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.

Documentation creation according to DIN EN ISO 9001:2015

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 9001:2015.

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

Copyright and Trademarks

Copyright © 2018 Fujitsu Technology Solutions GmbH.

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

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

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

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

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

For your safety

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

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

Radio interference

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

Aluminum electrolytic capacitors

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

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

High safety use

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

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

The device has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk of life or body if such safety cannot be assured.
These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

**Measures against momentary voltage drop**

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

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

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

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

**Harmonic Current Standards**

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

**Only for the Japanese market: About SATA hard disk drives**

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

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

http://jp.fujitsu.com/platform/server/primergy/harddisk/
Only for the Japanese market:

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

- CSS (Customer Self Service)
## Version history

<table>
<thead>
<tr>
<th>Issue number</th>
<th>Reason for update</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0 / November 2018</td>
<td>Update chapters 2, 5 and 6</td>
</tr>
</tbody>
</table>
## Contents

1 Introduction ................................................. 17

1.1 Notational conventions ............................... 18

2 Before you start ........................................... 19

2.1 Classification of procedures ....................... 21
   2.1.1 Customer Replaceable Units (CRU) .............. 21
   2.1.2 Upgrade and Repair Units (URU) ............... 22
   2.1.3 Field Replaceable Units (FRU) .................. 23

2.2 Average task duration ................................. 24

2.3 Tools you need at hand ............................... 25

2.4 Documents you need at hand .......................... 26

3 Important information ................................. 29

3.1 Safety instructions ................................... 29

3.2 CE conformity ........................................... 36

3.3 FCC Class A Compliance Statement ................. 37

3.4 Environmental protection ............................ 38

4 Basic hardware procedures .............................. 41

4.1 Using diagnostics information ....................... 41
   4.1.1 Accessing the management blade web interface .... 41
   4.1.2 Locating the defective server blade .............. 43
   4.1.3 Determining the error class .................... 44
   4.1.3.1 Global Error indicator ...................... 45
   4.1.3.2 Customer Self Service (CSS) indicator ......... 46
   4.1.4 Locating the defective component .............. 47

4.2 Shutting down the server blade ....................... 50
## Contents

4.3 Removing a server blade .............................................. 51
   4.3.1 Preliminary steps ............................................. 51
   4.3.2 Removing the server blade from the system unit ......... 52
4.4 Opening the server blade ........................................... 53
4.5 Closing the server blade ........................................... 54
4.6 Installing the server blade in the system unit ............... 55
4.7 Switching on the server blade ..................................... 58
4.8 Concluding software tasks .......................................... 59

5 Basic software procedures ........................................... 61
   5.1 Starting the maintenance task .................................. 61
      5.1.1 Launching a video redirection to a server blade .... 61
      5.1.2 Checking the server blade status ....................... 61
         5.1.2.1 Checking the server blade status via management
                     blade web interface .................................. 61
         5.1.2.2 Checking the server blade status via iRMC ........ 62
      5.1.3 Saving BIOS settings ...................................... 63
      5.1.4 Saving iRMC settings ...................................... 63
      5.1.5 Connecting virtual media to the managed server blade . 64
      5.1.6 Suspending BitLocker functionality .................... 65
      5.1.7 Disabling boot watchdog functionality .................. 66
         5.1.7.1 Viewing boot watchdog settings ................. 66
         5.1.7.2 Configuring boot watchdog settings ............ 67
      5.1.8 Verifying and configuring the backup software solution . 68
      5.1.9 Note on server maintenance in a Multipath I/O environment . 68
      5.1.10 Switching on the ID indicator ......................... 71
   5.2 Completing the maintenance task .............................. 72
      5.2.1 Updating or recovering the system board BIOS and iRMC .... 72
         5.2.1.1 Updating or recovering the system board BIOS ... 72
         5.2.1.2 Updating or recovering the iRMC ................. 75
      5.2.2 Restoring BIOS settings .................................. 78
      5.2.3 Restoring iRMC settings .................................. 79
      5.2.4 Updating mezzanine card firmware ...................... 79
      5.2.5 Enabling Option ROM scan ................................ 81
      5.2.6 Verifying and configuring the backup software solution .... 82
5.2.7  Resetting the boot retry counter ........................................ 83
5.2.7.1  Viewing the boot retry counter .................................... 83
5.2.7.2  Resetting the boot retry counter .................................. 83
5.2.8  Resetting the error status after replacing memory modules or processors ......................................................... 84
5.2.8.1  Memory modules ......................................................... 84
5.2.8.2  Processors .............................................................. 86
5.2.9  Enabling boot watchdog functionality ................................. 87
5.2.10  Enabling replaced components in the system BIOS .............. 88
5.2.11  Verifying the memory mode .......................................... 89
5.2.12  Verifying the system time settings ................................... 90
5.2.13  Viewing and clearing the System Event Log (SEL) ............... 91
5.2.13.1  Viewing the SEL ..................................................... 91
5.2.13.2  Saving the SEL ...................................................... 92
5.2.13.3  Clearing the SEL .................................................... 93
5.2.14  Updating the NIC configuration file in a Linux environment ... 93
5.2.15  Resuming BitLocker functionality .................................... 94
5.2.16  Performing a RAID array rebuild ................................... 95
5.2.17  Looking up changed MAC / WWN addresses ...................... 96
5.2.17.1  Looking up MAC addresses ....................................... 96
5.2.17.2  Looking up WWN addresses ...................................... 97
5.2.18  Using the Chassis ID Prom Tool ..................................... 97
5.2.19  Configuring LAN teaming ............................................. 98
5.2.19.1  After replacing / upgrading LAN/CNA controllers ............ 98
5.2.19.2  After replacing the server blade ................................ 98
5.2.20  Switching off the ID indicator ...................................... 99

6  Solid state drives ................................................................. 101

6.1  Basic information ............................................................. 101

6.2  Installing SSDs ................................................................. 102
6.2.1  Preliminary steps .......................................................... 102
6.2.2  Location of the drive modules inside the server blade .......... 103
6.2.3  Mounting the SSDs into their frames ............................... 105
6.2.4  Installing the drive module onto the mounting platform ........ 107
6.2.5  Concluding steps .......................................................... 108

6.3  Removing SSDs ................................................................. 109
6.3.1  Preliminary steps .......................................................... 109
6.3.2  Removing an SSD .......................................................... 110
6.3.3  Concluding steps .......................................................... 112
## Contents

6.4 Replacing SSDs ............................ 113
  6.4.1 Preliminary steps ......................... 113
  6.4.2 Removing an SSD .......................... 113
  6.4.3 Installing an SSD ......................... 114
  6.4.4 Concluding steps .......................... 114

6.5 Replacing SAS / PCH mounting frames .......... 115
  6.5.1 Preliminary steps ......................... 115
  6.5.2 Removing the mounting frame ............... 115
  6.5.3 Installing the mounting frame ............... 115
  6.5.4 Concluding steps .......................... 116

6.6 M.2 SSDs ................................ 117

6.7 Basic information .......................... 117

6.8 Installing M.2 SSDs .......................... 117
  6.8.1 Preliminary steps ......................... 117
  6.8.2 Location of the M.2 SSDs ................. 118
  6.8.3 Mounting the M.2 SSDs onto their backplanes 118
  6.8.4 Installing the first M.2 SSD ............... 120
  6.8.5 Installing the second M.2 SSD .............. 121
  6.8.6 Concluding steps .......................... 121

6.9 Removing M.2 SSDs .......................... 122
  6.9.1 Preliminary steps ......................... 122
  6.9.2 Removing the M.2 SSDs ................. 123
  6.9.3 Removing the second M.2 SSD .............. 123
  6.9.4 Concluding steps .......................... 124

6.10 Replacing M.2 SSDs .......................... 124
  6.10.1 Preliminary steps ......................... 124
  6.10.2 Removing an M.2 SSD ...................... 125
  6.10.3 Installing an M.2 SSD .................... 125
  6.10.4 Concluding steps .......................... 125

7 Mezzanine cards ............................... 127

7.1 Basic information ............................ 128
  7.1.1 Installing riser cards ..................... 130
  7.1.2 Removing riser cards ...................... 132
  7.1.3 Population rules for mezzanine cards ....... 134
### Contents

#### 7.2 Installing mezzanine cards
- Preliminary steps ........................................ 140
- Installing a mezzanine card ............................. 141
- Concluding steps ........................................ 145

#### 7.3 Removing mezzanine cards
- Preliminary steps ........................................ 146
- Removing a mezzanine card ............................. 147
- Concluding steps ........................................ 149

#### 7.4 Replacing mezzanine cards
- Preliminary steps ........................................ 150
- Removing a mezzanine card ............................. 150
- Installing a mezzanine card ............................ 150
- Concluding steps ........................................ 151

#### 8 Main memory

##### 8.1 Basic information
- Memory sequence ........................................ 154
- Population rules ........................................ 154
- Independent Channel Mode ............................ 156
- Mirrored Channel and Performance Modes ............ 158
- Rank Sparing Mode .................................... 159

##### 8.2 Installing memory modules
- Preliminary steps ........................................ 164
- Installing a memory module ........................... 164
- Concluding steps ........................................ 166

##### 8.3 Removing memory modules
- Preliminary steps ........................................ 167
- Removing a memory module ............................ 168
- Concluding steps ........................................ 168

##### 8.4 Replacing memory modules
- Preliminary steps ........................................ 170
- Removing a memory module ............................ 170
- Installing a memory module ............................ 170
- Concluding steps ........................................ 171

##### 8.5 Usage of dummy DIMM modules

---

BX2580 M2 Upgrade and Maintenance Manual
Contents

8.6 Handling of memory air cowls ..................................... 173
  8.6.1 Basic information ............................................ 173
  8.6.2 Installing the air cowls ....................................... 174
  8.6.3 Removing the air cowls ....................................... 175

9 Processors .......................................................... 177
  9.1 Basic information .................................................. 177
  9.2 Installing processors ............................................. 178
    9.2.1 Preliminary steps ........................................... 178
    9.2.2 Installing a processor ....................................... 179
    9.2.3 Concluding steps ........................................... 186
  9.3 Removing processors ............................................ 187
    9.3.1 Preliminary steps ........................................... 187
    9.3.2 Removing a processor ....................................... 188
    9.3.3 Concluding steps ........................................... 197
  9.4 Upgrading or replacing processors ............................... 198
    9.4.1 Preliminary steps ........................................... 198
    9.4.2 Upgrading or replacing a processor ......................... 199
    9.4.3 Concluding steps ........................................... 199
  9.5 Handling processor heat sinks ................................... 200
    9.5.1 Preliminary steps ........................................... 200
    9.5.2 Installing processor heat sinks ............................. 201
      9.5.2.1 Preparing heat sink and processor ...................... 203
      9.5.2.2 Installing the heat sink for CPU 1 ..................... 204
      9.5.2.3 Installing the heat sink for CPU 2 ..................... 205
    9.5.3 Removing processor heat sinks ................................ 207
    9.5.4 Removing the "dummy heat sink" of CPU 2 .................. 208
    9.5.5 Replacing processor heat sinks ................................ 209
      9.5.5.1 Removing the processor heat sink ...................... 209
      9.5.5.2 Applying thermal paste .................................. 209
      9.5.5.3 Installing the processor heat sink ..................... 209
    9.5.6 Concluding steps ........................................... 209
  9.6 Applying thermal paste .......................................... 210
## 10 System board components

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Basic information</td>
<td>213</td>
</tr>
<tr>
<td>10.2</td>
<td>Replacing the CMOS battery</td>
<td>214</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Preliminary steps</td>
<td>214</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Replacing the battery</td>
<td>215</td>
</tr>
<tr>
<td>10.2.3</td>
<td>Concluding steps</td>
<td>217</td>
</tr>
<tr>
<td>10.3</td>
<td>USB Flash Module (UFM)</td>
<td>218</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Installing the UFM</td>
<td>218</td>
</tr>
<tr>
<td>10.3.1.1</td>
<td>Preliminary steps</td>
<td>218</td>
</tr>
<tr>
<td>10.3.1.2</td>
<td>Installing the UFM</td>
<td>219</td>
</tr>
<tr>
<td>10.3.1.3</td>
<td>Concluding steps</td>
<td>221</td>
</tr>
<tr>
<td>10.3.1.4</td>
<td>Software configuration</td>
<td>222</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Removing the UFM</td>
<td>223</td>
</tr>
<tr>
<td>10.3.2.1</td>
<td>Preliminary steps</td>
<td>223</td>
</tr>
<tr>
<td>10.3.2.2</td>
<td>Removing the UFM</td>
<td>224</td>
</tr>
<tr>
<td>10.3.2.3</td>
<td>Concluding steps</td>
<td>224</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Replacing the UFM</td>
<td>225</td>
</tr>
<tr>
<td>10.3.3.1</td>
<td>Preliminary steps</td>
<td>225</td>
</tr>
<tr>
<td>10.3.3.2</td>
<td>Removing the UFM</td>
<td>226</td>
</tr>
<tr>
<td>10.3.3.3</td>
<td>Re-installing the UFM</td>
<td>227</td>
</tr>
<tr>
<td>10.3.3.4</td>
<td>Concluding steps</td>
<td>229</td>
</tr>
<tr>
<td>10.3.3.5</td>
<td>Software configuration</td>
<td>229</td>
</tr>
<tr>
<td>10.4</td>
<td>Trusted Platform Module (TPM)</td>
<td>230</td>
</tr>
<tr>
<td>10.4.1</td>
<td>Installing the TPM</td>
<td>230</td>
</tr>
<tr>
<td>10.4.1.1</td>
<td>Preliminary steps</td>
<td>230</td>
</tr>
<tr>
<td>10.4.1.2</td>
<td>Installing the TPM</td>
<td>231</td>
</tr>
<tr>
<td>10.4.1.3</td>
<td>Concluding steps</td>
<td>234</td>
</tr>
<tr>
<td>10.4.2</td>
<td>Removing the TPM</td>
<td>236</td>
</tr>
<tr>
<td>10.4.2.1</td>
<td>Preliminary steps</td>
<td>237</td>
</tr>
<tr>
<td>10.4.2.2</td>
<td>Removing the TPM</td>
<td>238</td>
</tr>
<tr>
<td>10.4.2.3</td>
<td>Concluding steps</td>
<td>239</td>
</tr>
<tr>
<td>10.4.3</td>
<td>Replacing the TPM</td>
<td>240</td>
</tr>
<tr>
<td>10.4.3.1</td>
<td>Preliminary steps</td>
<td>241</td>
</tr>
<tr>
<td>10.4.3.2</td>
<td>Removing the TPM</td>
<td>241</td>
</tr>
<tr>
<td>10.4.3.3</td>
<td>Re-installing the TPM</td>
<td>241</td>
</tr>
<tr>
<td>10.4.3.4</td>
<td>Concluding steps</td>
<td>241</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5</td>
<td><strong>SATA DOM</strong></td>
<td>242</td>
</tr>
<tr>
<td>10.5.1</td>
<td>Installing the SATA DOM</td>
<td>242</td>
</tr>
<tr>
<td>10.5.1.1</td>
<td>Preliminary steps</td>
<td>242</td>
</tr>
<tr>
<td>10.5.1.2</td>
<td>Mounting the SATA-DOM</td>
<td>243</td>
</tr>
<tr>
<td>10.5.1.3</td>
<td>Concluding steps</td>
<td>245</td>
</tr>
<tr>
<td>10.5.2</td>
<td>Removing the SATA-DOM</td>
<td>246</td>
</tr>
<tr>
<td>10.5.2.1</td>
<td>Preliminary steps</td>
<td>246</td>
</tr>
<tr>
<td>10.5.2.2</td>
<td>Removing the SATA DOM</td>
<td>247</td>
</tr>
<tr>
<td>10.5.2.3</td>
<td>Concluding steps</td>
<td>247</td>
</tr>
<tr>
<td>10.5.3</td>
<td>Replacing the SATA-DOM</td>
<td>248</td>
</tr>
<tr>
<td>10.5.3.1</td>
<td>Preliminary steps</td>
<td>248</td>
</tr>
<tr>
<td>10.5.3.2</td>
<td>Removing the SATA DOM</td>
<td>248</td>
</tr>
<tr>
<td>10.5.3.3</td>
<td>Installing the SATA DOM</td>
<td>248</td>
</tr>
<tr>
<td>10.5.3.4</td>
<td>Concluding steps</td>
<td>248</td>
</tr>
<tr>
<td>10.6</td>
<td><strong>iRMC microSD card</strong></td>
<td>250</td>
</tr>
<tr>
<td>10.6.1</td>
<td>Installing the iRMC microSD card</td>
<td>250</td>
</tr>
<tr>
<td>10.6.1.1</td>
<td>Preliminary steps</td>
<td>250</td>
</tr>
<tr>
<td>10.6.1.2</td>
<td>Installing the iRMC microSD card</td>
<td>251</td>
</tr>
<tr>
<td>10.6.1.3</td>
<td>Concluding steps</td>
<td>252</td>
</tr>
<tr>
<td>10.6.2</td>
<td>Removing the iRMC microSD card</td>
<td>252</td>
</tr>
<tr>
<td>10.6.2.1</td>
<td>Preliminary steps</td>
<td>252</td>
</tr>
<tr>
<td>10.6.2.2</td>
<td>Removing the iRMC microSD card</td>
<td>253</td>
</tr>
<tr>
<td>10.6.2.3</td>
<td>Concluding steps</td>
<td>253</td>
</tr>
<tr>
<td>10.6.3</td>
<td>Replacing the iRMC microSD card</td>
<td>254</td>
</tr>
<tr>
<td>10.6.3.1</td>
<td>Preliminary steps</td>
<td>254</td>
</tr>
<tr>
<td>10.6.3.2</td>
<td>Replacing the iRMC microSD card</td>
<td>254</td>
</tr>
<tr>
<td>10.6.3.3</td>
<td>Concluding steps</td>
<td>254</td>
</tr>
<tr>
<td>10.7</td>
<td><strong>Replacing the system board</strong></td>
<td>255</td>
</tr>
<tr>
<td>10.7.1</td>
<td>Preliminary steps</td>
<td>256</td>
</tr>
<tr>
<td>10.7.2</td>
<td>Removing the system board</td>
<td>257</td>
</tr>
<tr>
<td>10.7.3</td>
<td>Installing the system board</td>
<td>259</td>
</tr>
<tr>
<td>10.7.4</td>
<td>Concluding steps</td>
<td>261</td>
</tr>
</tbody>
</table>

| 11      | **Server blade**                           | 263  |
| 11.1    | **Replacing the server blade**             | 263  |
| 11.1.1  | Preliminary steps                          | 263  |
| 11.1.2  | Replacing steps                            | 264  |
| 11.1.3  | Concluding steps                           | 265  |
12 Appendix .......................................................... 267

12.1 Mechanical overview ........................................ 267
  12.1.1 Server blade front ........................................ 267
  12.1.2 Server blade interior ...................................... 268

12.2 Configuration tables .......................................... 269
  12.2.1 Memory configuration table .............................. 269
  12.2.2 Mezzanine card configuration table .................... 269

12.3 Connectors and indicators ................................... 270
  12.3.1 Connectors and indicators on the system board ...... 270
    12.3.1.1 Onboard connectors ................................ 270
    12.3.1.2 Onboard settings .................................... 271
    12.3.1.3 Onboard indicators and controls .................. 272
  12.3.2 Connectors and indicators on the front panel ....... 275
    12.3.2.1 Front panel connectors .............................. 275
    12.3.2.2 Front panel indicators .............................. 276

12.4 Minimum startup configuration ............................. 279
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 26.

