

PRIMERGY BX920 S4 Server Blade

Upgrade and Maintenance Manual

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 © 2014 Fujitsu Technology Solutions GmbH.

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 the Japanese market: About SATA hard disk drives

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

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

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

Only for the Japanese market:



Although described in this manual, some sections do not apply to the Japanese market. These options and routines include:

- CSS (Customer Self Service)



Contents

1	Introduction	19
1.1	Notational conventions	20
2	Before you start	21
2.1	Classification of procedures	23
2.1.1	Customer Replaceable Units (CRU)	23
2.1.2	Upgrade and Repair Units (URU)	24
2.1.3	Field Replaceable Units (FRU)	25
2.2	Average task duration	26
2.3	Tools you need at hand	27
2.4	Documents you need at hand	28
3	Important information	31
3.1	Safety instructions	31
3.2	CE conformity	38
3.3	FCC Class A Compliance Statement	39
3.4	Environmental protection	40
4	Basic hardware procedures	43
4.1	Using diagnostics information	43
4.1.1	Accessing the management blade web interface	43
4.1.2	Locating the defective server blade	45
4.1.3	Determining the error class	46
4.1.3.1	Global Error indicator	47
4.1.3.2	Customer Self Service (CSS) indicator	48
4.1.4	Locating the defective component	49
4.2	Opening the rack door	52
4.2.1	Opening the rack door of a PRIMECENTER rack	52
4.2.2	Opening the rack door of a PRIMECENTER M1 rack	52

Contents

4.3	Shutting down the server blade	53
4.4	Removing a server blade	54
4.4.1	Preliminary steps	54
4.4.2	Removing the server blade from the system unit	55
4.5	Opening the server blade	56
4.6	Closing the server blade	57
4.7	Installing the server blade in the system unit	58
4.8	Switching on the server blade	60
4.9	Concluding software tasks	61
4.10	Closing the rack door	62
4.10.1	Closing the rack door of a PRIMECENTER rack	62
4.10.2	Closing the rack door of a PRIMECENTER M1 rack	62
5	Basic software procedures	63
5.1	Starting the maintenance task	63
5.1.1	Launching a video redirection to a server blade	63
5.1.2	Checking the server blade status	63
5.1.2.1	Checking the server blade status via management blade web interface	63
5.1.2.2	Checking the server blade status via iRMC	64
5.1.3	Saving BIOS settings	65
5.1.4	Saving iRMC settings	65
5.1.5	Connecting virtual media to the managed server blade	65
5.1.6	Disabling BitLocker functionality	66
5.1.7	Disabling boot watchdog functionality	67
5.1.7.1	Viewing boot watchdog settings	67
5.1.7.2	Configuring boot watchdog settings	67
5.1.8	Verifying and configuring the backup software solution	69
5.1.9	Note on server maintenance in a Multipath I/O environment	70
5.1.10	Note on server maintenance in a Multipath I/O environment	71
5.1.11	Switching on the ID indicator	74
5.2	Completing the maintenance task	75
5.2.1	Updating or recovering the system board BIOS and iRMC	75
5.2.1.1	Updating or recovering the system board BIOS	75
5.2.1.2	Updating or recovering the iRMC	78
5.2.2	Restoring BIOS settings	80
5.2.3	Restoring iRMC settings	80

5.2.4	Updating mezzanine card firmware	80
5.2.5	Enabling Option ROM scan	82
5.2.6	Verifying and configuring the backup software solution	83
5.2.7	Resetting the boot retry counter	84
5.2.7.1	Viewing the boot retry counter	84
5.2.7.2	Resetting the boot retry counter	84
5.2.8	Enabling boot watchdog functionality	86
5.2.9	Enabling replaced components in the system BIOS	87
5.2.10	Verifying the memory mode	87
5.2.11	Verifying the system time settings	88
5.2.12	Viewing and clearing the System Event Log (SEL)	89
5.2.12.1	Viewing the SEL	89
5.2.12.2	Saving the SEL	90
5.2.12.3	Clearing the SEL	91
5.2.13	Updating the NIC configuration file in a Linux environment	91
5.2.14	Enabling BitLocker functionality	93
5.2.15	Performing a RAID array rebuild	94
5.2.16	Looking up changed MAC / WWN addresses	94
5.2.16.1	Looking up MAC addresses	94
5.2.16.2	Looking up WWN addresses	95
5.2.17	Using the Chassis ID Prom Tool	96
5.2.18	Configuring LAN teaming	96
5.2.18.1	After replacing / upgrading LAN/CNA controllers	96
5.2.18.2	After replacing the server blade	97
5.2.19	Switching off the ID indicator	97
6	Hard disk drives / solid state drives	99
6.1	Basic information	101
6.1.1	General equipping rules	102
6.2	Installing a 2.5-inch HDD/SSD module	103
6.2.1	Required tools	103
6.2.2	Preliminary steps	103
6.2.3	Removing the 2.5-inch dummy module	103
6.2.4	Installing the 2.5-inch HDD/SSD module	105
6.2.5	Concluding steps	107
6.3	Removing a 2.5-inch HDD/SSD module	108
6.3.1	Required tools	108
6.3.2	Preliminary steps	108
6.3.3	Removing the 2.5-inch HDD/SSD module	109

Contents

6.3.4	Installing the 2.5-inch dummy module	110
6.3.5	Concluding steps	110
6.4	Replacing a 2.5-inch HDD/SSD module	111
6.4.1	Required tools	111
6.4.2	Preliminary steps	112
6.4.3	Removing the defective 2.5-inch HDD/SSD module	112
6.4.4	Installing the new 2.5-inch HDD/SSD module	112
6.4.5	Concluding steps	112
6.5	Replacing HDD/SSD backplanes	113
6.5.1	Required tools	113
6.5.2	Preliminary steps	113
6.5.3	Removing the HDD/SSD backplane	114
6.5.4	Installing the HDD/SSD backplane	115
6.5.5	Concluding steps	116
7	Expansion cards and backup units	117
7.1	Mezzanine cards	118
7.1.1	Basic information	118
7.1.1.1	Installing riser cards	120
7.1.1.2	Removing riser cards	122
7.1.1.3	Population rules for mezzanine cards	124
7.1.2	Installing mezzanine cards	130
7.1.2.1	Required tools	130
7.1.2.2	Preliminary steps	130
7.1.2.3	Installing a mezzanine card	131
7.1.2.4	Concluding steps	135
7.1.3	Removing mezzanine cards	136
7.1.3.1	Required tools	136
7.1.3.2	Preliminary steps	136
7.1.3.3	Removing a mezzanine card	137
7.1.3.4	Concluding steps	139
7.1.4	Replacing mezzanine cards	140
7.1.4.1	Required tools	140
7.1.4.2	Preliminary steps	140
7.1.4.3	Removing a mezzanine card	141
7.1.4.4	Installing a mezzanine card	141
7.1.4.5	Concluding steps	141
7.2	SAS RAID HDD module	143
7.2.1	Basic information	143

7.2.2	Installing the SAS RAID HDD module	144
7.2.2.1	Required tools	144
7.2.2.2	Preliminary steps	144
7.2.2.3	Installing the SAS RAID HDD module	145
7.2.2.4	Concluding steps	146
7.2.3	Removing the SAS RAID HDD module	147
7.2.3.1	Required tools	147
7.2.3.2	Preliminary steps	147
7.2.3.3	Removing the SAS RAID HDD module	148
7.2.3.4	Concluding steps	148
7.2.4	Replacing the SAS RAID HDD module	150
7.2.4.1	Required tools	150
7.2.4.2	Preliminary steps	150
7.2.4.3	Replacing the SAS RAID HDD module	151
7.2.4.4	Concluding steps	151
7.2.5	Installing the FBU (Flash Backup Unit)	152
7.2.5.1	Required tools	152
7.2.5.2	Preliminary steps	152
7.2.5.3	Installing the FBU	153
7.2.5.4	Concluding steps	154
7.2.6	Removing the FBU (Flash Backup Unit)	155
7.2.6.1	Required tools	155
7.2.6.2	Preliminary steps	155
7.2.6.3	Removing the FBU	156
7.2.6.4	Concluding steps	157
7.2.7	Replacing the FBU (Flash Backup Unit)	158
7.2.7.1	Required tools	158
7.2.7.2	Preliminary steps	158
7.2.7.3	Removing the FBU	159
7.2.7.4	Installing the FBU	160
7.2.7.5	Concluding steps	161
8	Main memory	163
8.1	Basic information	164
8.1.1	Memory sequence	164
8.1.1.1	Population rules	164
8.1.1.2	Independant Channel mode	166
8.1.1.3	Mirrored channel mode	167
8.1.1.4	Performance channel mode	168

Contents

8.1.1.5	Rank Sparing Mode (single rank (1R) and dual rank (2R) RDIMM modules)	169
8.1.1.6	Rank Sparing Mode for quad rank (4R) and octa rank (8R) LRDIMM modules (minimizing waste of spare memory)	170
8.1.1.7	Dummy DIMM modules	171
8.2	Installing memory modules	172
8.2.1	Required tools	172
8.2.2	Preliminary steps	172
8.2.3	Installing a memory module	173
8.2.4	Concluding steps	174
8.3	Removing memory modules	175
8.3.1	Required tools	175
8.3.2	Preliminary steps	175
8.3.3	Removing a memory module	176
8.3.4	Concluding steps	177
8.4	Replacing memory modules	178
8.4.1	Required tools	178
8.4.2	Preliminary steps	178
8.4.3	Removing a memory module	179
8.4.4	Installing a memory module	179
8.4.5	Concluding steps	180
8.5	Handling of memory air cowls	181
8.5.1	Installing the air cowls	181
8.5.2	Removing the air cowls	182
9	Processors	183
9.1	Basic information	184
9.2	Installing processors	184
9.2.1	Required tools	184
9.2.2	Preliminary steps	185
9.2.3	Installing a processor	186
9.2.4	Concluding steps	190
9.3	Removing processors	191
9.3.1	Required tools	191
9.3.2	Preliminary steps	191
9.3.3	Removing a processor	193
9.3.4	Concluding steps	197

9.4	Upgrading or replacing processors	198
9.4.1	Required tools	198
9.4.2	Preliminary steps	198
9.4.3	Upgrading or replacing a processor	199
9.4.4	Concluding steps	199
9.5	Handling processor heat sinks	201
9.5.1	Required tools	201
9.5.2	Preliminary steps	201
9.5.3	Installing processor heat sinks	202
9.5.3.1	Preparing the heat sink and processor	203
9.5.3.2	Installing the heat sink	204
9.5.4	Removing processor heat sinks	206
9.5.5	Replacing processor heat sinks	207
9.5.5.1	Removing the processor heat sink	207
9.5.5.2	Applying thermal paste	207
9.5.5.3	Installing the processor heat sink	207
9.5.6	Concluding steps	207
9.6	Applying thermal paste	208
10	System board components	211
<hr/>		
10.1	Replacing the CMOS battery	211
10.1.1	Required tools	212
10.1.2	Preliminary steps	212
10.1.3	Removing the battery	213
10.1.4	Installing the CMOS battery	214
10.1.5	Concluding steps	215
10.2	USB Flash Module (UFM)	216
10.2.1	Installing the UFM	216
10.2.1.1	Required tools	216
10.2.1.2	Preliminary steps	216
10.2.1.3	Installing the UFM	217
10.2.1.4	Concluding steps	219
10.2.1.5	Software configuration	219
10.2.2	Removing the UFM	220
10.2.2.1	Required tools	220
10.2.2.2	Preliminary steps	220
10.2.2.3	Removing the UFM	221
10.2.2.4	Concluding steps	221
10.2.3	Replacing the UFM	222

Contents

10.2.3.1	Required tools	222
10.2.3.2	Preliminary steps	222
10.2.3.3	Removing the UFM	223
10.2.3.4	Re-installing the UFM	223
10.2.3.5	Concluding steps	225
10.2.3.6	Software configuration	225
10.3	Trusted Platform Module (TPM)	226
10.3.1	Installing the TPM	226
10.3.1.1	Required tools	226
10.3.1.2	Preliminary steps	226
10.3.1.3	Installing the TPM	227
10.3.1.4	Concluding steps	230
10.3.2	Removing the TPM	231
10.3.2.1	Required tools	231
10.3.2.2	Preliminary steps	232
10.3.2.3	Removing the TPM	233
10.3.2.4	Concluding steps	234
10.3.3	Replacing the TPM	235
10.3.3.1	Required tools	235
10.3.3.2	Preliminary steps	236
10.3.3.3	Removing the TPM	236
10.3.3.4	Re-installing the TPM	236
10.3.3.5	Concluding steps	237
10.4	Onboard SAS enabling key	238
10.4.1	Required tools	238
10.4.2	Preliminary steps	238
10.4.3	Removing the defective onboard SAS enabling key	239
10.4.4	Installing the new onboard SAS enabling key	240
10.4.5	Concluding steps	241
10.5	Replacing the system board	242
10.5.1	Required tools	243
10.5.2	Preliminary steps	244
10.5.3	Removing the system board	245
10.5.4	Installing the system board	247
10.5.4.1	Mounting the system board	247
10.5.4.2	Swapping the processor	248
10.5.5	Concluding steps	249
11	Server blade	251

11.1	Replacing the server blade	252
12	Appendix	255
12.1	Mechanical overview	255
12.1.1	Server blade front	255
12.1.2	Server blade interior	256
12.2	Configuration tables	257
12.2.1	Memory configuration table	257
12.2.2	Mezzanine card configuration table	257
12.3	Connectors and indicators	258
12.3.1	Connectors and indicators on the system board	258
12.3.1.1	Onboard connectors	258
12.3.1.2	Onboard settings	259
12.3.1.3	Onboard indicators and controls	260
12.3.2	Connectors and indicators on the front	262
12.3.2.1	Front panel connectors	262
12.3.2.2	Front panel indicators	263
12.3.2.3	Indicators on the hot-plug HDD/SSD module	265
12.4	Minimum startup configuration	266

Contents

Version history

Issue number	Reason for update
1.0 / January 2014	Initial release
2.0 / February 2014	Chapter 5.2.15

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 28).







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 23.

1.1 Notational conventions

The following notational conventions are used in this manual:

<i>Text in italics</i>	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 23
	indicates the average task duration, see " Average task duration " on page 26

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 31](#).
- ▶ Make sure that all necessary manuals are available. Refer to the documentation overview in section "[Documents you need at hand](#)" on [page 28](#). Print the PDF files if required.
- ▶ Make yourself familiar with the procedure categories introduced in section "[Classification of procedures](#)" on [page 23](#).
- ▶ Ensure that all required tools are available according to section "[Tools you need at hand](#)" on [page 27](#).

Installing optional components

The "PRIMERGY BX920 S4 Server Blade Operating manual" 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> (<http://jp.fujitsu.com/platform/server/primergy/manual/> for the Japanese market). Please refer to the following ServerView Suite topics:

- Operation
- Virtualization
- Maintenance



For the latest information on hardware options, refer to your server's hardware configurator available online at the following address:

for the EMEA market:

http://ts.fujitsu.com/products/standard_servers/blades/primergy_bx920s4.html

for the Japanese market:

<http://jp.fujitsu.com/platform/server/primergy/system/>

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 (EMEA market only).

Replacing a defective component

The global error indicators on the front side of the server blade 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 "PRIMERGY BX920 S4 Server Blade Operating Manual" and section "[Connectors and indicators](#)" on page 258.

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 43 and "[Connectors and indicators on the front](#)" on page 262.

If the defective component is a customer replaceable unit included in the CSS concept (Customer Self Service, only available for EMEA market), the CSS indicators on the front side of the server blade will light up.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual available online at <http://manuals.ts.fujitsu.com> (EMEA market) or <http://jp.fujitsu.com/platform/server/primergy/manual/> (Japanese market).

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 HDD / SSD modules

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*).



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

- Processors (upgrade kits)
- Mezzanine cards
- SAS RAID HDD module
- Flash Backup Unit (FBU)
- Memory modules

Components that are handled solely as Repair Units

- CMOS battery

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

- Processors (replacements)
- SAS / PCH backplanes
- Trusted Platform Module (TPM)
- USB Flash Module (UFM)
- Server blade (replacement)



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 26](#) 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 63 .
System unit removal, disassembly	yes	Making the server blade available, removing the server blade from the system unit
Transport	no	Transporting the server blade 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 blade to its installation site (where required) depends on local customer conditions.
Assembly, system unit installation	yes	Reassembling the server blade, installing the server blade in the system unit
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.

Screw driver / Bit insert	Screw	Usage	Type
Phillips PH2 / (+) No. 2 hexagonal cross SW5 / PZ2		Backup drives, optical disk drives, chassis	M3 x 4.5 mm (silver) C26192-Y10-C67
Phillips PH2 / (+) No. 2 hexagonal cross SW5 / PZ2		System board	M3 x 6 mm (silver) C26192-Y10-C68
Phillips PH2 / (+) No. 2 hexagonal cross SW5 / PZ2		Backup drives with UNC thread	UNC 6-32 x 4.76 mm (black) C26192-Y10-C75
Phillips PH0 / (+) No. 0		2.5-inch HDDs / SSDs	M3 x 3.5 mm Wafer head screw (silver) C26192-Y10-C102
TPM bit insert Dedicated TPM screw driver / TPM module fixing tool (for the Japanese market)		TPM screw One way head (black)	REM 3 x 15 mm (black) C26192-Y10-C176

Table 2: List of required tools and used screws


Before you start

Screw driver / Bit insert	Screw	Usage	Type
Phillips PH1 / (+) No. 1		UFM nylon screw	M3 x 4.5 mm (white) A3C40109082
Phillips PH2 / (+) No. 2		Foot mounting rail screws	M4 x 6 mm Combination screw (silver) C26192-Y10-C113

Table 2: List of required tools and used screws

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 *Industry standard servers*.

For the Japanese market please use the following address:
<http://jp.fujitsu.com/platform/server/primergy/manual/>

Document	Description
"Safety notes and regulations" manual "安全上のご注意" for the Japanese market	Important safety information, available online, or as a printed copy
"PRIMERGY BX920 S4 Server Blade" Operating Manual	available online
"D3142 BIOS Setup Utility for PRIMERGY BX920 S4" Reference Manual	Information on configurable BIOS options and parameters, available online
System board and service labels	Labels inside the side / top server cover outlining connectors, indicators and basic maintenance tasks
Software documentation	<ul style="list-style-type: none"> – "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1" user interface description or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1" user interface description – "ServerView Operations Manager - Server Management" user guide – "iRMC S4 – integrated Remote Management Controller" user guide
Illustrated Spares catalog	Spare parts identification and information system (EMEA market only), 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 the Japanese market	Important information on warranty regulations, recycling and service , available online or as a printed copy

Table 3: Documentation you need at hand

Before you start

Document	Description
"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 the Japanese market	
Additional documentation	<ul style="list-style-type: none">– "iRMC S4" user guide available online– RAID documentation, available online at http://manuals.ts.fujitsu.com under <i>Industry standard servers - Expansion Cards - Storage Adapters</i> <p>For the Japanese market please use the following address: http://jp.fujitsu.com/platform/server/primer-gy/manual/</p> <ul style="list-style-type: none">– Rack documentation
Third party documentation	<ul style="list-style-type: none">– Operating system documentation, online help– Peripherals documentation

Table 3: Documentation you need at hand

3 Important information



CAUTION!

Before installing and starting up a device, 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 device 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 device 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 device that do not relate to CSS failures shall be performed by service personnel. Please note that unauthorized interference with the system 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.
- Before installing/removing internal options 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 device, observe the instructions on environmental conditions for your device.
- If the device is brought in from a cold environment, condensation may form both inside and on the outside of the device.

Important information

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

- Transport the device only in the original packaging or in packaging that protects it from knocks and jolts.
For the Japanese market, transporting the device in its original packaging does not apply.

Installation and operation

- This unit should not be operated in ambient temperatures above 35 °C. For servers with Cool-safe[®] Advanced Thermal Design the ambient temperature can increase to 40 °C.
- If the unit 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 B connectors.
- The unit automatically adjusts itself to a mains voltage in a range of 100 VAC to 240 VAC. Ensure that the local mains voltage lies within these limits.
- This device must only be connected to properly grounded power outlets or connected to the grounded rack internal power distribution system with tested and approved power cords.
- Ensure that the device is connected to a properly grounded power outlet close to the device.
- Ensure that the power sockets on the device and the properly grounded power outlets are easily accessible.
- The On/Off button or the main power switch (if present) does not isolate the device from the mains power supply. In case of repair or servicing disconnect the device completely from the mains power supply, unplug all power plugs from the properly grounded power outlets.
- Always connect the server and the attached peripherals 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.
- Data cables must be adequately shielded.

- 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 system administrator or your customer service team. Only disconnect the system from the mains power supply if there is no risk of harming yourself.
- Proper operation of the system (in accordance with IEC 60950-1 resp. EN 60950-1) is only ensured if the casing is completely assembled and the rear covers for the installation slots have been fitted (electric shock, cooling, fire protection, interference suppression).
- Only install system 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 system or violate the safety regulations. Information on which system 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 system 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.
- Before installing/removing internal options to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the outlet. Failure to do so can cause electric shock.

Important information

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock and will void the warranty and exempt the manufacturer from all liability.
- Devices inside the server remain hot after shutdown. Wait for a while after shutdown before installing or removing internal options.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, if you are wearing an earthing band on your wrist when working with this type of module, connect it to an unpainted, non-conducting metal part of the system.
- 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 device/position. To use a screw of the different kind can cause a breakdown of equipment.
- The installation indicated on this document is sometimes changed to the kind of possible options without notice.

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 device may present a fire or chemical burn hazard if mistreated. Do not disassemble, heat about 100 °C (212F), or incinerate the 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 device (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.

Important information

- 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.
- 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

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

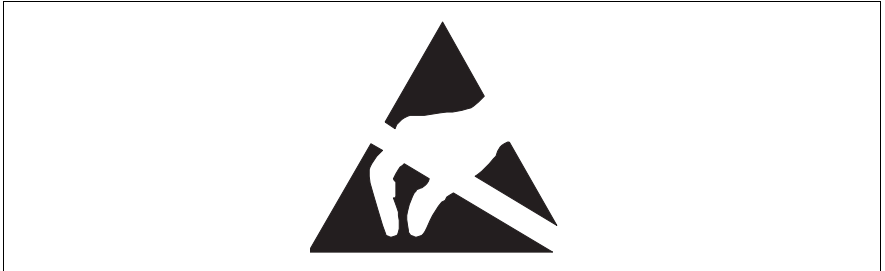


Figure 1: ESD label

When you handle components fitted with ESDs, you must always observe the following points:

- Switch off the system and remove the power plugs from the power outlets before installing or removing components with ESDs.
- 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, non-conducting metal part of the system.
- 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 system unit.
- Always hold components with ESDs at the edges or at the points marked green (touch points).
- Do not touch any connectors or conduction paths on an ESD.
- Place all the components on a pad which is free of electrostatic charge.



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

Important information

Transporting the server

- Only transport the device in its original packaging or in packaging that protects it from impacts and jolts.
For the Japanese market, transporting the device in its original packaging does not apply.
- Do not unpack the device until it is at its installation location.
- Never lift or carry the device by the handles on the front panel.

Notes on installing the server in the rack

- Never lift the server into the rack using the handles 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 protection is correctly fitted.
- For safety reasons, no more than one unit may be removed from the rack at any one time during installation and maintenance work.
- If several units are simultaneously removed from the rack, there is a risk that the rack could tip over.
- The rack must be connected to the power supply by an authorized specialist (electrician).
- 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.

3.2 CE conformity



The system complies with the requirements of the EC directives 2004/108/EC regarding "Electromagnetic Compatibility" and 2006/95/EC "Low Voltage Directive". This is indicated by the CE marking (CE = Communauté Européenne).

3.3 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.

WARNING:

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

3.4 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 EMEA market)
- <http://jp.fujitsu.com/platform/server/primergy/concept/> (for the Japanese market)

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 doesn't apply to the Japanese market.

Do not throw away the packaging. You may need it later for transporting the system. 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 2002/96/EC 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 from our recycling center in Paderborn:

Fujitsu Technology Solutions
Recycling Center
D-33106 Paderborn

Tel. +49 5251 525 1410
Fax +49 5251 525 32 1410

4 Basic hardware procedures

4.1 Using diagnostics information

The "PRIMERGY BX920 S4 Server Blade Operating Manual" gives an introduction to server blade features and provides an overview of available hardware options.

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.

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 (EMEA market only).

Perform the following diagnostics procedures to identify defective server blades and components:

4.1.1 Accessing the management blade web interface

For checking the current system status and administration of the server blade, connect a field service terminal (FST, e.g. notebook) to the management blade of the system unit and login to the management blade web interface.

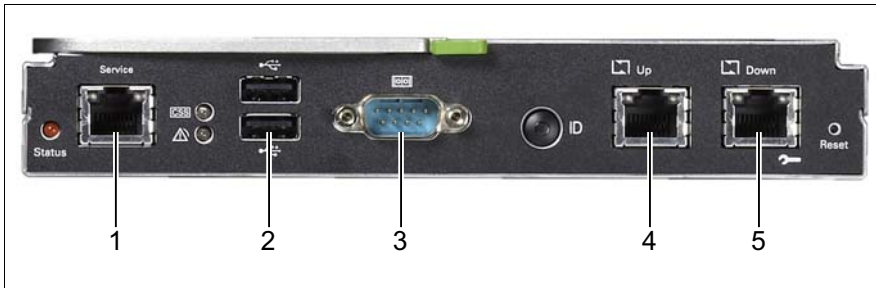


Figure 2: Connectors on the management blade

- ▶ Connect the FST to the management LAN connector. Customers must use the *Up* port (4) while the *Down* port (5) is reserved for service personnel.

- i** – If two management blades are installed, connect the FST to the master management blade. The status indicator of the master management blade glows yellow.
 - The FST must be on the same LAN with the same subnet as the management LAN port.

- ▶ Launch a web browser and enter the *Management Agent Administrative URL* to login to the management blade web interface. For further information, refer to the "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description" or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description".

- i** If you don't know the *Management Agent Administrative URL*, proceed as follows.

- ▶ Connect the FST to the serial port of the management blade (3) and open a terminal session, see the "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description" or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description".
- ▶ Open the *Management Agent – Management Agent Information* menu to view the *Management Agent Administrative URL*.
- ▶ Login to the management blade web interface as described above.

4.1.2 Locating the defective server blade

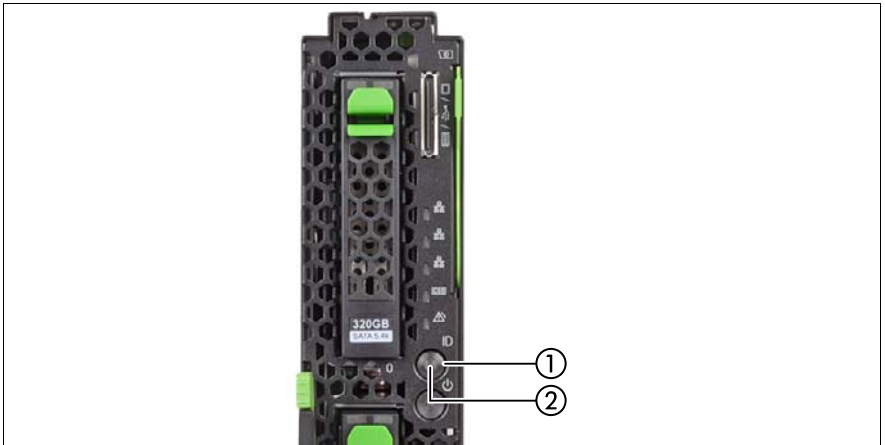


Figure 3: ID button and indicator on front panel

When working in a datacenter environment, switch on the ID indicator on the front panel of the server blade for easy identification.

- ▶ Press the ID button on the front panel (1), use the management blade web interface, or use the ServerView Operation Manager user interface to switch on the ID indicator (2).



For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual available online at <http://manuals.ts.fujitsu.com> (EMEA market) or <http://jp.fujitsu.com/platform/server/primergy/manual/> (Japanese market).

- ▶ When using management blade web interface to toggle the ID indicator, open the *Components - System - Server Blades - Server Blade-x* menu for the desired server blade, and press the *Locate* button in the server blade status frame.
- ▶ 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.

4.1.3 Determining the error class

The Local Service Concept (LSC) allows you to identify defective server blade 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 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 blade restart due to a power failure.

4.1.3.1 Global Error indicator

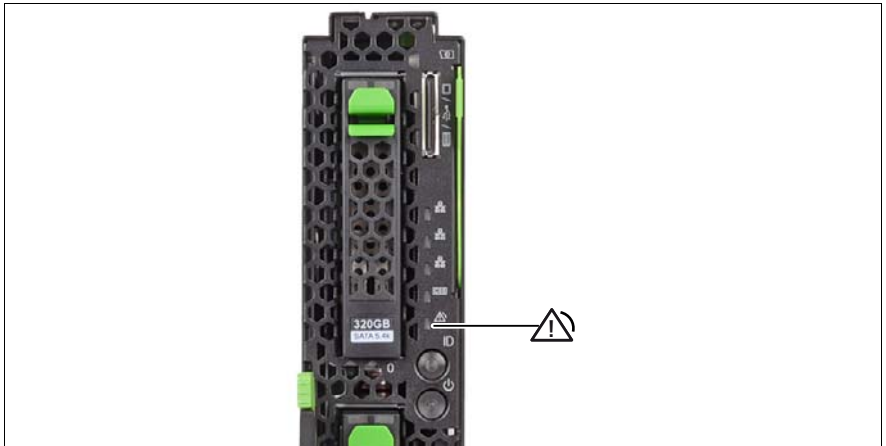


Figure 4: Global Error indicator on front panel

- ▶ Check the Global Error indicator on the front of the server blade:

Indicator	Status	Description
Global error indicator	off	no critical event (non CSS component)
	orange on	prefailure detected (non CSS component), requires (precautionary) service intervention
	orange flashing	non CSS component failure or software / agent related error, requires service intervention

- ▶ For further diagnostics, proceed as follows:

- Hardware errors:

Check the System Event Log (SEL) as described in section "[Viewing the SEL](#)" on page 89.

- Software / agent related errors:

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



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

4.1.3.2 Customer Self Service (CSS) indicator



Figure 5: CSS error indicator in front panel

- ▶ Check the CSS indicator on the front panel of the server blade:

Indicator	Status	Description
CSS indicator	off	no critical event (CSS component)
	yellow on	prefailure detected (CSS component)
	yellow flashing	CSS component failure

4.1.4 Locating the defective component

After determining the error class by the CSS or Global Error indicators (see section 4.1.3 on page 46) local diagnostic indicators on the system board allow you to identify the defective component.

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

Local diagnostic indicators on the system board

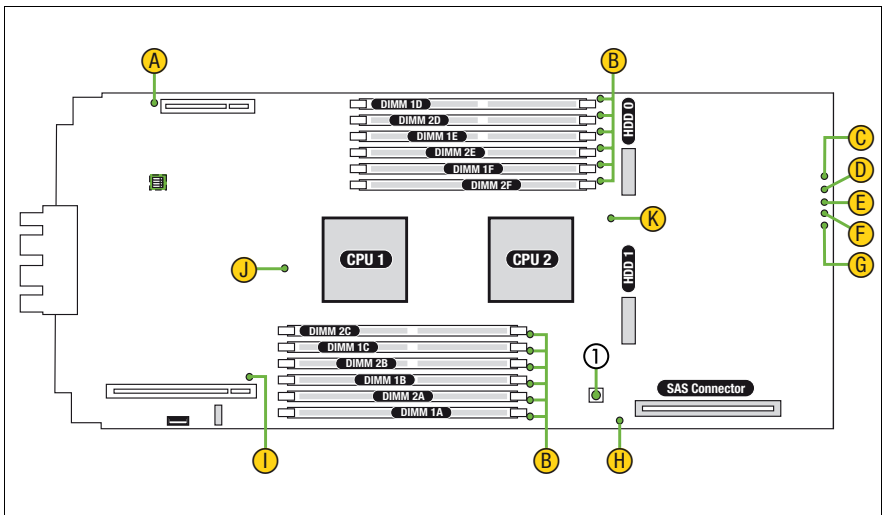


Figure 6: Onboard indicators and Indicate CSS button

No.	Description
1	Indicate CSS button

Using the Indicate CSS button

- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).

Basic hardware procedures

- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ Press the Indicate CSS button (1) to highlight defective components.

Component LEDs



LEDs C to G are visible from the frontside. All other LEDs are only visible if the server blade cover has been removed. In order to access memory LEDs (B), the air cowls need to be removed (see section ["Handling of memory air cowls" on page 181](#)).

