

FUJITSU Server PRIMERGY RX1330 M1

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 © 2015 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:

Shielded LAN cables should be used in this product.

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)
- USB Flash Module (UFM)

Version history

Issue number	Reason for update
1.0 / August 2014	Initial release
2.0 / September 2014	Max load label removed from photos
3.0 / May 2015	Section 11.2.7 note added, cable tie for front VGA cable added, iRMC microSD card added

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	ENERGY STAR	39
3.3	CE conformity	39
3.4	FCC Class A Compliance Statement	40
3.5	Environmental protection	41
4	Basic hardware procedures	43
4.1	Using diagnostics information	43
4.1.1	Locating the defective server	43
4.1.2	Determining the error class	44
4.1.2.1	Global Error indicator	44
4.1.2.2	Customer Self Service (CSS) indicator	44
4.1.3	Locating the defective component	45
4.1.3.1	Local diagnostic indicators on the system board	45
4.2	Shutting down the server	45

Contents

4.3	Disconnecting the server from the mains	46
4.4	Getting access to the component	47
4.4.1	Extending the server out of the rack	48
4.4.2	Removing the server from the rack	49
4.4.3	Removing the top cover	51
4.5	Reassembling	52
4.5.1	Installing the top cover	52
4.5.2	Mounting the server in the rack	53
4.5.3	Sliding the server into the rack	55
4.6	Connecting the server to the mains	55
4.7	Switching on the server	57
4.8	Handling riser modules	58
4.8.1	Removing a riser module	58
4.8.2	Installing a riser module	60
5	Basic software procedures	63
5.1	Starting the maintenance task	63
5.1.1	Suspending BitLocker functionality	63
5.1.2	Disabling SVOM boot watchdog functionality	64
5.1.2.1	Viewing boot watchdog settings	64
5.1.2.2	Configuring boot watchdog settings	65
5.1.3	Removing backup and optical disk media	66
5.1.4	Verifying and configuring the backup software solution	67
5.1.5	Note on server maintenance in a Multipath I/O environment	67
5.1.6	Switching on the ID indicator	70
5.2	Completing the maintenance task	71
5.2.1	Updating or recovering the system board BIOS and iRMC	71
5.2.1.1	Updating or recovering the system board BIOS	71
5.2.1.2	Updating or recovering the iRMC	71
5.2.2	Verifying system information backup / restore	73
5.2.3	Updating RAID controller firmware	74
5.2.4	Enabling Option ROM scan	75
5.2.5	Verifying and configuring the backup software solution	76
5.2.6	Resetting the boot retry counter	77
5.2.6.1	Viewing the boot retry counter	77
5.2.6.2	Resetting the boot retry counter	77
5.2.7	Enabling SVOM boot watchdog functionality	78

5.2.8	Enabling replaced components in the system BIOS	79
5.2.9	Verifying the memory mode	80
5.2.10	Verifying the system time settings	80
5.2.11	Viewing and clearing the System Event Log (SEL)	81
5.2.11.1	Viewing the SEL	81
5.2.11.2	Clearing the SEL	82
5.2.12	Updating the NIC configuration file in a Linux environment	83
5.2.13	Resuming BitLocker functionality	84
5.2.14	Performing a RAID array rebuild	85
5.2.15	Looking up changed MAC / WWN addresses	85
5.2.15.1	Looking up MAC addresses	86
5.2.15.2	Looking up WWN addresses	86
5.2.16	Using the Chassis ID Prom Tool	87
5.2.17	Configuring LAN teaming	88
5.2.17.1	After replacing / upgrading LAN controllers	88
5.2.17.2	After replacing the system board	89
5.2.18	Switching off the ID indicator	89
5.2.19	Performing a fan test after replacing a defective fan	89
6	Power supply	91
6.1	Basic information	92
6.2	Standard power supply	93
6.2.1	Replacing the standard power supply unit	93
6.2.1.1	Preliminary steps	93
6.2.1.2	Removing the defective standard power supply unit	93
6.2.1.3	Installing the new standard power supply unit	95
6.2.1.4	Concluding steps	96
6.3	Redundant power supply	97
6.3.1	Installing a hot-plug power supply unit	97
6.3.1.1	Preliminary steps	97
6.3.1.2	Removing the dummy cover	97
6.3.1.3	Installing a hot-plug power supply unit	98
6.3.1.4	Concluding steps	99
6.3.2	Removing a hot-plug power supply unit	100
6.3.2.1	Preliminary steps	102
6.3.2.2	Removing a hot-plug power supply unit	102
6.3.2.3	Installing the dummy cover	103
6.3.3	Replacing a hot-plug power supply unit	103
6.3.3.1	Preliminary steps	104

Contents

6.3.3.2	Removing the defective hot-plug power supply unit	104
6.3.3.3	Installing the new hot-plug power supply unit	105
6.3.3.4	Concluding steps	105
6.3.4	Replacing the power distribution board	105
6.3.4.1	Preliminary steps	105
6.3.4.2	Removing the defective power distribution board	106
6.3.4.3	Installing the new power distribution board	107
6.3.4.4	Concluding steps	108
6.4	Converting a standard power supply to a redundant power supply	108
6.4.1	Preliminary steps	109
6.4.2	Removing the standard power supply unit	109
6.4.3	Installing the upgrade kit	110
6.4.4	Concluding steps	114
7	Hard disk drives / solid state drives	115
7.1	Basic information	116
7.2	2.5-inch HDD/SSD configurations	117
7.2.1	Equipping the 2.5-inch HDD/SSD bays	117
7.2.2	Configuration with up to four HDD/SSD modules	117
7.2.3	Configuration with up to eight HDD/SSD modules	118
7.2.4	Configuration with up to 10 HDD/SSD modules	119
7.2.5	Installing 2.5-inch HDD/SSD modules	120
7.2.5.1	Preliminary steps	120
7.2.5.2	Removing a 2.5-inch HDD/SSD dummy module	120
7.2.5.3	Installing a 2.5-inch HDD/SSD module	121
7.2.5.4	Concluding steps	122
7.2.6	Removing 2.5-inch HDD/SSD modules	122
7.2.6.1	Preliminary steps	122
7.2.6.2	Removing a 2.5-inch HDD/SSD module	123
7.2.6.3	Installing a 2.5-inch HDD/SSD dummy module	124
7.2.6.4	Concluding steps	124
7.2.7	Replacing a 2.5-inch HDD/SSD module	124
7.2.7.1	Preliminary steps	125
7.2.7.2	Removing the defective 2.5-inch HDD/SSD module	125
7.2.7.3	Installing the new 2.5-inch HDD/SSD module	125
7.2.7.4	Concluding steps	125

7.2.8	Replacing the 4 x 2.5-inch HDD backplane	126
7.2.8.1	Preliminary steps	126
7.2.8.2	Removing the defective 4 x 2.5-inch HDD backplane	126
7.2.8.3	Installing the new 4 x 2.5-inch HDD backplane	128
7.2.8.4	Concluding steps	131
7.2.9	Replacing the 10 x 2.5-inch HDD backplane	132
7.2.9.1	Preliminary steps	132
7.2.9.2	Removing the SAS expander board	132
7.2.9.3	Removing the defective 10 x 2.5-inch HDD backplane	134
7.2.9.4	Installing the new 10 x 2.5-inch HDD backplane	135
7.2.9.5	Installing the SAS expander board	135
7.2.9.6	Concluding steps	137
7.2.10	Replacing the SAS expander board	138
7.2.10.1	Preliminary steps	138
7.2.10.2	Removing the defective SAS expander board	138
7.2.10.3	Installing the new SAS expander board	138
7.2.10.4	Concluding steps	138
7.2.11	Upgrading configuration from up to four to up to eight 2.5-inch HDDs/SSDs	139
7.2.11.1	Preliminary steps	139
7.2.11.2	Installing the second HDD backplane	139
7.2.11.3	Installing additional HDD/SSD modules	140
7.2.11.4	Concluding steps	140
7.3	3.5-inch HDD configurations	141
7.3.1	Equipping the 3.5-inch HDD bays	141
7.3.2	Installing 3.5-inch HDD modules	142
7.3.2.1	Preliminary steps	142
7.3.2.2	Removing a 3.5-inch HDD dummy module	142
7.3.2.3	Installing a 3.5-inch HDD module	143
7.3.2.4	Concluding steps	143
7.3.3	Removing 3.5-inch HDD modules	144
7.3.3.1	Preliminary steps	144
7.3.3.2	Removing a 3.5-inch HDD module	145
7.3.3.3	Installing a 3.5-inch dummy module	145
7.3.3.4	Concluding steps	145
7.3.4	Replacing a 3.5-inch HDD module	146
7.3.4.1	Preliminary steps	146
7.3.4.2	Removing the defective 3.5-inch HDD module	147
7.3.4.3	Installing the new 3.5-inch HDD module	147
7.3.4.4	Concluding steps	147

Contents

7.3.5	Replacing the 3.5-inch HDD backplane	147
7.3.5.1	Preliminary steps	147
7.3.5.2	Removing the defective 3.5-inch HDD backplane	147
7.3.5.3	Installing the new 3.5-inch HDD backplane	148
7.3.5.4	Concluding steps	149
8	Fans	151
8.1	Basic information	151
8.1.1	Numbering of the fan modules	152
8.2	Replacing a defective fan module	152
8.2.1	Preliminary steps	152
8.2.2	Removing the defective fan module	153
8.2.3	Installing the new fan module	154
8.2.4	Concluding steps	155
9	Expansion cards and backup units	157
9.1	Basic information	158
9.1.1	Equipping the PCIe slots	158
9.2	Handling slot brackets	161
9.2.1	Installing a slot bracket	161
9.2.2	Removing a slot bracket	163
9.2.2.1	Removing the slot bracket	163
9.3	Handling SFP+ transceiver modules	164
9.3.1	Installing SFP+ transceiver modules	164
9.3.2	Removing an SFP+ transceiver module	167
9.4	Expansion cards and riser cards	170
9.4.1	Installing an expansion card	170
9.4.1.1	Preliminary steps	170
9.4.1.2	Removing the slot cover	170
9.4.1.3	Installing the expansion card	171
9.4.1.4	Concluding steps	171
9.4.2	Removing an expansion card	172
9.4.2.1	Preliminary steps	172
9.4.2.2	Removing the expansion card	172
9.4.2.3	Installing the slot cover	173
9.4.2.4	Concluding steps	173

9.4.3	Replacing an expansion card	174
9.4.3.1	Preliminary steps	174
9.4.3.2	Removing the defective expansion card	174
9.4.3.3	Installing the new expansion card	175
9.4.3.4	Concluding steps	175
9.4.4	Replacing a riser card	176
9.4.4.1	Preliminary steps	176
9.4.4.2	Removing the defective riser card	176
9.4.4.3	Installing the new riser card	177
9.4.4.4	Concluding steps	177
9.4.5	Replacing a TFM	178
9.4.5.1	Preliminary steps	178
9.4.5.2	Removing the defective TFM	178
9.4.5.3	Installing the new TFM	180
9.4.5.4	Concluding steps	181
9.4.6	Upgrading to the full height riser module	182
9.4.6.1	Preliminary steps	182
9.4.6.2	Installing the upgrade kit	183
9.5	Backup units (BBU/FBU)	186
9.5.1	Installing a BBU	186
9.5.1.1	Preliminary steps	186
9.5.1.2	Preparing the BBU	187
9.5.1.3	Installing the BBU	189
9.5.1.4	Concluding steps	191
9.5.2	Installing an FBU	192
9.5.2.1	Preliminary steps	192
9.5.2.2	Preparing the FBU	193
9.5.2.3	Installing the FBU	194
9.5.2.4	Concluding steps	195
9.5.3	Removing a BBU	196
9.5.3.1	Preliminary steps	196
9.5.3.2	Removing the BBU with the holder	196
9.5.3.3	Removing the BBU from the holder	197
9.5.3.4	Disconnecting the BBU cable from the BBU	197
9.5.3.5	Concluding steps	197
9.5.4	Removing an FBU	198
9.5.4.1	Preliminary steps	198
9.5.4.2	Removing the FBU with the holder	198
9.5.4.3	Disconnecting the FBU cable from the FBU	199
9.5.4.4	Removing the FBU from the holder	199
9.5.4.5	Concluding steps	200

Contents

9.5.5	Replacing a BBU	200
9.5.5.1	Preliminary steps	200
9.5.5.2	Removing the defective BBU	200
9.5.5.3	Installing the new BBU	201
9.5.5.4	Concluding steps	201
9.5.6	Replacing an FBU	202
9.5.6.1	Preliminary steps	202
9.5.6.2	Removing the defective FBU	202
9.5.6.3	Installing the new FBU	202
9.5.6.4	Concluding steps	203
10	Main memory	205
10.1	Basic information	206
10.1.1	Memory sequence	207
10.1.1.1	Population rules	207
10.1.1.2	Modes of operation	208
10.2	Installing a memory module	209
10.2.1	Preliminary steps	209
10.2.2	Selecting the memory slot	209
10.2.3	Installing a memory module	209
10.2.4	Concluding steps	210
10.3	Removing a memory module	210
10.3.1	Preliminary steps	210
10.3.2	Removing a memory module	211
10.3.3	Concluding steps	211
10.4	Replacing a memory module	211
10.4.1	Preliminary steps	211
10.4.2	Removing the defective memory module	212
10.4.3	Installing the new memory module	212
10.4.4	Concluding steps	212
11	Processor	213
11.1	Basic information	214
11.1.1	Supported processors	214
11.2	Replacing the processor	214
11.2.1	Preliminary steps	215
11.2.2	Removing the heat sink	215

11.2.3	Removing the defective processor	216
11.2.4	Installing the new processor	217
11.2.5	Applying the thermal paste to the processor surface	218
11.2.6	Installing the heat sink	220
11.2.7	Concluding steps	220
11.3	Replacing the heat sink	221
11.3.1	Preliminary steps	221
11.3.2	Removing the defective heat sink	221
11.3.3	Installing the new heat sink	222
11.3.4	Concluding steps	222
12	Optical disk drive	223
<hr/>		
12.1	Basic information	224
12.2	Installing the ODD	227
12.2.1	Preliminary steps	227
12.2.2	Removing the dummy cover	227
12.2.3	Installing the ODD	228
12.2.4	Concluding steps	229
12.3	Removing the ODD	230
12.3.1	Preliminary steps	230
12.3.2	Removing the ODD	230
12.3.3	Installing the dummy cover	232
12.3.4	Concluding steps	232
12.4	Replacing the ODD	233
12.4.1	Preliminary steps	233
12.4.2	Removing the defective ODD	233
12.4.3	Installing the new ODD	233
12.4.4	Concluding steps	233
13	Front panel	235
<hr/>		
13.1	Basic information	235
13.2	Front panel module	236
13.2.1	Replacing the front panel module	236
13.2.1.1	Preliminary steps	236
13.2.1.2	Removing the front panel module	237
13.2.1.3	Installing the front panel module	239

Contents

13.2.1.4	Concluding steps	241
13.3	Front VGA board	241
13.3.1	Installing the front VGA board	241
13.3.1.1	Preliminary steps	241
13.3.1.2	Removing the dummy cover	242
13.3.1.3	Installing the front VGA board	242
13.3.1.4	Concluding steps	243
13.3.2	Removing the front VGA board	243
13.3.2.1	Preliminary steps	243
13.3.2.2	Removing the front VGA board	244
13.3.2.3	Installing the dummy cover	244
13.3.2.4	Concluding steps	244
13.3.3	Replacing the front VGA board	245
13.3.3.1	Preliminary steps	245
13.3.3.2	Removing the defective front VGA board	245
13.3.3.3	Installing the new front VGA board	245
13.3.3.4	Concluding steps	245
13.4	Front panel on QRL (10 x 2.5-inch HDD configuration)	246
13.4.1	Replacing the front panel on QRL	246
13.4.1.1	Preliminary steps	246
13.4.1.2	Removing the front panel on QRL	247
13.4.1.3	Installing the front panel on QRL	249
13.4.1.4	Concluding steps	250
14	System board and components	251
14.1	Basic information	251
14.2	CMOS battery	252
14.2.1	Replacing the CMOS battery	252
14.2.1.1	Preliminary steps	252
14.2.1.2	Replacing the defective CMOS battery	253
14.2.1.3	Concluding steps	253
14.3	USB Flash Module (UFM)	254
14.3.1	Installing the UFM	254
14.3.1.1	Preliminary steps	254
14.3.1.2	Installing the UFM	254
14.3.1.3	Concluding steps	255
14.3.1.4	Software configuration	256

14.3.2	Removing the UFM	256
14.3.2.1	Preliminary steps	256
14.3.2.2	Removing the UFM	257
14.3.2.3	Concluding steps	258
14.3.3	Replacing the UFM	259
14.3.3.1	Preliminary steps	259
14.3.3.2	Removing the defective UFM	259
14.3.3.3	Installing the new UFM	260
14.3.3.4	Concluding steps	260
14.3.3.5	Software configuration	261
14.4	Trusted Platform Module (TPM)	261
14.4.1	Installing the TPM	261
14.4.1.1	Preliminary steps	261
14.4.1.2	Installing the TPM	262
14.4.1.3	Concluding steps	264
14.4.2	Removing the TPM	265
14.4.2.1	Preliminary steps	265
14.4.2.2	Removing the TPM	267
14.4.2.3	Concluding steps	268
14.4.3	Replacing the TPM	269
14.4.3.1	Preliminary steps	269
14.4.3.2	Removing the defective TPM	270
14.4.3.3	Installing the new TPM	270
14.4.3.4	Concluding steps	270
14.5	iRMC microSD card	271
14.5.1	Installing the iRMC microSD card	271
14.5.1.1	Preliminary steps	271
14.5.1.2	Installing the iRMC microSD card	271
14.5.1.3	Concluding steps	272
14.5.2	Removing the iRMC microSD card	273
14.5.2.1	Preliminary steps	273
14.5.2.2	Removing the iRMC microSD card	273
14.5.2.3	Concluding steps	274
14.5.3	Replacing the iRMC microSD card	274
14.5.3.1	Preliminary steps	274
14.5.3.2	Replacing the iRMC microSD card	275
14.5.3.3	Concluding steps	275
14.6	System board	276
14.6.1	Replacing the system board	276
14.6.1.1	Preliminary steps	278
14.6.1.2	Removing the defective system board	279

Contents

14.6.1.3	Installing the new system board	280
14.6.1.4	Concluding steps	281
15	Cables	283
15.1	Overview cables	283
15.2	Cabling	285
16	Appendix	295
16.1	Mechanical overview	295
16.1.1	Server front	295
16.1.2	Server rear	297
16.1.3	Server interior	298
16.2	Connectors and indicators	300
16.2.1	Connectors and indicators on the system board	300
16.2.1.1	Onboard connectors	300
16.2.1.2	Onboard indicators and controls	302
16.2.1.3	I/O panel connectors	304
16.2.1.4	I/O panel indicators	304
16.2.1.5	Indicators on hot-plug power supply units (slide-in units)	305
16.2.2	Indicators on the front panel	306
16.2.3	Indicators on the accessible drives/components	308
16.3	Onboard settings	310
16.4	Minimum startup configuration	310

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](#).



CAUTION

In a system that has the Cool-safe[®] Advanced Thermal Design option, only components that support the higher operating range may be installed. Further information on this is available in the configurator.



The Cool-safe[®] Advanced Thermal Design option can only be ordered from the manufacturer and is indicated by the logo on the identification rating plate.

Installing optional components

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

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

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

Please refer to the following ServerView Suite topics:

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

Before you start



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/index.htm

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 indicator on the front of the server reports defective hardware components that need to be replaced. For further information on the controls and indicators of your server, refer to the operating manual of your server and section "[Connectors and indicators](#)" on page 300.

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 "[Indicators on the front panel](#)" on page 306.

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

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

2.1 Classification of procedures

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

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



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

2.1.1 Customer Replaceable Units (CRU)



Customer Replaceable Units (CRU)

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



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

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

Components that are handled as Customer Replaceable Units

- Hot-plug power supply units
- Hot-plug HDD / SSD modules

Peripherals that are handled as Customer Replaceable Units

- Keyboard
- Mouse

2.1.2 Upgrade and Repair Units (URU)



Upgrade and Repair Units (URU)

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



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

- Optical disk drives
- Expansion cards
- Battery backup units
- Memory modules
- iRMC microSD card

Components that are handled solely as Repair Units

- CMOS battery
- Fans

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

- Processor (replacement)
- SAS / SATA backplanes
- Power distribution board
- Front panel module
- System board
- Standard power supply unit
- Trusted Platform Module (TPM)
- USB Flash Module (UFM)



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

2.2 Average task duration



Hardware: 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 the following table 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.
Rack removal, disassembly	yes	making the server available, removing the server from the rack (if applicable)
Transport	no	Transporting the server to the service table (where required) depends on local customer conditions.
Maintenance procedures	yes	maintenance procedures including preliminary and concluding software tasks
Transport	no	Returning the server to its installation site (where required) depends on local customer conditions.
Assembly, rack installation	yes	reassembling the server, installing the server in the rack (if applicable)
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		Slot brackets	M3 x 3.5 mm (silver) C26192-Y10-C151
Phillips PH2 / (+) No. 2		SAS expander board	M3 x 4.5 mm (silver) C26192-Y10-C67
Phillips PH2 / (+) No. 2		System board, front panel	M3 x 6 mm (silver) C26192-Y10-C68
Torx Plus 6		ODD latch	M2 x 4 mm (black) C26192-Y10-C166
Phillips PH1 / (+) No. 1		Front VGA	M3 x 3.5 mm (silver) C26192-Y10-C102
Special bit insert		TPM screw	REM 3 x 15 mm (black) C26192-Y10-C176

Table 2: List of used screws (not applicable for the Japanese market)


Before you start

Screw driver/ bit insert	Screw	Usage	Type
Phillips PH1 / (+) No. 1		UFM nylon screw	M3 x 4.5 mm (white) C26192-Y10-C151
Phillips PH1 / (+) No. 1		TFM module	M2.5 x 4 mm (silver) C26192-Y10-C103

Table 2: List of used screws (not applicable for the Japanese market)

2.4 Documents you need at hand

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

-  – Ensure to store all printed manuals enclosed with your server in a save place for future reference.
- Unless stated otherwise, all manuals are available online at <http://manuals.ts.fujitsu.com> under *x86 Servers*.

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

Document	Description
"Quick Start Hardware - FUJITSU Server PRIMERGY RX1330 M1" leaflet	Quick installation poster for initial operation, available online
"ServerView Quick Start Guide" " ServerView クイックスタートガイド " for the Japanese market	Information on initial server setup and software configuration, available online

Table 3: Documentation you need at hand

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
"FUJITSU Server PRIMERGY RX1330 M1 Operating Manual"	available online
"D3229 BIOS Setup Utility for FUJITSU Server PRIMERGY RX1330 M1 Reference Manual"	Information on configurable BIOS options and parameters, available online
System board label	Label inside the top cover outlining connectors, indicators and jumper
Software documentation	<ul style="list-style-type: none"> – "ServerView Suite Local Service Concept (LSC)" user guide – "ServerView Operations Manager - Server Management" user guide – "iRMC S4 - Integrated Remote Management Controller" user guide – "ServerView embedded Lifecycle Management (eLCM)" 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
"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	

Table 3: Documentation you need at hand

Before you start

Document	Description
Additional documentation	RAID documentation, available online at http://manuals.ts.fujitsu.com under <i>x86 Servers - Expansion Cards - Storage Adapters</i> For the Japanese market please use the following address: http://jp.fujitsu.com/platform/server/primergy/manual/
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 A connectors.
- The unit automatically adjusts itself to a mains voltage in a range of 100 V - 240 V. 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, 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 CDs/DVDs/BDs and optical drives

When working with devices with optical 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.

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 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 drive.
- Before use, clean the optical disk tray using a soft, dry cloth.
- As a precaution, remove disks from the optical 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 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.
- Do not attach stickers or similar to the label side. Doing so may cause rotational eccentricity and abnormal vibrations.
- When a CD/DVD/BD is moved from a cold place to a warm place, moisture condensation on the CD/DVD/BD surface can cause data read errors. In this case, wipe the CD/DVD/BD with a soft, dry cloth then let it air dry. Do not dry the CD/DVD/BD using devices such as a hair dryer.
- To avoid dust, damage, and deformation, keep the CD/DVD/BD in its case whenever it is not in use.
- Do not store CDs/DVDs/BDs at high temperatures. Areas exposed to prolonged direct sunlight or near heating appliances are to be avoided.



You can prevent damage from the optical 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 drive complies with IEC 60825-1 laser class 1.



CAUTION!

The optical 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 drive casing!

Modules with Electrostatic-Sensitive Devices

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

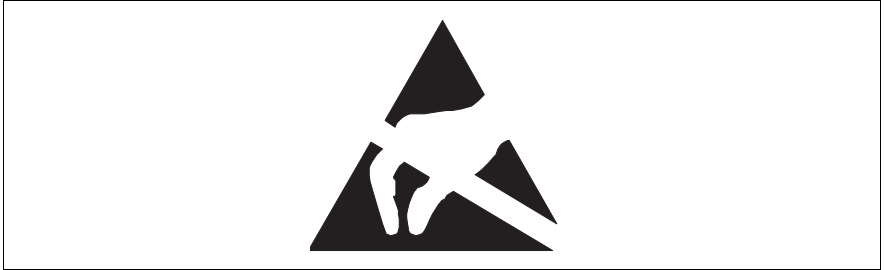


Figure 1: ESD label

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.
- You must always discharge static build-up (e.g. by touching a grounded object) before working with such components.
- 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).

Transporting the server

- Only transport the server 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 server until it is at its installation location.
- If you need to lift or transport the server, ask other people to help you.
- Never lift or carry the device by the handles on the front panel.

Notes on installing the server in the rack

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

(For the Japanese market, please refer to "安全上のご注意".)

- 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 ENERGY STAR



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

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

3.3 CE conformity



The system complies with the requirements of the EC directives 2004/108/EC regarding "Electromagnetic Compatibility" and 2006/95/EC "Low Voltage Directive" and the directive of the European Parliament and Council 2011/65/EU. This is indicated by the CE marking (CE = Communauté Européenne).

3.4 FCC Class A Compliance Statement

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

NOTE:

This equipment has been tested and found to comply with the limits for a "Class A" digital device, pursuant to Part 15 of the FCC rules and meets all requirements of the Canadian Interference-Causing Equipment Standard ICES-003 for digital apparatus. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in strict accordance with the instructions, may cause harmful interference to radio communications. However, there is no warranty that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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.

3.5 Environmental protection

Environmentally-friendly product design and development

This product has been designed in accordance with the Fujitsu standard for "environmentally friendly product design and development". This means that key factors such as durability, selection and labeling of materials, emissions, packaging, ease of dismantling and recycling have been taken into account.

This saves resources and thus reduces the harm done to the environment. Further information can be found at:

- http://ts.fujitsu.com/products/standard_servers/index.html (for the global 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

Important information

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

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 servers and components.

4.1.1 Locating the defective server

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

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



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

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

4.1.2 Determining the error class

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

- **Global Error** events that need to be resolved by maintenance personnel
- **Customer Self Service (CSS)** error events that may be resolved by operating personnel

Global Error and CSS LEDs indicate, if the defective component is a customer replaceable unit or if maintenance personnel needs to be dispatched to replace the part.



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

4.1.2.1 Global Error indicator

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

- Hardware errors:

Check the System Event Log (SEL) as described in section "[Viewing the SEL](#)" on page 81.

- Software / agent related errors:

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



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

4.1.2.2 Customer Self Service (CSS) indicator

- ▶ Check the CSS indicator on the front panel of the server.

4.1.3 Locating the defective component

After determining the error class by the CSS or Global Error indicators (see section ["Determining the error class" on page 44](#)) local diagnostic indicators on the system board, HDD modules and power supply units (only slide-in units) allow you to identify the defective component.



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

4.1.3.1 Local diagnostic indicators on the system board

Using the Indicate CSS button

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



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

- ▶ Press the Indicate CSS button to highlight defective components (see section ["Onboard indicators and controls" on page 302](#)).



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 44](#)).

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

4.2 Shutting down the server



CAUTION!

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



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

Basic hardware procedures

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



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

- ▶ Switch on the ID indicator on the front and rear connector panels of the server as described in section "[Locating the defective server](#)" on page 43.

4.3 Disconnecting the server from the mains

Standard power supply



Figure 2: Unlocking the cable tie of a standard power supply unit

- ▶ Pull out on the locking lever on the cable tie (1) and loosen the loop (2).
- ▶ Disconnect the power cord from the power supply unit and remove it from the cable tie.

Redundant power supply

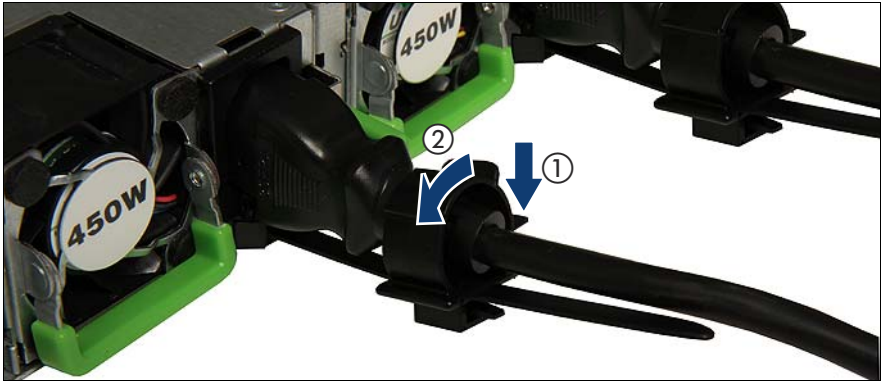


Figure 3: Unlocking the cable clamp of a power supply unit

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

4.4 Getting access to the component



CAUTION!

- Only for non-hot plug components:
Before removing or attaching covers, 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.
- The top cover must be replaced as soon as possible for purposes of cooling, to comply with EMC regulations (regulations regarding electromagnetic compatibility) and to prevent fires.
- For further safety information, please refer to chapter "[Important information](#)" on page 31.

4.4.1 Extending the server out of the rack



CAUTION!

- Use the anti-tilt plate to prevent the rack from tipping when installing the rack. Pulling the server out of the rack without having installed the anti-tilt plate may cause the rack to tip over.
 - Be careful not to pinch fingers or clothes when sliding out the server or pushing it back. Failure to do so may cause injury.
 - For further safety information, please refer to chapter "[Important information](#)" on page 31.
- ▶ Remove all remaining external cables from the rear connector panel and expansion cards.

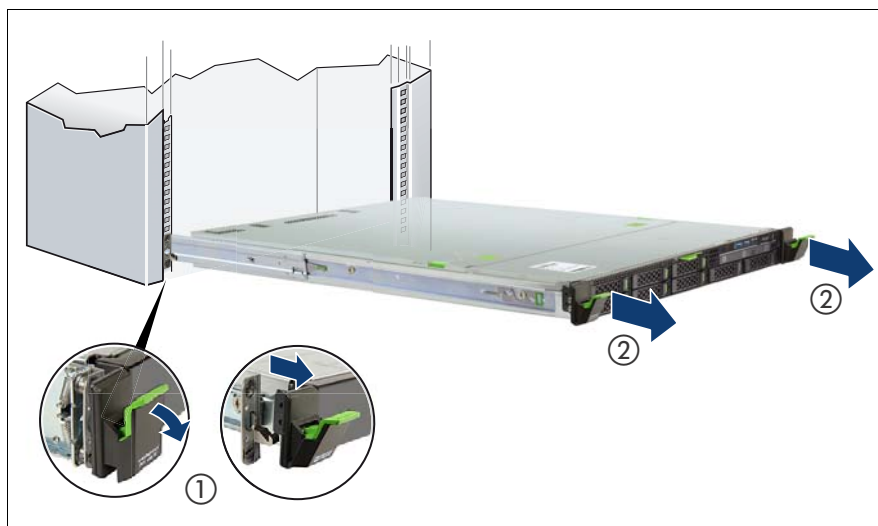


Figure 4: Extending the server out of the rack


- ▶ Fold down the two quick release levers (1).
- ▶ Pull the server out of the rack until it locks in place (2).



CAUTION!

Do not use the extended server as a surface on which to put things or as a work surface, and strictly avoid leaning on or against it.

4.4.2 Removing the server from the rack

 In most cases maintenance tasks can be performed while the server is extended from the rack. However, depending on accessibility or security guidelines, it may make sense to completely remove the server from the rack cabinet for maintenance purposes.



CAUTION!

At least two people are needed to lift the server out of the rack cabinet. (For the Japanese market, please refer to "安全上のご注意".)



For configurations below 32 kg:

At least two people are needed to lift the server out of the rack cabinet.



For configurations below 55 kg:

At least three people are needed to lift the server out of the rack cabinet.



For configurations above 55 kg:

At least four people are needed to lift the server out of the rack cabinet.

Additionally, a lifter is required in the following cases:

- The server weighs more than 50 kg.
- The server weighs more than 21 kg and is installed above the height of 25 U.

When using a lifter, this removal procedure needs to be carried out by maintenance personnel.

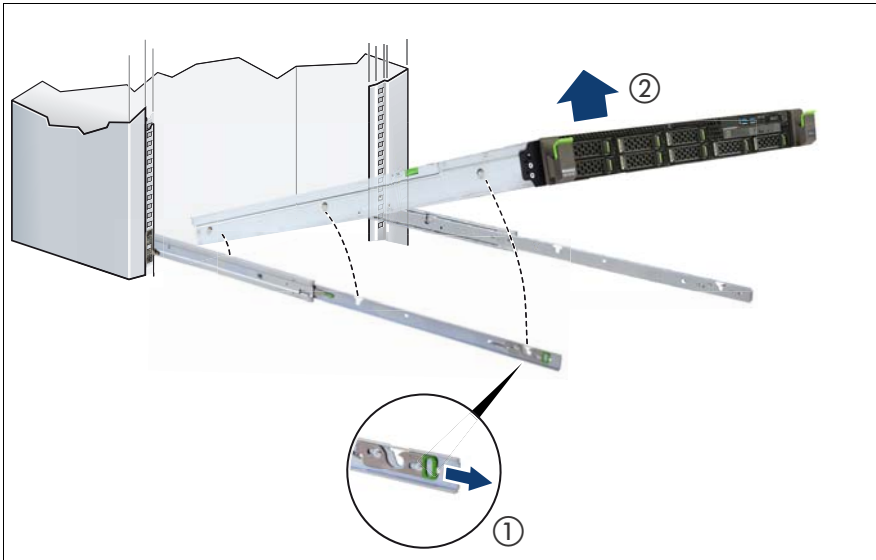


Figure 5: Removing the server from the rack

- ▶ Release the locking bars on both telescopic rails (1).
- ▶ Lift the server out of the telescopic rails (2) and place it on an even surface.

4.4.3 Removing the top cover

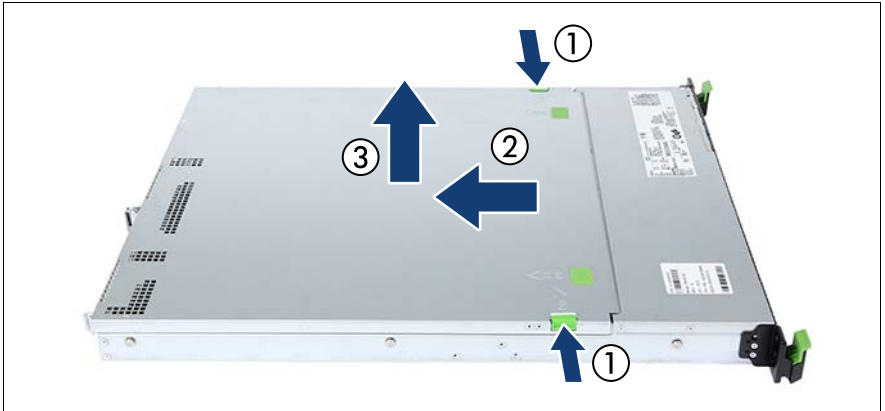


Figure 6: Removing the top cover

- ▶ Push green touch points inside (1).
- ▶ Push the top cover as far as it will go in the direction of the arrow (2).
- ▶ Lift off the top cover upward (3).

4.5 Reassembling



CAUTION!

- Before attaching the covers, make sure no unnecessary parts or tools are left inside the server.
- The top cover must be replaced as soon as possible for purposes of cooling, to comply with EMC regulations (regulations regarding electromagnetic compatibility) and to prevent fires.
- For further safety information, please refer to chapter "[Important information](#)" on page 31.

4.5.1 Installing the top cover

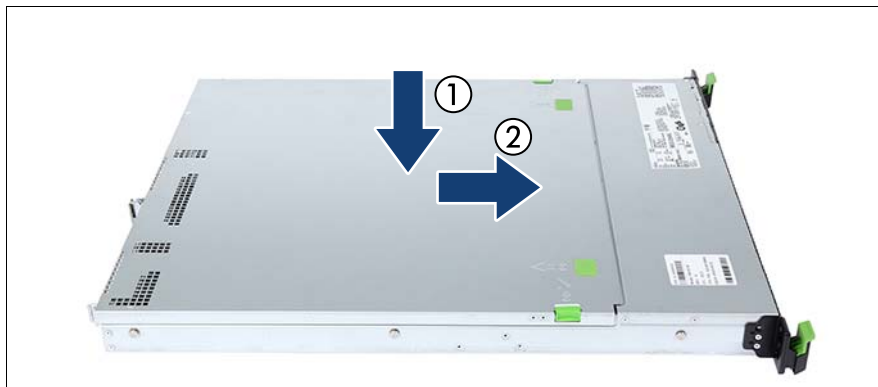


Figure 7: Attaching the top cover

- ▶ Place the top cover on the server (1).
- ▶ Push the top cover as far as it will go in the direction of the arrow (2) until it clicks in.

4.5.2 Mounting the server in the rack



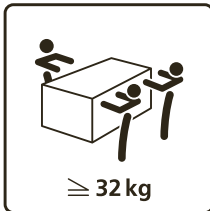
CAUTION!

At least two people are needed to position the server on the rack rails.
(For the Japanese market, please refer to "安全上のご注意".)



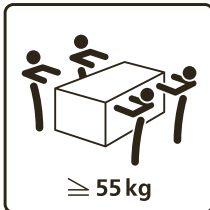
For configurations below 32 kg:

At least two people are needed to lift the server into the rack cabinet.



For configurations below 55 kg:

At least three people are needed to lift the server into the rack cabinet.



For configurations above 55 kg:

At least four people are needed to lift the server into the rack cabinet.

Additionally, a lifter is required in the following cases:

- The server weighs more than 50 kg.
- The server weighs more than 21 kg and is to be installed above the height of 25 U.

When using a lifter, this installation procedure needs to be carried out by maintenance personnel.

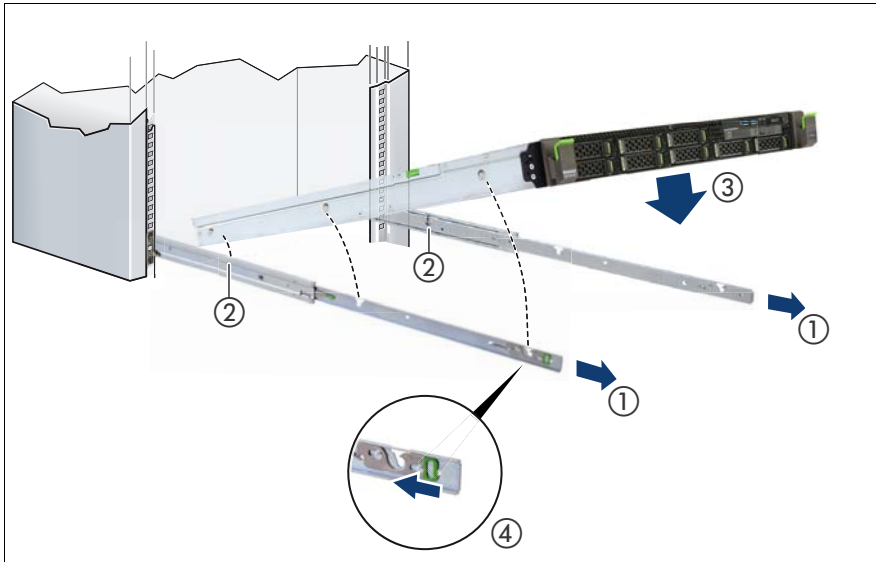


Figure 8: Inserting the server into the telescopic rails

- ▶ Fully extend the telescopic rails until they lock in place (1).
 - i** The telescopic rails must click into place so that they can no longer be moved.
- ▶ At a slight angle, lower the server onto the rear mounting point on the telescopic rails (2).
- ▶ Fold down the server, while pressing the rail to the server side (3). Ensure that all six rack mounting bolts are properly seated in the mounting points on the telescopic rails and that the locking bars engage (4).

4.5.3 Sliding the server into the rack

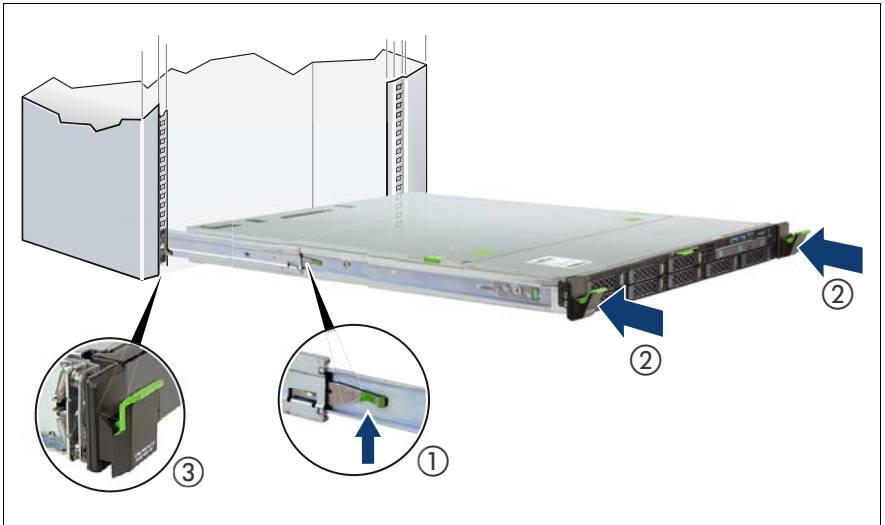


Figure 9: Sliding the server into the rack

- ▶ Release the locking mechanism of both rails (1).
- ▶ Push the server as far as it will go into the rack (2) until the quick-release levers engage (3).



CAUTION!

Be careful with your fingers. You can pinch them when the quick-release levers change to the release position.

- ▶ Reconnect all cables except the power cord to the server rear.

4.6 Connecting the server to the mains



CAUTION!

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

Standard power supply

- ▶ If applicable, connect the mains plug to a grounded mains outlet in the in-house power supply network.
- ▶ Connect the power cord to the power supply unit.

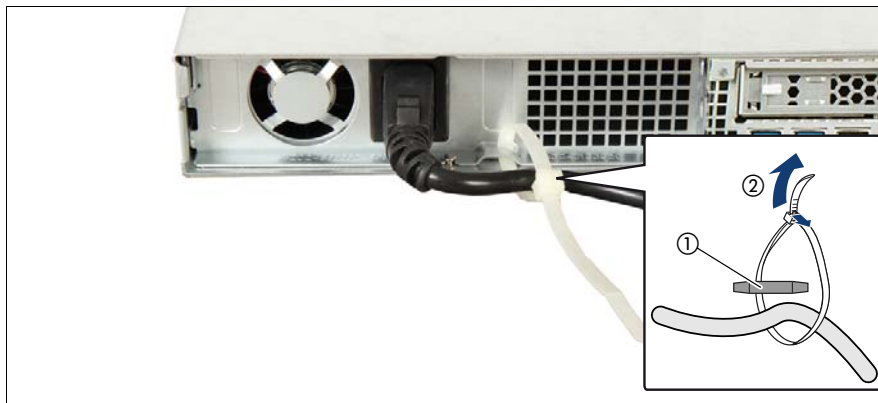


Figure 10: Example: Locking the cable tie of a standard power supply unit

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

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

Redundant power supply

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

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

- ▶ Connect the power cords to the power supply units.
- ▶ Ensure that the status indicator on the power supply unit is lit green (see section ["Indicators on hot-plug power supply units \(slide-in units\)" on page 305](#)).

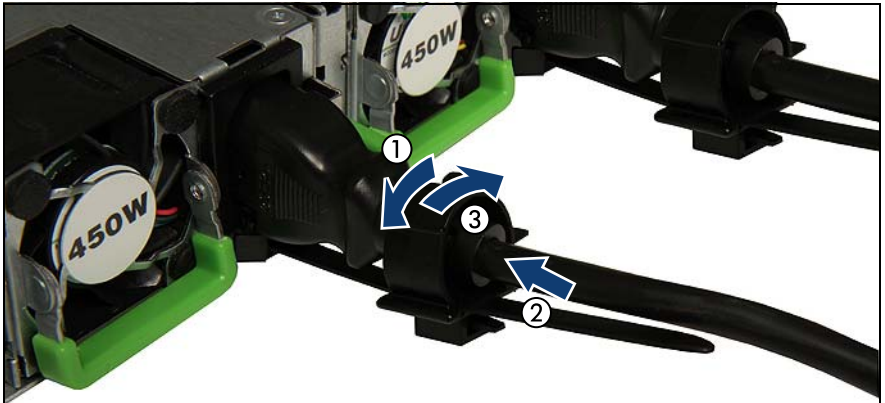


Figure 11: Example: Locking the cable clamp of a power supply unit

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

4.7 Switching on the server



CAUTION!

- Before switching on the server, make sure the top cover is closed. In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the server must not run while the top cover is removed.
 - For further safety information, please refer to chapter ["Important information" on page 31](#).
- ▶ Press the On / Off button to start up the server.
- ▶ Ensure that the power-on indicator above the On / Off button is lit green.
- ▶ Perform the required procedures described in the concluding steps of each upgrade or maintenance task.