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 21.
Introduction

1.1 Notational conventions

The following notational conventions are used in this manual:

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text in italics</td>
<td>indicates commands or menu items</td>
</tr>
<tr>
<td>fixed font</td>
<td>indicates system output</td>
</tr>
<tr>
<td>semi-bold fixed font</td>
<td>indicates text to be entered by the user</td>
</tr>
<tr>
<td>&quot;Quotation marks&quot;</td>
<td>indicate names of chapters and terms that are being emphasized</td>
</tr>
<tr>
<td>★</td>
<td>describes activities that must be performed in the order shown</td>
</tr>
<tr>
<td>Abc</td>
<td>indicates keys on the keyboard</td>
</tr>
<tr>
<td>CAUTION!</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>indicates additional information, notes and tips</td>
</tr>
<tr>
<td></td>
<td>indicates the procedure category in terms of complexity and qualification requirements, see &quot;Classification of procedures&quot; on page 21</td>
</tr>
<tr>
<td></td>
<td>indicates the average task duration, see &quot;Average task duration&quot; on page 24</td>
</tr>
</tbody>
</table>
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 29.
- Make sure that all necessary manuals are available. Refer to the documentation overview in section "Documents you need at hand" on page 26. Print the PDF files if required.
- Make yourself familiar with the procedure categories introduced in section "Classification of procedures" on page 21.
- Ensure that all required tools are available according to section "Tools you need at hand" on page 25.

Installing optional components

The "FUJITSU Server PRIMERGY BX2580 M2 Server Blade Operating manual" gives an introduction to server features and provides an overview of available hardware options.

Use the Fujitsu ServerView Suite management software to prepare hardware expansions. ServerView Suite documentation is available online at http://manuals.ts.fujitsu.com (http://jp.fujitsu.com/platform/server/primergy/manual/ for the Japanese market). Please refer to the following ServerView Suite topics:

- Operation
- Virtualization
- Maintenance

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

for the global market:

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 (global market only).
Before you start

Replacing a defective component

The global error indicators on the front side of the server blade as well as local diagnostic LEDs on the front panel report defective hardware components that need to be replaced. For further information on the controls and indicators of your server, refer to the "FUJITSU Server PRIMERGY BX2580 M2 Server Blade Operating Manual" and section "Connectors and indicators" on page 270.

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 41 and "Connectors and indicators on the front panel" on page 275.

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

– No hot-plug modules inside BX2580 M2
Before you start

2.1.2 Upgrade and Repair Units (URU)

Upgrade and Repair Units (URU)

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

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

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

**CAUTION!**

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

Components that are handled as Upgrade Units

- Processors (upgrade kits)
- Mezzanine cards
- Memory modules
- iRMC microSD card

Components that are handled solely as Repair Units

- CMOS battery
- Non hot-plug solid state drives
2.1.3 Field Replaceable Units (FRU)

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

CAUTION!

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

Components that are handled as Field Replaceable Units

- Processors (replacements)
- Memory modules
- Mezzanine cards
- SAS / PCH mounting frames
- Non-hot-plug SSD modules
- Trusted Platform Module (TPM)
- USB Flash Module (UFM)
- SATA DOM
- iRMC microSD card

Components that are handled solely as Repair Units

- CMOS battery

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 [table 1 on page 24](#) for an overview of steps taken into account for calculating the average task duration:

<table>
<thead>
<tr>
<th>Step</th>
<th>included</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server shutdown</td>
<td>no</td>
<td>Shutdown time depends on hardware and software configuration and may vary significantly. Software tasks necessary before maintenance are described in section &quot;Starting the maintenance task&quot; on page 61&quot;.</td>
</tr>
<tr>
<td>System unit removal, disassembly</td>
<td>yes</td>
<td>Making the server blade available, removing the server blade from the system unit.</td>
</tr>
<tr>
<td>Transport</td>
<td>no</td>
<td>Transporting the server blade to the service table (where required) depends on local customer conditions.</td>
</tr>
<tr>
<td>Maintenance procedures</td>
<td>yes</td>
<td>Maintenance procedures including preliminary and concluding software tasks.</td>
</tr>
<tr>
<td>Transport</td>
<td>no</td>
<td>Returning the server blade to its installation site (where required) depends on local customer conditions.</td>
</tr>
<tr>
<td>Assembly, system unit installation</td>
<td>yes</td>
<td>Reassembling the server blade, installing the server blade in the system unit.</td>
</tr>
<tr>
<td>Starting up</td>
<td>no</td>
<td>Booting time depends on hardware and software configuration and may vary significantly.</td>
</tr>
</tbody>
</table>

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.

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

Table 2: List of required tools and used screws
### Before you start

<table>
<thead>
<tr>
<th>Screw driver / Bit insert</th>
<th>Screw</th>
<th>Usage</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phillips PH1 / (+) No. 1</td>
<td></td>
<td>UFM and SATA DOM nylon screw</td>
<td>M3 x 4.5 mm (white) A3C40109082</td>
</tr>
<tr>
<td>Phillips PH2 / (+) No. 2</td>
<td></td>
<td>Foot mounting rail screws</td>
<td>M4 x 6 mm Combination screw (silver) C26192-Y10-C113</td>
</tr>
<tr>
<td>Phillips PH0 / (+) No. 0</td>
<td></td>
<td>M.2 SSDs</td>
<td>M2 x 3.1 mm (silver)</td>
</tr>
<tr>
<td>Phillips PH1 / (+) No. 1</td>
<td></td>
<td>M.2 SSDs</td>
<td>M3 3.3 mm (black)</td>
</tr>
</tbody>
</table>

Table 2: List of required tools and used screws

#### 2.4 Documents you need at hand

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

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

- Unless stated otherwise, all manuals are available online at [http://manuals.ts.fujitsu.com](http://manuals.ts.fujitsu.com) under *Industry standard servers*.

For the Japanese market please use the following address: [http://jp.fujitsu.com/platform/server/primergy/manual/](http://jp.fujitsu.com/platform/server/primergy/manual/)
### Before you start

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Safety notes and regulations&quot; manual&lt;br&gt;&quot;安全上のご注意 &quot; for the Japanese market</td>
<td>Important safety information, available online or as a printed copy</td>
</tr>
<tr>
<td>&quot;FUJITSU Server PRIMERGY BX2580 M2 Server Blade&quot; Operating Manual</td>
<td>Available online</td>
</tr>
<tr>
<td>&quot;D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2&quot; Reference Manual</td>
<td>Information on configurable BIOS options and parameters, available online</td>
</tr>
<tr>
<td>System board and service labels</td>
<td>Labels inside the side / top server cover outlining connectors, indicators and basic maintenance tasks</td>
</tr>
<tr>
<td>Illustrated Spares catalog</td>
<td>Spare parts identification and information system (global market only), available for online use or download (Windows OS) at <a href="http://manuals.ts.fujitsu.com/illustrated_spares">http://manuals.ts.fujitsu.com/illustrated_spares</a> or from the CSS component view of the ServerView Operations Manager</td>
</tr>
<tr>
<td>Glossary</td>
<td>Available online</td>
</tr>
</tbody>
</table>

Table 3: Documents you need at hand
### Before you start

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Warranty&quot; manual</td>
<td>Important information on warranty regulations, recycling and service, available online or as a printed copy</td>
</tr>
<tr>
<td>&quot;保証書&quot; for the Japanese market</td>
<td></td>
</tr>
<tr>
<td>&quot;Returning used devices&quot; manual</td>
<td></td>
</tr>
<tr>
<td>&quot;Service Desk&quot; leaflet</td>
<td>Recycling and contact information, available online or as a printed copy</td>
</tr>
<tr>
<td>&quot;サポート＆サービス&quot; for the Japanese market</td>
<td></td>
</tr>
</tbody>
</table>

**Additional documentation**
- "iRMC S4" user guide available online
- RAID documentation, available online at [http://manuals.ts.fujitsu.com](http://manuals.ts.fujitsu.com) under *Industry standard servers - Expansion Cards - Storage Adapters*
- Rack documentation

**Third party documentation**
- Operating system documentation, online help
- Peripherals documentation

Table 3: Documents 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 Fujitsu Advanced Thermal Design the ambient temperature can increase to 40 °C.

- If the unit is integrated into an installation that draws power from an industrial power supply network with an IEC309 connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for type B connectors.

- The unit automatically adjusts itself to a mains voltage in a range of 100 VAC to 240 VAC. Ensure that the local mains voltage lies within these limits.

- This device must only be connected to properly grounded power outlets or connected to the grounded rack internal power distribution system with tested and approved power cords.

- Ensure that the device is connected to a properly grounded power outlet close to the device.

- Ensure that the power sockets on the device and the properly grounded power outlets are easily accessible.

- The On/Off button or the main power switch (if present) does not isolate the device from the mains power supply. In case of repair or servicing disconnect the device completely from the mains power supply, unplug all power plugs from the properly grounded power outlets.

- Always connect the server and the attached peripherals to the same power circuit. Otherwise you run the risk of losing data if, for example, the server is still running but a peripheral device (e.g. memory subsystem) fails during a power outage.

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

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

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

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

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

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

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

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

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

• Only set screen resolutions and refresh rates that are specified in the operating manual for the monitor. Otherwise, you may damage your monitor. If you are in any doubt, contact your sales outlet or customer service center.

• Before installing/removing internal options to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the outlet. Failure to do so can cause electric shock.
Important information

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock and will void the warranty and exempt the manufacturer from all liability.

- Devices inside the server remain hot after shutdown. Wait for a while after shutdown before installing or removing internal options.

- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, if you are wearing an earthing band on your wrist when working with this type of module, connect it to an unpainted, 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
Important information

Working with optical disk drives and media

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

**CAUTION!**

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

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

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

Under certain circumstances, sharp CD/DVD/BD fragments can pierce the cover of the optical disk drive (equipment damage) and can fly out of the device (danger of injury, particularly to uncovered body parts such as the face or neck).

- High humidity and airborne dust levels are to be avoided. Electric shocks and/or server failures may be caused by liquids such as water, or metallic items, such as paper clips, entering a drive.
- Shocks and vibrations are also to be avoided.
- Do not insert any objects other than the specified CDs/DVDs/BDs.
- Do not pull on, press hard, or otherwise handle the CD/DVD/BD tray roughly.
- Do not disassemble the optical disk drive.
- Before use, clean the optical disk tray using a soft, dry cloth.
- As a precaution, remove disks from the optical disk drive when the drive is not to be used for a long time. Keep the optical disk tray closed to prevent foreign matter, such as dust, from entering the optical disk drive.
- Hold CDs/DVDs/BDs by their edges to avoid contact with the disk surface.
Important information

- Do not contaminate the CD/DVD/BD surface with fingerprints, oil, dust, etc. If dirty, clean with a soft, dry cloth, wiping from the center to the edge. Do not use benzene, thinners, water, record sprays, antistatic agents, or silicone-impregnated cloth.
- Be careful not to damage the CD/DVD/BD surface.
- Keep the CDs/DVDs/BDs away from heat sources.
- Do not bend or place heavy objects on CDs/DVDs/BDs.
- Do not write with ballpoint pen or pencil on the label (printed) side.
- When a CD/DVD/BD is moved from a cold place to a warm place, moisture condensation on the CD/DVD/BD surface can cause data read errors. In this case, wipe the CD/DVD/BD with a soft, dry cloth then let it air dry. Do not dry the CD/DVD/BD using devices such as a hair dryer.
- To avoid dust, damage, and deformation, keep the CD/DVD/BD in its case whenever it is not in use.
- Do not store CDs/DVDs/BDs at high temperatures. Areas exposed to prolonged direct sunlight or near heating appliances are to be avoided.

You can prevent damage from the optical disk drive and the CDs/DVDs/BDs, as well as premature wear of the disks, by observing the following suggestions:
- Only insert disks in the drive when needed and remove them after use.
- Store the disks in suitable sleeves.
- Protect the disks from exposure to heat and direct sunlight.

Laser information

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

CAUTION!

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

Never remove parts of the optical disk drive casing!
**Modules with Electrostatic-Sensitive Devices**

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

![Figure 1: ESD label](image)

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

- Switch off the system and remove the power plugs from the power outlets before installing or removing components with ESDs.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, you must wear an earthing band on your wrist when working with this type of module and connect it to an unpainted, conducting metal part of the system.
- Any devices or tools that are used must be free of electrostatic charge.
- Wear a suitable grounding cable that connects you to the external chassis of the system unit.
- Always hold components with ESDs at the edges or at the points marked green (touch points).
- Do not touch any connectors or conduction paths on an ESD.
- Place all the components on a pad which is free of electrostatic charge.

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

Transporting the server

- Only transport the device in its original packaging or in packaging that protects it from impacts and jolts. For the Japanese market, transporting the device in its original packaging does not apply.

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

- Never lift or carry the device by the handles on the front panel.

Notes on installing the server in the rack

- Never lift the server into the rack using the handles on the front panel.

- When connecting and disconnecting cables, observe the relevant instructions in the "Important Information" chapter of the technical manual for the corresponding rack. The technical manual is supplied with the corresponding rack.

- When installing the rack, make sure that the anti-tilt protection is correctly fitted.

- For safety reasons, no more than one unit may be removed from the rack at any one time during installation and maintenance work.

- If several units are simultaneously removed from the rack, there is a risk that the rack could tip over.

- The rack must be connected to the power supply by an authorized specialist (electrician).

- If the server is integrated into an installation that draws power from an industrial power supply network with an IEC309 type connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for the type A connector.

3.2 CE conformity

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

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

NOTE:

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

● Reorient or relocate the receiving antenna.

● Increase the separation between equipment and the receiver.

● Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

● Consult the dealer or an experienced radio/TV technician for help.

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

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

WARNING:

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

Environmentally-friendly product design and development

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

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


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
Important information

Pb Lead

Labels on plastic casing parts

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

Returns, recycling and disposal

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

The device must not be disposed of with domestic waste. This device is labeled in compliance with European directive 2002/96/EC on waste electrical and electronic equipment (WEEE).

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

Details regarding the return and recycling of devices and consumables within Europe can also be found in the "Returning used devices" manual, via your local Fujitsu branch or from our recycling center in Paderborn:

Fujitsu Technology Solutions
Recycling Center
D-33106 Paderborn

Tel. +49 5251 525 1410
Fax  +49 5251 525 32 1410
4 Basic hardware procedures

4.1 Using diagnostics information

The "FUJITSU Server PRIMERGY BX2580 M2 Server Blade Operating Manual" gives an introduction to server blade features and provides an overview of available hardware options.

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

- Operation
- Maintenance

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

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

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

4.1.1 Accessing the management blade web interface

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

Figure 2: Connectors on the management blade

- Connect the FST to the management LAN connector. Customers must use the Up port (4) while the Down port (5) is reserved for service personnel.
  - If two management blades are installed, connect the FST to the master management blade. The status indicator of the master management blade glows yellow.
  - The FST must be on the same LAN with the same subnet as the management LAN port.

- Launch a web browser and enter the Management Agent Administrative URL to login to the management blade web interface. For further information, refer to the "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description" or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description".
  - If you don't know the Management Agent Administrative URL, proceed as follows.
    - Connect the FST to the serial port of the management blade (3) and open a terminal session, see the "PRIMERGY BX900 Blade Server Systems ServerView Management Blade S1 User Interface Description" or "PRIMERGY BX400 Blade Server Systems ServerView Management Blade S1 User Interface Description".
    - Open the Management Agent – Management Agent Information menu to view the Management Agent Administrative URL.
    - Login to the management blade web interface as described above.
4.1.2 Locating the defective server blade

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

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

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

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

- When using ServerView Operations Manager to toggle the ID indicator, choose Single System View and press the Locate button.

- Remember to switch off the ID indicator after the maintenance task has been concluded successfully.
4.1.3 Determining the error class

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

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

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

![Information icon]

The indicators also light up in standby mode and after a server blade restart due to a power failure.
4.1.3.1 Global Error indicator

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

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global error indicator</td>
<td>off</td>
<td>no critical event (non CSS component)</td>
</tr>
<tr>
<td></td>
<td>orange on</td>
<td>prefailure detected (non CSS component), requires (precautionary) service intervention</td>
</tr>
<tr>
<td></td>
<td>orange flashing</td>
<td>non CSS component failure or software / agent related error, requires service intervention</td>
</tr>
</tbody>
</table>

For further diagnostics, proceed as follows:

- **Hardware errors:**
  
  Check the System Event Log (SEL) as described in section "Viewing the SEL" on page 91.