Indicator		Status	Description
A	Mezzanine card 1	off	Mezzanine card 1 operational
		orange on	Mezzanine card 1 failure
B	Memory	off	memory module operational
		orange on	memory module failure
C	Fabric 3/4	off	Fabric 3/4 no link
		green flashing	Fabric 3/4 link active
		green on	Fabric 3/4 link established
D	Fabric 2	off	Fabric 2 no link
		green flashing	Fabric 2 link active
		green on	Fabric 2 link established
E	Fabric 1	off	Fabric 1 no link
		green flashing	Fabric 1 link active
		green on	Fabric 1 link established
F	CSS	off	System is ok
		yellow flashing	CSS error detected
		yellow on	Prefailure event detected
G	Global Error	off	No critical event
		orange flashing	Error detected (requires service intervention)
		orange on	Prefailure event detected (requires service intervention)
H	SAS RAID HDD module	off	SAS RAID HDD module operational
		orange on	SAS RAID HDD module failure


Indicator		Status	Description
I	Mezzanine card 2	off	Mezzanine card 2 operational
		orange on	Mezzanine card 2 failure
J	CPU 1	off	CPU 1 operational
		orange on	CPU 1 failure
K	CPU 2	off	CPU 2 operational
		orange on	CPU 2 failure

i 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 46](#)).

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 Opening the rack door

4.2.1 Opening the rack door of a PRIMECENTER rack


 The following description only applies to the PRIMECENTER rack. For further instructions on opening or closing the 19-inch rack, please refer to the "19-inch Rack for PRIMERGY and RM systems" assembly guide, available online.

The PRIMECENTER rack is equipped with a split front door. The left-hand door contains an interlocking system that can be locked and opened with a key. Optionally, a revolving door knob can be mounted for key-less locking. To unlock and open the rack, proceed as follows:

- ▶ Insert and turn the key counter-clockwise by 180 degrees.
If applicable, turn the door knob counter-clockwise by 180 degrees.
- ▶ Open the left-hand door first, then the right-hand door.


 For further information, refer to the "PRIMECENTER" assembly guide available online at <http://manuals.ts.fujitsu.com>.

4.2.2 Opening the rack door of a PRIMECENTER M1 rack

 The following description only applies to the new PRIMECENTER M1 rack.

The new PRIMECENTER M1 rack is equipped with a one-piece front door. To unlock and open the rack, proceed as follows:

- ▶ Insert and turn the key clockwise as far as it will go.
- ▶ Pull the green marked grip to open the door.

 For further information, refer to the "PRIMECENTER M1 Rack" user guide available online.

4.3 Shutting down the server blade



CAUTION!

For further safety information, please refer to chapter ["Important information"](#) on page 31.

- ▶ Inform the system administrator that the server blade will be shut down and put offline.
- ▶ Terminate all applications.
- ▶ In case of Multipath I/O environments, please refer to section ["Note on server maintenance in a Multipath I/O environment"](#) on page 70.

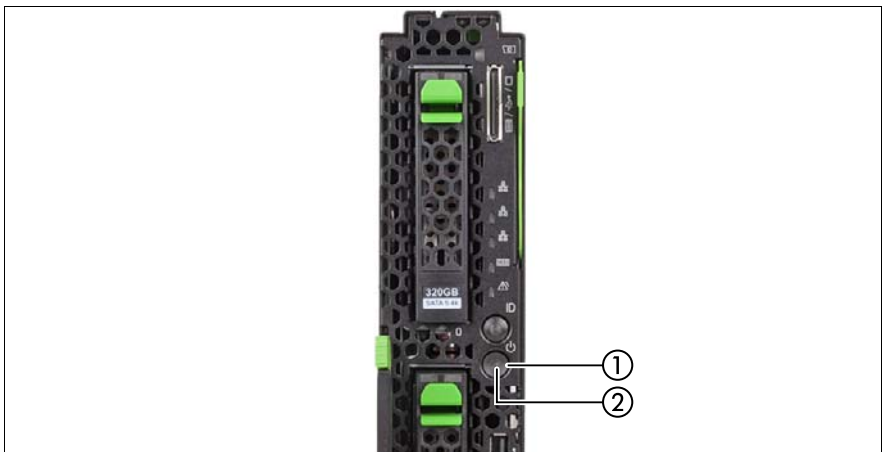


Figure 7: Power button on the front panel

- ▶ Shut down the server blade by pressing the On / Off button (1). The power indicator (2) turns off.



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 panel of the server blade as described in section ["Locating the defective server blade"](#) on page 45.

4.4 Removing a server blade



CAUTION!

For safety information, please refer to chapter ["Important information"](#) on [page 31](#).

4.4.1 Preliminary steps

- ▶ If applicable, open the rack door as described in section ["Opening the rack door"](#) on [page 52](#).
- ▶ Shut down and power off the server blade as described in section ["Shutting down the server blade"](#) on [page 53](#).

4.4.2 Removing the server blade from the system unit

- ▶ Shut down the server blade as described in section ["Preliminary steps" on page 54](#).

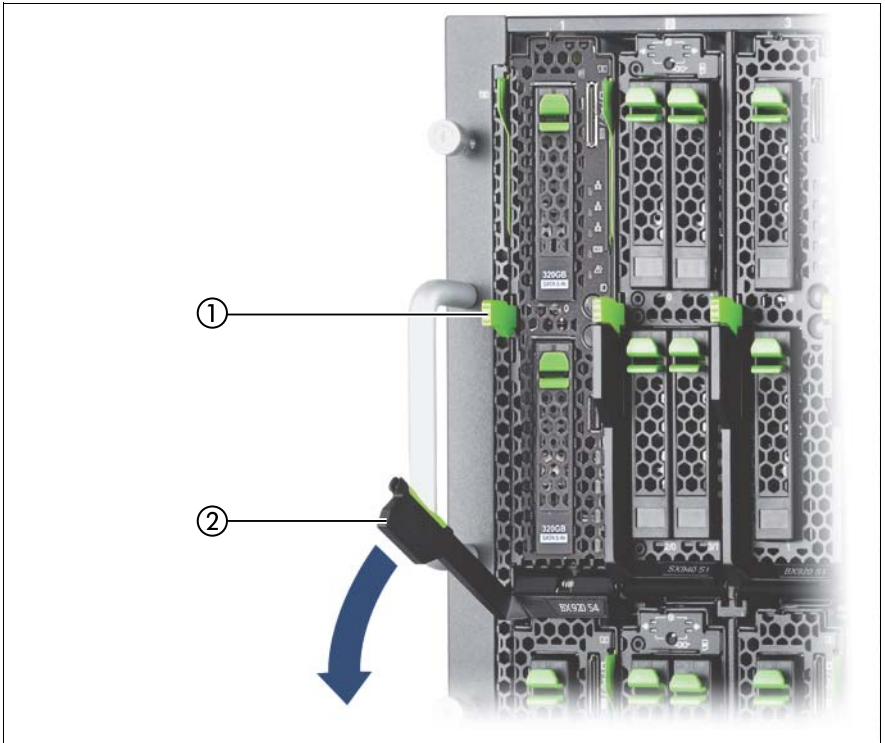


Figure 8: Removing the server blade from the system unit

- ▶ Push the release lever (1) up slightly to unlock the ejection lever (2).
- ▶ Swivel the ejection lever down until it is horizontal.
- ▶ Pull the server blade out of the system unit.

4.5 Opening the server blade



CAUTION!

For safety information, please refer to chapter "[Important information](#)" on [page 31](#).

Removing the cover

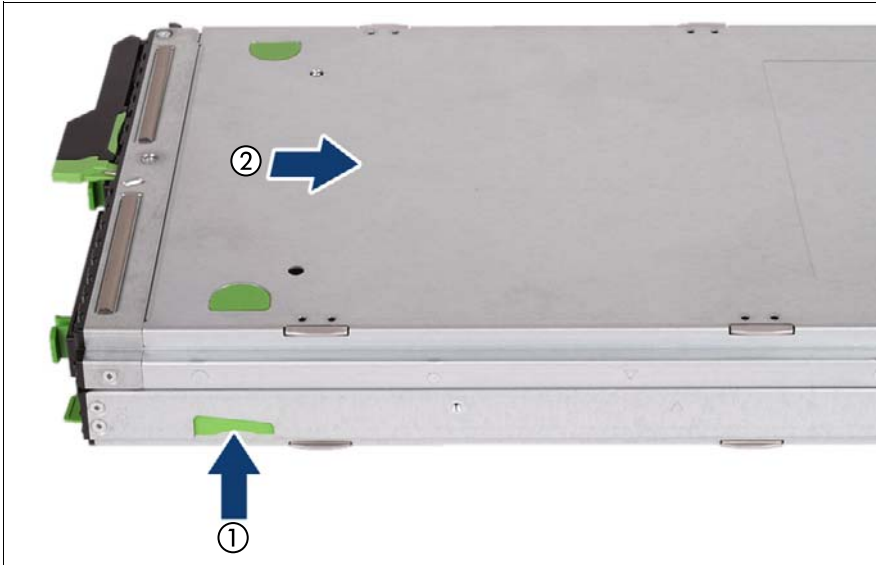


Figure 9: Removing the cover

- ▶ Push the locking lever in the direction of the arrow (1).
- ▶ Slide the housing cover backwards as far as possible (2).
- ▶ Take off the housing cover.

4.6 Closing the server blade



CAUTION!

- Before attaching the cover, 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 BX920 S4 server blade must not run while the cover is removed.
- For further safety information, please refer to chapter ["Important information"](#) on page 31.



Figure 10: Closing the server blade

- ▶ Place the cover on the server blade housing such that it lies flush with both sides, leaving a gap of approx. 1-2 cm from the front frame.
- ▶ Push the cover in the direction of the arrow until it snaps into place.

4.7 Installing the server blade in the system unit



CAUTION!

- Note the safety instructions and the information on handling electrostatically sensitive devices in [section "Safety instructions" on page 31](#).
- Note the population rules for power supply units and fan modules to ensure sufficient cooling of the system. You will find more detailed information on this in the operating manual for the system unit.

Installing the Server Blade



CAUTION!

Follow the safety instructions and information in [section "Modules with Electrostatic-Sensitive Devices" on page 37](#).

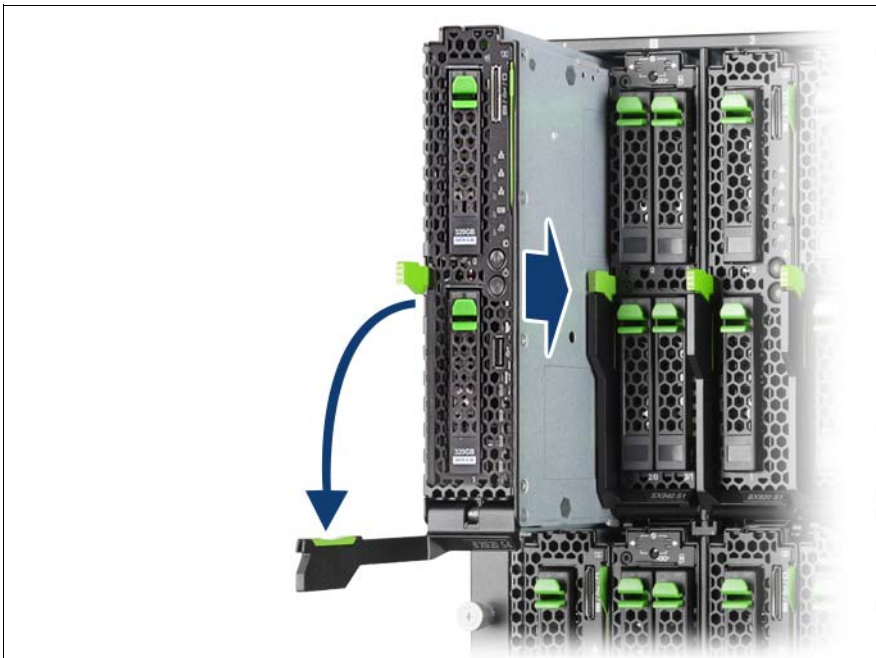


Figure 11: Installing the Server Blade

- ▶ Open the release lever.
- ▶ Push the server blade as far as possible into the slot.

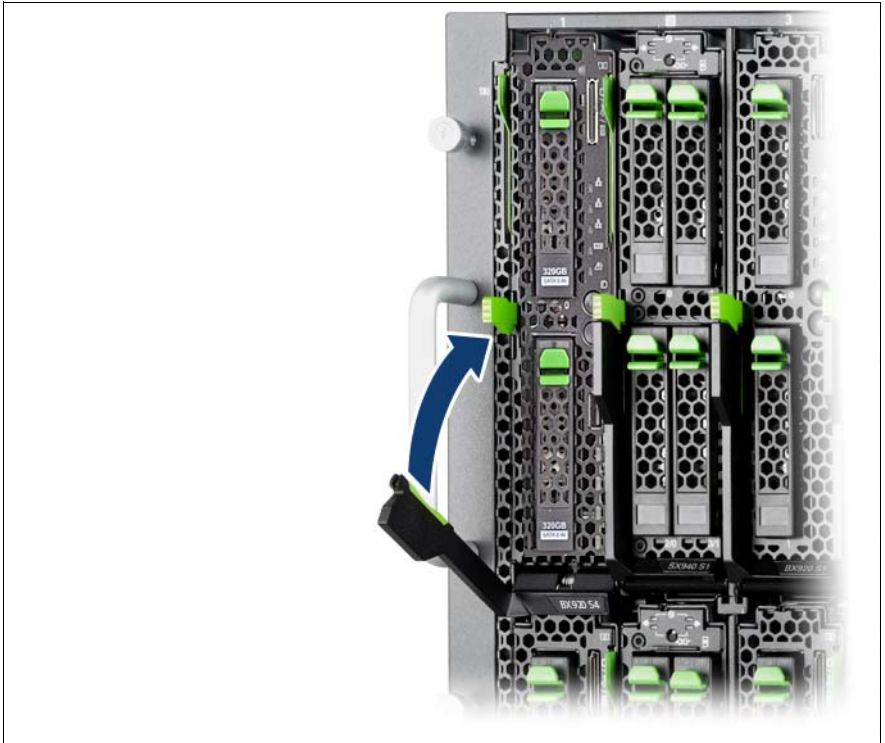


Figure 12: Locking the Server Blade

- ▶ Pull the release lever up until it engages.

It is not a breakdown though the power supply of the server blade intermittently repeats turning on/cutting when "Automatic inventory collection (Automatic Inventory Retrieval)" of the management blade is set to "Automatic" (default value) after the installation of the server blade.

4.8 Switching on the server blade



CAUTION!

- Before switching on the server blade, make sure the cover is closed. In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY BX920 S4 server blade must not run while the cover is removed.
- Follow the safety instructions in chapter ["Important information" on page 31](#).

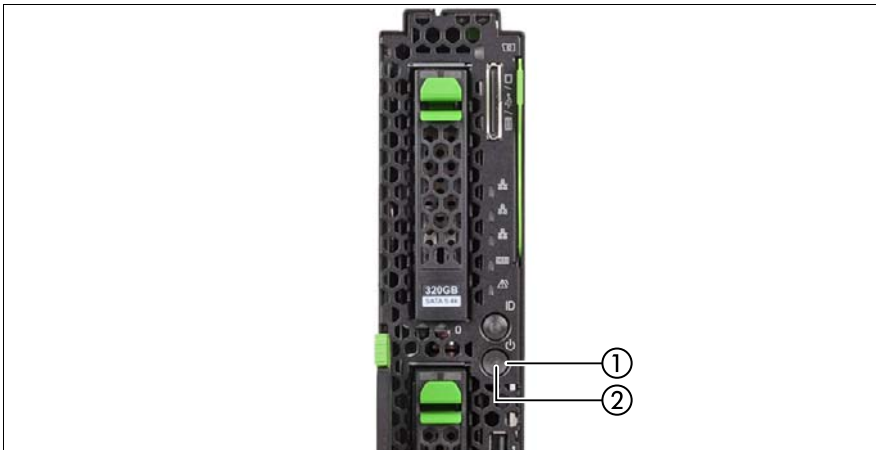


Figure 13: Power button on the front panel

- ▶ Press the On / Off button (1) to start up the server blade.
- ▶ Ensure that the power indicator (2) in the On / Off button is lit green.



For more information, refer to section ["Front panel indicators" on page 263](#).

4.9 Concluding software tasks

- ▶ Perform the following software tasks to put the server blade back in operation:
 - ["Resetting the boot retry counter" on page 84](#)
 - ["Verifying the system time settings" on page 88](#)
 - ["Viewing and clearing the System Event Log \(SEL\)" on page 89](#)
 - ["Updating the NIC configuration file in a Linux environment" on page 91](#)
 - ["Enabling BitLocker functionality" on page 93](#)
 - ["Performing a RAID array rebuild" on page 94](#)
 - ["Looking up changed MAC / WWN addresses" on page 94](#)

4.10 Closing the rack door

4.10.1 Closing the rack door of a PRIMECENTER rack

The PRIMECENTER rack is equipped with a split front door. The left-hand door contains an interlocking system that can be locked and opened with a key. Optionally, a revolving door knob can be mounted for key-less locking. To close and lock the rack, proceed as follows:

- ▶ Close the right-hand door first, then the left-hand door.
- ▶ Insert and turn the key clockwise by 180 degrees.
If applicable, turn the door knob clockwise by 180 degrees.



For further information, refer to the "PRIMECENTER" assembly guide available online.

4.10.2 Closing the rack door of a PRIMECENTER M1 rack

The new PRIMECENTER M1 rack is equipped with a one-piece front door. To close and lock the rack, proceed as follows:

- ▶ Close the door. The green marked grip will click into place.
- ▶ Insert and turn the key counter-clockwise as far as it will go.



For further information, refer to the "PRIMECENTER M1 Rack" user guide available online.

5 Basic software procedures

5.1 Starting the maintenance task

5.1.1 Launching a video redirection to a server blade

The management blade web interface uses the iRMC Advanced Video Redirection (AVR) function to provide a virtual console for the server blades. AVR allows you to control the mouse and keyboard of the managed server blade from your FST and to show the current graphical and text output from the managed server blade.

To open a virtual console for the server blade proceed as follows.

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Open the *Configuration* tab.
- ▶ Scroll to the *iRMC Address Configuration* box.
- ▶ Make sure that *Management LAN* is selected in the *LAN Port* list box.
- ▶ Click the *Video Redirection* button in the status frame of the server blade menu.



For detailed information on iRMC Advanced Video Redirection (AVR) refer to the "Integrated Remote Management Controller" user guides available online.

5.1.2 Checking the server blade status

5.1.2.1 Checking the server blade status via management blade web interface

To check the server blade status proceed as follows.

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System* menu.

- ▶ Click the  button in the *Server Blade Status* title bar to expand the server blade list.

The over all status of the installed server blades is indicated by the icons in the *Health* column.



For the meaning of the icons, refer to the *Help – On Page* function of the management blade web interface.

- ▶ Select the *Server Blade-x* entry to open the administration menu for the desired server blade.
- ▶ Scroll down in the *Information* tab to get status information about the following components.
 - Operating System
 - BIOS Version
 - Processors
 - Memory modules
 - Network components (on-board CNA controller and mezzanine cards)
 - Operating System
- ▶ Open the *Event Log* tab to read the system event log entries.

5.1.2.2 Checking the server blade status via iRMC

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Click the *Remote Management* button in the status frame of the server blade menu.

The iRMC web interface opens, where you can administer the server blade remotely.



For further information refer to the "Integrated Remote Management Controller" user guides available online.

5.1.3 Saving BIOS settings

The description for saving the BIOS settings can be found in chapter „Save & Exit menu“ in the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

For the Japanese market, follow the instructions provided separately.

5.1.4 Saving iRMC settings

- ▶ Open the iRMC web interface "FUJITSU ServerView® iRMC S4 Web Server" directly.



CAUTION!

Saving functionality of iRMC configuration is only supported with iRMC web interface directly. Saving functionality of iRMC configuration via MMB web interface is not supported.

- ▶ Open the *iRMC S4 – Network Settings – Ethernet*, and confirm *IP Address, Subnet Mask* and *Gateway*.
- ▶ Open the *iRMC S4 - Save Configuration*.
- ▶ Click the *Save All* button in section of "Save iRMC S4 Firmware settings in ServerView® WinSCU XML format".
- ▶ Store the backup file in the system of the FST.

5.1.5 Connecting virtual media to the managed server blade

The management blade web interface uses the iRMC *Virtual Media* function to provide the server blade a "virtual" drive which is located elsewhere in the network. This function can be used to boot a server blade from a remote DVD drive or ISO file.

To start the *Virtual Media* function for the server blade proceed as follows.

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.

- ▶ Click the *Video Redirection* button in the status frame of the server blade menu.
- ▶ Click *Virtual Media Wizard* in the menu bar of the video redirection window.



For further information on iRMC *Virtual Media* function refer to the "Integrated Remote Management Controller" user guides available online.

5.1.6 Disabling 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. On the operating system drive, BitLocker uses the compatible Trusted Platform Module (TPM) to detect if the computer's startup process has been modified from its original state.

Disabling BitLocker Drive Encryption is a temporary method for removing BitLocker protection without decrypting the drive Windows is installed on. Disable BitLocker before modifying the server's hardware configuration or startup files. Enable 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 disable BitLocker drive encryption before maintaining the server.
 - When disabled, 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 disable BitLocker-protection on the operating system drive, 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 temporarily disable BitLocker, click *Turn Off BitLocker*, and then click *Disable BitLocker Drive Encryption*.



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

For further information on how to disable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

5.1.7 Disabling boot watchdog functionality

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

5.1.7.1 Viewing boot watchdog settings

To view boot watchdog settings in management blade web interface, proceed as follows:

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab and see the *ASR* box to obtain detailed information about the current watchdog status, timeout intervals and actions that are triggered if watchdog timeouts are exceeded.



For more detailed information, refer to the *Help – On Page* function of the management blade web interface.

5.1.7.2 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 management blade web interface:

Configuring boot watchdog settings in the BIOS

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **F2** function key to 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 "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

Configuring boot watchdog settings using the management blade web interface

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab and scroll to the *ASR* box.
- ▶ Deactivate the *Enable Watchdog* option.
- ▶ Click *Apply* for the changes to take effect.



For more detailed information, refer to the *Help – On Page* function of the management blade web interface.

5.1.8 Verifying and configuring the backup software solution



This task only applies to the Japanese market.

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.

This is the case for the following backup software solution:

- BackupExec



Procedures may differ depending on the backup software. For details, refer to the dedicated documentation provided separately.

Further information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages.

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

When booting your server blade offline from the ServerView Suite DVD to perform an offline driver 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.

Before using the ServerView Update DVD or PrimeCollect in an offline environment, it is necessary to disconnect FC/LAN/SAS connections from the system.

- ▶ Ask the system administrator to disable the FC/iSCSI/CNA/SAS connections to the server blade via FC/LAN/SAS connection blade command.

After executing work, do the reconnection. Ask the system administrator.

Continue as follows:

- ▶ If performing an offline driver update, first of all prepare the ServerView Update DVD:
 - ▶ Download the latest ServerView Update DVD image from the Fujitsu FTP server at <ftp://ftp.ts.fujitsu.com/images/serverview>.
 - ▶ Burn the image to a DVD.

For the Japanese market:

- ▶ Locate, download and burn the ServerView Update DVD image available from the following URL:
<http://jp.fujitsu.com/platform/server/primergy/products/note/svsdvd/dvd/>
- ▶ Ensure that all external I/O connections have been removed from the server blade.



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

The server blade will now boot from the DVD.

- ▶ After the boot process is complete, select your preferred GUI language.
- ▶ In the initial Installation Manager startup window, choose either *Update Manager Express* or *PrimeCollect* from the *Installation Manager mode* section.
- ▶ Click *Continue* to proceed.

If *Update Manager Express* has been selected, insert the ServerView Update DVD into the DVD drive before proceeding.

- ▶ Finish the intended maintenance task. For further information, refer to the following manuals available online at <http://manuals.ts.fujitsu.com> (EMEA market) or <http://jp.fujitsu.com/platform/server/primergy/manual/> (Japanese market):
 - ServerView Update Manager Express:
"Local System Update for PRIMERGY Servers" user guide
 - PrimeCollect:
"PrimeCollect" user guide
- ▶ After the update or diagnostic procedure has been completed, it is necessary to connect FC/iSCSI/CNA/SAS connections on the system. Ask the system administrator to enable the FC/iSCSI/CNA/SAS connections to the server blade via FC/LAN/SAS connection blade command.
- ▶ If necessary, perform this procedure for all remaining servers within the Multipath environment.

5.1.10 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.

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

Continue as follows:

- ▶ If performing an offline BIOS / firmware update, first of all prepare the ServerView Update DVD:
 - ▶ Download the latest ServerView Update DVD image from the Fujitsu FTP server at:

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

- ▶ Burn the image to a DVD.

For the Japanese market:

- ▶ Locate, download and burn the ServerView Update DVD image available from the following URL:

<http://jp.fujitsu.com/platform/server/primergy/products/note/svsdvd/dvd/>

- ▶ Ensure that all external I/O connections have been removed from the server.



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.
The server will now boot from the DVD.
- ▶ After the boot process is complete, select your preferred GUI language.
- ▶ In the initial Installation Manager startup window, choose either *Update Manager Express* or *PrimeCollect* from the *Installation Manager mode* section.
- ▶ Click *Continue* to proceed.

If *Update Manager Express* has been selected, insert the ServerView Update DVD into the DVD drive before proceeding.

- ▶ Finish the intended maintenance task. For further information, refer to the following manuals:
 - ServerView Update Manager Express:
"Local System Update for PRIMERGY Servers" user guide
 - PrimeCollect:
"PrimeCollect" user guide

- ▶ 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.

5.1.11 Switching on the ID indicator

When working in a datacenter environment, switch on the ID indicator on the front of the server blade for easy identification.

Using the ID button on the front panel

- ▶ Press the ID button on the front panel to switch on the ID indicator.



When the ID button is pushed for five seconds or more and separated, it lights to blue.

In addition, when the ID button is pushed again within one second, NMI is issued.



For further information, refer to section ["Front panel indicators" on page 263](#).

Using management blade web interface

- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Press the *Locate* button in the server blade status frame to switch on the ID indicator.

Using ServerView Operations Manager

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

5.2 Completing the maintenance task

5.2.1 Updating or recovering the system board BIOS and iRMC

After replacing the server blade, a processor or memory modules, 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/> (EMEA market)

<http://jp.fujitsu.com/platform/server/primergy/downloads/> (Japanese market)



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

TFTP update procedure

- ▶ Ensure that the server blade has been shut down as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Log in to the management blade web interface.
- ▶ Open the *Information / Operation – Operation – Firmware Update* menu.
- ▶ Open the *Server Blade* tab.
- ▶ In the *Server Blade to be Updated* box select the desired server.
- ▶ In the *Update settings* box select the update firmware (BIOS).
- ▶ In the *Update settings* box enter the TFTP IPv4 or IPv6 address of the TFTP server and the pathname of the TFTP firmware file.



For more detailed information, refer to the *Help – On Page* function of the management blade web interface.

- ▶ Click the *Apply* button to start the update process.

The status column in the *Server Blade to be Updated* box provides information on the update progress.



CAUTION!

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

BIOS recovery procedure



For the Japanese market, follow the instructions provided separately.

- ▶ Prepare a USB stick with the following files:
 - Update tool
 - *Startup.nsh* (which will execute the update tool)
 - BIOS image file for update (16 MB with header information)
- ▶ Ensure that the server blade has been shut down as described in section ["Shutting down the server blade" on page 53](#).

First option: Recovering the server blade BIOS via management blade web interface

- ▶ Ensure that the server blade has been shut down as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Log in to the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab.
- ▶ In the *Boot Options* box activate the *BIOS Recovery Flash Bit Enabled* option.
- ▶ Connect the monitor, keyboard, mouse and USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.
- ▶ Switch on the server blade as described in section ["Switching on the server blade" on page 60](#).

After a short beep, the BIOS upload is executed. The status of the Flash operation is displayed on screen. Once the Flash operation is complete, information on how to proceed is displayed:



CAUTION!

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

- ▶ Switch off the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the Y cable.
- ▶ Deactivate the *BIOS Recovery Flash Bit Enabled* option in the management blade *Boot Options* menu.
- ▶ Switch on the server blade as described in section "[Switching on the server blade](#)" on page 60.
- ▶ You can now put the server blade back into operation.

Second option: Recovering the server blade BIOS via DIP switch

- ▶ Remove the server blade from the system unit as described in section "[Removing a server blade](#)" on page 54.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.
- ▶ Enter BIOS recovery mode using switch 3 of the user DIP switch bank, see section "[Onboard settings](#)" on page 259.
- ▶ Close the server blade as described in section "[Closing the server blade](#)" on page 57.
- ▶ Reinstall and secure the server blade in the system unit as described in section "[Installing the server blade in the system unit](#)" on page 58.
- ▶ Connect the monitor, keyboard, mouse and USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.
- ▶ Switch on the server blade as described in section "[Switching on the server blade](#)" on page 60.

After a short beep, the BIOS upload is executed. The status of the Flash operation is displayed on screen. Once the Flash operation is complete, information on how to proceed is displayed:



CAUTION!


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

- ▶ Switch off the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the Y-cable.

- ▶ Remove the server blade from the system unit as described in section "Removing a server blade" on page 54.
- ▶ Open the server blade as described in section "Opening the server blade" on page 56.
- ▶ Turn switch 3 of the user DIP switch bank to OFF, see section "Onboard settings" on page 259.
- ▶ Close the server blade as described in section "Closing the server blade" on page 57.
- ▶ Reinstall the server blade in the system unit as described in section "Installing the server blade in the system unit" on page 58.
- ▶ Switch on the server blade as described in section "Switching on the server blade" on page 60.
- ▶ You can now put the server blade back into operation.

5.2.1.2 Updating or recovering the iRMC

TFTP update procedure

- ▶ Log in to the management blade web interface.
 - ▶ Open the *Information / Operation – Operation – Firmware Update* menu.
 - ▶ Open the *Server Blade* tab.
 - ▶ In the *Server Blade to be Updated* box select the desired server.
 - ▶ In the *Update settings* box select the update firmware (iRMC).
 - ▶ In the *Update settings* box enter the TFTP IPv4 or IPv6 address of the TFTP server and the pathname of the TFTP firmware file.
-  For more detailed information, refer to the *Help – On Page* function of the management blade web interface.
- ▶ Click the *Apply* button to start the update process.

The status column in the *Server Blade to be Updated* box provides information on the update progress.



CAUTION!

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

iRMC recovery procedure

The iRMC recovery is performed via the *FlashDisk* menu executed from a bootable USB memory stick. For detailed information refer to the "Integrated Remote Management Controller" user guides available online.



For the Japanese market, follow the instructions provided separately.

- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Connect the monitor, keyboard, mouse and the bootable USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.
- ▶ Switch on the server blade while as described in section "[Switching on the server blade](#)" on page 60 to boot from the USB memory stick.

After completion of the boot operation, the *FlashDisk* menu opens.

- ▶ Select *Recovery_L* to carry out the recovery flash for firmware image 1 (low firmware image).
- ▶ Select *Recovery_U* to carry out the recovery flash for firmware image 2 (high firmware image).
- ▶ Once the update operation has been completed, click on *Exit*, to close the *FlashDisk* menu.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the Y-cable.
- ▶ Switch on the server blade as described in section "[Switching on the server blade](#)" on page 60.
- ▶ You can now put the server blade back into operation.

5.2.2 Restoring BIOS settings

The description for restoring the BIOS settings can be found in chapter „Flash BIOS Update“ in the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

For the Japanese market, follow the instructions provided separately.

5.2.3 Restoring iRMC settings

- ▶ Enter the management blade web interface.
- ▶ Open *Components - Server Blade - Server Blade-x* menu.
- ▶ Open the *Configuration* tab.
- ▶ In the *iRMC Address Configuration Box* set *IP Address, Subnet Mask, Gateway*.
- ▶ Click the *Apply* button.
- ▶ Open the iRMC web interface "FUJITSU ServerView® iRMC S4 Web Server" directly.



CAUTION!

Restoring functionality of iRMC configuration is only supported with iRMC web interface directly. Restoring functionality of iRMC configuration via MMB web interface is not supported.

- ▶ Open the *iRMC S4 - Save Configuration*.
- ▶ Select the backup file stored in the file system of FST in section "Import iRMC S4 Firmware settings in ServerView® WinSCU XML format from file".
- ▶ Click the *Apply* button.

5.2.4 Updating mezzanine card firmware

After replacing the mezzanine card, it is essential to upgrade the firmware to the latest version. The latest mezzanine card firmware version is available from the Fujitsu support web pages at:

<http://ts.fujitsu.com/support/> (EMEA market)

<http://jp.fujitsu.com/platform/server/primergy/downloads/> (Japanese market)



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

For the Japanese market, 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 available online at:

<http://manuals.ts.fujitsu.com> (EMEA market) or

<http://jp.fujitsu.com/platform/server/primergy/manual/> (Japanese market):

- 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/>.

- ▶ 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.



Observe the following note when you use the ServerView Operation Manager (SVOM) to administrate the server blade:

After replacing a Ethernet or Fiber Channel mezzanine card proceed as follows:

- ▶ Enter the SVOM *System Status – Network – Network Adapters – Monitored Components* menu.
- ▶ Click the *Acknowledge* button for the replaced mezzanine card.