4.8 Handling riser modules

4.8.1 Removing a riser module

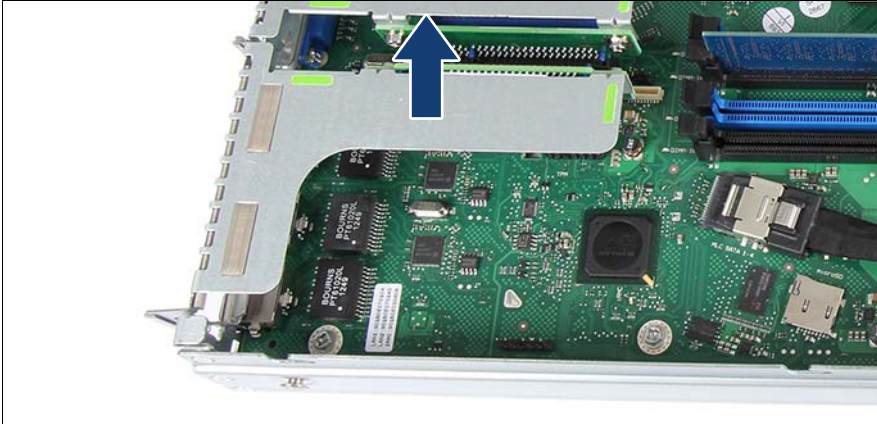


Figure 12: Removing the riser module 1

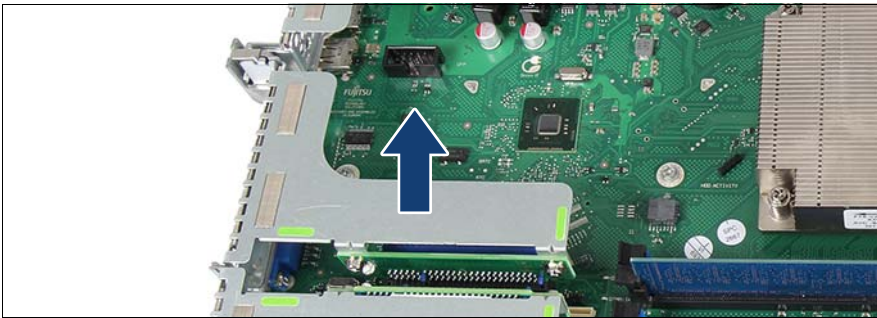


Figure 13: Removing the riser module 2

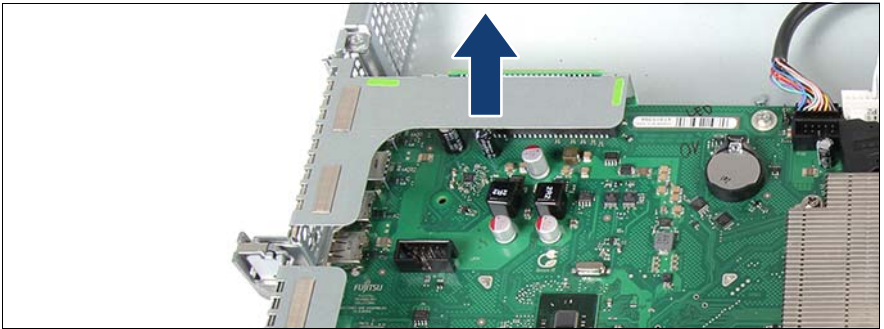


Figure 14: Removing the riser module 3

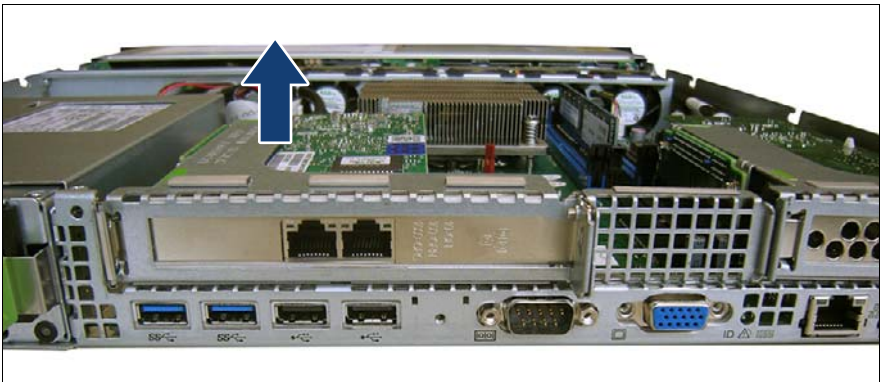


Figure 15: Removing the full height riser module

- ▶ If necessary, disconnect cables from the other components.
- ▶ Carefully pull out the riser module upward.

4.8.2 Installing a riser module

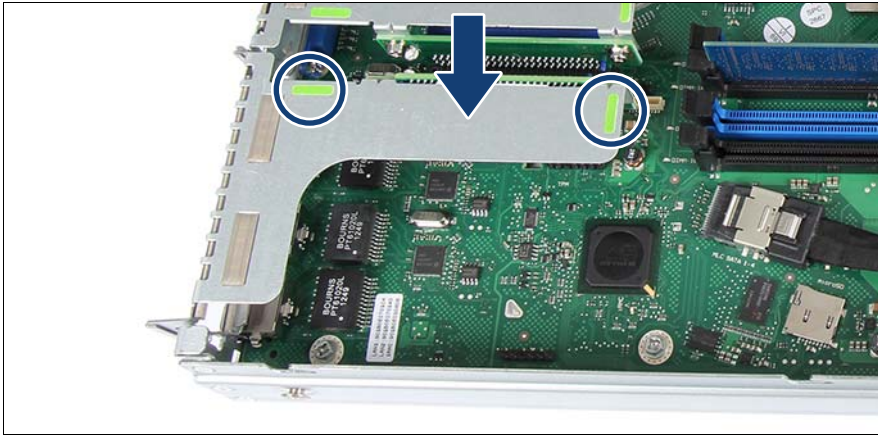


Figure 16: Installing the riser module 1

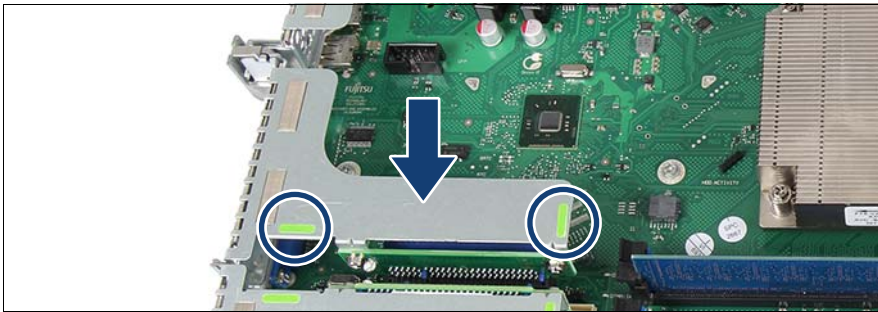


Figure 17: Installing the riser module 2

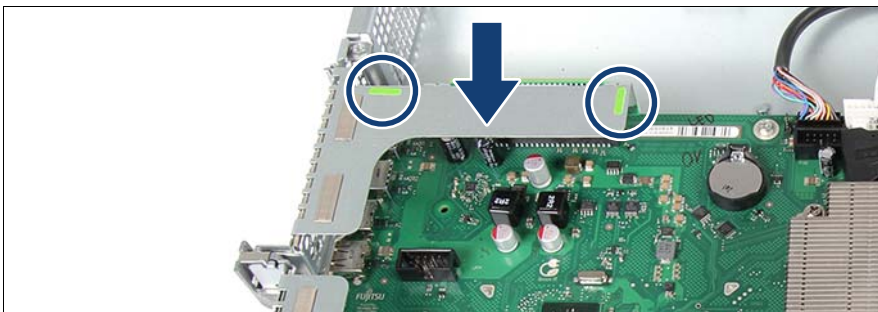


Figure 18: Installing the riser module 3

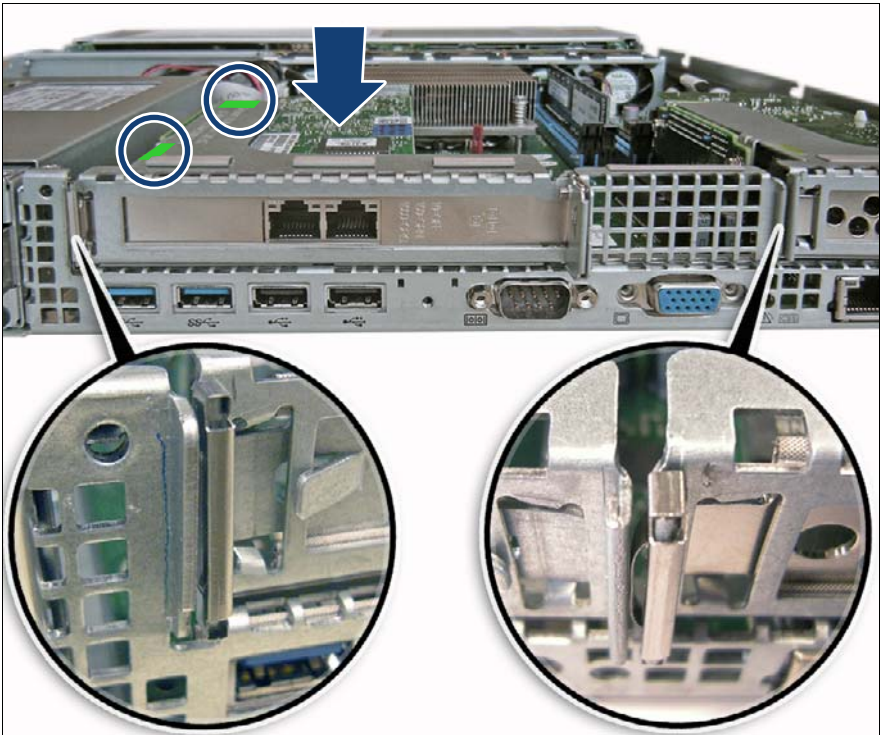


Figure 19: Installing the full height riser module

- ▶ Insert the riser card into the system board slot and press down the green touch points (see circles).



CAUTION!

Valid for the full height riser module:
Make sure that the EMC springs make contact correctly (see close-ups).


- ▶ If necessary, connect the cables to the other components.

5 Basic software procedures

5.1 Starting the maintenance task

5.1.1 Suspending BitLocker functionality

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

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

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



CAUTION!

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

Ensure to suspend BitLocker drive encryption before maintaining the server.

- When suspended, BitLocker uses a plain text key instead of the Trusted Platform Module (TPM) to read encrypted files. Keep in mind that information on this drive is not secure until BitLocker has been re-enabled.
- Ask the system administrator to suspend BitLocker-protection on the system volume, using the *BitLocker Drive Encryption* control panel item.



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

For Windows Server 2008:

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

For Windows Server 2008 R2 and above:

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



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

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

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

5.1.2 Disabling SVOM boot watchdog functionality

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

5.1.2.1 Viewing boot watchdog settings

Viewing boot watchdog settings in the BIOS

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

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



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

Viewing boot watchdog settings in the iRMC web frontend

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



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

Viewing boot watchdog settings in ServerView Operations Manager

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



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

5.1.2.2 Configuring boot watchdog settings

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



CAUTION!

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

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

Configuring boot watchdog settings in the BIOS

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



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

Configuring boot watchdog settings using the iRMC web frontend

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



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

5.1.3 Removing backup and optical disk media

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


<https://partners.ts.fujitsu.com/com/service/ps/Servers/PRIMERGY/Pages/TapeFacts.aspx>

For the Japanese market, please contact Fujitsu support, if "forcible" tape ejection is necessary.



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


5.1.4 Verifying and configuring the backup software solution

 This task only applies to 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.

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

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

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

Using Update Manager Express

- ▶ If performing an offline BIOS / firmware update, first of all prepare the ServerView Update DVD or USB stick:
 - ▶ Download the latest ServerView Update DVD image from Fujitsu:
 - for the EMEA market
<ftp://ftp.ts.fujitsu.com/images/serverview>
 - for the Japanese market:
<http://jp.fujitsu.com/platform/server/primergy/products/note/svsdvd/dvd/>

Basic software procedures

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



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

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

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

DVD: ▶ Switch on the server.

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

USB: ▶ Connect the USB stick to the server.

- ▶ Switch on the server.

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

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

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

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

The Update Manager Express main window will be displayed.

- ▶ Finish the intended maintenance task.



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

Using PrimeCollect

To start PrimeCollect, proceed as follows:

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



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

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

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

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

The server will now boot from the ServerView Suite DVD.

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



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

Concluding the procedure

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

5.1.6 Switching on the ID indicator

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



For further information, refer to section "[Locating the defective server](#)" on [page 43](#) or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

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



For further information, refer to section "[Indicators on the front panel](#)" on [page 306](#).

Using the iRMC web frontend

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

Using ServerView Operations Manager

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

5.2 Completing the maintenance task

5.2.1 Updating or recovering the system board BIOS and iRMC



For the Japanese market, follow the instructions provided separately.

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

<http://ts.fujitsu.com/support/> (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

BIOS flash procedure

- ▶ Perform the BIOS flash procedure as described in your server's "BIOS Setup Utility" reference manual.

BIOS recovery procedure

- ▶ Perform the BIOS recovery procedure as described in your server's "BIOS Setup Utility" reference manual.

5.2.1.2 Updating or recovering the iRMC


iRMC flash procedure

- ▶ Prepare a USB stick including the bootable iRMC firmware update image.
- ▶ Connect the USB stick to the USB port.



Ensure that only the USB device with the iRMC firmware is connected to the USB port. Remove all other USB devices temporarily.

- ▶ Restart the server.
- ▶ The system will detect the USB stick.

 If the BIOS cannot identify the USB stick, the pop-up message Failed to boot for Emergency flash. Please Reset now. will show up in the center of the screen.

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

Normal


Choose this option to update an existing system board.

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



CAUTION!


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

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


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

iRMC recovery procedure

- ▶ Prepare a USB stick including the bootable iRMC firmware update image.
- ▶ Ensure that the server has been shut down and disconnected from the mains as described in section ["Disconnecting the server from the mains" on page 46](#).
- ▶ Connect the USB stick to the USB port.

 Ensure that only the USB device with the iRMC firmware is connected to the USB port. Remove all other USB devices temporarily.

- ▶ Connect the server to the mains while pushing the ID button on the front panel. Ask a second person to help you if necessary.
- ▶ Ensure that the Global Error indicator and the ID indicator are flashing to indicate that the server is entering the iRMC recovery state.
- ▶ Press the Power On / Off button. The system starts the POST process.

 In iRMC recovery mode, the "FUJITSU" logo does not show up.

- ▶ The system will detect the USB stick.



If the BIOS cannot identify the USB stick, the pop-up message Failed to boot for Emergency flash. Please Reset now. will show up in the center of the screen.

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



CAUTION!

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



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

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

5.2.2 Verifying system information backup / restore

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

In order to verify whether the backup or restore process has been successful, check the System Event Log (SEL) using the ServerView Operations Manager (see also section ["Viewing and clearing the System Event Log \(SEL\)" on page 81](#)).

After replacing the system board

- ▶ Check the SEL log files as described in section ["Viewing and clearing the System Event Log \(SEL\)" on page 81](#) to verify whether the backup data on the Chassis ID EPROM has been restored to the system board:

```
Chassis IDPROM: BMC FW Restore successful
```



CAUTION!

There might be a case that the BIOS settings cannot be restored even if above message was logged after replacing the system board. For details please refer to section ["Replacing the system board" on page 276](#).

After replacing the Chassis ID EPROM



In case of the PRIMERGY RX1330 M1 server, the Chassis ID EPROM is integrated on the front panel board.

- ▶ Check the SEL log files as described in section "[Viewing and clearing the System Event Log \(SEL\)](#)" on page 81 to verify whether a backup copy of the system board settings has been transferred to the Chassis ID EPROM:
Chassis ID PROM: BMC FW Backup successful

5.2.3 Updating RAID controller firmware

After replacing the RAID controller, it is essential to upgrade the firmware to the latest version. The latest RAID controller 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:

- 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/> (EMEA market)

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

- ▶ Select *Drivers & Downloads*.

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

5.2.4 Enabling Option ROM scan

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

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

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



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

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

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

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



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

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

5.2.5 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 [5.1.4 on page 67](#), 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

5.2.6 Resetting the boot retry counter

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

5.2.6.1 Viewing the boot retry counter

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

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

5.2.6.2 Resetting the boot retry counter

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



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

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

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

Resetting the boot retry counter in the BIOS

- ▶ Enter the BIOS.
- ▶ Select the *Server Mgmt* menu.
- ▶ Under *Boot Retry Counter* press the \oplus or \ominus keys to specify the maximum number of boot attempts (0 to 7).
- ▶ Exit the BIOS.

Resetting the boot retry counter using the ServerView Operations Manager

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

Resetting the boot retry counter using iRMC web frontend

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



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

5.2.7 Enabling SVOM boot watchdog functionality


If ServerView Operations Manager boot watchdog functionality has been disabled for firmware upgrade purposes (see section [5.1.2 on page 64](#)), it has to be re-enabled to complete the maintenance task.

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

Configuring boot watchdog settings in the BIOS

- ▶ Enter the BIOS.

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

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

Configuring boot watchdog settings using the iRMC web frontend

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


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

5.2.8 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 will then reboot with only the intact hardware components remaining in the system configuration. After replacing the defective component, it needs to be re-enabled in the system board BIOS.

- ▶ Enter the BIOS.
- ▶ Select the *Advanced* menu.
- ▶ Select the status menu of the desired component:

- 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 corresponding BIOS Setup Utility reference manual.

5.2.9 Verifying the memory mode

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



For detailed information on memory operation modes available for your server, refer to section ["Modes of operation" on page 208](#).

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

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



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

5.2.10 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.

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



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

- ▶ Save your changes and exit the BIOS.



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

5.2.11 Viewing and clearing the System Event Log (SEL)

5.2.11.1 Viewing the SEL

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

Viewing the SEL in ServerView Operations Manager

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



Note on the SVOM Driver Monitor

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

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



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

Viewing the SEL using the iRMC web frontend

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



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

5.2.11.2 Clearing the SEL

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

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



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


5.2.12 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 LAN controllers in a server running Linux OS, the MAC address will change but not automatically be updated in the definition file.


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

To update the MAC address, proceed as follows:


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

- ▶ After replacing a network controller or the system board, switch on and boot the server as described in section ["Switching on the server" on page 57](#).

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.

5.2.13 Resuming BitLocker functionality

If BitLocker Drive Encryption has been suspended for maintenance purposes (see section "[Suspending BitLocker functionality](#)" on page 63), it has to be re-enabled to complete the service task.



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

- ▶ In this case, ask the system administrator to enter the recovery key in order to boot the operating system.
- ▶ Ask the system administrator to enable the previously suspended BitLocker-protection on the system volume, using the *BitLocker Drive Encryption* control panel item:

For Windows Server 2008:

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

For Windows Server 2008 R2 and above:

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



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

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

5.2.14 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 20: 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.

5.2.15 Looking up changed MAC / WWN addresses

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



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

5.2.15.1 Looking up MAC addresses

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



This information is only available with the iRMC S4 or above. Only network controllers supporting the Command Line Protocol (CLP) will be displayed.

- ▶ Inform the customer about the changed MAC address.

5.2.15.2 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 75](#).
- ▶ Restart the server.
- ▶ During boot, as soon as the Emulex BIOS utility option appears, press **[ALT]+[E]** or **[CTRL]+[E]**.
- ▶ Under *Emulex Adapters in the System* you will find all available Emulex adapters and their WWN addresses.
- ▶ Note down the new 16-digit WWN address.
- ▶ Press **[Esc]** to exit the Emulex BIOS utility.
- ▶ Inform the customer about the changed WWN address.

QLogic FC adapters

- ▶ Enable the network controller's Option ROM in the system board BIOS as described in section ["Enabling Option ROM scan" on page 75](#).
- ▶ Restart the server.
- ▶ During boot, as soon as the QLogic BIOS utility option appears, press **[ALT]+[Q]** or **[CTRL]+[Q]**.
- ▶ Under *Select Host Adapter* use the arrow keys **[↑]/[↓]** to select the desired FC / FCoE adapter and press **[Enter]**.

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

5.2.16 Using the Chassis ID Prom Tool

The Chassis ID EPROM located on a dedicated Chassis ID board or on your server's front panel board contains system information like server name and model, housing type, serial number and manufacturing data.

In order to integrate your system into the ServerView management environment and to enable server installation using the ServerView Installation Manager, system data needs to be complete and correct.

After replacing the Chassis ID EPROM, system information has to be entered using the Chassis ID Prom tool. The tool and further instructions are available to maintenance personnel from the Fujitsu Technology Solutions Extranet:

<https://partners.ts.fujitsu.com/com/service/ps/Servers/PRIMERGY/>

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



For the Japanese market, follow the instructions provided separately.

Note on Cool-safe® Advanced Thermal Design (ATD)



If the Cool-safe® Advanced Thermal Design (ATD) option is available and has been enabled for your server, please set information within the Chassis ID Prom Tool accordingly.



The ATD option can only be ordered from the manufacturer as a factory preset. To find out if your server is ATD-enabled, check for the ATD logo on the identification rating plate.

For further information on Cool-safe® Advanced Thermal Design (ATD), please refer to your server's operating manual.



CAUTION!

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

5.2.17 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.

5.2.17.1 After replacing / upgrading LAN controllers

Please note when re-using a replaced LAN controller:

- ▶ Confirm with the customer whether the LAN controller you have replaced has been used as part of a LAN teaming configuration.
- ▶ If LAN teaming has been active, you will need to restore the configuration using the LAN driver utility after replacing the LAN controller. Ensure that the controllers have been assigned as primary or secondary according to your requirements.



For details, refer to the relevant LAN driver manual.

5.2.17.2 After replacing the system board

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



For details, refer to the relevant LAN driver manual.

5.2.18 Switching off the ID indicator

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



For further information, refer to section "[Locating the defective server](#)" on [page 43](#) or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

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

Using the iRMC web frontend

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

Using ServerView Operations Manager

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

5.2.19 Performing a fan test after replacing a defective fan

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

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

Executing the fan test via the iRMC Web interface

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



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

Executing the fan test via ServerView Operations Manager

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

In the left-hand section of the window, the *Configuration* tab is being activated.

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



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

For the Japanese market: Executing the fan test via Chassis ID Prom Tool



Please follow the instructions provided separately.

6 Power supply

Safety notes



CAUTION!

- Do not disassemble the power supply unit. Doing so may cause electric shock.
- Areas around the power supply unit may remain extremely hot after shutdown. After shutting down the server, wait for hot components to cool down before removing the power supply unit.
- When installing the power supply unit, be sure to confirm that the connector of the power supply unit is not damaged or bent.
- Do not insert your hands in the power supply unit slot when removing the power supply unit. Doing so may cause electric shock.
- If the power supply unit is hard to remove, do not pull out it by force.
- The power supply unit is heavy, so handle it carefully. If you drop it by mistake, injuries may result.
- For further safety information, please refer to chapter ["Important information"](#) on page 31.

6.1 Basic information

The server can be equipped:

- with a standard power supply unit (permanently built-in)

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

- or up to two hot-plug power supply units (slide-in units)

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



CAUTION!

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

6.2 Standard power supply

6.2.1 Replacing the standard power supply unit



Field Replaceable Unit (FRU)



Hardware: 10 minutes

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

6.2.1.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

6.2.1.2 Removing the defective standard power supply unit

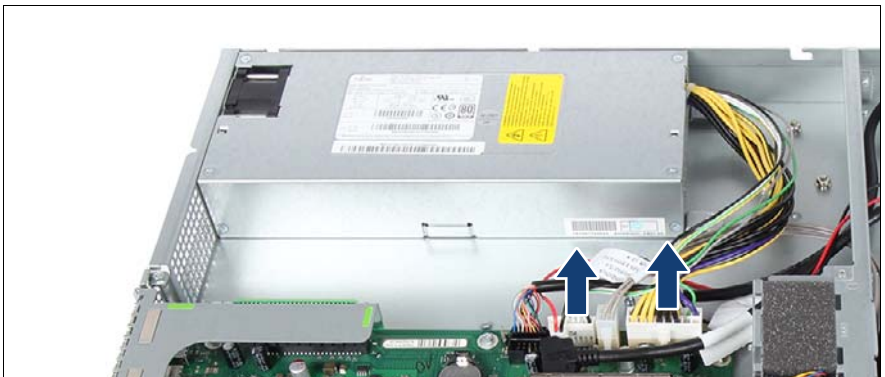


Figure 21: Disconnecting the power cables

- ▶ Disconnect the two power cables from the system board connectors "PC98" and "PWR1".

Power supply



Figure 22: Removing the screws

- ▶ Remove the two screws (see circles).

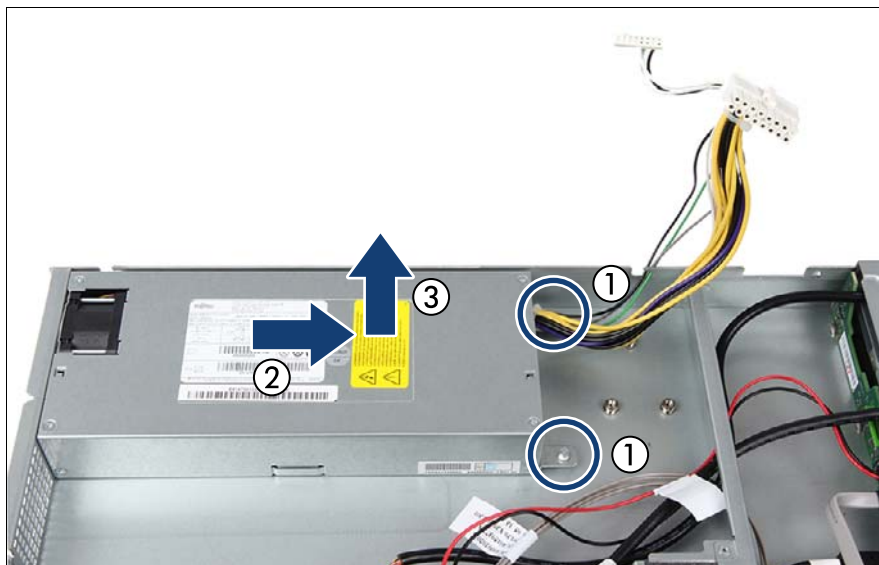


Figure 23: Taking out the standard power supply unit

- ▶ Remove the two screws (1).
- ▶ Pull the power supply unit a few centimeters toward the inside (2).
- ▶ Take the power supply unit out upward (3).

6.2.1.3 Installing the new standard power supply unit

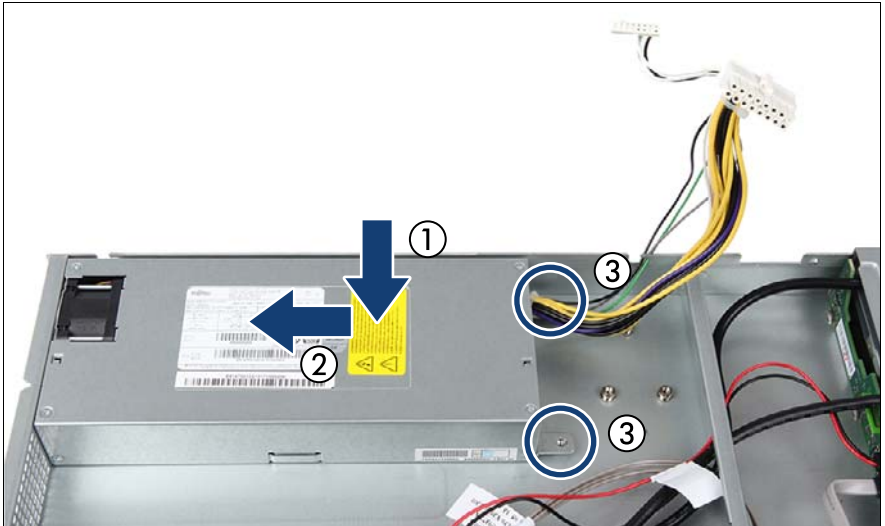


Figure 24: Inserting the standard power supply unit

- ▶ Insert the power supply unit into the bay (1).
- ▶ Push the power supply unit toward the adapter plate (2).
- ▶ Fasten the power supply unit with two screws in the chassis (3).
- ▶ Attach the power supply unit with two screws to the adapter plate (see figure [22](#)).



Figure 25: Connecting the power cables

- ▶ Connect the two power cables to the system board connectors "PC98" and "PWR1".

6.2.1.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)
- ▶ ["Performing a fan test after replacing a defective fan" on page 89](#)



CAUTION!

(Except for Japanese market) After replacing the power supply unit a fan calibration must be started for the PSU fan. You will find the description for this procedure in the manual "ServerStart".

6.3 Redundant power supply



Figure 26: PSU bays

6.3.1 Installing a hot-plug power supply unit



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less

6.3.1.1 Preliminary steps

No steps needed.

6.3.1.2 Removing the dummy cover

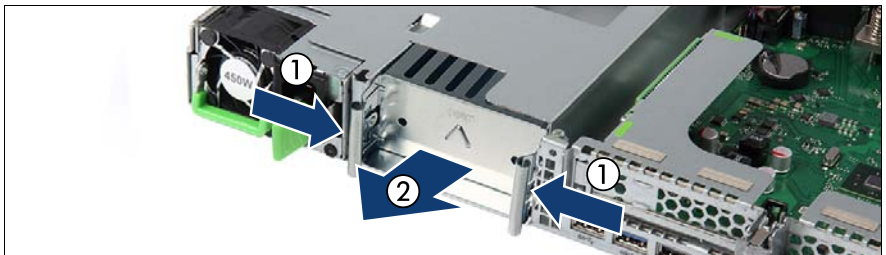


Figure 27: Removing a dummy cover

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



CAUTION!

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

6.3.1.3 Installing a hot-plug power supply unit



Figure 28: Folding up the handle

- ▶ Push the handle of the power supply unit halfway upward in the direction of the arrow.

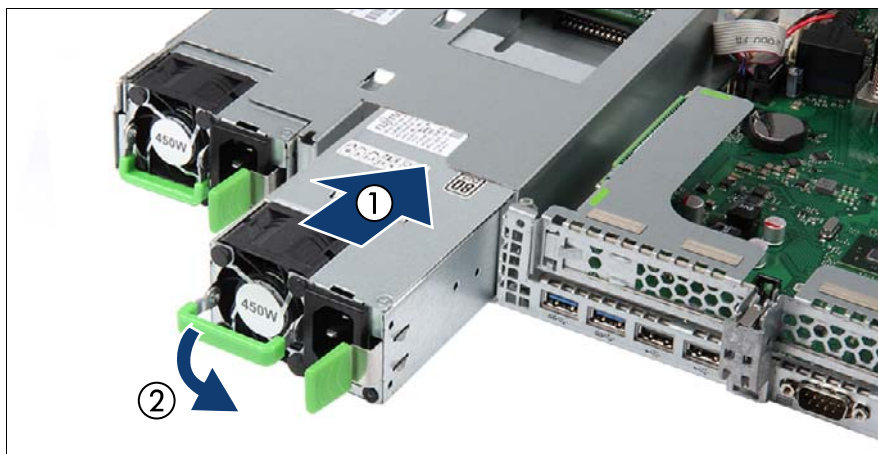


Figure 29: Installing the hot-plug power supply unit

- ▶ Push the power supply unit into its bay (1) as far as it will go until the locking latch snaps in place.
- ▶ If applicable, fold down the handle on the power supply unit (2).



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

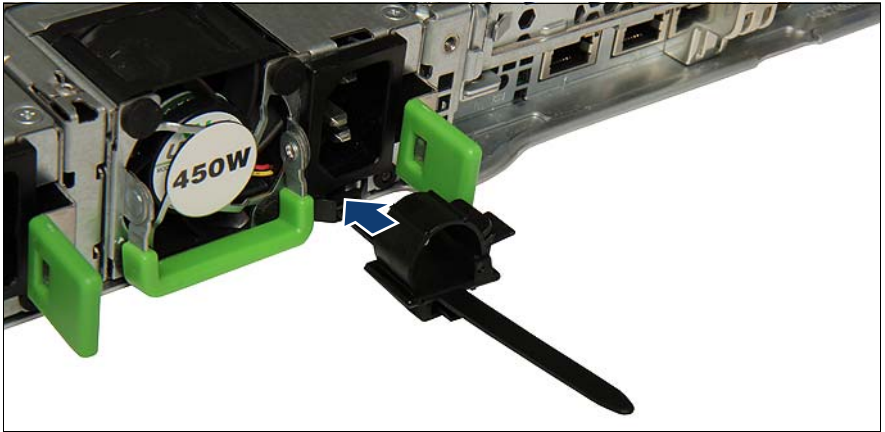


Figure 30: Installing the cable tie

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

6.3.1.4 Concluding steps

- ▶ ["Connecting the server to the mains" on page 55](#)

6.3.2 Removing a hot-plug power supply unit



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less

Note for servers using CMA (Cable Management Arm)

Regarding of removing power supply units, additional tasks are needed, due to an interference between CMA stopper and the power supply units.

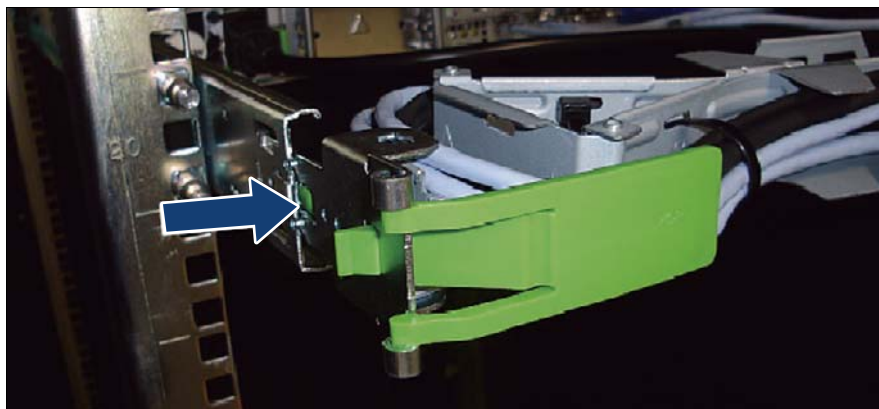


Figure 31: Unlocking the CMA stopper

- ▶ Push the lock spring inward to unlock the CMA stopper.



CAUTION!

In case of not enough space at the under side, unlock the CMA stopper of the server below and pull out the CMA to the rear side.



Figure 32: Removing the CMA stopper

- ▶ Remove the CMA stopper with the mounted crossbar.
- ▶ Hold the CMA stopper, the crossbar and the CMA including cables in the one hand.

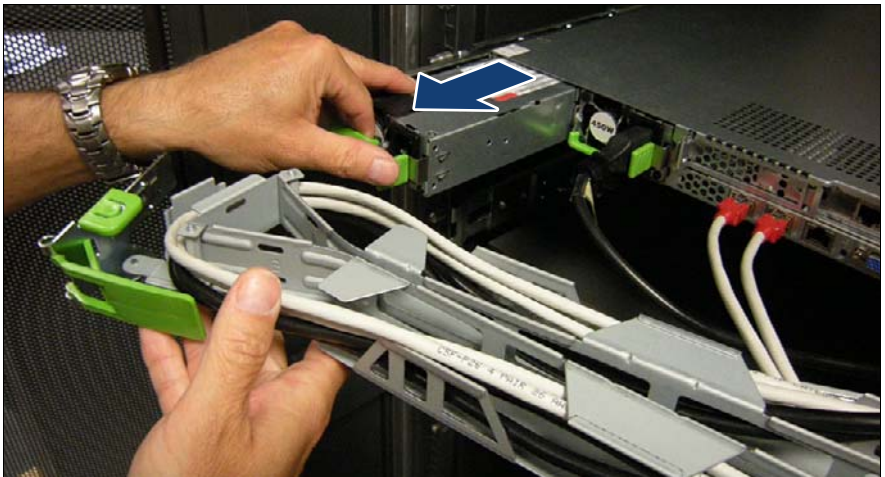


Figure 33: Removing the power supply unit

- ▶ Remove the power supply unit and install the dummy cover carefully.
- ▶ Mount the complete assembly (CMA stopper, the crossbar and the CMA) again into the rail.

Power supply

6.3.2.1 Preliminary steps

No steps needed.

6.3.2.2 Removing a hot-plug power supply unit

- ▶ Remove the power cord from the dedicated power supply unit as described in section ["Disconnecting the server from the mains"](#) on page 46.

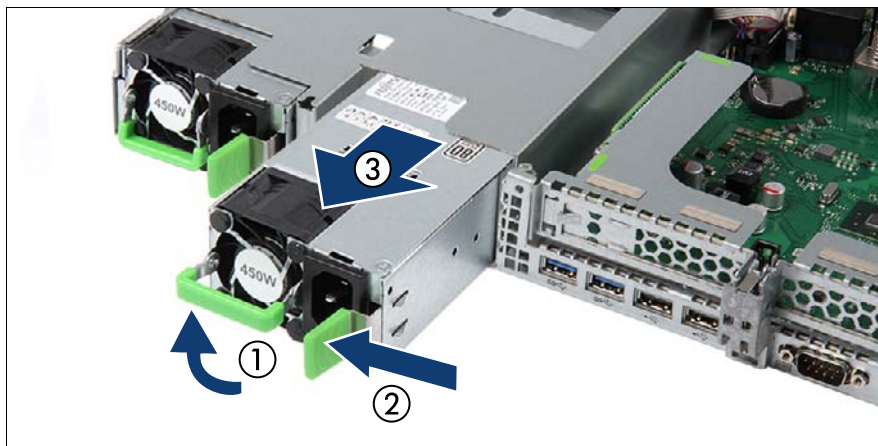


Figure 34: Unlocking and removing the hot-plug power supply unit

- ▶ Push the handle of the power supply unit halfway upward in the direction of the arrow (1).
- ▶ Push the lock in direction of the arrow (2).
- ▶ Grip the handle and pull out the power supply unit in the direction of the arrow (3).



CAUTION!

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

6.3.2.3 Installing the dummy cover

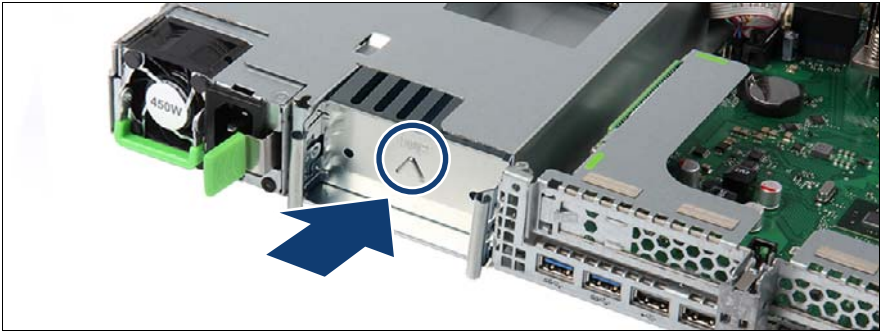


Figure 35: Installing the dummy cover

- ▶ Insert the dummy cover into the empty bay with the impressed arrow symbol facing to the top (see circle).
Ensure that the upper rear cant of the dummy cover fits under the PSU cage.
- ▶ Push the dummy cover into its bay until it locks in place.



CAUTION!

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

6.3.3 Replacing a hot-plug power supply unit



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less



CAUTION!

- When replacing a power supply unit in a non-redundant PSU configuration, the server must be switched off first.
- Replace the power supply unit after specifying the one that breaks down at work by revitalization.

Note for servers using CMA (Cable Management Arm)

Regarding of replacing power supply units, additional tasks are needed, due to an interference between CMA stopper and the power supply units.

- ▶ Push the lock spring inward to unlock the CMA stopper (see figure 31).



CAUTION!

In case of not enough space at the under side, unlock the CMA stopper of the server below and pull out the CMA to the rear side

- ▶ Remove the CMA stopper with the mounted crossbar (see figure 32).
- ▶ Hold the CMA stopper, the crossbar and the CMA including cables in the one hand.
- ▶ Remove the power supply unit (see figure 33) and install the new power supply unit carefully.
- ▶ Mount the complete assembly (CMA stopper, the crossbar and the CMA) again into the rail.

6.3.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Locating the defective component" on page 45](#)
- ▶ Check which power supply unit is defective.

A power supply unit is defective when the indicator (1) in [figure 228](#) lights orange. For more information see section ["Connectors and indicators" on page 300](#).

- ▶ Only when replacing a power supply unit in a non-redundant configuration: ["Shutting down the server" on page 45](#)
- ▶ Remove the power cord from the defective power supply unit as described in section ["Disconnecting the server from the mains" on page 46](#)

6.3.3.2 Removing the defective hot-plug power supply unit

- ▶ Remove the power supply unit as described in section ["Removing a hot-plug power supply unit" on page 102](#).

6.3.3.3 Installing the new hot-plug power supply unit

- ▶ Install the power supply unit as described in section "[Installing a hot-plug power supply unit](#)" on page 98.

6.3.3.4 Concluding steps

- ▶ Connect the power cord to the new power supply unit and secure it with a cable tie as described in section "[Connecting the server to the mains](#)" on page 55.
- ▶ Only when replacing a power supply unit in a non-redundant configuration: "[Switching on the server](#)" on page 57
- ▶ "[Performing a fan test after replacing a defective fan](#)" on page 89

6.3.4 Replacing the power distribution board



Field Replaceable Unit (FRU)



Hardware: 15 minutes

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

6.3.4.1 Preliminary steps

- ▶ "[Locating the defective server](#)" on page 43
- ▶ "[Suspending BitLocker functionality](#)" on page 63
- ▶ "[Shutting down the server](#)" on page 45
- ▶ "[Disconnecting the server from the mains](#)" on page 46
- ▶ "[Getting access to the component](#)" on page 47

6.3.4.2 Removing the defective power distribution board

- ▶ Remove all power supply units as described in section ["Removing a hot-plug power supply unit"](#) on page 102.

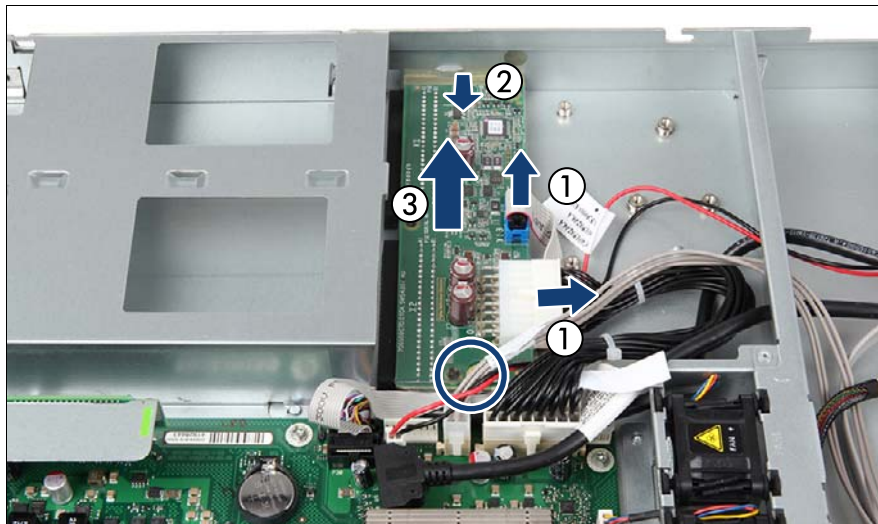


Figure 36: Removing the power distribution board

- ▶ Disconnect the two power cables from the power distribution board (1).
- ▶ Remove the screw (see circle).
- ▶ Slide the power distribution board out of the guidings of the chassis (2) and take it out upward (3).

6.3.4.3 Installing the new power distribution board

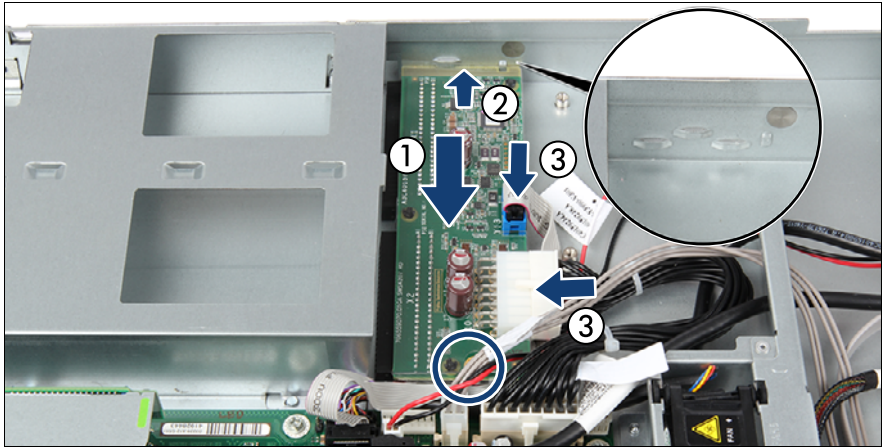


Figure 37: Installing the power distribution board

- ▶ Insert the power distribution board (1) and slide it in the guidings of the chassis (2).
- ▶ Fasten the power distribution board with one screw (see circle).
- ▶ Connect the two power cables to the power distribution board (3).
Check if the flat cable is correctly seated under the edge of the power distribution board:

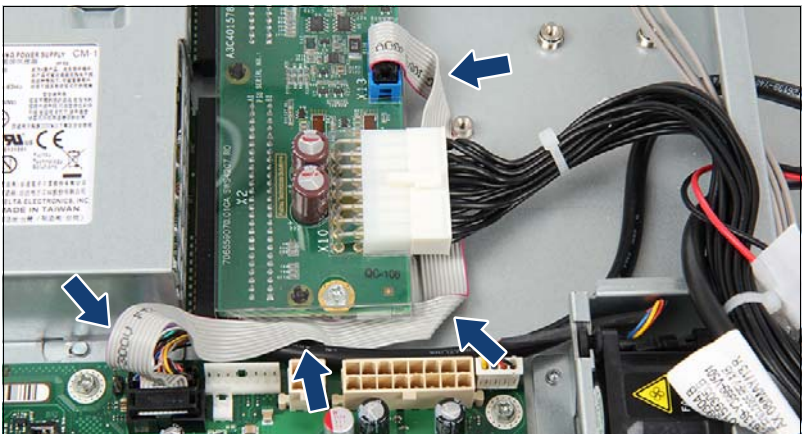


Figure 38: Routing the flat cable

- ▶ Install the power supply units as described in section ["Installing a hot-plug power supply unit"](#) on page 98.

6.3.4.4 Concluding steps

- ▶ ["Reassembling"](#) on page 52
- ▶ ["Connecting the server to the mains"](#) on page 55
- ▶ ["Switching on the server"](#) on page 57
- ▶ ["Resuming BitLocker functionality"](#) on page 84

6.4 Converting a standard power supply to a redundant power supply

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

The upgrade kit for the redundant power supply consists of the following parts:

- PSU cage with power distribution board
- two power cables
- one hot-plug power supply unit
- dummy cover (if only one power supply unit is installed, you have to install the dummy cover in the second bay)
- several screws
- one fan module



Field Replaceable Unit (FRU)



Hardware: 20 minutes

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

6.4.1 Preliminary steps

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

6.4.2 Removing the standard power supply unit

- ▶ Remove the power supply unit as described in section ["Removing the defective standard power supply unit" on page 93](#).

