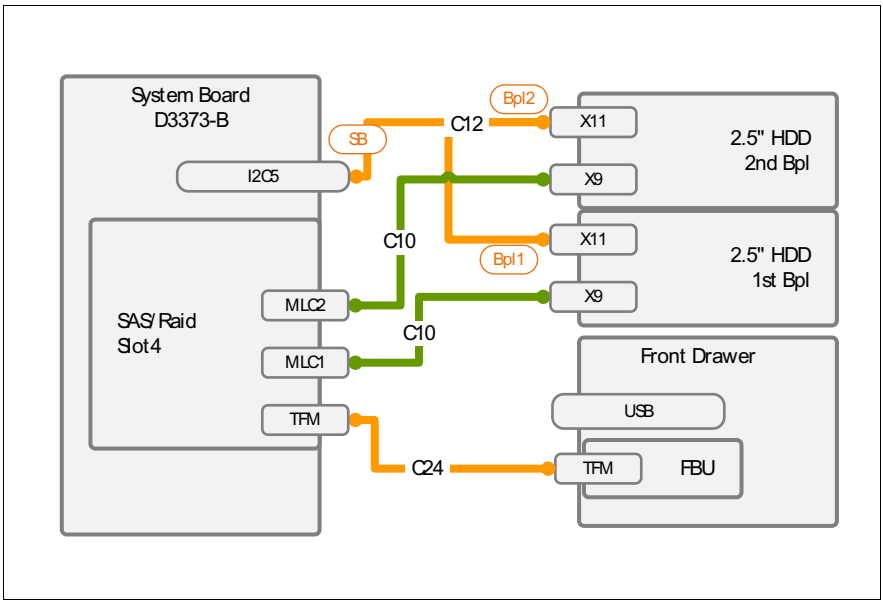

Figure 186: Cabling 4/8x 2.5-inch HDD wit SAS controller

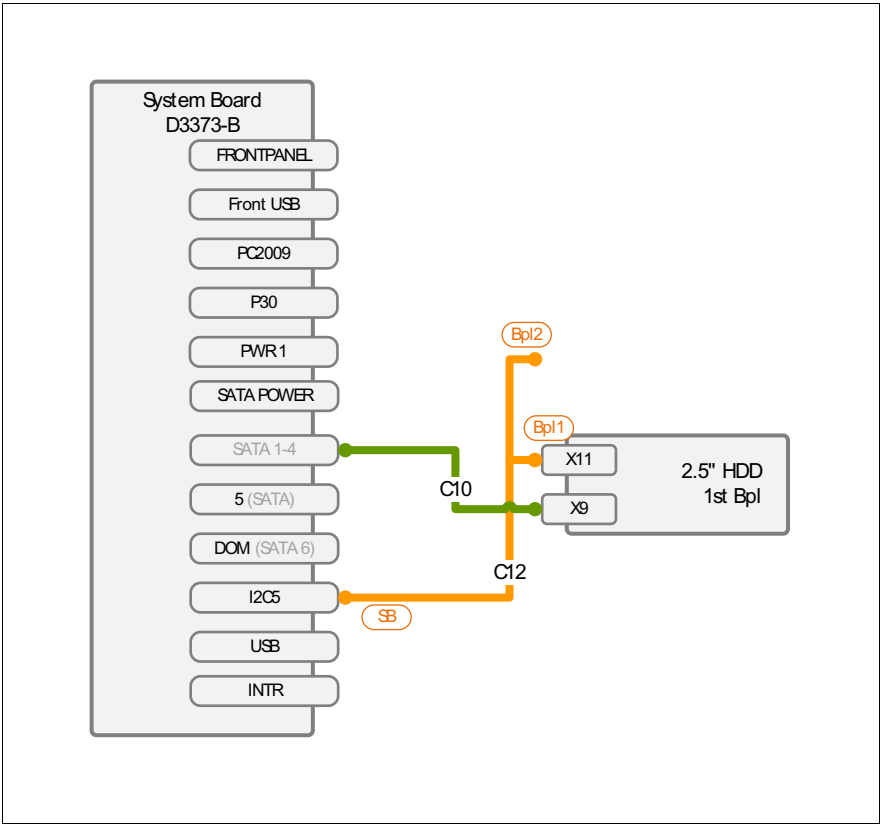

Figure 187: Cabling 2.5-inch HDD

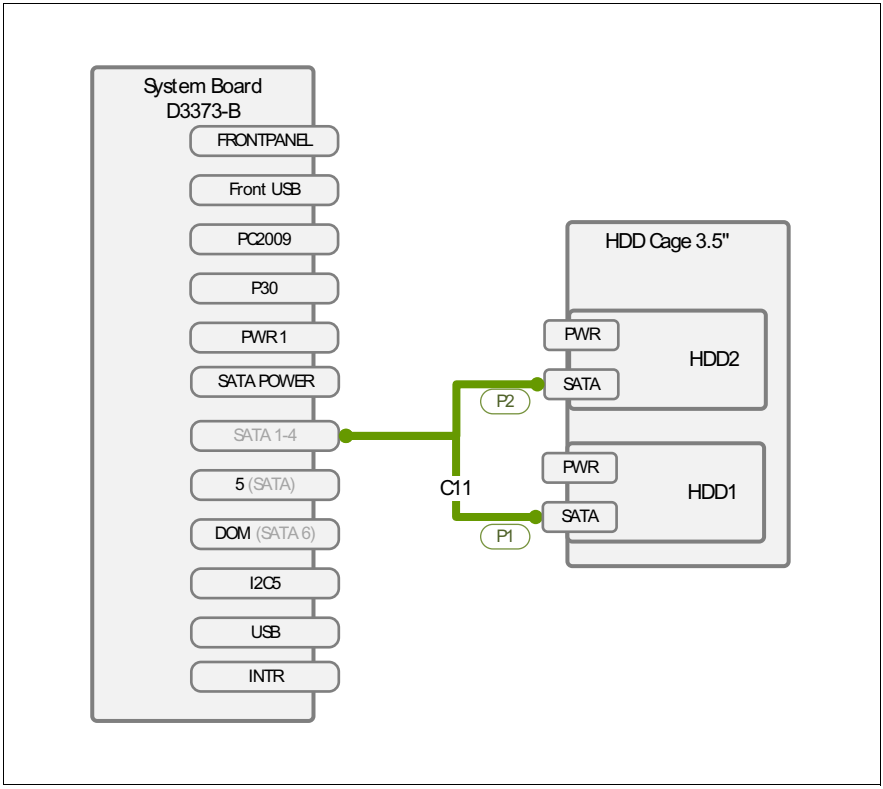

Figure 188: Cabling 3.5-inch HDD

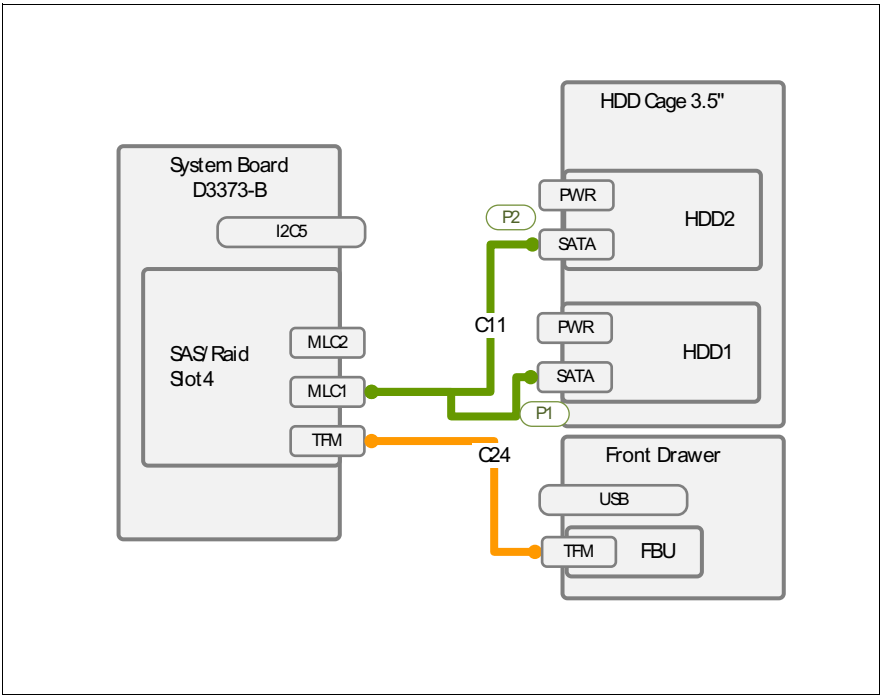

Figure 189: Cabling 3.5-inch HDD EP4

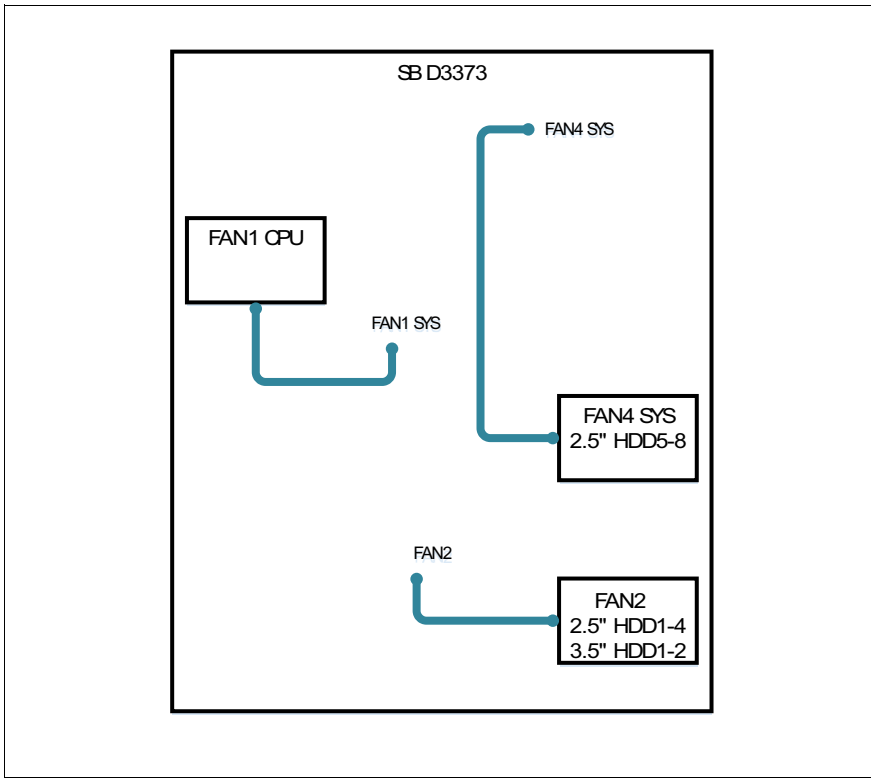

Figure 190: Cabling system fans

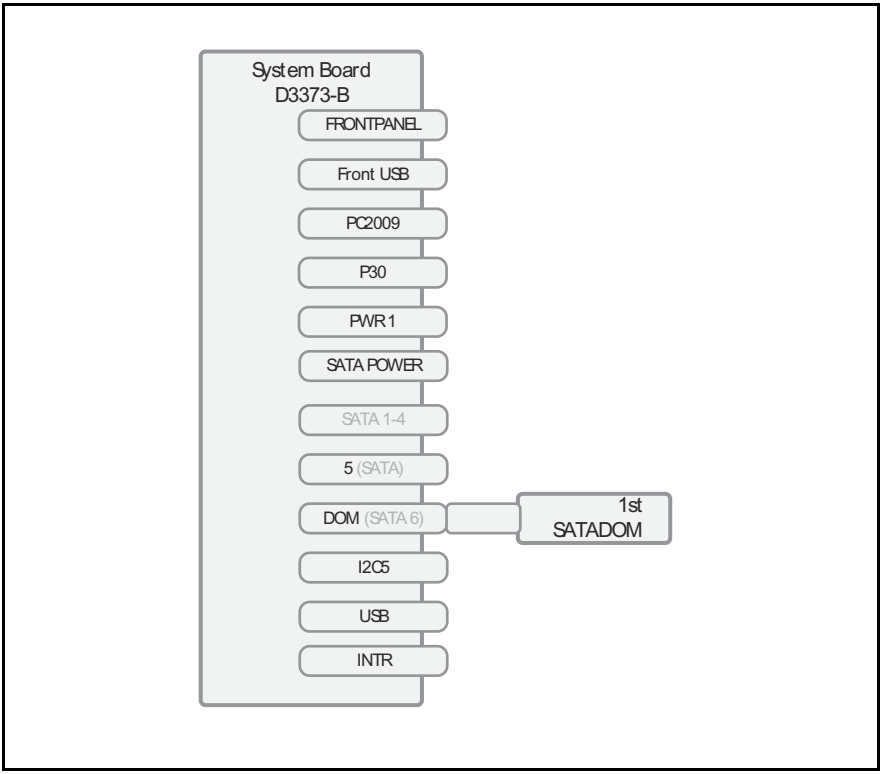

Figure 191: Cabling SATA DOM (option)