The status of the component will then be set to *ok*. To see the new status you must refresh the *Driver Monitor* view with *Refresh*.

5.2.5 Enabling Option ROM scan

In order to configure a mezzanine 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.



For SAN / iSCSI boot the card's Option ROM has to be enabled permanently.

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.

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **[F2]** function key to enter the BIOS.
- ▶ From the *Advanced* menu select *Option ROM Configuration*.



When iSCSI is used via an onboard CNA, from the *Advanced* menu select *Onboard Devices Configuration - Onboard CNA OpROM*.

- ▶ Identify the desired mezzanine card 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 the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

- ▶ From the *Advanced* menu select *Option ROM Configuration*. When iSCSI is used via an Onboard CNA, From the *Advanced* menu select *Onboard Devices Configuration - Onboard CNA OpROM*.


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.

5.2.6 Verifying and configuring the backup software solution


 This task only applies to the Japanese market.

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.

This is the case for the following backup software solutions:

- Netvault for Windows
- ARCServe
- BackupExec

 Procedures may differ depending on the backup software. For details, refer to the dedicated documentation provided separately.

Further information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet 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 69, it has to be re-enabled to complete the maintenance task.

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



Detailed information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages

5.2.7 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.

5.2.7.1 Viewing the boot retry counter

The current boot retry counter status is available in the management blade web interface:

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab and scroll to the *ASR* box.
- ▶ Under *Retry Counter 0-max.* 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.

5.2.7.2 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 management blade web interface

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab and scroll to the *ASR* box.
- ▶ Under *Retry Counter 0-max.* specify the maximum number of boot attempts (0 to 7).

5.2.8 Enabling boot watchdog functionality

If boot watchdog functionality has been disabled for firmware upgrade purposes (see section "[Disabling boot watchdog functionality](#)" on page 67), it has to be re-enabled to complete the maintenance task.

Timer settings can be configured using the management blade web interface:

Configuring boot watchdog settings in the BIOS

- ▶ Open a virtual console for your server blade as described in section "[Launching a video redirection to a server blade](#)" on page 63.
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **[F2]** function key to 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 "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

Configuring boot watchdog settings using the management blade web interface

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Select the *Configuration* tab and scroll to the *ASR* box.
- ▶ Activate the *Enable Watchdog* option.
- ▶ Click *Apply* for the changes to take effect.



For more detailed information, refer to the *Help – On Page* function of the management blade web interface.

5.2.9 Enabling replaced components in the system BIOS

When a processor, an expansion card, or a memory module fails, the defective component will be set to *Disabled* or *Failed* in the system BIOS. The server blade 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.

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **F2** function key to enter the BIOS.
- ▶ Select the *Advanced* menu.
- ▶ Select the status menu of the desired component:

- Processors: *CPU Status*



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.



For detailed information on how to access the BIOS and modify settings, refer to the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

5.2.10 Verifying the memory mode

If a memory module fails, the server blade 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, refer to section ["Mirrored channel mode" on page 167](#).

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.

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **[F2]** function key to 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 "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.

5.2.11 Verifying the system time settings



This task only applies to Linux 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.

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **[F2]** function key to 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 "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" 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) of the management blades and server blades using the management blade web interface and ServerView Operations Manager frontend:

Viewing the SEL using the management blade web interface

- ▶ Enter the management blade web interface.
- ▶ Select the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade and open the *Event Log* tab.
- ▶ In the *Event Log Content* box the SEL is being displayed.
- ▶ In the *Event Log Filter* box select the message type(s) you want to display:
 - All events
 - Informational
 - Minor
 - Major
 - Critical

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.

5.2.12.2 Saving the SEL

Saving the SEL via management blade web interface

- ▶ Enter the management blade web interface.
- ▶ Select the *Information / Operation – Information – Logging – System Event Log* menu.
- ▶ In the *Export Event Log* box select the export medium.
 - Local File or
 - USB Export File

This option is only available, if a USB memory stick is connected to the management blade.
- ▶ Click the *Start* button to save all available management blade and server blade event logs as text file to the selected medium.

Saving the SEL via iRMC

- ▶ Enter the management blade web interface.
- ▶ Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- ▶ Click the *Remote Administration* button in the status frame of the server blade menu.

The iRMC web interface opens, where you can administer the server blade remotely.

- ▶ Open the *Event Log – IPMI SEL content* menu.



For further information refer to the "Integrated Remote Management Controller" user guides available online at <http://manuals.ts.fujitsu.com> (EMEA market) or <http://jp.fujitsu.com/platform/server/primergy/manual/> (Japanese market):

5.2.12.3 Clearing the SEL

You can clear the System Event Log (SEL) using the management blade web interface:

- ▶ Enter the management blade web interface, see section "[Accessing the management blade web interface](#)" on page 43.
- ▶ Select the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade and open the *Event Log* tab.
- ▶ In the *Event Log Filter* box click *Clear All Entries* to clear the SEL.

5.2.13 Updating the NIC configuration file in a Linux 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 CNA controllers in a server running Linux OS, the MAC address will change but not automatically be updated in the definition file.


Basic software procedures


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:

-  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 blade" on page 60](#).

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 Enabling BitLocker functionality


If BitLocker Drive Encryption has been disabled for maintenance purposes (see section "[Disabling BitLocker functionality](#)" on page 66), it has to be re-enabled to complete the service task.

 If BitLocker Drive Encryption has been disabled 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 disabled, 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 BitLocker-protection on the operating system drive, 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 enable a temporarily disabled BitLocker, click *Turn On BitLocker*.
- ▶ Follow the instructions in the BitLocker Setup wizard.

 For further information on how to enable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

5.2.15 Performing a RAID array rebuild

After replacing a hard disk drive 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.

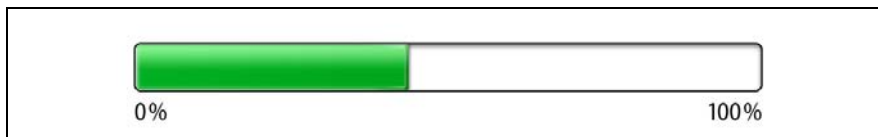


Figure 14: Progress bar (RAID array rebuild)



CAUTION!

The system is now operational, however, data redundancy will not be available until the RAID array rebuild is complete. Depending on the hard disk drive 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 or SFP+ transceiver module, 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

- ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
- ▶ Switch on or restart your server blade.

- ▶ Switch on or restart your server blade.
- ▶ As soon as the startup screen appears, press the **[F2]** function key to enter the BIOS.
- ▶ Depending on the number of network controllers in your system, you will find one or several *Port Configuration* menu items.

Use the arrow key **[→]** to scroll to the right and browse all available tabs.

Each *Port Configuration* tab will display detailed information on the related network controller, including its MAC address.

- ▶ Note down the new 12-digit MAC address.
- ▶ Press **[Esc]** to exit the BIOS.
- ▶ 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 82](#).
- ▶ 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.

5.2.17 Using the Chassis ID Prom Tool

The Chassis ID EPROM located on the system 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 server blade, system information has to be entered using the *ChassisId_Prom* Tool. The tool and further instructions are available to maintenance personnel from the Fujitsu Technology Solutions Extranet:

<http://partners.ts.fujitsu.com/com/service/intelservers/tools>



For the Japanese market, follow the instructions provided separately.

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/CNA controllers

Please note when re-using a replaced LAN/CNA controller:

- ▶ Confirm with the customer whether the LAN/CNA 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 LAN/CNA controller.

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



For details, refer to the relevant LAN/CNA driver manual.

5.2.18.2 After replacing the server blade

- ▶ Confirm with the customer whether the onboard CNA 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 CNA driver utility after replacing the server blade.



For details, refer to the relevant CNA driver manual.

5.2.19 Switching off the ID indicator

Press the ID button on the front panel or use management blade web interface to switch off the ID indicator after the maintenance task has been concluded successfully.



For further information, refer to section "[Locating the defective server blade](#)" on page 45.

Using the ID button on the front panel

- ▶ Press the ID button on the front panel to switch off the ID indicator.

Using management blade web interface

- ▶ In management blade web interface press the *Locate* button in the status frame to switch on the ID indicator.

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.

6 Hard disk drives / solid state drives

Safety notes



CAUTION!

- The hard disk drive or solid state drive 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 put back in their original places after an upgrade. If this is not done, existing data can be lost.
- The hot-plug function is only possible in conjunction with a corresponding RAID configuration.

Further information about the RAID configuration or RAID level can be found in the RAID controller documentation.

- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Before removing the unit, wait for about 30 seconds until the hard disk drive stops spinning completely.
- When a hard disk drive 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 hard disk drives. If a power failure should occur while the write cache is enabled, cached data may be lost.
- When disposing of, transferring, or returning a hard disk drive or solid state drive, wipe out the data on the drive for your own security.
- Rough handling of hard disk drives may damage the stored data. To cope with any unexpected problems, always back up important data. When backing up data to another hard disk drive, you should make backups on a file or partition basis.
- Be careful not to hit the hard disk drive or bring it into contact with metallic objects.
- Handle the device on a shock and vibration free surface.

Hard disk drives / solid state drives

- Do not use the device in extremely hot or cold locations, or locations with extreme temperature changes.
- Never attempt to disassemble the hard disk drive or solid state drive.
- Follow the safety instructions in chapter ["Important information" on page 31](#).

6.1 Basic information

The hard disk drives or solid state drives which can be ordered for the PRIMERGY BX920 S4 are supplied already mounted in an installation frame so that defective drives can be replaced and new drives can be added during operation. The hard disk drive or solid state drive and the installation frame together make up the HDD module or SSD module.

The server blade is shipped with one of the following configurations:

- configuration with SATA HDD/SSD modules and PCH backplanes
- configuration with SAS HDD/SSD modules, PCH backplanes and onboard controller SAS upgrade via onboard SAS enabling key
- configuration with SAS HDD/SSD modules, SAS backplanes and SAS RAID HDD module without cache (RAID level 0/1). This option requires CPU 2 installed.
- configuration with SAS HDD/SSD modules, SAS backplanes and SAS RAID HDD module with 512 MB cache (RAID level 0/1/1E/10/5/50/6/60). This option requires CPU 2 installed.

Each HDD/SSD module can accommodate a SAS/SATA hard disk drive or SAS/SATA solid state drive 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 SAS RAID HDD modules controlling the HDD/SSD modules see section ["SAS RAID HDD module" on page 143](#).

For information on installing the onboard SAS enabling key see section ["Onboard SAS enabling key" on page 238](#).

6.1.1 General equipping rules

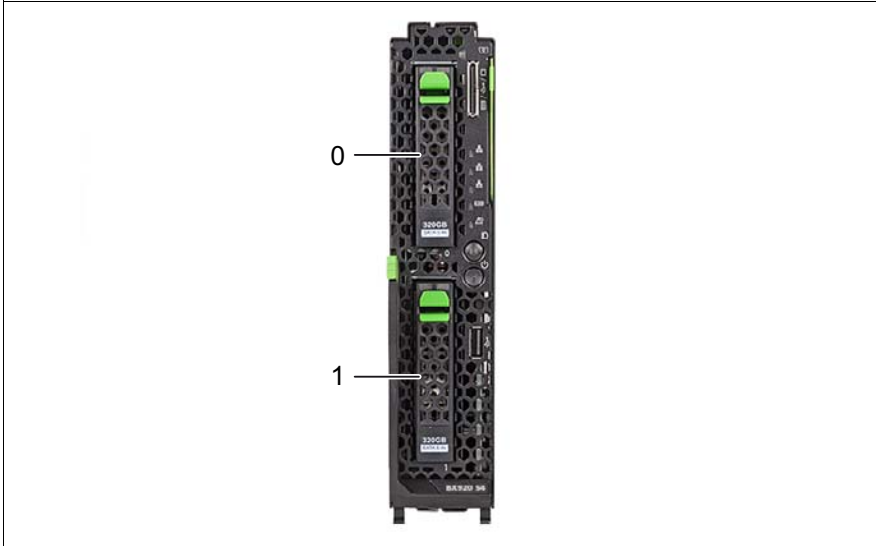


Figure 15: Numbering of HDD/SSD bays

- Solid state drives (SSDs) are always equipped before installing hard disk drives.
- 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.

6.2 Installing a 2.5-inch HDD/SSD module



Customer Replaceable Units (CRU)



Average task duration: 5 minutes

6.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Main steps: tool-less

6.2.2 Preliminary steps

Perform the following procedures:

- ▶ ["Opening the rack door" on page 52](#)
- ▶ When installing an SAS HDD/SSD drive make sure that one of the following conditions is fulfilled
 - SAS HDD/SSD backplanes are installed, see section ["Replacing HDD/SSD backplanes" on page 113](#).
 - PCH HDD/SSD backplanes and onboard SAS enabling key are installed, see section ["Replacing HDD/SSD backplanes" on page 113](#) and section ["Onboard SAS enabling key" on page 238](#).

6.2.3 Removing the 2.5-inch dummy module



Dummy modules protect free bays against environmental impact. Remove the dummy module before installing an additional HDD/SSD module.

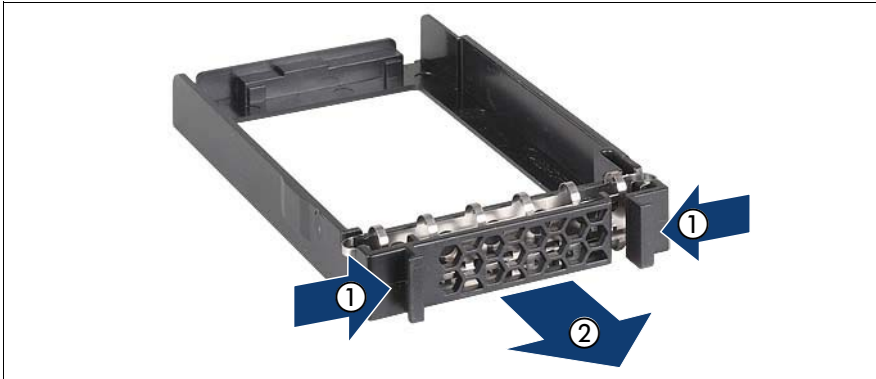


Figure 16: Removing the 2.5-inch dummy module

- ▶ Press both tabs on the dummy module together until the locking mechanism disengages (1).
- ▶ Pull the dummy module out of the bay (2).



CAUTION!

Store the dummy module in a safe place. If you have removed an HDD/SSD module and do not install a new one in its place, put the dummy module back in its place for cooling, to comply with EMC regulations (regulations regarding electromagnetic compatibility), and for protection against fire. Ensure that the dummy module engages correctly in the bay.

6.2.4 Installing the 2.5-inch HDD/SSD module



Figure 17: Unlocking the 2.5-inch HDD/SSD module

- ▶ Release the locking mechanism as follows:
 1. Press the two green tabs of the locking lever together (1).
 2. Push the handle of the HDD/SSD module fully in the direction of the arrow (2). The HDD/SSD module is now unlocked.

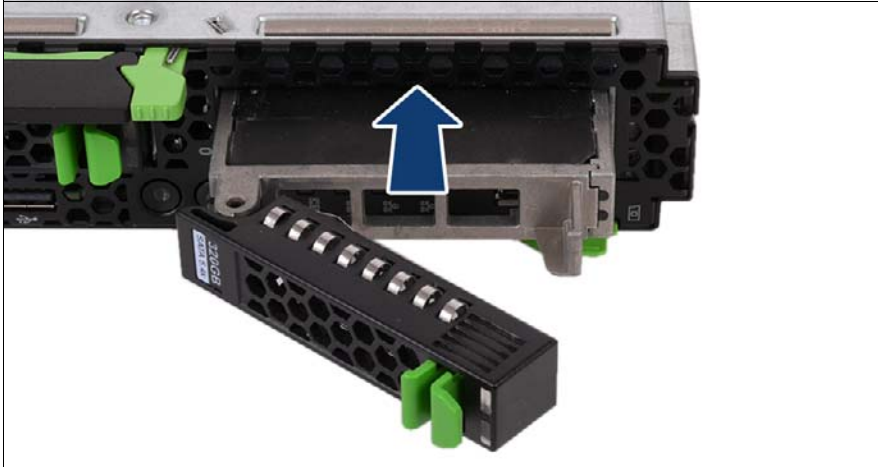


Figure 18: Installing the 2.5-inch HDD/SSD module

- ▶ Carefully push the HDD/SSD module into the empty bay until it stops.



Figure 19: Installing the 2.5-inch HDD/SSD module

- ▶ Push the handle completely in the direction of the arrow until the locking mechanism engages.

6.2.5 Concluding steps

Perform the following procedures:

- ▶ ["Closing the rack door" on page 62](#)
- ▶ If applicable, please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild" on page 94](#)

6.3 Removing a 2.5-inch HDD/SSD module



Customer Replaceable Units (CRU)



Average task duration: 5 minutes



Only applicable for removing non-defective HDD/SSD modules:

- ▶ Set the drive to "Offline" via the software (RAID controller configuration software), before removing an HDD/SSD module that is not defective.

6.3.1 Required tools

- Preliminary and concluding steps: tool-less
- Main steps: tool-less

6.3.2 Preliminary steps

Perform the following procedures:

- ▶ Only applicable for removing intact HDD/SSD modules (for example: preventive exchange in case of S.M.A.R.T.):

Ensure that the HDD/SSD module to be removed is not combined into a RAID array. If the drive is part of a RAID array, you first need to delete the array using ServerView RAID Manager.



CAUTION!

All data on all HDDs/SSDs in the array will be lost! 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, available online.

- ▶ ["Opening the rack door" on page 52](#)

6.3.3 Removing the 2.5-inch HDD/SSD module



Figure 20: Unlocking the 2.5-inch HDD/SSD module

- ▶ Release the locking mechanism as follows:

1. Press the two green tabs of the locking lever together (1).
2. Push the handle of the HDD/SSD module fully in the direction of the arrow (2). The HDD/SSD module is now unlocked.

- ▶ Pull the HDD/SSD module out a few centimeters.
- ▶ Wait for at least 30 seconds.

i This period is necessary for the RAID controller to recognize that an HDD/SSD module has been removed and for the hard disk drive to come to a stop.

- ▶ Pull the HDD/SSD module out completely.

6.3.4 Installing the 2.5-inch dummy module

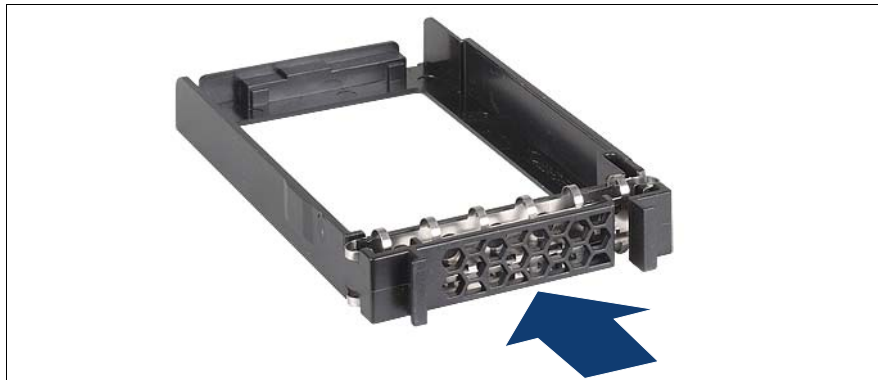


Figure 21: Installing the 2.5-inch dummy module

- ▶ Push the dummy module into the empty bay until it engages.

6.3.5 Concluding steps

Perform the following procedures:

- ▶ ["Closing the rack door" on page 62](#)

6.4 Replacing a 2.5-inch HDD/SSD module



Customer Replaceable Units (CRU)



Average task duration: 5 minutes



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 "[Indicators on the hot-plug HDD/SSD module](#)" on page 265.
- Under no circumstances should you remove an HDD/SSD module while the system is in operation if you are not sure that the drive is operated by a RAID controller and belongs to a disk array that is operating in RAID level 1, 1E, 10, 5, 50, 6 or 60.

An HDD/SSD module can only be replaced during operation in conjunction with a corresponding RAID configuration.
- 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.



Only applicable for removing non-defective HDD/SSD modules:

- ▶ Set the drive to "Offline" via the software (RAID controller configuration software), before removing an HDD/SSD module that is not defective.

6.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Main steps: tool-less

6.4.2 Preliminary steps

Perform the following procedures:

- ▶ ["Opening the rack door" on page 52](#)
- ▶ ["Locating the defective server blade" on page 45](#)
- ▶ ["Locating the defective component" on page 49](#)

6.4.3 Removing the defective 2.5-inch HDD/SSD module

- ▶ Remove the HDD/SSD module as described in section ["Removing the 2.5-inch HDD/SSD module" on page 109](#).

6.4.4 Installing the new 2.5-inch HDD/SSD module

- ▶ Install the HDD/SSD module as described in section ["Installing the 2.5-inch HDD/SSD module" on page 105](#).

6.4.5 Concluding steps

Perform the following procedures:

- ▶ ["Closing the rack door" on page 62](#)
- ▶ If applicable, please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild" on page 94](#)

6.5 Replacing HDD/SSD backplanes



Field Replaceable Units (FRU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes

6.5.1 Required tools

- Preliminary and concluding steps: tool-less
- Replacing the SAS backplane:
 - Phillips PH2 / (+) No. 2 screw driver

6.5.2 Preliminary steps

Before replacing a HDD/SSD backplane, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.
- ▶ Remove the HDD/SSD module from the relevant bay as described in section "[Removing the 2.5-inch HDD/SSD module](#)" on page 109.

6.5.3 Removing the HDD/SSD backplane

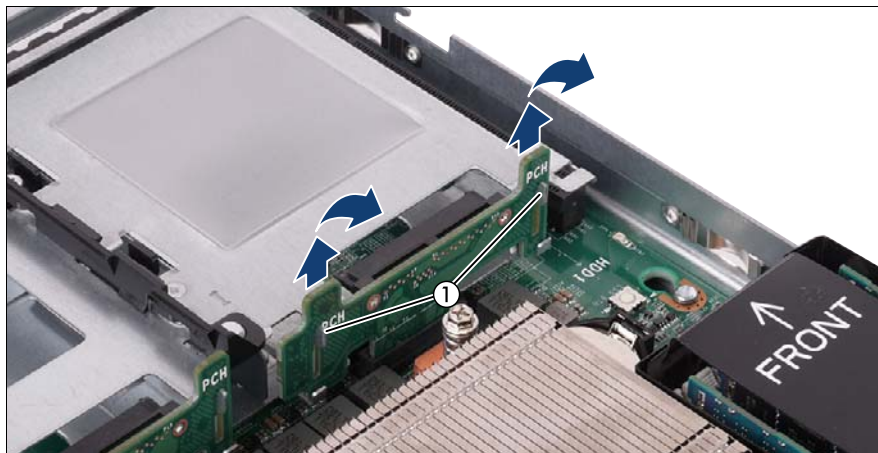


Figure 22: Removing the HDD/SSD backplane

- ▶ Lift the HDD/SSD backplane up and remove it from the fixing brackets (1).

6.5.4 Installing the HDD/SSD backplane

There are two variants of HDD/SSD backplanes available, PCH and SAS backplanes. While PCH backplanes are used to connect SATA drives, SAS backplanes can be used to connect to SAS drives.

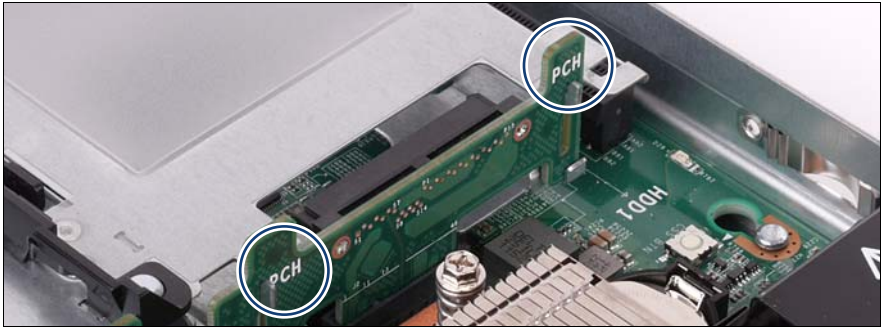


Figure 23: Labeling of a PCH HDD/SSD backplane



Both backplane variants have the same form factor, so note the labeling (see ovals).

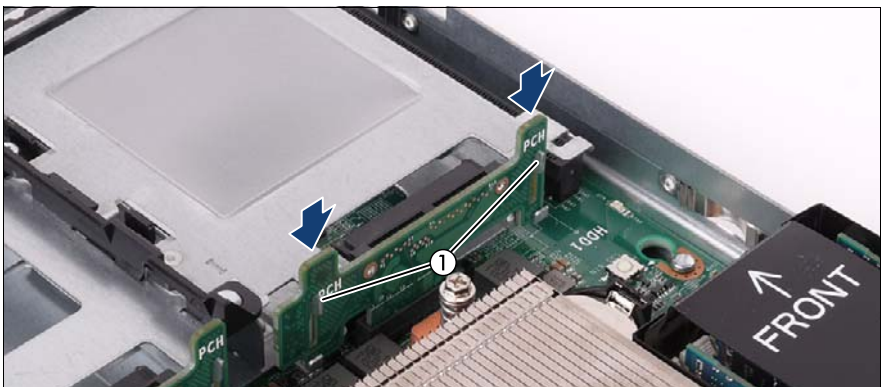


Figure 24: Installing the HDD/SSD backplane

- ▶ Lift the HDD/SSD backplane over the fixing brackets (1).
- ▶ Press the HDD/SSD backplane into the slot (see arrows).

6.5.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Reinstall the HDD/SSD drive as described in section ["Installing a 2.5-inch HDD/SSD module" on page 103](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

7 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 blade remain hot after shutdown. After shutting down the server blade, 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 31.

7.1 Mezzanine cards

7.1.1 Basic information

One or two mezzanine cards can be installed in a BX920 S4 server blade. Additional Fibre Channel, SAS, Ethernet and/or Infiniband I/O channels can be set up using these cards.

All mezzanine cards have the same form factor.



Figure 25: Sample of a 8 Gbit/s fibre-channel card with 2 ports

The mezzanine cards are fastened on a special carrier and then connected together with the carrier to the system board.

The figure below shows the two kinds of unpopulated carriers for mezzanine cards. All installation/removal procedures are identical for both carriers.

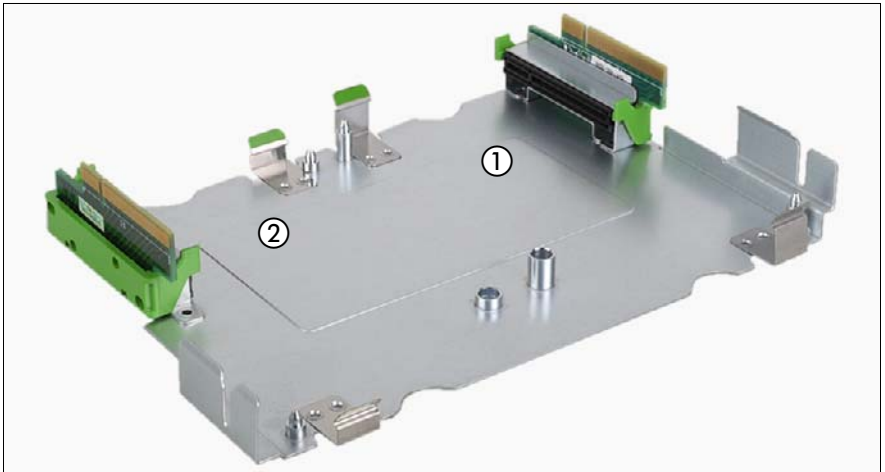


Figure 26: Carrier for mezzanine cards with two "x8" riser cards

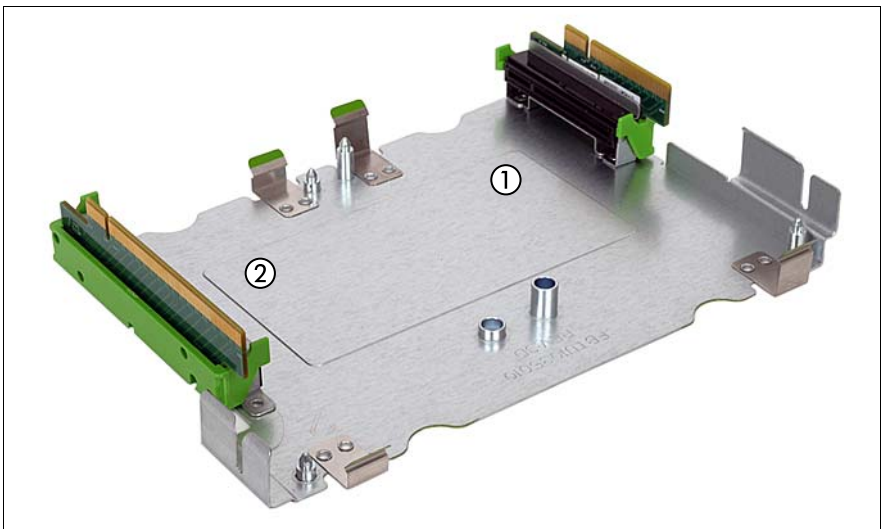


Figure 27: Carrier for mezzanine cards with one "x8" and one "x16" (2) riser card



Note the numbering of the mezzanine card slots.

7.1.1.1 Installing riser cards

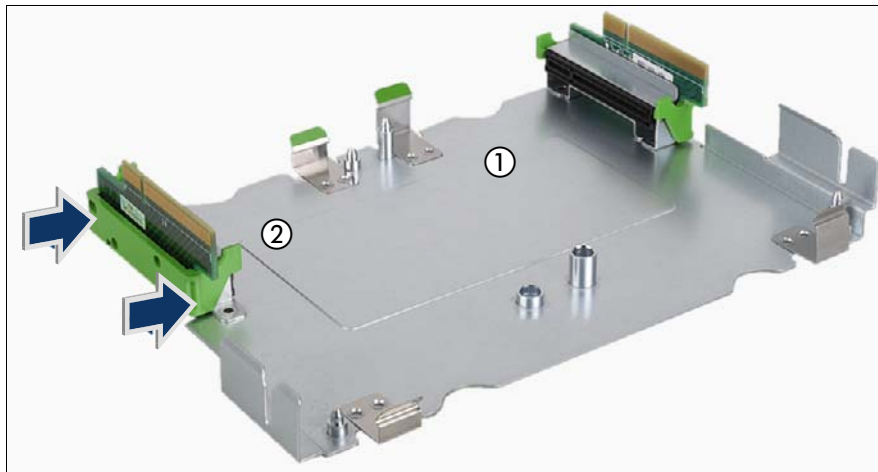


Figure 28: Installing the riser card x8

- ▶ Connect the riser card to the carrier. Make sure that the green clips click into place.

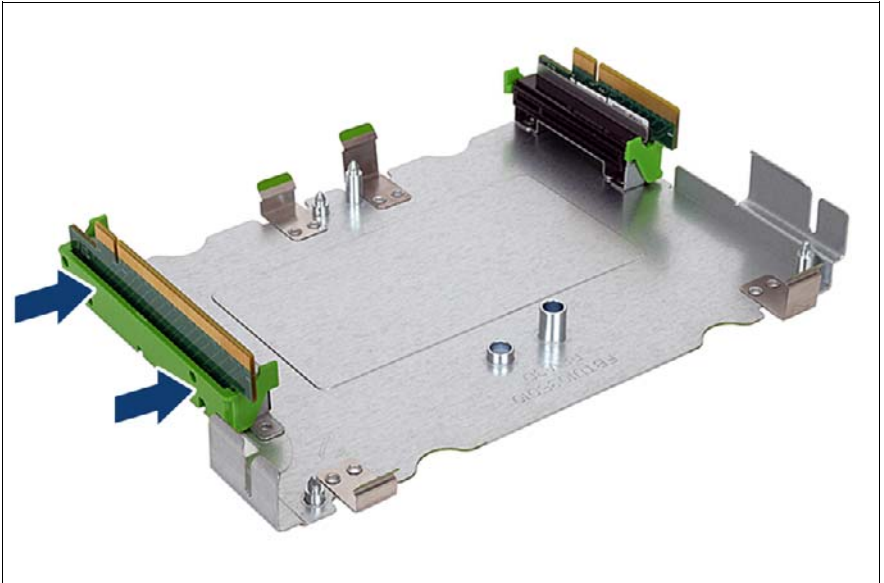


Figure 29: Installing the riser card x16

- ▶ Connect the riser card to the carrier. Make sure that the green clips click into place.