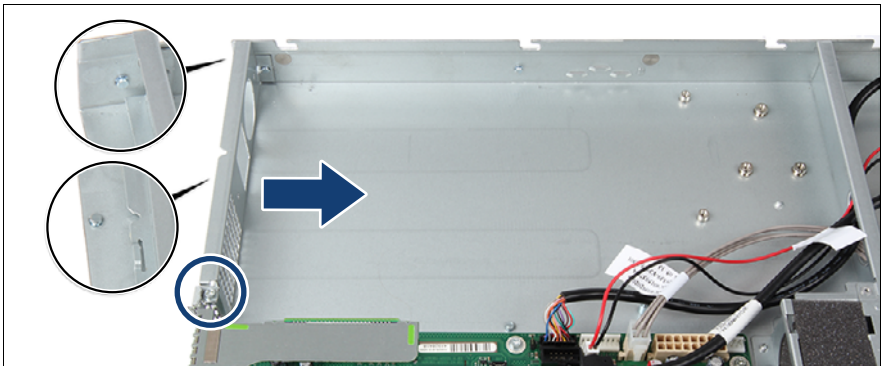


Figure 39: Removing the adapter plate

- ▶ Remove the screw (see circle) which attach the adapter plate of the power supply unit to the housing.
- ▶ Push the adapter plate a few centimeters inward to detach it from the two bolts (see close-ups).
- ▶ Remove the adapter plate.

6.4.3 Installing the upgrade kit

Installing the PSU cage

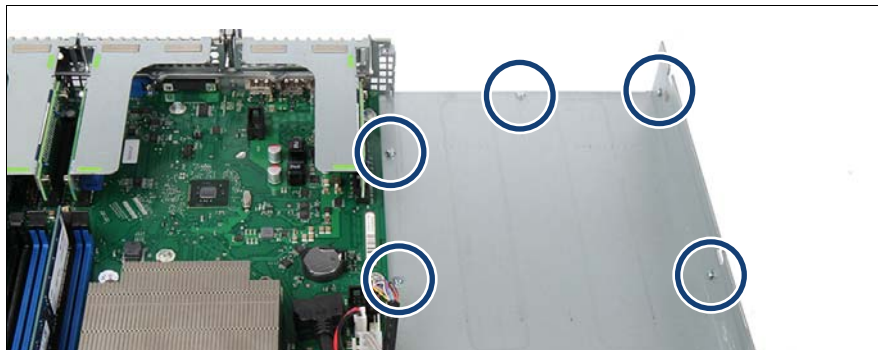


Figure 40: Positions of the bolts

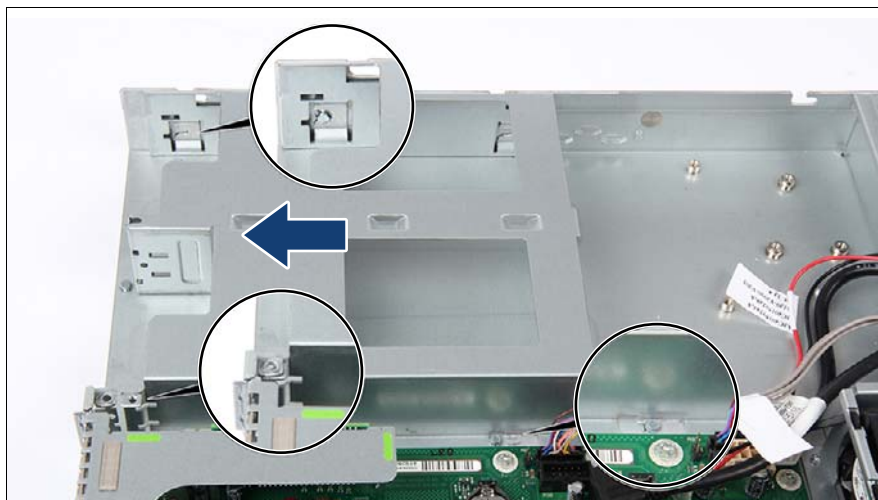


Figure 41: Inserting the PSU cage

- ▶ Insert the PSU cage in the housing and push it to the rear side.



CAUTION!

The PSU cage must engage in the five bolts (positions see [figure 40](#)).



Figure 42: Fastening the PSU cage

- ▶ Fasten the PSU cage with one screw.

Installing the power distribution board



Figure 43: Folding the flat cable

- ▶ Fold the flat cable as shown.
- ▶ Install the power distribution board as described in section ["Installing the new power distribution board"](#) on page 107.

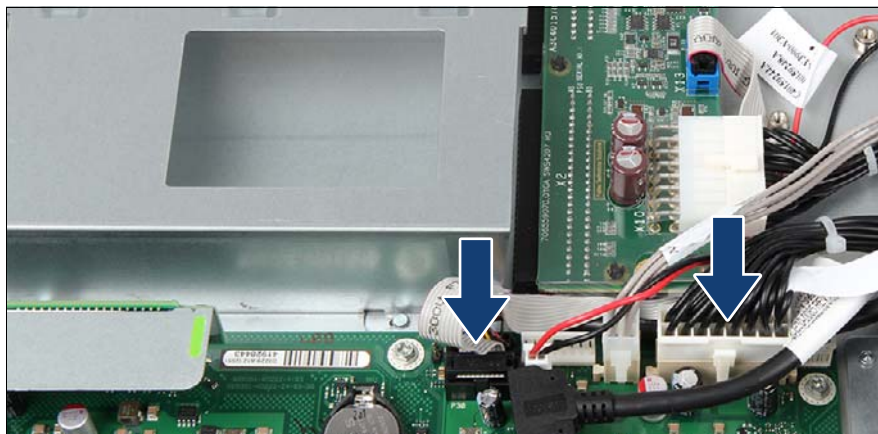


Figure 44: Connecting the power cables to the system board

- ▶ Connect the two power cables to the system board connectors "P30" and "PWR1".

Installing hot-plug power supply unit and dummy cover

- ▶ Install the power supply unit as described in section "[Installing a hot-plug power supply unit](#)" on page 98.



The power supply unit must be installed in the first bay (left bay seen from rear side). The dummy cover must be installed in the second bay.

- ▶ Install the dummy cover as described in section "[Installing the dummy cover](#)" on page 103.

Installing the additional fan module

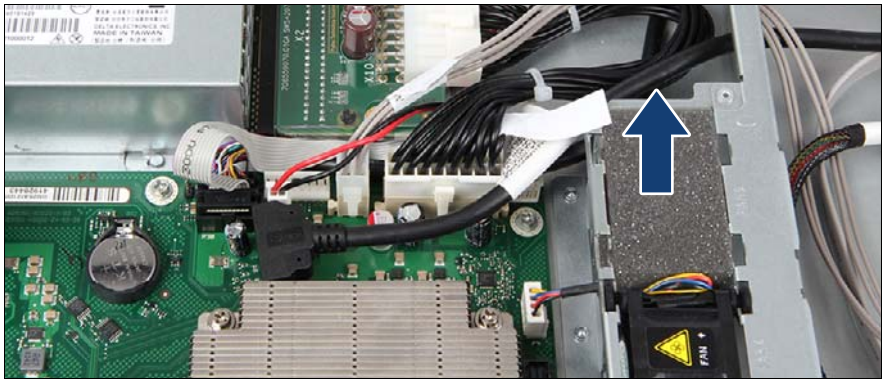


Figure 45: Removing the sponge

- ▶ Remove the sponge.

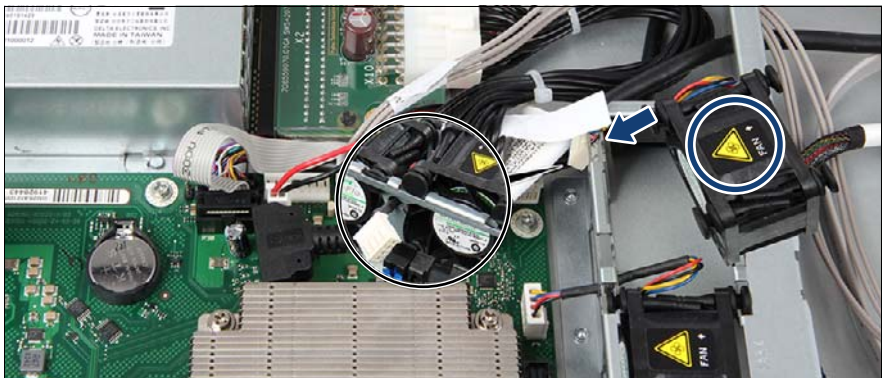


Figure 46: Routing fan cable

- ▶ Thread the fan cable through the opening of the fan cage and insert the fan module. Notice the direction of the fan label (see circle).

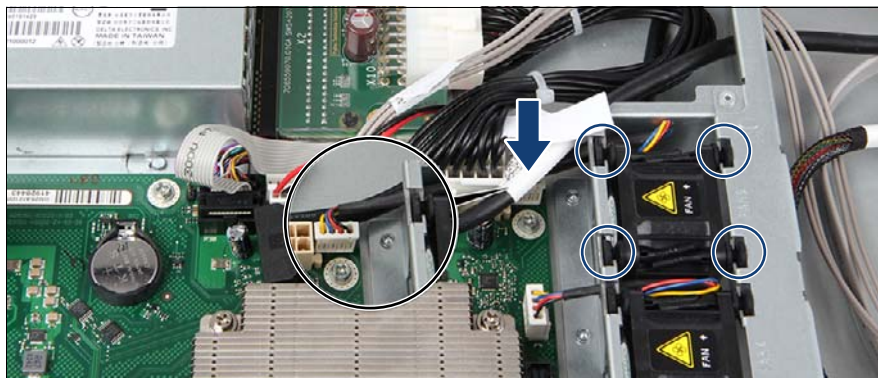


Figure 47: Installing fan module 5

- ▶ Press down the four rubber pins until they engage (see circles).
- ▶ Connect the fan cable to connector "FAN5" on the system board.

6.4.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

7 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 reinstalled into their original mounting locations after replacement. Otherwise, data may be lost.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Before removing a hard disk drive, wait for about 30 seconds until the disk has stopped 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.
- 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.
- For further safety information, please refer to chapter ["Important information" on page 31](#).

7.1 Basic information

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

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

– 3.5-inch HDD subsystem:

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

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

– 2.5-inch HDD/SSD subsystem:

Up to four (one HDD backplane), eight (two HDD backplanes) or ten (one HDD backplane) 2.5-inch SAS/SATA HDD/SSD modules can be installed. Each HDD/SSD module can accommodate a SAS/SATA hard disk drive or 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 RAID controllers controlling the HDD/SSD modules see chapter ["Expansion cards and backup units" on page 157](#).

7.2 2.5-inch HDD/SSD configurations

7.2.1 Equipping the 2.5-inch 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 1. Free bays must be equipped with a dummy module.

7.2.2 Configuration with up to four HDD/SSD modules

Mounting order



Figure 48: Mounting order with up to four 2.5-inch HDDs/SSDs

HDD/SSD naming scheme

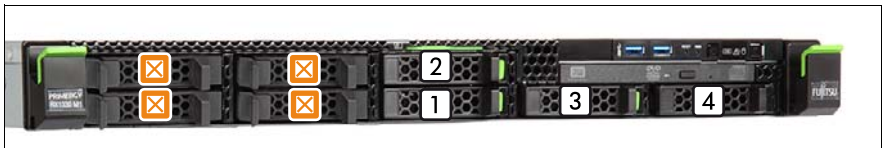


Figure 49: Naming scheme with up to four 2.5-inch HDDs/SSDs

i The HDD/SSD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

Position	Logical drive number	ServerView RAID Manager display name
①	0	HDD vendor name (0)
②	1	HDD vendor name (1)
③	2	HDD vendor name (2)
④	3	HDD vendor name (3)

7.2.3 Configuration with up to eight HDD/SSD modules

Mounting order



Figure 50: Mounting order with up to eight HDD/SSD bays

HDD/SSD naming scheme

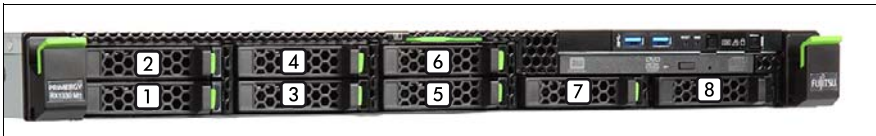


Figure 51: Naming scheme with up to eight 2.5-inch HDDs/SSDs

i The HDD/SSD numbering as listed in the ServerView RAID Manager differs from the HDD/SSD mounting order:

Position	Logical drive number	ServerView RAID Manager display name
1	0	HDD vendor name (0)
2	1	HDD vendor name (1)
3	2	HDD vendor name (2)
4	3	HDD vendor name (3)
5	4	HDD vendor name (4)
6	5	HDD vendor name (5)
7	6	HDD vendor name (6)
8	7	HDD vendor name (7)

7.2.4 Configuration with up to 10 HDD/SSD modules

Mounting order



Figure 52: Mounting order with up to ten HDD/SSD bays

HDD/SSD naming scheme

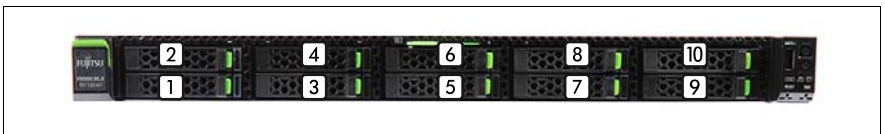


Figure 53: Naming scheme with up to ten 2.5-inch HDDs/SSDs

i The HDD/SSD numbering as listed in the ServerView RAID Manager differs from the HDD/SSD mounting order:

Position	Logical drive number	ServerView RAID Manager display name
1	0	HDD vendor name (0)
2	1	HDD vendor name (1)
3	2	HDD vendor name (2)
4	3	HDD vendor name (3)
5	4	HDD vendor name (4)
6	5	HDD vendor name (5)
7	6	HDD vendor name (6)
8	7	HDD vendor name (7)
9	8	HDD vendor name (8)
10	9	HDD vendor name (9)

7.2.5 Installing 2.5-inch HDD/SSD modules



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less

7.2.5.1 Preliminary steps

- ▶ Locate the correct drive bay as described in section ["2.5-inch HDD/SSD configurations" on page 117](#).

7.2.5.2 Removing a 2.5-inch HDD/SSD dummy module



In configuration with only one 4 x 2.5-inch HDD backplane dummy locks are installed to make it impossible to equip the bays with no HDD backplane behind.



Figure 54: Removing dummy lock

- ▶ Only valid after upgrading the server with the second HDD backplane: pull the dummy lock out of the dummy cover. Please be aware that the dummy lock can be damaged.

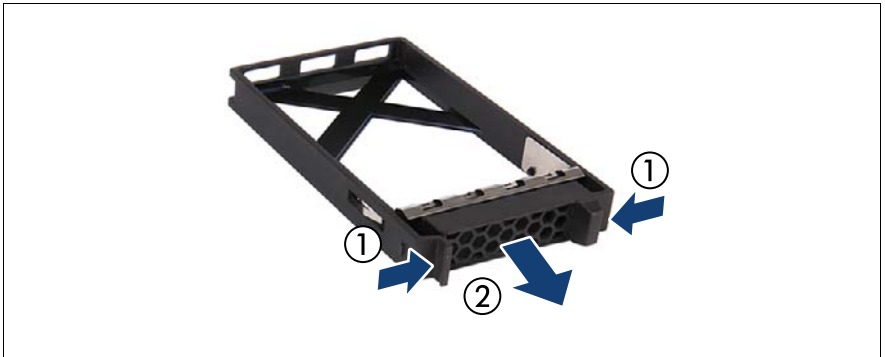


Figure 55: Removing a 2.5-inch dummy module

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



CAUTION!

Save the dummy module for future use.

Always replace dummy modules into unused HDD/SSD bays to comply with applicable EMC regulations and satisfy cooling requirements.

7.2.5.3 Installing a 2.5-inch HDD/SSD module

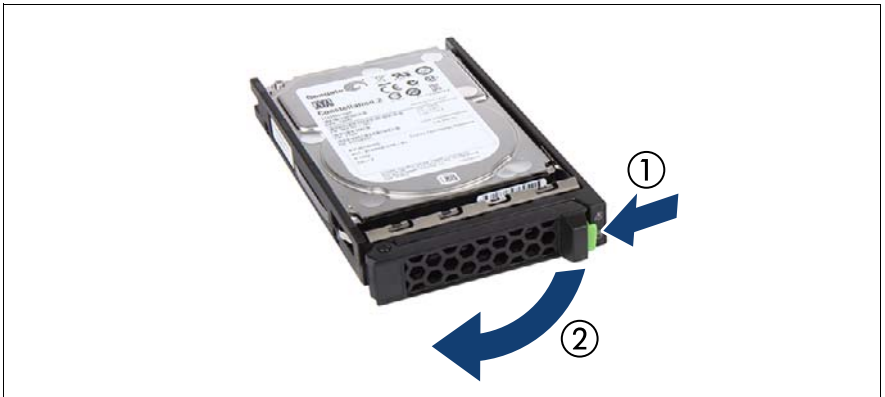


Figure 56: Opening the 2.5-inch HDD/SSD module locking lever

- ▶ Pinch the green locking clip (1) and open the locking lever (2).

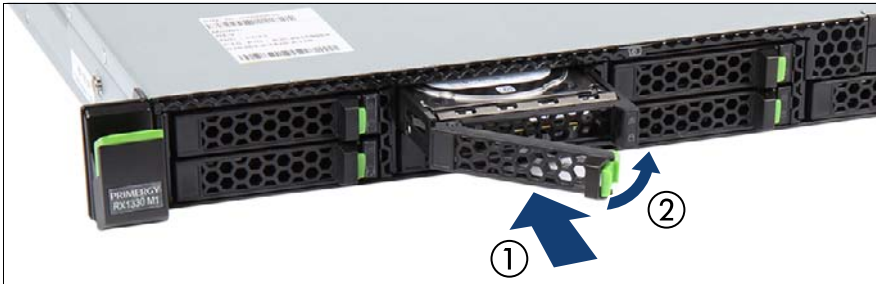


Figure 57: Installing the 2.5-inch HDD/SSD module

- ▶ Insert the HDD/SSD module into a drive bay and carefully push back as far as it will go (1).
- ▶ Close the locking lever to lock the hard disk drive in place (2).

7.2.5.4 Concluding steps

- ▶ ["Performing a RAID array rebuild" on page 85](#)

7.2.6 Removing 2.5-inch HDD/SSD modules



Customer Replaceable Unit (CRU)





Hardware: 5 minutes

Tools: tool-less

7.2.6.1 Preliminary steps

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

RAID level	Procedure
RAID 0	<p>Only remove an HDD module combined in a RAID 0 array if defective.</p> <p> CAUTION! Removing an operational HDD module will result in data loss!</p>

RAID level	Procedure
RAID 1 RAID 5	<p>Removing an HDD module from a RAID 1 or RAID 5 array will not result in data loss. However, the removed drive needs to be replaced immediately by an HDD module of the same or larger capacity.</p> <p> After replacing the HDD module, RAID rebuild will be performed as a background process as described in section "Performing a RAID array rebuild" on page 85.</p>

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



CAUTION!

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

7.2.6.2 Removing a 2.5-inch HDD/SSD module

- ▶ Pinch the green locking clips and open the locking lever (see figure 56).
- ▶ Pull the HDD/SSD module out a few centimeters.
- ▶ Wait about 30 seconds to allow the hard disk drive to spin down.



This is not necessary when removing a solid state drive.



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

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

7.2.6.3 Installing a 2.5-inch HDD/SSD dummy module



CAUTION!

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



Figure 58: Installing a 2.5-inch dummy module

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

7.2.6.4 Concluding steps

No steps needed.

7.2.7 Replacing a 2.5-inch HDD/SSD module



Customer Replaceable Unit
(CRU)



Hardware: 5 minutes

Tools: tool-less



CAUTION!

- Only remove an HDD/SSD module during operation if the drive is not currently being accessed. Observe the indicators for the corresponding HDD/SSD modules, see section ["Indicators on the hot-plug HDD module"](#) on page 309.

- 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.

7.2.7.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Locating the defective component" on page 45](#)

Only applicable for removing intact HDD/SSD modules:

- ▶ Before removing a non-defective HDD/SSD module, put the drive into "Offline" mode using your RAID configuration software.

7.2.7.2 Removing the defective 2.5-inch HDD/SSD module

- ▶ Remove the HDD/SSD module as described in section ["Removing 2.5-inch HDD/SSD modules" on page 122](#).

7.2.7.3 Installing the new 2.5-inch HDD/SSD module

- ▶ Install the HDD/SSD module as described in section ["Installing 2.5-inch HDD/SSD modules" on page 120](#).

7.2.7.4 Concluding steps

- ▶ ["Performing a RAID array rebuild" on page 85](#)

7.2.8 Replacing the 4 x 2.5-inch HDD backplane



Field Replaceable Unit (FRU)



Hardware: 10 minutes

Tools: tool-less

7.2.8.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Release all HDD/SSD modules and pull them out a few centimeters, see section ["Removing 2.5-inch HDD/SSD modules" on page 122](#)



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

7.2.8.2 Removing the defective 4 x 2.5-inch HDD backplane



For configurations with up to four 2.5-inch HDDs/SSDs, please refer to: section ["Left side 4 x 2.5-inch HDD backplane \(A3C40157852\)" on page 127](#).

For configurations with up to eight 2.5-inch HDDs/SSDs, please refer to: section ["Left side 4 x 2.5-inch HDD backplane \(A3C40157852\)" on page 127](#) or ["Right side 4 x 2.5-inch HDD backplane \(A3C40157828\)" on page 128](#).

Left side 4 x 2.5-inch HDD backplane (A3C40157852)

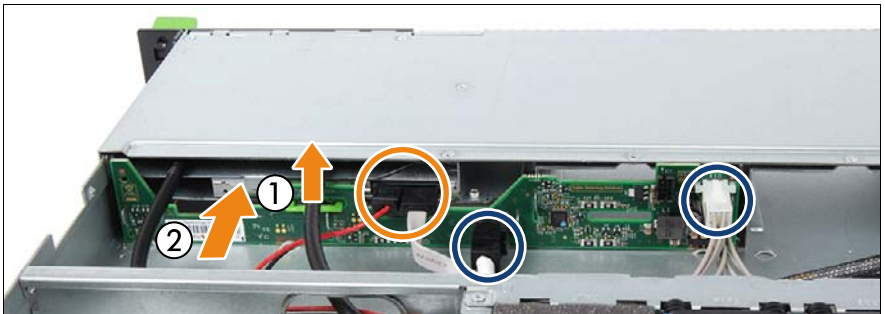


Figure 59: Releasing the ODD latch and disconnecting the cables

- ▶ If applicable, disconnect both cables from the ODD (see orange circle).
- ▶ If applicable, pull the ODD latch upward (1) until it disengages and push the ODD somewhat in direction of the front side (2).
- ▶ Disconnect all cables from the HDD backplane (see blue circles).



If applicable, remove the OOB cable from the HDD backplane, too.

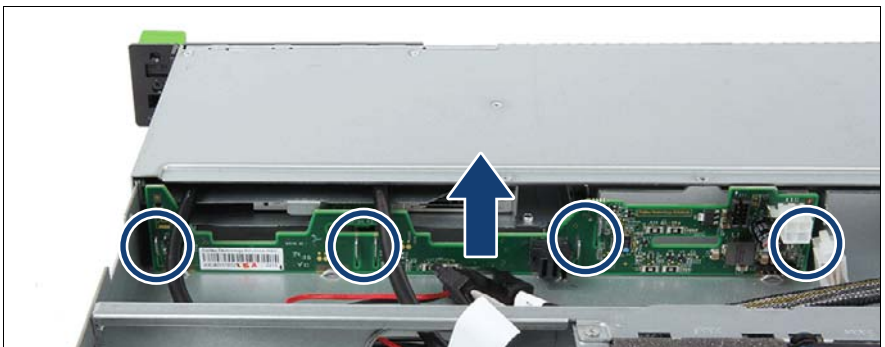


Figure 60: Removing the 4 x 2.5-inch HDD backplane

- ▶ Pull the HDD backplane upward until the six hooks disengage (see circles).
- ▶ Take out the HDD backplane.

Right side 4 x 2.5-inch HDD backplane (A3C40157828)

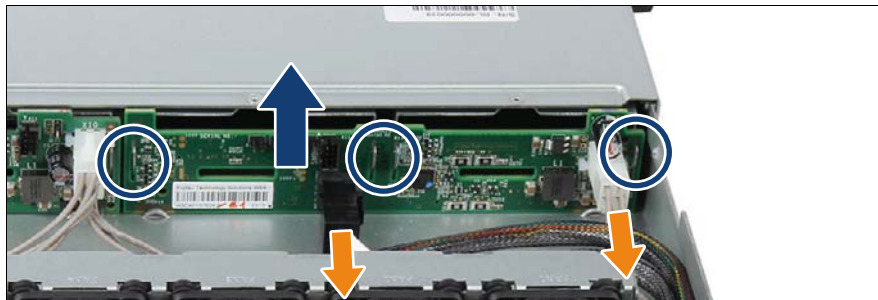


Figure 61: Removing the 4 x 2.5-inch HDD backplane

- ▶ Disconnect all cables from the HDD backplane (see orange arrows).
 - i** If applicable, remove the OOB cable from the HDD backplane, too.
- ▶ Pull the HDD backplane upward until the four hooks disengage (see circles).
- ▶ Take out the HDD backplane.

7.2.8.3 Installing the new 4 x 2.5-inch HDD backplane

i For configurations with up to four 2.5-inch HDDs/SSDs, please refer to: section "[Left side 4 x 2.5-inch HDD backplane \(A3C40157852\)](#)" on [page 129](#).

For configurations with up to eight 2.5-inch HDDs/SSDs, please refer to: section "[Left side 4 x 2.5-inch HDD backplane \(A3C40157852\)](#)" on [page 129](#) or "[Right side 4 x 2.5-inch HDD backplane \(A3C40157828\)](#)" on [page 131](#).

Left side 4 x 2.5-inch HDD backplane (A3C40157852)

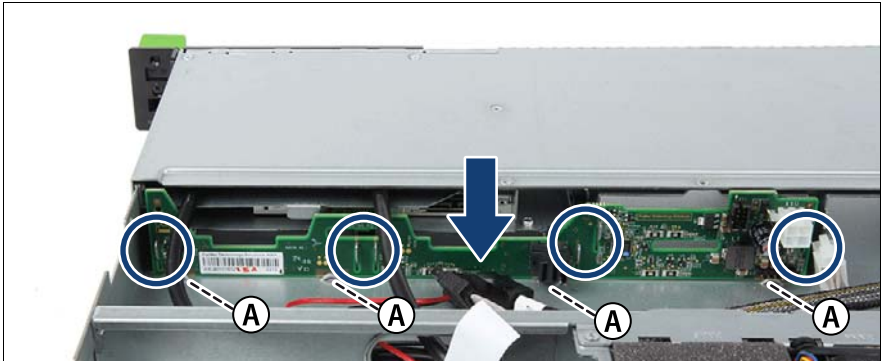


Figure 62: Installing the 4 x 2.5-inch HDD backplane

- ▶ Position the HDD backplane on the six hooks (see circles).
- ▶ Push the HDD backplane downward. Make sure that the lower cant of the HDD backplane fits in the guides (A).



CAUTION!

Ensure that none of the cables are strained or damaged!

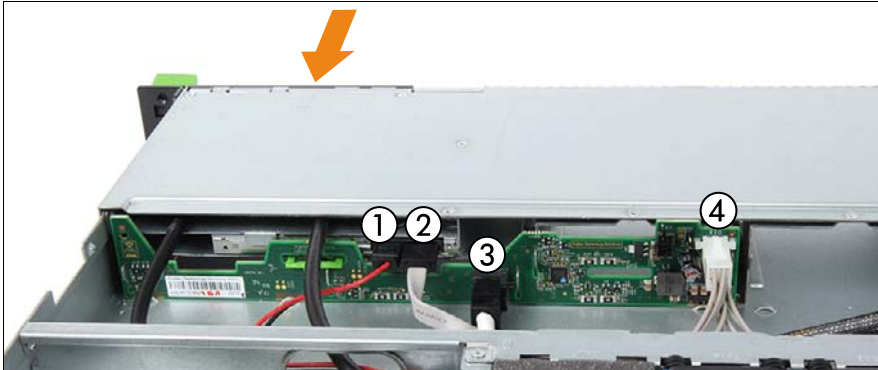


Figure 63: Connecting the cables to the ODD and the 4 x 2.5-inch HDD backplane

- ▶ If applicable, push the ODD in its bay until the ODD latch engages (see orange arrow).
- ▶ Connect the following cables to the ODD and the HDD backplane:
 - (1) power cable to ODD (if applicable)
 - (2) SATA cable to ODD (if applicable)
 - (3) SAS cable to connector "X5" on the HDD backplane
 - (4) power cable to connector "PWR" on the HDD backplane

i If applicable, connect the OOB cable to connector "SMBus" on the HDD backplane.

For the cable plan see section ["Cabling" on page 285](#).

Right side 4 x 2.5-inch HDD backplane (A3C40157828)

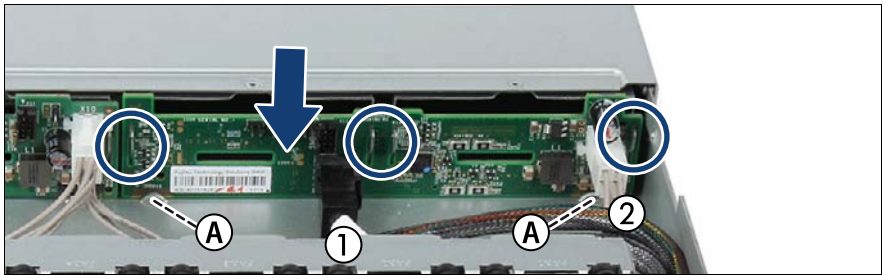


Figure 64: Installing the 4 x 2.5-inch HDD backplane

- ▶ Position the HDD backplane on the four hooks (see circles).
- ▶ Push the HDD backplane downward. Make sure that the lower cant of the HDD backplane fits in the guides (A).



CAUTION!

Ensure that none of the cables are strained or damaged!

- ▶ Connect the following cables to the HDD backplane:
 - (1) SAS cable to connector "X5" on the HDD backplane
 - (2) power cable to connector "PWR" on the HDD backplane



If applicable, connect the OOB cable to connector "SMBus" on the HDD backplane.

For the cable plan see section "[Cabling](#)" on page 285.

7.2.8.4 Concluding steps

- ▶ Insert all HDD/SSD modules, see section "[Installing 2.5-inch HDD/SSD modules](#)" on page 120.



Make sure that you reinstall the HDD/SSD module in the bay it was located before the HDD backplane replacement.

- ▶ "[Reassembling](#)" on page 52
- ▶ "[Connecting the server to the mains](#)" on page 55
- ▶ "[Switching on the server](#)" on page 57

7.2.9 Replacing the 10 x 2.5-inch HDD backplane



Field Replaceable Unit (FRU)



Hardware: 15 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver (for removing/installing SAS expander board)

7.2.9.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Release all HDD/SSD modules and pull them out a few centimeters, see section ["Removing 2.5-inch HDD/SSD modules" on page 122](#)



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

7.2.9.2 Removing the SAS expander board



Figure 65: Disconnecting power cable from the HDD backplane

- ▶ Disconnect the power cable from the HDD backplane.

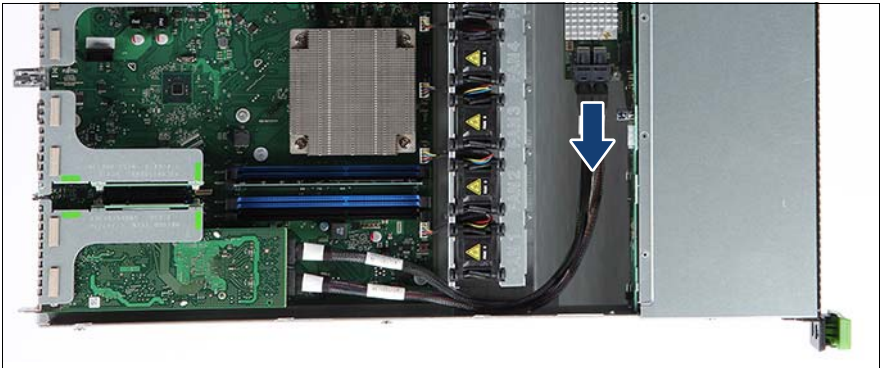


Figure 66: Disconnecting SAS cables

- ▶ Disconnect the two SAS cables from the SAS expander board.



Figure 67: Removing the SAS expander board (A)

- ▶ Remove the two screws (see circles).

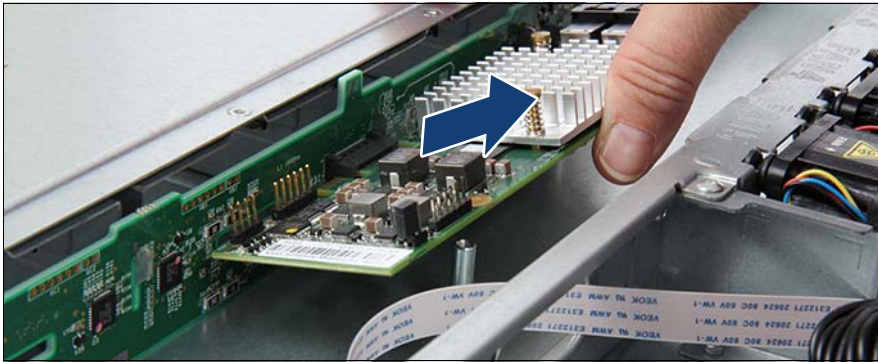


Figure 68: Removing the SAS expander board (B)

- ▶ Get the SAS expander board out of the two connectors of the HDD backplane and remove it.



CAUTION!

Lift up the SAS expander board while removing it in order to prevent the components to be damaged by the stand-offs of the chassis.

7.2.9.3 Removing the defective 10 x 2.5-inch HDD backplane

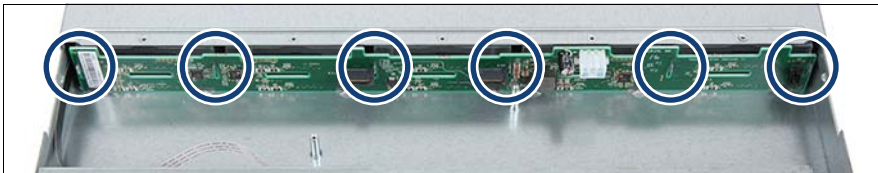


Figure 69: Removing the 10 x 2.5-inch HDD backplane

- ▶ Pull the HDD backplane upward until the six hooks disengage (see circles).
- ▶ Take out the HDD backplane.

7.2.9.4 Installing the new 10 x 2.5-inch HDD backplane

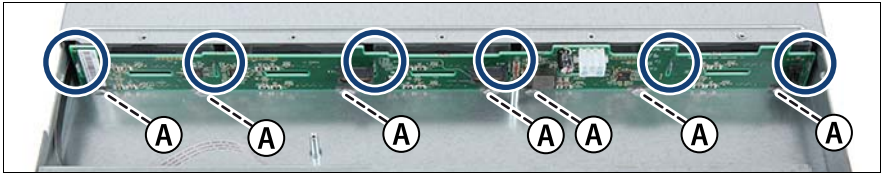


Figure 70: Installing the 10 x 2.5-inch HDD backplane

- ▶ Position the HDD backplane on the six hooks (see circles).
- ▶ Push the HDD backplane downward. Make sure that the lower cant of the HDD backplane fits in the guides (A).

7.2.9.5 Installing the SAS expander board

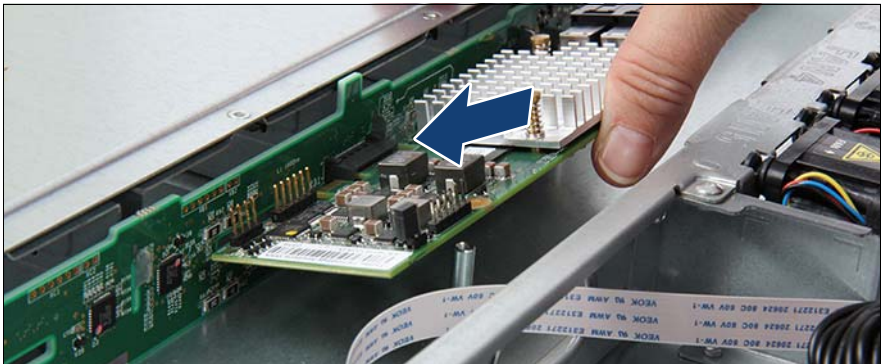


Figure 71: Installing the SAS expander board (A)

- ▶ Insert the SAS expander board into the two connectors of the HDD backplane.



CAUTION!

Lift up the SAS expander board while inserting it in order to prevent the components to be damaged by the stand-offs of the chassis.

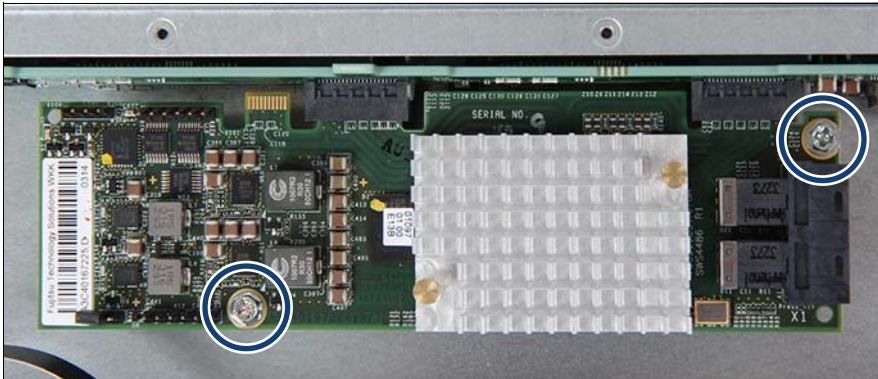


Figure 72: Installing the SAS expander board (B)

- ▶ Fasten the SAS expander board with two screws (see circles).

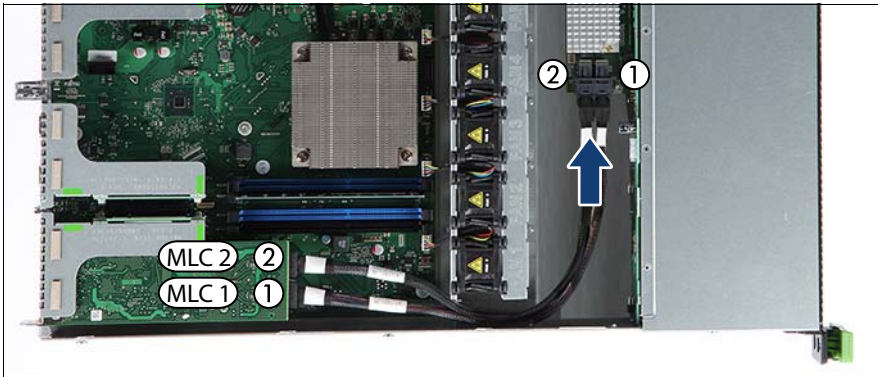


Figure 73: Connecting SAS cables

- ▶ Connect the two SAS cables to the SAS expander board:
 - (1) from SAS controller connector MLC1 to SAS expander board
 - (2) from SAS controller connector MLC2 to SAS expander board



Figure 74: Connecting power cable to the HDD backplane

- ▶ Connect the power cable to the HDD backplane.

7.2.9.6 Concluding steps

- ▶ Insert all HDD/SSD modules, see section "[Installing 2.5-inch HDD/SSD modules](#)" on page 120.



Make sure that you reinstall the HDD/SSD module in the bay it was located before the HDD backplane replacement.

- ▶ "[Reassembling](#)" on page 52
- ▶ "[Connecting the server to the mains](#)" on page 55
- ▶ "[Switching on the server](#)" on page 57

7.2.10 Replacing the SAS expander board



Field Replaceable Unit (FRU)



Hardware: 10 minutes

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

7.2.10.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

7.2.10.2 Removing the defective SAS expander board

- ▶ Remove the SAS expander board as described in section ["Removing the SAS expander board" on page 132](#).

7.2.10.3 Installing the new SAS expander board

- ▶ Install the SAS expander board as described in section ["Installing the SAS expander board" on page 135](#).

7.2.10.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

7.2.11 Upgrading configuration from up to four to up to eight 2.5-inch HDDs/SSDs



Upgrade and Repair Unit (URU)



Hardware: 10 minutes

Tools: tool-less



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.

7.2.11.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Release all HDD/SSD modules and pull them out a few centimeters, see section ["Removing 2.5-inch HDD/SSD modules" on page 122](#)



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

7.2.11.2 Installing the second HDD backplane

- ▶ Install the second HDD backplane as described in section ["Right side 4 x 2.5-inch HDD backplane \(A3C40157828\)" on page 131](#).
- ▶ If applicable, install a dual-channel RAID controller as described in section ["Installing an expansion card" on page 170](#).
- ▶ Disconnect the SAS cable connected to the HDD backplane (A3C40157852) from the system board connector "MLC SATA1-4" or from the RAID controller connector "MLC1".

- ▶ Connect the SAS cables:
The shorter SAS cable connected to HDD backplane (A3C40157828) to connector "MLC1" of the dual-channel RAID controller (1)
The longer SAS cable connected to HDD backplane (A3C40157852) to connector "MLC2" of the dual-channel RAID controller (2)

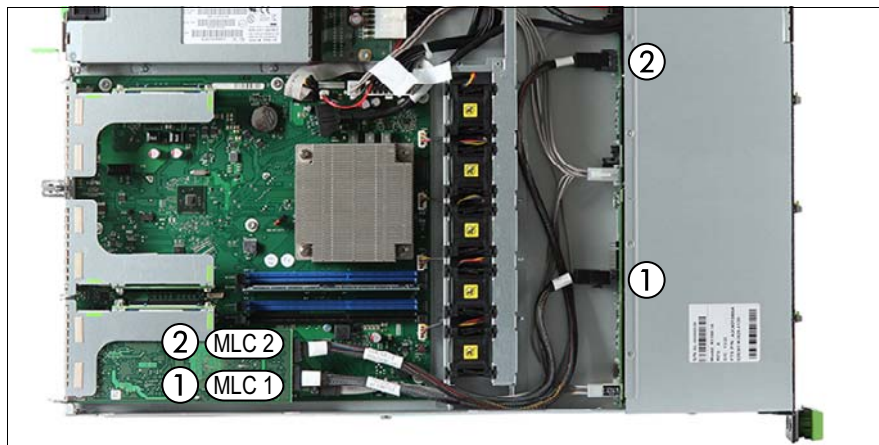


Figure 75: Routing SAS cables

- ▶ Route the SAS cables as shown in the figure above.

7.2.11.3 Installing additional HDD/SSD modules

- ▶ Remove the dummy locks as described in section ["Removing a 2.5-inch HDD/SSD dummy module" on page 120](#).
- ▶ Move the HDD/SSD modules installed in the former HDD bays 1 to 4 (see figure 48) to the new HDD bays 1 to 4 (see figure 50).
- ▶ Insert additional HDD/SSD modules as described in section ["Installing 2.5-inch HDD/SSD modules" on page 120](#).

7.2.11.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Performing a RAID array rebuild" on page 85](#)

7.3 3.5-inch HDD configurations

7.3.1 Equipping the 3.5-inch HDD bays

- If only one HDD module is installed, the HDD module will be installed in the left bay (seen from the front) and dummy modules must be installed in the free bays.
- Installing different capacities, install the biggest capacity first.
- Installing different rotating speed, install the fastest rotating speed first.

Mounting order



Figure 76: Mounting order with up to four 3.5-inch HDDs

HDD naming scheme



Figure 77: Naming scheme with up to four 3.5-inch HDDs

i The HDD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

Position	Logical drive number	ServerView RAID Manager display name
①	0	HDD vendor name (0)
②	1	HDD vendor name (1)
③	2	HDD vendor name (2)
④	3	HDD vendor name (3)

7.3.2 Installing 3.5-inch HDD modules



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less

7.3.2.1 Preliminary steps

- ▶ Locate the correct drive bay as described in section ["3.5-inch HDD configurations"](#) on page 141.

7.3.2.2 Removing a 3.5-inch HDD dummy module

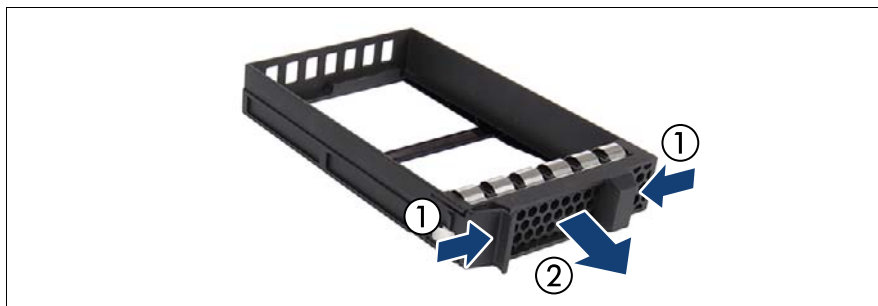


Figure 78: Removing a 3.5-inch dummy module

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



CAUTION!

Save the dummy module for future use.

Always replace dummy modules into unused HDD bays to comply with applicable EMC regulations and satisfy cooling requirements.

7.3.2.3 Installing a 3.5-inch HDD module



Figure 79: Opening the 3.5-inch HDD module locking lever

- ▶ Pinch the green locking clip (1) and open the locking lever (2).

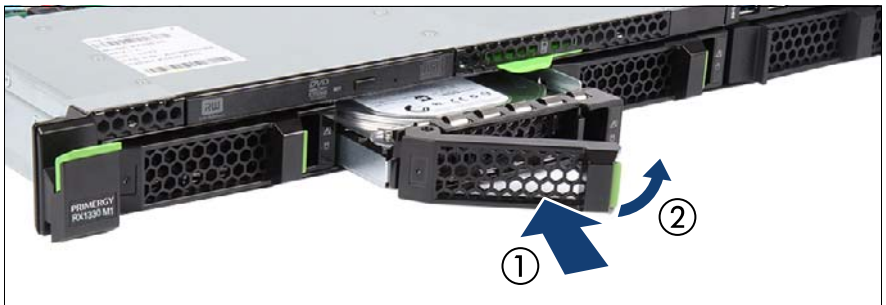


Figure 80: Installing the 3.5-inch HDD module

- ▶ Insert the HDD module into a drive bay and carefully push back as far as it will go (1).
- ▶ Close the locking lever to lock the hard disk drive in place (2).

7.3.2.4 Concluding steps

- ▶ ["Performing a RAID array rebuild" on page 85](#)

7.3.3 Removing 3.5-inch HDD modules



Customer Replaceable Unit (CRU)





Hardware: 5 minutes

Tools: tool-less

7.3.3.1 Preliminary steps

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

RAID level	Procedure
RAID 0	Only remove an HDD module combined in a RAID 0 array if defective.  CAUTION! Removing an operational HDD module will result in data loss!
RAID 1 RAID 5	Removing an HDD module from a RAID 1 or RAID 5 array will not result in data loss. However, the removed drive needs to be replaced immediately by an HDD module of the same or larger capacity.  After replacing the HDD module, RAID rebuild will be performed as a background process as described in section " Performing a RAID array rebuild " on page 85.