- **Software / agent related errors:**
  
  Check the ServerView System Monitor, available on Windows or Linux based server blades with ServerView agents installed.

  For further information, please refer to the "ServerView System Monitor" user guide.
Check the CSS indicator on the front panel of the server blade:

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSS indicator</td>
<td>off</td>
<td>no critical event (CSS component)</td>
</tr>
<tr>
<td></td>
<td>orange on</td>
<td>prefailure detected (CSS component)</td>
</tr>
<tr>
<td></td>
<td>orange flashing</td>
<td>CSS component failure</td>
</tr>
</tbody>
</table>
4.1.4 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 allow you to identify the defective component.

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

Local diagnostic indicators on the system board

---

Using the Indicate CSS button

- Shut down the server blade as described in section "Shutting down the server blade" on page 50.
- Remove the server blade from the system unit as described in section "Removing the server blade from the system unit" on page 52.
- Open the server blade as described in section "Opening the server blade" on page 53.
- Press the Indicate CSS button (1) to highlight defective components.
Basic hardware procedures

Component LEDs

LEDs C to G (see figure 6 on page 47) are visible from the frontside. All other LEDs are only visible if the server blade cover has been removed. In order to access memory LEDs (B), the air cowls need to be removed (see section "Handling of memory air cowls" on page 173).

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>off</td>
<td>Mezzanine card 1 operational</td>
</tr>
<tr>
<td>A</td>
<td>yellow on</td>
<td>Mezzanine card 1 failure</td>
</tr>
<tr>
<td>B</td>
<td>off</td>
<td>memory module operational</td>
</tr>
<tr>
<td>B</td>
<td>yellow on</td>
<td>memory module module failure</td>
</tr>
<tr>
<td>C</td>
<td>off</td>
<td>Fabric 3/4 no link</td>
</tr>
<tr>
<td>C</td>
<td>green flashing</td>
<td>Fabric 3/4 link active</td>
</tr>
<tr>
<td>C</td>
<td>green on</td>
<td>Fabric 3/4 link established</td>
</tr>
<tr>
<td>D</td>
<td>off</td>
<td>Fabric 2 no link</td>
</tr>
<tr>
<td>D</td>
<td>green flashing</td>
<td>Fabric 2 link active</td>
</tr>
<tr>
<td>D</td>
<td>green on</td>
<td>Fabric 2 link established</td>
</tr>
<tr>
<td>E</td>
<td>off</td>
<td>Fabric 1 no link</td>
</tr>
<tr>
<td>E</td>
<td>green flashing</td>
<td>Fabric 1 link active</td>
</tr>
<tr>
<td>E</td>
<td>green on</td>
<td>Fabric 1 link established</td>
</tr>
<tr>
<td>F</td>
<td>off</td>
<td>System is ok</td>
</tr>
<tr>
<td>F</td>
<td>orange flashing</td>
<td>CSS error detected</td>
</tr>
<tr>
<td>F</td>
<td>orange on</td>
<td>Prefailure event detected</td>
</tr>
<tr>
<td>G</td>
<td>off</td>
<td>No critical event</td>
</tr>
<tr>
<td>G</td>
<td>orange flashing</td>
<td>Error detected (requires service intervention)</td>
</tr>
<tr>
<td>G</td>
<td>orange on</td>
<td>Prefailure event detected (requires service intervention)</td>
</tr>
<tr>
<td>H</td>
<td>off</td>
<td>Mezzanine card 2 operational</td>
</tr>
<tr>
<td>H</td>
<td>yellow on</td>
<td>Mezzanine card 2 failure</td>
</tr>
<tr>
<td>I</td>
<td>off</td>
<td>CPU 1 operational</td>
</tr>
<tr>
<td>I</td>
<td>yellow on</td>
<td>CPU 1 failure</td>
</tr>
<tr>
<td>J</td>
<td>off</td>
<td>CPU 2 operational</td>
</tr>
<tr>
<td>J</td>
<td>yellow on</td>
<td>CPU 2 failure</td>
</tr>
</tbody>
</table>
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.
Basic hardware procedures

4.2 Shutting down the server blade

⚠️ CAUTION!

For further safety information, please refer to chapter "Important information" on page 29.

- Inform the system administrator that the server blade will be shut down and put offline.
- Terminate all applications.
- In case of Multipath I/O environments, please refer to section "Note on server maintenance in a Multipath I/O environment" on page 68.

Figure 7: Power button on the front panel

- Shut down the server blade by pressing the On / Off button (1). The power indicator (2) turns off.
  
  🔄 If the system is running an ACPI-compliant operating system, pressing the On / Off button will perform a graceful shutdown.
  
- Switch on the ID indicator on the front connector panel of the server as described in section "Locating the defective server blade" on page 43.
4.3 Removing a server blade

CAUTION!

For safety information, please refer to chapter "Important information" on page 29.

4.3.1 Preliminary steps

- Shut down and power off the server blade as described in section "Shutting down the server blade" on page 50.
4.3.2 Removing the server blade from the system unit

Push the release lever (1) up slightly to unlock the ejection lever (2).

Swivel the ejection lever down until it is horizontal.

Pull the server blade out of the system unit.

Figure 8: Removing the server blade from the system unit
4.4 Opening the server blade

CAUTION!

For safety information, please refer to chapter "Important information" on page 29.

Removing the cover

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

Figure 9: Removing the cover
4.5 Closing the server blade

**CAUTION!**

- Before attaching the cover, make sure no unnecessary parts or tools are left inside the server.

- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY BX2580 M2 server blade must not run while the cover is removed.

- For further safety information, please refer to chapter "Important information" on page 29.

Figure 10: Closing the server blade

- Place the cover on the server blade housing such that it lies flush with both sides, leaving a gap of approx. 1-2 cm from the front frame.

- Push the cover in the direction of the arrow until it snaps into place.
4.6 Installing the server blade in the system unit

CAUTION!

- Note the safety instructions and the information on handling electrostatically sensitive devices in section "Safety instructions" on page 29.
- Note the population rules for power supply units and fan modules to ensure sufficient cooling of the system. You will find more detailed information on this in the operating manual for the system unit.

Installing the Server Blade

CAUTION!

Follow the safety instructions and information in section "Notes on installing the server in the rack" on page 36.

Please check that the connector is neither damaged nor pins are deformed etc. when setting it up.

Do not use the server blade when abnormality of the connector or of the pins can be seen.
Basic hardware procedures

Figure 11: Installing the Server Blade

- Open the release lever (1).
- Push the server blade as far as possible into the slot (2).
Pull the release lever up until it engages.

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

CAUTION!

Before switching on the server blade, make sure the cover is closed. In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the server blade must not run while the cover is removed.

Follow the safety instructions in chapter "Important information" on page 29.

Press the On / Off button (1) to start up the server blade.

Ensure that the power-on indicator (2) in the On / Off button is lit green.

For more information, refer to section "Front panel indicators" on page 276.
4.8 Concluding software tasks

Perform the following software tasks to put the server blade back into operation:

- "Resetting the boot retry counter" on page 83
- "Verifying the system time settings" on page 90
- "Viewing and clearing the System Event Log (SEL)" on page 91
- "Updating the NIC configuration file in a Linux environment" on page 93
- "Resuming BitLocker functionality" on page 94
- "Performing a RAID array rebuild" on page 95
- "Looking up changed MAC / WWN addresses" on page 96
Basic hardware procedures
5 Basic software procedures

5.1 Starting the maintenance task

5.1.1 Launching a video redirection to a server blade

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

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

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

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

5.1.2 Checking the server blade status

5.1.2.1 Checking the server blade status via management blade web interface

To check the server blade status proceed as follows.

- Enter the management blade web interface.
- Open the Components – System menu.
Basic software procedures

► Click the button in the Server Blade Status title bar to expand the server blade list.

The overall status of the installed server blades is indicated by the icons in the Health column.

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

► Select the Server Blade-x entry to open the administration menu for the desired server blade.

► Scroll down in the Information tab to get status information about the following components.
  – Operating System
  – BIOS Version
  – Processors
  – Memory modules
  – Network components (on-board CNA controller and mezzanine cards)
  – Operating System

► Open the Event Log tab to read the system event log entries.

5.1.2.2 Checking the server blade status via iRMC

► Enter the management blade web interface.

► Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.

► Click the Remote Management button in the status frame of the server blade menu.

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

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

Proceed as follows:

- Shut down and power off the server blade as described in section "Shutting down the server blade" on page 50.
- Enter the management blade web interface.
- Open Components - Server Blade - Server Blade-x menu.
- Open the Configuration tab.
- In the iRMC Address Configuration Box, write down IP Address, Subnet Mask and Gateway.
- Open the iRMC web interface "FUJITSU ServerView® iRMC S4 Web Server" directly.

**CAUTION!**

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

- Open the BIOS - Backup/Restoration menu.
- Click the Request BIOS Parameter Backup button in section of "Backup BIOS Single Parameters in ServerView® WinSCU XML format".
- If Backup Status is "Operation successful", click the Save Backup to File button.
- Store the backup file in the system of the FST.

5.1.4 Saving iRMC settings

Proceed as follows:

- Enter the management blade web interface.
- Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.
- Open the Configuration tab.
- Scroll to the iRMC Address Configuration box.
- Write down IP Address, Subnet Mask and Gateway.
Basic software procedures

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

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

- Open the iRMC S4 – Network Settings – Ethernet, and confirm IP Address, Subnet Mask and Gateway.

- Open the iRMC S4 - Save Configuration.

- Click the Save All button in section of "Save iRMC S4 Firmware settings in ServerView® WinSCU XML format".

- Store the backup file in the system of the FST.

5.1.5 Connecting virtual media to the managed server blade

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

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

- Enter the management blade web interface.

- Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.

- Click the Video Redirection button in the status frame of the server blade menu.

- Click Media - Virtual Media Wizard in the menu bar of the video redirection window.

For further information on iRMC Virtual Media function refer to the "Integrated Remote Management Controller" user guides available online.
5.1.6 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*. 
Basic software procedures

- 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.

5.1.7 Disabling boot watchdog functionality

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

5.1.7.1 Viewing boot watchdog settings

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

- Enter the management blade web interface.

- Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.

- Select the Configuration tab and see the ASR box to obtain detailed information about the current watchdog status, timeout intervals and actions that are triggered if watchdog timeouts are exceeded.

For more detailed information, refer to the Help – On Page function of the management blade web interface.
5.1.7.2 Configuring boot watchdog settings

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

**CAUTION!**

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

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

**Configuring boot watchdog settings in the BIOS**

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the **F2** function key to enter the BIOS.
- Select the **Server Mgmt** menu.
- Under **Boot Watchdog** set the **Action** setting to **Continue**.
- Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.

**Configuring boot watchdog settings using the management blade web interface**

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

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

5.1.8 Verifying and configuring the backup software solution

This task only applies to the Japanese market.

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

This is the case for the following backup software solution:

- BackupExec

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

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

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

When booting your server 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:
Basic software procedures

for the EMEA market

for the Japanese market:

► 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 $[\uparrow]$ and $[\downarrow]$ cursor keys to select your DVD drive or USB stick as boot device and press $[\text{ENTER}]$.

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

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

The Update Manager Express main window will be displayed.

► Finish the intended maintenance task.

ℹ️ 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.

ℹ️ 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.

ℹ️ 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.

5.1.10 Switching on the ID indicator

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

Using the ID button on the front panel

- Press the ID button on the front panel to switch on the ID indicators.
  
  When the ID button is pushed for five seconds or more and separated, it lights to blue.
  In addition, when the ID button is pushed again within one second, NMI is issued.

  For further information, refer to section "Front panel indicators" on page 276.

Using management blade web interface

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

Using ServerView Operations Manager

- In ServerView Operations Manager Single System View and press the Locate button in the title bar to switch on the ID indicator.
5.2 Completing the maintenance task

5.2.1 Updating or recovering the system board BIOS and iRMC

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

http://ts.fujitsu.com/support/ (global market)

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

For the Japanese market, follow the instructions provided separately.

5.2.1.1 Updating or recovering the system board BIOS

TFTP update procedure

► Ensure that the server blade has been shut down as described in section "Shutting down the server blade" on page 50.

► Log in to the management blade web interface.

► Open the Information / Operation – Operation – Firmware Update menu.

► Open the Server Blade tab.

► In the Server Blade to be Updated box select the desired server.

► In the Update settings box select the update firmware (BIOS).

► In the Update settings box enter the TFTP IPv4 or IPv6 address of the TFTP server and the pathname of the TFTP firmware file.

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

► Click the Start button to start the update process.

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

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

BIOS recovery procedure (use InternalSW package)

For the Japanese market, follow the instructions provided separately.

- Prepare a bootable USB stick as described in section Flash BIOS Update with a USB stick.
- Switch off the system and disconnect the power plug.
- Open the chassis and switch on "Recovery" (RCVR) using the jumper / DIP switch on the system board.
- Reconnect the power plug and start the system with the inserted bootable USB stick.
- Observe the update process on the screen, until it is finished.
  The recovery update may take several minutes.
- Switch-off the system and disconnect the power plug.
- Remove the USB stick.
- Return the "Recovery" (RCVR) jumper / DIP switch which have been changed to the initial position.
- Reconnect the power plug and switch on the system.
  The system will be booted with the new BIOS revision.
- Check the settings in the BIOS setup utility. If necessary, reconfigure the settings again.

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

- Ensure that the server blade has been shut down as described in section "Shutting down the server blade" on page 50.
- Login to the management blade web interface.
- Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.
- Select the Configuration tab.
Basic software procedures

- In the *Boot Options* box activate the *BIOS Recovery Flash Bit Enabled* option.

- Connect the monitor, keyboard, mouse and USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.

- Switch on the server blade as described in section "Switching on the server blade" on page 58.

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

**CAUTION!**

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

- Switch off the server blade as described in section "Shutting down the server blade" on page 50.

- Remove the Y cable.

- Deactivate the *BIOS Recovery Flash Bit Enabled* option in the management blade *Boot Options* menu.

- Switch on the server blade as described in section "Switching on the server blade" on page 58.

- You can now put the server blade back into operation.

**Second option: Recovering the server blade BIOS via DIP switch**

- Remove the server blade from the system unit as described in section "Removing a server blade" on page 51.

- Open the server blade as described in section "Opening the server blade" on page 53.

- Enter BIOS recovery mode using switch 3 of the user DIP switch bank, see section "Onboard settings" on page 271.

- Close the server blade as described in section "Closing the server blade" on page 54.

- Reinstall and secure the server blade in the system unit as described in section "Installing the server blade in the system unit" on page 55.

- Connect the monitor, keyboard, mouse and USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.
Switch on the server blade as described in section "Switching on the server blade" on page 58.

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

**CAUTION!**

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

Switch off the server blade as described in section "Shutting down the server blade" on page 50.

Remove the Y-cable.

Remove the server blade from the system unit as described in section "Removing a server blade" on page 51.

Open the server blade as described in section "Opening the server blade" on page 53.

Turn switch 3 of the user DIP switch bank to OFF, see section "Onboard settings" on page 271.

Close the server blade as described in section "Closing the server blade" on page 54.

Reinstall the server blade in the system unit as described in section "Installing the server blade in the system unit" on page 55.

Switch on the server blade as described in section "Switching on the server blade" on page 58.

You can now put the server blade back into operation.

### 5.2.1.2 Updating or recovering the iRMC

**TFTP update procedure**

Login to the management blade web interface.

Open the Information / Operation – Operation – Firmware Update menu.

Open the Server Blade tab.

In the Server Blade to be Updated box select the desired server.
Basic software procedures

- In the **Update settings** box select the update firmware (iRMC).
- In the **Update settings** box enter the TFTP IPv4 or IPv6 address of the TFTP server and the pathname of the TFTP firmware file.
  
  For more detailed information, refer to the *Help – On Page* function of the management blade web interface.
- Click the **Start** button to start the update process.
  
  The status column in the **Server Blade to be Updated** box provides information on the update progress.

**CAUTION!**

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

iRMC recovery procedure

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

For the Japanese market, follow the instructions provided separately.

- Shut down the server blade as described in section "Shutting down the server blade" on page 50.
- Connect the monitor, keyboard, mouse and the bootable USB memory stick to the port on the front of the server blade using the Y cable, see the Operating Manual.
- Switch on the server blade while as described in section "Switching on the server blade" on page 58 to boot from the USB memory stick.
  
  After completion of the boot operation, the **FlashDisk** menu opens.
- Select **Recovery_L** to carry out the recovery flash for firmware image 1 (low firmware image).
- Select **Recovery_U** to carry out the recovery flash for firmware image 2 (high firmware image).
- Once the update operation has been completed, click on **Exit**, to close the **FlashDisk** menu.
Basic software procedures

- Shut down the server blade as described in section "Shutting down the server blade" on page 50.
- Remove the Y-cable.
- Switch on the server blade as described in section "Switching on the server blade" on page 58.
- You can now put the server blade back into operation.
5.2.2 Restoring BIOS settings

Proceed as follows:

- Shut down and power off the server blade as described in section "Shutting down the server blade" on page 50.
- Enter the management blade web interface.
- Open Components - Server Blade - Server Blade-x menu.
- Open the Configuration tab.
- In the iRMC Address Configuration Box, set IP Address, Subnet Mask and Gateway.
- Click the Apply button.
- Open the iRMC web interface "FUJITSU ServerView® iRMC S4 Web Server" directly.