7.1.1.2 Removing riser cards

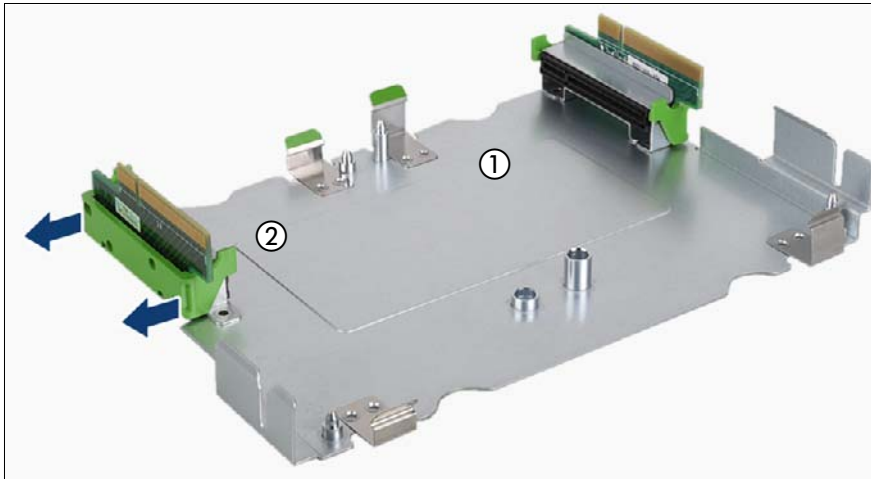


Figure 30: Removing the riser card x8

- ▶ Remove the riser card from the holder at the slot of mezzanine card 2.

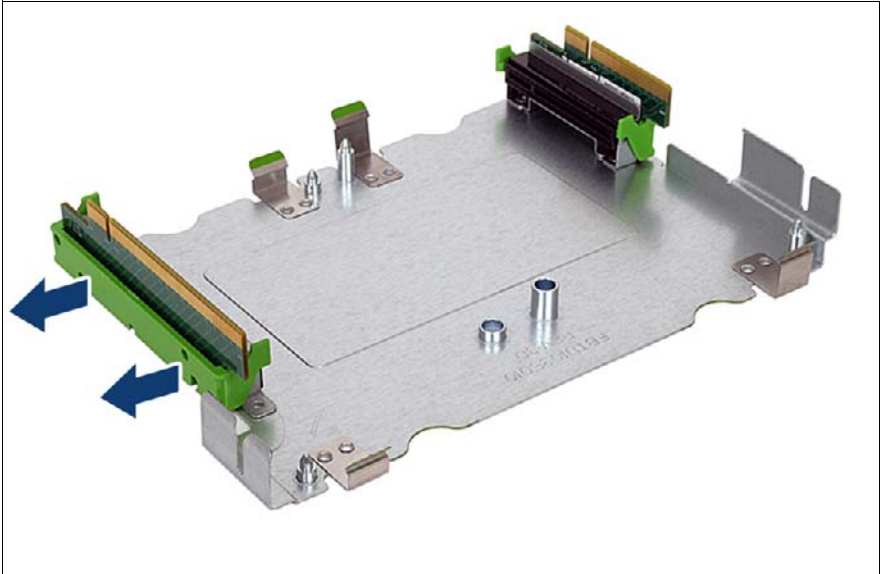


Figure 31: Removing the riser card x16

- ▶ Remove the riser card from the holder.

7.1.1.3 Population rules for mezzanine cards

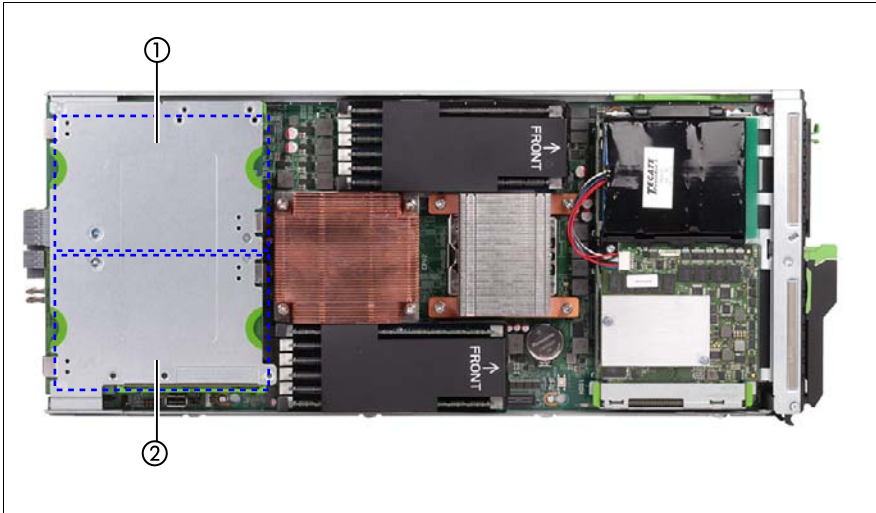


Figure 32: Slot numbering for mezzanine cards

The slots of the mezzanine cards in the server blade are connected to certain connection blade slots on the back of the system unit. You therefore need to observe how the connection blade slots are populated on the back of the system unit when installing mezzanine cards.

Population rules for mezzanine cards in the BX900 S1/S2 system unit



Figure 33: Connection blade slots

The table below shows the connections of the connection blade slots to the slots of the mezzanine cards.

System unit		Server blade	Mezzanine card
Connection blade slots			
Fabric 1	CB1: 1Gb Ethernet or 10 Gb Ethernet	CB2: 1Gb Ethernet or 10Gb Ethernet	Onboard CNA-controller - - -
Fabric 2	CB3: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or Infiniband (CB3/4)	CB4: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or Infiniband (CB3/4)	Mezzanine card 1 Eth 1Gb 4port or Eth 10Gb 2port FC 8Gb 2port or IB 40/56 Gb 2port
Fabric 3	CB5: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or SAS or Infiniband (CB5/6)	CB6: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or SAS or Infiniband (CB5/6)	Mezzanine card 2 Eth 1Gb 4port or Eth 10Gb 2port FC 8Gb 2port or SAS or IB 40/56 Gb 2port
Fabric 4	CB7: 1Gb Ethernet or Infiniband (CB7/8)	CB8: 1Gb Ethernet or Infiniband (CB7/8)	Eth 1Gb 4port or IB 40/56 Gb 2port

Table 4: Fitting rules for connection blade slots

i Connection blades within one fabric must have the same technology, i.e. either Ethernet or Fibre Channel or Infiniband.

When installing the different types of mezzanine cards, make sure that the slots in fabrics 2, 3 and 4 of the system unit are fitted with the appropriate connection blades.

The following rules apply for fitting the mezzanine card slots of the server blades:

- If a 1 Gb Ethernet mezzanine card is installed in slot 1 of a server blade, at least one 1 Gb Ethernet connection blade must be installed in fabric 2 of the system unit.
- If a 10 Gb Ethernet mezzanine card or a 10Gb CNA mezzanine card is installed in slot 1 of a server blade, at least one 10 Gb Ethernet connection blade must be installed in fabric 2 of the system unit.

Expansion cards and backup units

- If an FC mezzanine card is installed in slot 1, at least one FC connection blade must be installed in fabric 2.
- If an Infiniband mezzanine card is installed in slot 1, an Infiniband connection blade must be installed in fabric 2.



In this case, only one of two channels of the Infiniband mezzanine card is used.

- If a 1 Gb Ethernet mezzanine card is installed in slot 2 of a server blade, at least one 1 Gb Ethernet connection blade must be installed in fabric 3 or in fabric 4 of the system unit.
- If a 10 Gb Ethernet mezzanine card or a 10Gb CNA mezzanine card is installed in slot 2 of a server blade, at least one 10 Gb Ethernet connection blade must be installed in fabric 3 of the system unit.
- If an FC mezzanine card is installed in slot 2, at least one FC connection blade must be installed in fabric 3.
- If an Infiniband mezzanine card is installed in slot 2, Infiniband connection blades should be installed in fabrics 3 and 4.



In this case, both channels of the Infiniband mezzanine card are used.

- If a SAS Expander mezzanine card is installed in slot 2, at least one SAS connection blade must be installed in fabric 3.
- You can install combinations of FC, Ethernet, Infiniband and SAS mezzanine cards in a server blade. In this case, the mezzanine card slots may be equipped as follows:

Mezzanine slot 1	Mezzanine slot 2
1 Gb Ethernet	10 Gb Ethernet / 10 Gb CNA
1 Gb Ethernet	Fibre Channel
1 Gb Ethernet	Infiniband
1 Gb Ethernet	SAS Expander
10 Gb Ethernet / 10 Gb CNA	Fibre Channel
10 Gb Ethernet / 10 Gb CNA	Infiniband
10 Gb Ethernet / 10 Gb CNA	SAS Expander
Fibre Channel	Infiniband
Fibre Channel	SAS Expander
Infiniband	SAS Expander

Table 5: Allowed combinations of different mezzanine cards

i The SAS Expander mezzanine card requires SAS RAID HDD module installed to establish connection to SAS connection blade, see section "SAS RAID HDD module" on page 143.

For the latest information on supported expansion cards, refer to your server's hardware configurator available online at the following address:

for the EMEA market:

http://ts.fujitsu.com/products/standard_servers/tower/primergy_bx920s3.html

for the Japanese market:

<http://jp.fujitsu.com/platform/server/primergy/system/>

Population rules for mezzanine cards in the BX400 S1 system unit

The connection blade slots of the BX400 S1 system unit are numbered as follows.



Figure 34: Connection blade slots (BX400 S1 system unit)

The table below shows the connections of the connection blade slots to the slots for mezzanine cards.

Server blade	Midplane	Connection blade slots	
Onboard CNA	Fabric 1	CB1:	1 or 10 Gb Ethernet
Mezzanine card slot 1	Fabric 2	CB2:	1 or 10 Gb Ethernet or Fibre Channel
Mezzanine card slot 2	Fabric 3	CB3:	1 or 10 Gb Ethernet or Fibre Channel or SAS
		CB4:	1 or 10 Gb Ethernet or Fibre Channel or SAS or Infiniband

Table 6: Fitting rules for connection blade slots (BX400 S1 system unit)



Connection blades within one fabric must have the same technology, i.e. either Ethernet or Fibre Channel or Infiniband.

As a result, the rules for populating the mezzanine card slots are as follows:

- If a 1 Gb Ethernet mezzanine card is installed in slot 1 of a server blade, at least one 1 Gb Ethernet connection blade must be installed in CB slot 2 of the system unit.
- If a 10 Gb Ethernet mezzanine card or a 10Gb CNA mezzanine card is installed in slot 1 of a server blade, at least one 10 Gb Ethernet connection blade must be installed in CB slot 2 of the system unit.

- If an FC mezzanine card is installed in slot 1, at least one FC connection blade must be installed in CB slot 2 of the system unit.
- If a 1 Gb Ethernet mezzanine card is installed in slot 2 of a server blade, at least one 1 Gb Ethernet connection blade must be installed in CB slot 3 or in CB slot 4 of the system unit.
- If a 10 Gb Ethernet mezzanine card or a 10Gb CNA mezzanine card is installed in slot 2 of a server blade, at least one 10 Gb Ethernet connection blade must be installed in CB slot 3 or in CB slot 4 of the system unit.
- If an FC mezzanine card is installed in slot 2, at least one FC connection blade must be installed in CB slot 3 or in CB slot 4 of the system unit.
- If an Infiniband mezzanine card is installed in slot 2, an Infiniband connection blade must be installed in CB slots 3 and 4 of the system unit.
- If a SAS Expander mezzanine card is installed in slot 2, at least one SAS connection blade must be installed in fabric 3.
- You can install a combination of FC, Ethernet and Infiniband mezzanine cards in a server blade. In this case, the Ethernet mezzanine card should be installed in slot 1 and the FC or Infiniband mezzanine card in slot 2 of the server blade.

7.1.2 Installing mezzanine cards



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.1.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing mezzanine cards: tool-less

7.1.2.2 Preliminary steps

Before installing an expansion card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ When installing a SAS Expander mezzanine card make sure, that an SAS RAID HDD module is installed as described in section ["Installing the SAS RAID HDD module" on page 144](#).

7.1.2.3 Installing a mezzanine card

The following section illustrates how to install a mezzanine card in slot 2.

Removing the mezzanine cards carrier

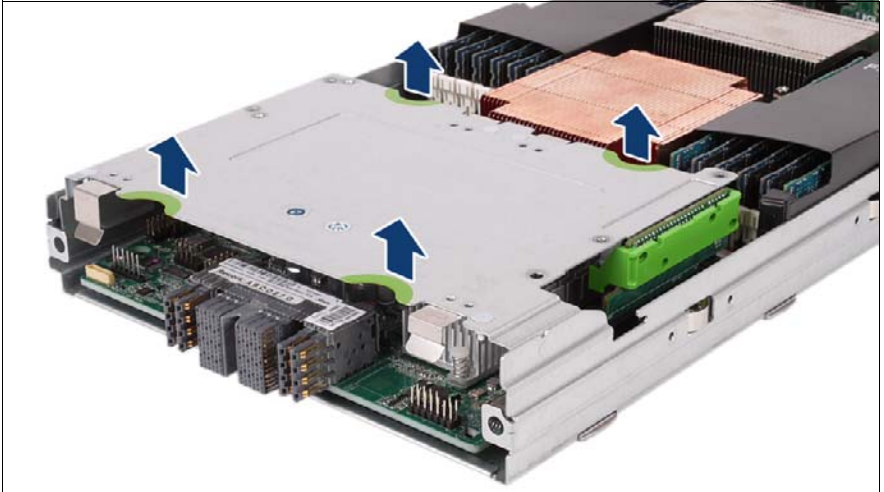


Figure 35: Removing the mezzanine cards carrier

- ▶ Remove the mezzanine cards carrier from the server blade housing by lifting it up, keeping it as horizontal as possible.

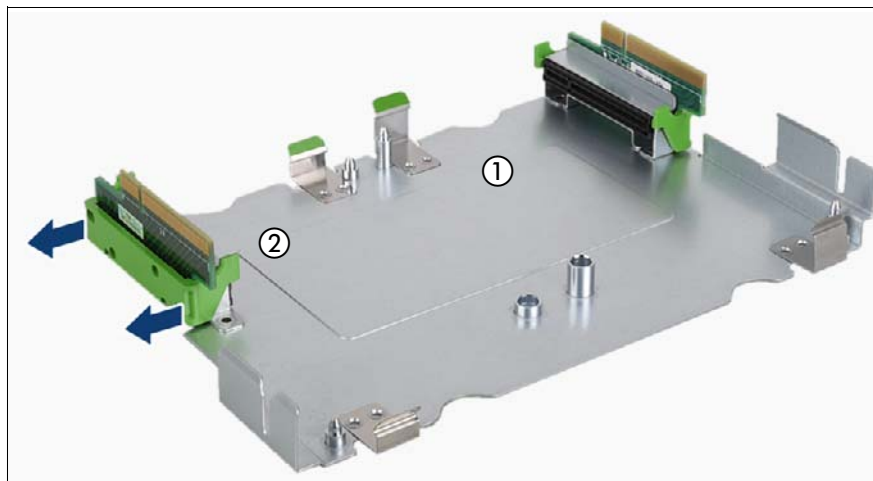


Figure 36: Removing the riser card

- ▶ Remove the riser card from the holder at the slot of mezzanine card 2.

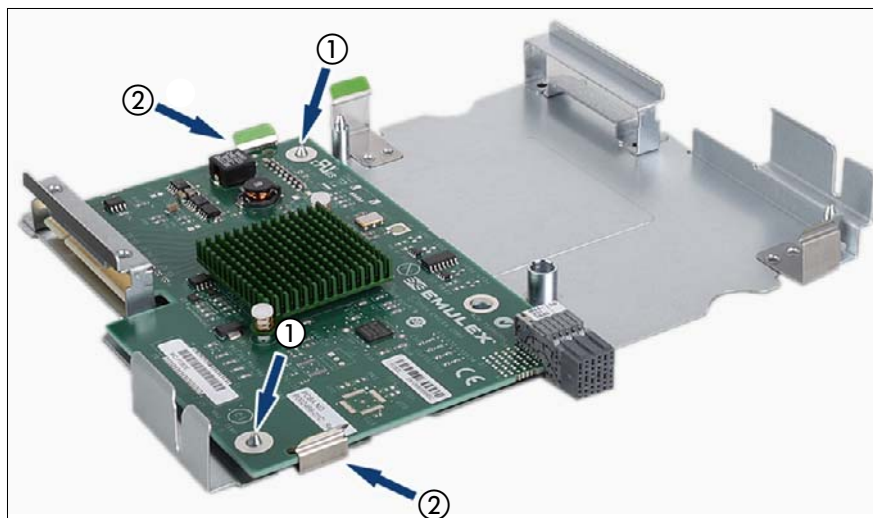


Figure 37: Inserting the mezzanine card

- ▶ Place the mezzanine card on the two guide pins (1) at the slot of mezzanine card 2 and press the mezzanine card down so that it clicks into place between the two clips (2).

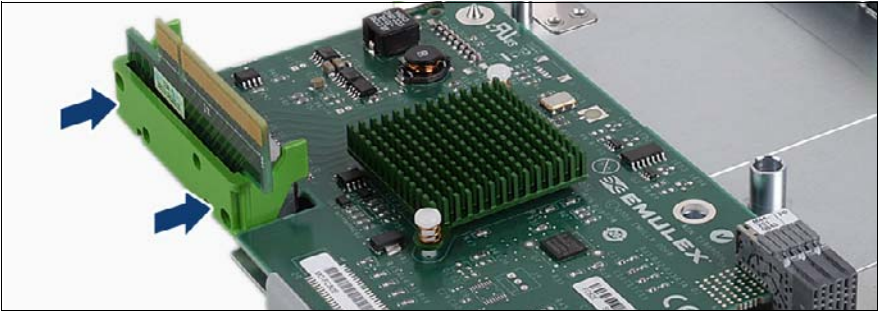


Figure 38: Reconnecting the riser card

- ▶ Connect the riser card to the mezzanine card. Make sure that the green clips click into place.

i Mezzanine card 1 is fastened to the carrier with the component side facing downward. Mezzanine card 1 is otherwise installed in the same way as mezzanine card 2.

Installing the mezzanine card carrier

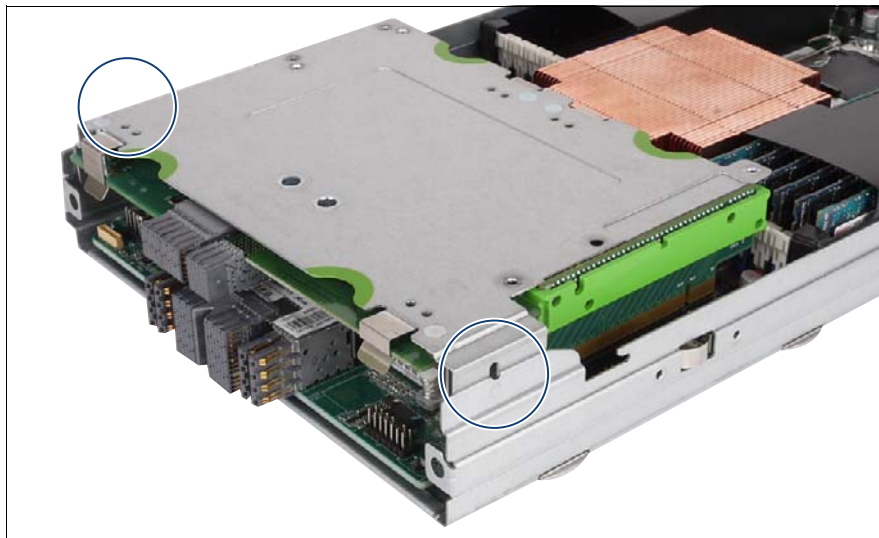


Figure 39: Installing the mezzanine cards carrier

- ▶ Install the carrier with the mezzanine cards in the server blade housing. As you do this, the riser cards are inserted in the corresponding system board slots. Make sure that the coding on the carrier matches that on the server blade housing.

7.1.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Update the firmware as described in section ["Updating mezzanine card firmware" on page 80](#).
- ▶ In order to configure a mezzanine card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. For SAN / iSCSI boot the card's Option ROM has to be enabled permanently. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ If applicable, restore LAN teaming configurations as described in section ["Configuring LAN teaming" on page 96](#).

7.1.3 Removing mezzanine cards



Upgrade and Repair Units (URU)



average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.1.3.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing expansion cards: tool-less

7.1.3.2 Preliminary steps

Before removing an expansion card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

7.1.3.3 Removing a mezzanine card

The following section illustrates how to remove a mezzanine card in slot 2.

Removing the mezzanine card carrier

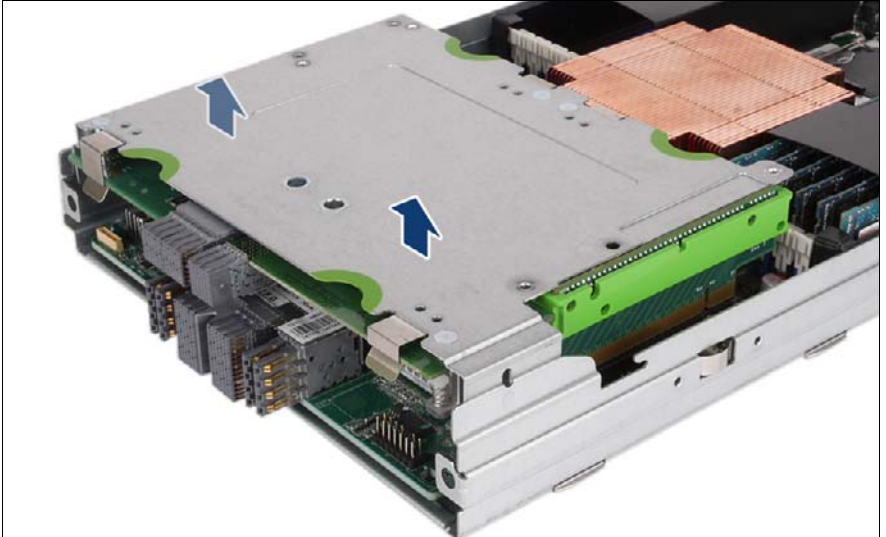


Figure 40: Removing the mezzanine cards carrier

- ▶ Remove the carrier from the server blade housing by lifting it up, keeping it as horizontal as possible.

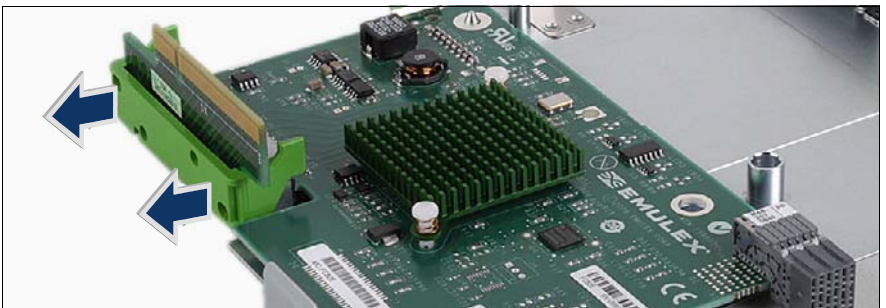


Figure 41: Removing the riser card

- ▶ Remove the riser card from the holder at the slot of mezzanine card 2.

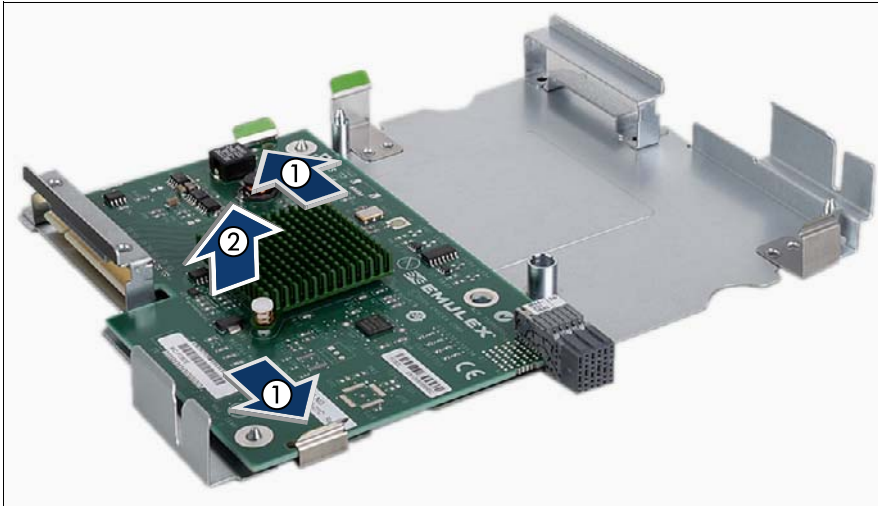


Figure 42: Removing the mezzanine card

- ▶ Press the two clips (1) and remove the mezzanine card (2).

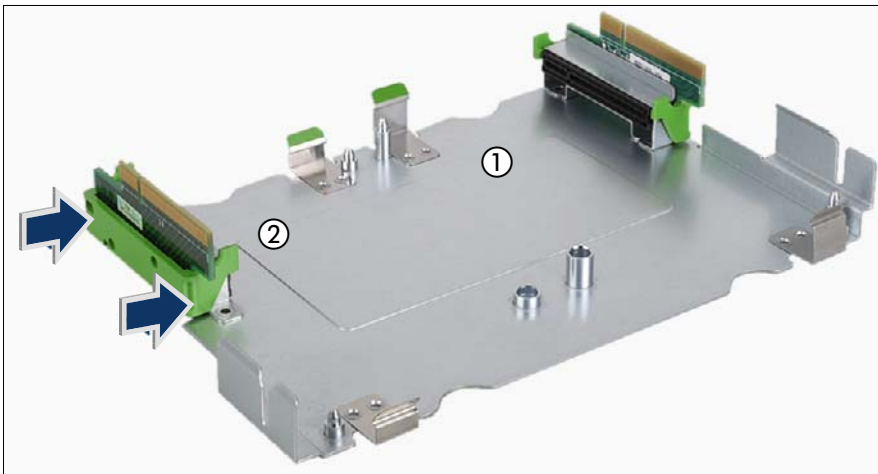


Figure 43: Reconnecting the riser card

- ▶ Connect the riser card to the mezzanine card. Make sure that the green clips click into place.

7.1.3.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ In order to configure a mezzanine card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. For SAN / iSCSI boot the card's Option ROM has to be enabled permanently. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ If applicable, restore LAN teaming configurations as described in section ["After replacing / upgrading LAN/CNA controllers" on page 96](#).

7.1.4 Replacing mezzanine cards



Upgrade and Repair Units (URU)



average hardware task duration: 10 minutes



Average software task duration: 5 minutes

7.1.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Replacing expansion cards: tool-less

7.1.4.2 Preliminary steps



Note on network settings recovery

When replacing network controllers or onboard CNA, 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 the controller.

Before replacing an mezzanine card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).

- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ Locate the defective mezzanine card using the onboard Local Diagnostic LEDs as described in section ["Onboard indicators and controls" on page 260](#).

7.1.4.3 Removing a mezzanine card

- ▶ Remove the defective mezzanine card as described in section ["Removing a mezzanine card" on page 137](#).

7.1.4.4 Installing a mezzanine card

- ▶ Install the new mezzanine card as described in section ["Installing a mezzanine card" on page 131](#).

7.1.4.5 Concluding steps



If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard CNA). For further information, please refer to section ["Note on network settings recovery" on page 140](#).

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Enable the PCI slot of the replaced mezzanine card as described in section ["Enabling replaced components in the system BIOS" on page 87](#).
- ▶ Inform the customer about changed WWN and MAC addresses. For further information, refer to section ["Looking up changed MAC / WWN addresses" on page 94](#).

Expansion cards and backup units

- ▶ After replacing a network controller in a server blade running Linux OS, update its MAC address in the related NIC definition file as described in section ["Updating the NIC configuration file in a Linux environment" on page 91](#).
- ▶ Update the firmware as described in section ["Updating mezzanine card firmware" on page 80](#).
- ▶ In order to configure a mezzanine card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. For SAN / iSCSI boot the card's Option ROM has to be enabled permanently. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ If applicable, restore LAN teaming configurations as described in section ["After replacing / upgrading LAN/CNA controllers" on page 96](#).

7.2 SAS RAID HDD module

7.2.1 Basic information

A SAS RAID HDD module can be installed in a BX920 S4 server blade to provide SAS RAID connections to SAS HDD/SSD drives. The SAS RAID HDD module is also used to establish connection to the SAS connection blade via SAS Expander mezzanine card, see section ["Mezzanine cards" on page 118](#). Two SAS RAID HDD module variants are available.

- SAS RAID HDD module without cache (RAID level 0/1).
- SAS RAID HDD module with 512 MB cache (RAID level 0/1/1E/10/5/50/6/60) with Flash Backup Unit (FBU) option

i Both SAS RAID HDD module variants require SAS HDD/SSD backplanes and CPU 2 installed, see section ["Replacing HDD/SSD backplanes" on page 113](#) and ["Installing processors" on page 184](#).

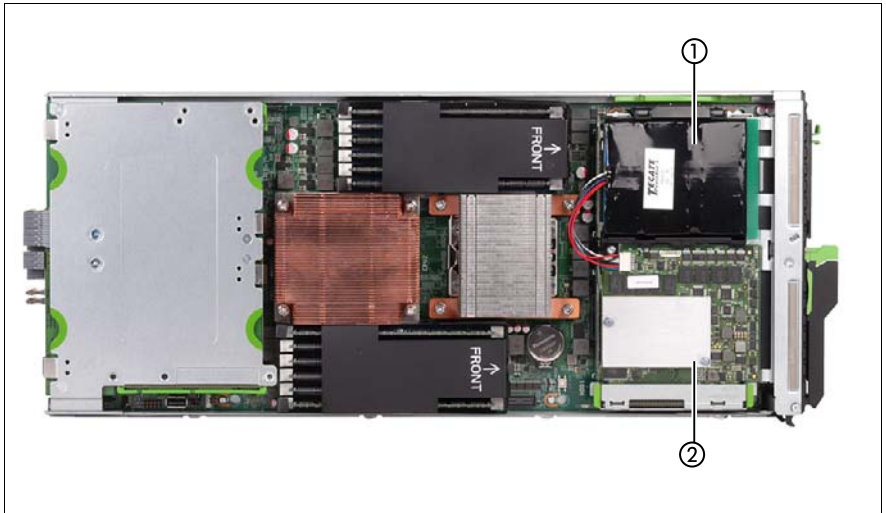


Figure 44: Mounting place for SAS RAID HDD module and FBU

- 1 FBU (Flash Backup Unit)
- 2 SAS RAID HDD module with 512 MB cache

7.2.2 Installing the SAS RAID HDD module



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing SAS RAID HDD module: tool-less

7.2.2.2 Preliminary steps

Before installing the SAS RAID HDD module card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

7.2.2.3 Installing the SAS RAID HDD module

i The following procedure is identical for both variants of SAS RAID HDD modules.

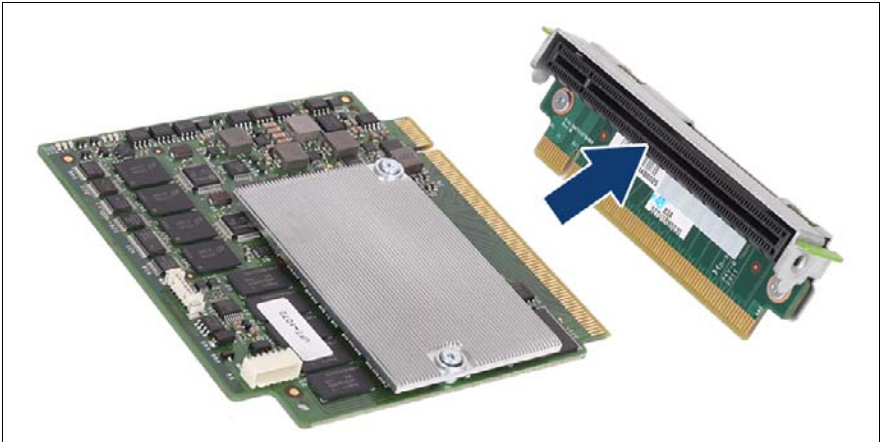


Figure 45: Connecting the SAS RAID HDD module to the riser card

- ▶ Connect the SAS RAID HDD module to the riser card.