16 Appendix

16.1 Mechanical overview

16.1.1 Server front

2.5-inch HDD model

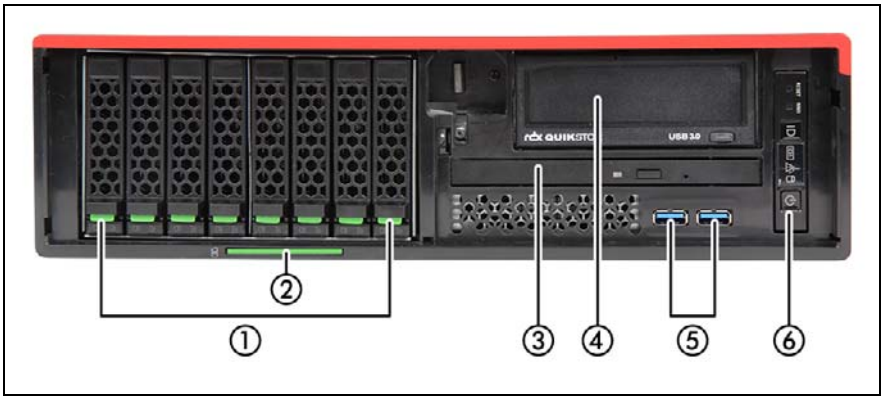

Figure 192: PRIMERGY TX1320 M3 front - 2.5-inch HDD model

Pos.	Component
1	2.5-inch HDDs/SSDs
2	ID card
3	ODD
4	Backup drive
5	USB connectors
6	Front panel module

3.5-inch HDD model

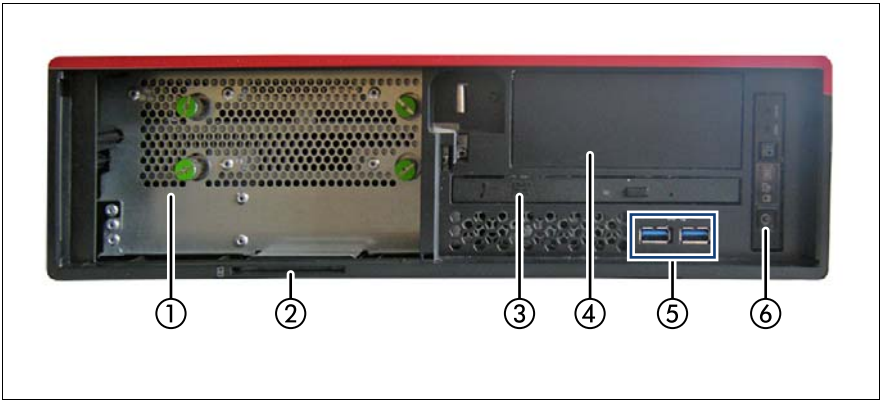

Figure 193: PRIMERGY TX1320 M3 front - 3.5-inch HDD model

Pos.	Component
1	3.5-inch HDDs
2	ID card slot
3	ODD