**CAUTION!**

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

- Open the BIOS - Backup/Restoration menu.
- Select the backup file stored in the file system of FST in section "Restoration BIOS Single Parameters in ServerView® WinSCU XML format".
- Click the Upload button.
- If "Are you sure you want to update the system bios with this file?" is displayed, click the Confirm button.
- If Restoration Status is "Operation successful", restoring BIOS settings is completed.
5.2.3 Restoring iRMC settings

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

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

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

5.2.4 Updating mezzanine card firmware

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

http://ts.fujitsu.com/support/ (global market)

ℹ️ 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.
Basic software procedures

Using the ServerView Update Manager

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

- ServerView Update Manager:
  "ServerView Update Management" user guide

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

Using the flash tool

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

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

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

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

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

The status of the component will then be set to ok. To see the new status you must refresh the Driver Monitor view with Refresh.
5.2.5 Enabling Option ROM scan

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

Option ROM can be enabled permanently (e.g. in case of a boot controller that may require frequent setup) or temporarily for one-time configuration.

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

When permanently enabling a controller’s Option ROM, keep in mind that only two Option ROMs can be activated in the system board BIOS at a time.

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the \[F2\] function key to enter the BIOS.
- From the Advanced menu select Option ROM Configuration.
  - When iSCSI is used via an onboard CNA, from the Advanced menu select Onboard Devices Configuration - Onboard CNA OpROM.
- Identify the desired mezzanine card slot and set its Launch Slot # OpROM setting to Enabled.
- Save your changes and exit the BIOS.

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

For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.

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

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

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

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

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

5.2.6 Verifying and configuring the backup software solution

This task only applies to the Japanese market.

Disabling backup drives

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

This is the case for the following backup software solutions:
- Netvault for Windows
- ARCServe
- BackupExec

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

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

Re-enabling backup drives

If a backup drive has been disabled or deleted from the backup software drive list as described in section "Verifying and configuring the backup software solution" on page 68, it has to be re-enabled to complete the maintenance task.

- Re-enable backup drives and revise backup software settings and cronjobs.
Detailed information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages.

5.2.7 Resetting the boot retry counter

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

5.2.7.1 Viewing the boot retry counter

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

- Enter the management blade web interface.
- Open the Components – System – Server Blades – Server Blade-x menu for the desired server blade.
- Select the Configuration tab and scroll to the ASR box.
- Under Retry Counter 0-max. the current number of remaining boot attempts is displayed. The value is further decremented with every failed boot attempt or system reboot resulting from critical system errors.

5.2.7.2 Resetting the boot retry counter

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

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

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

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

Resetting the boot retry counter in the management blade web interface

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

5.2.8 Resetting the error status after replacing memory modules or processors

5.2.8.1 Memory modules

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

**Important note**

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

Using the iRMC web frontend

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

Using ServerView Maintenance Tools (Windows only)

▸ Launch the ServerView Maintenance Tools:
  – Windows Server 2008 R2 and below:
    Start > (All) Programs > Fujitsu > ServerView Suite > Agents > Maintenance Tools
  – Windows Server 2012 and above:
    Start > Apps > Fujitsu > Maintenance Tools

▸ Choose the Memory status tab.

▸ Select the memory module which shows the pre-failure status.

▸ Click on Reset Status.

  The Reset Status button will only be available if the selected memory module contains errors.

▸ Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

Using the command line interface (Linux only)

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

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

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

▸ Log in as root.

▸ Enter the command below, followed by [ENTER]:
  /usr/sbin/meclear

▸ Select the number of a memory module with a status other than "OK" or "Not available".

▸ Repeat the step above until all memory modules show the "OK" status.

▸ Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.
5.2.8.2 Processors

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

**Important note**

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

**Using ServerView Maintenance Tools (Windows only)**

- Launch the ServerView Maintenance Tools:
  - Windows Server 2008 R2 and below:
    
    ![Start](Windows icon) > (All) Programs > Fujitsu > ServerView Suite > Agents > Maintenance Tools

  - Windows Server 2012 and above:
    
    ![Start](Windows icon) > Apps > Fujitsu > Maintenance Tools

- Choose the CPU status tab.

- Select the CPU which shows the pre-failure status.

- Click on Reset Status.

- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

**Using the command line (Linux only)**

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

- Log in as root.

- Enter the command below, followed by [ENTER]:
  - For rack and tower servers (RX and TX server series):
    
    `/usr/sbin/eecdcp -c oc=0609 oi=<CPU#>`

  - For blade and scale-out servers (BX and CX server series):
    
    `/usr/sbin/eecdcp -c oc=0609 oi=<CPU#> cab=<cabinet nr>`

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

  `<CPU#>` parameters are "0" for CPU 1 and "1" for CPU 2.
If the error status cannot be reset with the method above, please use the following procedure for resetting the error counter of all processors:

- Log in as root.

- Enter the commands below, followed by [ENTER]:

  1. /etc/init.d/srvmagt stop
     /etc/init.d/srvmagt_scs stop
     /etc/init.d/eecd stop
     /etc/init.d/eecd_mods_src stop
  2. cd /etc/srvmagt
  3. rm -f cehist.bin
  4. /etc/init.d/eecd_mods_src start
     /etc/init.d/eecd start
     /etc/init.d/srvmagt start
     /etc/init.d/srvmagt_scs start

- Ensure that all pre-fail / fail status issues have been resolved in ServerView Operations Manager.

### 5.2.9 Enabling boot watchdog functionality

If boot watchdog functionality has been disabled for firmware upgrade purposes (see section "Disabling boot watchdog functionality" on page 66), it has to be re-enabled to complete the maintenance task.

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

#### Configuring boot watchdog settings in the BIOS

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the F2 function key to enter the BIOS.
- Select the Server Mgmt menu.
- Under Boot Watchdog set the Action setting to Reset.
- Save your changes and exit the BIOS.
Basic software procedures

For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.

Configuring boot watchdog settings using the management blade web interface

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

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

5.2.10 Enabling replaced components in the system BIOS

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

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.

- Switch on or restart your server blade.

- As soon as the startup screen appears, press the [F2] function key to enter the BIOS.

- Select the Advanced menu.

- Select the status menu of the desired component:
  - Processors: CPU Status
    
    This option is only available for multi-processor systems.

  - Memory: Memory Status
Basic software procedures

- 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 "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.

5.2.11 Verifying the memory mode

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

For detailed information on memory operation modes available, refer to section "Mirrored Channel and Performance Modes" on page 158".

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

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the \[F2\] function key to enter the BIOS.
- Select the Advanced menu.
- Under Memory Status verify that none of the memory modules are marked as Failed.
- Save your changes (if applicable) and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.
5.2.12 Verifying the system time settings

This task only applies to Linux / VMware environments.

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

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

- After replacing the system board, ask the system administrator whether the RTC or UTC time standard is to be used as system time.
  - If the system time (RTC) is set to UTC, the SEL (System Event Log) time stamps may differ from the local time.
- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the \[F2\] function key to enter the BIOS.
- Select the Main menu.
- Under System Time and System Date specify the correct time and date.
  - By default, the system time set in the BIOS is RTC (Real Time Clock) local time. If your IT infrastructure relies on universally accepted time standards, set the System Time to UTC (Universal Time, Coordinated) instead. Greenwich Mean Time (GMT) can be considered equivalent to UTC.
    - It is necessary to change to "Disabled" when making it to UTC.
- Save your changes and exit the BIOS.
- For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.
5.2.13 Viewing and clearing the System Event Log (SEL)

5.2.13.1 Viewing the SEL

You can view the System Event Log (SEL) of the management blades and server blades using the management blade web interface and ServerView Operations Manager frontend:

Viewing the SEL using the management blade web interface

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

Viewing the SEL in ServerView Operations Manager

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

Note on the SVOM Driver Monitor

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

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

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

### 5.2.13.2 Saving the SEL

#### Saving the SEL via management blade web interface

- Enter the management blade web interface.
- Select the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade and open the *Event Log* tab.
- In the *Export Event Log* box select the export medium.
  - Local File or
  - USB Export File
    - This option is only available, if a USB memory stick is connected to the management blade.
- Click the *Start* button to save all available management blade and server blade event logs as text file to the selected medium.

#### Saving the SEL via iRMC

- Enter the management blade web interface.
- Open the *Components – System – Server Blades – Server Blade-x* menu for the desired server blade.
- Click the *Remote Management* button in the status frame of the server blade menu.
  - The iRMC web interface opens, where you can administer the server blade remotely.
- Open the *Event Log – IPMI SEL content* menu.
5.2.13.3 Clearing the SEL

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

- Enter the management blade web interface, see section "Accessing the management blade web interface" on page 41.
- Select the Components – System – Server Blades – Server Blade-x menu for the desired server blade and open the Event Log tab.
- In the Event Log Filter box click Clear All Entries to clear the SEL.

5.2.14 Updating the NIC configuration file in a Linux environment

In order to prevent errors caused by changing network device names (eth<x>), it is recommended to store the MAC address (hardware address) of a network interface card in the related NIC configuration file of the Linux OS.

When replacing a network controller or the system board with onboard CNA controllers in a server running Linux OS, the MAC address will change but not automatically be updated in the definition file.

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

To update the MAC address, proceed as follows:

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

- After replacing a network controller or the system board, switch on and boot the server as described in section "Switching on the server blade" on page 58.

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

*i*  *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:

```
```

- 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.

**5.2.15 Resuming BitLocker functionality**

If BitLocker Drive Encryption has been suspended for maintenance purposes (see section "Suspending BitLocker functionality" on page 65), 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.
Basic software procedures

► 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.

5.2.16 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.
Basic software procedures

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.

5.2.17 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.

5.2.17.1 Looking up MAC addresses

- Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
- Switch on or restart your server blade.
- As soon as the startup screen appears, press the \[F2\] function key to enter the BIOS.
- Depending on the number of network controllers in your system, you will find one or several Port Configuration menu items.
  Use the arrow key \[→\] to scroll to the right and browse all available tabs.
  Each Port Configuration tab will display detailed information on the related network controller, including its MAC address.
Basic software procedures

- Note down the new 12-digit MAC address.
- Press [Esc] to exit the BIOS.
- Inform the customer about the changed MAC address.

5.2.17.2 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 81.
- Restart the server.
- During boot, as soon as the Emulex BIOS utility option appears, press [ALT]+[E] or [CTRL]+[E].
- Under Emulex Adapters in the System you will find all available Emulex adapters and their WWN addresses.
- Note down the new 16-digit WWN address.
- Press [Esc] to exit the Emulex BIOS utility.
- Inform the customer about the changed WWN address.

5.2.18 Using the Chassis ID Prom Tool

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

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

After replacing the server blade, system information has to be entered using the ChassisId_Prom Tool. The tool and further instructions are available to maintenance personnel from the Fujitsu Technology Solutions Extranet:

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

For the Japanese market, follow the instructions provided separately.
5.2.19 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.

5.2.19.1 After replacing / upgrading LAN/CNA controllers

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

- Confirm with the customer whether the LAN/CNA controller you have replaced has been used as part of a LAN teaming configuration.

- If LAN teaming has been active, you will need to restore the configuration using the LAN driver utility after replacing the LAN/CNA controller.

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

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

5.2.19.2 After replacing the server blade

- Confirm with the customer whether the onboard CNA controller you have replaced has been used as part of a LAN teaming configuration.

- If LAN teaming has been active, you will need to restore the configuration using the CNA driver utility after replacing the server blade.

For details, refer to the relevant CNA driver manual.
5.2.20 Switching off the ID indicator

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

For further information, refer to section "Locating the defective server blade" on page 43.

Using the ID button on the front panel

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

Using management blade web interface

► In management blade web interface press the Locate button in the status frame to switch off the ID indicator.

Using ServerView Operations Manager

► In ServerView Operations Manager Single System View and press the Locate button in the title bar to switch off the ID indicator.
6 Solid state drives

Safety notes

CAUTION!

- The drive must not be removed from the installation frame by anyone except a service technician.

- Drive modules must all be marked clearly so that they can be reinstalled into their original mounting locations after an upgrade. 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.

- Depending on the OS, you can configure the write cache settings for the 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 or solid state drive, wipe out the data on the drive for your own security.

- Rough handling of 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.

- Do not use the device in extremely hot or cold locations, or locations with extreme temperature changes.

- Never attempt to disassemble a solid state drive.

- For further safety information, please refer to chapter "Important information" on page 29.

6.1 Basic information

- No hard disk drives are allowed within BX2580 M2.
- Up to two solid state drives (SSDs) are supported within BX2580 M2.
- SSDs with different capacities are installed from highest to lowest capacity.
- No mix of different bus technologies (SAS or PCH) is allowed.
6.2 Installing SSDs

Upgrade and Repair Unit (URU)                                      Hardware: 5 minutes

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

6.2.1 Preliminary steps

Before installing an SSD, perform the following steps:

► "Locating the defective server blade" on page 43.
► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
Solid state drives

6.2.2 Location of the drive modules inside the server blade

The drive modules can only be mounted above the mounting location of CPU 2, either on the heat sink or on the dummy heat sink (if CPU 2 is not installed).

Mounting the drive modules on the dummy heat sink

The first drive module has to be mounted on location for SSD 0 (see pos. #2 in figure above).

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mounting location of SSD 1</td>
</tr>
<tr>
<td>2</td>
<td>Mounting location of SSD 0</td>
</tr>
</tbody>
</table>
Solid state drives

Mounting the drive modules on the heat sink for CPU 2

The first drive has to be mounted on location for SSD 0 (see pos. #2 in figure above).

Figure 16: Mounting locations of the drive modules on top of the heat sink of CPU 2

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mounting location of SSD 1</td>
</tr>
<tr>
<td>2</td>
<td>Mounting location of SSD 0</td>
</tr>
</tbody>
</table>
6.2.3 Mounting the SSDs into their frames

The SSDs have to be installed into mounting frames. Two different types of mounting frames (PCH or SAS) are available.

The following figure shows both types of mounting frames:

![Figure 17: PCH and SAS drive mounting frames](image)

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PCH mounting frame</td>
</tr>
<tr>
<td>2</td>
<td>SAS mounting frame</td>
</tr>
</tbody>
</table>

The mounting frames are placed above the mounting location for CPU 2 (see section "Location of the drive modules inside the server blade" on page 103.)
Solid state drives

Inserting a drive into its mounting frame

► Choose the desired mounting frame (PCH or SAS).

The following installation procedure is identical for SSD 0 and SSD 1.

Figure 18: Shifting a drive into a mounting frame

► In a slight angle (see circle) shift the drive into the mounting frame (1) until it is fully plugged into the connector (2).

The drive and its mounting frame together are called "drive module".
6.2.4 Installing the drive module onto the mounting platform

The procedure to install the drive module is identical for SSD 0 and SSD 1.

The drive module has to be installed as follows:

- Shift the drive module into the cut-out of the mounting platform (see pos. #1 and close-up).
- Plug the drive module into the connector on the system board (2).

Figure 19: Installing the mounting frame into its location
Solid state drives

Figure 20: Securing the drive module

- Secure the drive module with the knurled screw (see arrow).
  Torque: **0.6 Nm** (not applicable for the Japanese market)

### 6.2.5 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Performing a RAID array rebuild" on page 95.
6.3 Removing SSDs

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tool: Phillips PH2 (+) No. 2 screw driver

6.3.1 Preliminary steps

Before removing an SSD module, perform the following steps:

Only applicable for removing intact SSD modules:

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

CAUTION!

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

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

► "Locating the defective server blade" on page 43.
► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
Solid state drives

6.3.2 Removing an SSD

The removal procedure is identical for SSD 0 and SSD 1.

Removing the drive module out of the mounting platform

Figure 21: Loosening the drive module

- Loosen the knurled screw of the mounting frame (see arrow).
Unplug the drive module from the connector on the system board by lifting it off from the mounting platform (1).

Remove the drive module out of the cut-out of the mounting platform (2).
Solid state drives

Removing the drive out of its mounting frame

Figure 23: Removing the drive from the mounting frame

- Press on the green tab of the mounting frame (1).
- Shift the drive out of the mounting frame in the direction of the arrow (2).

6.3.3 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
6.4 Replacing SSDs

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

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

CAUTION!
All SSDs must be uniquely identified so that they can be reinstalled in their original mounting locations later. If this is not done, existing data can be lost.

6.4.1 Preliminary steps

Before replacing an SSD, perform the following steps:

► "Suspending BitLocker functionality" on page 65.
► "Locating the defective server blade" on page 43.
► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
► "Locating the defective component" on page 47.

Only applicable for removing intact SSDs:

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

6.4.2 Removing an SSD

► "Removing an SSD" on page 110.
6.4.3 Installing an SSD

- "Mounting the SSDs into their frames" on page 105
- "Installing the drive module onto the mounting platform" on page 107.

6.4.4 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Performing a RAID array rebuild" on page 95.
- "Resuming BitLocker functionality" on page 94.
6.5  Replacing SAS / PCH mounting frames

Field Replaceable Unit (FRU)

Hardware: 5 minutes  
Software: 5 minutes

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

6.5.1  Preliminary steps

Before replacing SAS / PCH mounting frames, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.

6.5.2  Removing the mounting frame

**CAUTION!**

Ensure that the drives are uniquely identified so that you can reinsert them into their original locations after replacing the mounting frames.

- Remove the respective drive module from its mounting platform as described in section "Removing the drive module out of the mounting platform" on page 110.
- Remove the SSD from the mounting frame as described in section "Removing the drive out of its mounting frame" on page 112.

6.5.3  Installing the mounting frame

- Install the SSD into the mounting frame as described in section "Inserting a drive into its mounting frame" on page 106.
Solid state drives

- Install the respective drive module into its mounting platform as described in section "Installing the drive module onto the mounting platform" on page 107.

6.5.4 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Resuming BitLocker functionality" on page 94.
6.6 M.2 SSDs

► If applicable, remove the old SSDs drives.

Please refer to "Removing SSDs" on page 109 for removing the SSDs.

6.7 Basic information

– No hard disk drives are allowed within BX2580 M2.
– Up to two M.2 SSDs are supported within BX2580 M2.
– M.2 SSDs with different capacities are installed from highest to lowest capacity.
– No mix of different bus technologies (SAS or PCH) is allowed.
– Mixed configuration of M.2 SSD and 1.8" SATA SSD is not possible.