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



CAUTION!

All data on all HDDs 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.

7.3.3.2 Removing a 3.5-inch HDD module

- ▶ Pinch the green locking clips and open the locking lever (see figure 79).
- ▶ Pull the HDD module out a few centimeters.
- ▶ Wait about 30 seconds to allow the hard disk drive to spin down.



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

- ▶ Pull the HDD module completely out of its bay.

7.3.3.3 Installing a 3.5-inch dummy module



CAUTION!

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



Figure 81: Installing the 3.5-inch dummy module

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

7.3.3.4 Concluding steps

No steps needed.

7.3.4 Replacing a 3.5-inch HDD module



Customer Replaceable Unit (CRU)



Hardware: 5 minutes

Tools: tool-less



CAUTION!

- Only remove an HDD module during operation if the drive is not currently being accessed. Observe the indicators on the HDD module, see section ["Indicators on the hot-plug HDD module" on page 309](#).
- Under no circumstances should you remove an HDD 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 module can only be replaced during operation in conjunction with a corresponding RAID configuration.

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

7.3.4.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Locating the defective component" on page 45](#)

Only applicable for removing intact HDD modules:

- ▶ Before removing a non-defective HDD module, put the drive into "Offline" mode using your RAID configuration software.



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

7.3.4.2 Removing the defective 3.5-inch HDD module

- ▶ Remove the HDD module as described in section ["Removing a 3.5-inch HDD module" on page 145](#).

7.3.4.3 Installing the new 3.5-inch HDD module

- ▶ Install the HDD module as described in section ["Installing a 3.5-inch HDD module" on page 143](#).

7.3.4.4 Concluding steps

- ▶ ["Performing a RAID array rebuild" on page 85](#)

7.3.5 Replacing the 3.5-inch HDD backplane



Field Replaceable Unit (FRU)



Hardware: 10 minutes

Tools: tool-less

7.3.5.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Release all HDD modules and pull them out a few centimeters, see section ["Removing a 3.5-inch HDD module" on page 145](#)



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

7.3.5.2 Removing the defective 3.5-inch HDD backplane

- ▶ Disconnect all cables from the HDD backplane.

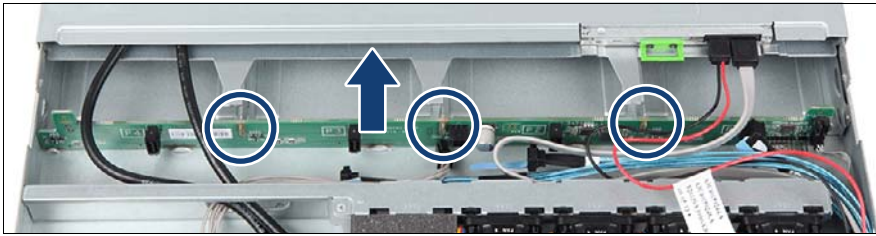


Figure 82: Removing the 3.5-inch HDD backplane

- ▶ Pull the HDD backplane upward until the three hooks disengage (see circles).
- ▶ Take out the HDD backplane.

7.3.5.3 Installing the new 3.5-inch HDD backplane

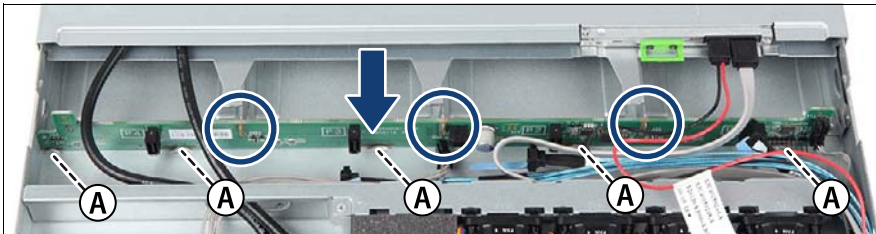


Figure 83: Installing the 3.5-inch HDD backplane

- ▶ Position the HDD backplane on the three hooks (see circles).
- ▶ Push the HDD backplane downward. Make sure that the lower cant of the HDD backplane fits in the guides (A).



CAUTION!

Ensure that none of the cables are strained or damaged!

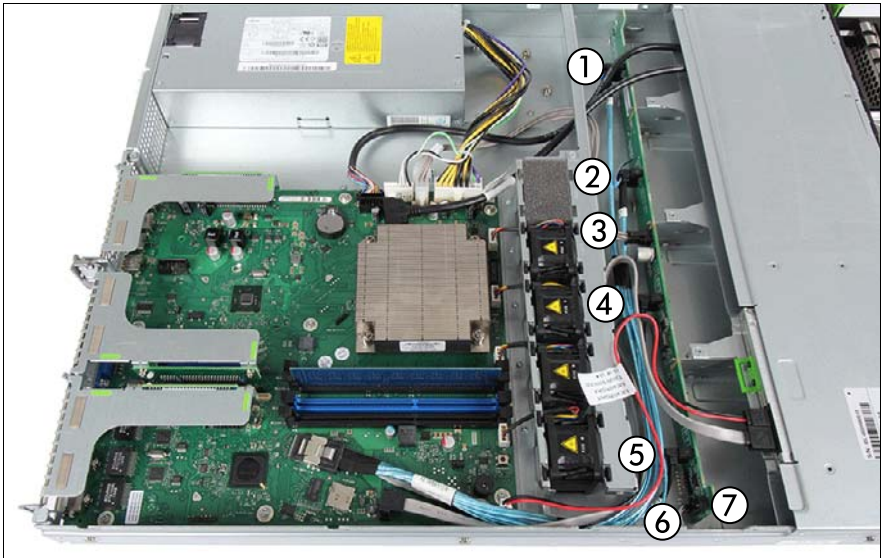


Figure 84: Connecting the cables to the 3.5-inch HDD backplane

- ▶ Connect the following cables to the HDD backplane:
 - SAS/SATA data cable:
 - (1), (2), (4), (5) to connectors "P1", "P2", "P3", "P4" according to the length
 - (6) plug P6 to connector "SGPIO"
 - (3) power cable to connector "PWR"
 - (7) OOB cable to connector "SMBus" (if applicable)

For the cable plan see section "[Cabling](#)" on page 285.

7.3.5.4 Concluding steps

- ▶ Insert all HDD modules, see section "[Installing a 3.5-inch HDD module](#)" on page 143.



Make sure that you reinstall the HDD module in the bay it was located before the HDD backplane replacement.

- ▶ "[Reassembling](#)" on page 52
- ▶ "[Connecting the server to the mains](#)" on page 55
- ▶ "[Switching on the server](#)" on page 57

8 Fans

Safety notes



CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices 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. Before handling them, first touch a metal part of the server to discharge static electricity from your body.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- The installation indicated on this note is sometimes changed to the kind of possible options without notice.
- For further safety information, please refer to chapter "[Important information](#)" on page 31.

8.1 Basic information

Base units with a standard power supply are supplied with four fan modules without redundancy.



CAUTION!

In the configuration with four fan modules, defective system fans have to be replaced immediately.

Base units with a redundant power supply are supplied with five fan modules in a 1 of 5 redundancy. In other words, if one of the five fan modules fails, the system will operate without any problem.

8.1.1 Numbering of the fan modules

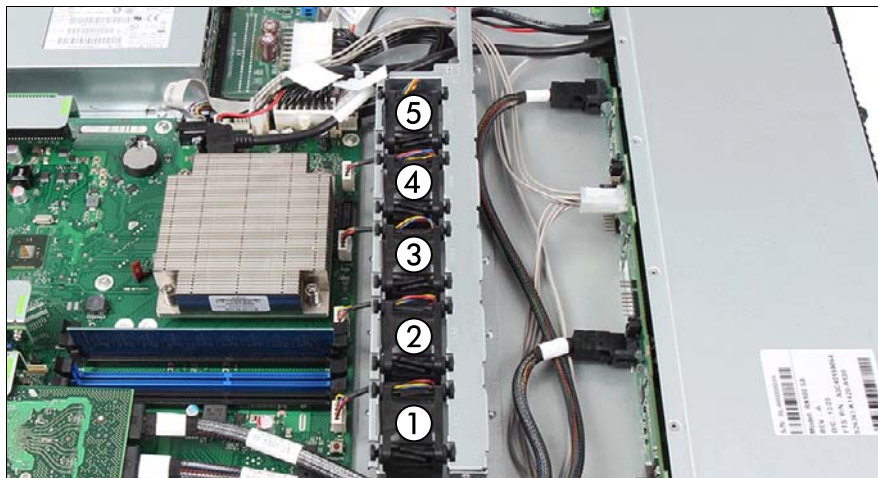


Figure 85: Numbering of the fan modules

8.2 Replacing a defective fan module



Field Replaceable Unit (FRU)



Hardware: 10 minutes

Tools: tool-less

8.2.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)

8.2.2 Removing the defective fan module

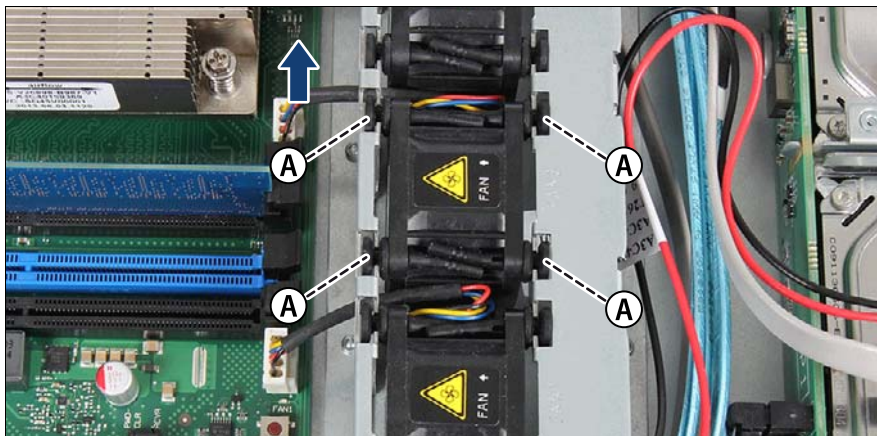


Figure 86: Disconnecting the fan cable

- ▶ Disconnect the fan cable of the fan module from the system board.
- ▶ Lift off the fan module upward about 2 cm.
To do this, press up the four rubber pins (A).

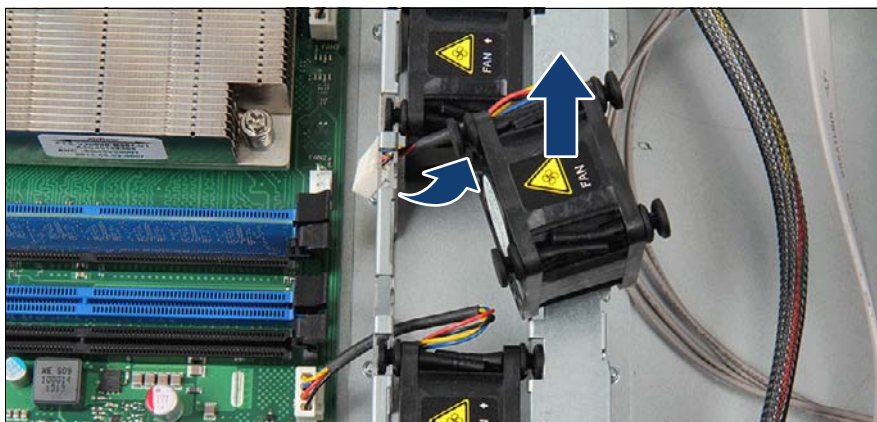


Figure 87: Removing the fan module

- ▶ Push the fan cable through the opening of the fan cage.
- ▶ Take out the fan module.

8.2.3 Installing the new fan module

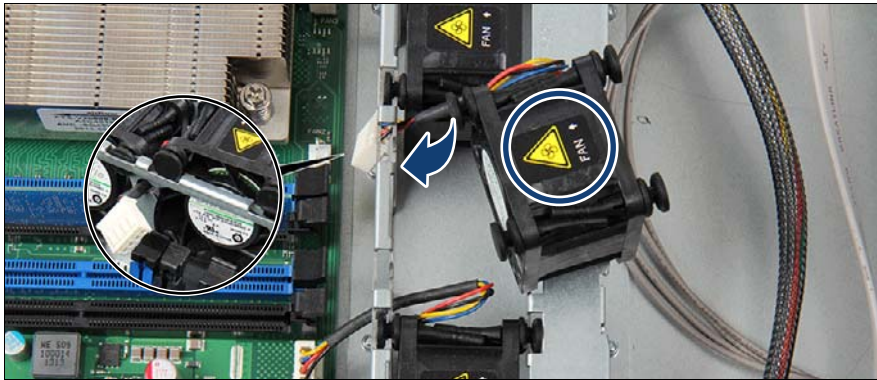


Figure 88: Installing the fan module

- ▶ Thread the fan cable through the opening of the fan cage (see close-up) and insert the fan module. Notice the direction of the fan label (see circle).

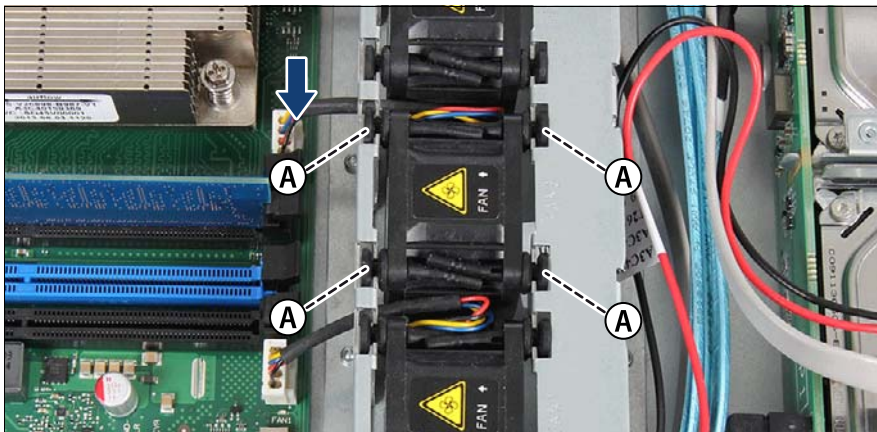


Figure 89: Connecting the fan cable

- ▶ Press down the four rubber pins until they engage (A).
- ▶ Connect the fan cable to the system board.

8.2.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Performing a fan test after replacing a defective fan" on page 89](#)

9 Expansion cards and backup units

Safety notes



CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- For further safety information, please refer to chapter ["Important information" on page 31](#).

9.1 Basic information

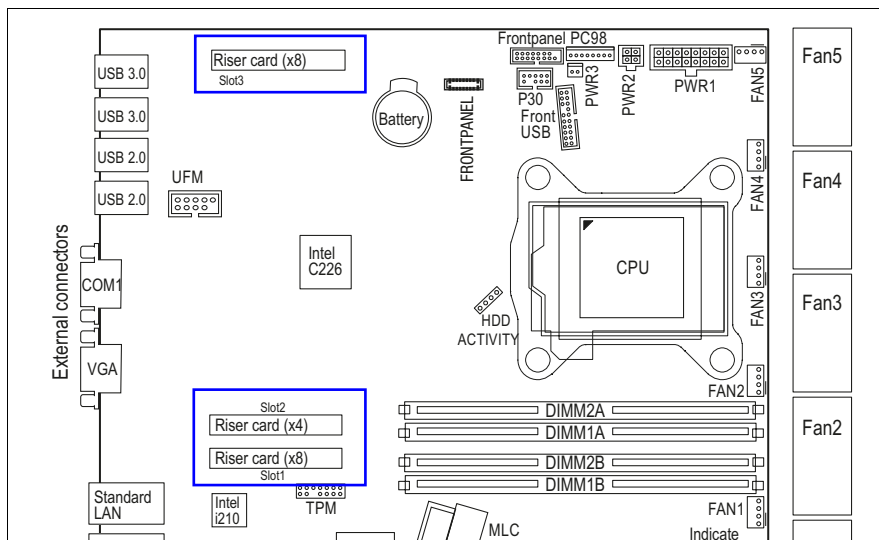


Figure 90: PCI slots for riser cards

9.1.1 Equipping the PCIe slots

PCI slot	Riser module	Type	Description
Slot 1	Riser module 1	PCIe G3 x8 (x8 wired)	Low-profile slot, maximum length 175 mm; dedicated slot for modular RAID controller
Slot 2	Riser module 2	PCIe G2 x8 (x4 wired)	Low-profile slot, maximum length 175 mm
Slot 3	Riser module 3	PCIe G3 x8 (x8 wired)	Low-profile slot, maximum length 175 mm



As an option a full height riser module can be installed (see section ["Upgrading to the full height riser module" on page 182](#)). In this case the slot 2 is not available and slot 3 can be equipped with a full height expansion card.

Expansion cards and backup units

Adapter Installation Sequence Order within Adapter Category (Cluster)	Adapter Vendor	Adapter Product Name Description (Softwarepool)	Adapter Customer Order No."	Max # Adapter	Slot#1	Slot# 2	Slot# 3
VGA							
1	Nvidia	PGRA CP NVS 1GB VGA PCIe x16 card / PGRA CP NVS 1GB LP VGA PCIe x16 card	S26361-F2748-E/L538 (FH)	1	-	-	1
2	Nvidia	PY VGA Card 512MB PCI-e x1 (NVIDIA NVS 300)	S26361-F2748-E/L537 (FH) S26361-F2748-E/L637 (LP)	1	-	1	2
SAS RAID							
1	Fujitsu Technology Solutions	PRAID EP400i	S26361-F5243-E1 / L1	1	1	-	-
2	Fujitsu Technology Solutions	PRAID EP420i	S26361-F5243-E2 / L2	1	1	-	-
3	Fujitsu Technology Solutions	RAID Ctrl SAS 6G 5/6 512MB (D2616)	S26361-F3554-E512 / L512	1	1	-	-
4	Fujitsu Technology Solutions	PRAID CP400i	S26361-F3842-E1 / -L501	1	1	-	-
5	Fujitsu Technology Solutions	RAID Ctrl SAS 6G 0/1 (D2607)	S26361-F3554-E8 / L8	1	1	-	-
SAS Backup							
1	Fujitsu Technology Solutions	PSAS CP400i	S26361-F3842-E2 / -L502	1	1	-	-
2	LSI Logic	PSAS CP400e	S26361-F3845-E1	1	-	2	1
Fiber Channel							
1	EMULEX	FC CTRL LPe12002	S26361-F3961-E2 / S26361-F3961-E202 / S26361-F3961-L2 / S26361-F3961-L202	1	-	1	2
2	EMULEX	FC CTRL LPe1250	S26361-F3961-E1 / S26361-F3961-E201 / S26361-F3961-L1 / S26361-F3961-L201	1	-	1	2
3	Qlogic	FC CTRL QLE2560	S26361-F3631-E1 / S26361-F3631-L1 / S26361-F3631-E201 / S26361-F3631-L201	1	-	1	2
4	Qlogic	FC CTRL QLE2562	S26361-F3631-E2 / S26361-F3631-L2 / S26361-F3631-E202 / S26361-F3631-L202	1	-	1	2
Communication / Ethernet							
1	Fujitsu Technology Solutions	Eth Ctrl 2x10Gbit PCIe x8 D2755 SFP+	S26361-F3629-E2 / E202 / L502 / E702	1	-	2	1
2	Intel	Eth Ctrl 2x10GBase-T PCIe x8 X540-T2	S26361-F3752-E2 / E202 / L502	1	-	2	1
3	Intel	PLAN CP 4x1Gbit Cu Intel I350-T4	S26361-F4610-E4 / E204 / L504 / E704	2	-	1	2
4	Intel	PLAN CP 2x1Gbit Cu Intel I350-T2	S26361-F4610-E2 / E202 / L502 / E702	2	-	1	2
5	Intel	Eth Ctrl 1x1Gbit PCI-e Gigabit CT DT Cu	S26361-F3516-E1 / L1 / E201 / L201	2	-	1	2
11	Intel	PLAN AP 1x1Gbit Cu Intel I210-T1	S26361-F3852-E201	2	-	1	2

Figure 91: Example list

Expansion cards and backup units



For the latest information of the installing order, refer to your server's hardware configurator available online at the following address:

for the EMEA market:

http://ts.fujitsu.com/products/standard_servers/index.htm

for the Japanese market:

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

9.2 Handling slot brackets

9.2.1 Installing a slot bracket



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

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



Use the low profile bracket perforated for the ModularRAID controllers based on LSI MegaRAID.

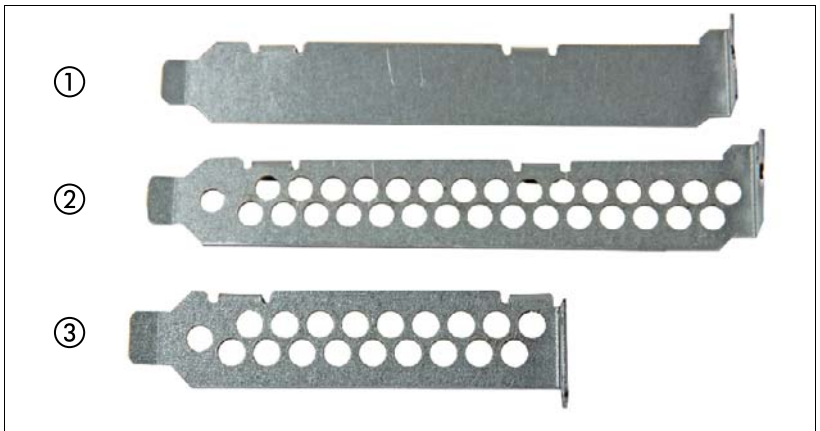


Figure 92: Perforated and non-perforated slot brackets

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

Installing the slot bracket

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

Example network adapter D2755

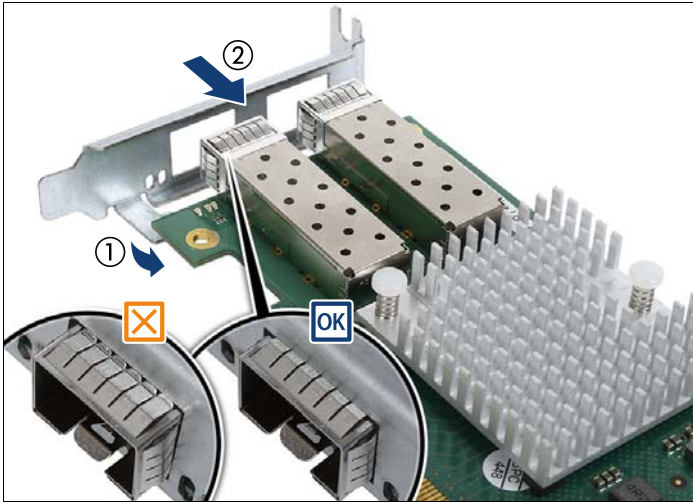


Figure 93: Placing the slot bracket - D2755

- ▶ Place the controller on the mounting tabs on the slot bracket (1).
- ▶ Carefully shift the slot bracket towards the controller until the plug shells engage with the cut-outs in the slot bracket connector panel (2).
- ▶ Ensure that the ESD springs on the plug shells properly engage with the slot bracket as shown (see circles).

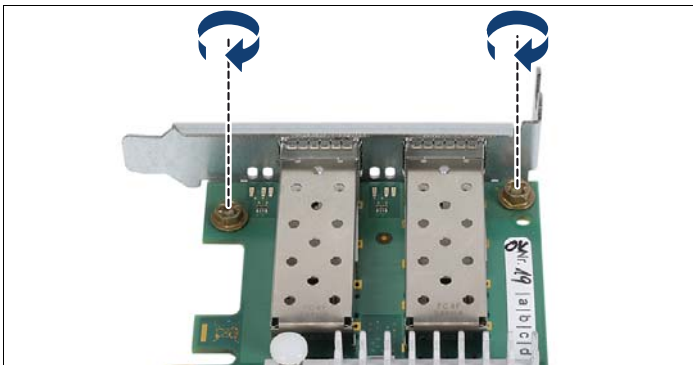


Figure 94: Fastening the slot bracket - D2755

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

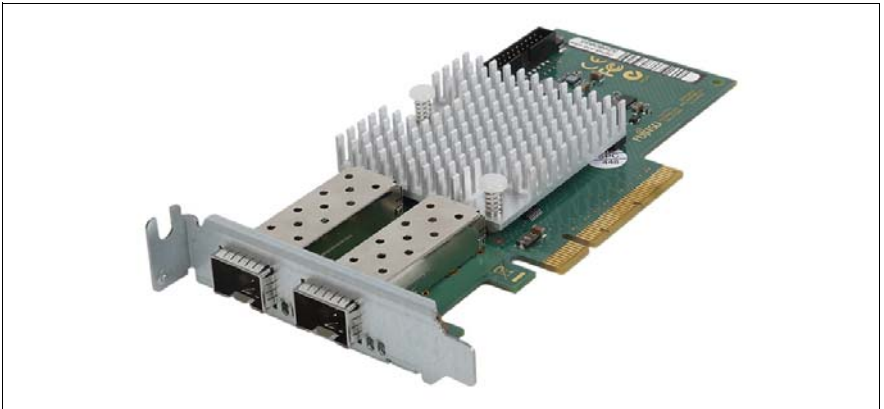


Figure 95: Assembled network adapter D2755

9.2.2 Removing a slot bracket



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

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

9.2.2.1 Removing the slot bracket

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

9.3 Handling SFP+ transceiver modules

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

9.3.1 Installing SFP+ transceiver modules



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

Tools: tool-less

Preparing the SFP+ transceiver module



Figure 96: Removing the protective optical port plug

- ▶ Remove the SFP+ transceiver module from its protective packaging.
- ▶ Remove the optical port plug from the new / additional SFP+ transceiver module.



CAUTION!

- Always keep the protective port plugs attached to the transceiver optical bores and fiber-optic cable connectors until you are ready to make a connection.
- Save the protective port plug for future use.



Figure 97: Unlatching the locking bail

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

Inserting the SFP+ transceiver module



Figure 98: Inserting the SFP+ transceiver module

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



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

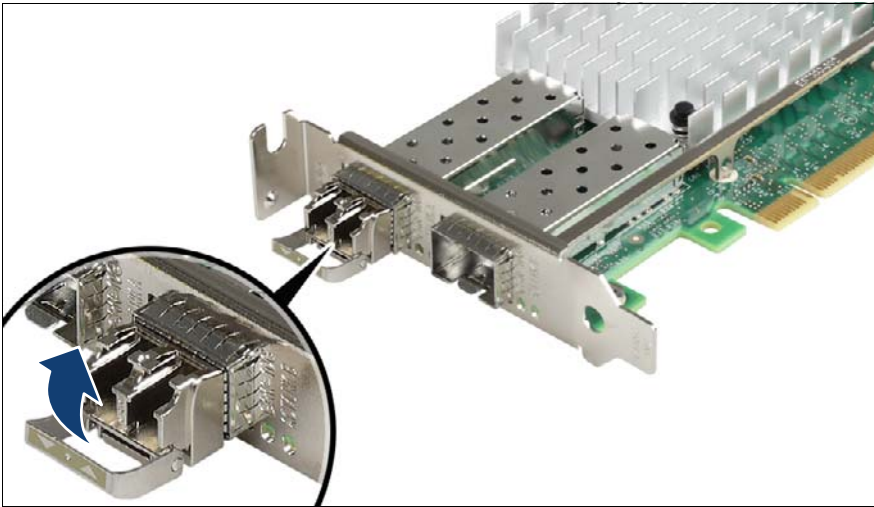


Figure 99: Latching the locking bail

- ▶ Carefully fold up and latch the locking bail.

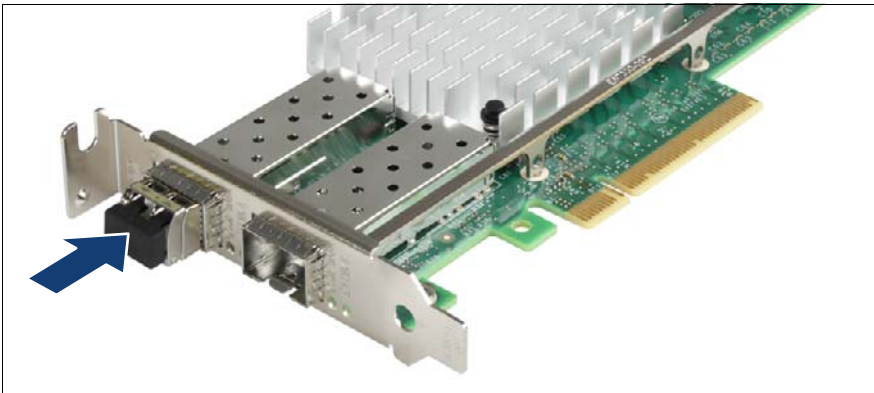


Figure 100: Installing the protective optical port plug

- ▶ If the SFP+ transceiver module is not immediately connected to an LC connector, attach the protective optical port plug to the transceiver optical bores.

Installing the secondary SFP+ transceiver module



Figure 101: Installing the secondary SFP+ transceiver module

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

9.3.2 Removing an SFP+ transceiver module



**Upgrade and Repair Unit
(URU)**



Hardware: 5 minutes

Tools: tool-less

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

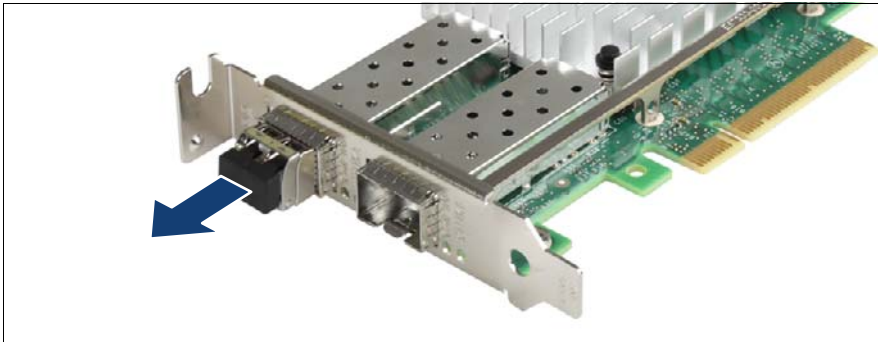


Figure 102: Removing the protective optical port plug

- ▶ If present, remove the protective optical port plug from the SFP+ transceiver module.



CAUTION!

Save the protective port plug for future use.

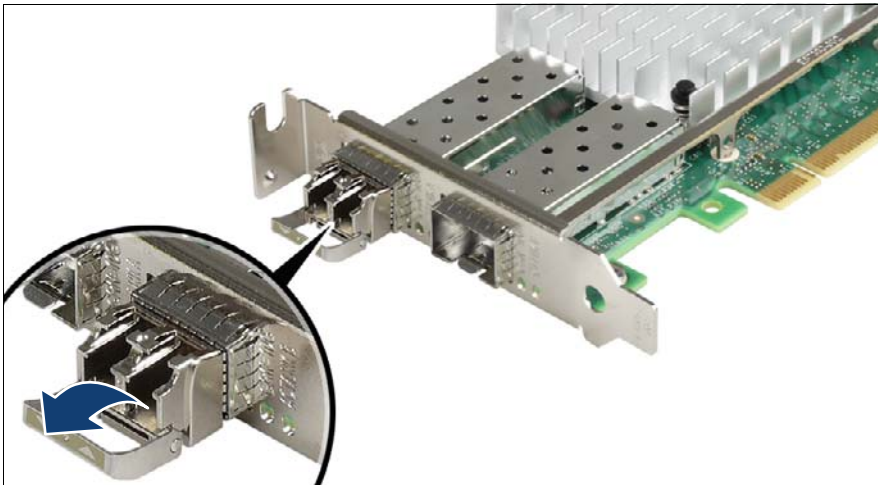


Figure 103: Unlatching the locking bail

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

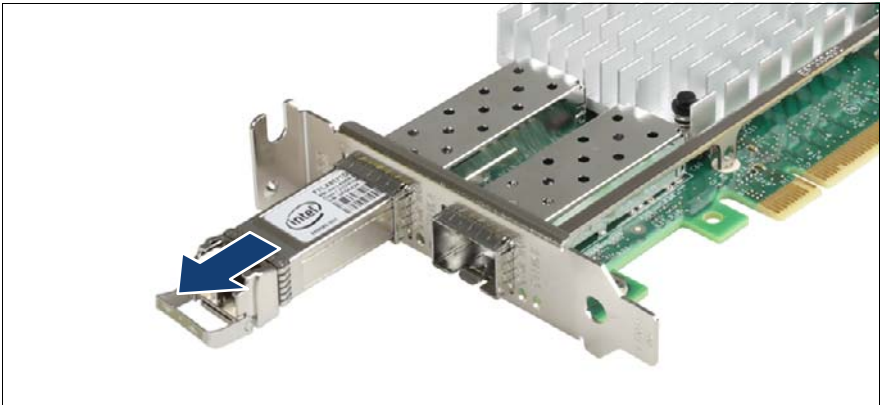



Figure 104: Removing the SFP+ transceiver module

- ▶ Pull the SFP+ transceiver module out of its socket connector.
 - ▶ Attach the protective optical port plug to the transceiver optical bores.
-  Place the removed SFP+ transceiver module in an antistatic bag or other protective environment.

9.4 Expansion cards and riser cards

9.4.1 Installing an expansion card



Upgrade and Repair Unit (URU)



Hardware: 10 minutes
Software: 5 minutes

Tools: tool-less

9.4.1.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the corresponding riser module as described in section ["Removing a riser module" on page 58](#).

9.4.1.2 Removing the slot cover

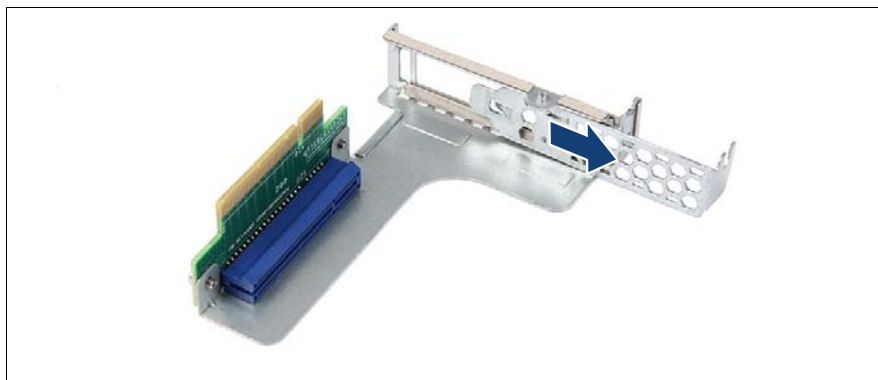


Figure 105: Removing the slot cover - example riser module 1

- ▶ Remove the slot cover.



CAUTION!

Keep the slot cover for future use. If the expansion card is removed and not replaced with a new one, the slot cover must be reinstalled due to cooling, to comply with applicable EMC regulations and to protect against fire.

9.4.1.3 Installing the expansion card

- ▶ Please read the documentation supplied with the expansion card.
- ▶ If applicable, install a slot bracket to the expansion card as described in section ["Installing a slot bracket" on page 161](#).

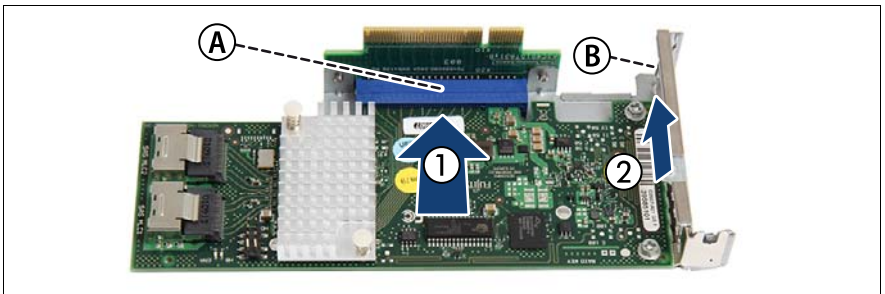


Figure 106: Installing an expansion card - example riser module 1

- ▶ Carefully press the expansion card into the riser card slot (A), until it clicks into place (1). Make sure that the lug on the slot cover (B) clicks into place in the corresponding hole (2).

9.4.1.4 Concluding steps

- ▶ Install the corresponding riser module as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating RAID controller firmware" on page 74](#)
- ▶ ["Enabling Option ROM scan" on page 75](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)

- ▶ ["Resuming BitLocker functionality" on page 84](#)

9.4.2 Removing an expansion card



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

Tools: tool-less

9.4.2.1 Preliminary steps

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the corresponding riser module as described in section ["Removing a riser module" on page 58](#).

9.4.2.2 Removing the expansion card

- ▶ If necessary, disconnect the cables from the expansion card.

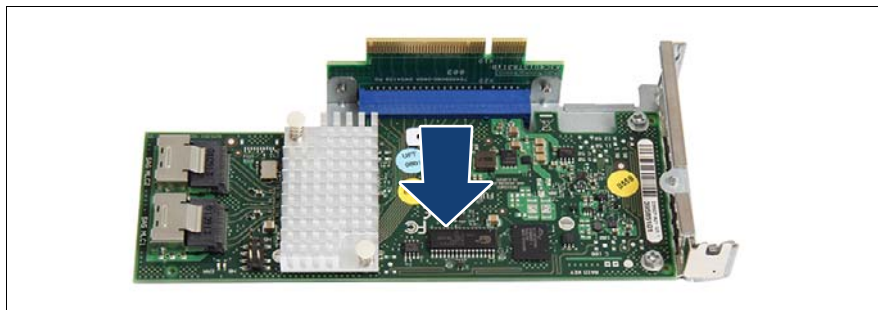


Figure 107: Removing the expansion card - example riser module 1

- ▶ Pull out the expansion card from the riser card slot.

9.4.2.3 Installing the slot cover

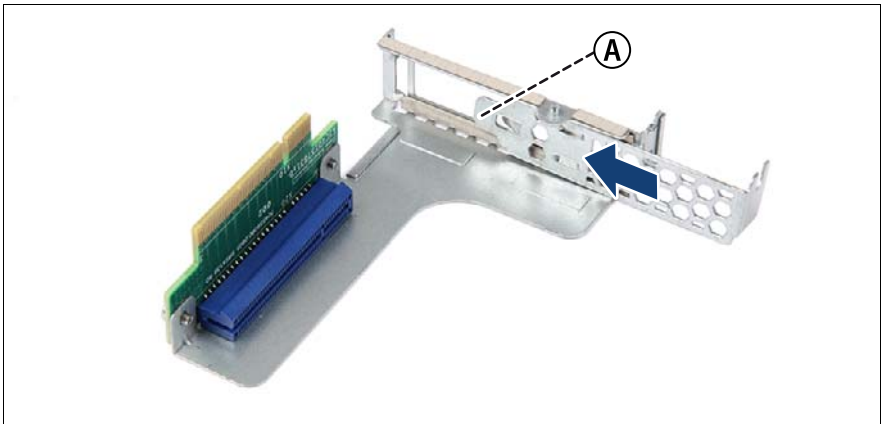


Figure 108: Installing the slot cover - example riser module 1

- ▶ Insert the slot cover. Make sure that the lug on the slot cover (A) clicks into place in the corresponding hole.

9.4.2.4 Concluding steps

- ▶ Install the corresponding riser module as described in section ["Installing a riser module"](#) on page 60.
- ▶ ["Reassembling"](#) on page 52
- ▶ ["Connecting the server to the mains"](#) on page 55
- ▶ ["Switching on the server"](#) on page 57
- ▶ ["Resuming BitLocker functionality"](#) on page 84

9.4.3 Replacing an expansion card



Upgrade and Repair Unit (URU)



Hardware: 10 minutes
Software: 5 minutes

Tools: tool-less

Note on network settings recovery



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

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

9.4.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ If applicable, ensure to note down your current network settings in the operating system.
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)
- ▶ Remove the corresponding riser module as described in section ["Handling riser modules" on page 58](#).

9.4.3.2 Removing the defective expansion card


- ▶ Remove the expansion card as described in section ["Removing the expansion card" on page 172](#).

- ▶ If the slot bracket on the defective expansion card is to be reused, remove it from the expansion card as described in section ["Removing a slot bracket" on page 163](#).

9.4.3.3 Installing the new expansion card

- ▶ If applicable, install the slot bracket as described in section ["Installing a slot bracket" on page 161](#).
- ▶ Install the expansion card as described in section ["Installing the expansion card" on page 171](#).

9.4.3.4 Concluding steps

- ▶ Install the corresponding riser module as described in section ["Handling riser modules" on page 58](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Enabling replaced components in the system BIOS" on page 79](#)
- ▶ ["Updating RAID controller firmware" on page 74](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)
- ▶ After replacing a network controller in a server running Linux OS, ["Updating the NIC configuration file in a Linux environment" on page 83](#).
- ▶ If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard).
 -  Configuration of network settings should be performed by the customer. For further information, please refer to section ["Note on network settings recovery" on page 174](#).
- ▶ If applicable, restore LAN teaming configurations, see ["After replacing / upgrading LAN controllers" on page 88](#).
- ▶ Inform the customer about changed WWN and MAC addresses, see ["Looking up changed MAC / WWN addresses" on page 85](#).

9.4.4 Replacing a riser card



Field Replaceable Unit (FRU)



Hardware: 5 minutes

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

9.4.4.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)
- ▶ Remove the corresponding riser module as described in section ["Handling riser modules" on page 58](#).

9.4.4.2 Removing the defective riser card

- ▶ Remove the expansion card as described in section ["Removing the expansion card" on page 172](#).

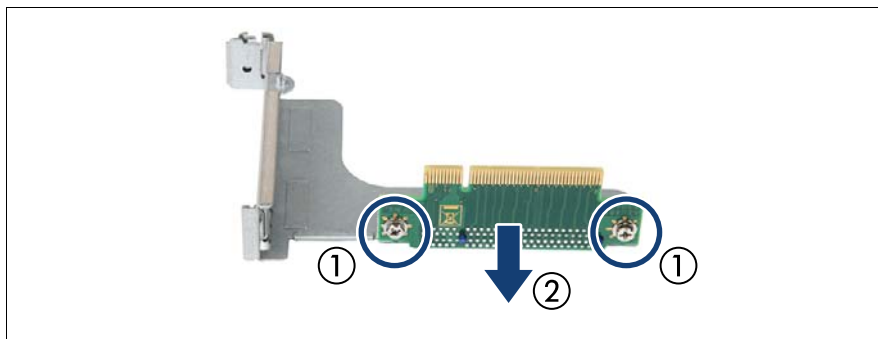


Figure 109: Removing the riser card - example riser module 1

- ▶ Remove the two screws (1).
- ▶ Remove the riser card (2).

9.4.4.3 Installing the new riser card

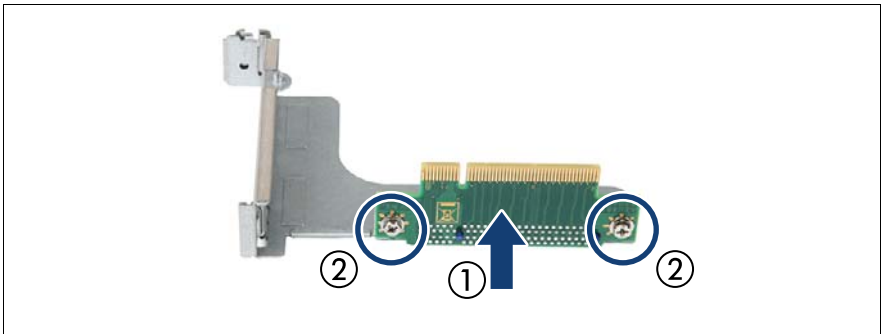


Figure 110: Installing the riser card - example riser module 1

- ▶ Insert the riser card (1).
- ▶ Fasten the riser card with two screws (2).
- ▶ Install the expansion card as described in section ["Installing the expansion card" on page 171](#).

9.4.4.4 Concluding steps

- ▶ Install the corresponding riser module as described in section ["Handling riser modules" on page 58](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

9.4.5 Replacing a TFM

Notes for variants of TFM

Depending on the RAID controller, different TFM kits are available.

RAID controller	TFM kit
PRAID EP400i S26361-D3216-Axx	TFM 4G (LSZ:03-25444-05)
PRAID EP420i S26361-D3216-Bxx	TFM 8G (LSZ:03-25444-01)



**Upgrade and Repair Unit
(URU)**



Hardware: 10 minutes

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

9.4.5.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)

9.4.5.2 Removing the defective TFM

- ▶ Remove the depending expansion card as described in section ["Removing the expansion card" on page 172](#).

Example RAID controller D3216

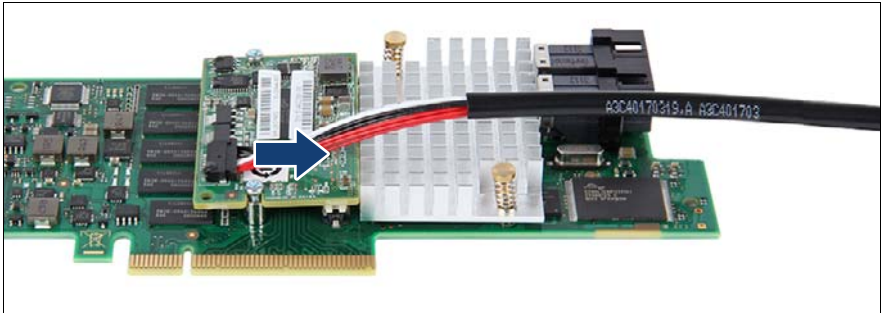


Figure 111: Disconnecting the FBU adapter cable from the TFM

- ▶ Disconnect the FBU adapter cable from the TFM.