4	Backup drive
5	USB connectors
6	Front panel module

16.1.2 Server rear

16.1.2.1 Standard power supply

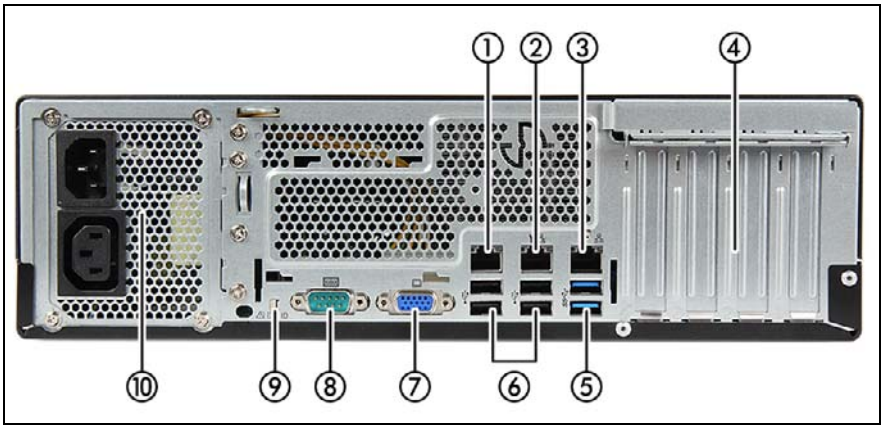

Figure 194: PRIMERGY TX1320 M3 rear - standard PSU

Pos.	Component
1	Management LAN connector
2	Shared LAN connector (LAN1)
3	Standard LAN connector (LAN2)
4	Optional expansion card (4x)
5	USB 3.0 connector (2x)
6	USB connector 2.0 (4x)
7	VGA video connector
8	Serial connector
9	CSS / Global Error / ID indicators
10	Standard PSU