6.8 Installing M.2 SSDs

Upgrade and Repair Unit
(URU)

Hardware: 5 minutes

Tool:
Phillips PH0 / (+) No. 0 screw driver
Phillips PH1 / (+) No. 1 screw driver
Phillips PH2 / (+) No. 2 screw driver

6.8.1 Preliminary steps

Before installing an M.2 SSD, perform the following steps:

► "Locating the defective server blade" on page 43.
► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
Solid state drives

6.8.2 Location of the M.2 SSDs

The M.2 SSDs can be installed in slots SSD 0 and SSD 1.

![Slots for installing M.2 SSDs](image)

- Install the first M.2 SSD in slot SSD 0 (2).
- Install the second M.2 SSD in slot SSD 1 (1).

6.8.3 Mounting the M.2 SSDs onto their backplanes

![M.2 SSD](image)

Before you can install the M.2 SSD to the slot you have to install the M.2 SSD to their backplane.
Solid state drives

Figure 26: Installing the M.2 SSD on the backplane

- Insert the M.2 SSD on the backplane and fasten the M.2 SSD with the two screws (see circles).

  Torque: 0.6 Nm (not applicable for the Japanese market).

Figure 27: Installing the M.2 SSD on the backplane

- Fasten the M.2 SSD with the silver screw (1).
- Make sure that the silver screw fits into the cut-out of the M.2 SSD board (see close-up).

  Torque: 0.2 Nm (not applicable for Japan).
Solid state drives

6.8.4 Installing the first M.2 SSD

Push the M.2 SSD backplane under the metal carrier (1).

Push the connector of the M.2 SSD to the connector of slot SSD 0 (2).

Take care of the circle guide while pushing the M.2 SSD backplane down (1).

Fasten the M.2 SSD with the green screw (2).

Torque: 0.6 Nm (not applicable for Japan).
6.8.5 Installing the second M.2 SSD

- Install the second M.2 SSD in the same way.

Figure 30: Two M.2 SSDs installed

6.8.6 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Performing a RAID array rebuild" on page 95.
6.9 Removing M.2 SSDs

Upgrade and Repair Unit (URU)

Tool:
- Phillips PH0 / (+) No. 0 screw driver
- Phillips PH1 / (+) No. 1 screw driver
- Phillips PH2 / (+) No. 2 screw driver

Hardware: 5 minutes

6.9.1 Preliminary steps

Before removing an M.2 SSD, perform the following steps:

Only applicable for removing intact M.2 SSD modules:

- Ensure that the M.2 SSD module to be removed is not combined into a RAID array. If the drive is part of a RAID array, you first need to delete the array using ServerView RAID Manager.

  CAUTION!

  All data on all HDDs/SSDs/M.2 SSDs in the array will be lost! Be sure to back up your data before deleting a RAID array.

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

  "Locating the defective server blade" on page 43.
  "Shutting down the server blade" on page 50.
  "Removing the server blade from the system unit" on page 52.
  "Opening the server blade" on page 53.
6.9.2 Removing the M.2 SSDs

- Loosen the green screw (1) of the M.2 SSD.
- Take care of the circle guide drawing the M.2 SSD backplane upwards (2).

6.9.3 Removing the second M.2 SSD

- Remove the second M.2 SSD in the same way.
6.9.4 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.

6.10 Replacing M.2 SSDs

**CAUTION!**

All M.2 SSDs must be uniquely identified so that they can be reinstalled in their original mounting locations later. If this is not done, existing data can be lost.

### 6.10.1 Preliminary steps

Before replacing an M.2 SSD, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Locating the defective component" on page 47.
Solid state drives

Only applicable for removing intact M.2 SSDs:

- Before removing a non-defective M.2 SSD, put the drive into "Offline" mode using your RAID configuration software.

6.10.2 Removing an M.2 SSD

- "Removing the M.2 SSDs" on page 123.

6.10.3 Installing an M.2 SSD

- "Mounting the M.2 SSDs onto their backplanes" on page 118
- "Installing the first M.2 SSD" on page 120.

6.10.4 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Performing a RAID array rebuild" on page 95.
- "Resuming BitLocker functionality" on page 94.
Solid state drives
7 Mezzanine cards

Safety notes

CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.

- Devices and components inside the server blade remain hot after shutdown. After shutting down the server blade, wait for hot components to cool down before installing or removing internal options.

- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).

- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.

- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.

- For further information, please refer to chapter "Important information" on page 29.
Mezzanine cards

7.1 Basic information

One or two mezzanine cards can be installed in a BX2580 M2 server blade. Additional Fibre Channel, SAS and/or Ethernet I/O channels can be set up using these cards.

All mezzanine cards have the same form factor.

![Sample of a 8 Gbit/s fibre-channel card with 2 ports](image)

Figure 33: Sample of a 8 Gbit/s fibre-channel card with 2 ports

The mezzanine cards are fastened on a special carrier and then connected together with the carrier to the system board.
The figure below shows the two kinds of unpopulated carriers for mezzanine cards. All installation/removal procedures are identical for both carriers.

Figure 34: Carrier for mezzanine cards with two "x8" riser cards

Figure 35: Carrier for mezzanine cards with one "x8" (1) and one "x16" (2) riser card

Note the numbering of the mezzanine card slots.
7.1.1 Installing riser cards

Installing the riser card x8

Figure 36: Installing the riser card x8

- Connect the riser card to the carrier. Make sure that the green clips click into place.
Installing the riser card x16

Figure 37: Installing the riser card x16

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

7.1.2 Removing riser cards

Removing the riser card x8

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

Figure 38: Removing the riser card x8
Removing the riser card x16

Figure 39: Removing the riser card x16

- Remove the riser card from the holder.
7.1.3 Population rules for mezzanine cards

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

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

Figure 40: Slot numbering for mezzanine cards

Figure 41: Connection blade slots
The table below shows the connections of the connection blade slots to the slots of the mezzanine cards.

<table>
<thead>
<tr>
<th>System unit</th>
<th>Connection blade slots</th>
<th>Server blade</th>
<th>Mezzanine card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric 1</td>
<td>CB1: 1Gb Ethernet or 10 Gb Ethernet</td>
<td>CB2: 1Gb Ethernet or 10Gb Ethernet</td>
<td>Onboard CNA-controller</td>
</tr>
<tr>
<td>Fabric 2</td>
<td>CB3: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel</td>
<td>CB4: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel</td>
<td>Mezzanine card 1</td>
</tr>
<tr>
<td>Fabric 3</td>
<td>CB5: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or SAS</td>
<td>CB6: 1Gb Ethernet or 10Gb Ethernet or Fibre-Channel or SAS</td>
<td>Mezzanine card 2</td>
</tr>
<tr>
<td>Fabric 4</td>
<td>CB7: 1Gb Ethernet</td>
<td>CB8: 1Gb Ethernet</td>
<td>- - -</td>
</tr>
</tbody>
</table>

Table 4: Fitting rules for connection blade slots

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

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

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

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

- If a 1 Gb Ethernet mezzanine card is installed in slot 2 of a server blade, at least one 1 Gb Ethernet connection blade must be installed in fabric 3 or in fabric 4 of the system unit.

- If a 10 Gb Ethernet mezzanine card or a 10Gb CNA mezzanine card is installed in slot 2 of a server blade, at least one 10 Gb Ethernet connection blade must be installed in fabric 3 of the system unit.

- If an FC mezzanine card is installed in slot 2, at least one FC connection blade must be installed in fabric 3.

- If a SAS/SAS RAID mezzanine card is installed in slot 2, at least one SAS connection blade must be installed in fabric 3.

- You can install combinations of FC, Ethernet and SAS mezzanine cards in a server blade. In this case, the mezzanine card slots may be equipped as follows:
### Mezzanine cards

<table>
<thead>
<tr>
<th>Mezzanine slot 1</th>
<th>Mezzanine slot 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gb Ethernet</td>
<td>10 Gb Ethernet / 10 Gb CNA</td>
</tr>
<tr>
<td>1 Gb Ethernet</td>
<td>Fibre Channel</td>
</tr>
<tr>
<td>1 Gb Ethernet</td>
<td>SAS/SAS RAID</td>
</tr>
<tr>
<td>10 Gb Ethernet / 10 Gb CNA</td>
<td>Fibre Channel</td>
</tr>
<tr>
<td>10 Gb Ethernet / 10 Gb CNA</td>
<td>SAS/SAS RAID</td>
</tr>
<tr>
<td>Fibre Channel</td>
<td>SAS/SAS RAID</td>
</tr>
</tbody>
</table>

Table 5: Allowed combinations of different mezzanine cards

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

for the global market:  

for the Japanese market:  
Mezzanine cards

Population rules for mezzanine cards in the BX400 S1 system unit

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

![Connection blade slots (BX400 S1 system unit)](image)

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

<table>
<thead>
<tr>
<th>Server blade</th>
<th>Midplane</th>
<th>Connection blade slots</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onboard CNA</td>
<td>Fabric 1</td>
<td>CB1: 1 or 10 Gb Ethernet</td>
</tr>
<tr>
<td>Mezzanine card slot 1</td>
<td>Fabric 2</td>
<td>CB2: 1 or 10 Gb Ethernet or Fibre Channel</td>
</tr>
<tr>
<td>Mezzanine card slot 2</td>
<td>Fabric 3</td>
<td>CB3: 1 or 10 Gb Ethernet or Fibre Channel or SAS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CB4: 1 or 10 Gb Ethernet or Fibre Channel or SAS</td>
</tr>
</tbody>
</table>

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

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

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

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

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

7.2 Installing mezzanine cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

7.2.1 Preliminary steps

Before installing an expansion card, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
7.2.2 Installing a mezzanine card

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

Removing the mezzanine card carrier

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

Figure 44: Removing the riser card

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

Figure 45: Inserting the mezzanine card

- Place the mezzanine card on the two guide pins (see arrows) at the slot of mezzanine card 2 and press the mezzanine card down so that it clicks into place between the two clips (1).
Connect the riser card to the mezzanine card. Make sure that the green clips click into place.

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

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

- Close the server blade, re-insert it in the system unit and switch it on as described in section "Closing the server blade" on page 54 and following.
7.2.3 Concluding steps

Perform the following procedures to complete the task:

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating mezzanine card firmware" on page 79.
- In order to configure a mezzanine card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. For SAN / iSCSI boot the card's Option ROM has to be enabled permanently. If applicable, proceed as described in section "Enabling Option ROM scan" on page 81.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
- If applicable, "After replacing / upgrading LAN/CNA controllers" on page 98.
7.3 Removing mezzanine cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

7.3.1 Preliminary steps

Before removing an expansion card, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
7.3.2 Removing a mezzanine card

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

Removing the mezzanine card carrier

- Remove the carrier from the server blade housing as described in section "Removing the mezzanine card carrier" on page 141.

Figure 48: Removing the riser card

- Remove the riser card from the holder at the slot of mezzanine card 2 as described in section "Removing riser cards" on page 132.
Mezzanine cards

Figure 49: Replacing the mezzanine card

> Press against the two clips (1) and remove the mezzanine card (2).
> Install the new mezzanine card.

Figure 50: Reconnecting the riser card

> Connect the riser card to the mezzanine card. Make sure that the green clips click into place.
> Reinstall the mezzanine card carrier as described in section "Installing the mezzanine card carrier" on page 144.
7.3.3 Concluding steps

Perform the following procedures to complete the task:

► "Closing the server blade" on page 54.
► "Installing the server blade in the system unit" on page 55.
► "Enabling boot watchdog functionality" on page 87.
► "Resuming BitLocker functionality" on page 94.
► If applicable, "After replacing / upgrading LAN/CNA controllers" on page 98.
7.4 Replacing mezzanine cards

Upgrade and Repair Unit (URU)

<table>
<thead>
<tr>
<th>Hardware: 10 minutes</th>
<th>Software: 5 minutes</th>
</tr>
</thead>
</table>

**Tools:** tool-less

7.4.1 Preliminary steps

**Note on network settings recovery**

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

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

Before replacing an mezzanine card, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Onboard indicators and controls" on page 272.

7.4.2 Removing a mezzanine card

- "Removing a mezzanine card" on page 147.

7.4.3 Installing a mezzanine card

- "Installing a mezzanine card" on page 141.
7.4.4 Concluding steps

If applicable, reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard CNA). For further information, please refer to section "Note on network settings recovery" on page 150.

Please refer to the "PRIMERGY BX900/BX400 Blade Server Systems Connection Blade SAS Switch 6 Gb 18/6" manual when exchanging a SAS Expander mezzanine card.

Perform the following procedures to complete the task:

► "Closing the server blade" on page 54.
► "Installing the server blade in the system unit" on page 55.
► "Enabling replaced components in the system BIOS" on page 88.
► "Looking up changed MAC / WWN addresses" on page 96.
► "Updating the NIC configuration file in a Linux environment" on page 93.
► "Updating mezzanine card firmware" on page 79.
► In order to configure a mezzanine card that has been installed or replaced, the card’s Option ROM has to be enabled in the system board BIOS. For SAN / iSCSI boot the card's Option ROM has to be enabled permanently. If applicable, proceed as described in section "Enabling Option ROM scan" on page 81.
► "Enabling boot watchdog functionality" on page 87.
► "Resuming BitLocker functionality" on page 94.
► If applicable, "After replacing / upgrading LAN/CNA controllers" on page 98.
Mezzanine cards
8 Main memory

Safety notes

CAUTION!

● Do not install unsupported third party memory modules. For further information on supported memory modules, refer to section "Basic information" on page 154.

● Memory modules remain hot after shutdown. Wait for components to cool down before installing or removing memory modules to prevent burns.

● Do not insert and remove memory modules repeatedly. Doing so may cause failures.

● Pressing out the securing clips on the memory module connector will eject the installed memory module. To prevent damage and injuries eject memory modules carefully without applying excessive force.

● For further information, please refer to chapter "Important information" on page 29.
Main memory

8.1 Basic information

- The system board is equipped with 24 memory connectors (12 connectors per CPU) for DDR4 DIMM modules.
- In mono processor configurations only 12 memory connectors are usable.
- The system has to be equipped with at least one memory module per processor.
- Supported capacities: 8 GB, 16 GB, 32 GB, 64 GB or 128 GB
- Maximum amount of RAM:
  1536 GB of LRDIMM or 384 GB of RDIMM (for one processor)
  3072 GB of LRDIMM or 768 GB of RDIMM (for two processors)
- Supported memory modules:

<table>
<thead>
<tr>
<th>Type</th>
<th>Ranking(^1)</th>
<th>Error Correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDR4-1600/1866/2133/2400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDIMMs (Registered DIMMs)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>LRDIMMs (Load-Reduced DIMMs)</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

\(^1\) 1R: Single-Rank, 2R: Dual-Rank, 4R: Quad-Rank, 8R: Octa Rank

8.1.1 Memory sequence

8.1.1.1 Population rules

- Populate memory slot 1 / channel A (DIMM 1A) first.
- In case of dual processor configurations, populate memory slot 1 / channel E (DIMM 1E) second.
- Within all channels, memory slot 1 must be populated prior to slot 2. Slot 2 must be populated prior to Slot 3 (for all CPUs).
- If memory modules with different ranks are used, always populate the higher number rank DIMM first (starting from slot 1).
- If memory modules with different capacities are used:
  - Populate modules with higher capacities first.
  - Within a channel, populate modules in descending order of capacity.

- If memory modules with different speeds are used, the lowest clock rate applies for all DIMMs.

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

- Mixing RDIMMs or LRDIMMs is not allowed.
- Mixing ECC and non-ECC DIMMs is not allowed.
- Mixing of quad-rank DIMMs in one channel and three DIMMs in another channel (3DPC) on the same CPU is not allowed. This is not valid for LRDIMMs.

Figure 51: Overview of the slot numbering and the memory channels
## 8.1.1.2 Independent Channel Mode

<table>
<thead>
<tr>
<th>Channel</th>
<th>Color</th>
<th>Slot No. of Modules</th>
<th>1 CPU populated</th>
<th>2 CPUs populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>blue</td>
<td>1A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>blue</td>
<td>1B</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>green</td>
<td>1C</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>blue</td>
<td>2D</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>green</td>
<td>3E</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>blue</td>
<td>2F</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>G</td>
<td>green</td>
<td>3G</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>H</td>
<td>blue</td>
<td>1H</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>I</td>
<td>green</td>
<td>1I</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note: Colors correspond to different components, and the slot and no. of modules indicate the configuration for the CPU.*
Independent Channel Mode using Xeon E5-2637v4, E5-2643v4, E5-2667v4, E5-2697v4, E5-2697Av4 or E5-2699v4

### Notes on Independent Channel Mode
- Due to wider heat sink DIMMs cannot be installed in DIMM slot 3B and DIMM slot 3D.
Main memory

8.1.1.3 Mirrored Channel and Performance Modes

<table>
<thead>
<tr>
<th>CPU Channel</th>
<th>A</th>
<th>B</th>
<th>D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>black</td>
<td>blue</td>
<td>green</td>
<td>black</td>
</tr>
<tr>
<td>Slot 1A</td>
<td>1</td>
<td>2A</td>
<td>3A</td>
<td>1B</td>
</tr>
<tr>
<td></td>
<td>2B</td>
<td>3B</td>
<td>3D</td>
<td>2D</td>
</tr>
<tr>
<td></td>
<td>TD</td>
<td>1D</td>
<td>3C</td>
<td>2C</td>
</tr>
<tr>
<td></td>
<td>1C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU 1 No of Modules</th>
<th>1 CPU populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>8</td>
<td>2 1 2 1</td>
</tr>
<tr>
<td>12</td>
<td>3 2 1 3 2 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU 2 No of Modules</th>
<th>2 CPUs populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>1 3 1 3</td>
</tr>
<tr>
<td>12</td>
<td>3 1 3 1</td>
</tr>
<tr>
<td>16</td>
<td>5 3 5 3 1</td>
</tr>
<tr>
<td>20</td>
<td>5 3 1 5 3 1</td>
</tr>
<tr>
<td>24</td>
<td>5 3 1 5 3 1</td>
</tr>
</tbody>
</table>

Mirrored Channel and Performance Modes using Xeon E5-2637v4, E5-2643v4, E5-2667v4, E5-2697v4, E5-2697Av4 or E5-2699v4

<table>
<thead>
<tr>
<th>CPU Channel</th>
<th>A</th>
<th>B</th>
<th>D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>black</td>
<td>blue</td>
<td>green</td>
<td>black</td>
</tr>
<tr>
<td>Slot 1A</td>
<td>1</td>
<td>2A</td>
<td>3A</td>
<td>1B</td>
</tr>
<tr>
<td></td>
<td>2B</td>
<td>3B</td>
<td>3D</td>
<td>2D</td>
</tr>
<tr>
<td></td>
<td>TD</td>
<td>1D</td>
<td>3C</td>
<td>2C</td>
</tr>
<tr>
<td></td>
<td>1C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU 1 No of Modules</th>
<th>1 CPU populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>8</td>
<td>2 1 2 1</td>
</tr>
<tr>
<td>12</td>
<td>3 2 1 3 2 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU 2 No of Modules</th>
<th>2 CPUs populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>1 3 1 3</td>
</tr>
<tr>
<td>12</td>
<td>3 1 3 1</td>
</tr>
<tr>
<td>16</td>
<td>5 3 5 3 1</td>
</tr>
<tr>
<td>20</td>
<td>5 3 1 5 3 1</td>
</tr>
<tr>
<td>24</td>
<td>5 3 1 5 3 1</td>
</tr>
</tbody>
</table>

Notes on Mirrored Channel and Performance modes

- Always populate memory modules in multiples of 4.
- Same numbers mean identical modules (capacity, rank).
- Due to wider heat sink DIMMs cannot be installed in DIMM slot 3B and DIMM slot 3D.
8.1.1.4 Rank Sparing Mode

Rank Sparing Mode requires identical modules (same capacity and technology) within the same channel.