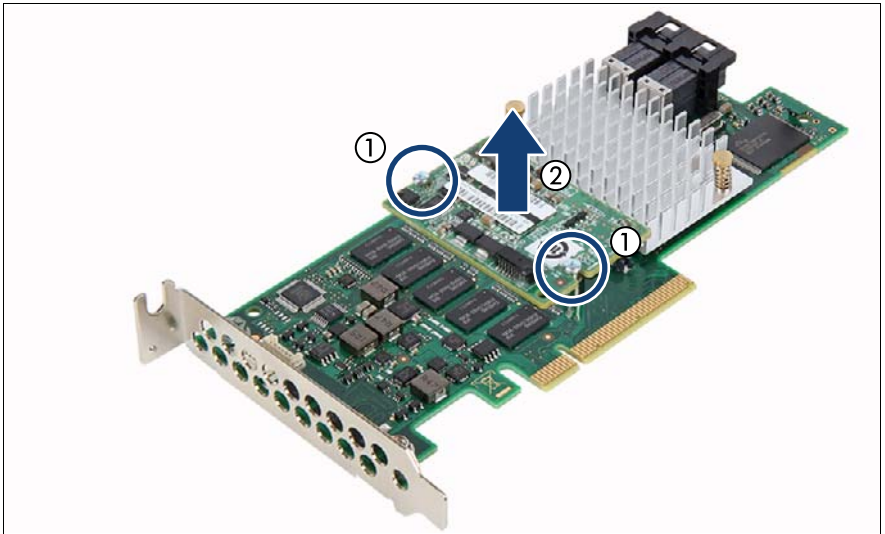


Figure 112: Removing the TFM

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



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

9.4.5.3 Installing the new TFM

Example RAID controller D3216

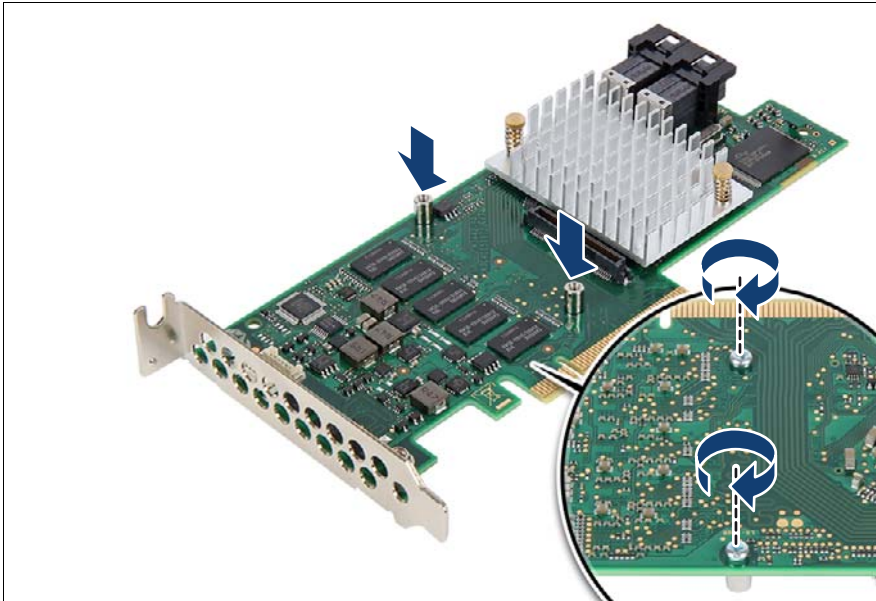


Figure 113: Installing the TFM (A)

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

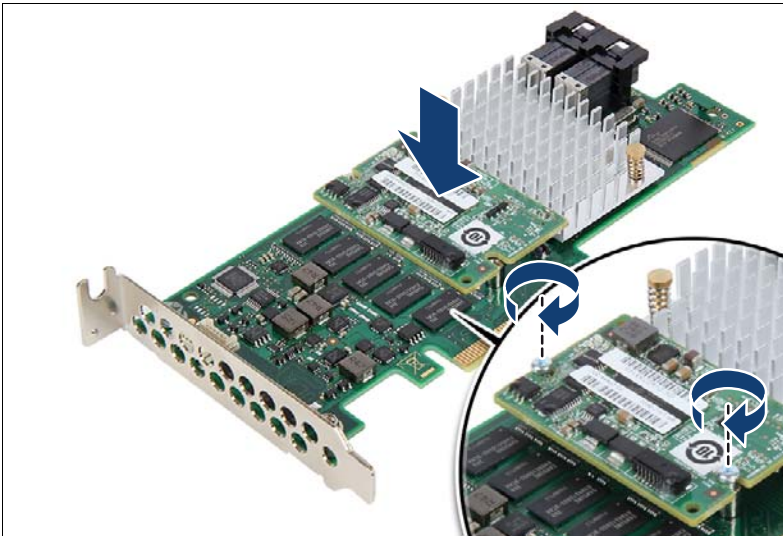


Figure 114: Installing the TFM (B)

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



Figure 115: Connecting the FBU adapter cable

- ▶ Connect the FBU adapter cable to the TFM.
- ▶ Install the expansion card as described in section ["Installing the expansion card" on page 171](#).

9.4.5.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

9.4.6 Upgrading to the full height riser module



Upgrade and Repair Unit (URU)



Hardware: 10 minutes

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

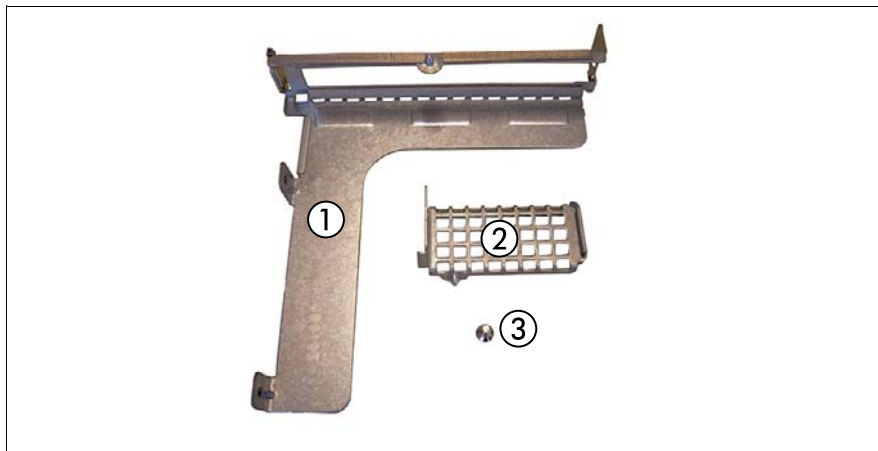


Figure 116: Upgrade kit

1	Full height riser module
2	Extension bracket
3	Screw

9.4.6.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 2 and the riser module 3 as described in section ["Handling riser modules" on page 58](#).

9.4.6.2 Installing the upgrade kit

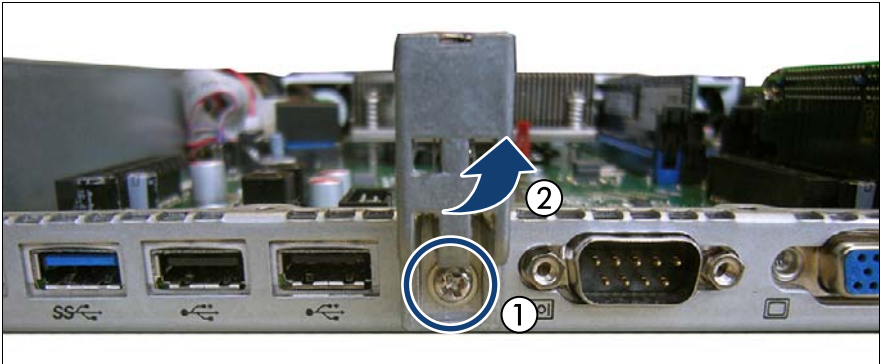


Figure 117: Removing the riser module support

- ▶ Remove the screw (1).
- ▶ Remove the riser module support (2).
- ▶ Remove the riser card from riser module 3 as described in section ["Removing the defective riser card" on page 176](#).

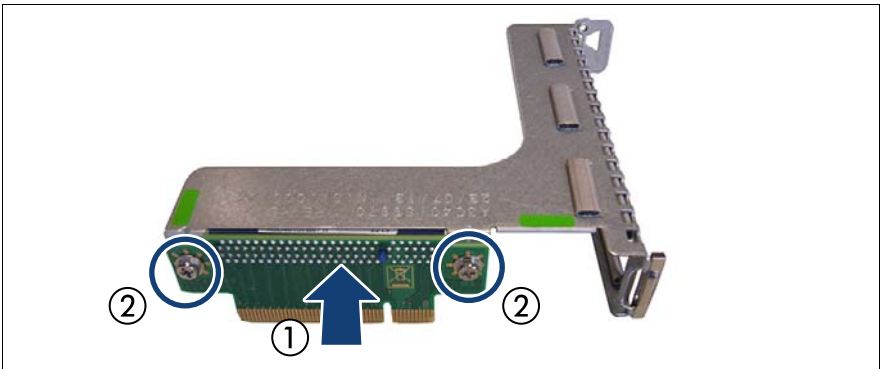


Figure 118: Installing the riser card - example full height riser module

- ▶ Insert the riser card (1).
- ▶ Fasten the riser card with two screws (2).
- ▶ If applicable, install a full height slot bracket to the expansion card as described in section ["Installing a slot bracket" on page 161](#).

Expansion cards and backup units

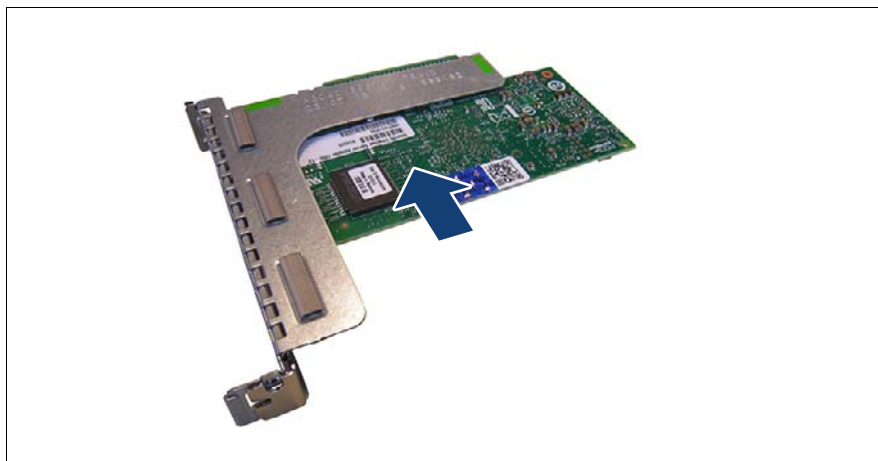


Figure 119: Installing the expansion card - example full height riser module

- ▶ Install the expansion card as described in section ["Installing the expansion card"](#) on page 171.

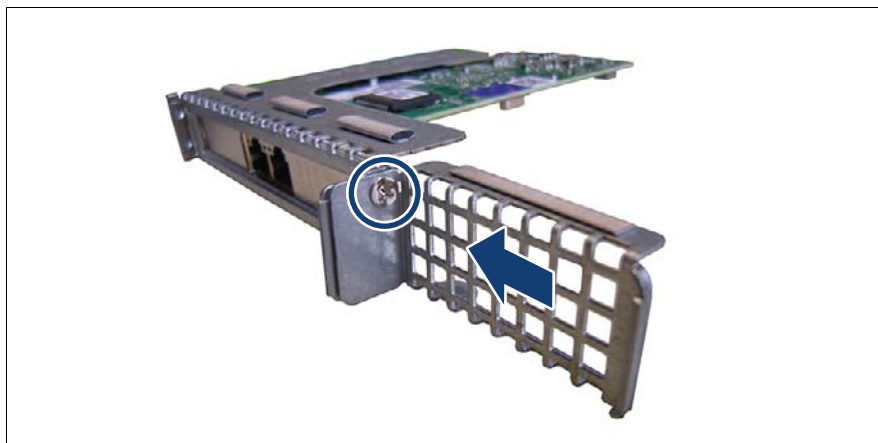


Figure 120: Installing the extension bracket

- ▶ Fasten the extension bracket with one screw to the full height riser module (see circle).

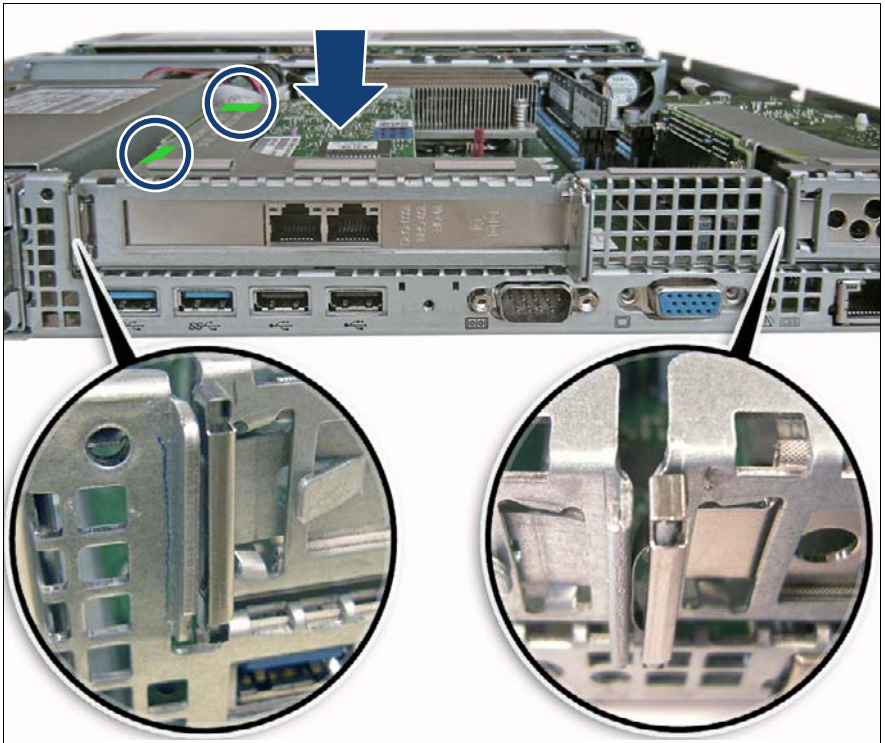


Figure 121: Installing the full height riser module

- ▶ Insert the riser card into the system board slot and press down the green touch points (see circles).



CAUTION!

Make sure that the EMC springs make contact correctly (see close-ups).

9.5 Backup units (BBU/FBU)

The server offers different backup units depending on the used RAID controller:

- BBU (Battery Backup Unit)
- FBU (Flash Backup Unit)

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

9.5.1 Installing a BBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

Tools: tool-less

9.5.1.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.1.2 Preparing the BBU



CAUTION!

Do not connect the cable using excessive force, the connector is weak.

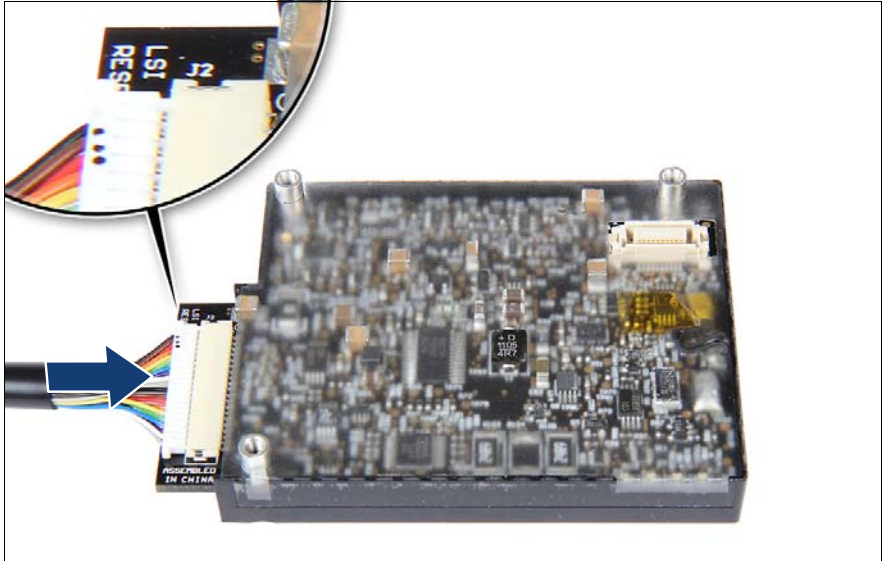


Figure 122: Connecting the BBU cable

- ▶ Connect the BBU cable to the BBU.



CAUTION!

Make sure that the connector side with the three dots is on the top (see close-up). Otherwise you risk short-circuits.

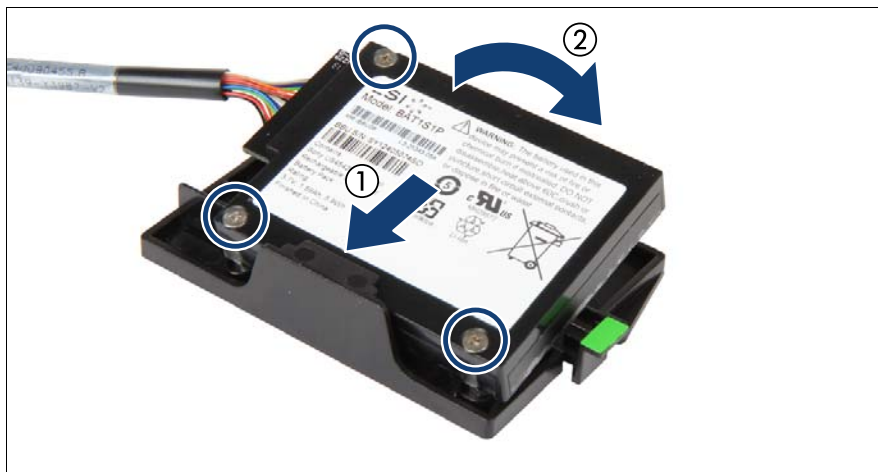


Figure 123: Installing the BBU in the holder

- ▶ At a slight angle, fit the BBU under the right retaining bracket on the holder (1).
- ▶ Fold down the BBU until it locks in place (2).

9.5.1.3 Installing the BBU

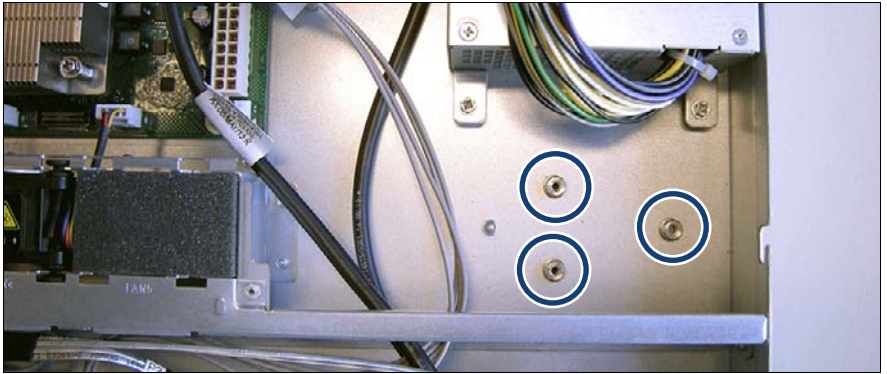


Figure 124: Position of the shoulder screw caps



Figure 125: Installing the BBU with the holder

- ▶ Insert the holder into the chassis so that the three shoulder screw caps on the chassis floor rest in the wide ends of the keyhole slots on the holder.
- ▶ Slide the holder in direction of the arrow.
The shoulder screw caps on the chassis floor will lock in the narrow ends of the keyhole slots on the holder.
- ▶ Ensure that the locking handle on the holder properly snaps in place (see circle).

Expansion cards and backup units

- ▶ Install a RAID controller as described in section "Installing an expansion card" on page 170.

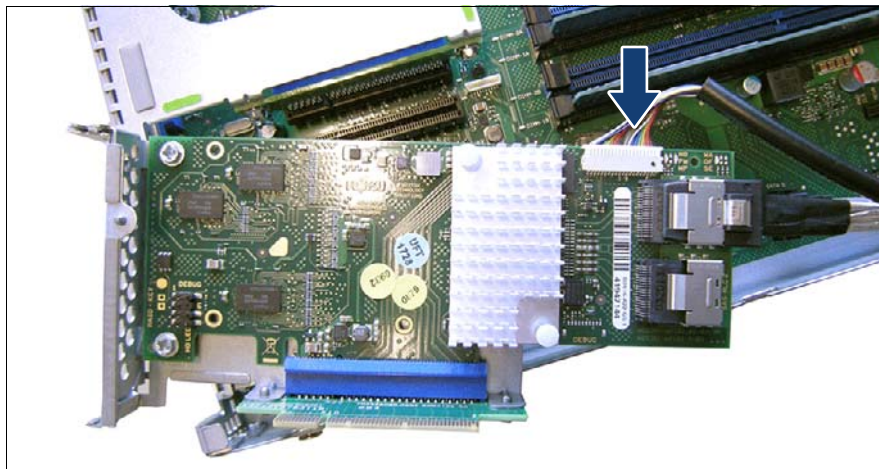


Figure 126: Connecting the BBU cable to the RAID controller

- ▶ Connect the BBU cable to the RAID controller.



CAUTION!

- Make sure that the connector side with the three dots is on the top. Otherwise you risk short-circuits.
- Do not connect the cable using excessive force, the connector is weak.

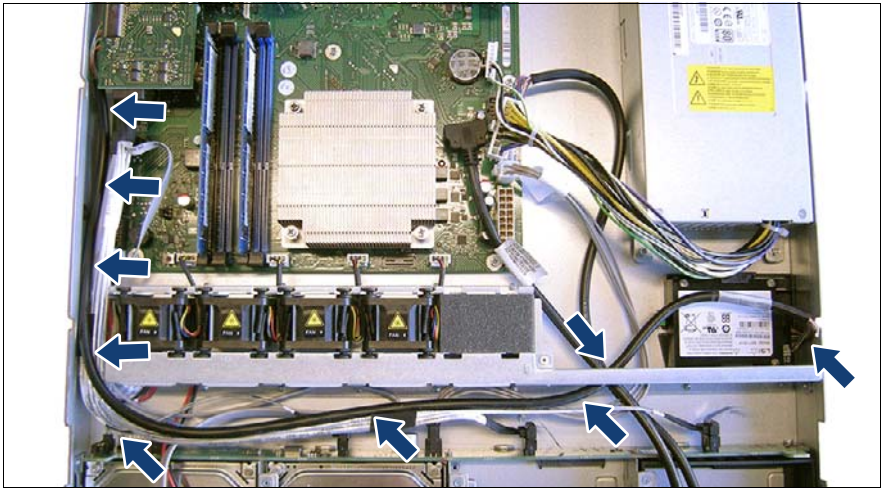


Figure 127: Routing the BBU cable

- ▶ Route the BBU cable as shown in the figure.

9.5.1.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating RAID controller firmware" on page 74](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)

Note on BBU charging and calibration

The BBU may be deeply discharged due to extended storage time and wrongly show as bad or defective in the ServerView RAID Manager. In this case, the BBU will automatically enter a trickle charge cycle for recovery. This initial charge may take up to 12 hours before the BBU will initiate a recalibration cycle.

- ▶ Enter the ServerView RAID Manager and check the current BBU status.



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

Expansion cards and backup units

- ▶ If the BBU is shown as bad or defective, do not power off the server for at least 12 hours to allow the charge and calibration cycles to finish.
- ▶ If the BBU status does not change after 12 hours, please try to initiate the recalibration process manually using the ServerView RAID Manager.



If this procedure still does not fix the BBU status, please contact your local Fujitsu customer service partner.

9.5.2 Installing an FBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

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

9.5.2.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.2.2 Preparing the FBU

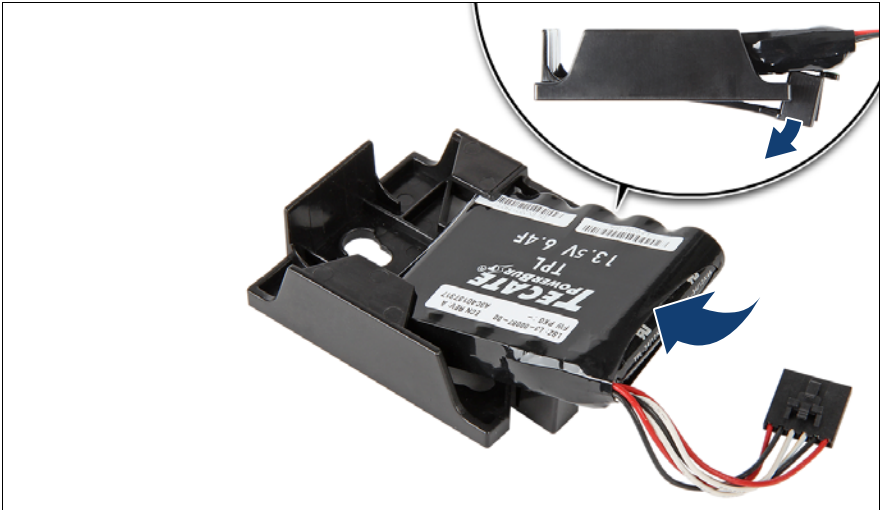


Figure 128: Installing the FBU in the holder (A)

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

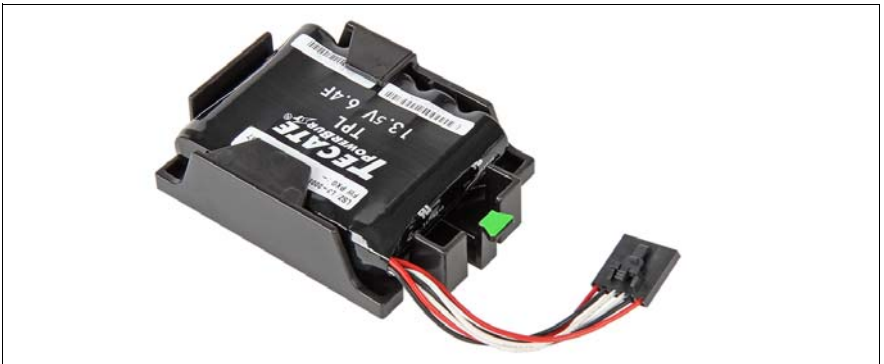


Figure 129: Installing the FBU in the holder (B)

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

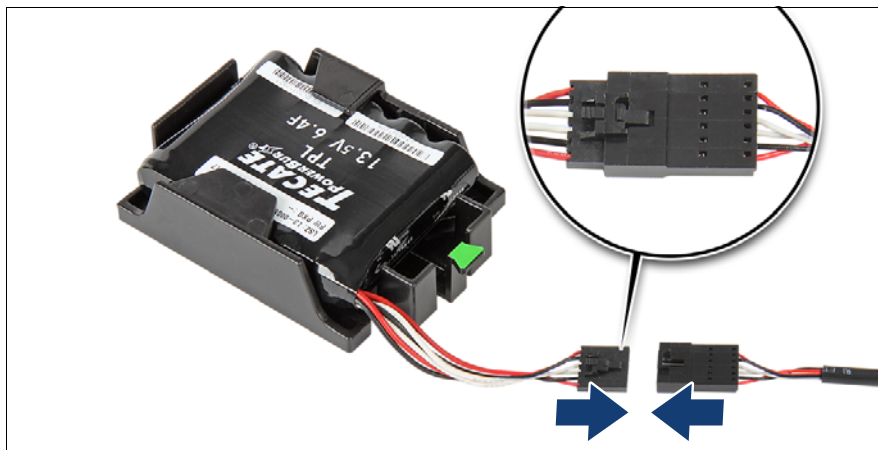


Figure 130: Connecting the FBU adapter cable to the FBU

- ▶ Connect the cable end on the FBU to the FBU adapter cable as shown.

9.5.2.3 Installing the FBU

- ▶ Install the FBU with the holder as described in section "[Installing the BBU](#)" on page 189.
- ▶ If applicable, install the TFM as described in section "[Installing the new TFM](#)" on page 180.
- ▶ Connect the FBU adapter cable to the TFM as described in section "[Installing the new TFM](#)" on page 180.
- ▶ Install the RAID controller with the TFM as described in section "[Installing an expansion card](#)" on page 170.

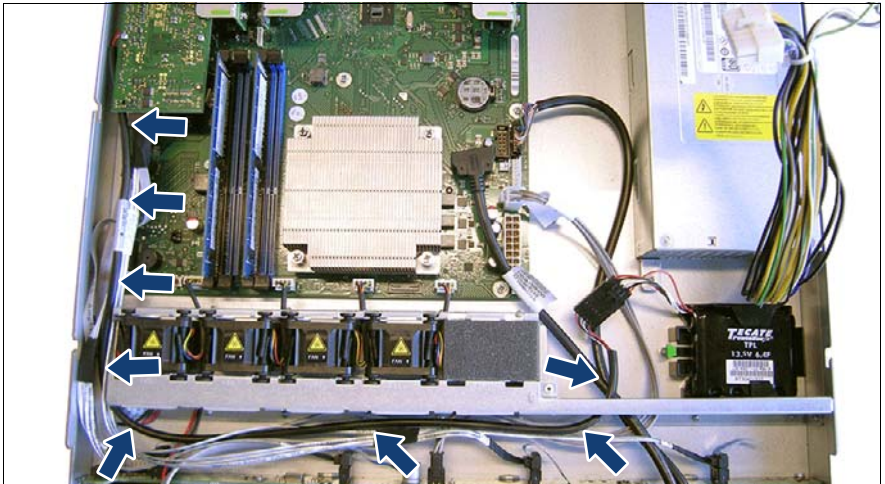


Figure 131: Routing the FBU cable

- ▶ Route the FBU cable as shown in the figure.

9.5.2.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating RAID controller firmware" on page 74](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)

9.5.3 Removing a BBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

Tools: tool-less

9.5.3.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.3.2 Removing the BBU with the holder



Figure 132: Removing the BBU with the holder

- ▶ Lift up the green locking handle on the holder (see circle) while sliding the holder in direction of the arrow as far as it will go.



After that, the shoulder screw caps on the chassis floor will rest in the wide ends of the keyhole slots on the holder.

- ▶ Lift the holder out of the chassis.

9.5.3.3 Removing the BBU from the holder

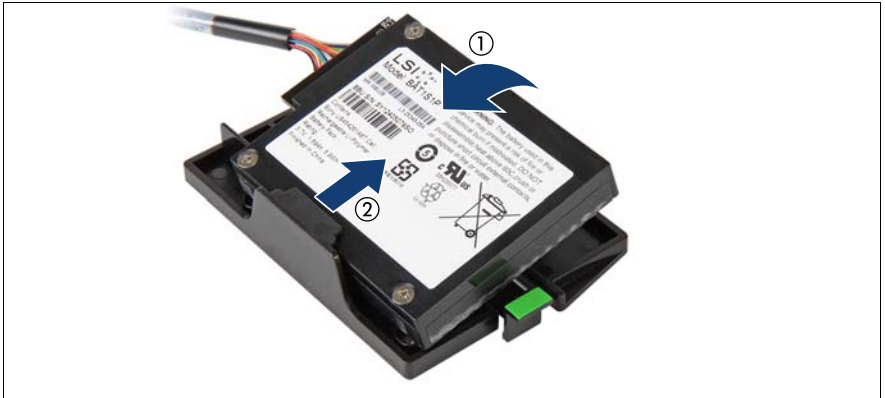


Figure 133: Removing the BBU from the holder

- ▶ Fold up the BBU (1) and at a slight angle remove it from the holder (2).

9.5.3.4 Disconnecting the BBU cable from the BBU

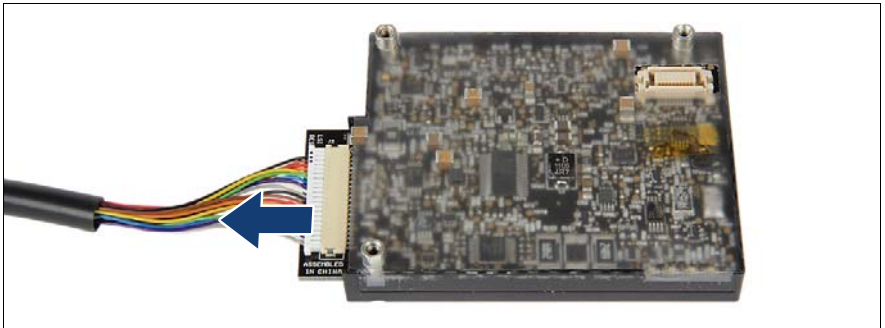


Figure 134: Disconnecting the BBU cable from the BBU

- ▶ Disconnect the BBU cable from the BBU.

9.5.3.5 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

9.5.4 Removing an FBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

Tools: tool-less



CAUTION!

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

9.5.4.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.4.2 Removing the FBU with the holder

- ▶ Remove the FBU with the holder as described in section ["Removing the BBU with the holder" on page 196](#).

9.5.4.3 Disconnecting the FBU cable from the FBU

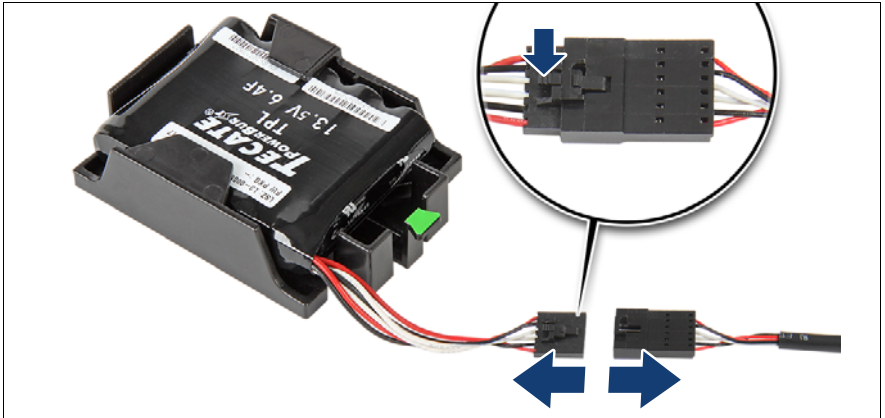


Figure 135: Disconnecting the FBU cable from the FBU

- ▶ Disconnect the FBU cable from the FBU.

9.5.4.4 Removing the FBU from the holder

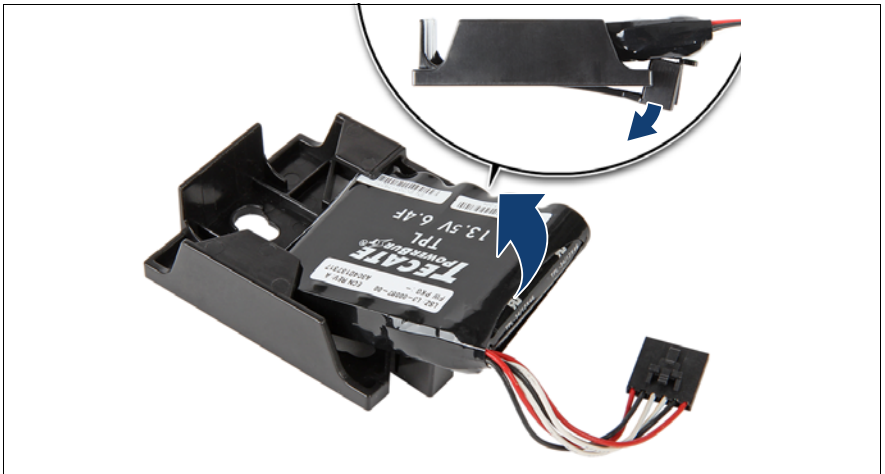


Figure 136: Removing the FBU from the holder

- ▶ Pull the FBU at a slight angle out of the holder.

9.5.4.5 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

9.5.5 Replacing a BBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

Tools: tool-less



CAUTION!

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

9.5.5.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.5.2 Removing the defective BBU

- ▶ Remove the BBU with the holder as described in section ["Removing the BBU with the holder" on page 196](#).
- ▶ Remove the BBU from the holder as described in section ["Removing the BBU from the holder" on page 197](#).
- ▶ Disconnect the BBU cable from the BBU as described in section ["Disconnecting the BBU cable from the BBU" on page 197](#).

9.5.5.3 Installing the new BBU

- ▶ Connect the BBU cable to the BBU and install the BBU in the holder as described in section "[Preparing the BBU](#)" on page 187.
- ▶ Install the BBU with the holder as described in section "[Installing the BBU](#)" on page 189.

9.5.5.4 Concluding steps

- ▶ "[Reassembling](#)" on page 52
- ▶ "[Connecting the server to the mains](#)" on page 55
- ▶ "[Updating RAID controller firmware](#)" on page 74
- ▶ "[Enabling SVOM boot watchdog functionality](#)" on page 78
- ▶ "[Switching on the server](#)" on page 57

Note on BBU charging and calibration

The BBU may be deeply discharged due to extended storage time and wrongly show as bad or defective in the ServerView RAID Manager.

In this case, the BBU will automatically enter a trickle charge cycle for recovery. This initial charge may take up to 12 hours before the BBU will initiate a recalibration cycle.

- ▶ Enter the ServerView RAID Manager and check the current BBU status.



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

- ▶ If the BBU is shown as bad or defective, do not power off the server for at least 12 hours to allow the charge and calibration cycles to finish.
- ▶ If the BBU status does not change after 12 hours, please try to initiate the recalibration process manually using the ServerView RAID Manager.



If this procedure still does not fix the BBU status, please contact your local Fujitsu customer service partner.

9.5.6 Replacing an FBU



Upgrade and Repair Unit (URU)



Hardware: 15 minutes

Tools: tool-less



CAUTION!

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

9.5.6.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

9.5.6.2 Removing the defective FBU

- ▶ Remove the FBU with the holder as described in section ["Removing the FBU with the holder" on page 198](#).
- ▶ Disconnect the FBU cable from the FBU as described in section ["Disconnecting the FBU cable from the FBU" on page 199](#).
- ▶ Remove the FBU from the holder as described in section ["Removing the FBU from the holder" on page 199](#).

9.5.6.3 Installing the new FBU

- ▶ Install the FBU in the holder and connect the FBU adapter cable to the FBU as described in section ["Preparing the FBU" on page 193](#).
- ▶ Install the FBU with the holder as described in section ["Installing the FBU" on page 194](#).

9.5.6.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating RAID controller firmware" on page 74](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)

10 Main memory

Safety notes



CAUTION!

- Do not install unsupported third party memory modules. For further information on supported memory modules, refer to section "[Types of memory modules](#)" on page 206. Doing so may cause electric shock, a fire, or failures.
- 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.
- If the memory module has not been correctly inserted, it may cause a fire. Insert the memory module with attention to its direction.
- 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 safety information, please refer to chapter "[Important information](#)" on page 31.

10.1 Basic information

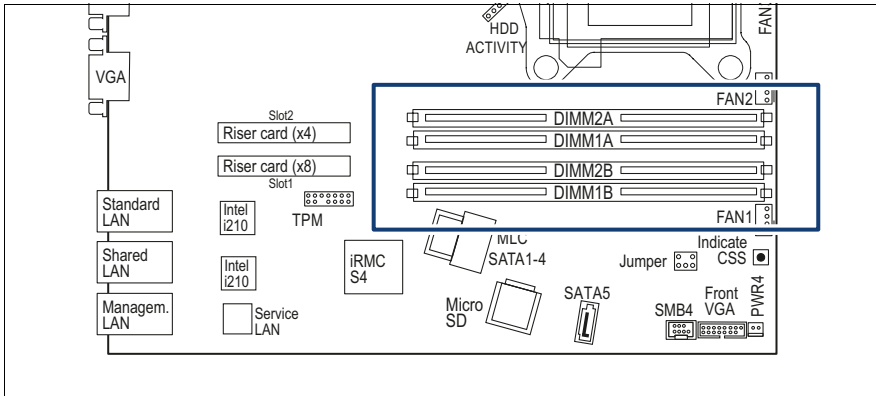


Figure 137: Slots of the main memory

The system board offers four slots for memory modules.

Types of memory modules

Technology: DDR3 1600 unbuffered single rank (SR) or dual rank (DR) UDIMM memory modules with ECC. Support for up to 4 UDIMM memory modules.

Total memory size: up to 32 GB

Configuration per channel	Max. speed	DIMM-2	DIMM-1
1	DDR3-1600	empty	SR/DR
2	DDR3-1600	SR/DR	SR/DR



For system relevant information, refer to your server's hardware configurator available online at the following address:

for the EMEA market:

http://ts.fujitsu.com/products/standard_servers/index.htm

for the Japanese market:

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

10.1.1 Memory sequence

10.1.1.1 Population rules

- Populate memory slot 1 / channel A (DIMM 1A) first.
- Within all channels memory slot 1 must be populated prior to slot 2.
- Install memory modules within a channel in descending order of capacity: higher capacity in slot 1, lower capacity in slot 2.

Channel		A		B	
Slot ID		2A	1A	2B	1B
DIMM #	1		(1)		
	2		(1)		(2)
	3	(3)	(1)		(2)
	4	(3)	(1)	(4)	(2)

Table 4: Mounting order

10.1.1.2 Modes of operation

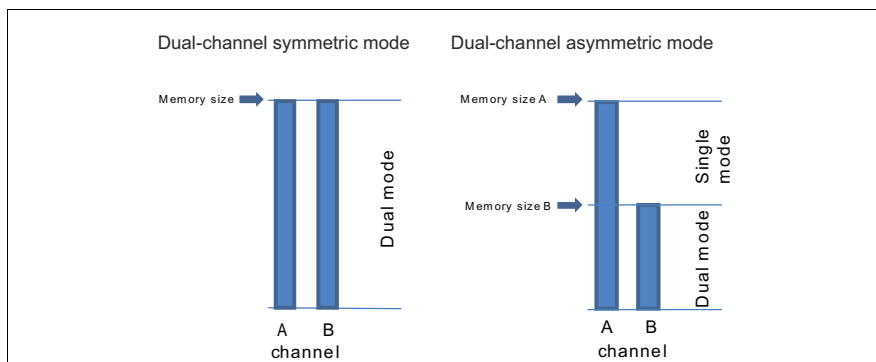


Figure 138: Dual-channel symmetric and asymmetric mode

- The maximum performance can be achieved in a symmetric dual-channel configuration. Therefore both channels have to be populated with the same amount of memory. The DRAM device technology (1Gbit / 2Gbit / 4Gbit) may vary from one channel to the other.
- If the amount of memory differs between the two channels, the system board will run in dual-channel asymmetric mode.
- Regardless of the mode, all DIMMs will run at the highest common frequency that is allowed by the SPD Data of the DIMMs and the max. speed of the selected configuration.
- Single-channel mode is used when 1 memory module is populated in DIMM 1A.

10.2 Installing a memory module



Upgrade and Repair Unit
(URU)



Hardware: 5 minutes

Tools: tool-less

10.2.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

10.2.2 Selecting the memory slot

- ▶ Choose the memory slot according to the configuration rules in ["Basic information" on page 206](#).

10.2.3 Installing a memory module

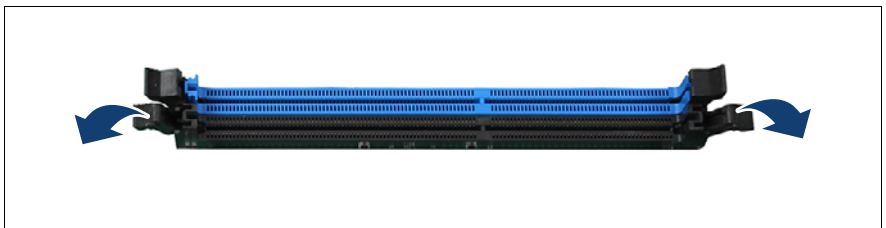


Figure 139: Opening the securing clips

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

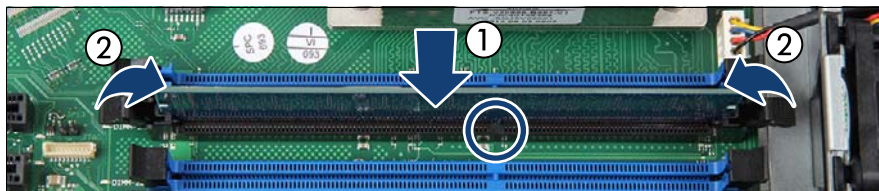


Figure 140: Installing a memory module

- ▶ Carefully press the memory module into the memory slot (1) until the securing clips on both sides of it engage (2). Notice the coding (see circle).

10.2.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating or recovering the system board BIOS and iRMC" on page 71](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

10.3 Removing a memory module



**Upgrade and Repair Unit
(URU)**



Hardware: 5 minutes

Tools: tool-less

10.3.1 Preliminary steps

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

10.3.2 Removing a memory module

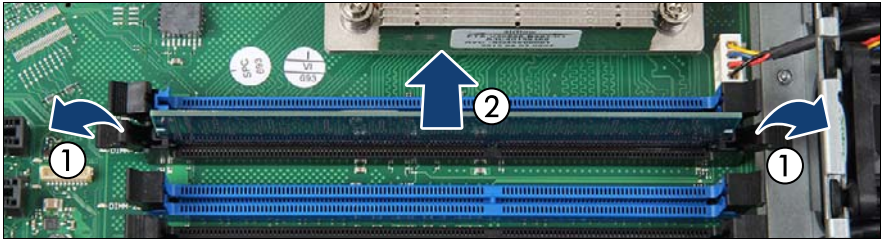


Figure 141: Removing the memory module

- ▶ Press the securing clips on both sides of the memory slot concerned outward (1).
- ▶ Pull the memory module out of the slot (2).

10.3.3 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

10.4 Replacing a memory module



**Upgrade and Repair Unit
(URU)**



Hardware: 5 minutes

Tools: tool-less

10.4.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)

10.4.2 Removing the defective memory module

- ▶ Remove the memory module as described in section ["Removing a memory module" on page 211](#).

10.4.3 Installing the new memory module

- ▶ Install the memory module as described in section ["Installing a memory module" on page 209](#).

10.4.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Updating or recovering the system board BIOS and iRMC" on page 71](#)
- ▶ ["Enabling replaced components in the system BIOS" on page 79](#)
- ▶ ["Verifying the memory mode" on page 80](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

11 Processor

Safety notes



CAUTION!

- Do not install unsupported processors. For further information on supported processors, refer to section "[Supported processors](#)" on [page 214](#).
- 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 safety information, please refer to chapter "[Important information](#)" on [page 31](#).

11.1 Basic information

11.1.1 Supported processors

- one Intel® Quad-Core Xeon E3-12xxv3 or one Dual Core i3-4xxx or one Dual Core Pentium G3xxx processor
- one processor socket LGA 1150



For system relevant information, refer to your server's hardware configurator available online at the following address:

for the EMEA market:

http://ts.fujitsu.com/products/standard_servers/index.htm

for the Japanese market:

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

11.2 Replacing the processor



Field Replaceable Unit (FRU)



**Hardware: 15 minutes
Software: 5 minutes**

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



CAUTION!

Processors are modules which are extremely sensitive to electrostatic discharges and therefore must always be handled with care. After a processor has been removed from its protective sleeve or from its socket, place it with its smooth side down on a non-conducting, antistatic surface. Never push a processor over a surface.