16.1.2.2 Redundant power supply

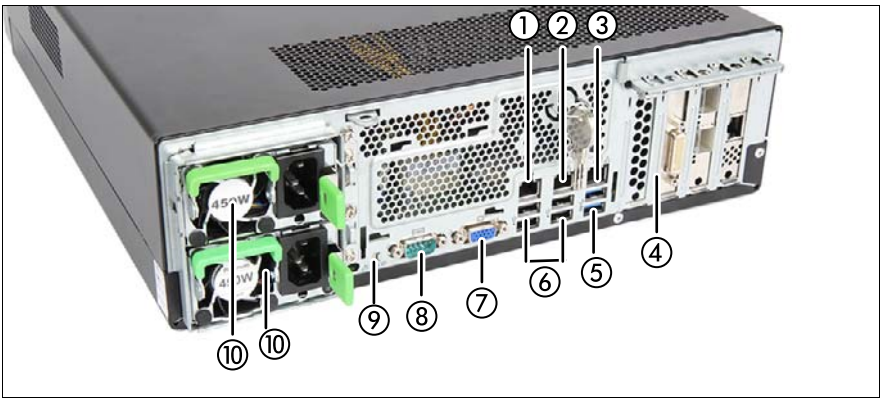

Figure 195: PRIMERGY TX1320 M3 rear - redundant PSU

Pos.	Component
1	Management LAN connector
2	Shared LAN connector (LAN1)
3	Standard LAN connector (LAN2)
4	Optional expansion card (4x)
5	USB 3.0 connector (2x)
6	USB connector 2.0 (4x)
7	VGA video connector
8	Serial connector
9	CSS / Global Error / ID indicators
10	Redundant PSU

16.1.3 Server interior

16.1.3.1 2.5-inch HDD variant

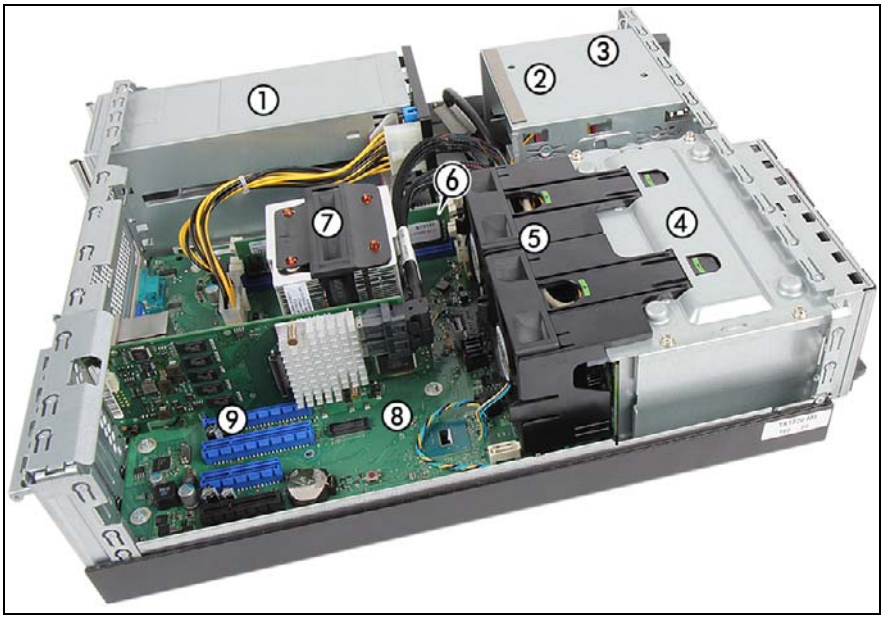

Figure 196: PRIMERGY TX1320 M3 interior (2.5-inch HDD / redundant PSU variant)

Pos.	Component
1	Redundant PSU
2	Accessible drive bay
3	Front panel module bay
4	HDD/SSD bays
5	HDD-Fans
6	Memory modules
7	CPU / heat sink
8	System board D3373
9	Expansion card slots

16.1.3.2 3.5-inch HDD variant

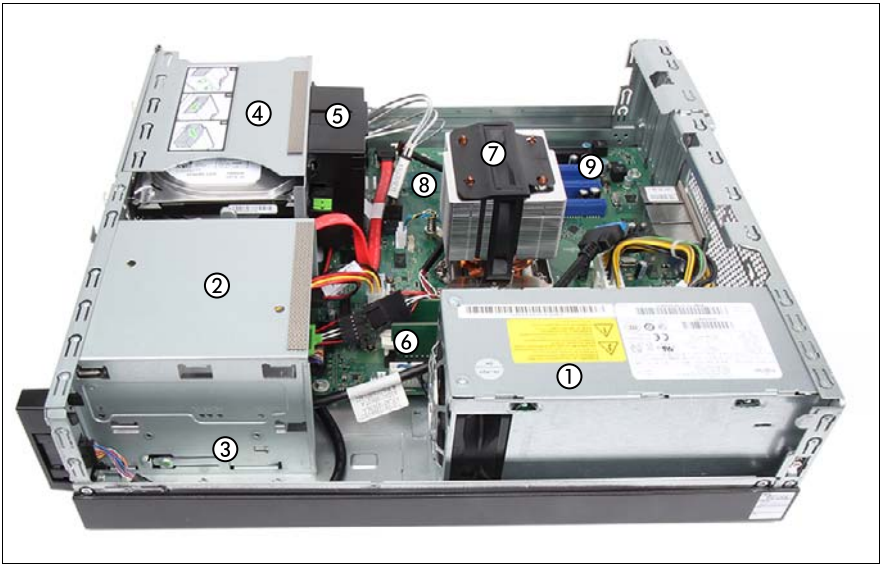

Figure 197: PRIMERGY TX1320 M3 interior (3.5-inch HDD / standard PSU variant)

Pos.	Component
1	Standard PSU
2	Accessible drive bay
3	Front panel module bay
4	HDD/SSD bays
5	HDD-Fans
6	Memory modules
7	CPU / heat sink
8	System board D3373
9	Expansion card slots