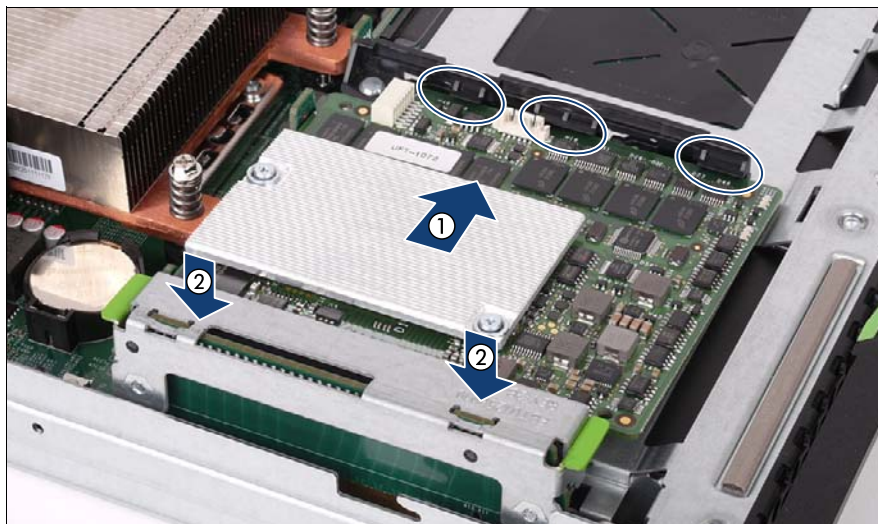


Figure 46: Installing the SAS RAID HDD module

- ▶ Push the SAS RAID HDD module under the three plastic catches of the holder (see ovals) (1).
- ▶ Connect the riser card to the SAS connector on the system board (2).

7.2.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ After installing or replacing an SAS RAID HDD module, update the firmware as described in section ["Updating mezzanine card firmware" on page 80](#).
- ▶ In order to configure an SAS RAID HDD module that has been installed or replaced, the module's Option ROM has to be enabled in the system board BIOS. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).

- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ Please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild" on page 94](#).

7.2.3 Removing the SAS RAID HDD module



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.3.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing SAS RAID HDD module: tool-less

7.2.3.2 Preliminary steps

Before removing the SAS RAID HDD module card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).

Expansion cards and backup units

- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit"](#) on page 55.
- ▶ Open the server blade as described in section ["Opening the server blade"](#) on page 56.

7.2.3.3 Removing the SAS RAID HDD module

i The following procedure is identical for both variants of SAS RAID HDD modules.

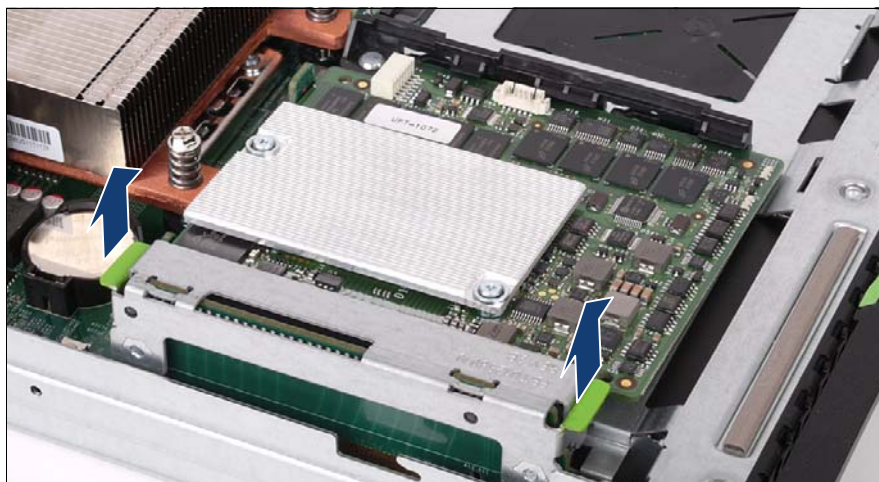


Figure 47: Removing the SAS RAID HDD module

- ▶ Remove the SAS RAID HDD module together with the riser card from the system board.

7.2.3.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade"](#) on page 57.
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit"](#) on page 58.
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality"](#) on page 86.

- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality"](#) on page 93.
- ▶ Please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild"](#) on page 94.

7.2.4 Replacing the SAS RAID HDD module



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing SAS RAID HDD module: tool-less

7.2.4.2 Preliminary steps

Before removing the SAS RAID HDD module card, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

7.2.4.3 Replacing the SAS RAID HDD module



The following procedure is identical for both variants of SAS RAID HDD modules.

- ▶ Remove the defective SAS RAID HDD module as described in section ["Removing the SAS RAID HDD module" on page 147](#).
- ▶ Install the new SAS RAID HDD module as described in section ["Installing the SAS RAID HDD module" on page 144](#).

7.2.4.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ After installing or replacing an SAS RAID HDD module, update the firmware as described in section ["Updating mezzanine card firmware" on page 80](#).
- ▶ In order to configure an SAS RAID HDD module that has been installed or replaced, the module's Option ROM has to be enabled in the system board BIOS. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ Please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild" on page 94](#).

7.2.5 Installing the FBU (Flash Backup Unit)



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.5.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing FBU: tool-less

7.2.5.2 Preliminary steps

Before installing the FBU, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

7.2.5.3 Installing the FBU

i The FBU requires the SAS RAID HDD module with 512 MB cache installed, see section "[SAS RAID HDD module](#)" on page 143.

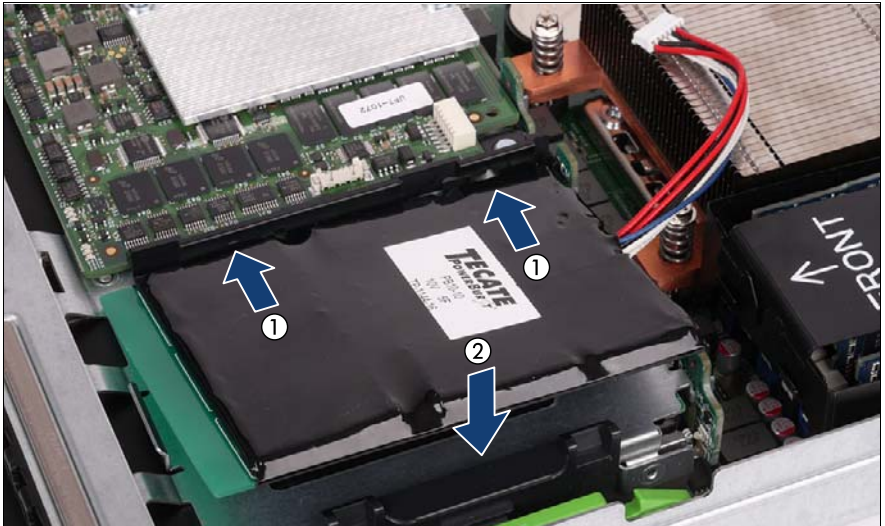


Figure 48: Installing the FBU

- ▶ Slide the FBU module to the frame rail (1).
- ▶ Fold down the FBU (2). The FBU clicks into place in its final position.

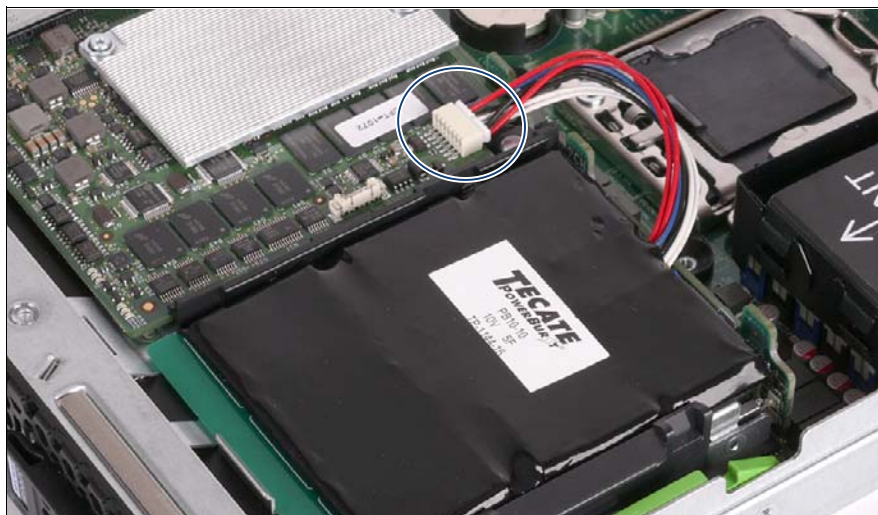


Figure 49: Connecting the FBU

- ▶ Connect the FBU to the SAS RAID HDD module (see circle).

7.2.5.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

7.2.6 Removing the FBU (Flash Backup Unit)



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.6.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing FBU: tool-less

7.2.6.2 Preliminary steps

Before removing the FBU, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

7.2.6.3 Removing the FBU

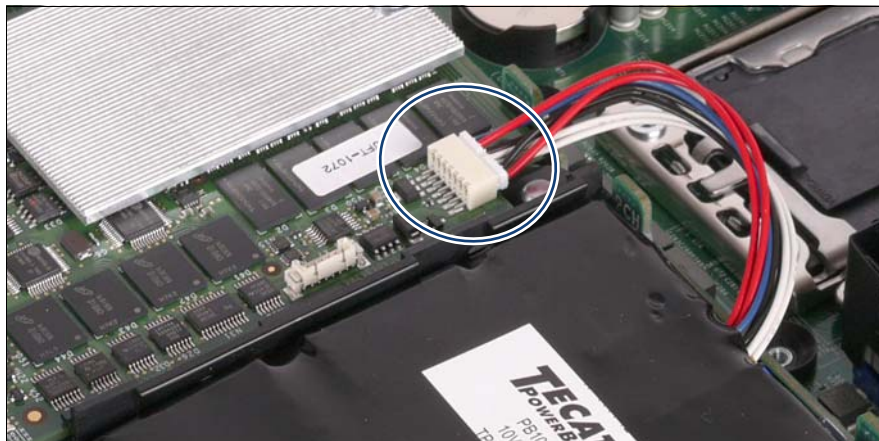


Figure 50: Connecting the FBU

- ▶ Disconnect the FBU from the SAS RAID HDD module (see circle).

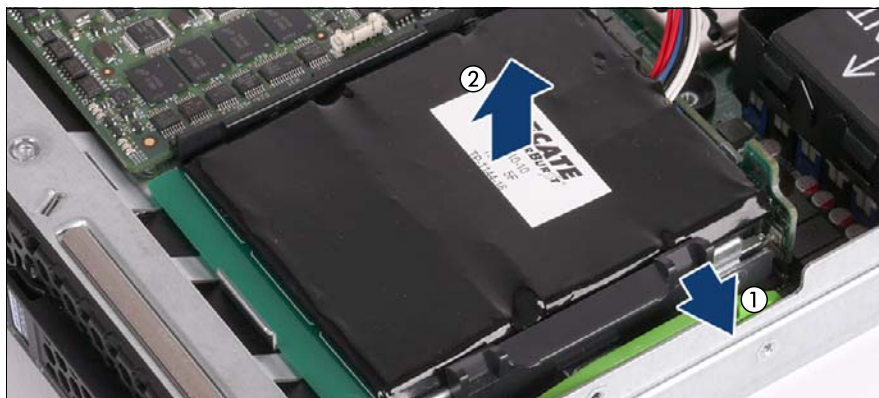


Figure 51: Installing the FBU

- ▶ Unclasp the plastic bracket (1) and remove the FBU (2).

7.2.6.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

7.2.7 Replacing the FBU (Flash Backup Unit)



Upgrade and Repair Units (URU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

7.2.7.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing FBU: tool-less

7.2.7.2 Preliminary steps

Before replacing the FBU, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

7.2.7.3 Removing the FBU

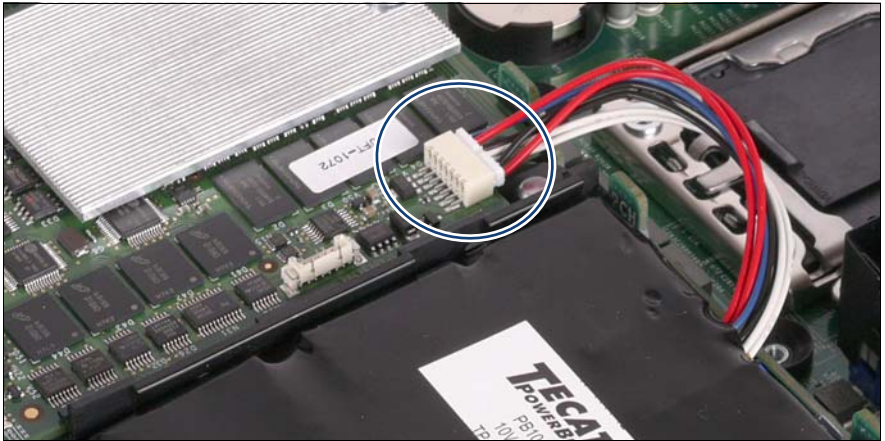


Figure 52: Connecting the FBU

- ▶ Disconnect the defective FBU from the SAS RAID HDD module (see circle).

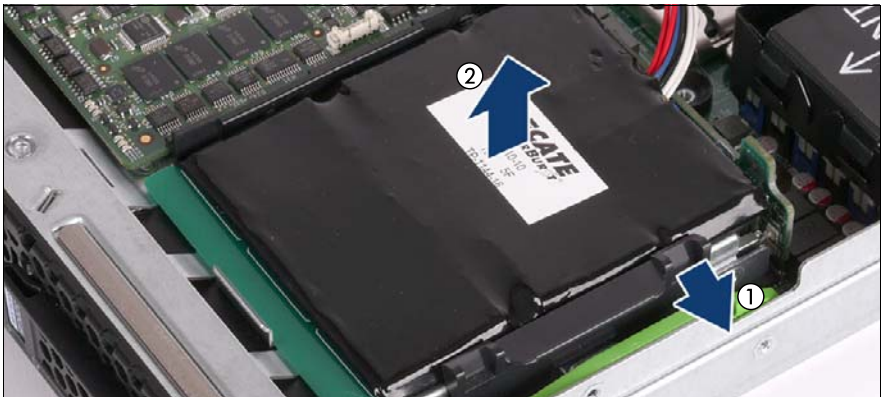


Figure 53: Installing the FBU

- ▶ Unclasp the plastic bracket (1) and remove the defective FBU (2).

7.2.7.4 Installing the FBU

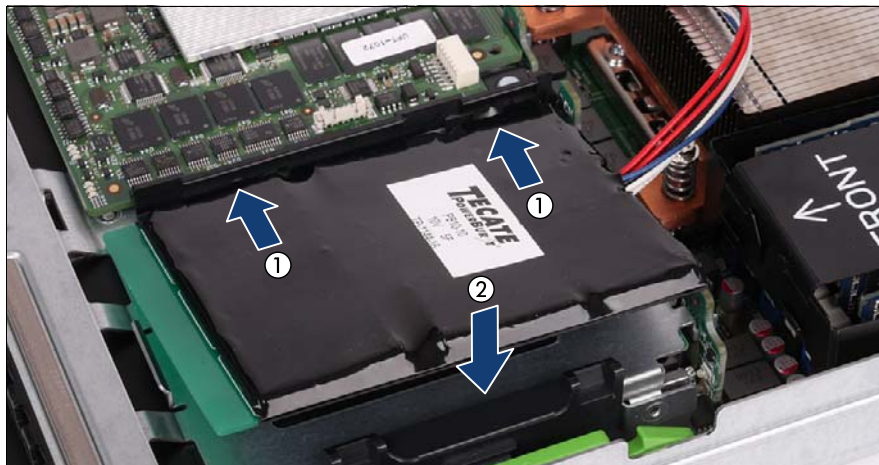


Figure 54: Installing the FBU

- ▶ Slide the FBU module to the frame rail (1).
- ▶ Fold down the FBU (2). The FBU clicks into place in its final position.

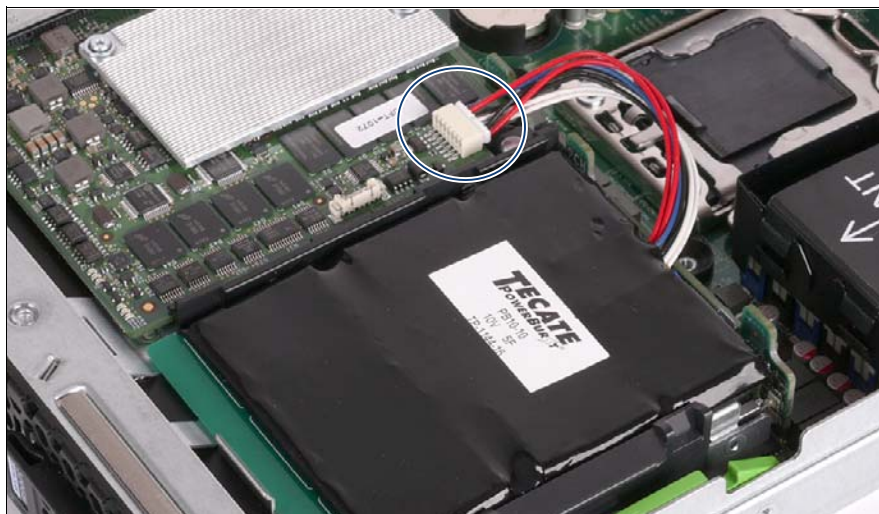


Figure 55: Connecting the FBU

- ▶ Connect the FBU to the SAS RAID HDD module (see circle).

7.2.7.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

8 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 164.
- 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 31.

8.1 Basic information

- The system board is equipped with 12 memory connectors (6 connectors per CPU).
- In mono processor configurations only 6 memory connectors are usable.
- The system has to be equipped with at least one memory module per processor.
- Supported capacities: 4 GB, 8 GB, 16 GB, 32 GB or 64 GB
- Maximum amount of RAM: 768 GB
- Supported memory modules:

Type		Ranking ¹				Error Correction
		1R	2R	4R	8R	
DDR3-1333 PC3-12800	RDIMMs (Registered DIMMs)	x	x	x		ECC or non-ECC
DDR3-1600 PC3-14900	LRDIMMs (Load-Reduced DIMMs)			x	x	

¹ 1R: Single-Rank, 2R: Dual-Rank, 4R: Quad-Rank, 8R: Octa Rank

8.1.1 Memory sequence

8.1.1.1 Population rules

- Populate memory slot 1 / channel A (DIMM 1A) first.
- In case of dual processor configurations, populate memory slot 1 / channel D (DIMM 1D) second.
- Within all channels, memory slot 1 must be populated prior to slot 2.
- If memory modules with different ranks are used, always populate the higher number rank DIMM first (starting from slot 1).
- If memory modules with different capacities are used:
 - Populate modules with higher capacities first.

- Within a channel, populate modules in descending order of capacity.
- If memory modules with different speeds are used, the lowest clock rate applies for all DIMMs.

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.

- Mixing RDIMMs or LRDIMMs is not allowed.
- Mixing ECC and non-ECC DIMMs is not allowed.

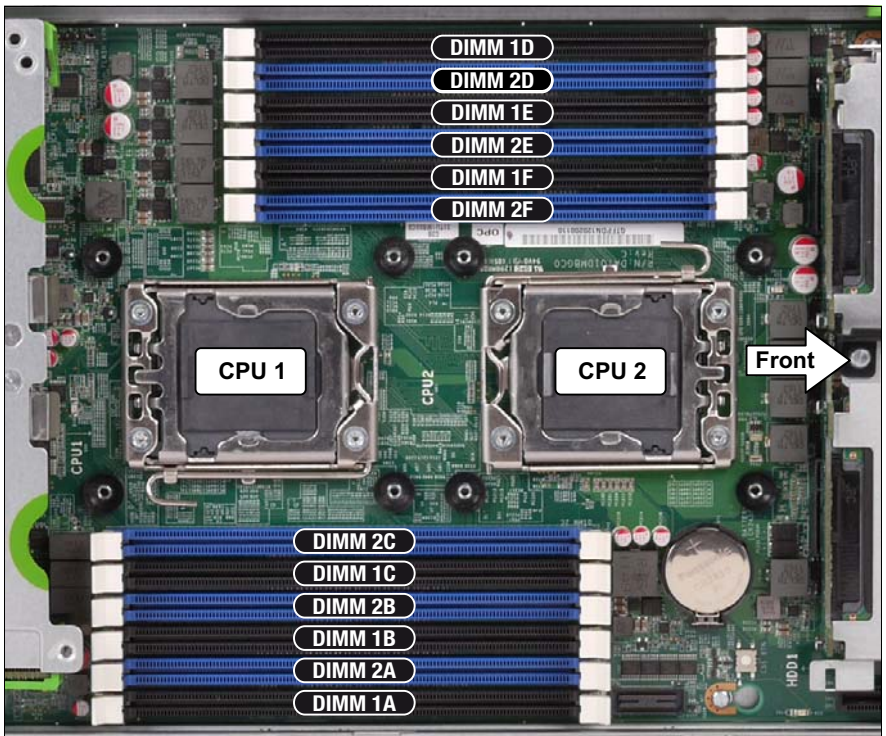


Figure 56: Overview of the DIMM slot numbering

Main memory

8.1.1.2 Independant Channel mode

CPU		CPU 1						CPU 2					
Channel		A		B		C		F		E		D	
Slot descriptor		1A	2A	1B	2B	1C	2C	2F	1F	2E	1E	2D	1D
# DIMMS	1 CPU populated												
1	1												
2	1		2										
3	1		2		3								
4	1	4	2		3								
5	1	4	2	5	3								
6	1	4	2	5	3	6							
	2 CPU populated												
2	1												2
3	1		3										2
4	1		3								4		2
5	1		3		5						4		2
6	1		3		5			6			4		2
7	1	7	3		5			6			4		2
8	1	7	3		5			6			4	8	2
9	1	7	3	9	5			6			4	8	2
10	1	7	3	9	5			6	10		4	8	2
11	1	7	3	9	5	11		6	10		4	8	2
12	1	7	3	9	5	11	12	6	10		4	8	2



All empty DIMM sockets must be fitted with dummy DIMMs. Once the DIMM sockets have been fitted with DIMMs and dummy DIMMs, the air cowl must be laid over the DIMM slots.

Numbering of DIMMs indicates the fitting sequence.

Example: If 6 DIMM modules are to be fitted with 2 CPUs installed, the follow the sequence 1A, 1D, 1B, 1E, 1C, 1F.

8.1.1.3 Mirrored channel mode

CPU		CPU 1						CPU 2					
Channel		A		B		C		F		E		D	
Slot descriptor		1A	2A	1B	2B	1C	2C	2F	1F	2E	1E	2D	1D
# DIMMS		1 CPU populated											
2				1		1							
4				1	2	1	2						
# DIMMS		2 CPU populated											
4				1		1			2		2		
6				1	3	1	3		2		2		
8				1	3	1	3	4	2	4	2		

i All empty DIMM sockets must be fitted with dummy DIMMs. Once the DIMM sockets have been fitted with DIMMs and dummy DIMMs, the air cowl must be laid over the DIMM slots.

Same numbers mean identical modules (capacity, rank).

Main memory

8.1.1.4 Performance channel mode

CPU		CPU 1						CPU 2					
Channel		A		B		C		F		E		D	
Slot descriptor		1A	2A	1B	2B	1C	2C	2F	1F	2E	1E	2D	1D
# DIMMS		1 CPU populated											
3		1		1		1							
6		1	2	1	2	1	2						
		2 CPU populated											
6		1		1		1			2		2		2
9		1	3	1	3	1	3		2		2		2
12		1	3	1	3	1	3		4	2	4	2	4



All empty DIMM sockets must be fitted with dummy DIMMs. Once the DIMM sockets have been fitted with DIMMs and dummy DIMMs, the air cowl must be laid over the DIMM slots.

Same numbers mean identical modules (capacity, rank).

8.1.1.5 Rank Sparring Mode (single rank (1R) and dual rank (2R) RDIMM modules)

CPU	CPU 1							CPU 2					
Channel	A		B		C			F		E		D	
Slot descriptor	1A	2A	1B	2B	1C	2C		2F	1F	2E	1E	2D	1D
# DIMMS	1 CPU populated												
2	1	1											
4	1	1	1	1									
6	1	1	1	1	1	1							
	1 CPU populated												
4	1	1										2	2
6	1	1	1	1								2	2
8	1	1	1	1						2	2	2	2
10	1	1	1	1	1	1				2	2	2	2
12	1	1	1	1	1	1		2	2	2	2	2	2



All empty DIMM sockets must be fitted with dummy DIMMs. Once the DIMM sockets have been fitted with DIMMs and dummy DIMMs, the air cowl must be laid over the DIMM slots.

Same numbers mean identical modules (capacity, rank).

Main memory

8.1.1.6 Rank Sparring Mode for quad rank (4R) and octa rank (8R) LRDIMM modules (minimizing waste of spare memory)

CPU		CPU 1						CPU 2					
Channel		A		B		C		F		E		D	
Slot descriptor		1A	2A	1B	2B	1C	2C	2F	1F	2E	1E	2D	1D
# DIMMS	1 CPU populated												
1	1												
2	1			1									
3	1			1		1							
4	1	1		1		1							
5	1	1		1	1	1							
6	1	1		1	1	1	1						
# DIMMS	2 CPU populated												
2	1												2
3	1			1									2
4	1			1							2		2
5	1			1		1					2		2
6	1			1		1			2		2		2
7	1	1		1		1			2		2		2
8	1	1		1		1			2		2	2	2
9	1	1		1	1	1			2		2	2	2
10	1	1		1	1	1			2	2	2	2	2
11	1	1		1	1	1	1		2	2	2	2	2
12	1	1		1	1	1	1		2	2	2	2	2



All empty DIMM sockets must be fitted with dummy DIMMs. Once the DIMM sockets have been fitted with DIMMs and dummy DIMMs, the air cowl must be laid over the DIMM slots.

Same numbers mean identical modules (capacity, rank).

8.1.1.7 Dummy DIMM modules

All empty DIMM slots must be fitted with dummy DIMM modules to ensure sufficient cooling of the system.



Figure 57: Dummy DIMM module

Dummy modules are installed and removed in the same way as the DIMM modules as described in sections ["Installing a memory module"](#) on page 173 and ["Removing a memory module"](#) on page 176.

8.2 Installing memory modules



Upgrade and Repair Units (URU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes

8.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing memory modules: tool-less

8.2.2 Preliminary steps

Before installing a memory module, perform the following steps:

- ▶ [Disable BitLocker functionality as described in section "Disabling BitLocker functionality" on page 66.](#)
- ▶ [Disable boot watchdog functionality as described in section "Disabling boot watchdog functionality" on page 67.](#)
- ▶ [If applicable, open the rack door as described in section "Opening the rack door" on page 52.](#)
- ▶ [Locate the desired server blade as described in section "Locating the defective server blade" on page 45.](#)
- ▶ [Shut down the defective server blade as described in section "Shutting down the server blade" on page 53.](#)
- ▶ [Remove the server blade from the system unit as described in section "Removing the server blade from the system unit" on page 55.](#)
- ▶ [Open the server blade as described in section "Opening the server blade" on page 56.](#)
- ▶ [If applicable, remove the air cowls as described in section "Removing the air cowls" on page 182.](#)

- ▶ If applicable, remove the dummy DIMM module.

8.2.3 Installing a memory module

- ▶ Identify the correct memory slot according to the mounting order described in section ["Memory sequence" on page 164](#).
- ▶ If required, remove the mezzanine carrier for better handling of the DIMMs of CPU 1.

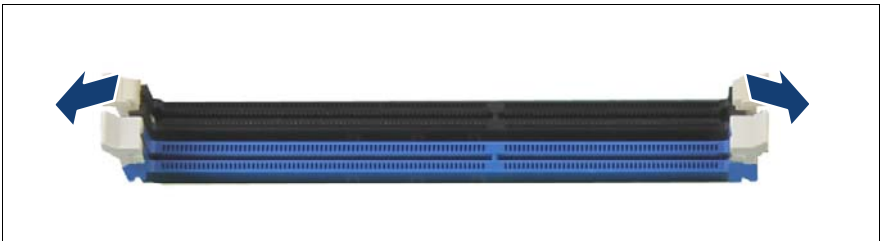


Figure 58: Opening the securing clips

- ▶ Press the securing clips on both sides of the relevant memory slot outward.

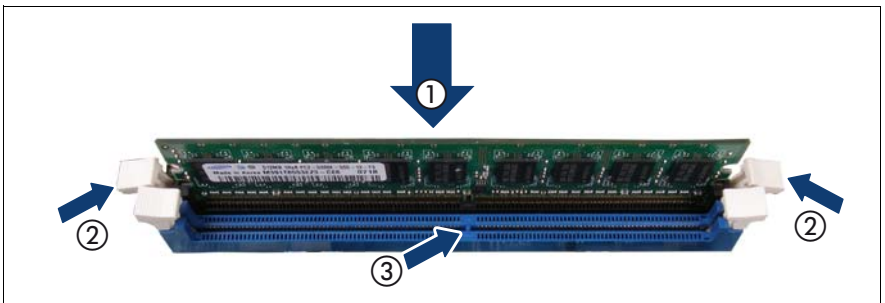


Figure 59: Inserting the memory module

- ▶ Place the DIMM module over the respective slot (1).
- ▶ Make sure the two securing clips (2) are opened out.
- ▶ Align the notch on the bottom of the module with the crossbar in the connector (3).
- ▶ Press down on the memory module (1) until the securing clips snap into the cutouts at each end of the module (2).

8.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Reinstall the air cowls as described in section ["Installing the air cowls" on page 181](#).
- ▶ If applicable, reinstall the mezzanine carrier as described in section ["Installing mezzanine cards" on page 130](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If available, update the system board BIOS to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#) (not applicable for the Japanese market).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If applicable, configure the memory mode as described in section ["Verifying the memory mode" on page 87](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

8.3 Removing memory modules



Upgrade and Repair Units (URU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes

8.3.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing memory modules: tool-less

8.3.2 Preliminary steps

Before removing a memory module, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the defective server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.
- ▶ If applicable, remove the air cowls as described in section "[Removing the air cowls](#)" on page 182.

8.3.3 Removing a memory module

- ▶ Identify the desired memory slot according to the mounting order described in section ["Memory sequence" on page 164](#).



CAUTION!

Ensure to maintain an operational configuration when removing memory modules. For additional information, please refer to section ["Memory sequence" on page 164](#).

- ▶ If required, remove the mezzanine carrier for better handling of the DIMMs of CPU 1.



Figure 60: Opening the securing clips

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

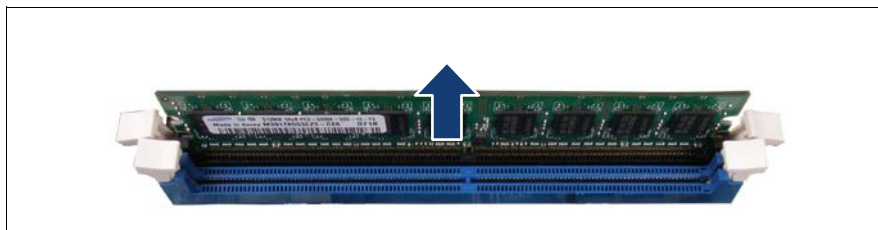


Figure 61: Removing memory modules

- ▶ Remove the ejected memory module.

8.3.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Fit the empty DIMM slot with a dummy DIMM module.
- ▶ Reinstall the air cowls as described in section ["Installing the air cowls" on page 181](#).
- ▶ If applicable, reinstall the mezzanine carrier as described in section ["Installing mezzanine cards" on page 130](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If available, update the system board BIOS to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#) (not applicable for the Japanese market).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

8.4 Replacing memory modules



Upgrade and Repair Units (URU)



average hardware task duration: 15 minutes



Average software task duration: 5 minutes

8.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Replacing memory modules: tool-less

8.4.2 Preliminary steps

Before replacing a memory module, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the defective server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the defective server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ If applicable, remove the air cowls as described in section ["Removing the air cowls" on page 182](#).

- ▶ Locate the defective memory module using the onboard Local Diagnostic LEDs as described in section ["Onboard indicators and controls"](#) on [page 260](#).

8.4.3 Removing a memory module

- ▶ Remove the defective memory module as described in section ["Removing a memory module"](#) on [page 176](#).

8.4.4 Installing a memory module

- ▶ Replace the defective memory module as described in section ["Installing a memory module"](#) on [page 173](#).

8.4.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Reinstall the air cowls as described in section ["Installing the air cowls" on page 181](#).
- ▶ If applicable, reinstall the mezzanine carrier as described in section ["Installing mezzanine cards" on page 130](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If available, update the system board BIOS to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#) (not applicable for the Japanese market).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ Enable the replaced memory module(s) as described in section ["Enabling replaced components in the system BIOS" on page 87](#).
- ▶ Verify if the memory mode has been restored to its original state as described in section ["Verifying the memory mode" on page 87](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

8.5 Handling of memory air cowls

The memory modules have to be covered by air cowls for cooling reasons.