Single-/Dual-Rank (1R/2R) RDIMMs

<table>
<thead>
<tr>
<th>CPU</th>
<th>CPU 1</th>
<th>CPU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>Color</td>
<td>1A</td>
<td>2A</td>
</tr>
<tr>
<td>Slot</td>
<td>1G</td>
<td>2G</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No. of Modules</th>
<th>1 CPU populated</th>
<th>2 CPUs populated</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 CPUs populated

- CPU 1
- CPU 2
### Main memory

**Rank Sparing Mode using Xeon E5-2637v4, E5-2643v4, E5-2667v4, E5-2697v4, E5-2697Av4 or E5-2699v4**

<table>
<thead>
<tr>
<th>Channel</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>1A</td>
<td>2A</td>
<td>3A</td>
<td>1B</td>
<td>2B</td>
<td>3B</td>
<td>3D</td>
<td>2D</td>
<td>1D</td>
</tr>
<tr>
<td>Slot No. of Modules</td>
<td>1 CPU populated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **1 CPU populated**

- **2 CPUs populated**

- Same numbers mean identical modules (capacity, rank).
- Due to wider heat sink DIMMs cannot be installed in DIMM slot 3B and DIMM slot 3D.

For detailed population rules, refer to section "Notes on Rank Sparing mode" on page 162.
## Rank Sparing Mode with Octa-/Quad-Rank LR-DIMMs

<table>
<thead>
<tr>
<th>CPU 1</th>
<th>CPU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channel</strong></td>
<td><strong>A</strong></td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Slot</strong></td>
<td>1A</td>
</tr>
<tr>
<td><strong>No. of Modules</strong></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
</tr>
</tbody>
</table>

1 CPU populated

2 CPUs populated

<table>
<thead>
<tr>
<th>CPU 1</th>
<th>CPU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channel</strong></td>
<td><strong>A</strong></td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Slot</strong></td>
<td>1A</td>
</tr>
<tr>
<td><strong>No. of Modules</strong></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>1</td>
</tr>
</tbody>
</table>

2 CPUs populated
Main memory

Rank Sparing Mode with Octa-/Quad-Rank LR-DIMMs using Xeon E5-2637v4, E5-2643v4, E5-2667v4, E5-2697v4, E5-2697Av4 or E5-2699v4

Notes on Rank Sparing mode

- Same numbers mean identical modules (capacity, rank).
- Due to wider heat sink DIMMs cannot be installed in DIMM slot 3B and DIMM slot 3D.
- In case of Single-/Dual-Rank memory configurations, at least two 1R or 2R modules must be populated per a channel.
- In case of Octa-/Quad-Rank memory modules, please note the following: Due to performance reasons, always populate a new channel before installing the 3rd memory slot of a channel.
- Only one memory module capacity per CPU is allowed.
If two different memory module capacities have been ordered for Rank Sparing mode, populate them on different CPUs, so that each CPUs only comprises modules of one capacity. See the example on the next page.

*Example:*

12 modules have been ordered, 8 x 4 GB and 4 x 8 GB.
In this case, proceed as follows:

- Use the capacity group with more memory modules for CPU 1 and populate them according to the population sequence for mono CPU configurations.

- Populate the other capacity group on CPU 2 according to the population rules for mono CPU configurations.

In order to satisfy cooling requirements, populate memory channels on alternating sides of the processor:

<table>
<thead>
<tr>
<th>Order</th>
<th>CPU 1</th>
<th>CPU 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Channel A</td>
<td>Channel E</td>
</tr>
<tr>
<td>2</td>
<td>Channel C</td>
<td>Channel G</td>
</tr>
<tr>
<td>3</td>
<td>Channel B</td>
<td>Channel F</td>
</tr>
<tr>
<td>4</td>
<td>Channel D</td>
<td>Channel H</td>
</tr>
</tbody>
</table>
Main memory

8.2 Installing memory modules

Upgrade and Repair Unit (URU)  Hardware: 15 minutes
Software: 5 minutes

Tools: tool-less

8.2.1 Preliminary steps

Before installing a memory module, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- If applicable, "Removing the air cowls" on page 175.

8.2.2 Installing a memory module

- Identify the correct memory slot according to the mounting order described in section "Memory sequence" on page 154.
- If required, remove the mezzanine carrier for better handling of the DIMMs of CPU 1.
Main memory

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

- Align the notch on the bottom of the module with the crossbar in the connector (see close-up).
Press down on the memory module (1) until the securing clips snap into the cutouts at each end of the module (2).

### 8.2.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing the air cowls" on page 174.
- If applicable, "Installing mezzanine cards" on page 140.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating or recovering the system board BIOS and iRMC" on page 72.
- "Enabling boot watchdog functionality" on page 87.
- If applicable, "Verifying the memory mode" on page 89.
- "Resuming BitLocker functionality" on page 94.
8.3 Removing memory modules

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

Tools: tool-less

8.3.1 Preliminary steps

Before removing a memory module, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- If applicable, "Removing the air cowls" on page 175.
8.3.2 Removing a memory module

- Identify the desired memory slot according to the mounting order described in section "Memory sequence" on page 154.

![CAUTION!]
Ensure to maintain an operational configuration when removing memory modules. For additional information, please refer to section "Memory sequence" on page 154.

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

![Figure 55: Removing memory modules]

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

- Remove the ejected memory module.

8.3.3 Concluding steps

Perform the following procedures to complete the task:

- If applicable, "Installing the air cowls" on page 174.

- "Installing the mezzanine card carrier" on page 144.
Main memory

- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating or recovering the system board BIOS and iRMC" on page 72.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
Main memory

8.4 Replacing memory modules

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

Tools: tool-less

8.4.1 Preliminary steps

Before replacing a memory module, perform the following steps:
- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the air cowls" on page 175.
- "Onboard indicators and controls" on page 272.

8.4.2 Removing a memory module

Remove the defective memory module as described in section "Removing a memory module" on page 168.

8.4.3 Installing a memory module

Replace the defective memory module as described in section "Installing a memory module" on page 164.
8.4.4 Concluding steps

Perform the following procedures to complete the task:

► "Installing the air cowls" on page 174.
► "Installing mezzanine cards" on page 140.
► "Closing the server blade" on page 54.
► "Installing the server blade in the system unit" on page 55.
► "Updating or recovering the system board BIOS and iRMC" on page 72.
► "Enabling boot watchdog functionality" on page 87.
► "Enabling replaced components in the system BIOS" on page 88.
► "Verifying the memory mode" on page 89.
► "Resuming BitLocker functionality" on page 94.
Main memory

8.5 Usage of dummy DIMM modules

**CAUTION!**

Empty DIMM sockets have to be filled with dummy DIMM modules (see following figure) to ensure sufficient cooling of the system. The following has to be observed:

- In case only CPU 1 is installed, all empty DIMM slots for CPU 1 have to be equipped with dummy modules. These DIMM slots must be covered with an air cowl (see section "Installing the air cowls" on page 174).

- In case CPU 2 is additionally installed, all empty DIMM slots for CPU 2 also have to be equipped with dummy DIMM modules. These DIMM slots must be covered with an air cowl (see section "Installing the air cowls" on page 174).

![Figure 56: Dummy DIMM module](image)

Dummy DIMM modules are installed and removed in exactly the same way as DIMM modules (as described in sections "Installing a memory module" on page 164 and "Removing a memory module" on page 168).
8.6 Handling of memory air cowls

8.6.1 Basic information

The following figure shows the different types of air cowls:

Figure 57: Air cowl types

<table>
<thead>
<tr>
<th>Air cowl type</th>
<th>#1</th>
<th>#2</th>
<th>#3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 1: only with 135 W heat sink</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 2: with both heat sink types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 1: only with 145 W heat sink and only for DIMMs &quot;A&quot; to &quot;B&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 2: not to be used</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 1: only with 145 W heat sink and only for DIMMs &quot;C&quot; to &quot;D&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 2: not to be used</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CPU 1:
DIMM slots of CPU 1 must be covered with air cowls.

CPU 2:
DIMM slots of CPU 2 must be covered with air cowls.
8.6.2 Installing the air cowls

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

**CAUTION!**

For cooling reasons the air cowls must be installed when operating.
8.6.3 Removing the air cowls

Figure 59: Lifting up the air cowls

- Remove the air cowls from the DIMMs by lifting them up.
Main memory
9 Processors

Safety notes

CAUTION!

- Do not install unsupported processors. For further information on supported processors, refer to section "Basic information" on page 177.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs)
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- When removing or installing the processor, be careful not to touch or bend the spring contacts on the processor socket.
- Never touch the underside of the processor. Even minor soiling such as grease from the skin can impair the processor’s operation or destroy the processor.
- For further information, please refer to chapter "Important information" on page 29.

9.1 Basic information

The system board D3321 offers two sockets for Intel Xeon processors.

Supported processors

- CPU: Intel Xeon processor E5-2600v4 family
- Socket type: LGA2011-3 package
- Thermal Design Power (TDP) class: up to 145 W
9.2 Installing processors

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

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

CAUTION!

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

9.2.1 Preliminary steps

Before installing a processor, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- If applicable, "Removing the mounting frame" on page 115
- If CPU 2 has to be installed, "Removing the "dummy heat sink" of CPU 2" on page 208.
9.2.2 Installing a processor

This description applies to the following procedures:

- Installing the second CPU in a single-processor configuration
- Transferring a CPU after replacing the system board (see section "Removing processors" on page 187 and "Installing processors" on page 178).

Figure 60: Opening socket release lever 1

- Unlatch the socket release lever marked *Open 1st* by pushing it down and away from the socket (1).
- The socket release lever will slightly lift up (2).
Processors

Figure 61: Opening socket release lever 2

- Unlatch the socket release lever marked Close 1st by pushing it down and away from the socket (1).
- Fully fold back the socket release lever marked Close 1st (2).

Figure 62: Opening the load plate (A)

- Push down on the socket release lever marked Open 1st (1) to lift the load plate away from the socket (2).
Figure 63: Opening the load plate (B)

- Fully open the load plate.

**CAUTION!**

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

- Make sure that the load plate is in the fully open position.
Processors

Figure 64: Installing the processor

- Hold the processor with your thumb and index finger.
- Make sure that the four notches on the processor align with the posts on the socket.
- Lower the processor straight down without tilting or sliding it in the socket.

**CAUTION!**

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

When closing the load plate, the protective socket cover will automatically detach.

Remove the socket cover and save it for future use.

**CAUTION!**

Always replace the socket cover if you remove the processor from the socket!
Figure 66: Closing socket release lever 2

- Fully close and hold shut the load plate.
- Close the socket release lever marked *Close 1st* (1) and latch it under the load plate retention tab to lock down the load plate (2).
Close the socket release lever marked *Open 1st* (1) and latch it under the load plate retention tab (2).

- If applicable, install the other processor accordingly.
9.2.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing processor heat sinks" on page 201.
- If applicable, "Installing the mounting frame" on page 115
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating or recovering the system board BIOS and iRMC" on page 72.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
- "Enabling replaced components in the system BIOS" on page 88.
9.3 Removing processors

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

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

**CAUTION!**

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

9.3.1 Preliminary steps

Before removing a processor, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing a memory module" on page 168.
- If applicable, "Removing the mounting frame" on page 115
- "Removing processor heat sinks" on page 207.
9.3.2 Removing a processor

This description applies to the following procedures:

- Removing CPU 2 from a dual-processor configuration
- Removing CPUs from a system board (see section "Removing processors" on page 187)

- Remove the desired processor heat sink as described in section "Removing processor heat sinks" on page 207.

Figure 68: Opening socket release lever 1

- Unlatch the socket release lever marked Open 1st by pushing it down and away from the socket (1).
- The socket release lever will slightly lift up (2).
Unlatch the socket release lever marked *Close 1st* by pushing it down and away from the socket (1).

Fully fold back the second socket release lever (2).

Push down on the socket release lever marked *Open 1st* (1) to lift the load plate away from the socket (2).
Processors

Figure 71: Opening the load plate (B)

► Fully open the load plate.
Carefully remove the defective processor from its socket in a vertical motion.

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

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

**CAUTION!**
Processors are extremely sensitive to electrostatic discharge and must be handled with care. After a processor has been removed from its protective sleeve or from its socket, place it upside down on a nonconducting, antistatic surface. Never push a processor over a surface.
Figure 73: Closing the load plate

- Carefully close the load plate over the empty processor socket.

CAUTION!

Be careful not to touch or bend the spring contacts on the processor socket.
Carefully lower the protective socket cover onto the CPU socket in a vertical motion until it snaps in place.

**CAUTION!**

Always replace the socket cover if you remove the processor from the socket!
Ensure that the protective socket cover is properly installed on the socket as shown above.
Figure 76: Closing socket release lever 2

- Fully close and hold shut the load plate.
- Close the socket release lever marked Close 1st (1) and latch it under the load plate retention tab to lock down the load plate (2).
Close the socket release lever marked *Open 1st* (1) and latch it under the load plate retention tab (2).
9.3.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing processor heat sinks" on page 201.
- If applicable, "Installing the mounting frame" on page 115.
- "Installing a memory module" on page 164.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating or recovering the system board BIOS and iRMC" on page 72.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
9.4 Upgrading or replacing processors

Upgrade and Repair Unit (URU)  Hardware: 15 minutes
Software: 5 minutes

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

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

9.4.1 Preliminary steps

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

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing a memory module" on page 168.
- If applicable, "Removing the mounting frame" on page 115
- "Removing processor heat sinks" on page 207.
9.4.2 Upgrading or replacing a processor

- Remove the desired processor as described in section "Removing processors" on page 187.
- Install the new processor as described in section "Installing processors" on page 178.

9.4.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing processor heat sinks" on page 201.
- If applicable, "Installing the mounting frame" on page 115
- "Installing memory modules" on page 164.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.

Information: After the server has been switched on, an error message like "CPU has been changed" might be generated and Global error indicator might flash. The message neither is to show that the installing CPU composition was changed nor a functional problem. The flashing Global error indicator disappears by selecting "Save change and Exit" or "Save change and Reset" in the BIOS setup utility.

- "Updating or recovering the system board BIOS and iRMC" on page 72.
- "Resetting the error status after replacing memory modules or processors" on page 84.
- "Enabling replaced components in the system BIOS" on page 88.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
9.5  Handling processor heat sinks

Field Replaceable Unit (FRU)  
Hardware: 15 minutes

Upgrade and Repair Unit (URU)

if thermal paste is involved

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

9.5.1  Preliminary steps

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

► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
► If applicable, "Removing the mounting frame" on page 115
► If applicable, "Removing a memory module" on page 168.
9.5.2 Installing processor heat sinks

The figures on the following pages show the different heat sink types for this server blade.

Heat sink types for CPU 1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heat sink for CPUs with a TDP of up to 135 W</td>
</tr>
<tr>
<td>2</td>
<td>Heat sink for CPUs with a TDP of up to 145 W</td>
</tr>
</tbody>
</table>

This heat sink is wider than the one for CPUs with a TDP <= 135 W (see pos. #1 in figure above) and occupies DIMM slots "3B" and "3D" of CPU 1. Therefore, when using this heat sink, you have to use the smaller air cowls (see "Handling of memory air cowls" on page 173).
Processors

Heat sink types for CPU 2

Figure 79: Heat sink types for CPU 2 (with platform for SSDs)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heat sink for CPUs with a TDP of up to 135 W</td>
</tr>
<tr>
<td>2</td>
<td>Heat sink for CPUs with a TDP of up to 145 W</td>
</tr>
</tbody>
</table>

The heat sink for CPUs with a TDP of 145 W has more fins than the one for CPUs with a TDP <= 135 W (see pos. #1 in figure above)
9.5.2.1 Preparing heat sink and processor

When installing a new heat sink

![Heat sink with protective cover](image)

Figure 80: Heat sink with protective cover

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

  **CAUTION!**

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

When reusing a heat sink

- Ensure that all residual thermal paste has been thoroughly cleaned off the copper surface of the heat sink.