16.2 Connectors and indicators

16.2.1 Connectors and indicators on the system board

16.2.1.1 Onboard connectors

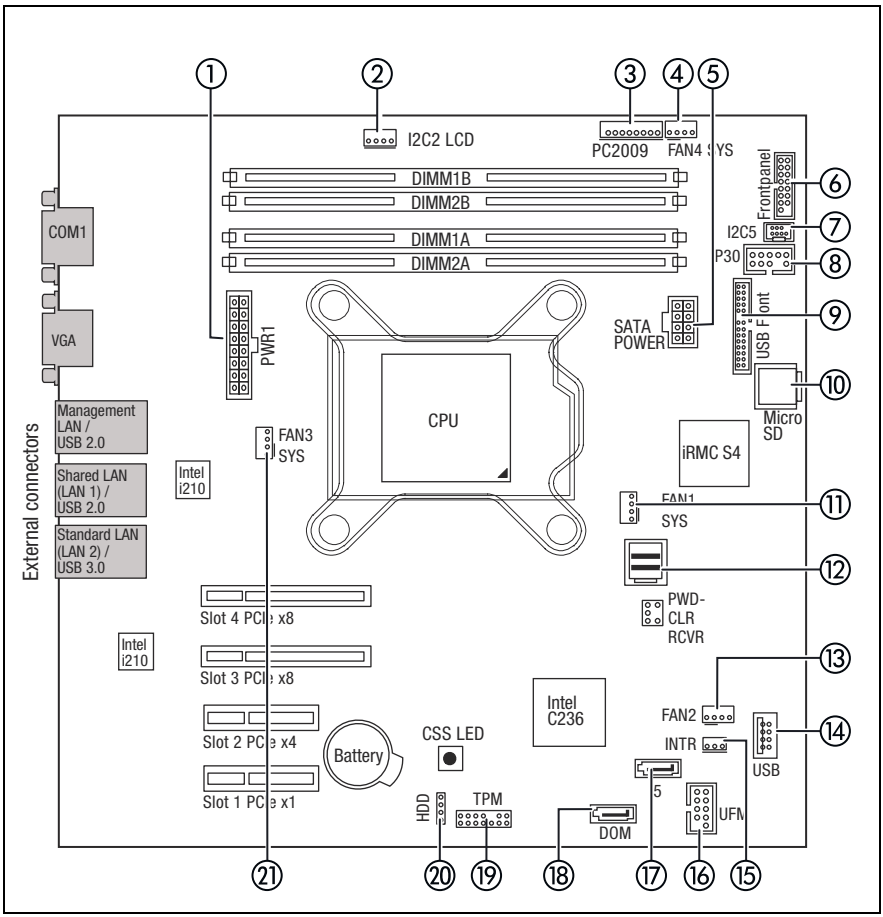

Figure 198: Internal connectors of system board D3373

No.	Print	Description
1	PWR1	ATX PSU connector
2	I2C2 LCD	Connector for LSD
3	PC2009	Power management connector
4	FAN4 SYS	Connector for HDD extension box fan
5	SATA POWER	Power distribution for SAS/SATA backplanes and accessible drives
6	FRONTPANEL	Front panel
7	I2C5	OOB connector
8	P30	PSU connector
9	USB Front	Connector for front USB
10	Micro SD	iRMC microSD card
11	FAN1 SYS	Connector for CPU fan
12		SATA 1-4 Connector for SAS 3.0 cable
13	FAN2	Connector for 3.5" HDD 1-2 or 2.5" HDD 1-4 fan
14	USB	Connector for RDX drive
15	INTR	Intrusion switch cable connector (not used)
16	UFM	Connector for USB Flash Module (UFM)
17	5	Connector SATA 5
18	DOM	Connector for SATA 6/DOM
19	TPM	Connector for Trusted Platform Module (TPM)
20	HDD	(not used)
21	FAN3 SYS	Connector for system fan (rear) (not used)

16.2.1.2 Onboard indicators and controls

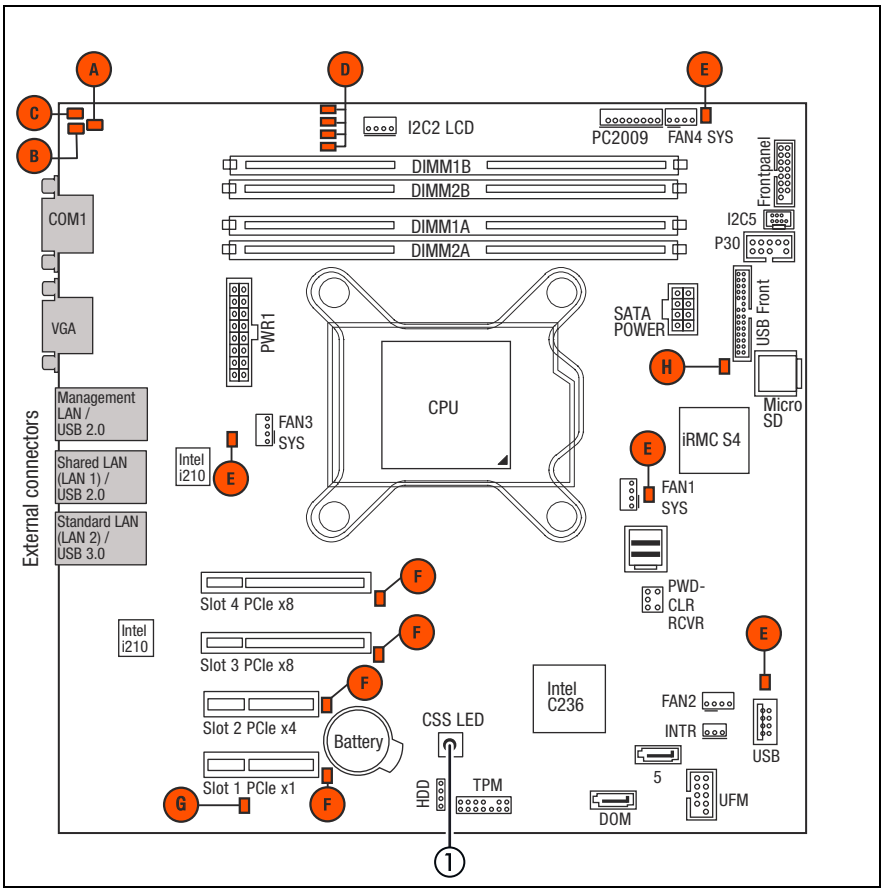

Figure 199: Onboard indicators and Indicate CSS button

1	Indicate CSS button

Component LEDs

LEDs A, B and C are visible from the outside on the server rear. All other LEDs are only visible if the server cover has been opened. In order to access memory LEDs (D), the HDD fan module(s) needs to be removed (see section "Fans" on page 173).