8.5.1 Installing the air cowls

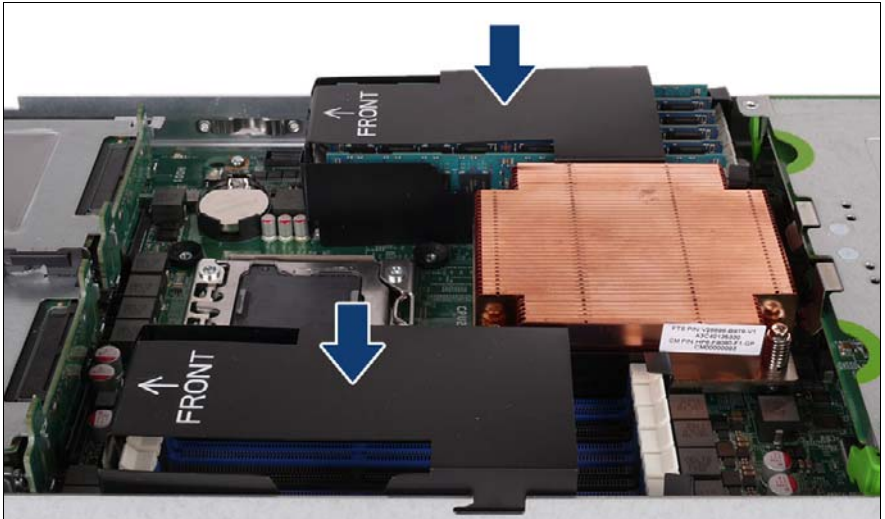


Figure 62: Installing the air cowls

- ▶ Place the air cowls over the DIMMs as shown in the figure.



For cooling reasons the air cowls must be installed when operating!

8.5.2 Removing the air cowls

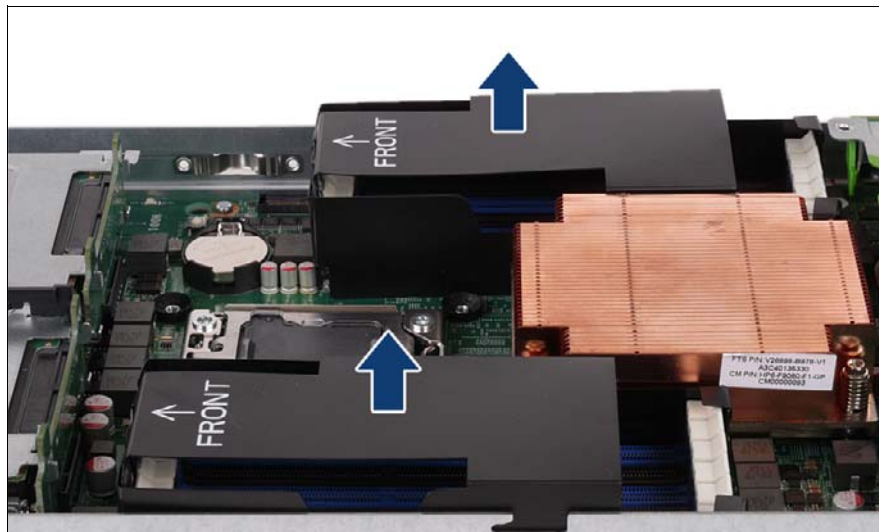


Figure 63: Lifting up the air cowls

- ▶ Lift up the air cowls from the DIMMs.

9 Processors

Safety notes



CAUTION!

- Do not install unsupported processors. For further information on supported processors, refer to section ["Basic information" on page 184](#).
- 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 processor, be careful not to touch or bend the spring contacts on the processor socket.
- Never touch the underside of the processor. Even minor soiling such as grease from the skin can impair the processor's operation or destroy the processor.
- For further information, please refer to chapter ["Important information" on page 31](#).

9.1 Basic information

The system board D3142 offers two sockets for Intel Xeon processors.

Supported processors

- CPU: Intel® Xeon® processor E5-2400v2 family
- Socket type: LGA1356-2 package
- Thermal Design Power (TDP) class: up to 95 W

9.2 Installing processors



Field Replaceable Units (FRU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes



CAUTION!

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

9.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing and installing the processor heat sink:
 - Phillips PH2 / (+) No. 2 screw driver
- Installing the processor: tool-less

9.2.2 Preliminary steps

Before installing a processor, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

9.2.3 Installing a processor



This description applies to the following procedures:

- Installing the second CPU in a single-processor configuration
- Transferring a CPU after replacing the system board (see section ["Swapping the processor" on page 248](#))

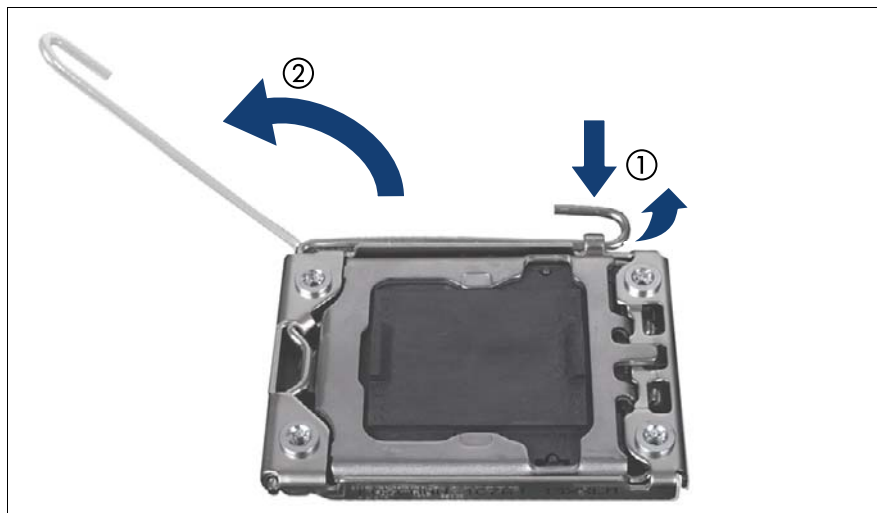


Figure 64: Opening socket release lever

- ▶ Unlatch the socket release lever by pushing it down and away from the socket (1) , and then swivel it up (2).

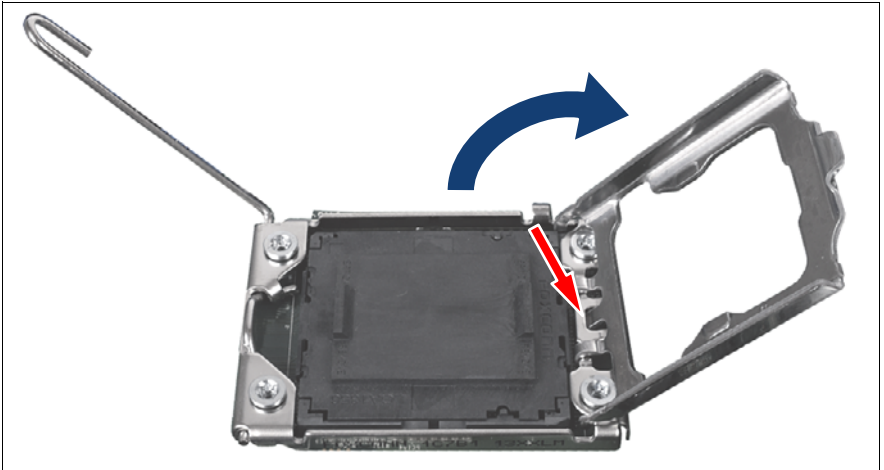


Figure 65: Opening the load plate

- ▶ Open the load plate of the processor socket.



CAUTION!

Handle the locking frame carefully.

In a vertical position, the small clip (see red arrow) can scratch the system board.

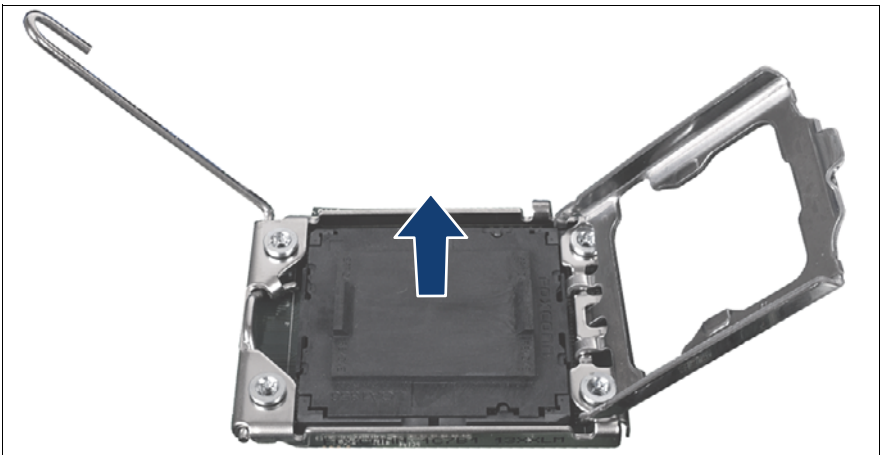


Figure 66: Removing the protective cover

- ▶ Remove the black protective cover from the processor socket.

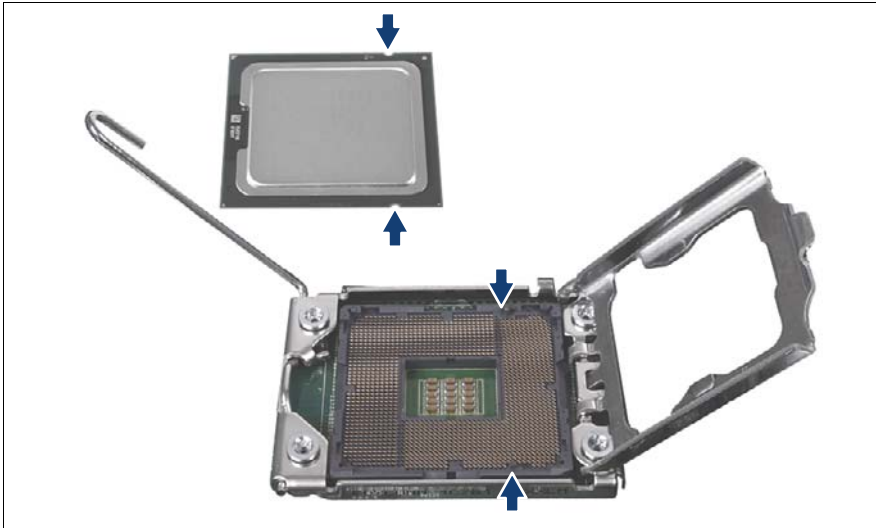


Figure 67: Installing the processor

- ▶ Hold the processor with your thumb and index finger.
- ▶ Place the new processor on the socket.



Make sure that the recesses on the processor are aligned with the corresponding markings on the socket.



CAUTION!

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

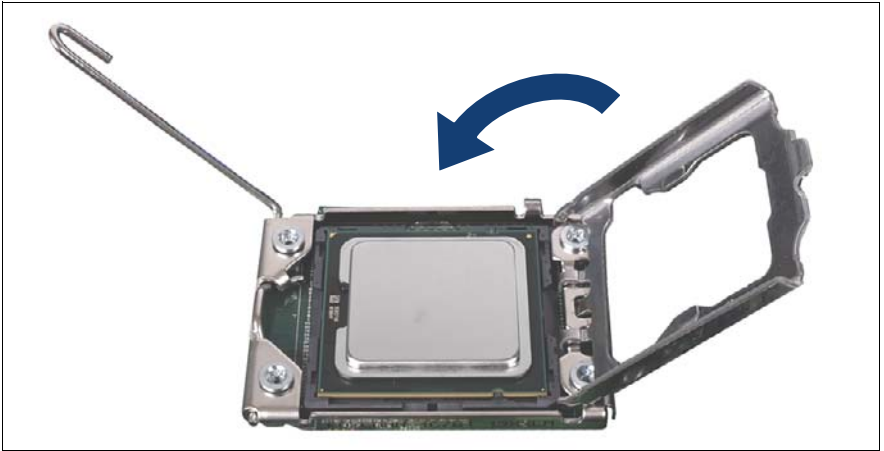


Figure 68: Closing the load plate

- ▶ Close the load plate of the processor.

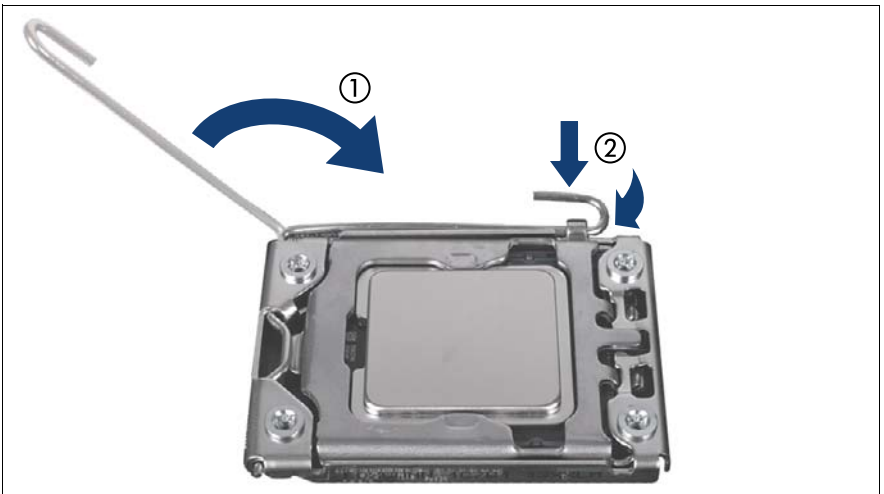


Figure 69: Closing the socket release lever

- ▶ Close the socket release lever (1) and latch it under the load plate retention tab (2) to lock down the load plate.
- ▶ If applicable, install the second processor accordingly.

9.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Install the processor heat sink onto the processor as described in section ["Installing processor heat sinks" on page 202](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If available, update the system board BIOS and the iRMC to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ Enable the replaced processor as described in section ["Enabling replaced components in the system BIOS" on page 87](#).

9.3 Removing processors



Field Replaceable Units (FRU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes



CAUTION!

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

9.3.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing and installing the processor heat sink:
 - Phillips PH2 / (+) No. 2 screw driver
- Removing the processor: tool-less

9.3.2 Preliminary steps

Before removing a processor, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).

Processors

- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ If necessary, remove the memory modules as described in section ["Removing a memory module" on page 176](#).
- ▶ Remove the desired processor heat sink as described in section ["Removing processor heat sinks" on page 206](#).

9.3.3 Removing a processor



This description applies to the following procedures:

- Removing CPU 2 from a dual-processor configuration
 - Removing CPUs from a defective system board (see section ["Swapping the processor" on page 248](#))
- Remove the desired processor heat sink as described in section ["Removing processor heat sinks" on page 206](#).

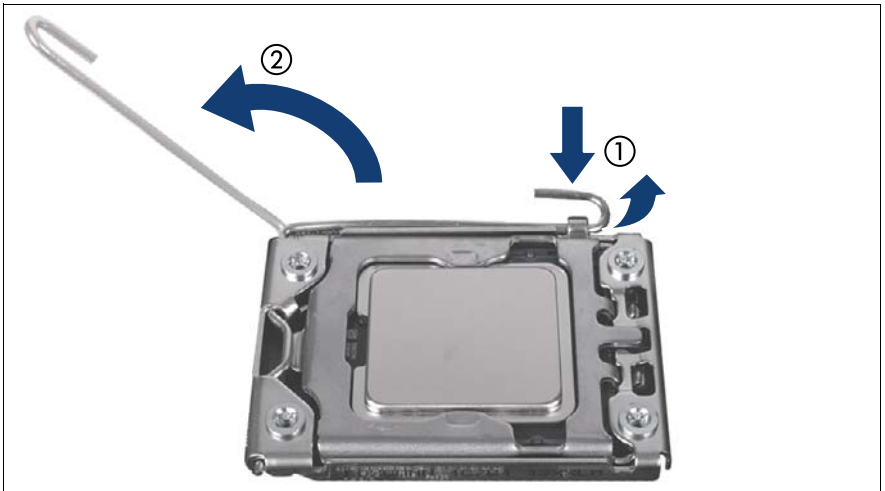


Figure 70: Opening socket release lever

- Unlatch the socket release lever by pushing it down and away from the socket (1) , and then swivel it up (2).

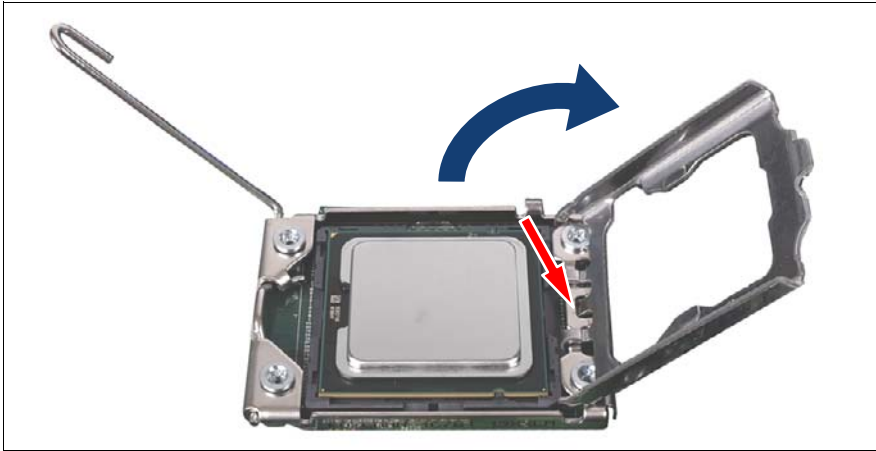


Figure 71: Opening the load plate

- ▶ Open the load plate of the processor socket.



CAUTION!

Handle the locking frame carefully.

In a vertical position, the small clip (see red arrow) can scratch the system board.

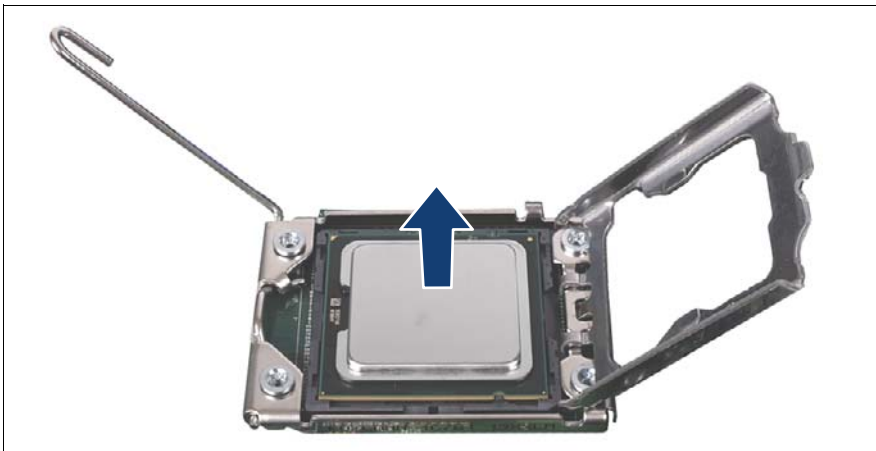


Figure 72: Removing the processor

- ▶ Carefully remove the defective processor from its socket in a vertical motion.

**CAUTION!**

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

- ▶ Thoroughly clean residual thermal paste from the processor surface using a lint-free cloth.
- ▶ Store the processor in a safe place for later reuse.

**CAUTION!**

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

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

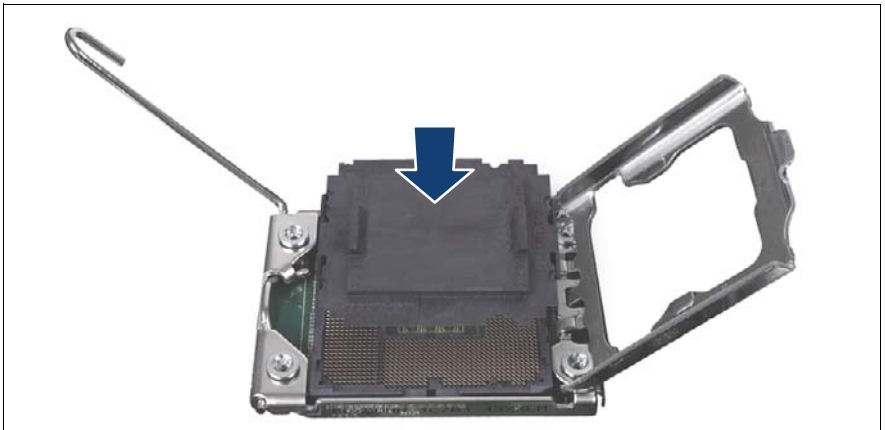


Figure 73: Attaching the protective socket cover

- ▶ Carefully lower the protective socket cover onto the CPU socket in a vertical motion until it snaps in place.

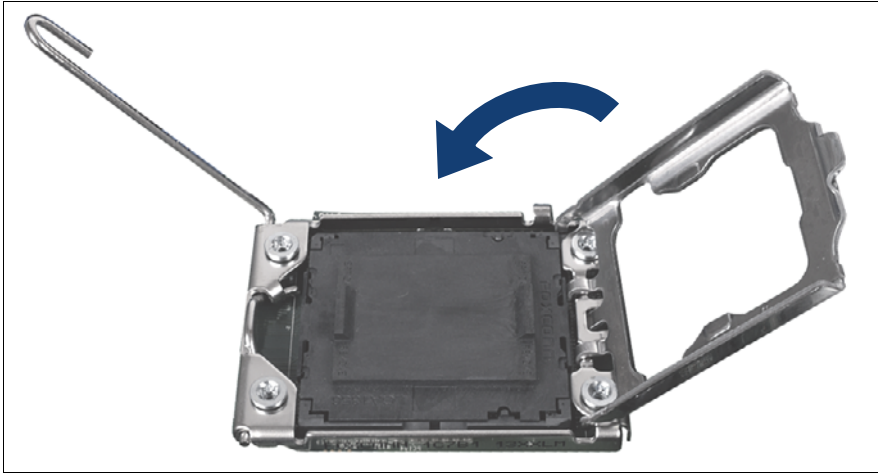


Figure 74: Closing the load plate

- ▶ Close the load plate of the processor.

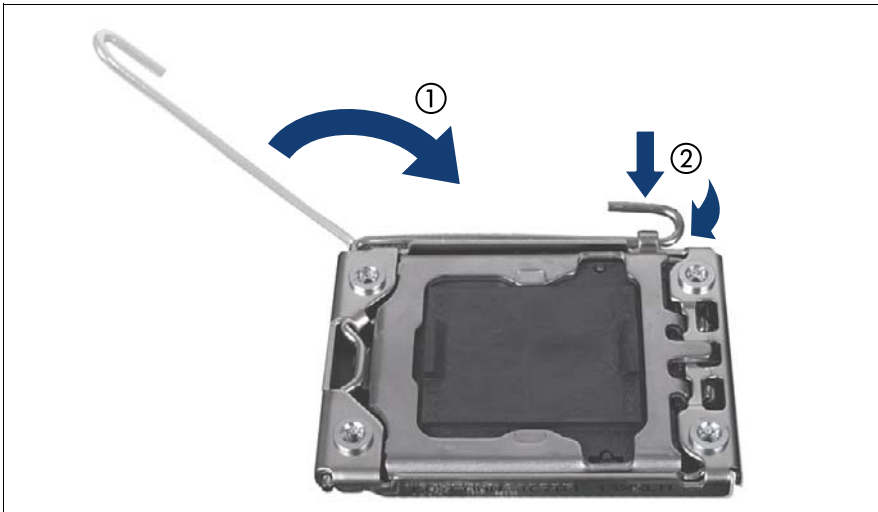


Figure 75: Close the socket release lever

- ▶ Close the socket release (1) lever and latch it under the load plate retention tab to lock down the load plate (2).

9.3.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Install the processor heat sink onto the processor as described in section ["Installing processor heat sinks" on page 202](#).
- ▶ If memory modules have been removed, install the memory into their original location as described in section ["Installing a memory module" on page 173](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

9.4 Upgrading or replacing processors



Field Replaceable Units (FRU)



Average hardware task duration: 15 minutes



Average software task duration: 5 minutes



CAUTION!

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

9.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing and installing the processor heat sink:
 - Phillips PH2 / (+) No. 2 screw driver
- Upgrading or replacing the processor: tool-less

9.4.2 Preliminary steps

Before upgrading or replacing the processor, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).

- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).
- ▶ If necessary, remove the memory modules as described in section ["Removing a memory module" on page 176](#).
- ▶ Remove the desired processor heat sink as described in section ["Removing processor heat sinks" on page 206](#).

9.4.3 Upgrading or replacing a processor

- ▶ Remove the desired processor as described in section ["Removing a processor" on page 193](#).
- ▶ Remove the new processor as described in section ["Installing a processor" on page 186](#).

9.4.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Install the processor heat sink onto the processor as described in section ["Installing processor heat sinks" on page 202](#).
- ▶ If memory modules have been removed, install the memory into their original location as described in section ["Installing a memory module" on page 173](#).
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If available, update the system board BIOS and the iRMC to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#).

Processors

- ▶ Enable the the replaced processor as described in section ["Enabling replaced components in the system BIOS" on page 87](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

9.5 Handling processor heat sinks



Field Replaceable Units (FRU)



Average task duration: 15 minutes

9.5.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing or removing the processor heat sink:
 - Phillips PH2 / (+) No. 2 screw driver

9.5.2 Preliminary steps

Before installing, removing or replacing the processor heat sink, perform the following steps:

- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ If necessary, remove the memory modules as described in section "[Removing a memory module](#)" on page 176.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

9.5.3 Installing processor heat sinks

The following figures show the heat sink types used in the BX920 S4 server blade:

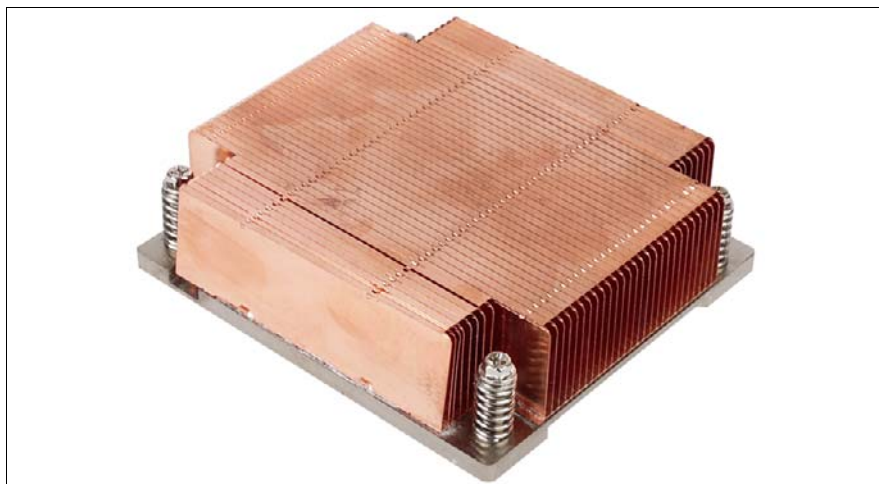


Figure 76: Heat sink for CPU 1

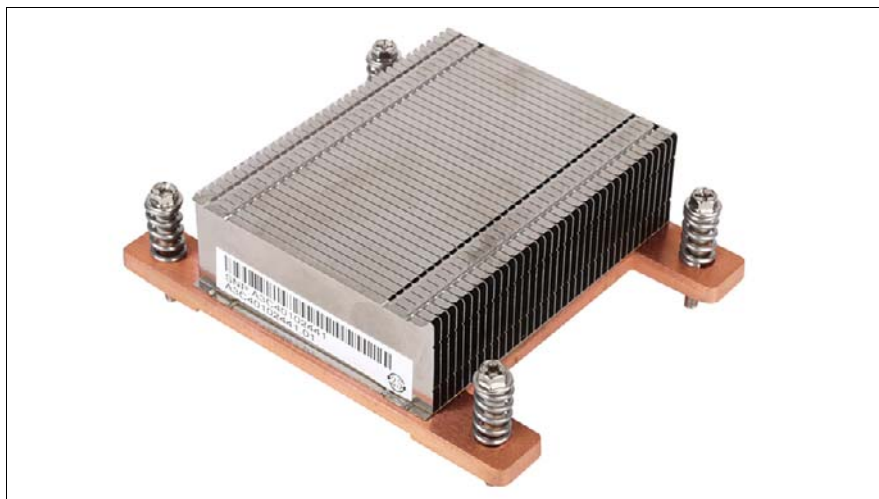


Figure 77: Heat sink for CPU 2

9.5.3.1 Preparing the heat sink and processor

When installing a new heat sink

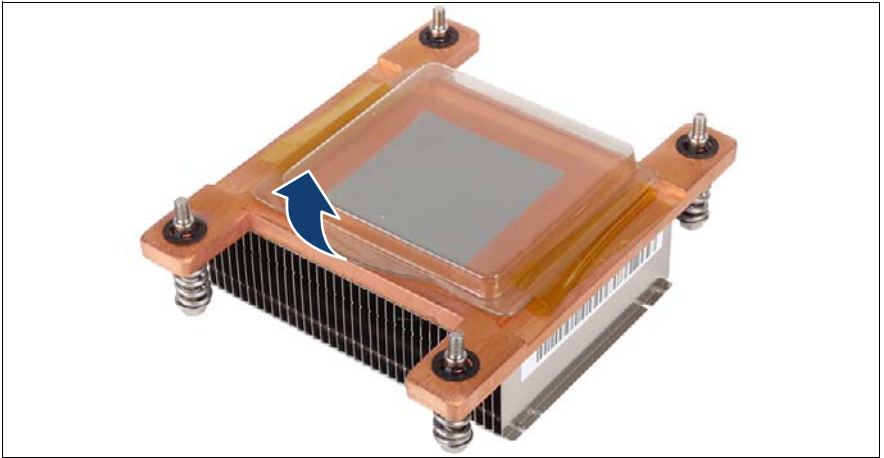


Figure 78: Heat sink with protective cover

- ▶ Remove the protective cover from the heat sink (see arrow).



CAUTION!

Ensure not to touch the heat-conductive paste on the bottom of the heat sink.

When reusing a heat sink

- ▶ Ensure that all residual thermal paste has been thoroughly cleaned off the copper surface of the heat sink.
- ▶ Apply thermal paste to the processor surface as described in section ["Applying thermal paste" on page 208](#).

9.5.3.2 Installing the heat sink

i The following procedure is identical for the heat sinks of both CPUs.

- ▶ Align the heat sink with the four threaded holes of the processor socket.

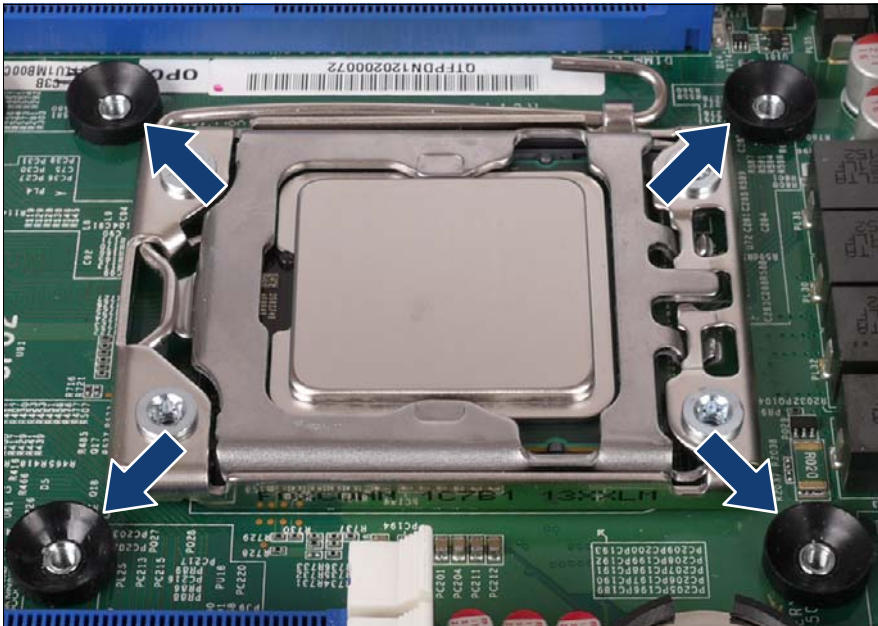


Figure 79: Installing the heat sink

- ▶ Carefully seat the heat sink on the four threaded holes as shown (see arrows).



CAUTION!

- Ensure that the screws on the heat sink are properly seated on the threaded holes.
- Ensure that the heat sink cooling fins match the direction of the airflow!

- ▶ Keep pressing on the heat sink to prevent it from tilting until two screws (1) and (2) are fixed.

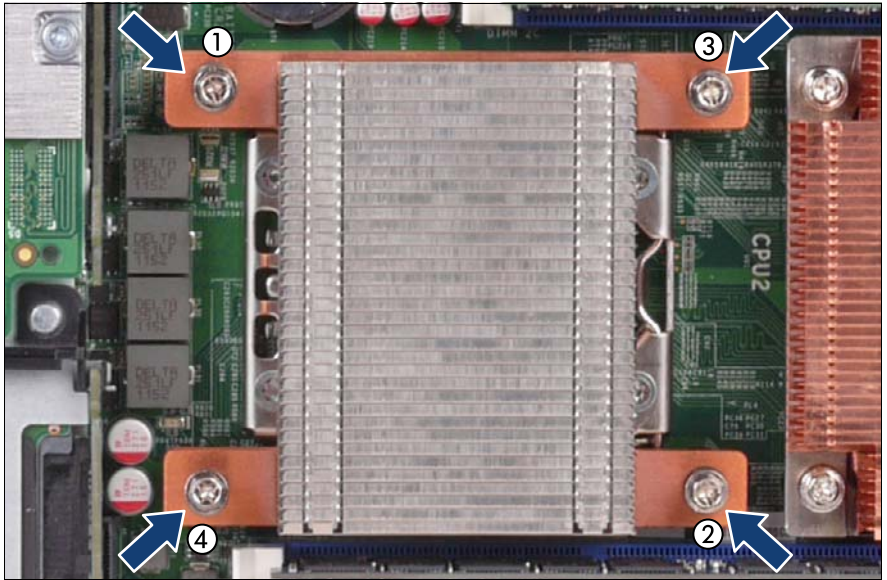


Figure 80: Fastening the heat sink

- ▶ Fasten the four captive screws (combihexagon) on the heat sink in the following pattern: (1)->(2)->(3)->(4).