- Apply thermal paste to the processor surface as described in section "Applying thermal paste" on page 210.
9.5.2.2 Installing the heat sink for CPU 1

- Align the heat sink with the four threaded holes of the processor socket (see figure 82 on page 205).
- Carefully seat the heat sink on the four threaded holes as shown (see arrows).

**CAUTION!**

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

![Figure 81: Fastening the heat sink for CPU 1](image)

- Keep pressing on the heat sink to prevent it from tilting until two screws (1) and (2) are fixed.
- Fasten the four captive screws (combihexagon) on the heat sink in the following pattern: (1) ->(2) ->(3) ->(4).

**Torque: 0.6 Nm**, not applicable for the Japanese market

- When using the heat sink for CPUs with a TDP of 145 W two memory slots (3B and 3D) are not available.
9.5.2.3 Installing the heat sink for CPU 2

![Image of the heat sink installation process]

- Align the edge of the heat sink with the memory slot levers (see red line).
- Carefully seat the captive screws of the heat sink onto the four threaded holes (see arrows).

**CAUTION!**
- Ensure that the captive screws of the heat sink are properly seated on the threaded holes.
- Ensure that the heat sink cooling fins match the direction of the airflow.
Keep pressing on the heatsink to avoid tilting until the screws (1) and (2) are fixed.

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

**Torque: 0.6 Nm**, not applicable for the Japanese market.
9.5.3 Removing processor heat sinks

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

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

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

- Lift the heat sink out of the chassis.
- Thoroughly clean residual thermal paste from the surface of the heat sink and the processor using a lint-free cloth.
9.5.4 Removing the "dummy heat sink" of CPU 2

In case that no CPU 2 is installed, a "dummy heat sink" has been installed for cooling reasons.

The installation of the "dummy heat sink" has to be done in reverse order.

![Figure 85: Removing the "dummy heat sink" of CPU 2](image)

- Loosen the four captive screws (combihexagon) of the "dummy heat sink" in the following pattern: (4) ->(3) ->(2) ->(1) (see figure).
- Lift the "dummy heat sink" out of the chassis.

**CAUTION!**
Pay special attention not to damage any system board components surrounding the processor socket.
**9.5.5 Replacing processor heat sinks**

**9.5.5.1 Removing the processor heat sink**

- Remove the processor heat sink as described in section "Removing processor heat sinks" on page 207.

**9.5.5.2 Applying thermal paste**

- Apply thermal paste to the processor surface as described in section "Applying thermal paste" on page 210.

**9.5.5.3 Installing the processor heat sink**

- Install the processor heat sink as described in sections "Preparing heat sink and processor" on page 203 and "Installing the heat sink for CPU 1" on page 204.

**9.5.6 Concluding steps**

Perform the following procedures to complete the task:

- If applicable, "Installing a memory module" on page 164.
- If applicable, "Installing the mounting frame" on page 115
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
9.6 Applying thermal paste

Field Replaceable Unit (FRU)  Hardware: 5 minutes

Tool: tool-less

For the Japanese market, the service engineer must follow the instruction provided separately.

If the processor upgrade or replacement kit contains a new CPU heat sink, a thin layer of thermal compound has already been pre-applied to its lower surface. In this case, please proceed with section "Installing processor heat sinks" on page 201.

Figure 86: Thermal paste syringe

One thermal compound syringe contains thermal paste for three processors.
Apply a dot of thermal paste to the center of the processor surface as shown.

Two graduation marks on the syringe equal the correct amount of thermal paste for one processor.

CAUTION!
Do not mix different types of thermal paste.
Processors
10 System board components

Safety notes

CAUTION!

● Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.

● Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).

● Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.

● For further information, please refer to chapter "Important information" on page 29.

10.1 Basic information

● CMOS battery

CMOS memory (volatile BIOS memory) and the real-time clock are powered by a lithium coin cell (CMOS battery). This cell lasts up to ten years, depending on ambient temperature and use.

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

● UFM (USB Flash Module)

The server blade can be equipped with a USB Flash Module (UFM).

● TPM (Trusted Platform Module)

The system board is optionally equipped with a Trusted Platform Module (TPM). This module enables programs from third party manufacturers to store key information, for example drive encryption using Windows Bitlocker Drive Encryption.

● SATA DOM

The server blade can be equipped with a SATA DOM.
System board components

- MicroSD card
  The server blade can be equipped with a microSD card.

10.2 Replacing the CMOS battery

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

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 FUJITSU Server PRIMERGY BX2580 M2 Server Blade Operating Manual.

10.2.1 Preliminary steps

Before replacing the CMOS battery, perform the following steps:

- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
10.2.2 Replacing the battery

The CMOS battery is located on the system board between the CPUs resp. their heat sinks (see following figure).

![Image of system board components showing CMOS battery location]

Figure 88: Location of the CMOS battery on the system board D3321
System board components

Removing the depleted battery

- Rotate the depleted CMOS battery (1).
- Remove the CMOS battery (2).

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

Inserting the new battery

- Insert the fresh CMOS battery taking care of the direction. (3).
- Rotate the fresh CMOS battery up to the vertical. (4).
10.2.3 **Concluding steps**

Perform the following procedures to complete the task:

- Dispose of the CMOS battery in accordance with local regulations concerning special waste.
- "Installing the air cowls" on page 174.
- "Installing mezzanine cards" on page 140.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Verifying the system time settings" on page 90.
- "Restoring BIOS settings" on page 78.
10.3 USB Flash Module (UFM)

10.3.1 Installing the UFM

**Field Replaceable Unit (FRU)**

Hardware: 5 minutes  
Software: 5 minutes

**Tools:** tool-less

10.3.1.1 Preliminary steps

Before installing the UFM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141
10.3.1.2 Installing the UFM

Figure 90: UFM kit

Pre-assembled UFM flash module kit:

1. 8 GB UFM SLC
2. UFM spacer
   - This black spacer will not be used. A white spacer is already mounted instead.
3. UFM nylon screw
UFM mounting location on the system board:

1. UFM multi-pin connector
2. UFM spacer
10.3.1.3 Concluding steps

Perform the following procedures to complete the task:

▶ "Installing the mezzanine card carrier" on page 144.
▶ "Closing the server blade" on page 54.
▶ "Installing the server blade in the system unit" on page 55.
▶ "Enabling boot watchdog functionality" on page 87.
▶ "Resuming BitLocker functionality" on page 94.
10.3.1.4 Software configuration

Please set the license key only for a free version that limits the license key or the function of the VMware vSphere product separately bought according to the product attachment material of UFM when using it.
10.3.2 Removing the UFM

Field Replaceable Unit (FRU)  
Hardware: 5 minutes  
Software: 5 minutes

Tools: Phillips PH0 / (+) No. 0 screw driver

10.3.2.1 Preliminary steps

Before removing the UFM, perform the following steps:

► "Suspending BitLocker functionality" on page 65.
► "Disabling boot watchdog functionality" on page 66.
► "Locating the defective server blade" on page 43.
► "Shutting down the server blade" on page 50.
► "Removing the server blade from the system unit" on page 52.
► "Opening the server blade" on page 53.
► "Removing the mezzanine card carrier" on page 141
10.3.2.2 Removing the UFM

- Remove the nylon screw (see arrow) from the defective UFM.
- Grasp the UFM on its corners, then pull it out gradually and carefully.
  The UFM spacer remains on the system board.

10.3.2.3 Concluding steps

Perform the following procedures to complete the task:
- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Resuming BitLocker functionality" on page 94.
10.3.3 Replacing the UFM

**Upgrade and Repair Unit (URU)**

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

**Tools:**  
– Phillips PH0 / (+) No. 0 screw driver  
– combination pliers and flat nose pliers

10.3.3.1 Preliminary steps

Before replacing the UFM, perform the following steps:

▶ "Suspending BitLocker functionality" on page 65.
▶ "Disabling boot watchdog functionality" on page 66.
▶ "Locating the defective server blade" on page 43.
▶ "Shutting down the server blade" on page 50.
▶ "Removing the server blade from the system unit" on page 52.
▶ "Opening the server blade" on page 53.
▶ "Removing the mezzanine card carrier" on page 141
10.3.3.2 Removing the UFM

Figure 94: Removing the UFM

- Remove the nylon screw (see arrow) from the defective UFM.
- Grasp the UFM on its corners, then pull it out gradually and carefully.
  The UFM spacer remains on the system board.
10.3.3.3 Re-installing the UFM

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

Figure 95: Preparing the new UFM
System board components

Destroying the defective UFM

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

Figure 96: Destroying the defective UFM

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

Perform the following procedures to complete the task:

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.

10.3.3.5 Software configuration

- Please set the license key only for a free version that limits the license key or the function of the VMware vSphere product separately bought according to the product attachment material of UFM when using it.
10.4 Trusted Platform Module (TPM)

10.4.1 Installing the TPM

**Upgrade and Repair Unit (URU)**

- Hardware: 5 minutes
- Software: 5 minutes

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

Installing the TPM:
- Bit screw driver
- TPM bit insert (*)

(*) For the Japanese market:
- TPM module fixing tool (S26361-F3552-L909)

10.4.1.1 Preliminary steps

Before installing the TPM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141.
10.4.1.2 Installing the TPM

The TPM kit consists of:

1. TPM module
2. TPM spacers
   - Use the black TPM spacer.
   - The white TPM spacer is not used in this server.
3. TPM special screw
4. TPM bit insert for TPM special screw
TPM mounting location on the system board:

1. TPM multi-pin connector
2. Cut-out for TPM spacer
System board components

Figure 99: Installing the TPM spacer

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

Figure 100: TPM bit insert

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

Figure 101: Mounting the TPM

- Connect the new TPM to the system board.
- Secure the TPM with the TPM screw (see arrow) using the TPM bit insert (see figure 100 on page 233).

![Image of TPM mounting]

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

10.4.1.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- Enable TPM in the system board BIOS. Proceed as follows:
  - Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.
▶ Switch on or restart your server blade.
▶ As soon as the startup screen appears, press the \[F2\] function key to enter the BIOS.
▶ Select the *Advanced* menu.
▶ Select the *Trusted Computing* submenu.
▶ Set the *TPM Support* and *TPM State* settings to *Enabled*.
▶ Under *Pending TPM operation*, select the desired TPM operation mode.
▶ Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual available online.

▶ "Resuming BitLocker functionality" on page 94.
## 10.4.2 Removing the TPM

<table>
<thead>
<tr>
<th>Field Replaceable Unit (FRU)</th>
<th>Hardware: 30 minutes</th>
</tr>
</thead>
</table>

**Tools:** Removing the system board:
- Phillips PH2 / (+) No. 2 screw driver

Removing the TPM:
- flat nose pliers
- thin slotted screw driver (2 x 0.4 mm)

(*) For the Japanese market:
- Dedicated TPM screw driver (CWZ8291A)

### Note on TPM

The server blade 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 server blade and connected to the new server blade. For a detailed description, please refer to section "Replacing the TPM" on page 240.

The TPM is activated in the system BIOS.

**CAUTION!**
- Before replacing the server blade, 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 server blade the TPM must be enabled. You may not clear the TPM data.

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

Before removing the TPM, perform the following steps:

► Before removing the TPM, it is necessary to remove BitLocker-protection from the computer and to decrypt the volume.

Ask the system administrator to turn off BitLocker-protection using the BitLocker setup wizard available either from the Control Panel or Windows Explorer:

► Open Bitlocker Drive Encryption by clicking the Start button, clicking Control Panel, clicking Security, and then clicking Bitlocker Drive Encryption.

Administrant permission required If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

► To turn off BitLocker and decrypt the volume, click Turn Off BitLocker, and then click Decrypt the volume.

Decrypting the volume may be time-consuming. By decrypting the volume, all of the information stored on that computer is decrypted.

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

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

► Disable TPM in the system board BIOS. Proceed as follows:

► Open a virtual console for your server blade as described in section "Launching a video redirection to a server blade" on page 61.

► Switch on or restart your server blade.

► As soon as the startup screen appears, press the [F2] function key to enter the BIOS.

► Select the Advanced menu.

► Select the Trusted Computing submenu.

► Set the TPM Support and TPM State settings to Disabled.

► Save your changes and exit the BIOS.
For detailed information on how to access the BIOS and modify settings, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual available online.

- Locate the desired server blade as described in section "Locating the defective server blade" on page 43.
- Shut down the server blade as described in section "Shutting down the server blade" on page 50.
- Remove the server blade from the system unit as described in section "Removing the server blade from the system unit" on page 52.
- Open the server blade as described in section "Opening the server blade" on page 53.
- Remove the mezzanine cards carrier as described in section "Removing the mezzanine card carrier" on page 141.

10.4.2.2 Removing the TPM

- Remove the system board as described in section "Removing the system board" on page 257.
- Lay the system board on a soft, antistatic surface with its component side facing down.

Figure 102: Removing the TPM screw from the underside of the system board

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

Ensure to turn the screw **clockwise** in order to remove it!

Slowly and carefully increase the pressure on the screw until it begins to turn. The effort when loosing the screw should be as low as possible.

Otherwise the thin metal bar may break, rendering it impossible to loosen the screw.

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

### 10.4.2.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
10.4.3 Replacing the TPM

Field Replaceable Unit (FRU)

Tools: Removing the system board:
- Phillips PH2 / (+) No. 2 screw driver

Replacing the TPM:
- Bit screw driver
- TPM bit insert (*)
- flat nose pliers
- thin slotted screw driver (2 x 0.4 mm) (*)

(*) For 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 will cause to lose all data.
10.4.3.1 Preliminary steps

Before replacing the TPM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141
- "Removing the system board" on page 257.

10.4.3.2 Removing the TPM

Remove the TPM as described in section "Removing the TPM" on page 236.

10.4.3.3 Re-installing the TPM

The TPM spacer is already present on the system board.

Re-install the TPM as described in section "Installing the TPM" on page 230.

10.4.3.4 Concluding steps

Perform the following procedures to complete the task:

- "Installing the system board" on page 259.
- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Resuming BitLocker functionality" on page 94.
System board components

10.5  SATA DOM

10.5.1  Installing the SATA DOM

Upgrade and Repair Unit (URU)  Hardware: 10 minutes
Software: 5 minutes

Tools: Phillips PH1 / (+) No. 1 cross-head screwdriver

10.5.1.1  Preliminary steps

Before installing the SATA DOM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141
**10.5.1.2 Mounting the SATA-DOM**

Optionally a SATA DOM (DOM = Disk on module) can be installed. The connector for the SATA DOM is located under the slot for mezzanine card 1.

Figure 103: SATA DOM

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Nylon screw</td>
</tr>
<tr>
<td>2</td>
<td>Connector with release clip</td>
</tr>
<tr>
<td>3</td>
<td>Plastic post (already mounted on the system board)</td>
</tr>
</tbody>
</table>

The nylon spacer that comes with the SATA DOM Kit is not used for this server blade. Use the nylon spacer already mounted on the system board.
System board components

Figure 104: Inserting the SATA DOM

- Insert the SATA DOM into the SATA connector on the system board until it snaps into place (1).
- Fix the SATA DOM with the nylon screw (2). Torque: **0.06 Nm**

  Not applicable for the Japanese market.
10.5.1.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
System board components

10.5.2 Removing the SATA-DOM

Upgrade and Repair Unit (URU)  Hardware: 10 minutes
Software: 5 minutes

Tools: Phillips PH1 / (+) No. 1 cross-head screwdriver

10.5.2.1 Preliminary steps

Before removing the SATA-DOM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141
10.5.2.2 Removing the SATA DOM

Figure 105: Removing the SATA DOM

- Remove the nylon screw (1).
- Press on the clip (2) and lift up the SATA DOM out of the SATA connector in order to remove it from the system board.

10.5.2.3 Concluding steps

Perform the following procedures to complete the task:

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
System board components

10.5.3 Replacing the SATA-DOM

Upgrade and Repair Unit (URU)  Hardware: 5 minutes
Software: 5 minutes

Tools: Phillips PH1 / (+) No. 1 cross-head screwdriver

10.5.3.1 Preliminary steps

Before replacing the SATA-DOM, perform the following steps:

- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141

10.5.3.2 Removing the SATA DOM

- "Removing the SATA-DOM" on page 246.

10.5.3.3 Installing the SATA DOM

- "Installing the SATA DOM" on page 242.

10.5.3.4 Concluding steps

Perform the following procedures to complete the task:

Only for the Japanese market:
Please make sure to return the nylon spacer with a removed SATA DOM.

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
System board components

- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
10.6  iRMC microSD card

10.6.1 Installing the iRMC microSD card

![Upgrade and Repair Unit (URU)](image)

**Tools:** tool-less

**Hardware:** 5 minutes

10.6.1.1 Preliminary steps

- "Shutting down the server blade" on page 50
- "Removing the server blade from the system unit" on page 52
- "Opening the server blade" on page 53
- "Removing the mezzanine card carrier" on page 141
10.6.1.2 Installing the iRMC microSD card

The terminal side of the Micro SD card is upward, insert the iRMC microSD card into the microSD card slot (1) as far as it will go (2).

- The onboard position of the microSD card slot can be found in section "Server blade interior" on page 268.
10.6.1.3 Concluding steps

- "Installing the mezzanine card carrier" on page 144.
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.

10.6.2 Removing the iRMC microSD card

Upgrade and Repair Unit (URU)

Average task duration: 5 minutes

**Tools:** Side-cutting pliers

10.6.2.1 Preliminary steps

- "Shutting down the server blade" on page 50
- "Removing a server blade" on page 51
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141
10.6.2.2 Removing the iRMC microSD card

![Image of iRMC microSD card being removed](image)

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.

10.6.2.3 Concluding steps

- "Installing the mezzanine card carrier" on page 144
- "Closing the server blade" on page 54
- "Installing the server blade in the system unit" on page 55
System board components

10.6.3 Replacing the iRMC microSD card

Upgrade and Repair Unit (URU) Average task duration: 5 minutes

Tools: Side-cutting pliers

10.6.3.1 Preliminary steps

- "Shutting down the server blade" on page 50
- "Removing a server blade" on page 51
- "Opening the server blade" on page 53.
- "Removing the mezzanine card carrier" on page 141

10.6.3.2 Replacing the iRMC microSD card

- Remove the defective iRMC microSD card as described in section "Removing the iRMC microSD card" on page 252.
- Install the new iRMC microSD card as described in section "Installing the iRMC microSD card" on page 250.