Indicator		Status	Description
A	GEL (Global Error LED)	off	no critical event (non CSS component)
		orange on	prefailure detected (non CSS component)
		orange flashing	non CSS component failure Possible reasons: – sensors report overheating – sensor is defective – CPU error – software reports an error
B	CSS (Customer Self Service)	off	no critical event (CSS component)
		orange on	prefailure detected (CSS component)
		orange flashing	CSS component failure
C	Identification	blue on	server has been highlighted using the ID button on the front panel for easy identification
		blue flashing	server has been highlighted using IRMC (AVR) when local VGA off for easy identification
D	Memory	off	memory module operational
		orange on	memory module failure
E	System fans	off	fan running
		orange on	fan failure
F	PCI card	off	PCI card operational
		orange on	PCI card failure
G	AUX power	yellow on	AUX voltages are within range
H	iRMC	green flashing	iRMC S4 management controller is operational

16.2.2 Server front

16.2.2.1 Indicators on the front panel

Figure 200: Indicators on the front panel

Pos.	Label	Indicator	Status	Description
1	**ID**	ID indicator, see also "iRMC-related status signals" on page 343	blue on	The server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification.
			blue flashing	The server has been highlighted for easy identification using the iRMC (AVR) with disabled local VGA output.
2	CSS	CSS indicator	off	No critical event detected (CSS component).
			orange on	Prefailure event detected (CSS component). For HDDs see also "HDD prefailure detection" on page 344
			orange flashing	CSS component failure detected.

Pos.	Label	Indicator	Status	Description
3		Global Error indicator, see also "iRMC-related status signals" on page 343	off	No critical event detected (non CSS component).
			orange on	Prefailure event detected (non CSS component).
			orange flashing	Non CSS component failure detected. Possible causes: – System is out of the temperature specified range – Defective sensor – CPU error – Error detected by server management software
4		HDD/SSD activity indicator	green flashing	Data access in progress.
5		Power-on indicator	off	The server is switched off.
			green on	– The server has been switched on but Power Cycle Delay settings delay it from turning on for a specified time. – The server is switched on and operating normally.
			green flashing slowly	The BMC firmware is starting up after the server has been connected to the mains.

Pos.	Label	Indicator	Status	Description
6		AC connected indicator	green on	– The server is switched off and connected to the mains (standby mode). – The server has been switched on but Power Cycle Delay settings delay it from turning on for a specified time. After connecting the server to the mains, it will take about 60 seconds until the server will enter standby mode and can be switched on.
			off	– The server is switched off and not connected to the mains. – The server is switched on and operating normally.

iRMC-related status signals

ID indicator	Global error indicator	Description
blue flashing	off	A remote connection has been established. Local VGA output has been disabled during the remote session.
blue flashing	orange flashing	An emergency flash of the iRMC firmware is in progress.

Please refer to chapter "Updating or recovering the system board BIOS and iRMC" on page 84.

HDD prefailure detection

Depending on your hardware configuration HDD prefailure detection will be supported.

The requirements are:

– iRMC Firmware 7.14 or later

– supported OOB RAID system

16.2.2.2 ODD activity indicator

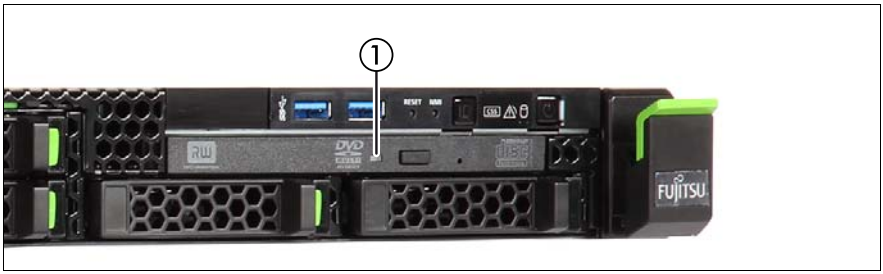

Figure 201: Indicator on the ODD

Pos.	Indicator	Status	Description
1	Activity indicator	off	ODD inactive
		green on	storage medium is being accessed

Depending on your system configuration the activity indicator may not be installed.

16.2.2.3 Indicators on the hot-plug HDD/SSD module

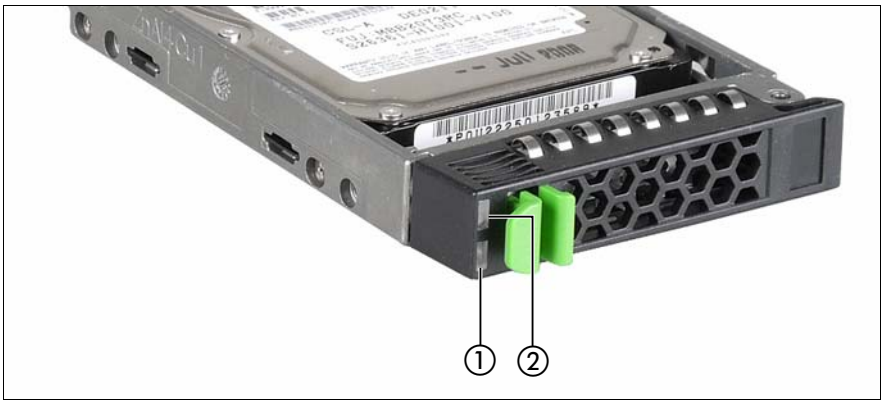

Figure 202: Indicators on the hot-plug HDD/SSD module

Pos.	Label	Indicator	Status	Description
1		Access indicator	off	The HDD/SSD is inactive.
			green on	The HDD/SSD being accessed
2		Error indicator	off	No HDD/SSD error detected.
			orange on	An HDD/SSD error has been detected. Possible causes: – The drive is defective and needs replacing. – A RAID rebuild process has failed. – The HDD/SSD module has not been inserted correctly.
			orange flashing slowly	HDD/SSD RAID rebuild is in progress. Data is being restored after replacing a drive that has been combined into a RAID array.