11.2.1 Preliminary steps

- ▶ "Locating the defective server" on page 43
- ▶ "Disabling SVOM boot watchdog functionality" on page 64
- ▶ "Suspending BitLocker functionality" on page 63
- ▶ "Shutting down the server" on page 45
- ▶ "Disconnecting the server from the mains" on page 46
- ▶ "Getting access to the component" on page 47
- ▶ "Removing a riser module" on page 58

11.2.2 Removing the heat sink

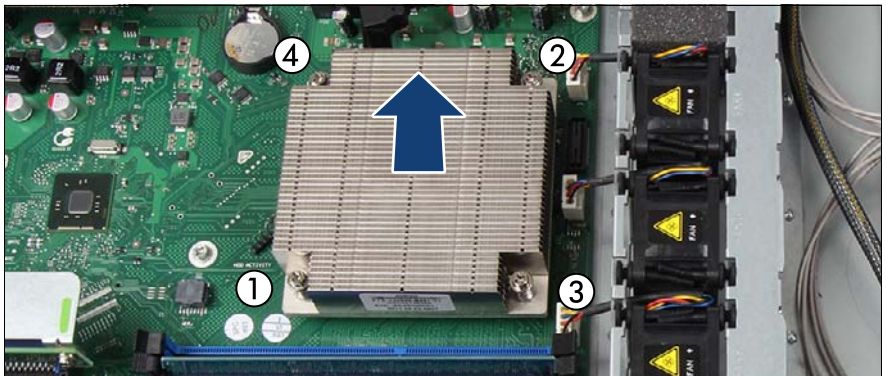


Figure 142: Removing the heat sink

- ▶ Loosen the four screws of the heat sink in a crossover pattern according to the numbering.
- ▶ Carefully turn the heat sink back and forth to detach it from the processor.



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



CAUTION!

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

- ▶ Lift the heat sink out of the chassis.

Processor

- ▶ Remove the residual thermal paste from the underside of the heat sink and the surface of the processor.
- ▶ Clean the underside of the heat sink and the surface of the processor using a lint-free cloth.

11.2.3 Removing the defective processor



Figure 143: Opening the lever

- ▶ Press down the lever (1) and unhook it.
- ▶ Open the lever (2).



Figure 144: Opening the holder

- ▶ Take the holder by the small grip (1) and open it (2).



Figure 145: Removing the processor

- ▶ Lift the processor carefully out of the processor socket.



CAUTION!

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

11.2.4 Installing the new processor

- ▶ Remove the protective cap from the bottom side of the processor.

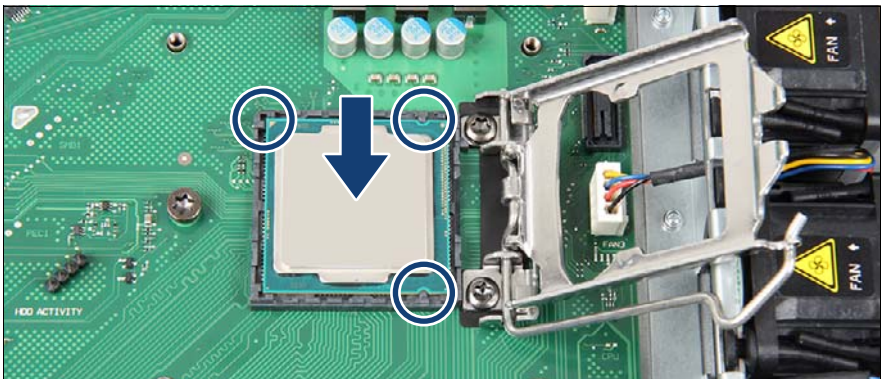


Figure 146: Installing the processor

- ▶ Insert the new processor carefully into the processor socket. Notice the coding (see circles).



CAUTION!

To avoid damaging the pins or the processor, do not force it into the processor socket.

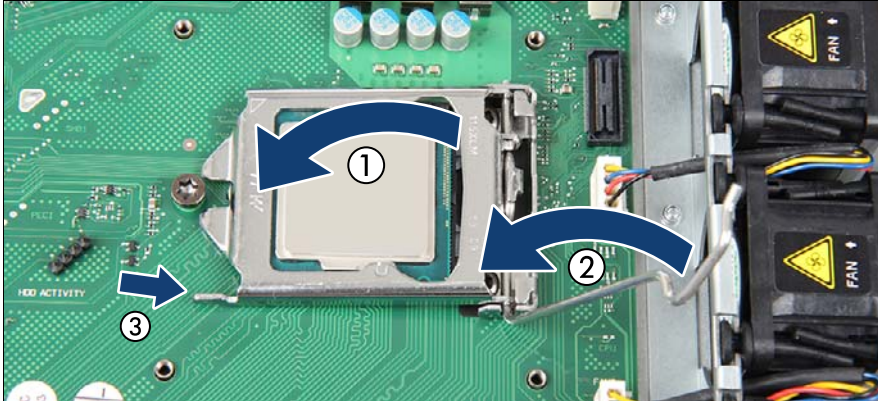


Figure 147: Closing the holder

- ▶ Close the holder (1).



CAUTION!

The holder must fall down by itself. Do not close with force, because soldering pads may be damaged.

- ▶ Press the lever slowly downward (2) until it is hooked in again (3).

11.2.5 Applying the thermal paste to the processor surface



- For the Japanese market, the service engineer must follow the instruction provided separately.
- If the processor replacement kit contains a new heat sink, a thin layer of thermal compound has already been pre-applied to its lower surface. In this case, please proceed with section "[Installing the heat sink](#)" on page 220.

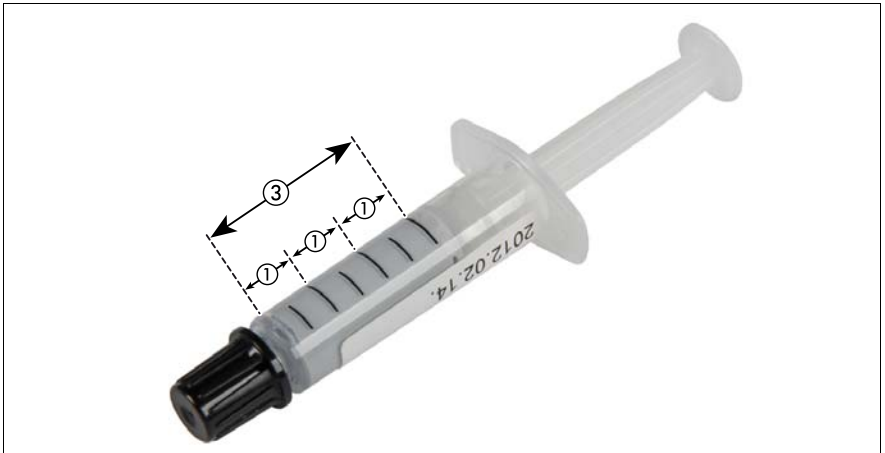


Figure 148: Thermal paste syringe

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



Figure 149: Applying the thermal paste

- ▶ Apply a small point-shaped amount 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.

11.2.6 Installing the heat sink

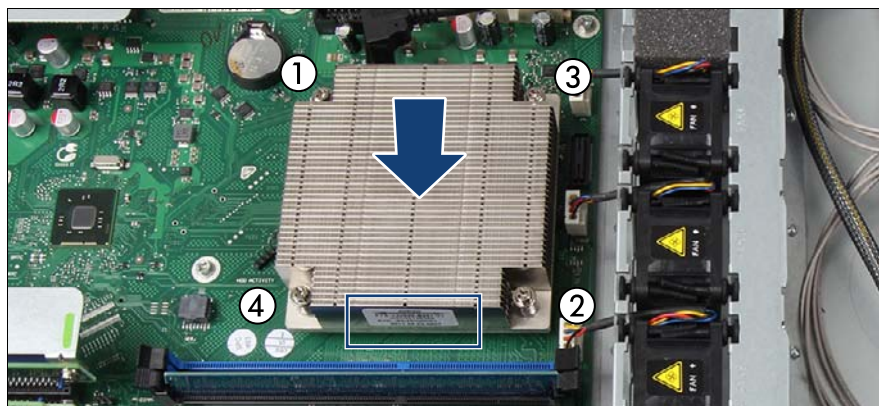


Figure 150: Installing the heat sink

- ▶ Align the heat sink and fit it on the processor socket.
- ▶ Position the screws in the holes carefully, making sure they are upright.
- ▶ Fasten it in a crossover pattern with four screws according to the numbering (torque 6.0 Nm, the description of this torque value doesn't apply to the Japanese market). Notice the position of the air flow label.

11.2.7 Concluding steps

- ▶ ["Installing a riser module" on page 60](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)

i If the Global Error LED is flashing with the error message "CPU has been changed" on the display after the system is powered on, please follow the steps below.

- ▶ Restart the system and wait until the screen output appears.
- ▶ Press **F2**.
- ▶ If a password is assigned, enter this password and confirm with **Enter**.
The BIOS setup main menu will be displayed on the screen.

- ▶ Select "Save Changes and Exit" or "Save Changes and Reset" on the Save & Exit menu.
- ▶ Confirm that the Global Error LED is off.

This is only information regarding to the change of the CPU configuration. There is no technical problem.

- ▶ ["Updating or recovering the system board BIOS and iRMC" on page 71](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

11.3 Replacing the heat sink



Field Replaceable Unit (FRU)



Hardware: 15 minutes

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

11.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Removing a riser module" on page 58](#)

11.3.2 Removing the defective heat sink

- ▶ Remove the heat sink as described in section ["Removing the heat sink" on page 215](#).
- ▶ Remove the residual thermal paste from the processor surface.
- ▶ Clean the processor surface using a lint-free cloth.

11.3.3 Installing the new heat sink

- ▶ Remove the protective cover on the underside of the heat sink.



CAUTION!

Do not touch the thermal paste on the underside of the heat sink.

- ▶ Install the heat sink as described in section ["Installing the heat sink" on page 220](#).

11.3.4 Concluding steps

- ▶ ["Installing a riser module" on page 60](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

12 Optical disk drive

Safety notes



CAUTION!

- Before installing/removing an accessible drive to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cables from the outlet. Failure to do so can cause electric shock.
- When installing an accessible drive, hold it by the side. Applying force to the top may cause failures.
- Do not touch the circuitry on boards and soldered parts. Hold the metallic areas or the edge of the circuit boards.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Before handling them, first touch a metal part on the server to discharge static electricity from your body.
- Before installing an internal accessible drive, see the manual for the accessible drive.
- When forcing an accessible drive into a server, be careful so as not to pinch the cable etc. connected to an accessible drive.
- For further safety information, please refer to chapter "[Important information](#)" on page 31.

12.1 Basic information

You can install one 5.25-inch slimline optical disk drive (ODD). The installation bay depends on the 2.5-inch or 3.5-inch HDD configuration.

The proceeding for installing/removing is identic except the routing of the cables and the depending ODD power connector on the system board (see section ["Onboard connectors" on page 300](#)).

3.5-inch HDD configuration



Figure 151: Position of the ODD bay - example 3.5-inch HDD configuration

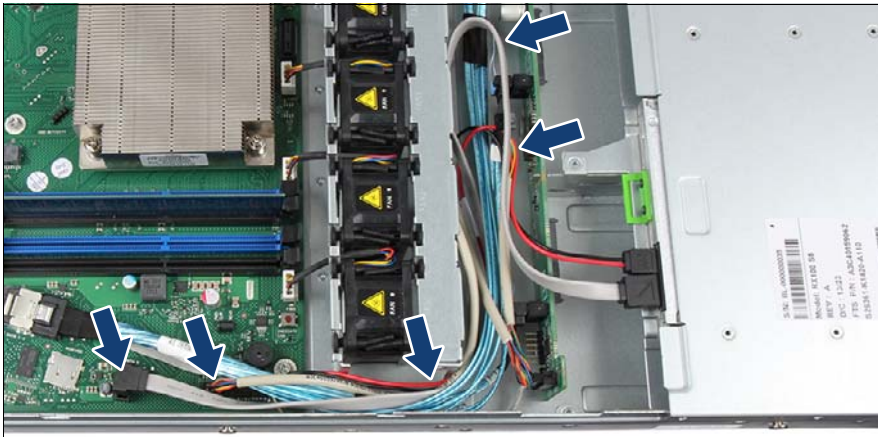


Figure 152: Routing ODD cables - example 3.5-inch HDD configuration

2.5-inch HDD configuration



Figure 153: Position of the ODD bay - example 2.5-inch HDD configuration

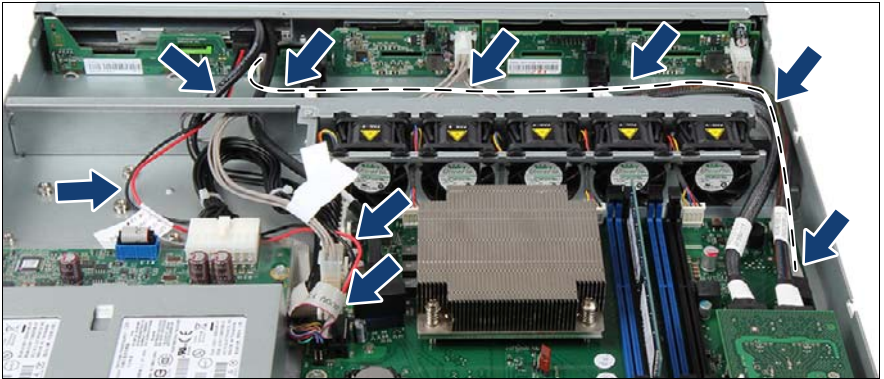


Figure 154: Routing ODD cables - example 2.5-inch HDD configuration

Storing the ODD latch

Depending on chassis variants the ODD latch can be stored in different ways:

- ODD latch and two screws in a package
- fastened with two screws to the chassis of the fan bridge

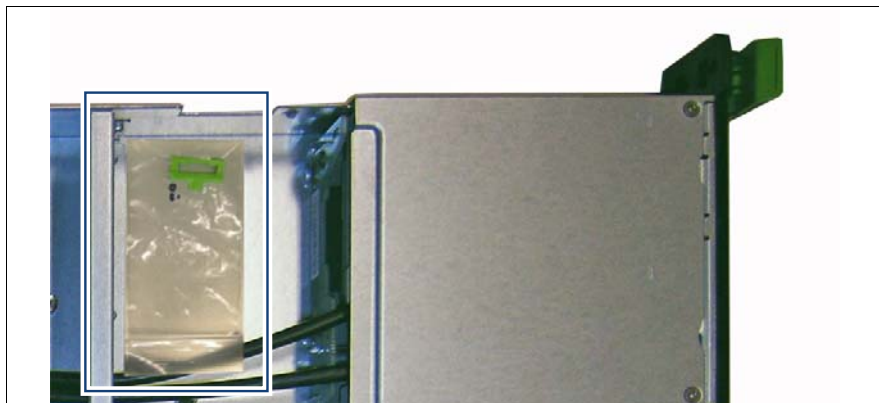


Figure 155: Example ODD latch in a package

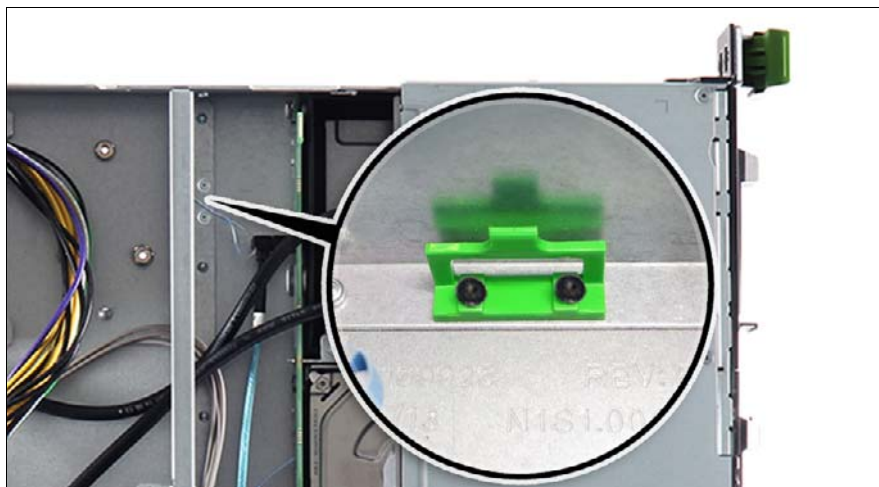


Figure 156: Example ODD latch on fan bridge

12.2 Installing the ODD



Upgrade and Repair Unit
(URU)



Hardware: 5 minutes

Tools: Torx Plus 6 screw driver

12.2.1 Preliminary steps

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

12.2.2 Removing the dummy cover



Figure 157: Removing the dummy cover

- ▶ Pull the dummy cover out of the bay.



CAUTION!

Keep the dummy cover for future use. If you remove the accessible drive again and do not replace it with a new one, the dummy cover must be reinstalled to comply with EMC regulations and to satisfy cooling requirements and fire protection measures.

12.2.3 Installing the ODD

- ▶ If no ODD has been installed before:
 - ▶ Remove the ODD latch from its package (see figure 155) or
 - ▶ Remove the two screws and take the ODD latch from the fan bridge (see figure 156).



Figure 158: Installing the ODD latch on the ODD

- ▶ Fasten the ODD latch with two screws to the rear side of the ODD.



Figure 159: Installing the ODD

- ▶ Push the ODD into the bay (1) simultaneously pressing the front of the ODD slightly down until the ODD latch engages (2).

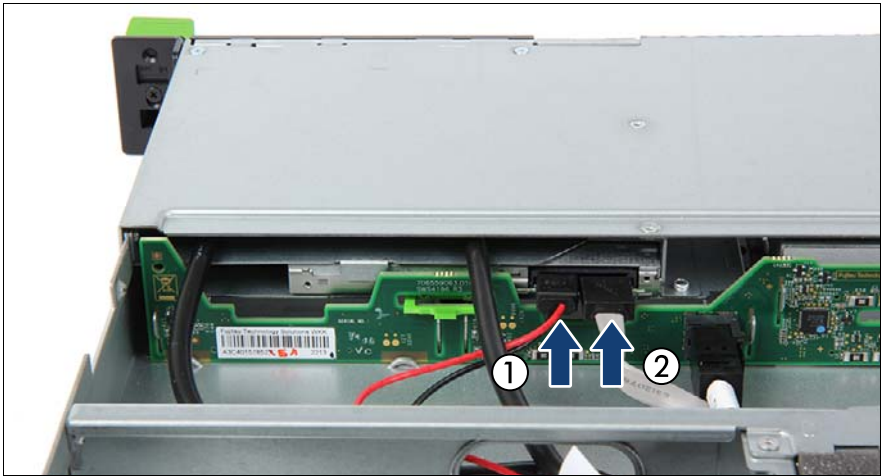


Figure 160: Connecting the cables to the ODD

- ▶ Connect the ODD power cable (1) to the ODD.
- ▶ Connect the SATA cable (2) to the ODD.



The ODD power cable and the SATA cable are preinstalled.

12.2.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

12.3 Removing the ODD



Field Replaceable Unit
(FRU)



Hardware: 5 minutes

Tools: Torx Plus 6 screw driver

12.3.1 Preliminary steps

- ▶ ["Removing backup and optical disk media" on page 66](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

12.3.2 Removing the ODD

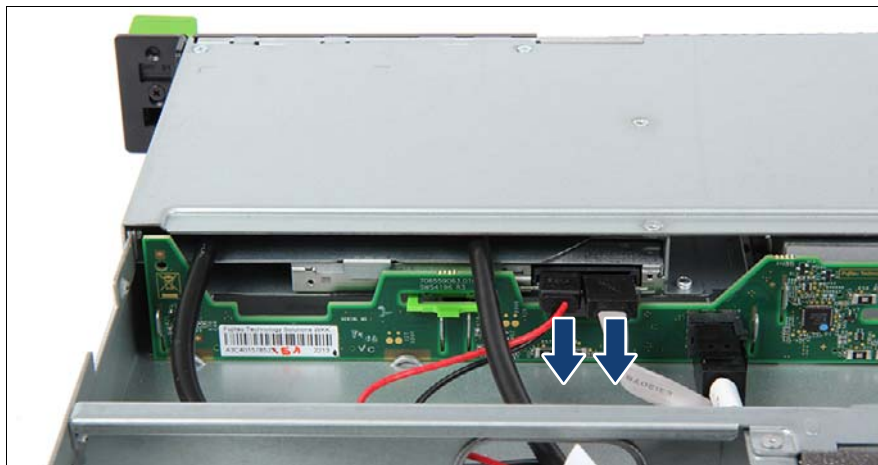


Figure 161: Disconnecting the cables from the ODD

- ▶ Disconnect the ODD power cable and the SATA cable from the ODD.



Figure 162: Removing the ODD

- ▶ Press the ODD latch in direction of the arrow until it disengages (1).
- ▶ Pull the ODD out of the bay (2).



Figure 163: Removing the ODD latch from the ODD

- ▶ Remove the two screws (see circles).
- ▶ Remove the ODD latch.
- ▶ If no new ODD will be installed:
 - ▶ Store the ODD latch in a package (see figure 155) or
 - ▶ Fasten the ODD latch with two screws to the fan bridge (see figure 156).

12.3.3 Installing the dummy cover



Figure 164: Installing the dummy cover

- ▶ Push the dummy cover inward until it engages at the right side.

12.3.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)
- ▶ ["Verifying and configuring the backup software solution" on page 76](#)

12.4 Replacing the ODD



Field Replaceable Unit (FRU)



Hardware: 5 minutes

Tools: Torx Plus 6 screw driver

12.4.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Removing backup and optical disk media" on page 66](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

12.4.2 Removing the defective ODD

- ▶ Remove the ODD as described in section ["Removing the ODD" on page 230](#).

12.4.3 Installing the new ODD

- ▶ Install the ODD as described in section ["Installing the ODD" on page 228](#).

12.4.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

13 Front panel

Safety notes



CAUTION!

- When inserting the front panel into the server, ensure not to pinch or strain any connected cables.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs)
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "[Important information](#)" on page 31.

13.1 Basic information

The server's chassis ID is stored on both the front panel and the system board. After replacing the front panel, it is necessary to program the ChassisID prom of the front panel.

Beside the CPU temperature sensor and housing temperature sensor provided on the system board, an ambient temperature sensor is also included on the front panel. In case of a defective ambient temperature sensor, please replace the front panel.

Front panel module

The front panel module consists of a holder and a front panel board. These components are already pre-assembled. The USB connector of the front USB cable must be installed in the dependant recesses of the holder. As an option the holder can be equipped with a front VGA connector.

Front panel on QRL (10 x 2.5-inch HDD configuration)

The front panel on QRL (Quick Release Lever) is only available for the servers with a 10 x 2.5-inch HDD configuration. The front panel is mounted on the right side ear. A flat cable is used for connection to the system board.

13.2 Front panel module

13.2.1 Replacing the front panel module



Field Replaceable Unit (FRU)



Hardware: 10 minutes
Software: 5 minutes

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

Note on system information backup / restore



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

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



CAUTION!

For that reason the front panel and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

13.2.1.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)

13.2.1.2 Removing the front panel module

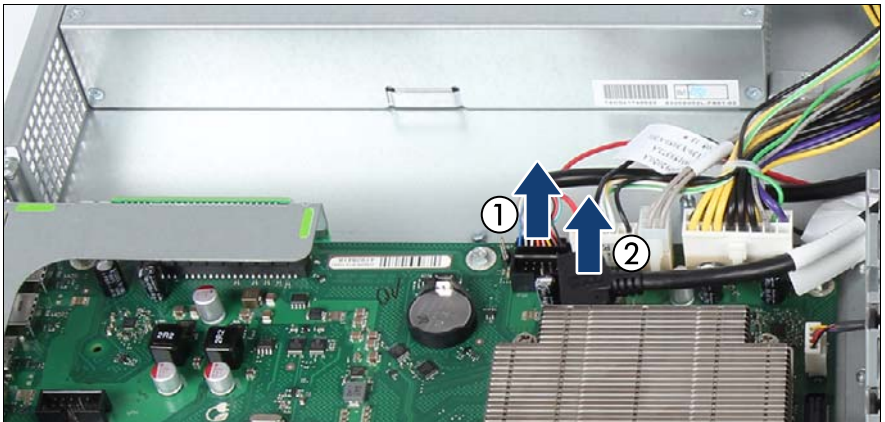


Figure 165: Disconnecting the cables (A)

- ▶ Disconnect the front panel cable (1) and the front USB cable (2) from the system board.

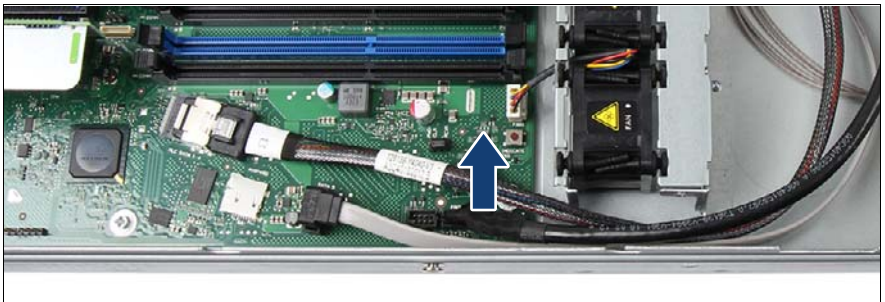


Figure 166: Disconnecting the cables (B)

- ▶ If applicable, disconnect the front VGA cable from the system board.

Front panel

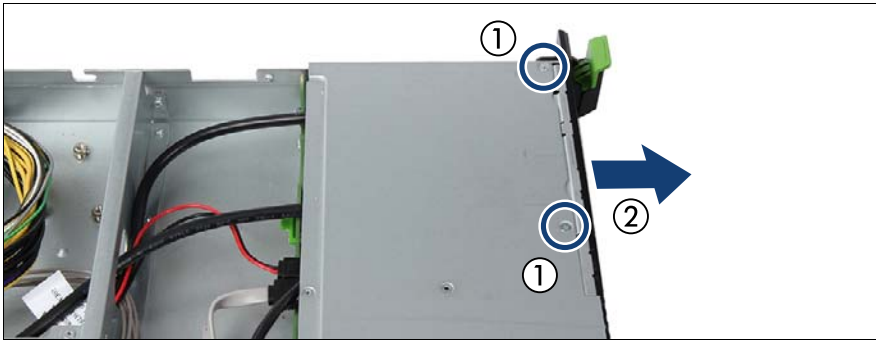


Figure 167: Removing the front panel module

- ▶ Remove the two screws (1).
- ▶ Pull the front panel module out of its bay (2) until the holder is completely accessible.

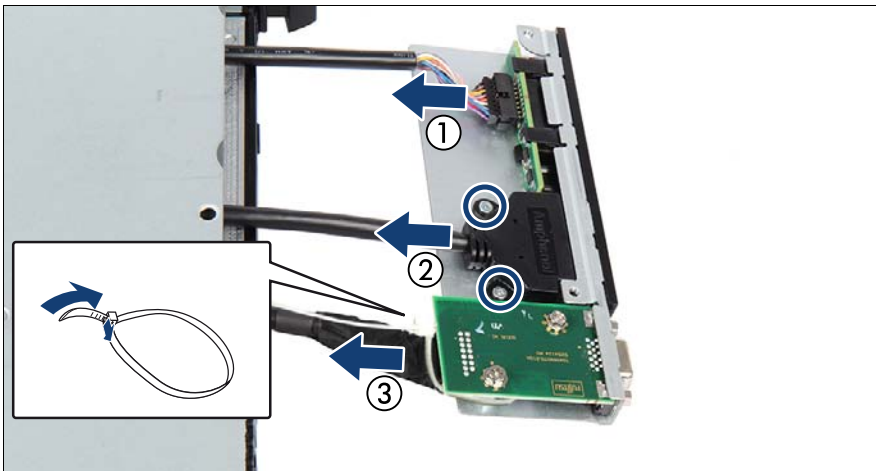


Figure 168: Removing cables from the front panel module

- ▶ Disconnect the front panel cable (1).
- ▶ Remove the two corresponding screws and disconnect the front USB cable (2).
- ▶ If applicable, disconnect the front VGA cable (3).



If the VGA cable is secured with a cable tie, open the cable tie. Please do not cut the cable tie.

- ▶ If applicable, remove the front VGA board with the front VGA connector as described in section "Removing the front VGA board" on page 244.

13.2.1.3 Installing the front panel module

- ▶ If applicable, install the front VGA board with the front VGA connector as described in section "Installing the front VGA board" on page 242.

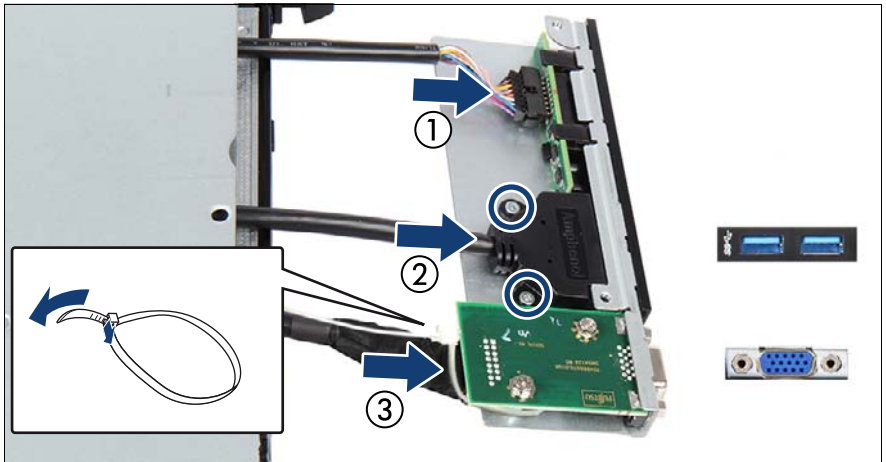


Figure 169: Connecting cables to the front panel module

- ▶ Connect the front panel cable (1).
- ▶ Push the front USB connector in the corresponding recess and fasten the front USB cable with two screws (2).
- ▶ If applicable, connect the front VGA cable to the front VGA board (3).



If the VGA cable was secured with a cable tie, secure the VGA cable with the cable tie.

Front panel

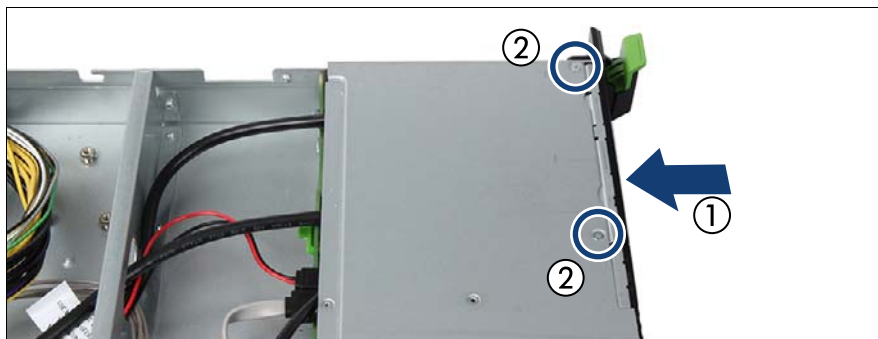


Figure 170: Installing the front panel module

- ▶ Push the front panel module in its bay (1).
- ▶ Fasten the front panel module with two screws (2).

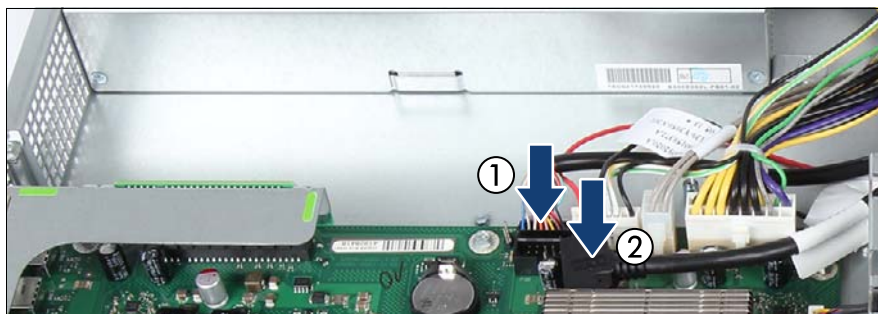


Figure 171: Connecting the cables (A)

- ▶ Connect the front panel cable (1) and the front USB cable (2) to the system board.

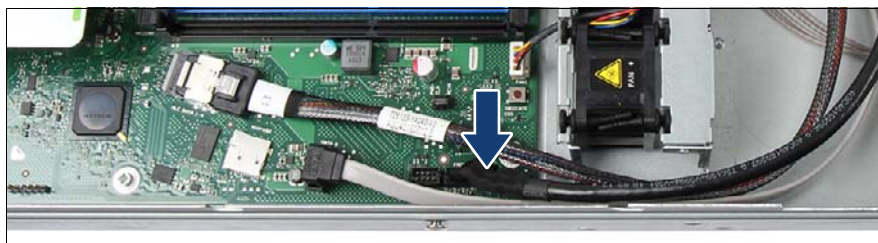


Figure 172: Connecting the cables (B)

- ▶ If applicable, connect the front VGA cable to the system board.

13.2.1.4 Concluding steps

- ▶ "Reassembling" on page 52
- ▶ "Connecting the server to the mains" on page 55
- ▶ "Enabling SVOM boot watchdog functionality" on page 78
- ▶ "Using the Chassis ID Prom Tool" on page 87
- ▶ "Switching on the server" on page 57
- ▶ "Verifying system information backup / restore" on page 73
- ▶ "Resuming BitLocker functionality" on page 84

13.3 Front VGA board

13.3.1 Installing the front VGA board



**Upgrade and Repair Unit
(URU)**



Hardware: 10 minutes

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

13.3.1.1 Preliminary steps

- ▶ "Shutting down the server" on page 45
- ▶ "Disconnecting the server from the mains" on page 46
- ▶ "Getting access to the component" on page 47
- ▶ "Removing the front panel module" on page 237

13.3.1.2 Removing the dummy cover

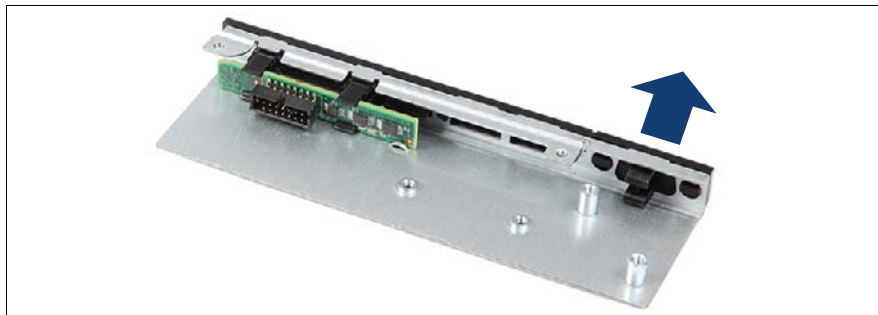


Figure 173: Removing the dummy cover

- ▶ Remove the dummy cover.



CAUTION!

Keep the dummy cover for future use. If you remove the front VGA board again and do not replace it with a new one, the dummy cover must be reinstalled to comply with EMC regulations and to satisfy cooling requirements and fire protection measures.

13.3.1.3 Installing the front VGA board

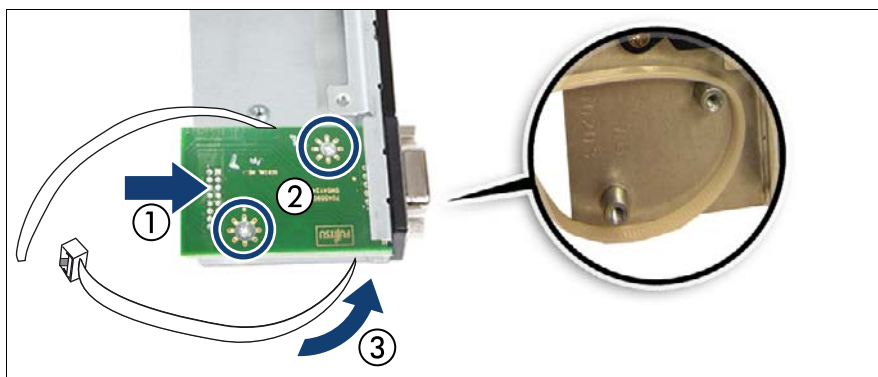


Figure 174: Installing the front VGA board

- ▶ Push the front VGA connector in the corresponding recess (1) and fasten the front VGA board with two screws (2).
- ▶ Route the cable tie under the front VGA board (3).

13.3.1.4 Concluding steps

- ▶ ["Installing the front panel module" on page 239](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

13.3.2 Removing the front VGA board



**Upgrade and Repair Unit
(URU)**



Hardware: 10 minutes

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

13.3.2.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Removing the front panel module" on page 237](#)

13.3.2.2 Removing the front VGA board

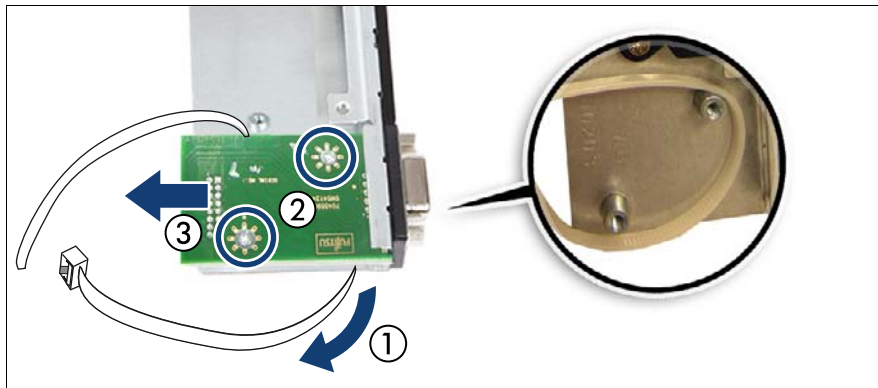


Figure 175: Removing the front VGA board

- ▶ If the VGA cable was secured with a cable tie, pull out the cable tie (1).
- ▶ Remove the two screws (2) and remove the front VGA board (3).

13.3.2.3 Installing the dummy cover

- ▶ Install the dummy cover (see figure [173](#)).

13.3.2.4 Concluding steps

- ▶ ["Installing the front panel module" on page 239](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

13.3.3 Replacing the front VGA board



**Upgrade and Repair Unit
(URU)**



Hardware: 10 minutes

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

13.3.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Removing the front panel module" on page 237](#)

13.3.3.2 Removing the defective front VGA board

- ▶ Remove the front VGA board as described in section ["Removing the front VGA board" on page 244](#).

13.3.3.3 Installing the new front VGA board

- ▶ Install the front VGA board as described in section ["Installing the front VGA board" on page 242](#).

13.3.3.4 Concluding steps

- ▶ ["Installing the front panel module" on page 239](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

13.4 Front panel on QRL (10 x 2.5-inch HDD configuration)

13.4.1 Replacing the front panel on QRL



Field Replaceable Unit (FRU)



**Hardware: 10 minutes
Software: 5 minutes**

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

Note on system information backup / restore



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

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




CAUTION!

For that reason the front panel and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

13.4.1.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Locating the defective component" on page 45](#)

13.4.1.2 Removing the front panel on QRL

 The front panel on QRL and the front panel cable are combined in one spare part.

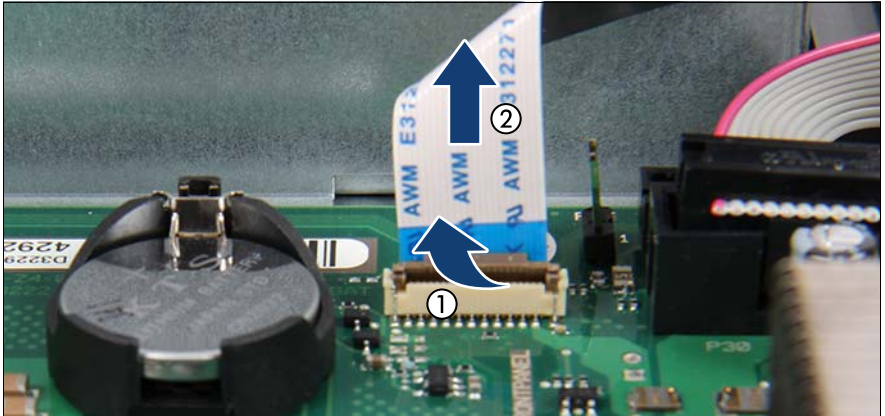


Figure 176: Disconnecting the front panel cable

- ▶ Pull up the locking bar (1).
- ▶ Remove the front panel cable (2).

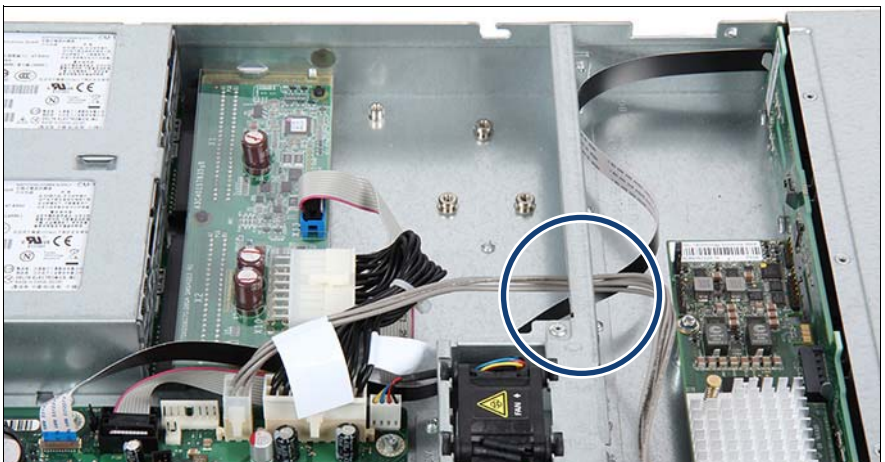


Figure 177: Disconnecting the front panel cable (B)

- ▶ Thread the front panel cable through the opening (see circle).

Front panel



Figure 178: Removing the front panel on QRL (A)

- ▶ Remove the two screws (see circles).

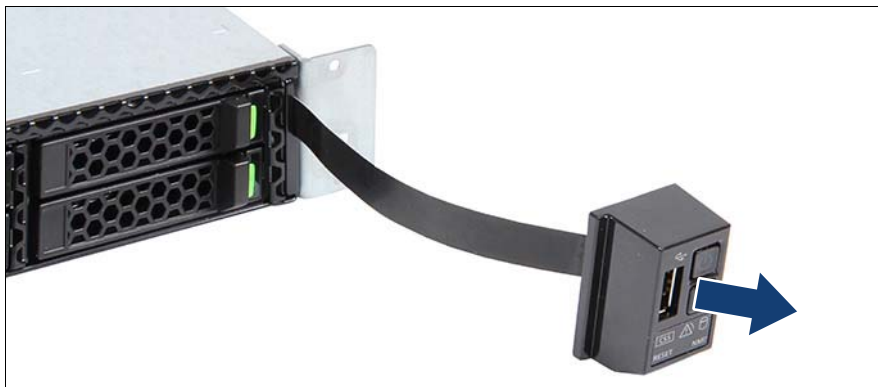


Figure 179: Removing the front panel on QRL (B)

- ▶ Remove the front panel.
- ▶ Pull the front cable out of the opening.

13.4.1.3 Installing the front panel on QRL

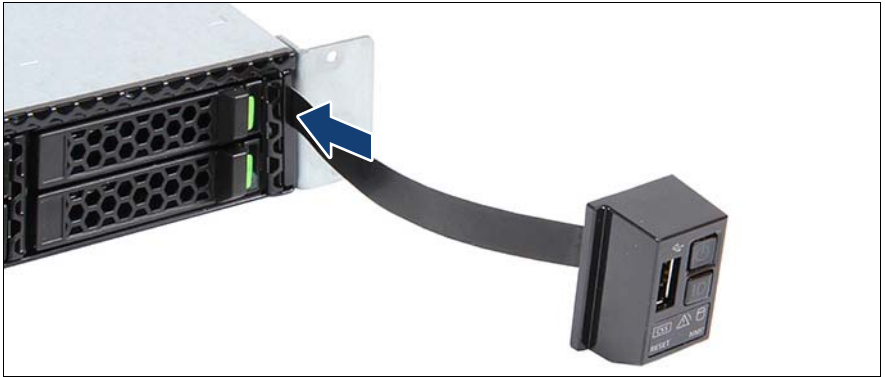


Figure 180: Installing the front panel (A)

- ▶ Thread the front panel cable through the opening.



Figure 181: Installing the front panel (B)

- ▶ Position the front panel on the ear.
- ▶ Fasten the front panel with two screws (see figure [178](#)).

Front panel

- ▶ Thread the front panel cable through the opening (see figure 177).

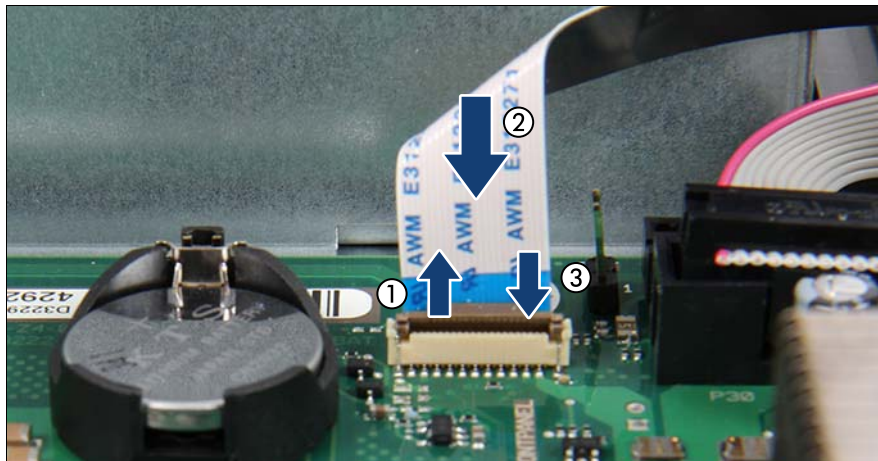


Figure 182: Connecting the front panel cable (B)

- ▶ Pull up the locking bar (1).
- ▶ Bend the cable 90 degrees by hand for easier routing.
- ▶ Insert the front panel cable (2). Please make sure that the front panel cable is assembled as shown (blue marking).
- ▶ Press down the locking bar (3).

13.4.1.4 Concluding steps

- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Using the Chassis ID Prom Tool" on page 87](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Verifying system information backup / restore" on page 73](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

14 System board and components

Safety notes



CAUTION!

- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "[Important information](#)" on page 31.

14.1 Basic information

This section provides instructions for the system board and the following components:

- CMOS memory (volatile BIOS memory) and the real-time clock are powered by a lithium coin cell (CMOS battery). This cell lasts up to ten years, depending on ambient temperature and use.

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

- UFM (USB Flash Module)

The server can be equipped with a USB Flash Module (UFM).

- TPM (Trusted Platform Module)

The system board is optionally equipped with a Trusted Platform Module (TPM). This module enables programs from third party manufacturers to store key information, for example drive encryption using Windows Bitlocker Drive Encryption.

- iRMC microSD card

The iRMC microSD card is necessary for using the embedded Lifecycle Management (eLCM) functionality of the iRMC.

14.2 CMOS battery

14.2.1 Replacing the CMOS battery



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

Tools: tool-less; recommended: tooth pick

Safety notes



CAUTION!