Torque: 0.6 Nm, not applicable for the Japanese market

9.5.4 Removing processor heat sinks

i The following procedure is identical for the heat sinks of both CPUs.

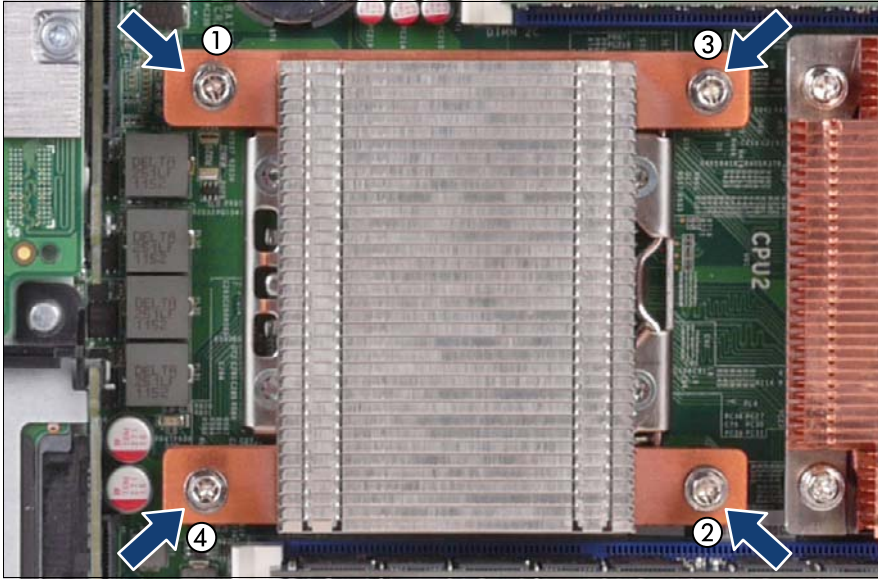


Figure 81: Removing the processor heat sink (A)

- ▶ Loosen the four captive screws (combihexagon) on the heat sink in the following pattern: (4)->(3)->(2)->(1).

i Keep pressing on the heatsink to avoid tilting until the screws (1) and (2) are removed.

- ▶ Carefully turn the heat sink back and forth to detach it from the processor.

i This may be necessary due to the adhesive quality of the thermal paste located between the heat sink and processor.



CAUTION!

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

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

9.5.5 Replacing processor heat sinks

9.5.5.1 Removing the processor heat sink

- ▶ Remove the processor heat sink as described in section ["Removing processor heat sinks" on page 206](#).

9.5.5.2 Applying thermal paste

- ▶ Apply thermal paste to the processor surface as described in section ["Applying thermal paste" on page 208](#).

9.5.5.3 Installing the processor heat sink

- ▶ Install the processor heat sink as described in sections ["Preparing the heat sink and processor" on page 203](#) and ["Installing the heat sink" on page 204](#).

9.5.6 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ If memory modules have been removed, install the memory into their original location as described in section ["Installing a memory module" on page 173](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).

9.6 Applying thermal paste



Field Replaceable Units (FRU)



Average task duration: 5 minutes



- For the Japanese market, the service engineer must follow the instruction provided separately.
- If the processor upgrade or replacement kit contains a new CPU 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 processor heat sinks" on page 202](#).

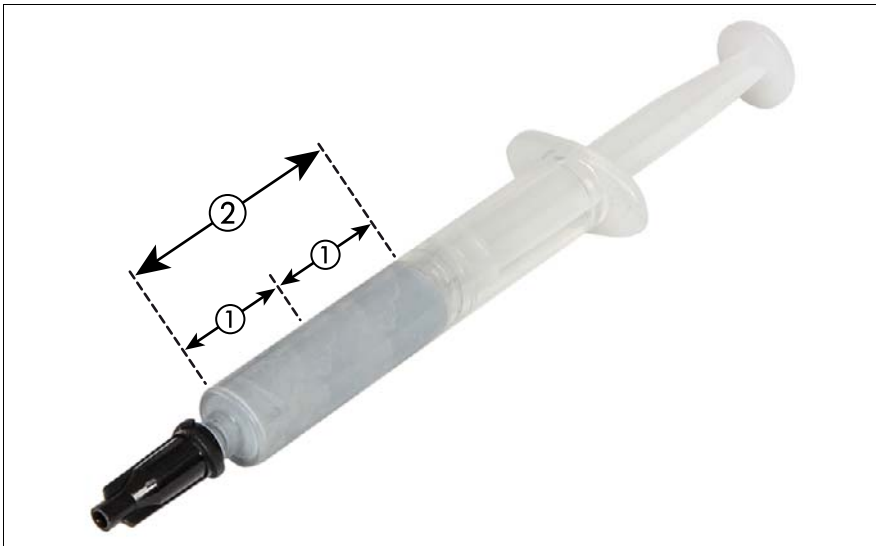


Figure 82: Thermal paste syringe

One thermal compound syringe (FSP:P304000003) contains thermal paste for two processors.

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


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



Figure 83: Applying thermal paste

- ▶ Apply a small streak of thermal paste (1.0 gram, see description above) to the center of the processor surface as shown.



CAUTION!

Do not mix different types of thermal paste.

10 System board 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 31.

10.1 Replacing the CMOS battery



Upgrade and Repair Units (URU)



Average task duration: 5 minutes

CMOS memory (volatile BIOS memory) and the real-time clock are powered by a lithium coin cell (CMOS battery).

If the CMOS battery is depleted or falls below minimum voltage levels, it need to be replaced immediately.

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.

System board components

- 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 PRIMERGY BX920 S4 Operating Manual.
- **Ensure to insert the CMOS battery with the positive pole facing up!**

10.1.1 Required tools

- Preliminary and concluding steps: tool-less
- Replacing the battery: tool-less

10.1.2 Preliminary steps

Before replacing the CMOS battery, perform the following steps:

- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.1.3 Removing the battery

The CMOS battery is located on the system board near CPU2 and HDD1 (see following figure).



Figure 84: Location of the CMOS battery on the system board D3142 (see circle)



Figure 85: Replacing the CMOS battery

- ▶ Press out on the locking spring to eject the depleted CMOS battery (see arrow).
- ▶ Carefully pry the depleted CMOS battery out of its socket.
- ▶ Remove the CMOS battery.



Do not throw the CMOS battery into the trash can. Lithium batteries must be disposed of in accordance with local regulations concerning special waste.

10.1.4 Installing the CMOS battery



Figure 86: Installing the CMOS battery

- ▶ At a slight angle, fit the new CMOS battery into its socket as shown in the figure above.



CAUTION!

Ensure to insert the CMOS battery with the positive pole (label side) facing up as shown.

- ▶ Press on the CMOS battery until it locks in place.
- ▶ Ensure that the locking spring is properly engaged.

10.1.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Dispose of the CMOS battery in accordance with local regulations concerning special waste.
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Verify and update time settings as described in section ["Verifying the system time settings" on page 88](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).

10.2 USB Flash Module (UFM)

10.2.1 Installing the UFM



Field Replaceable Units (FRU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

10.2.1.1 Required tools

- Preliminary and concluding steps: tool-less
- Installing the UFM:
 - Phillips PH1 / (+) No. 1 cross-head screwdriver

10.2.1.2 Preliminary steps

Before installing the UFM, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.2.1.3 Installing the UFM

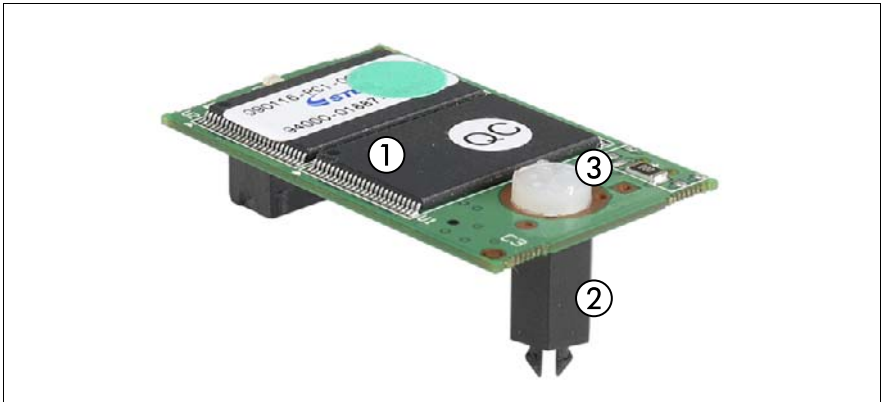


Figure 87: UFM kit

Pre-assembled UFM flash module kit (S26361-F3514-V3):

1 2 GB UFM SLC
A3C40104433

2 UFM spacer
A3C40109081

i This black spacer will not be used. A white spacer is already mounted instead.

3 UFM nylon screw
A3C40109082

System board components

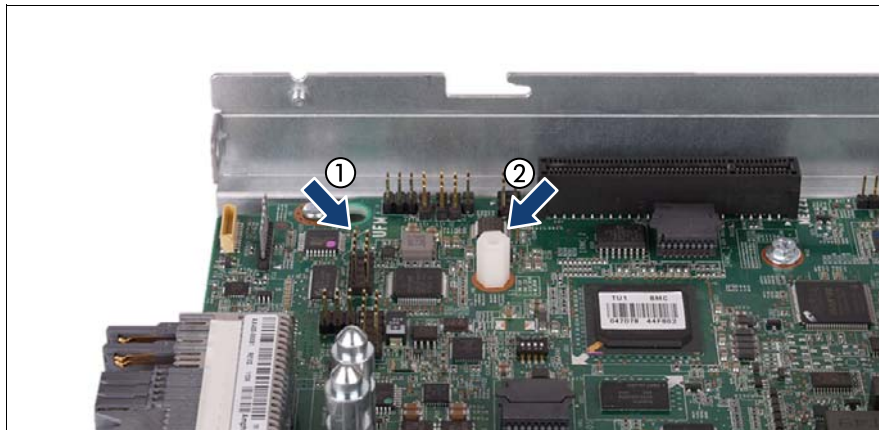


Figure 88: UFM mounting location

UFM mounting location on the system board:

- 1 UFM connector
- 2 UFM spacer



Figure 89: Installing the UFM

- ▶ Connect the UFM to the system board.
- ▶ Secure the UFM with the nylon screw (see arrow).

10.2.1.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure it in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

10.2.1.5 Software configuration

The UFM delivery set includes the "Recovery Tool CD" to setup the ESXi configuration. Proceed as follows:

- ▶ Switch on the server blade.
- ▶ Right after switching on the server, insert the "Recovery Tool CD" into the DVD drive and close the drive tray.
- ▶ The server should now boot from the "Recovery Tool CD".
- ▶ Follow the on-screen instructions.

10.2.2 Removing the UFM



Field Replaceable Units (FRU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

10.2.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing the UFM:
 - Phillips PH1 / (+) No. 1 screw driver

10.2.2.2 Preliminary steps

Before removing the UFM, perform the following steps:

- ▶ Disable BitLocker functionality as described in section "[Disabling BitLocker functionality](#)" on page 66.
- ▶ Disable boot watchdog functionality as described in section "[Disabling boot watchdog functionality](#)" on page 67.
- ▶ If applicable, open the rack door as described in section "[Opening the rack door](#)" on page 52.
- ▶ Locate the desired server blade as described in section "[Locating the defective server blade](#)" on page 45.
- ▶ Shut down the server blade as described in section "[Shutting down the server blade](#)" on page 53.
- ▶ Remove the server blade from the system unit as described in section "[Removing the server blade from the system unit](#)" on page 55.
- ▶ Open the server blade as described in section "[Opening the server blade](#)" on page 56.

10.2.2.3 Removing the UFM

- ▶ Remove the nylon screw from the defective UFM.

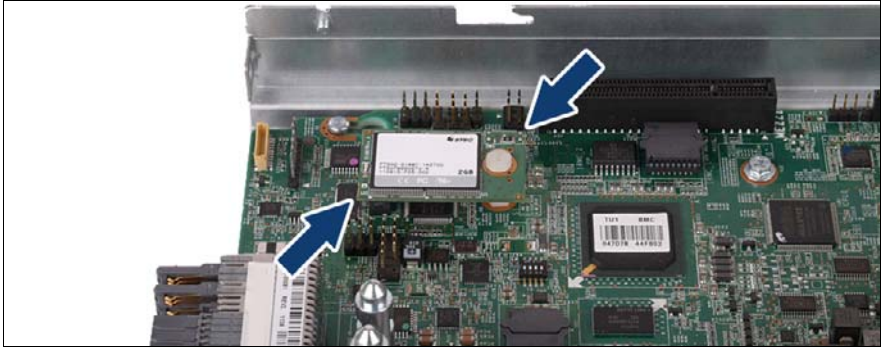


Figure 90: Removing the UFM

- ▶ Grasp the UFM on its corners (see arrows), then pull it out gradually and carefully.

The UFM spacer remains on the system board.

10.2.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

10.2.3 Replacing the UFM



Field Replaceable Units (FRU)



Average hardware task duration: 10 minutes



Average software task duration: 5 minutes

10.2.3.1 Required tools

- Preliminary and concluding steps:
 - combination pliers and flat nose pliers
- Replacing the UFM:
 - Phillips PH1 / (+) No. 1 screw driver

10.2.3.2 Preliminary steps

Before replacing the UFM, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.2.3.3 Removing the UFM

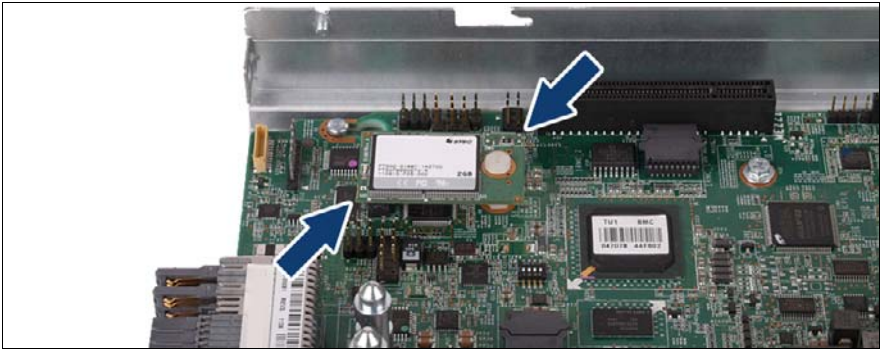


Figure 91: Removing the UFM

- ▶ Grasp the UFM on its corners (see arrows), then pull it out gradually and carefully.

The UFM spacer remains on the system board.

10.2.3.4 Re-installing the UFM

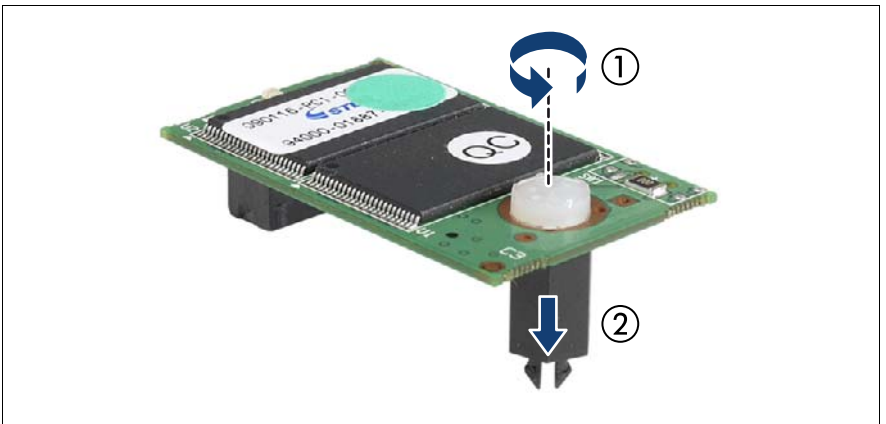


Figure 92: Preparing the new UFM

- ▶ Remove the nylon screw (1) and the black spacer (2) from the new UFM.
- ▶ Fit the new UFM on the UFM connector and the remaining UFM spacer.
- ▶ Secure the UFM to the UFM spacer with the nylon screw.

Destroying the defective UFM



CAUTION!

The UFM contains customer information (e.g. IP address, license numbers). After replacing the UFM, hand the defective UFM over to the customer. If the customer requests disposal of the defective UFM, proceed as follows:

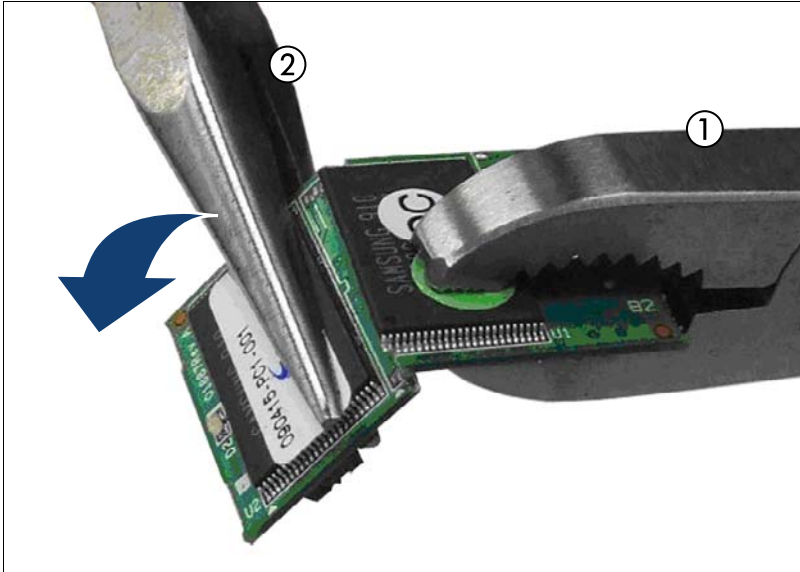


Figure 93: Destroying the defective UFM

- ▶ Use a pair of combination pliers (1) and flat nose pliers (2) to break the UFM in half as shown.

10.2.3.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

10.2.3.6 Software configuration

The UFM delivery set includes the "Recovery Tool CD" to setup the ESXi configuration. Proceed as follows:

- ▶ Connect a remote DVD drive to the server blade as described in section ["Connecting virtual media to the managed server blade" on page 65](#).
- ▶ Insert the "Recovery Tool CD" into the remote DVD drive and close the drive tray.
- ▶ Switch on the server blade.
- ▶ The server blade should now boot from the "Recovery Tool CD".
- ▶ Follow the on-screen instructions.

10.3 Trusted Platform Module (TPM)

This section provides information on how to install, remove or replace the Trusted Platform Module (TPM).

10.3.1 Installing the TPM



Field Replaceable Units (FRU)



Average hardware task duration: 5 minutes



Average software task duration: 5 minutes

10.3.1.1 Required tools

- Preliminary and concluding steps:
 - Phillips PH2 / (+) No. 2 screw driver
 - Installing the TPM:
 - Bit screw driver
 - TPM bit insert (*)
- (*) For the Japanese market:
- TPM module fixing tool (S26361-F3552-L909)

10.3.1.2 Preliminary steps

Before installing the TPM, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).

- ▶ Shut down the server blade as described in section "Shutting down the server blade" on page 53.
- ▶ Remove the server blade from the rack as described in section "Removing the server blade from the system unit" on page 55.
- ▶ Open the server blade as described in section "Opening the server blade" on page 56.

10.3.1.3 Installing the TPM

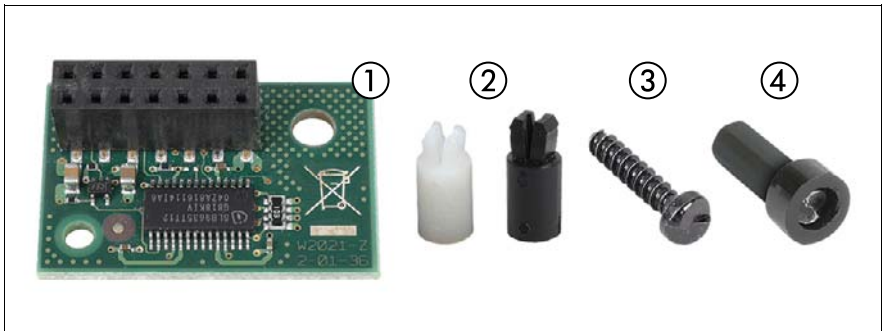


Figure 94: TPM kit

TPM kit (S26361-F3299-E2):

- 1 TPM module
S26361-D2727-A10
- 2 TPM spacers
 - i** Use the black TPM spacer.
The white TPM spacer is not used in this server blade.
- 3 TPM special screw
C26192-Y10-C176
- 4 TPM bit insert for TPM special screw

System board components

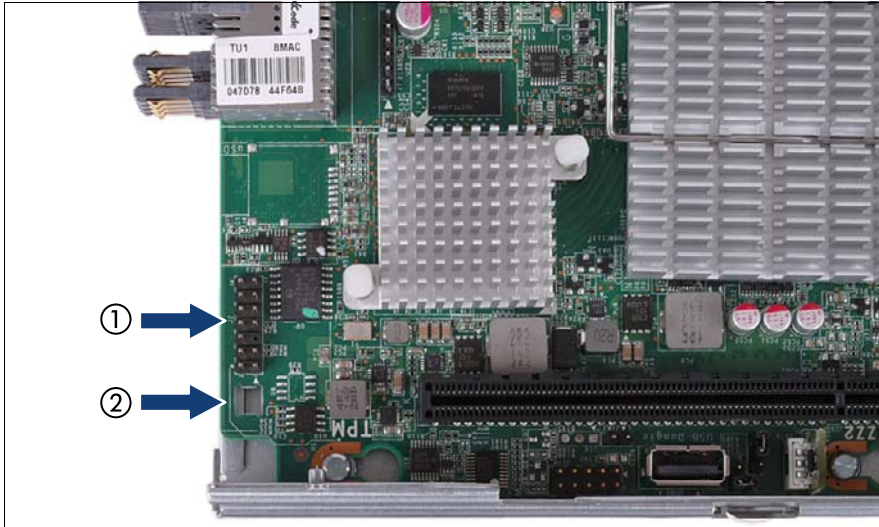


Figure 95: TPM mounting location

TPM mounting location on the system board:

- 1 TPM connector
- 2 Cut-out for TPM spacer

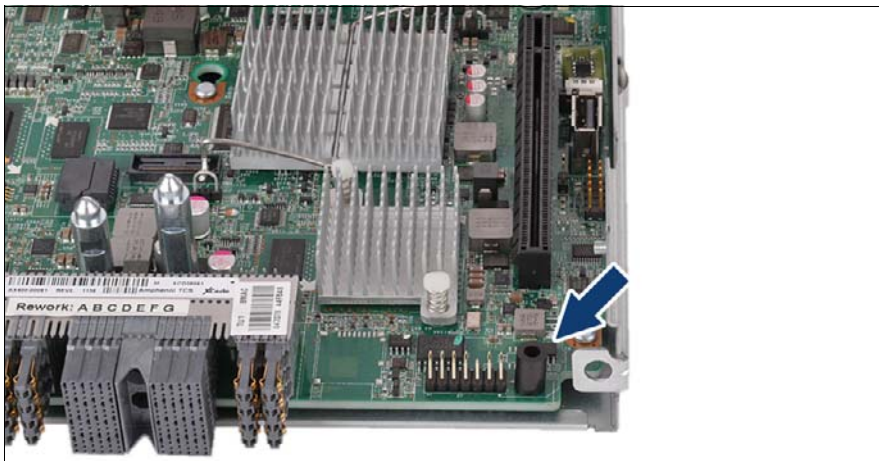


Figure 96: Installing the TPM spacer

- ▶ Snap the TPM spacer into the cut-out in the system board (see arrow).



Figure 97: TPM bit insert

- ▶ Attach the TPM bit insert or TPM module fixing tool (Japanese market) to a bit screw driver.

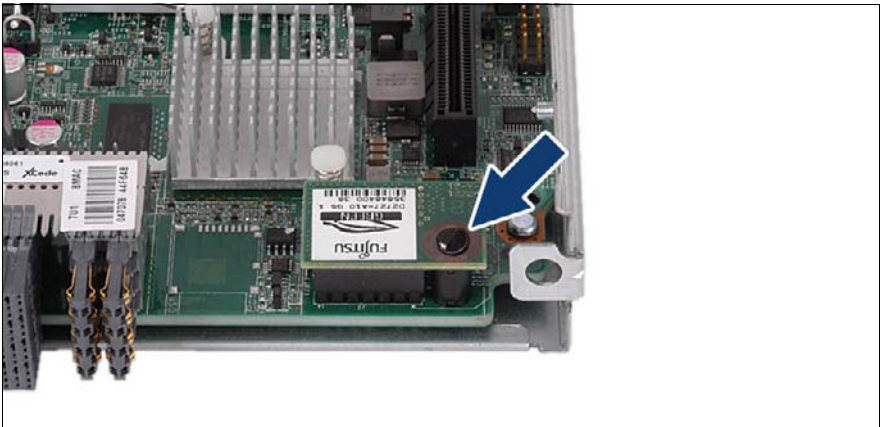


Figure 98: Mounting the TPM

- ▶ Connect the new TPM to the system board.
- ▶ Secure the TPM with the TPM screw (see arrow) using the TPM bit insert (see [figure 97 on page 229](#)).



Do not fasten the screw too firmly. Stop as soon as the head of the screw lightly touches the TPM.

10.3.1.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Enable TPM in the system board BIOS. Proceed as follows:
 - ▶ Open a virtual console for your server blade as describe in section ["Launching a video redirection to a server blade" on page 63](#).
 - ▶ Switch on or restart your server blade.
 - ▶ 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 detailed information on how to access the BIOS and modify settings, refer to the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual available online.

- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

10.3.2 Removing the TPM



Field Replaceable Units (FRU)



Average task duration: 30 minutes



CAUTION!

Advise your contact persons that they must provide you with TPM backup copies. For security reasons, the TPM must be restored/re-saved by the customer. After installing a new system board, the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

10.3.2.1 Required tools

- Preliminary and concluding steps: tool-less
- Removing the system board:
 - Phillips PH2 / (+) No. 2 screw driver
- Removing the TPM:
 - thin slotted screw driver (2 x 0.4 mm)

For the Japanese market:

- Dedicated TPM screw driver (CWZ8291A)

10.3.2.2 Preliminary steps

Before removing the TPM, perform the following 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.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

- ▶ Disable TPM in the system board BIOS. Proceed as follows:
 - ▶ Open a virtual console for your server blade as described in section ["Launching a video redirection to a server blade" on page 63](#).
 - ▶ Switch on or restart your server blade.
 - ▶ 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 "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual available online.

- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.3.2.3 Removing the TPM

- ▶ Remove the system board as described in section ["Removing the system board" on page 245](#).
- ▶ Lay the system board on a soft, antistatic surface with its component side facing down.

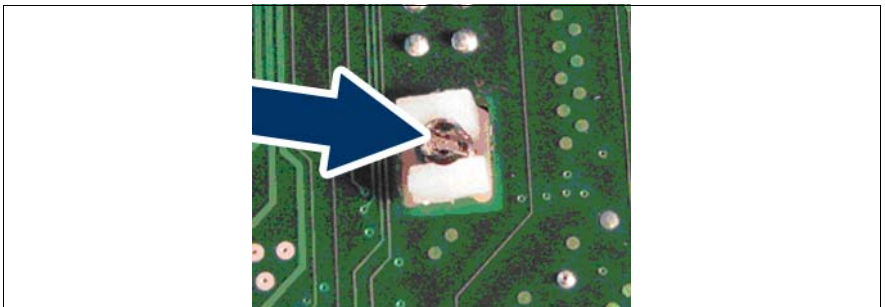


Figure 99: Removing the TPM screw from the underside of the system board

- ▶ Locate the slotted lower end of the TPM screw (see arrow).
- ▶ Carefully loosen the TPM screw using a thin slotted screw driver (e.g. watchmaker's screw driver) or the dedicated TPM screw driver (Japanese market).



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 loosening 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.
- ▶ Remove the defective TPM on the upper side of the system board.

10.3.2.4 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).

10.3.3 Replacing the TPM



Field Replaceable Units (FRU)



Average task duration: 40 minutes



CAUTION!

Advise your contact persons that they must provide you with TPM backup copies. For security reasons, the TPM must be restored/re-saved by the customer. After installing a new system board, the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

10.3.3.1 Required tools

- Preliminary and concluding steps: tool-less
 - Removing the system board:
 - Phillips PH2 / (+) No. 2 screw driver
 - Replacing the TPM:
 - Bit screw driver
 - TPM bit insert (*)
 - thin slotted screw driver (2 x 0.4 mm) (*)
- (*) For the Japanese market:
- Dedicated TPM screw driver (CWZ8291A)
 - TPM module fixing tool (S26361-F3552-L909)

System board components

10.3.3.2 Preliminary steps

Before replacing the TPM, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.3.3.3 Removing the TPM

- ▶ Remove the TPM as described in section ["Removing the TPM" on page 231](#).

10.3.3.4 Re-installing the TPM

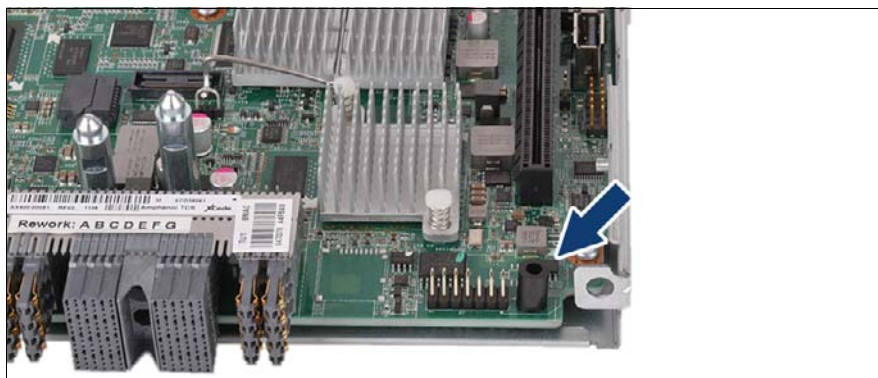


Figure 100: TPM spacer

The TPM spacer is already present on the system board.

- ▶ Re-install the TPM as described in section ["Installing the TPM" on page 226](#).

10.3.3.5 Concluding steps

Perform the following procedures to complete the task:

- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).

10.4 Onboard SAS enabling key

The onboard SAS enabling key enables the SAS functionality of the Onboard controller.



Upgrade and Repair Units (URU)



Average task duration: 5 minutes

10.4.1 Required tools

- Preliminary and concluding steps: tool-less
- Main steps: tool-less

10.4.2 Preliminary steps

Perform the following procedures:

- ▶ ["Opening the rack door" on page 52](#)
- ▶ ["Locating the defective server blade" on page 45](#)
- ▶ ["Shutting down the server blade" on page 53](#)
- ▶ ["Removing a server blade" on page 54](#)
- ▶ ["Opening the server blade" on page 56](#)

10.4.3 Removing the defective onboard SAS enabling key

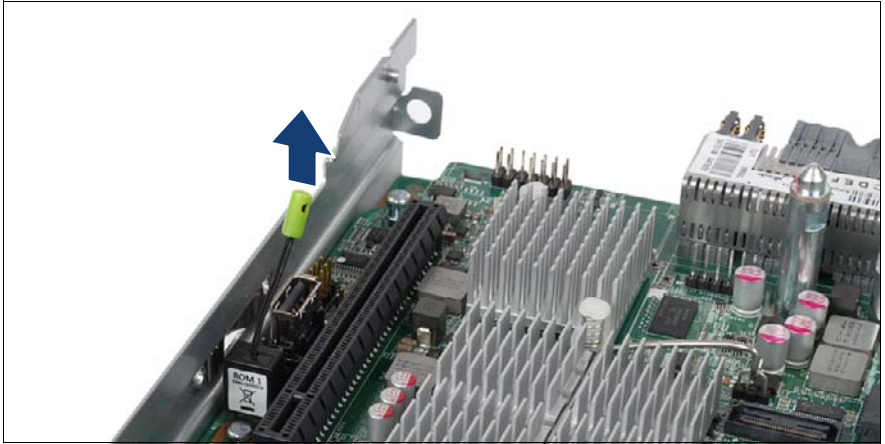


Figure 101: Removing the onboard SAS enabling key

- ▶ Pull the onboard SAS enabling key from the connector on the system board using the green removal tool.