16.2.3 Server rear

16.2.3.1 Connectors on the I/O panel

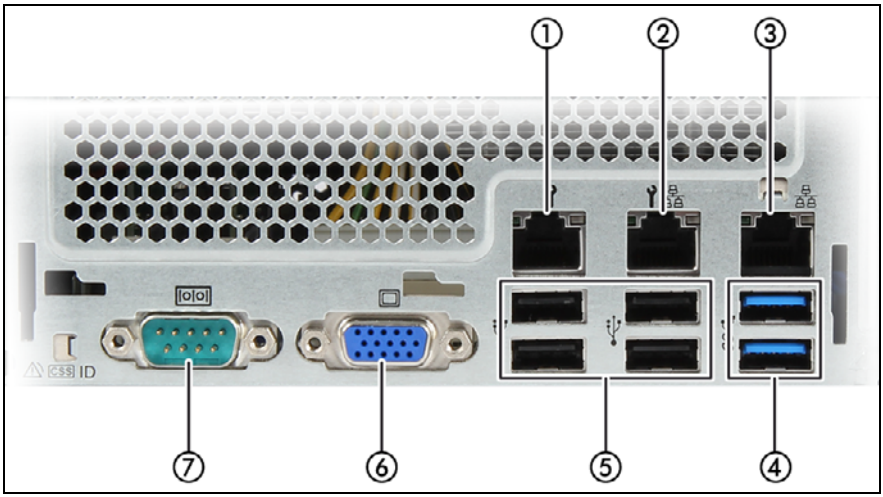

Figure 203: TX1320 M3 I/O panel connectors

1	Management LAN connector, for iRMC S4 server management function
2	Shared LAN connector (LAN1)
3	Standard LAN connector (LAN2)
4	USB 3.0 connectors
5	USB 2.0 connectors
6	Video connector (VGA)
7	Serial connector COM1

Depending on BIOS settings, the shared LAN connector may also be used as a management LAN connector. For further information, please refer to the "D3373 BIOS Setup Utility for FUJITSU Server PRIMERGY TX1320 M3 Reference Manual".

The serial connector COM1 can be used as default interface or to communicate with the iRMC S4.

The chipset offers two integrated USB 2.0 Rate Matching Hubs (RMHs). that enable lower power requirements and manages the transition of the communication data rate from the high speed of the host controller to the lower speed of USB full speed / low speed devices.

16.2.3.2 Indicators on the I/O panel

ID, CSS and Global Error indicators

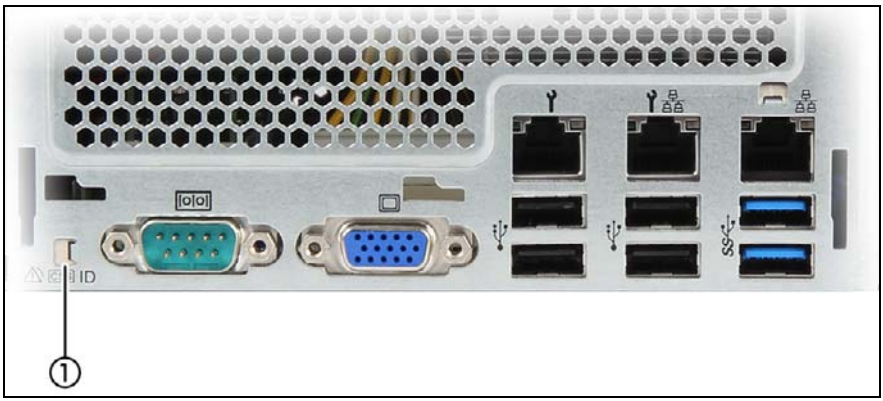

Figure 204: Indicators on the connector panel: CSS, Global Error and ID indicators

Pos.	Label	Indicator	Status	Description
1	ID	ID indicator, see also "iRMC-related status signals" on page 349	blue on	The server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification
			blue flashing	The server has been highlighted for easy identification using the iRMC (AVR) with disabled local VGA output.
	CSS	CSS indicator	off	No critical event detected (CSS component).
			orange on	Prefailure event detected (CSS component). For HDDs see also "HDD prefailure detection" on page 349
			orange flashing	CSS component failure detected.
	⚠	Global Error indicator, see also "iRMC-related status signals" on page 349	off	No critical event detected (non CSS component).
			orange on	Prefailure event detected (non CSS component).
			orange flashing	Non CSS component failure detected. Possible causes: – System is out of the specified temperature range – Defective sensor – CPU error – Error detected by server management software

Note on CSS and Global Error indicators on the I/O panel

If CSS and Global Error indicators are located in the same place on your server's I/O panel, please also check the indicators on the front panel to determine if a CSS or Global Error event has been detected.

For further details on detected errors, refer to the System Event Log (SEL) or use the ServerView Operations Manager or iRMC S4 web interface.

iRMC-related status signals

ID indicator	Global error indicator	Description
blue flashing	off	A remote connection has been established. Local VGA output has been disabled during the remote session.
blue flashing	orange flashing	An emergency flash of the iRMC firmware is in progress.

For further information please refer to section "Updating or recovering the system board BIOS and iRMC" on page 84.

HDD prefailure detection

Depending on your hardware configuration HDD prefailure detection will be supported.