- The CMOS battery must be replaced with an identical battery or with a battery type recommended by the manufacturer.
- Keep lithium batteries away from children.
- Do not throw batteries into the trash can. Lithium batteries must be disposed of in accordance with local regulations concerning special waste.
- For further safety information, please refer to section "Environmental protection" in the operating manual of your server.
- **Ensure to insert the CMOS battery with the positive pole facing up!**

14.2.1.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

14.2.1.2 Replacing the defective CMOS battery

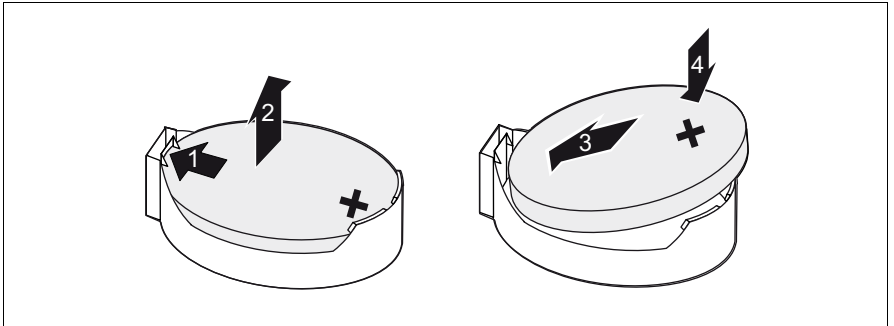


Figure 183: Replacing the CMOS battery

- ▶ Press the locking spring into direction of the arrow (1), so that the CMOS battery jumps out of its socket.
- ▶ Remove the CMOS battery (2).



CAUTION!

Sharp tools such as screw drivers might damage system board components in case of slipping.

If the CMOS battery cannot be ejected without the help of a tool, it is recommended to use a tooth pick.

- ▶ Insert a new CMOS battery of the same type into the socket (3) and (4).

14.2.1.3 Concluding steps

- ▶ Dispose of the CMOS battery in accordance with local regulations concerning special waste.
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Verifying system information backup / restore" on page 73](#)
- ▶ ["Verifying the system time settings" on page 80](#)

14.3 USB Flash Module (UFM)

14.3.1 Installing the UFM



Field Replaceable Unit
(FRU)



Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

14.3.1.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 3 as described in section ["Removing a riser module" on page 58](#).

14.3.1.2 Installing the UFM

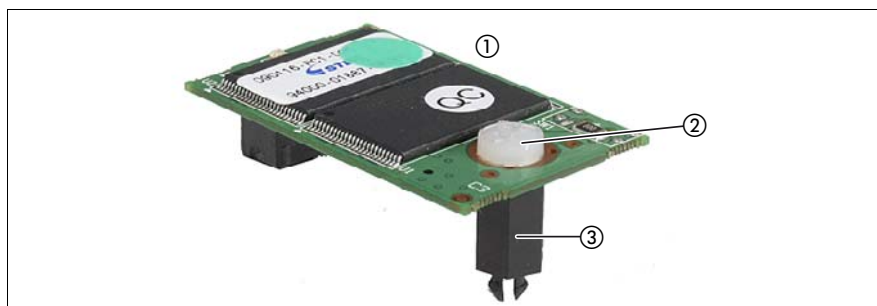


Figure 184: UFM installation kit

1	USB Flash Module (UFM)	3	UFM spacer
2	UFM nylon screw		

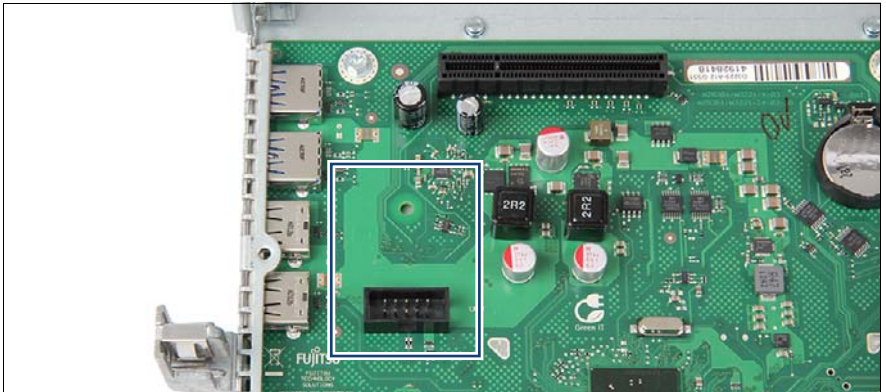


Figure 185: Position on the system board



Figure 186: Installing the UFM

- ▶ Connect the UFM to the system board. The UFM spacer must click into the hole on the system board.

14.3.1.3 Concluding steps

- ▶ Install the riser module 3 as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)

System board and components

- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

14.3.1.4 Software configuration

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

- ▶ Switch on the server.
- ▶ 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.

14.3.2 Removing the UFM



Field Replaceable Unit (FRU)



Hardware: 5 minutes

Tools: <ul style="list-style-type: none">– Phillips PH1 / (+) No. 1 screw driver– combination pliers and flat nose pliers

14.3.2.1 Preliminary steps

- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 3 as described in section ["Removing a riser module" on page 58](#).

14.3.2.2 Removing the UFM

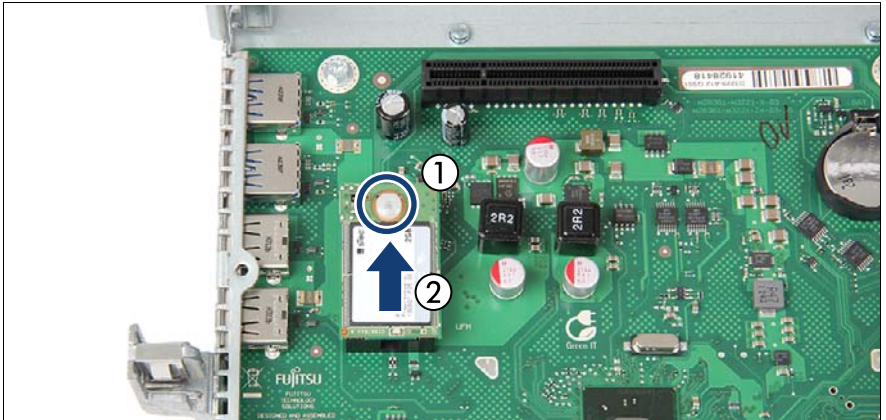


Figure 187: Removing the UFM

- ▶ Remove the nylon screw of the UFM (1).
- ▶ Disconnect and remove the UFM (2).
The UFM spacer remains on the system board.



Figure 188: Remaining UFM spacer



CAUTION!

UFM contains customer information (e.g. IP address, License etc.). After replacing the UFM, you must pass the defective UFM to the customer, and ask for disposal. If the disposal of the defective UFM is requested by the customer, you break it according to the following procedure, and dispose it.



Figure 189: Tools for breaking the UFM

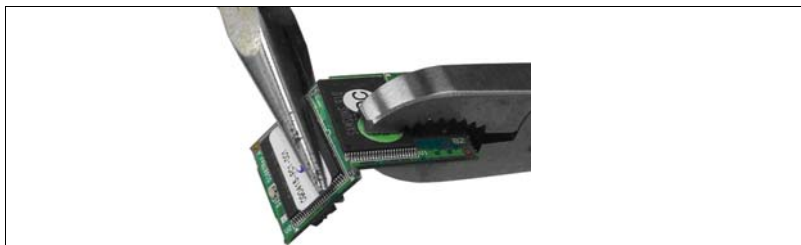


Figure 190: UFM breaking method

- ▶ Use a long nose pliers and a combination pliers to break the UFM in half as shown in the figure.

14.3.2.3 Concluding steps

- ▶ Install the riser module 3 as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)

- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

14.3.3 Replacing the UFM



Field Replaceable Unit (FRU)



Hardware: 5 minutes
Software: 5 minutes

Tools: – Phillips PH1 / (+) No. 1 screw driver – combination pliers and flat nose pliers
--

14.3.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 3 as described in section ["Removing a riser module" on page 58](#).

14.3.3.2 Removing the defective UFM

- ▶ Remove the UFM as described in section ["Removing the UFM" on page 257](#).
- ▶ The UFM spacer remains on the system board.

14.3.3.3 Installing the new UFM

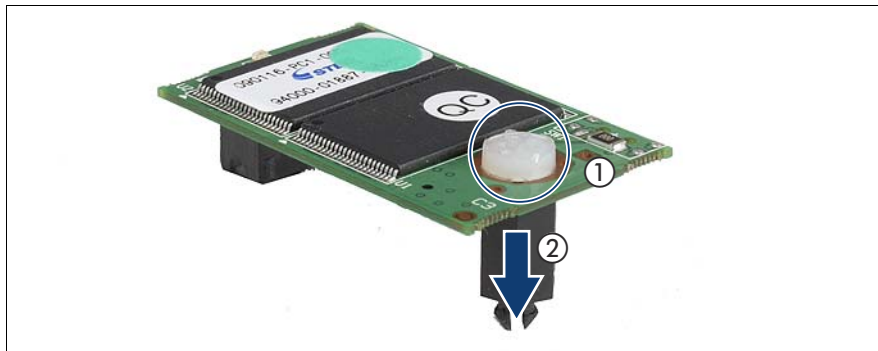


Figure 191: Removing the UFM spacer

- ▶ Remove the nylon screw from the UFM (1).
- ▶ Remove the UFM spacer (2).

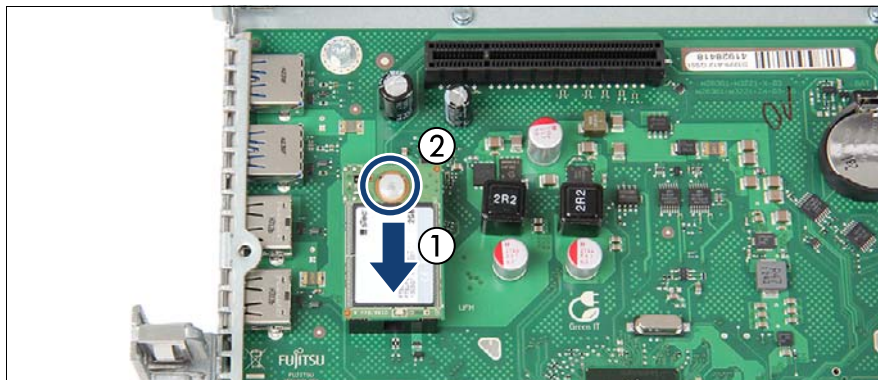


Figure 192: Installing the UFM

- ▶ Connect the UFM to the system board and the remaining UFM spacer (1).
- ▶ Fasten the UFM to the UFM spacer with the nylon screw (2).

14.3.3.4 Concluding steps

- ▶ Install the riser module 3 as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)

- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)

14.3.3.5 Software configuration

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

- ▶ Switch on the server.
- ▶ 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.

14.4 Trusted Platform Module (TPM)

14.4.1 Installing the TPM



Field Replaceable Unit (FRU)



Hardware: 5 minutes
Software: 5 minutes

Tools:

- Bit screw driver
- TPM bit insert (*)

(*) For the Japanese market:

- TPM module fixing tool (S26361-F3552-L909)

14.4.1.1 Preliminary steps

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)

System board and components

- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 1 as described in section ["Removing a riser module" on page 58.](#)

14.4.1.2 Installing the TPM

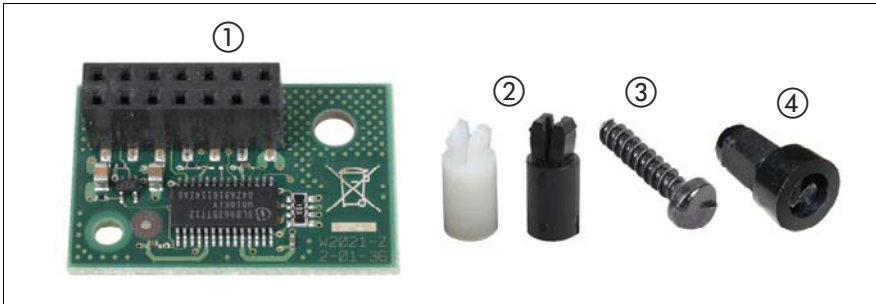


Figure 193: TPM installation kit


1	TPM (Trusted Platform Module)	3	Special screw for TPM
2	TPM spacer  The black TPM spacer is not used in this server.	4	TPM bit insert for TPM special screw



Figure 194: Position on the system board



Figure 195: Inserting the TPM spacer on the system board

- ▶ Insert the TPM spacer into the hole on the system board.



Figure 196: TPM bit insert

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

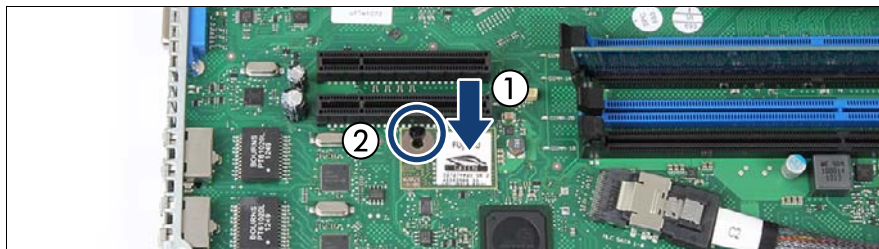


Figure 197: Installing the TPM

- ▶ Connect the TPM to the system board (1).
- ▶ Fasten the TPM with the special screw for the TPM using the TPM bit insert or TPM module fixing tool (Japanese market) (2).



CAUTION!

Do not fasten the screw too firmly. Stop it by extent where the head of the screw lightly touches the TPM (torque value of 0.6 Nm).

14.4.1.3 Concluding steps

- ▶ Install the riser module 1 as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)
- ▶ Enable TPM in the system board BIOS. Proceed as follows:
 - ▶ Switch on or restart your server.
 - ▶ As soon as the startup screen appears, press the **[F2]** function key to enter the BIOS.
 - ▶ Select the *Advanced* menu.
 - ▶ Select the *Trusted Computing* submenu.
 - ▶ Set the *TPM Support* and *TPM State* settings to *Enabled*.
 - ▶ Under *Pending TPM operation*, select the desired TPM operation mode.

- ▶ Save your changes and exit the BIOS.



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

14.4.2 Removing the TPM



Field Replaceable Unit (FRU)



Hardware: 30 minutes

Tools: Removing the system board:

- Phillips PH2 / (+) No. 2 screw driver

Removing the TPM:

- Bit screw driver
- flat nose pliers
- TPM bit insert (*)

(*) For the Japanese market:

- TPM module fixing tool (S26361-F3552-L909)



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 removing the TPM will cause to lose all data.

14.4.2.1 Preliminary steps

Before removing the TPM board, perform the following steps:

- ▶ Before removing the TPM board, 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:

System board and components

- ▶ 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:
 - ▶ Switch on or restart your server.
 - ▶ As soon as the startup screen appears, press the **[F2]** function key to enter the BIOS.
 - ▶ Select the *Advanced* menu.
 - ▶ Select the *Trusted Computing* submenu.
 - ▶ Set the *TPM Support* and *TPM State* settings to *Disabled*.
 - ▶ Save your changes and exit the BIOS.



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

- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)

14.4.2.2 Removing the TPM

- ▶ "Removing the defective system board" on page 279
- ▶ Lay the system board on a soft, antistatic surface with its component side facing down.

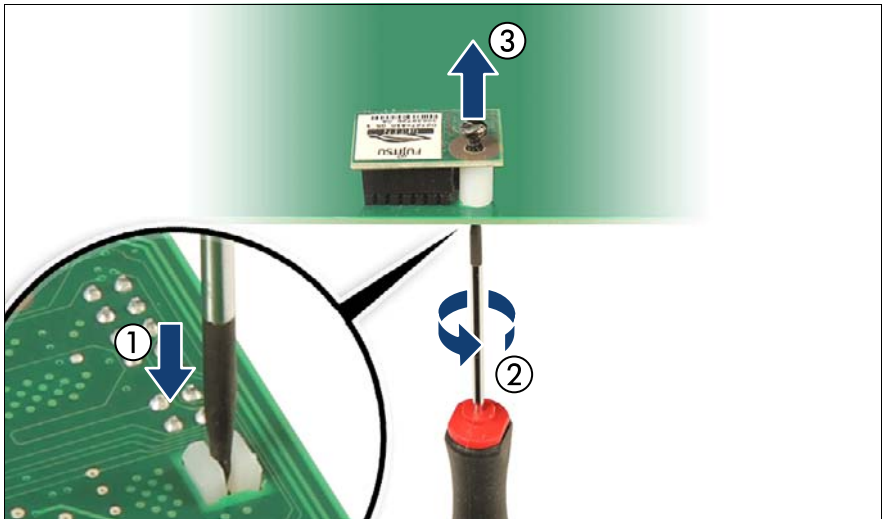


Figure 198: Removing the TPM screw

- ▶ Locate the slotted lower end of the TPM screw (1).
- ▶ Carefully loosen the TPM screw using a thin slotted screw driver (e.g. watchmaker's screw driver) or the dedicated TPM screw driver (Japanese market) (2).



CAUTION!

Ensure to turn the screw **clockwise** in order to remove it!

Slowly and carefully increase the pressure on the screw until it begins to turn. The effort when 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 (3).
- ▶ Remove the TPM on the upper side of the system board.

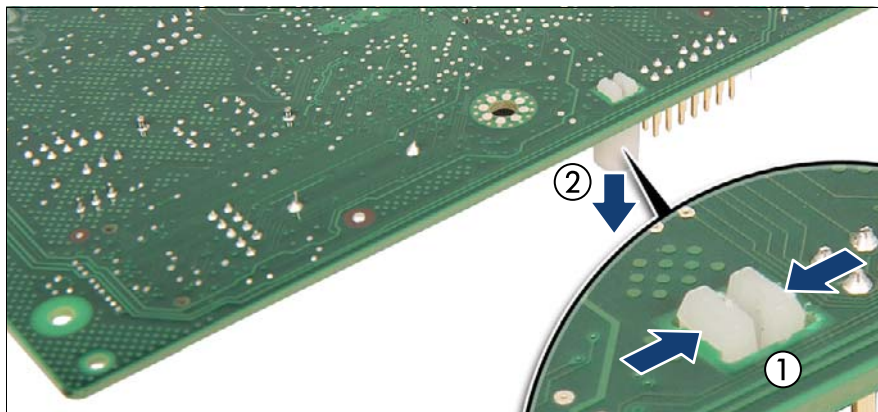


Figure 199: Removing the TPM spacer

- ▶ Using a flat nose pliers, press together the hooks on the TPM spacer (1, see close-up) and remove it from the system board (2).

i If the TPM is to be replaced, the TPM spacer may remain on the system board.

14.4.2.3 Concluding steps

- ▶ ["Installing the new system board" on page 280](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

14.4.3 Replacing the TPM



Field Replaceable Unit (FRU)



Hardware: 30 minutes

Tools: 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)



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 board will cause to lose all data.

14.4.3.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ ["Removing the defective system board" on page 279](#)

14.4.3.2 Removing the defective TPM

- ▶ Remove the TPM as described in section ["Removing the TPM" on page 265](#).
- ▶ Leave the TPM spacer on the system board when removing the defective TPM.

14.4.3.3 Installing the new TPM



The TPM spacer is already present on the system board.

- ▶ Install the TPM as described in section ["Installing the TPM" on page 262](#).

14.4.3.4 Concluding steps

- ▶ Reinstall the system board as described in section ["Installing the new system board" on page 280](#)
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)
- ▶ ["Resuming BitLocker functionality" on page 84](#)



You can find information on configuring the TPM in the corresponding BIOS Setup Utility reference manual.

14.5 iRMC microSD card

i The iRMC microSD card is necessary for using the Embedded Lifecycle Management (eLCM) functionality of the iRMC. It requires a valid eLCM license key, which is always purchased together with the iRMC microSD card and activated through the iRMC web frontend.

For further information, please refer to the “ServerView embedded Lifecycle Management (eLCM)” user guide.

14.5.1 Installing the iRMC microSD card



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

Tools: tool-less

14.5.1.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 1 as described in section ["Removing a riser module" on page 58](#).

14.5.1.2 Installing the iRMC microSD card



Figure 200: iRMC microSD card

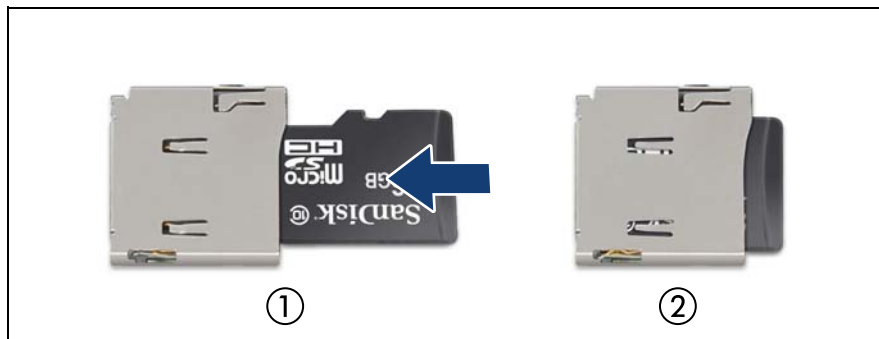


Figure 201: Installing the iRMC microSD card

- ▶ With the label facing up, insert the iRMC microSD card into the microSD card slot (1) until it locks in place (2).



The onboard position of the microSD card slot can be found in section ["Connectors and indicators on the system board"](#) on page 300.

14.5.1.3 Concluding steps

- ▶ Install the riser module 1 as described in section ["Installing a riser module"](#) on page 60.
- ▶ ["Reassembling"](#) on page 52
- ▶ ["Connecting the server to the mains"](#) on page 55
- ▶ ["Switching on the server"](#) on page 57

14.5.2 Removing the iRMC microSD card



Upgrade and Repair Unit
(URU)



Hardware: 5 minutes

Tools: a pair of side-cutting pliers

14.5.2.1 Preliminary steps

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove the riser module 1 as described in section ["Removing a riser module" on page 58](#).

14.5.2.2 Removing the iRMC microSD card

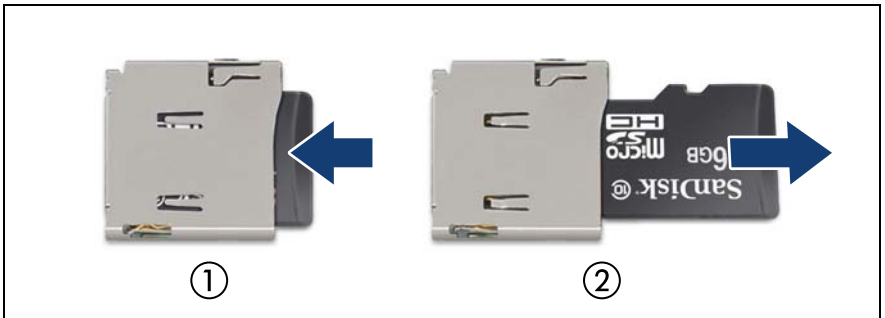


Figure 202: Removing the iRMC microSD card

- ▶ To eject the iRMC microSD card, gently push it in and then let go (1).
- ▶ Pull the iRMC microSD card straight out of its slot (2).

Destroying the defective iRMC microSD card



CAUTION!

The iRMC microSD card contains customer information. After replacing the iRMC microSD card, hand the defective card over to the customer. If the customer requests disposal of the defective iRMC microSD card, proceed as follows:

- ▶ Using a pair of side-cutting pliers, cut the iRMC microSD card in half.

14.5.2.3 Concluding steps

- ▶ Install the riser module 1 as described in section "[Installing a riser module](#)" on page 60.
- ▶ "[Reassembling](#)" on page 52
- ▶ "[Connecting the server to the mains](#)" on page 55
- ▶ "[Switching on the server](#)" on page 57

14.5.3 Replacing the iRMC microSD card



Upgrade and Repair Unit (URU)



Hardware: 5 minutes

Tools: a pair of side-cutting pliers

14.5.3.1 Preliminary steps

- ▶ "[Locating the defective server](#)" on page 43
- ▶ "[Shutting down the server](#)" on page 45
- ▶ "[Disconnecting the server from the mains](#)" on page 46
- ▶ "[Getting access to the component](#)" on page 47
- ▶ Remove the riser module 1 as described in section "[Removing a riser module](#)" on page 58.

14.5.3.2 Replacing the iRMC microSD card

- ▶ Remove the defective iRMC microSD card as described in section ["Removing the iRMC microSD card" on page 273](#).
- ▶ Install the new iRMC microSD card as described in section ["Installing the iRMC microSD card" on page 271](#).

14.5.3.3 Concluding steps

- ▶ Install the riser module 1 as described in section ["Installing a riser module" on page 60](#).
- ▶ ["Reassembling" on page 52](#)
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ ["Switching on the server" on page 57](#)

14.6 System board

14.6.1 Replacing the system board



Field Replaceable Unit (FRU)



Hardware: 40 minutes
Software: 20 minutes

Tools: Replacing the system board:

- Phillips PH2 / (+) No. 2 screw driver
- Magnifying glass for inspecting processor socket springs (recommended)

Replacing the TPM:

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

(*) For the Japanese market:

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

If an UFM is installed:

- Phillips PH1 / (+) No. 1 screw driver

Note on TPM



The system board can be equipped with an optional TPM (Trusted Platform Module). This module enables third party programs to store key information (e. g. drive encryption using Windows Bitlocker Drive Encryption).

If the customer is using TPM functionality, the TPM has to be removed from the defective system board and connected to the new system board. For a detailed description, please refer to [section "Replacing the TPM" on page 269](#).

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 board will cause to lose all data.

Note on system information backup / restore



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

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



CAUTION!

For that reason the front panel and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

Note on network settings recovery



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

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

14.6.1.1 Preliminary steps

- ▶ ["Locating the defective server" on page 43](#)
- ▶ ["Note on network settings recovery" on page 277](#)
- ▶ ["Disabling SVOM boot watchdog functionality" on page 64](#)
- ▶ ["Suspending BitLocker functionality" on page 63](#)
- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ Disconnect all external cables.
- ▶ ["Getting access to the component" on page 47](#)
- ▶ Remove all memory modules, see section ["Removing a memory module" on page 211](#).



Before removing the memory modules, take a note on the installation slot number for each memory module. Make sure that you reinstall the memory modules in the slot they were located before the replacement.

- ▶ Remove the heat sink, see section ["Removing the heat sink" on page 215](#).
- ▶ Remove all expansion cards, see section ["Expansion cards and riser cards" on page 170](#).



Before removing the expansion cards, take a note on the installation slot number for each card. Make sure that you reinstall the card in the slot it was located before the replacement.

- ▶ Remove the UFM (if applicable), see section ["Removing the defective UFM" on page 259](#).



Remove the UFM spacer from the defective system board and fasten it with the UFM screw to the UFM board.

- ▶ Remove the iRMC microSD card (if applicable), see section ["Removing the iRMC microSD card" on page 273](#).

14.6.1.2 Removing the defective system board

- ▶ Disconnect all cables from the system board.

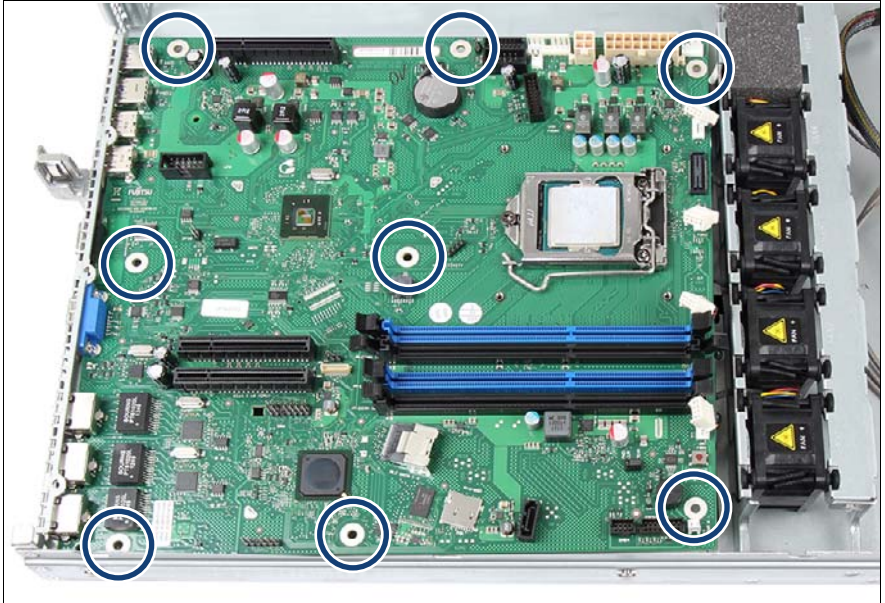


Figure 203: Position of the screws

- ▶ Remove the eight screws from the system board.

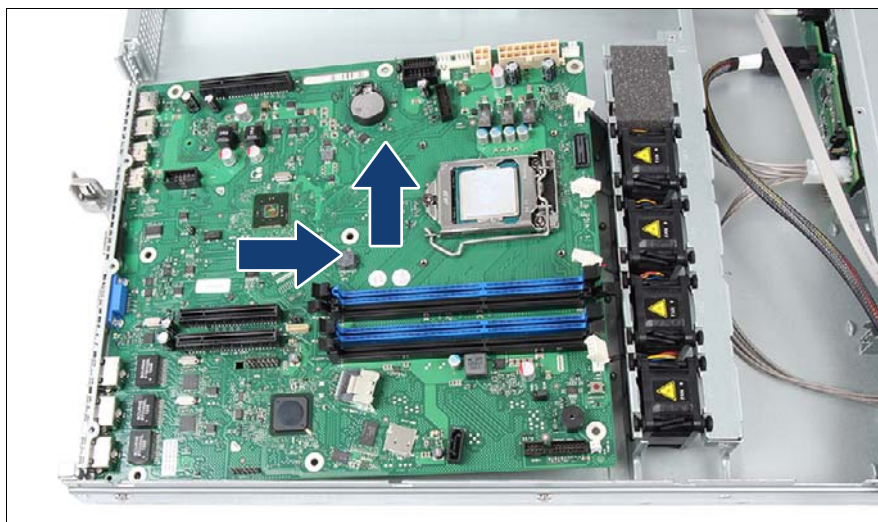


Figure 204: Removing the system board

- ▶ Use both hands to lift the system board carefully out of the chassis in a slight angle. Thereby you pull the connectors out of the connector panel.



CAUTION!

Always take the system board with both hands!

Never lift the system board one-sided or at a heat sink, because the solder connections between the socket and the system board come under tension and increase the risk of damage and malfunction!

Don't damage the EMI springs which are essential to comply with applicable EMC regulations and satisfy cooling requirements and fire protection measures.

- ▶ Place the removed and the new system board on an antistatic surface.
- ▶ Remove the TPM as described in section ["Removing the TPM" on page 265](#).

14.6.1.3 Installing the new system board

- ▶ Check the settings on the new system board (see section ["Onboard settings" on page 310](#)).
- ▶ Insert the system board by holding it at a slight angle. Slide the connectors into the connector panel (see figure [204 on page 280](#)).

- ▶ Lower the system board carefully into the chassis.
- ▶ Adjust the system board. If necessary adjust the position of the system board with a gentle twisting motion.
- ▶ Fasten the system board with the eight screws (see [figure 203 on page 279](#)).
- ▶ Remove the processor from the defective system board as described in section "[Removing the defective processor](#)" on page 216.
- ▶ Remove the protective plastic cover from the processor socket of the new system board and fit it onto the socket of the defective system board which will be sent back to spares.



Returned system boards without this cover probably have to be scrapped.

- ▶ Install the processor on the new system board as described in section "[Installing the new processor](#)" on page 217.
- ▶ Reconnect all cables to the system board:
 - Two power cables of power supply
 - Fan cables
 - Front panel cable
 - Front USB cable
 - Power cable for HDD backplane
 - SATA cable(s) for HDD backplane
 - SATA cable for ODD (if applicable)
 - Power cable for ODD (if applicable)
 - Front VGA cable (if applicable)
 - OOB cable (if applicable)

For the cable plan see section "[Cabling](#)" on page 285.

14.6.1.4 Concluding steps

- ▶ "[Installing the iRMC microSD card](#)" on page 271 (if applicable)
- ▶ "[Installing the TPM](#)" on page 261 (if applicable)
- ▶ "[Installing the UFM](#)" on page 254 (if applicable)
- ▶ Install the memory modules, see section "[Installing a memory module](#)" on page 209.




Make sure that you reinstall each memory module in the slot it was located before the replacement.

System board and components

- ▶ Install the heat sink, see section ["Installing the heat sink" on page 220](#).
- ▶ Install all expansion cards see section ["Expansion cards and riser cards" on page 170](#).



Make sure that you reinstall each card in the slots it was located before the replacement.

- ▶ ["Reassembling" on page 52](#)
 - ▶ ["Connecting the server to the mains" on page 55](#)
 - ▶ Connect all external cables.
 - ▶ ["Updating or recovering the system board BIOS and iRMC" on page 71](#)
 - ▶ If applicable, activate TPM functionality in the system BIOS under *Security > TPM (Security Chip) Setting > Security Chip*. For more information, refer to the corresponding BIOS Setup Utility reference manual.
 - ▶ ["Verifying system information backup / restore" on page 73](#)
 - ▶ If customer BIOS settings are not restored automatically, please change the settings manually (using the information collected during "preliminary steps"). If you couldn't determine the BIOS version, ask the customer to reconfigure all BIOS settings and password.
 - ▶ ["Verifying the system time settings" on page 80](#)
 - ▶ ["Looking up changed MAC / WWN addresses" on page 85](#)
 - ▶ ["Updating the NIC configuration file in a Linux environment" on page 83](#)
 - ▶ ["Enabling SVOM boot watchdog functionality" on page 78](#)
 - ▶ ["Switching on the server" on page 57](#)
 - ▶ ["Resuming BitLocker functionality" on page 84](#)
 - ▶ If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard).
-  Configuration of network settings should be performed by the customer. For further information, please refer to section ["Note on network settings recovery" on page 277](#).
- ▶ If applicable, restore LAN teaming configurations as described in section ["After replacing the system board" on page 89](#)

15 Cables

15.1 Overview cables

No.	Part number	Description	From - to
C1	T26139-Y4015-V301	CBL_FRONT_PANEL	System board to front panel
C2	T26139-Y3959-V301	CBL_HDD_2.5_POWER	System board to HDD backplane 1
C3	T26139-Y3990-V301	CBL_ODD_Power	System board to ODD power
C4	T26139-Y4028-V103	CBL SATA 530	System board to ODD data
C5	T26139-Y3994-V301	CBL_Front_VGA	System board to Front VGA
C6	T26139-Y4015-V601	CBL_OOB_HDD_2BP	System board to HDD backplane 1 and 2
C7	T26139-Y3999-V501	CBL_FRONT_USB	System board to front USB
C8	T26139-Y3964-V301	CBL_4HDD_DATA3.5	System board or RAID card 3.5-inch HDD backplane
C9	T26139-Y4041-V1	CBL_PDB_POWER	System board to power distribution board
C10	T26139-Y3956-V3	CBL_PDB_SIDE BAND	System board to power distribution board
C11	T26139-Y4040-V2	CBL 4HDD SAS 2.5	RAID card to 4x 2.5-inch HDD backplane
C12	T26139-Y4040-V3	CBL 4HDD SAS 2.5	RAID card to 4x 2.5-inch HDD backplane, L-shape
C13	T26139-Y3959-V351	CBL_HDD_3.5_POWER	From System board to 3.5-inch HDD backplane
C14	T26139-Y3959-V302	CBL PWR HDD 10X2.5	From System board to 10x 2.5-inch HDD backplane
C15	T26139-Y4042-V2	CBL FLEXP 22PL 600	System board to front panel on QRL (The front panel on QRL and the front panel cable are combined in one spare part.)
C16	T26139-Y3987-V1	LTG IBBU 700	BBU to RAID card
C17	T26139-Y4032-V1	CBL FBU02 620	FBU to RAID card
C18	T26139-Y4040-V9	CBL HOST-BP 540	Cougar4 to 4x 2.5-inch HDD backplane, L-shape

Cables

No.	Part number	Description	From - to
C19	T26139-Y4040-V15	CBL_4HDD_DATA3.5	Cougar4 to 3.5-inch HDD backplane
C20	T26139-Y4040-V20	CBL_SAS3.0_385	Cougar4 to 4x 2.5-inch HDD backplane. rectangular, Expander
C21	T26139-Y4031-V103	CBL FBU03 700	Cougar4 to FBU