10.4.4 Installing the new onboard SAS enabling key

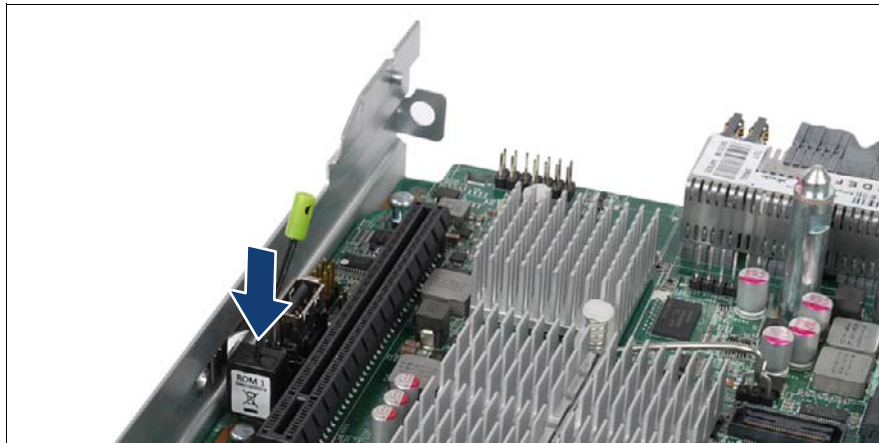


Figure 102: Installing the onboard SAS enabling key

- ▶ Connect the onboard SAS enabling key to the connector on the system board.

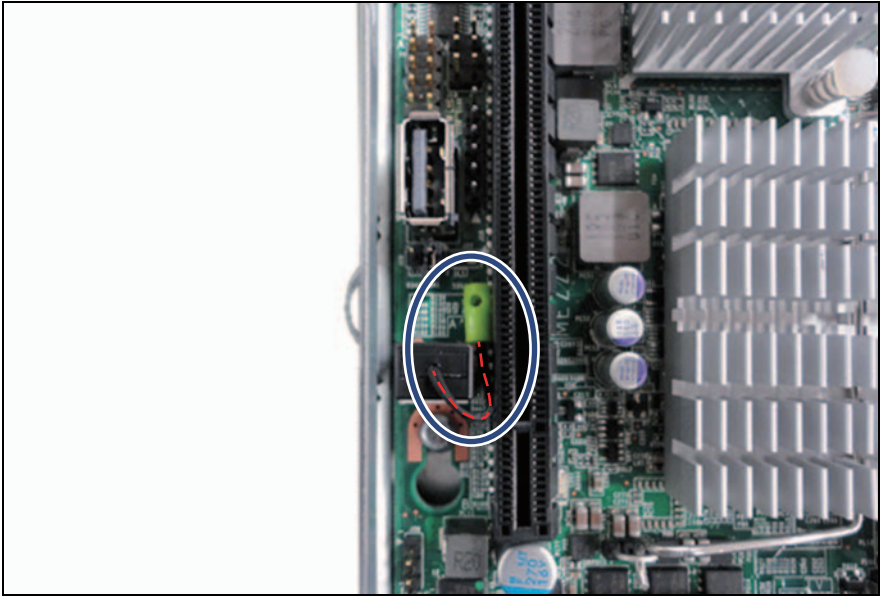


Figure 103: Routing the holding rope

- ▶ Route the holding rope (see oval) of the onboard SAS enabling key into the gap between its own socket and the connector of the mezzanine bracket on the system board as shown in the figure.

10.4.5 Concluding steps

Perform the following procedures:

- ▶ ["Closing the server blade" on page 57](#)
- ▶ ["Installing the server blade in the system unit" on page 58](#)
- ▶ ["Switching on the server blade" on page 60](#)
- ▶ ["Closing the rack door" on page 62](#)

10.5 Replacing the system board



Field Replaceable Units (FRU)



Average hardware task duration: 50 minutes



Average software task duration: 10 minutes

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 235](#).

The TPM is activated 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 TPM backup copies. For security reasons, the TPM must be restored / re-saved by the customer. After installing a new system board the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

Note on system information backup / restore



The server blade contains the Chassis ID EPROM that contains system information like server name and model, housing type, serial number and manufacturing data.

10.5.1 Required tools

- Preliminary and concluding steps: tool-less
- Replacing the system board:
 - Phillips PH2 / (+) No. 2 screw driver
- Replacing the system board:
 - Magnifying glass for inspecting CPU socket springs (recommended)

If a TPM module is installed:

- Bit screw driver
- TPM bit insert (*)
- thin slotted screw driver (2 x 0.4 mm) (*)

(*) For the Japanese market:

- Dedicated TPM screw driver (CWZ8291A)
- TPM module fixing tool (S26361-F3552-L909)

10.5.2 Preliminary steps

Before replacing the system board, perform the following steps:

- ▶ Disable BitLocker functionality as described in section ["Disabling BitLocker functionality" on page 66](#).
- ▶ Disable boot watchdog functionality as described in section ["Disabling boot watchdog functionality" on page 67](#).
- ▶ If applicable, open the rack door as described in section ["Opening the rack door" on page 52](#).
- ▶ Locate the desired server blade as described in section ["Locating the defective server blade" on page 45](#).
- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ If applicable, remove the HDD/SSD modules from the server blade, see section ["Removing the 2.5-inch HDD/SSD module" on page 109](#).



Ensure to take note of the HDD/SSD modules mounting positions for reassembly.

- ▶ Remove the server blade from the rack as described in section ["Removing the server blade from the system unit" on page 55](#).
- ▶ Open the server blade as described in section ["Opening the server blade" on page 56](#).

10.5.3 Removing the system board

- ▶ Remove the following components from the system board as shown in the related sections:

- Heat sink: see [section "Removing processor heat sinks" on page 206](#)



Leave the processor on the defective board for now.

- Memory modules: refer to [section "Removing memory modules" on page 175](#)



Ensure to take note of the memory modules' mounting positions for reassembly.

- Mezzanine cards: refer to the [section "Removing mezzanine cards" on page 136](#)



Ensure to take note of the controllers' mounting positions and cable connections for reassembly.

- UFM: refer to [section "Replacing the UFM" on page 222](#)



Figure 104: Detaching the system board (A)

- ▶ Remove the screw from the system board (see circle).

System board components

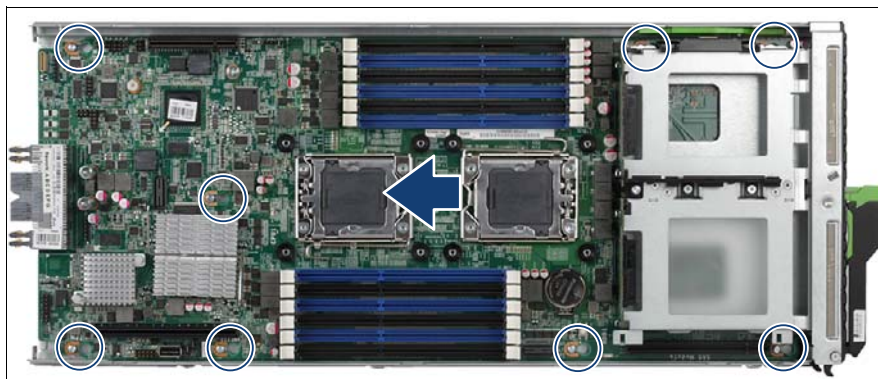


Figure 105: Detaching the system board (B)

- ▶ Carefully shift the system board to the front (see arrow) in order to detach it from the centering bolts (see circles).
- ▶ Hold the defective system board by the memory module ejectors and at a slight angle lift it out of the chassis.
- ▶ If applicable, remove the TPM as described in [section "Removing the TPM" on page 233](#).

10.5.4 Installing the system board

10.5.4.1 Mounting the system board

- ▶ Hold the new system board by the memory module ejectors.
- ▶ At a slight angle, lower the system board into the chassis.

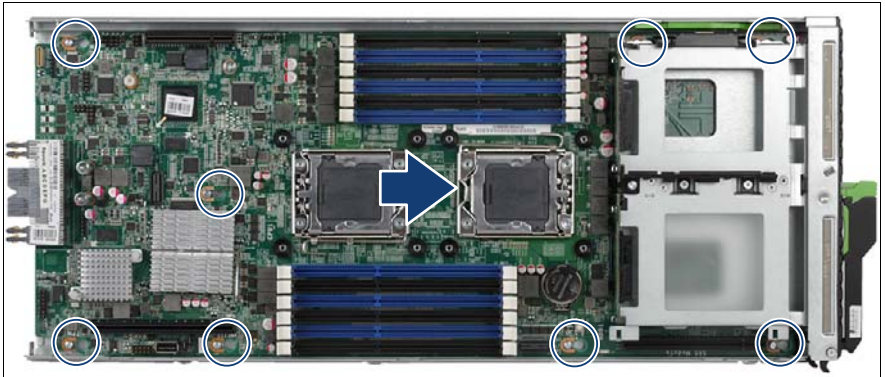


Figure 106: Installing the system board (A)

- ▶ Lower the system board onto the centering bolts (see circles). Ensure that the system board is properly seated on the centering bolts.
- ▶ Carefully shift the system board towards the server rear as far as it will go (see arrow).



Figure 107: Installing the system board (B)

- ▶ Secure the system board with the screw (M3 x 6 mm, C26192-Y10-C68) (see circle).



Screw torque: 0.6 Nm (not applicable for the Japanese market)

- ▶ Verify the settings on the new system board (jumpers and/or switch).



For a detailed description, please refer to section ["Onboard settings" on page 259](#).

10.5.4.2 Swapping the processor

- ▶ Carefully remove the processor from its socket on the defective system board as described in [section "Removing processors" on page 191](#).



CAUTION!

Be careful not to touch or bend the pins on the processor socket!





Always replace the socket cover if you remove the processor from the socket.

- ▶ Install the processor on the new system board as described in [section "Installing processors" on page 184](#).



Since the defective system board is sent back for repair, protect the delicate processor socket springs with a socket cover.

10.5.5 Concluding steps

- ▶ If applicable, reinstall the air cowls as described in section ["Installing the air cowls" on page 181](#).
- ▶ Reinstall all remaining system board components as shown in the related sections:
 - Heat sinks: refer to section ["Installing processor heat sinks" on page 202](#)
 - Memory modules: refer to section ["Installing a memory module" on page 173](#)
 -  Install all memory modules into their original slots.
 - Mezzanine cards: refer to section ["Installing mezzanine cards" on page 130](#)
 -  Install all mezzanine cards into their original slots.
 - SAS RAID HDD module: refer to section ["Installing the SAS RAID HDD module" on page 144](#)
 - UFM: refer to section ["Installing the UFM" on page 216](#)
 - TPM (if applicable): refer to section [section "Installing the TPM" on page 226](#)
- ▶ Close the server blade as described in section ["Closing the server blade" on page 57](#).
Use the cover from the defective server blade because the COA label is stuck there.
- ▶ Reinstall the HDD/SSD modules in their original mounting bays as described in section ["Installing a 2.5-inch HDD/SSD module" on page 103](#).
- ▶ Reinstall and secure the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ If applicable, close the rack door as described in section ["Closing the rack door" on page 62](#).
- ▶ Update the system board BIOS and iRMC to the latest version as described in section ["Updating or recovering the system board BIOS and iRMC" on page 75](#).

System board components

- ▶ When iSCSI boot is used via onboard CNA, the Onboard CNA OpROM has to be enabled in the system board BIOS. If applicable, proceed as described in section ["Enabling Option ROM scan" on page 82](#).
- ▶ If applicable, activate TPM functionality in the system BIOS under *Security > TPM (Security Chip) Setting > Security Chip*. For more information, refer to the "D3142 BIOS Setup Utility for PRIMERGY BX920 S4" reference manual.
- ▶ Verify and update time settings as described in section ["Verifying the system time settings" on page 88](#).
- ▶ Inform the customer about changed WWN and MAC addresses. For further information, refer to section ["Looking up changed MAC / WWN addresses" on page 94](#).
- ▶ After replacing the system board in a server blade running Linux OS, update the MAC address of the onboard network controller in the related NIC definition file as described in section ["Updating the NIC configuration file in a Linux environment" on page 91](#).
- ▶ Enable boot watchdog functionality as described in section ["Enabling boot watchdog functionality" on page 86](#).
- ▶ If BitLocker functionality is used and has been disabled before starting the maintenance task, re-enable BitLocker as described in section ["Enabling BitLocker functionality" on page 93](#).
- ▶ If applicable, restore LAN teaming configurations as described in section ["After replacing the server blade" on page 97](#).
- ▶ Please observe the notes on RAID rebuild in section ["Performing a RAID array rebuild" on page 94](#).

11 Server blade

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 blade remain hot after shutdown. After shutting down the server blade, 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 31.

11.1 Replacing the server blade



Field Replaceable Units (FRU)



Average hardware task duration: 50 minutes



Average software task duration: 10 minutes



Ensure to note down your current network settings before replacing the server blade.

When replacing server blade, 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.

- ▶ If possible, save the BIOS settings as described in section ["Saving BIOS settings" on page 65](#).
- ▶ If possible, save the iRMC settings as described in section ["Saving iRMC settings" on page 65](#).
- ▶ Exit all applications and shut down the server blade correctly. If your operating system has not switched off the server blade, press the on/off button on the server blade control panel.
- ▶ If applicable, remove the HDD/SSD modules from the server blade, see section ["Removing the 2.5-inch HDD/SSD module" on page 109](#).



Ensure to take note of the HDD/SSD modules mounting positions for reassembly.

- ▶ Remove the server blade from the system unit, see section ["Removing a server blade" on page 54](#).
- ▶ Open both server blades, see section ["Opening the server blade" on page 56](#).
- ▶ Remove the heat sinks from the defective server blade, see section ["Handling processor heat sinks" on page 201](#).
- ▶ Remove the processors from the defective server blade and install it into the new server blade, see section ["Upgrading or replacing processors" on page 198](#).

- ▶ Install the heat sinks in the new server blade, see section ["Handling processor heat sinks" on page 201](#).
- ▶ Remove the mezzanine cards carrier with the installed mezzanine card(s) from the defective server blade, see section ["Removing mezzanine cards" on page 136](#).
- ▶ Remove the memory modules from the defective server blade and install it into the new server blade and install it into the new server blade, see section ["Replacing memory modules" on page 178](#).
- ▶ If the SAS backplane is installed, remove the SAS backplane from the defective server blade and remove the SATA backplane from the new server blade as described in section of ["Removing the HDD/SSD backplane" on page 114](#).
- ▶ Install the SAS backplane to the new server blade as described in section of ["Installing the HDD/SSD backplane" on page 115](#).
- ▶ If an UFM is installed, remove it from the defective server blade and install it into the new server blade, see section ["Replacing the UFM" on page 222](#).
- ▶ If an TPM is installed, remove it from the defective server blade and install it into the new server blade, see section ["Replacing the TPM" on page 235](#).
- ▶ If an onboard SAS enabling key is installed, remove it from the defective server blade and install it into the new server blade, see section ["Onboard SAS enabling key" on page 238](#).
- ▶ Install the mezzanine cards carrier into the new server blade, see section ["Installing mezzanine cards" on page 130](#).
- ▶ If an FBU is installed, remove it from the defective server blade, see section ["Removing the FBU \(Flash Backup Unit\)" on page 155](#).
- ▶ If an SAS RAID HDD module is installed, remove it from the defective server blade and install it into the new server blade, see section ["Replacing the SAS RAID HDD module" on page 150](#).
- ▶ If applicable, install the FBU in the new server blade, see section ["Installing the FBU \(Flash Backup Unit\)" on page 152](#).
- ▶ Use the cover from the defective server blade and close the server blade, see section ["Closing the server blade" on page 57](#).
Use the cover from the defective server blade because the COA label is stuck there.



It is necessary to complete ID card with the model name and the serial number. Please use the new label.

- If applicable, reinstall the HDD/SSD modules in their original mounting bays, see section "[Installing the 2.5-inch HDD/SSD module](#)" on page 105.
- Insert the server blade in the system unit see section "[Installing the server blade in the system unit](#)" on page 58.
- If available, update the system board BIOS and the iRMC to the latest version as described in section "[Updating or recovering the system board BIOS and iRMC](#)" on page 75.
- If available, restore the BIOS settings as described in section "[Restoring BIOS settings](#)" on page 80.
- If available, restore the iRMC settings as described in section "[Restoring iRMC settings](#)" on page 80.



In order to enable ServerView Operations Manager and ServerView Installation Manager to identify the system, it is necessary to program the chassis ID prom using the "ChassisIDProm Tool" after installing the new Server Blade.

12 Appendix

12.1 Mechanical overview

12.1.1 Server blade front

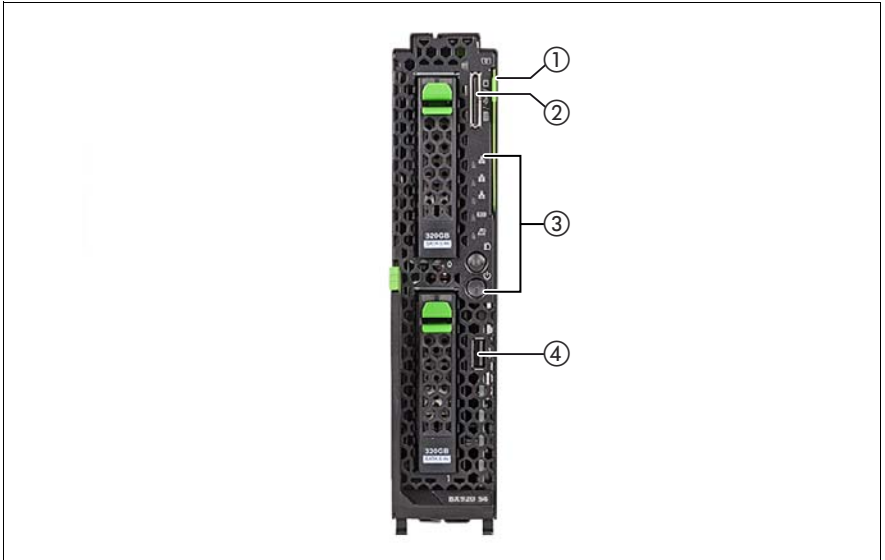


Figure 108: PRIMERGY BX920 S4 server blade front

Pos.	Component
1	ID card
2	Y-cable connector
3	Front panel (buttons and indicators)
4	USB connector

12.1.2 Server blade interior

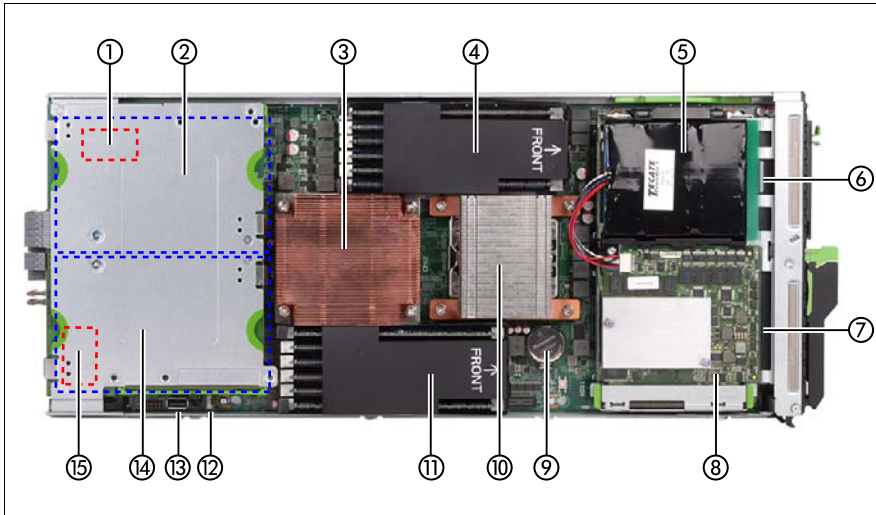


Figure 109: PRIMERGY BX920 S4 interior

Pos.	Component
1	UFM (option, on the system board, in the figure below mezzanine card 1)
2	Mezzanine card 1 slot (under the support plate)
3	CPU 1 / Heatsink
4	Memory modules for CPU 2
5	FBU
6	Mounting bay for HDD 0
7	Mounting bay for HDD 1
8	SAS RAID HDD module
9	CMOS battery
10	CPU 2 / Heatsink
11	Memory modules for CPU 1
12	Onboard SAS enabling key connector
13	Onboard USB connector
14	Mezzanine card 2 slot (under the support plate)
15	TPM (option, on the system board, in the figure below mezzanine card 2)

12.2 Configuration tables

12.2.1 Memory configuration table

Please refer to chapter ["Main memory"](#) on page 163.

12.2.2 Mezzanine card configuration table

Please refer to chapter ["Population rules for mezzanine cards"](#) on page 124.

12.3 Connectors and indicators

12.3.1 Connectors and indicators on the system board

12.3.1.1 Onboard connectors

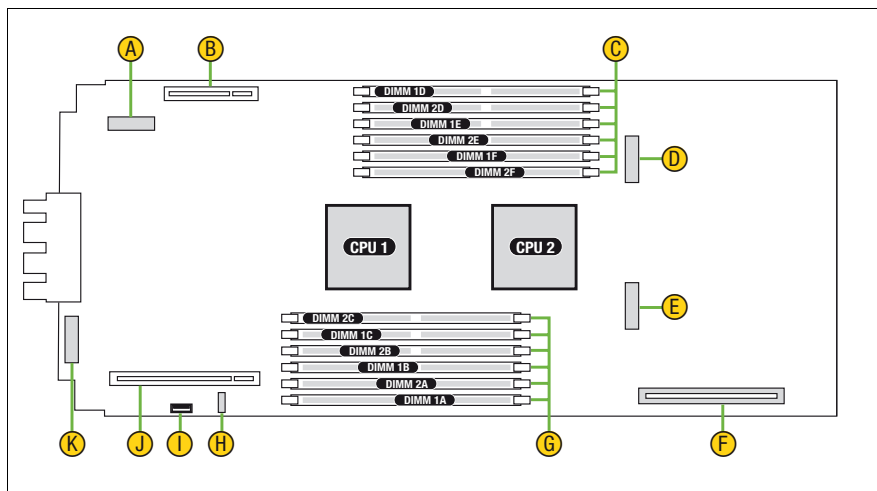


Figure 110: Internal connectors of system board D3142

No.	Print	Description
A	UFM	Connector for UFM
B	Mezz 1	Connector for mezzanine card 1
C	Memory modules	Connectors for memory modules
D	HDD 0	Connector for HDD 0
E	HDD 1	Connector for HDD 1
F	SAS Module	Connector for SAS RAID HDD module
G	Memory modules	Connectors for memory modules
H	Onboard SAS enabling key	Connector for onboard SAS enabling key
I	USB Dongle	Connector for onboard USB port
J	Mezz 2	Connector for mezzanine card 2
K	TPM	Connector for TPM

12.3.1.2 Onboard settings

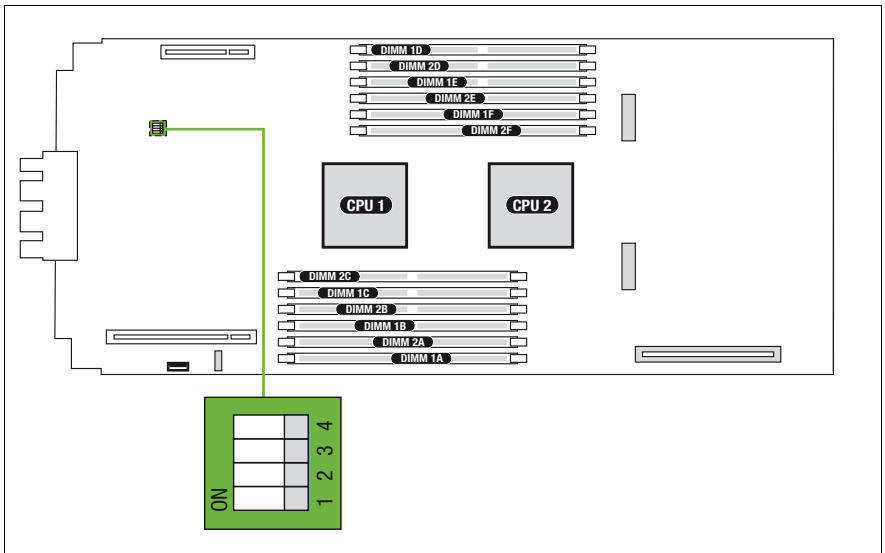


Figure 111: Onboard settings on system board D3142

Switch	Status	Description
Switch 1	On	CMOS clear
Switch 2	On	Clear Password
Switch 3	On	System BIOS recovery / NVRAM clear
Switch 4	On	ME_RCVR (for service personnel only)



Default settings: Switch 1 to 4 = *Off*

12.3.1.3 Onboard indicators and controls

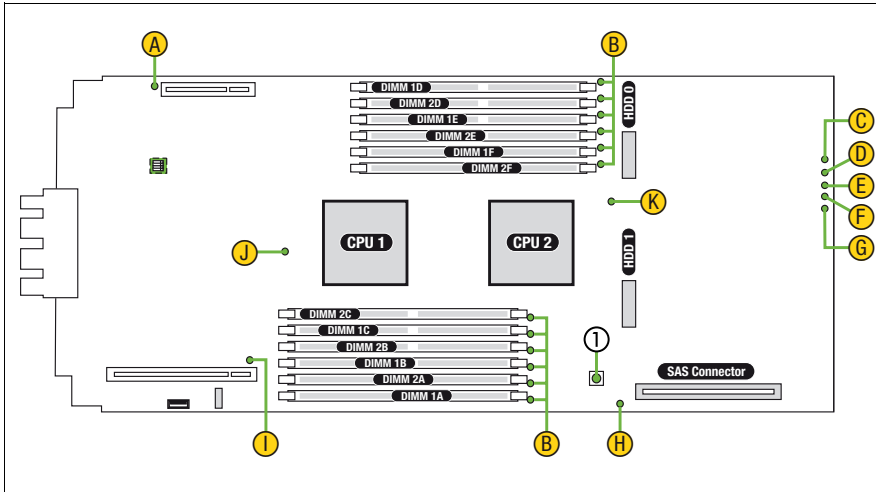


Figure 112: Onboard indicators and Indicate CSS button

No.	Description
1	Indicate CSS button

Using the Indicate CSS button

- ▶ Shut down the server blade as described in section ["Shutting down the server blade"](#) on page 53.
- ▶ Remove the server blade from the system unit as described in section ["Removing the server blade from the system unit"](#) on page 55.
- ▶ Open the server blade as described in section ["Opening the server blade"](#) on page 56.
- ▶ Press the Indicate CSS button (1) to highlight defective components.

Component LEDs



The LEDs C to G are visible from the outside. All other LEDs are only visible if the server blade has been opened. In order to access memory LEDs (B), the air cowls need to be removed (see section ["Removing the air cowls"](#) on page 182).

Indicator		Status	Description
A	Mezzanine card 1	off	Mezzanine card 1 operational
		orange on	Mezzanine card 1 failure
B	Memory	off	memory module operational
		orange on	memory module failure
C	Fabric 3/4	off	Fabric 3/4 no network connection
		green flashing	Fabric 3/4 network connection
		green on	Fabric 3/4 an active network connection
D	Fabric 2	off	Fabric 2 no network connection
		green flashing	Fabric 2 network connection
		green on	Fabric 2 an active network connection
E	Fabric 1	off	Fabric 1 no network connection
		green flashing	Fabric 1 network connection
		green on	Fabric 1 an active network connection
F	CSS	off	System is ok
		yellow flashing	An error was detected that you can fix yourself with the CSS concept.
		yellow on	A prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept.
G	Global Error	off	No critical event
		orange flashing	An error was detected that requires service intervention.
		orange on	A prefailure event has been detected that requires (precautionary) service intervention.
H	SAS RAID HDD module	off	SAS RAID HDD module operational
		orange on	SAS RAID HDD module failure
I	Mezzanine card 2	off	Mezzanine card 2 operational
		orange on	Mezzanine card 2 failure
J	CPU 1	off	CPU 1 operational
		orange on	CPU 1 failure
K	CPU 2	off	CPU 2 operational
		orange on	CPU 2 failure

12.3.2 Connectors and indicators on the front

12.3.2.1 Front panel connectors

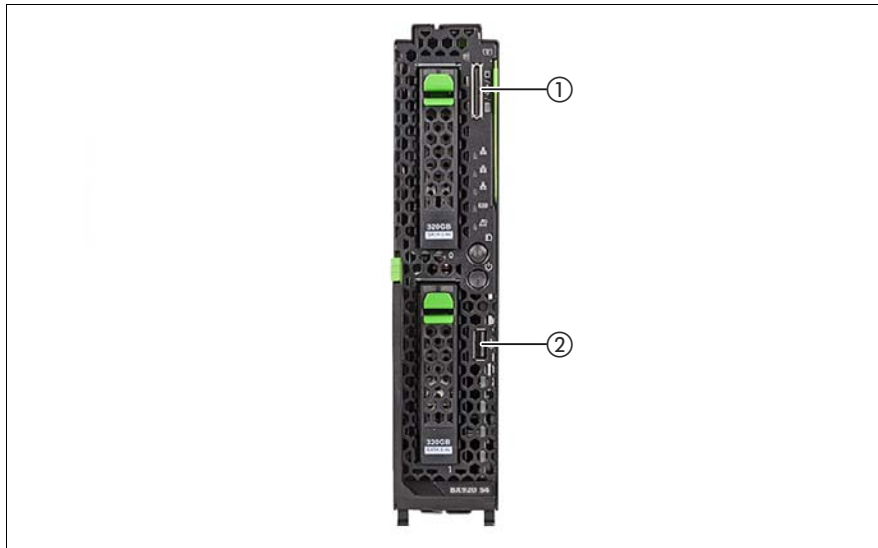


Figure 113: Front panel connectors

Pos.	Component
1	Y-cable port
2	USB connector

12.3.2.2 Front panel indicators



Figure 114: I/O panel indicators

Indicator		Status	Description
1	Fabric 3/4	off	Fabric 3/4 no network connection
		green flashing	Fabric 3/4 an active network connection
		green on	Fabric 3/4 network connection
2	Fabric 2	off	Fabric 2 no network connection
		green flashing	Fabric 2 an active network connection
		green on	Fabric 2 network connection
3	Fabric 1	off	Fabric 1 no network connection
		green flashing	Fabric 1 an active network connection
		green on	Fabric 1 network connection

Appendix

Indicator		Status	Description
4	CSS indicator	off	System is ok
		yellow on	A prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept.
		yellow flashing	An error was detected that you can fix yourself with the CSS concept.
5	Global error indicator	off	No critical event
		orange on	A prefailure event has been detected that requires (precautionary) service intervention.
		orange flashing	An error was detected that requires service intervention.
6	ID indicator	blue on	Server has been highlighted using management blade web interface, ServerView Operations Manager, or the ID button on the front panel for easy identification.
7	Power indicator	off	No line voltage is present.
		green flashing	Server has been switched on and is in standby mode.
		green on	Server is switched on.
		orange on	Server is switched off but line voltage is present.
		yellow on	Power supply error.

12.3.2.3 Indicators on the hot-plug HDD/SSD module



Figure 115: Indicators on the 2.5-inch HDD module

1	<p>HDD/SSD BUSY (green)</p> <ul style="list-style-type: none"> – Lights up: HDD/SSD in active phase – Does not light: HDD/SSD inactive (drive inactive)
2	<p>HDD/SSD FAULT (orange) (in conjunction with a RAID controller)</p> <ul style="list-style-type: none"> – Does not light: no HDD/SSD error – Lights up: HDD/SSD Faulty or Rebuild Stopped (drive defective, needs replacing, a rebuild process was stopped or the HDD/SSD module is not correctly inserted) – Slow flashing: HDD/SSD Rebuild (the data is being restored after changing a drive) – Fast flashing: HDD/SSD Identify

12.4 Minimum startup configuration



Field Replaceable Units (FRU)

If the server blade 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:

Component	Notes and reference
BX920 S4 server blade	
1 CPU with heat sink	Installed in slot CPU 1, see section "Basic information" on page 184 .
1 memory module	Installed in socket DIMM 1A, see section "Basic information" on page 164

Table 7: Minimum startup configuration - components

- ▶ Shut down the server blade as described in section ["Shutting down the server blade" on page 53](#).
- ▶ Remove the server blade from the system unit as described in section ["Removing a server blade" on page 54](#).
- ▶ Take the server blade down to its minimum startup configuration.
- ▶ Reinstall the server blade in the system unit as described in section ["Installing the server blade in the system unit" on page 58](#).
- ▶ Switch on the server blade as described in section ["Switching on the server blade" on page 60](#).
- ▶ Login to the management blade web interface, see section ["Accessing the management blade web interface" on page 43](#).