The requirements are:

– iRMC Firmware 7.14 or later

– supported OOB RAID system

LAN indicators

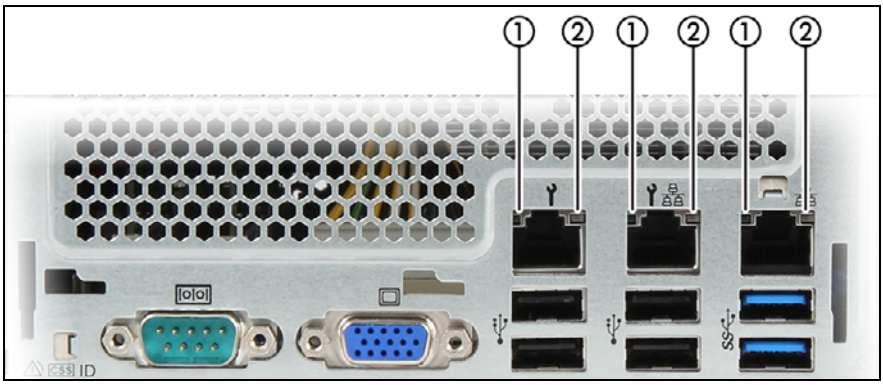

Figure 205: Indicators on the connector panel: LAN indicators

Pos.	Indicator	Status	Description
1	LAN link/transfer indicator	green on	A LAN connection has been established.
		off	LAN is not connected.
		green flashing	LAN data transfer is in progress
2	LAN speed indicator	yellow on	Data traffic at a transfer rate of 1 Gbit/s
		green on	Data traffic at a transfer rate of 100 Mbit/s
		off	Data traffic at a transfer rate of 10 Mbit/s.

Note on the onboard LAN controller

The system board is equipped with a Gigabit Ethernet Controller that supports transfer rates of 10 Mbit/s, 100 Mbit/s and 1 Gbit/s.

The separate management LAN connector is used as a management interface (iRMC S4) and is prepared for operation with the Remote Management. Optionally LAN connector 1 can also be used for iRMC S4 server management.

16.2.3.3 Indicators on hot-plug PSUs

Figure 206: PSU status indicator

Pos.	Indicator	Status	Description
1	PSU status indicator	green flashing	The server is switched off, but mains voltage is present (standby mode).
		green on	The server is switched on and operating properly.
		orange flashing	An overload has been detected. The power supply unit is still running, but failure might be imminent.
		orange on	An PSU failure has been detected. Possible causes: – Over/under voltage – Overheating – Fan failure

16.2.3.4 Indicators on Fujitsu battery units (FJBU)

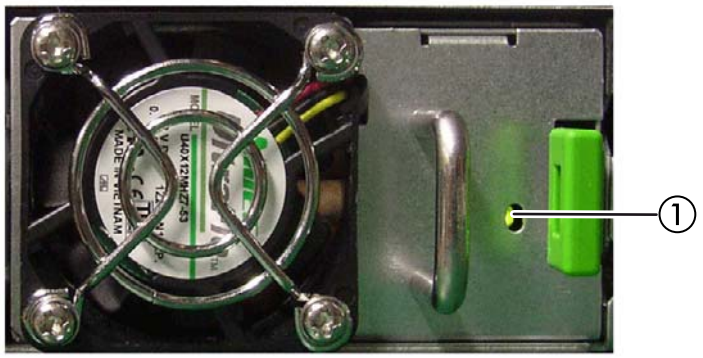

Figure 207: FJBU status indicator

Pos.	Indicator	Status	Description
1	FJBU status indicator	green flashing	The battery unit is charging.
		green flashing slowly	The battery unit is discharging.
		green on	The battery unit is fully charged.
		orange flashing	A battery unit failure has been detected. Possible causes: – Capacity failure – Overheating
		orange on	A general battery failure has occurred.

16.3 Onboard settings

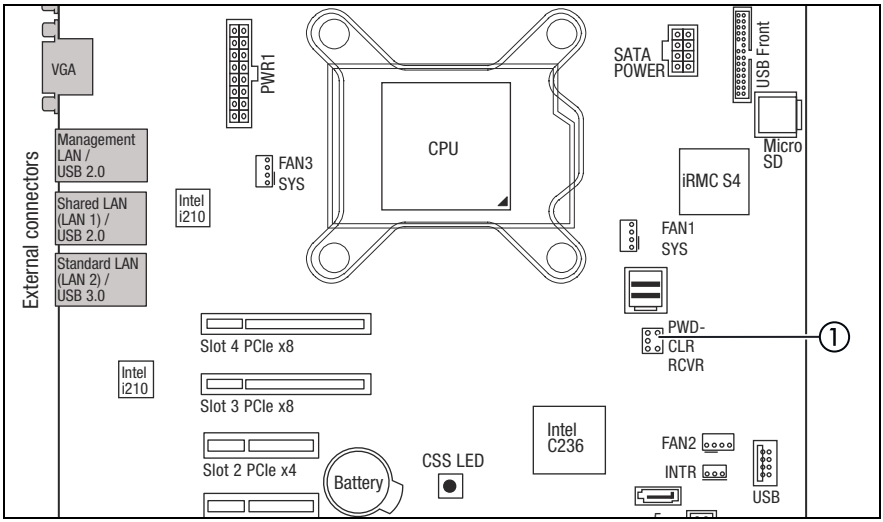

Figure 208: Onboard settings on system board D3373

Setting		Status	Description
1	Jumper settings		Default: Password Clear and Recovery BIOS disabled
			RCVR: Recovery BIOS enabled
			PWD-CLR: Password Clear enabled

16.4 Minimum startup configuration

Field Replaceable Units (FRU)

If the server does not start up or other problems occur, it may be necessary to take the system down to its most basic configuration in order to isolate the defective component.

The minimum startup configuration consists of the following components and cables:

Component	Notes and reference
System board	no TPM, UFM or expansion cards installed
1 CPU with heat sink	no fan (disconnect fan cable)
1 memory module	installed in DIMM slot 1A, see section "Memory sequence" on page 223
Front panel module	
1 PSU	

Table 7: Minimum startup configuration - components

Cable	Notes and reference
Front panel cable	
Power cable	

Table 8: Minimum startup configuration - cables

- Shut down the server as described in section "Shutting down the server" on page 52.
- Remove the AC power cord from the cable tie and disconnect it from the system as described in section "Disconnecting the power cord" on page 53.
- Take the system down to its minimum startup configuration.
- Connect the AC power cord to the PSU and secure it with a cable tie as described in section "Connecting the power cord" on page 64.
- Connect a keyboard, mouse and display to the server.

► Switch on the server as described in section "Switching on the server" on page 69.

CAUTION!

Since the fan module is not included in the minimum startup configuration, the server must be shut down immediately after the diagnostic process is complete (POST phase has been passed).

The minimum startup configuration must be used exclusively for diagnostic purposes by maintenance personnel, never in daily operation!