15.2 Cabling

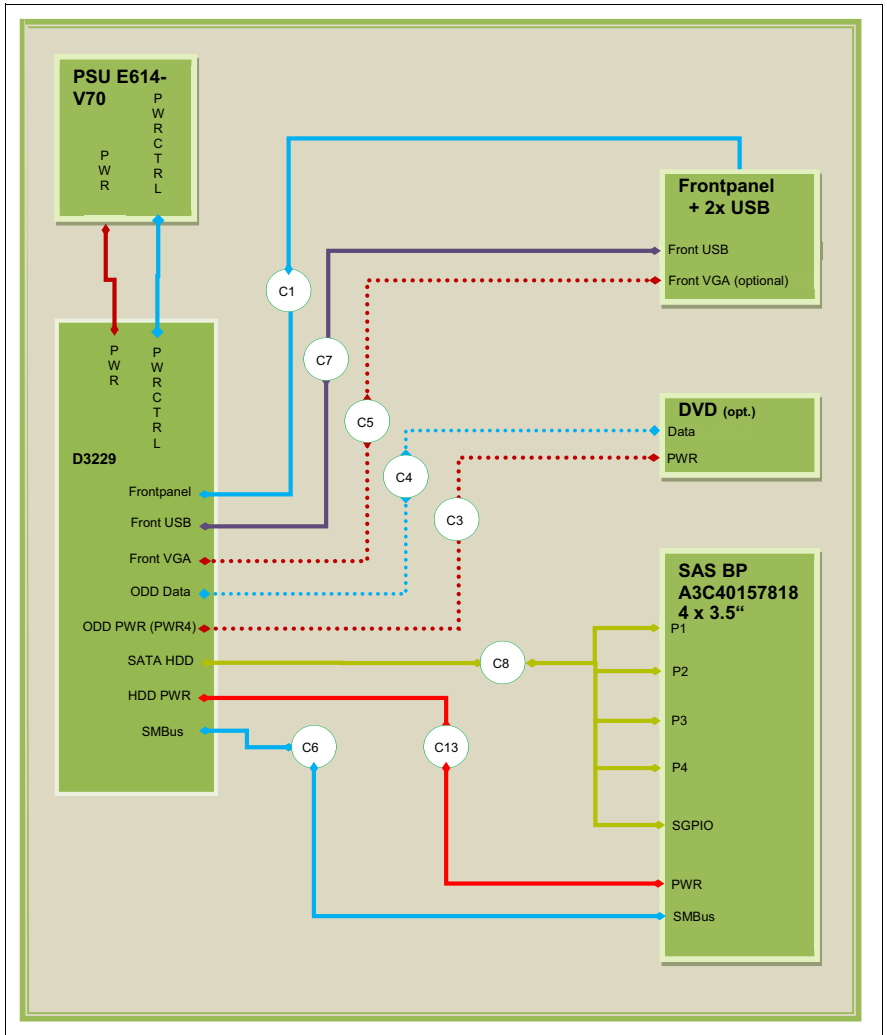


Figure 205: Cabling 4x 3.5-inch HDD, standard power supply

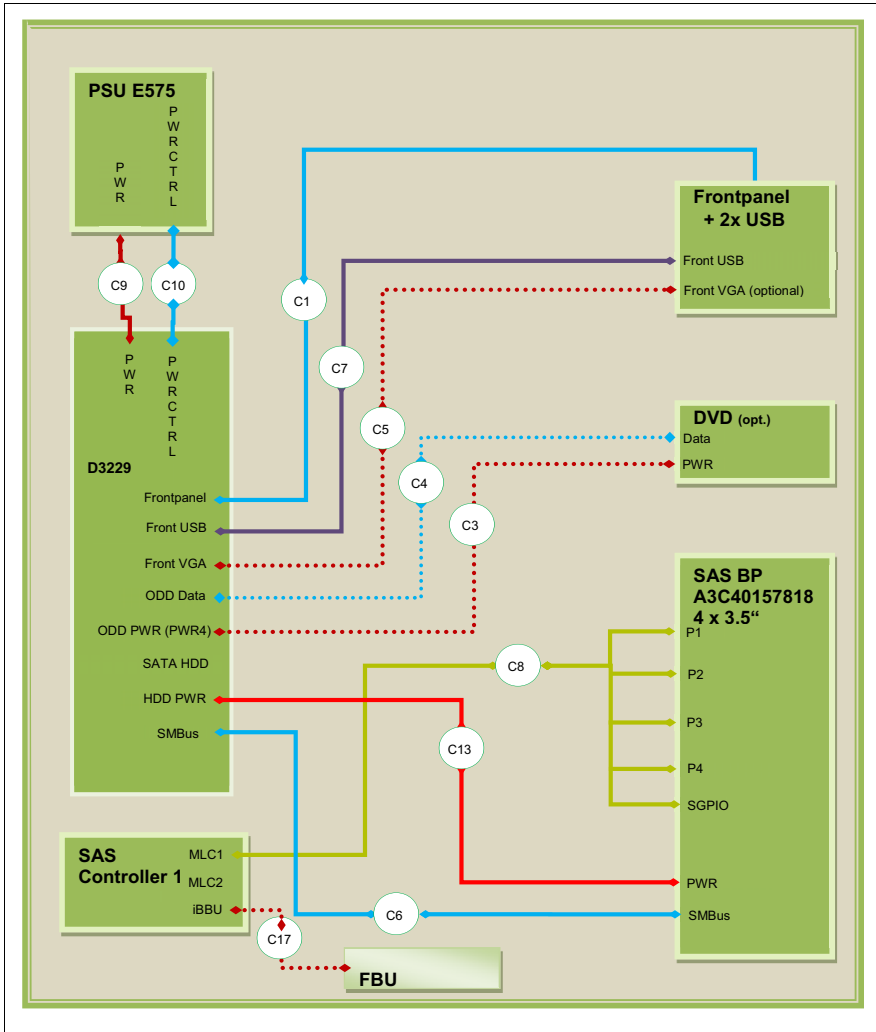


Figure 206: Cabling 4x 3.5-inch HDD, redundant power supply

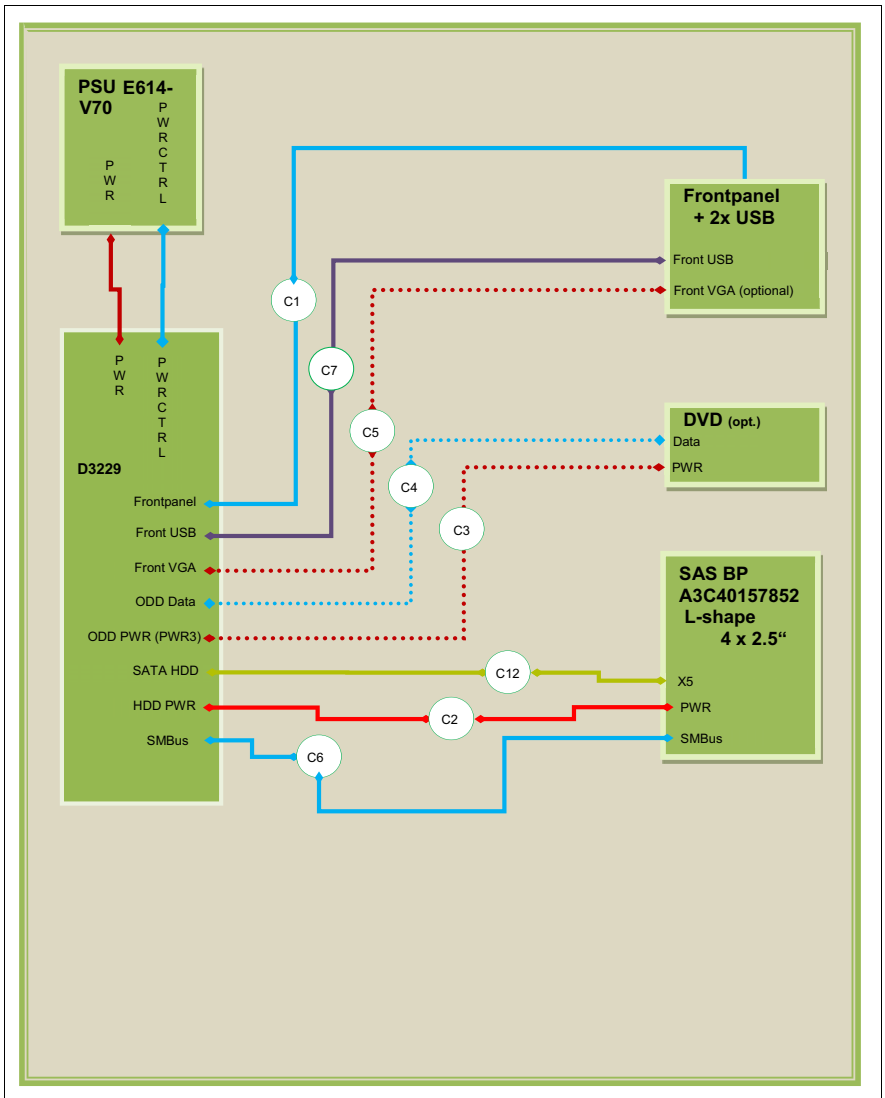


Figure 207: Cabling 4x 2.5-inch HDD, standard power supply

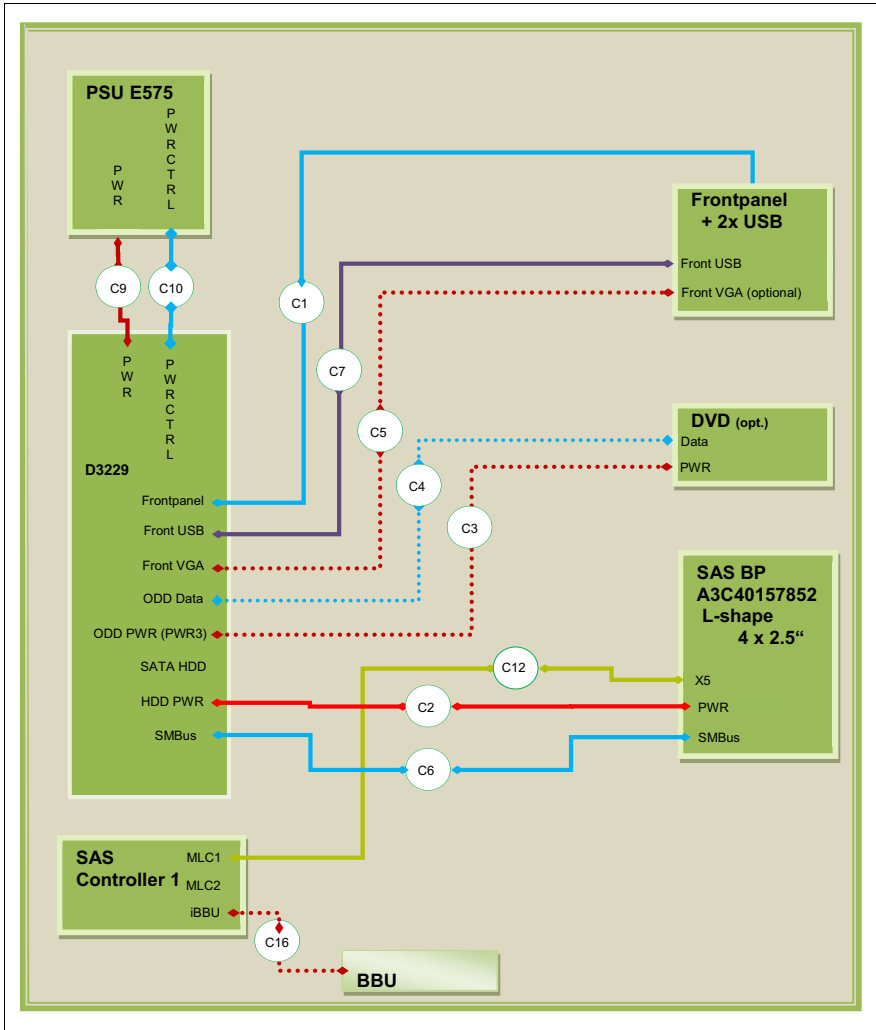


Figure 208: Cabling 4x 2.5-inch HDD, BBU, redundant power supply

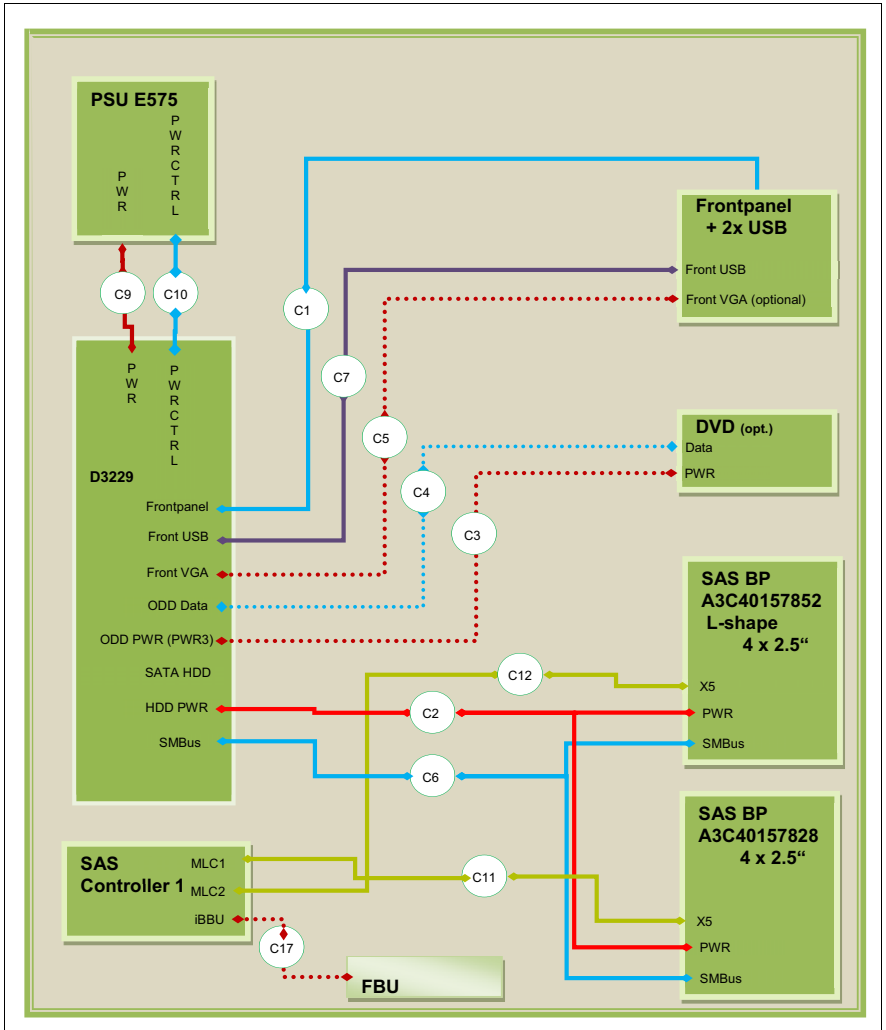


Figure 209: Cabling 8x 2.5-inch HDD, FBU, redundant power supply

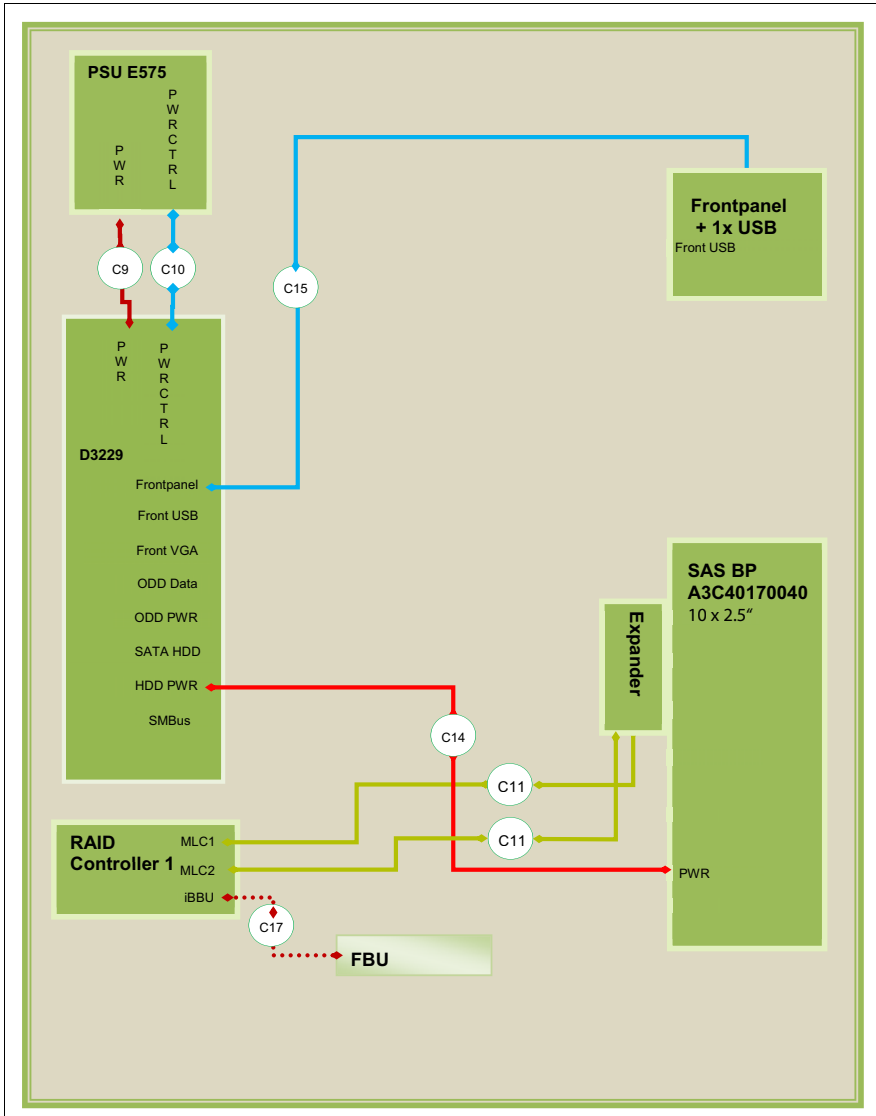


Figure 210: Cabling 10x 2.5-inch HDD, FBU, redundant power supply

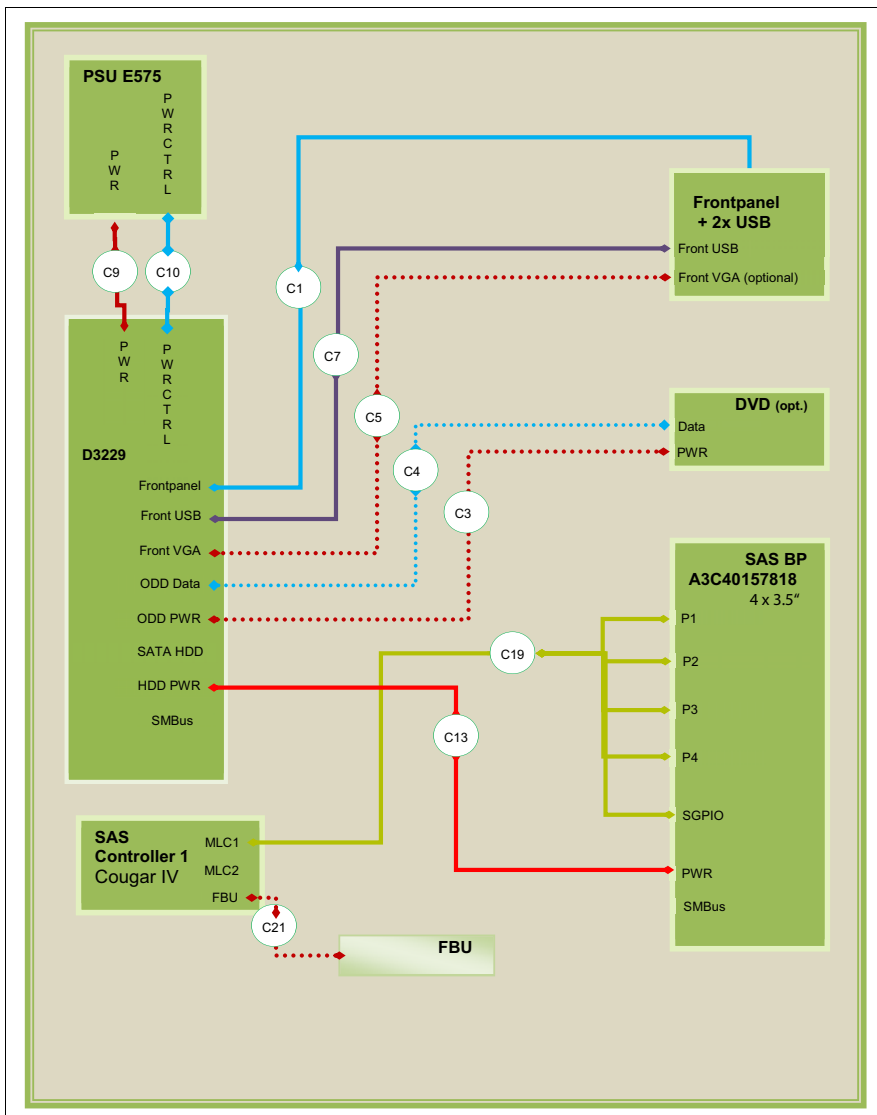


Figure 211: Cabling 4x 3.5-inch HDD, redundant power supply, Cougar 4

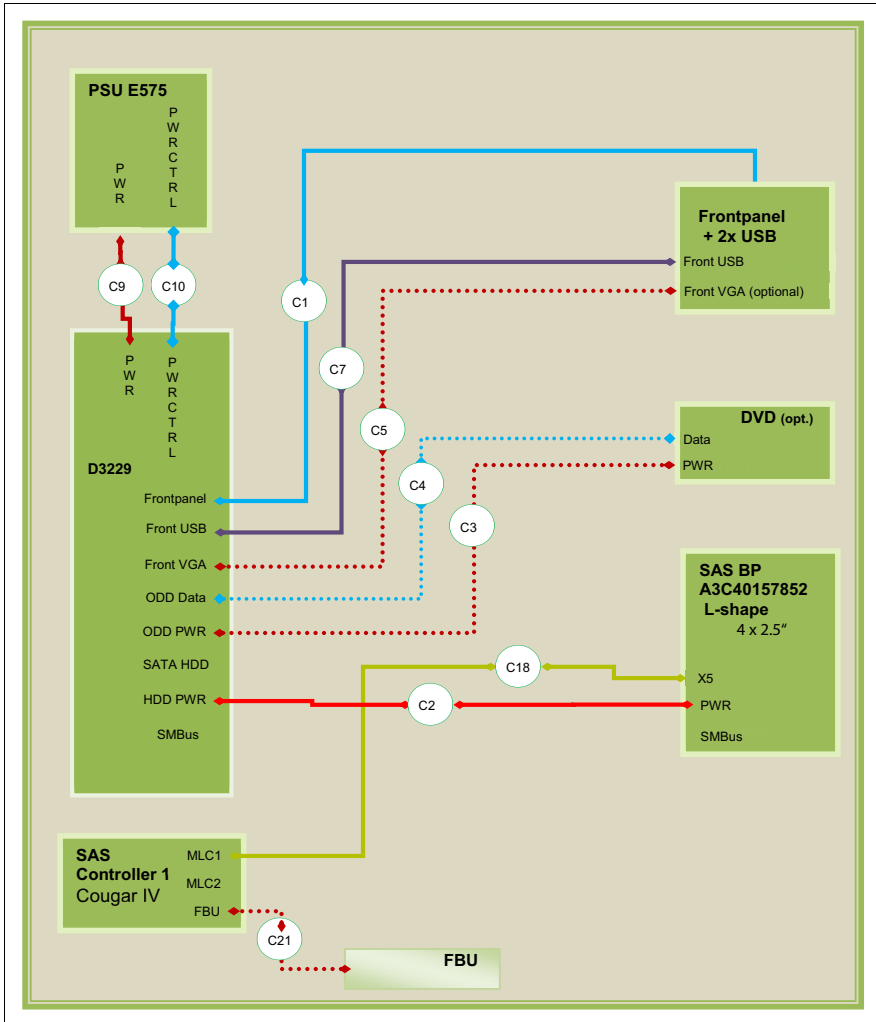


Figure 212: Cabling 4x 2.5-inch HDD, redundant power supply, Cougar 4

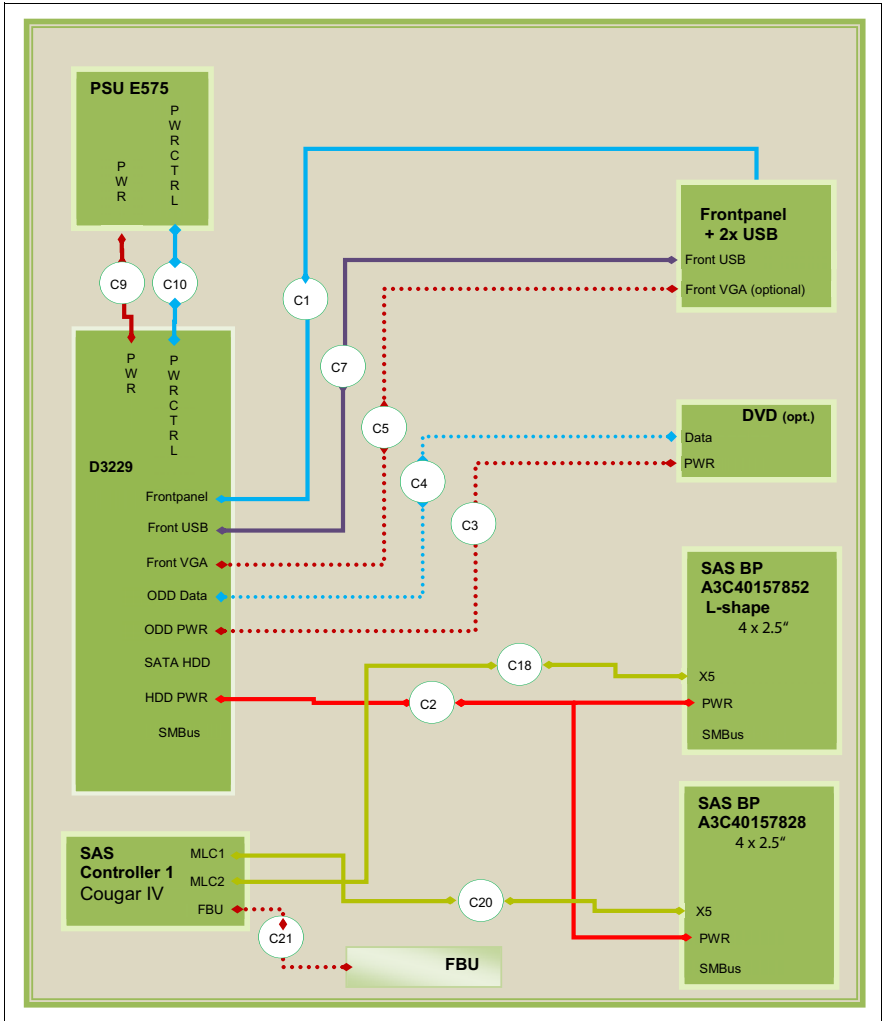


Figure 213: Cabling 8x 2.5-inch HDD, redundant power supply, Cougar 4

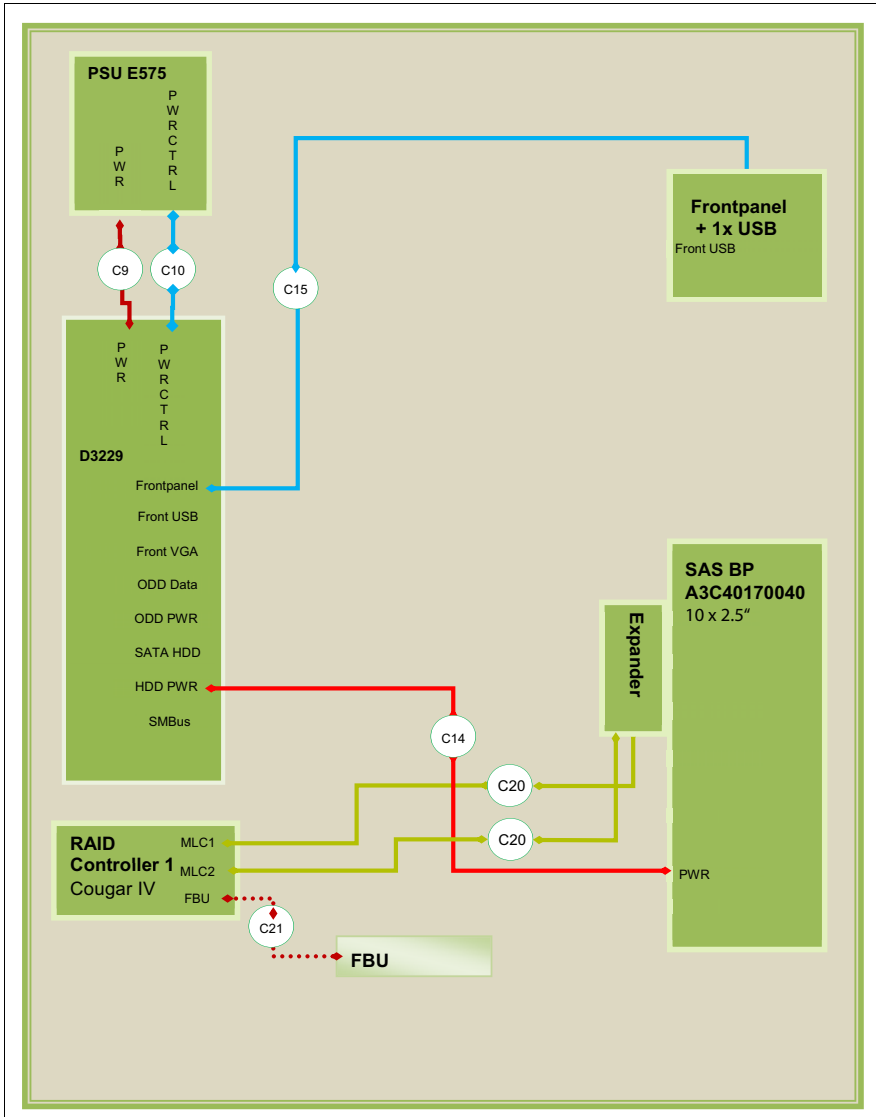


Figure 214: Cabling 10x 2.5-inch HDD, redundant power supply, Cougar 4

16 Appendix

16.1 Mechanical overview

16.1.1 Server front

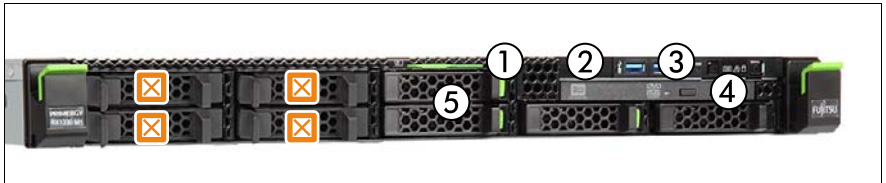


Figure 215: Front side 2.5-inch HDDs (up to 4 HDDs)

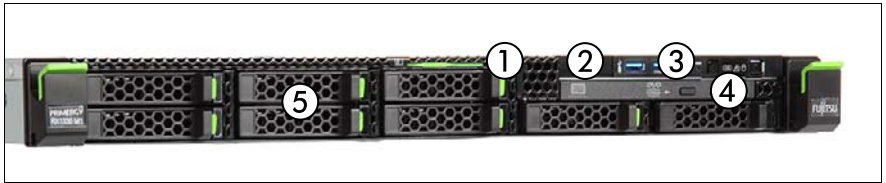


Figure 216: Front side 2.5-inch HDDs (up to 8 HDDs)

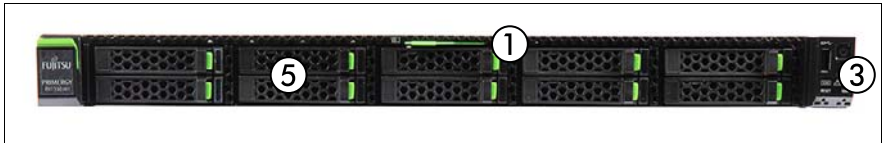


Figure 217: Front side 2.5-inch HDDs (up to 10 HDDs)

Pos.	Component
1	ID card
2	Front VGA (option) / dummy cover
3	Front panel and indicators
4	ODD (option) / dummy cover
5	4x /8x /10x 2.5-inch hard disk drives / dummy modules



Figure 218: Front side 3.5-inch HDDs

Pos.	Component
1	ODD (option) / dummy cover
2	ID card
3	Front VGA (option) / dummy cover
4	Front panel and indicators
5	4x 3.5-inch hard disk drives / dummy modules

16.1.2 Server rear



Figure 219: Rear side (standard power supply)

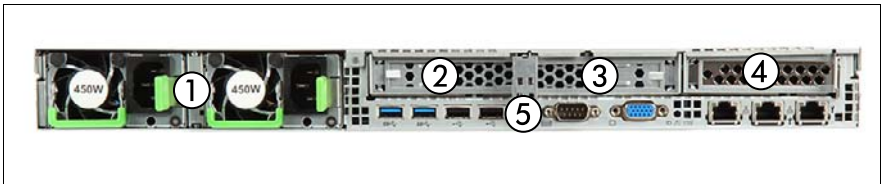


Figure 220: Rear side (redundant power supply)



Figure 221: Rear side (redundant power supply and full height riser module)

Pos.	Component
1	Standard power supply: one power supply unit Redundant power supply: up to 2 hot-plug power supply units / dummy cover
2	PCI slot 3 / riser module 3
3	PCI slot 2 / riser module 2
4	PCI slot 1 / riser module 1
5	I/O panel
6	PCI slot 3 / full height riser module

16.1.3 Server interior

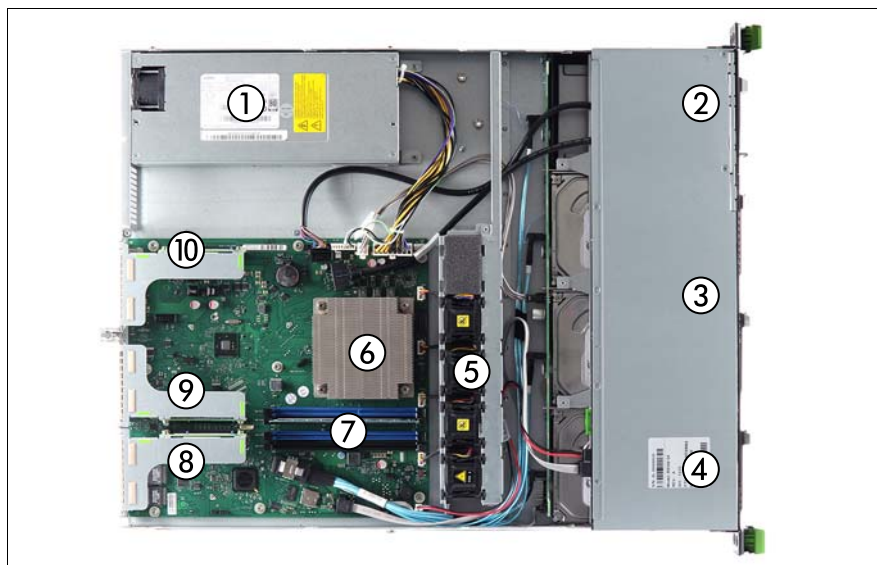


Figure 222: Interior (example 3.5-inch HDDs and standard power supply)

Pos.	Component
1	Standard power supply: one power supply unit
2	Front panel module / front VGA (option) / dummy cover
3	Up to 4x 3.5-inch hard disk drives / dummy modules
4	ODD (option) / dummy cover
5	4x fan modules
6	Processor
7	Main memory
8	Riser module 1
9	Riser module 2
10	Riser module 3

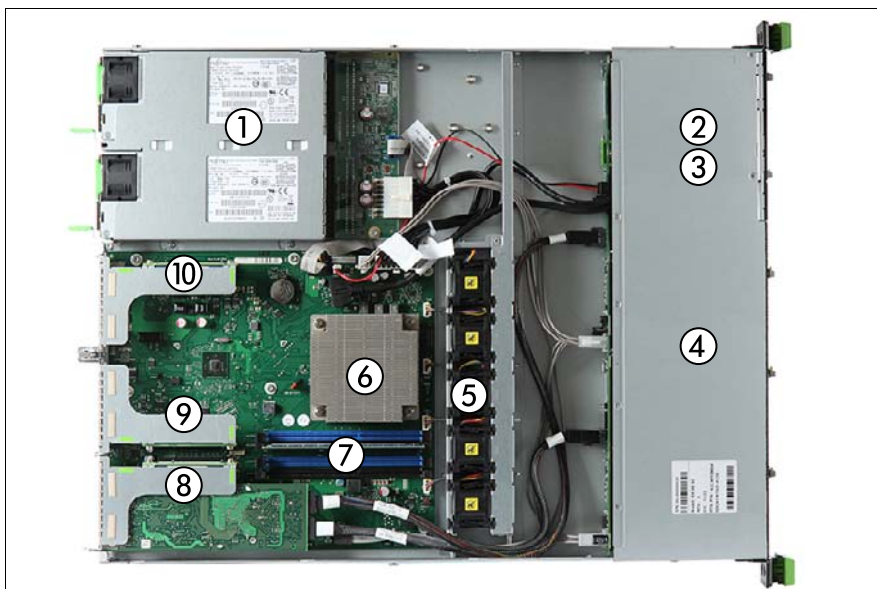


Figure 223: Interior (example: 2.5-inch HDDs and redundant power supply)

Pos.	Component
1	Redundant power supply: up to 2 hot-plug power supply units / dummy cover
2	Front panel module / front VGA (option) / dummy cover
3	ODD (option) / dummy cover
4	Up to 8x 2.5-inch hard disk drives / dummy modules
5	5x fan modules
6	Processor
7	Main memory
8	Riser module 1
9	Riser module 2
10	Riser module 3

16.2 Connectors and indicators

16.2.1 Connectors and indicators on the system board

16.2.1.1 Onboard connectors

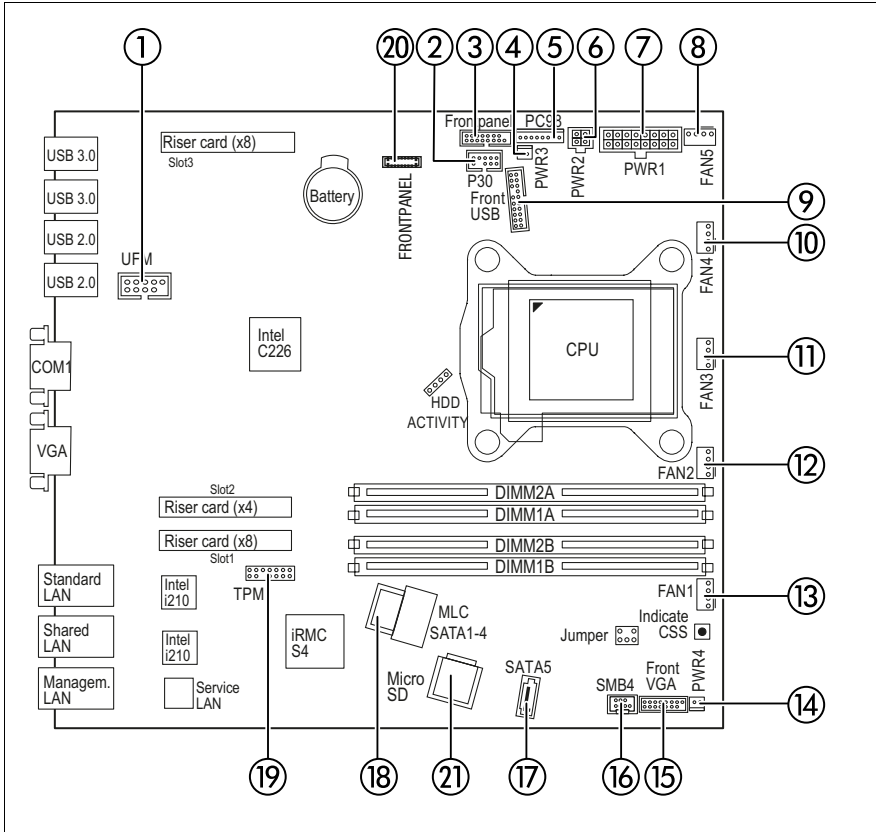


Figure 224: Internal connectors of the system board D3229

No.	Print	Description
1	UFM	Connector for optional USB Flash Module (UFM)
2	P30	Power supply connector (redundant power supply only)
3	FRONT PANEL	Front panel connector (front panel module)
4	PWR3	Power supply connector for ODD (2.5-inch HDD configuration)
5	PC98	Power supply connector (standard power supply only)
6	PWR2	Power connector for HDD backplane
7	PWR1	Power supply connector 12V
8	FAN5	Power connector for system fan 5
9	USB FRONT	Front USB connector
10	FAN4	Power connector for system fan 4
11	FAN3	Power connector for system fan 3
12	FAN2	Power connector for system fan 2
13	FAN1	Power connector for system fan 1
14	PWR4	Power supply connector for ODD (3.5-inch HDD configuration)
15	FRONT VGA	Connector for optional front VGA
16	SMB4	OOB (Out Of Band) connector for HDD backplane
17	SATA 5	SATA connector for ODD
18	MLC SATA 1-4	SATA HDD connector
19	TPM	Connector for optional TPM
20	FRONT PANEL	Front panel connector (front panel on QRL)
21	micro SD	iRMC microSD card

16.2.1.2 Onboard indicators and controls

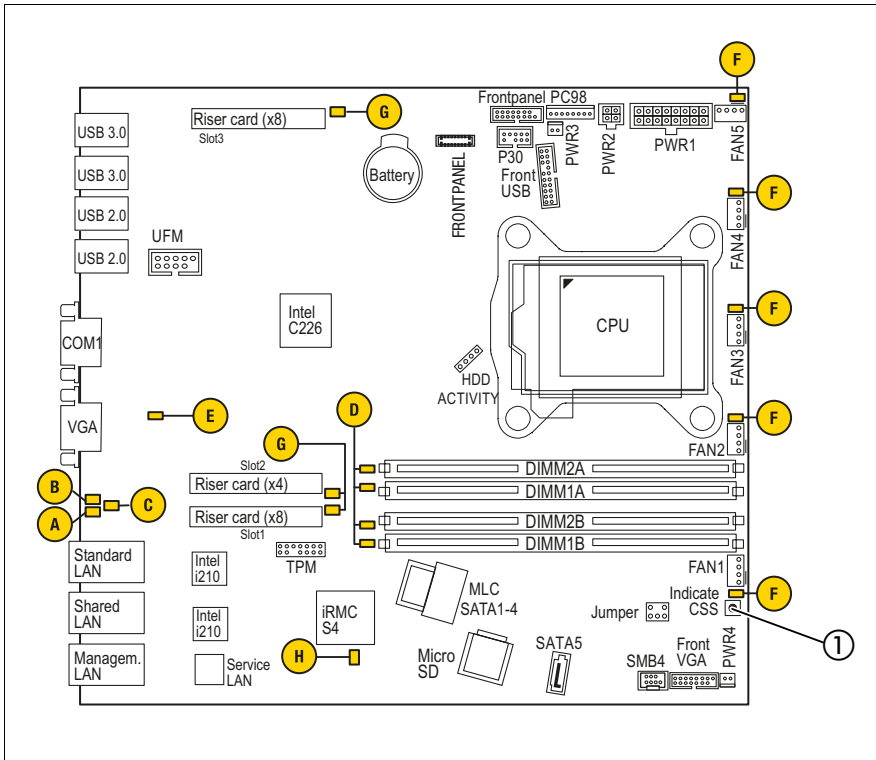


Figure 225: Onboard indicators and Indicate CSS button

No.	Description
1	Indicate CSS button



LEDs A, B and C are visible from outside on the server rear. All other LEDs are only visible if the server cover has been opened.

If the server has been powered off (power plugs must be disconnected) it is possible to indicate the faulty component by pressing the indicate CSS button.

The LEDs have the following meaning:

LED	Indicator	Meaning
A - CSS (Customer Self Service)	off	no error (CSS component)
	orange on	indicates a prefailure (CSS component)
	orange flashing	indicates a failure (CSS component)
B - GEL (Global Error LED)	off	no error (non CSS component)
	orange on	indicates a prefailure (non CSS component)
	orange flashing	indicates a failure of a non CSS component. Reasons for a failure may be: <ul style="list-style-type: none"> – over temperature measured by one of the sensors – sensor is defective – CPU error – software detected an error
C - Identification	blue on	server has been highlighted using iRMC web frontend, ServerView Operations Manager or the ID button on the front panel for easy identification
	blue flashing	local monitor off
D - Memory	off	memory module running
	orange on	memory module failure
E - AUX power	off	
	orange on	voltages okay
F - System fan	off	system fan running
	orange on	system fan failure
G - PCI card	off	PCI card okay
	orange on	PCI card failure (PCI card installed on riser card)
H - iRMC	off	iRMC S4 inactive
	green flashing	iRMC S4 okay

16.2.1.3 I/O panel connectors

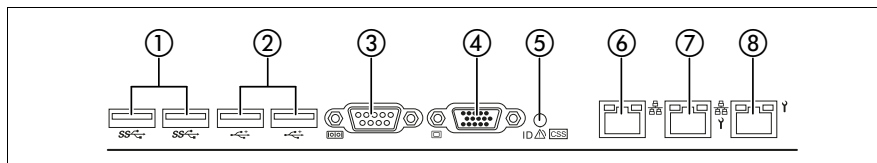


Figure 226: Connector panel

No.	Description
1	2x USB 3.0 connectors
2	2x USB 2.0 connectors
3	Serial connector COM1 (can be used as default interface or to communicate with the iRMC S4)
4	Video connector (VGA)
5	Error indicator (orange), ID indicator (blue); (description see preceding section)
6	Standard LAN connector; this connector is displayed in BIOS Setup Utility and MAC address label as LAN1
7	Shared LAN connector (for WOL/PXE/iSCSI function); this connector is displayed in BIOS Setup Utility and MAC address label as LAN2
8	Management LAN connector (for iRMC S4 server management function)

16.2.1.4 I/O panel indicators

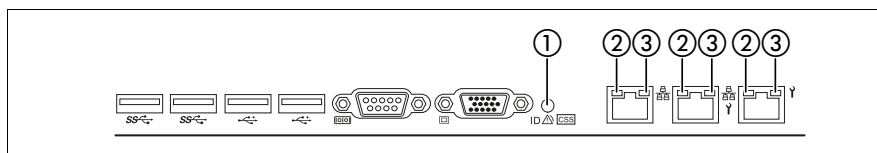


Figure 227: I/O panel indicators

Indicator	Status	Description	
1	Error indicator	off	no critical event
		orange on	prefailure detected
		orange flashing	component failure

Indicator		Status	Description
1	ID indicator	blue on	server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification
		blue flashing	local monitor off
2	LAN link / transfer indicator	green on	LAN connection established
		off	no LAN connection
		green flashing	data transfer in progress
3	LAN speed indicator	yellow on	traffic a transfer rate of 1 Gbit/s
		green on	traffic a transfer rate of 100 Mbit/s
		off	traffic a transfer rate of 10 Mbit/s

16.2.1.5 Indicators on hot-plug power supply units (slide-in units)

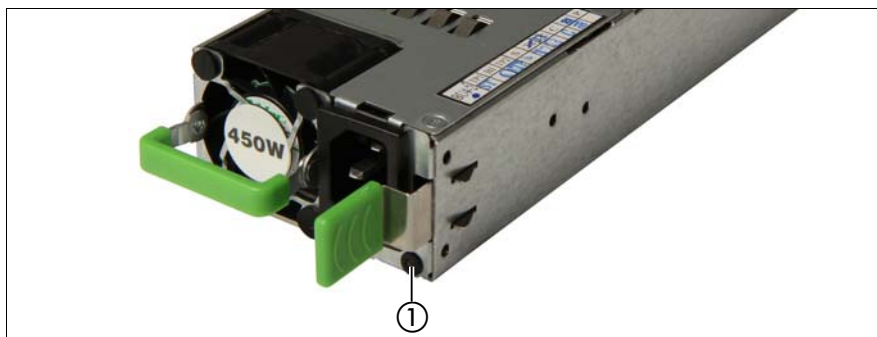


Figure 228: Indicator on the hot-plug power supply unit

Indicator	Status	Description
Status indicator	green flashing	power supply unit operational (standby mode)
	green on	power supply unit operational (server operating)
	orange on	power supply unit failure

16.2.2 Indicators on the front panel

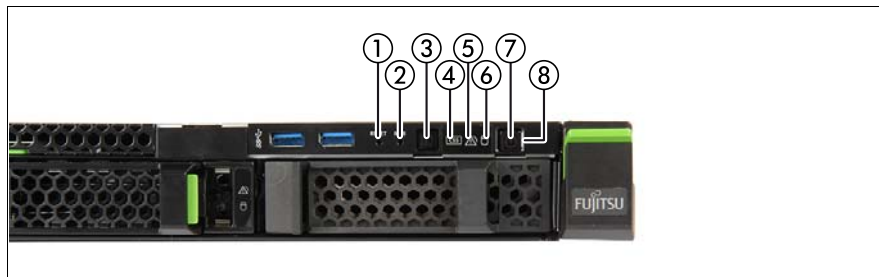


Figure 229: Indicators on the front panel module

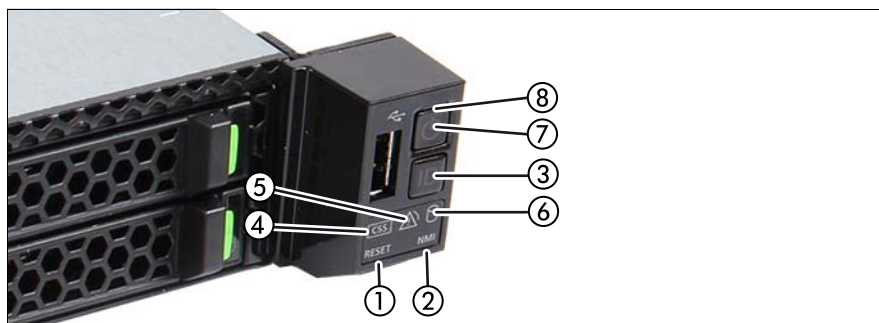


Figure 230: Indicators on the front panel on QRL

1	Reset button
2	NMI button
3	ID button / ID indicator
4	CSS indicator (orange)
5	Global Error indicator (orange)
6	HDD / SSD activity indicator
7	On/Off button / power-on indicator
8	Power-off indicator (AC connected); near by the On/Off button



The meaning of the buttons is described in the corresponding operating manual.

Status indicators

Pos.	Indicator	Status	Description
3	ID indicator	blue on	server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification
		blue flashing	local monitor off
4	CSS indicator	off	no critical event (CSS component)
		orange on	prefailure detected (CSS component)
		orange flashing	CSS component failure
5	Global Error indicator	off	no critical event (non CSS component)
		orange on	prefailure detected (non CSS component)
		orange flashing	indicates a failure of a non CSS component. Reasons for a failure may be: <ul style="list-style-type: none"> – over temperature measured by one of the sensors – sensor is defective – CPU error – software detected an error
6	HDD / SSD activity indicator	green on	data access in progress
7	Power-on indicator	off	is off in the following case: <ul style="list-style-type: none"> – the system is in power-off mode but connected to the mains (AC connected)
		green on	is on in the following cases: <ul style="list-style-type: none"> – the system has been switched on and is in power-on delay – the system is powered on and in normal operation (S0)
		flashes slowly (1/2 Hz)	iRMC S4 is not ready

Pos.	Indicator	Status	Description
8	Power-off indicator (AC connected)	green on	<p>is on in the following cases:</p> <ul style="list-style-type: none"> – the system is in power-off mode but connected to the mains (AC connected) – the system has been switched on and is in power-on delay <p>i After connecting the server to the mains it takes about 60 seconds until the server enters the standby mode.</p>
		off	<p>is off in the following cases:</p> <ul style="list-style-type: none"> – the system is not connected to the mains – the system is powered on and in normal operation (S0)

16.2.3 Indicators on the accessible drives/components

Optical drive activity indicator

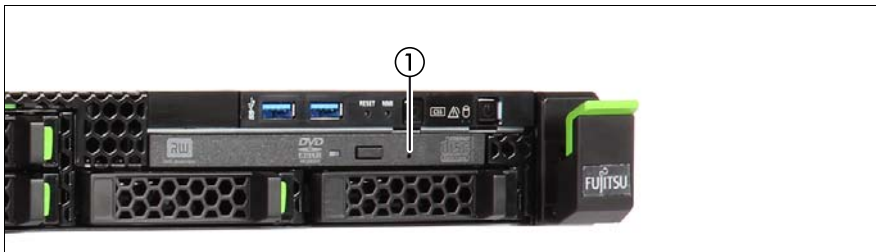


Figure 231: Indicator on the optical drive

Pos.	Indicator	Status	Description
1	Activity indicator	off	optical drive inactive
		green on	storage medium is being accessed

Indicators on the hot-plug HDD module

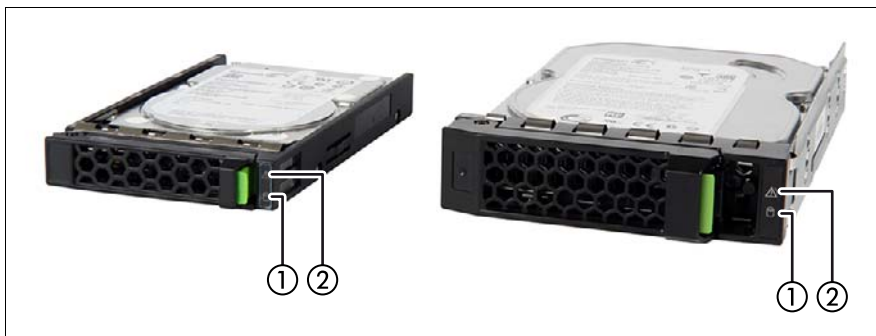


Figure 232: Indicators on the hot-plug HDD module

Pos.	Indicator	Status	Description
1	HDD BUSY	off	HDD inactive
		green on	HDD in active phase (drive active, drive being accessed)
2	HDD FAULT	off	no HDD error
		orange on	HDD faulty or rebuild stopped (drive defective/needs replacing, a rebuild process was stopped or the HDD module is not correctly inserted)
		orange slow flashing	HDD rebuild (the data is being restored after changing a drive)

16.3 Onboard settings

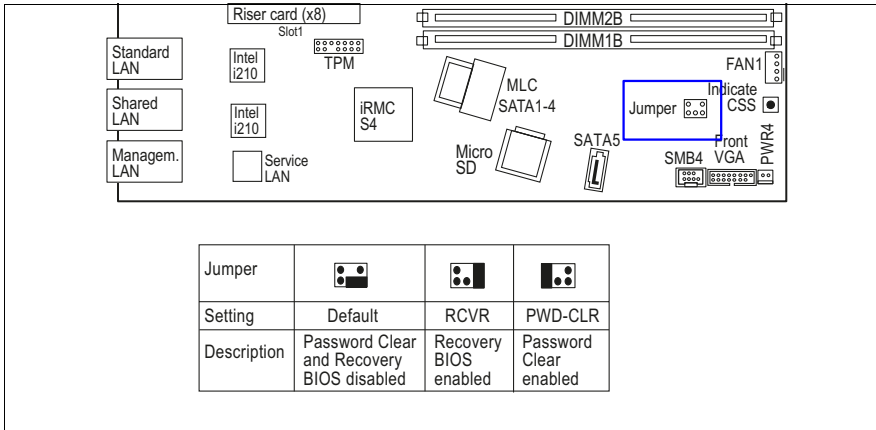


Figure 233: Jumper

Print	Setting
PWD-CLR	open: normal operation (default) short: clear password and apply the default BIOS settings
RCVR	1-2 normal operation (default) 2-3 recovery mode

16.4 Minimum startup configuration



Field Replaceable Units (FRU)

If the server does not start up or other problems occur, it may be necessary to take the system down to its most basic configuration in order to isolate the defective component.

The minimum startup configuration consists of the following components and cables:

Component	Notes
System board	no TPM, UFM or expansion cards installed
CPU with CPU heat sink	
1 memory module	installed in DIMM slot 1A
Front panel module	
Power supply unit	

Table 5: Minimum startup configuration - components

Cable	Notes
Front panel cable	
Power cable	

Table 6: Minimum startup configuration - cables

- ▶ ["Shutting down the server" on page 45](#)
- ▶ ["Disconnecting the server from the mains" on page 46](#)
- ▶ Take the system down to its minimum startup configuration.
- ▶ ["Connecting the server to the mains" on page 55](#)
- ▶ Connect a keyboard, mouse and display to the server.
- ▶ Switch on the server as described in section ["Switching on the server" on page 57](#).

**CAUTION!**

Since the fan module is not included in the minimum startup configuration, the server must be shut down immediately after the diagnostic process is complete (POST phase has been passed).

The minimum startup configuration must be used exclusively for diagnostic purposes by maintenance personnel, never in daily operation!