10.6.3.3 Concluding steps

- "Installing the mezzanine card carrier" on page 144
- "Closing the server blade" on page 54
- "Installing the server blade in the system unit" on page 55
10.7 Replacing the system board

Field Replaceable Unit (FRU) Hardware: 50 minutes

Software: 10 minutes

Tools:
- Phillips PH2 / (+) No. 2 screw driver
- Magnifying glass for inspecting processor socket springs (recommended)

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)

If a UFM is installed:
- Phillips PH1 / (+) No. 1 screw driver

Note on TPM

The system board can be equipped with an optional TPM (Trusted Platform Module). This module enables third party programs to store key information (e.g. drive encryption using Windows Bitlocker Drive Encryption).

If the customer is using TPM functionality, the TPM has to be removed from the defective system board and connected to the new system board. For a detailed description, please refer to section "Replacing the TPM" on page 240.

The TPM is activated in the system BIOS.

CAUTION!
- Before replacing the system board, ask the customer whether TPM functionality is used.
System board components

- If the customer is using TPM functionality, remove the TPM from the old system board and install it on the new system board.

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

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

Note on system information backup / restore

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

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

10.7.1 Preliminary steps

Before replacing the system board, perform the following steps:

- "Note on network settings recovery" on page 150.
- "Saving BIOS settings" on page 63
- "Saving iRMC settings" on page 63
- "Suspending BitLocker functionality" on page 65.
- "Disabling boot watchdog functionality" on page 66.
- "Locating the defective server blade" on page 43.
- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- "Opening the server blade" on page 53.
10.7.2 Removing the system board

- Remove the following components from the system board as shown in the related sections:
  - Solid state drives: see section "Removing the mounting frame" on page 115
  - Heat sink: see section "Removing processor heat sinks" on page 207 and, if applicable "Removing the "dummy heat sink" of CPU 2" on page 208.
    - Leave the processor on the defective board for now.
  - Memory modules: refer to section "Removing memory modules" on page 167
    - Ensure to take note of the memory modules’ mounting positions for reassembly.
  - Mezzanine cards: refer to the section "Removing the mezzanine card carrier" on page 141
  - UFM: refer to section "Removing the UFM" on page 223
  - SATA DOM: refer to section "Removing the SATA-DOM" on page 246
  - iRMC microSD card: refer to section "Removing the iRMC microSD card" on page 252
System board components

Figure 109: Detaching the system board (A)

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

Figure 110: Detaching the system board (B)

- Carefully shift the system board to the rear (see arrow) in order to detach it from the centering bolts (see circles).
- Hold the system board by the memory module ejectors and at a slight angle lift it out of the chassis.
- If applicable, remove the TPM as described in section "Removing the TPM" on page 238.
10.7.3 Installing the system board

Mounting the system board

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

Lower the system board onto the centering bolts (see circles). Ensure that the system board is properly seated on the centering bolts.

Carefully shift the system board towards the server front as far as it will go (see arrow).
System board components

Figure 112: Installing the system board (B)

- Secure the system board with the screw (M3 x 6 mm, see circle).
  - **Torque: 0.6 Nm** (not applicable for the Japanese market)

- Verify the settings on the new system board (jumpers and/or switch).
  - For a detailed description, please refer to section "Onboard settings" on page 271.

**Swapping the processor**

- Carefully remove the processor from its socket on the defective system board as described in section "Removing processors" on page 173.
  - **CAUTION!**
    - Be careful not to touch or bend the pins on the processor socket!
  - Always replace the socket cover if you remove the processor from the socket.

- Install the processor on the new system board as described in section "Installing processors" on page 178.
  - Since the defective system board is sent back for repair, protect the delicate processor socket springs with a socket cover.
10.7.4 Concluding steps

- Reinstall all remaining system board components as shown in the related sections:
  - Heat sinks: see section "Installing processor heat sinks" on page 201 and, if applicable, in reverse order: "Removing the "dummy heat sink" of CPU 2" on page 208.
  - Solid state drives: see section "Installing the mounting frame" on page 115
  - "Installing memory modules" on page 164
    - Install the memory modules into their original slots.
  - "Installing the TPM" on page 230
  - "Installing the UFM" on page 218
  - "Installing the SATA DOM" on page 242
  - "Installing the iRMC microSD card" on page 250
  - "Installing the mezzanine card carrier" on page 144
- "Closing the server blade" on page 54.
- "Installing the server blade in the system unit" on page 55.
- "Updating or recovering the system board BIOS and iRMC" on page 72.
- If applicable, "Enabling Option ROM scan" on page 81.
- If applicable, activate TPM functionality in the system BIOS under Security > TPM (Security Chip) Setting > Security Chip. For more information, refer to the "D3321 BIOS Setup Utility for FUJITSU Server PRIMERGY BX2580 M2" reference manual.
- "Verifying the system time settings" on page 90.
- "Looking up changed MAC / WWN addresses" on page 96.
- "Updating the NIC configuration file in a Linux environment" on page 93.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
- If applicable, "After replacing the server blade" on page 98.
System board components

- "Performing a RAID array rebuild" on page 95.
- "Restoring BIOS settings" on page 78
- "Restoring iRMC settings" on page 79
- If applicable, "Note on network settings recovery" on page 150.
11 Server blade

11.1 Replacing the server blade

Field Replaceable Unit (FRU)          Hardware: 50 minutes
Software: 10 minutes

Tools: tool-less

11.1.1 Preliminary steps

Note on network settings recovery

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

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

► "Suspending BitLocker functionality" on page 65.
► "Disabling boot watchdog functionality" on page 66.
► "Saving BIOS settings" on page 63.
► "Saving iRMC settings" on page 63.
► "Verifying and configuring the backup software solution" on page 82.
► Exit all applications and shut down the server blade correctly. If your operating system has not switched off the server blade, press the on/off button on the server blade control panel.
► "Locating the defective server blade" on page 43.
► "Removing a server blade" on page 51.
Server blade

11.1.2 Replacing steps

- Open both server blades, see section "Opening the server blade" on page 53.

- Remove the mounting frames with the SSDs, see section "Removing the mounting frame" on page 115.

- Remove the heat sinks and the processors from the defective server blade and install it into the new server blade, see section "Handling processor heat sinks" on page 200 and install it into the new server blade, see section "Upgrading or replacing processors" on page 198.

- Remove the mezzanine card carrier with the installed mezzanine card(s) from the defective server blade, see section "Replacing mezzanine cards" on page 150.

- Remove the memory modules from the defective server blade and install it into the new server blade, see section "Replacing memory modules" on page 170.

- If a UFM is installed, remove it from the defective server blade and install it into the new server blade, see section "USB Flash Module (UFM)" on page 218.

- If a TPM is installed, remove it from the defective server blade and install it into the new server blade, see section "Trusted Platform Module (TPM)" on page 230.

- If a SATA DOM is installed, remove it from the defective server blade and install it into the new server blade, see section "SATA DOM" on page 242.

- If an iRMC microSD card is installed, remove it from the defective server blade and install it into the new server blade, see section "iRMC microSD card" on page 250.

- Install the mezzanine card carrier into the new server blade, see section "Replacing mezzanine cards" on page 150.

- Use the cover from the defective server blade and close the server blade, see section "Closing the server blade" on page 54. Use the cover from the defective server blade because the COA label is stuck there.

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

Note on network settings recovery

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

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

- "Installing the server blade in the system unit" on page 55.
- "Restoring BIOS settings" on page 78

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

- "Restoring iRMC settings" on page 79.
- "Enabling boot watchdog functionality" on page 87.
- "Resuming BitLocker functionality" on page 94.
12 Appendix

12.1 Mechanical overview

12.1.1 Server blade front

Figure 113: PRIMERGY BX2580 M2 server blade front

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ID card</td>
</tr>
<tr>
<td>2</td>
<td>Y-cable connector</td>
</tr>
<tr>
<td>3</td>
<td>Front panel (buttons and indicators)</td>
</tr>
<tr>
<td>4</td>
<td>USB connector</td>
</tr>
</tbody>
</table>
Appendix

12.1.2 Server blade interior

Figure 114: PRIMERGY BX2580 M2 interior (example: no CPU 2 installed)

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SATA DOM</td>
</tr>
<tr>
<td>2</td>
<td>Slot for mezzanine card 1</td>
</tr>
<tr>
<td>3</td>
<td>Memory modules for CPU 1</td>
</tr>
<tr>
<td>4</td>
<td>CPU 1 processor / heat sink</td>
</tr>
<tr>
<td>5</td>
<td>SSD 1</td>
</tr>
<tr>
<td>6</td>
<td>Memory modules for CPU 2</td>
</tr>
<tr>
<td>7</td>
<td>CPU 2 processor / heat sink (with SSD platform)</td>
</tr>
<tr>
<td>8</td>
<td>SSD 0</td>
</tr>
<tr>
<td>9</td>
<td>CSS button</td>
</tr>
<tr>
<td>10</td>
<td>CMOS battery</td>
</tr>
<tr>
<td>11</td>
<td>Onboard USB port</td>
</tr>
<tr>
<td>12</td>
<td>Slot for mezzanine card 2</td>
</tr>
<tr>
<td>13</td>
<td>UFM</td>
</tr>
<tr>
<td>14</td>
<td>TPM</td>
</tr>
<tr>
<td>15</td>
<td>MicroSD card</td>
</tr>
</tbody>
</table>
12.2 Configuration tables

12.2.1 Memory configuration table

Please refer to chapter "Main memory" on page 153.

12.2.2 Mezzanine card configuration table

Please refer to chapter "Population rules for mezzanine cards" on page 134.
Appendix

12.3 Connectors and indicators

12.3.1 Connectors and indicators on the system board

12.3.1.1 Onboard connectors

Figure 115: Internal connectors of system board D3321

<table>
<thead>
<tr>
<th>No.</th>
<th>Print</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>SATA DOM</td>
<td>Connector for SATA DOM</td>
</tr>
<tr>
<td>B</td>
<td>Mezz 1</td>
<td>Connector for mezzanine card 1</td>
</tr>
<tr>
<td>C</td>
<td>DIMM</td>
<td>Connectors for memory modules</td>
</tr>
<tr>
<td>D</td>
<td>SSD 1</td>
<td>Connector for SSD 1</td>
</tr>
<tr>
<td>E</td>
<td>SSD 0</td>
<td>Connector for SSD 0</td>
</tr>
<tr>
<td>F</td>
<td>Dongle USB</td>
<td>Connector for onboard USB port</td>
</tr>
<tr>
<td>G</td>
<td>Mezz 2</td>
<td>Connector for mezzanine card 2</td>
</tr>
<tr>
<td>H</td>
<td>TPM</td>
<td>Connector for TPM</td>
</tr>
<tr>
<td>I</td>
<td>UFM</td>
<td>Connector for UFM</td>
</tr>
</tbody>
</table>
12.3.1.2 Onboard settings

**Figure 116: Onboard settings on system board D3321**

<table>
<thead>
<tr>
<th>Switch</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1</td>
<td>On</td>
<td>CMOS clear</td>
</tr>
<tr>
<td>Switch 2</td>
<td>On</td>
<td>Clear Password</td>
</tr>
<tr>
<td>Switch 3</td>
<td>On</td>
<td>System BIOS recovery / NVRAM clear</td>
</tr>
<tr>
<td>Switch 4</td>
<td>On</td>
<td>ME_RCVR (for service personnel only)</td>
</tr>
</tbody>
</table>

**Default settings: Switch 1 to 4 = Off**
Appendix

12.3.1.3 Onboard indicators and controls

Figure 117: Onboard indicators and Indicate CSS button

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indicate CSS button</td>
</tr>
</tbody>
</table>

Using the Indicate CSS button

- Shut down the server blade as described in section "Shutting down the server blade" on page 50.
- Remove the server blade from the system unit as described in section "Removing the server blade from the system unit" on page 52.
- Open the server blade as described in section "Opening the server blade" on page 53.
- Press the Indicate CSS button (1) to highlight defective components.

Component LEDs

The LEDs C to G are visible from the outside. All other LEDs are only visible if the server blade has been opened. In order to access memory LEDs (B), the air cowls need to be removed (see section "Removing the air cowls" on page 175).
<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Mezzanine card 1</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>yellow on</td>
</tr>
<tr>
<td>B</td>
<td>Memory modules</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>yellow on</td>
</tr>
<tr>
<td>C</td>
<td>Fabric 3/4</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green flashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green on</td>
</tr>
<tr>
<td>D</td>
<td>Fabric 2</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green flashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green on</td>
</tr>
<tr>
<td>E</td>
<td>Fabric 1</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green flashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>green on</td>
</tr>
<tr>
<td>F</td>
<td>CSS</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>orange flashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>orange on</td>
</tr>
<tr>
<td>G</td>
<td>Global Error</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>orange flashing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>orange on</td>
</tr>
<tr>
<td>H</td>
<td>Mezzanine card 2</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>yellow on</td>
</tr>
</tbody>
</table>
## Appendix

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>CPU 1</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPU 1 operational</td>
</tr>
<tr>
<td></td>
<td>yellow on</td>
<td>CPU 1 failure</td>
</tr>
<tr>
<td>J</td>
<td>CPU 2</td>
<td>off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPU 2 operational</td>
</tr>
<tr>
<td></td>
<td>yellow on</td>
<td>CPU 2 failure</td>
</tr>
</tbody>
</table>
12.3.2 Connectors and indicators on the front panel

12.3.2.1 Front panel connectors

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y-cable port</td>
</tr>
<tr>
<td>2</td>
<td>USB connector</td>
</tr>
</tbody>
</table>

Figure 118: Front panel connectors
12.3.2.2 Front panel indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric 3/4</td>
<td>off</td>
<td>Fabric 3/4 no network connection</td>
</tr>
<tr>
<td></td>
<td>green flashing</td>
<td>Fabric 3/4 an active network connection</td>
</tr>
<tr>
<td></td>
<td>green on</td>
<td>Fabric 3/4 network connection</td>
</tr>
</tbody>
</table>

Figure 119: I/O panel indicators
### Indicator Status Description

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Fabric 2</td>
<td>off</td>
<td>Fabric 2 no network connection</td>
</tr>
<tr>
<td></td>
<td>green flashing</td>
<td>Fabric 2 an active network connection</td>
</tr>
<tr>
<td></td>
<td>green on</td>
<td>Fabric 2 network connection</td>
</tr>
<tr>
<td>3 Fabric 1</td>
<td>off</td>
<td>Fabric 1 no network connection</td>
</tr>
<tr>
<td></td>
<td>green flashing</td>
<td>Fabric 1 an active network connection</td>
</tr>
<tr>
<td></td>
<td>green on</td>
<td>Fabric 1 network connection</td>
</tr>
<tr>
<td>4 CSS indicator</td>
<td>off</td>
<td>System is ok</td>
</tr>
<tr>
<td></td>
<td>orange on</td>
<td>A prefailure event was detected for a CSS component that you can fix yourself (for reasons of precaution) with the CSS concept.</td>
</tr>
<tr>
<td></td>
<td>orange flashing</td>
<td>An error was detected that you can fix yourself with the CSS concept.</td>
</tr>
<tr>
<td>5 Global error indicator</td>
<td>off</td>
<td>No critical event</td>
</tr>
<tr>
<td></td>
<td>orange on</td>
<td>A prefailure event has been detected that requires (precautionary) service intervention.</td>
</tr>
<tr>
<td></td>
<td>orange flashing</td>
<td>An error was detected that requires service intervention.</td>
</tr>
<tr>
<td>6 ID indicator</td>
<td>blue on</td>
<td>Server has been highlighted using management blade web interface, ServerView Operations Manager, or the ID button on the front panel for easy identification.</td>
</tr>
</tbody>
</table>
### Power-on indicator

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No mains voltage is present.</td>
<td></td>
</tr>
<tr>
<td>Light-green/orange flashing</td>
<td>iRMC booting. After present the server to the mains (system unit is switched on / after mains failure) the iRMC will boot. The system cannot be switched on, until the iRMC boot sequence is complete. During this time, the power-on indicator will flash light-green/orange.</td>
<td></td>
</tr>
<tr>
<td>Green on</td>
<td>Server is switched on.</td>
<td></td>
</tr>
<tr>
<td>Orange on</td>
<td>Server is switched off, but mains voltage is present (standby mode).</td>
<td></td>
</tr>
<tr>
<td>Light-green on</td>
<td>Power-on delay. After shutting down, the server cannot be switched on again right away. If the On/Off button is pressed right after shutting down the server, the power-on indicator will light up light-green until the delay period ends and the server will boot. If line voltage is insufficient, the server cannot be switched on. If the On/Off button is pressed in this state, the power-on indicator will light up light-green.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix

12.4 Minimum startup configuration

Field Replaceable Units (FRU)

If the server blade does not start up or other problems occur, it may be necessary to take the system down to its most basic configuration in order to isolate the defective component.

The minimum startup configuration consists of the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Notes and reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>BX2580 M2 server blade</td>
<td></td>
</tr>
<tr>
<td>1 CPU with heat sink</td>
<td>Installed in slot CPU 1, see section &quot;Basic information&quot; on page 101.</td>
</tr>
<tr>
<td>1 memory module</td>
<td>Installed in socket DIMM 1A, see section &quot;Basic information&quot; on page 154.</td>
</tr>
</tbody>
</table>

Table 7: Minimum startup configuration - components

- "Shutting down the server blade" on page 50.
- "Removing the server blade from the system unit" on page 52.
- Take the server blade down to its minimum startup configuration.
- "Installing the server blade in the system unit" on page 55.
- "Switching on the server blade" on page 58.
- "Accessing the management blade web interface" on page 41.